Time-Frequency Quantum Key Distribution: Numerical Assessment and Implementation over a Free-Space Link

Dissertation
zur Erlangung des akademischen Grades
doctor rerum naturalium
(Dr. rer. nat.)

Im Fach Physik: Experimentalphysik

Eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät
der
Humboldt-Universität zu Berlin

von

M. Sc. Jasper Rödiger

Präsidentin der Humboldt-Universität zu Berlin:
Prof. Dr.-Ing. Dr. Sabine Kunst

Dekan der Mathematisch-Naturwissenschaftlichen Fakultät:
Prof. Dr. Elmar Kulke

Gutachter/innen:	1. Prof. Dr. rer. nat. Oliver Benson 2. Prof. Dr.-Ing. Ronald Freund 3. Prof. Dr. Harald Weinfurter
Tag der mündlichen Prüfung:	17. Dezember 2019

Abstract

Quantum key distribution (QKD), the first applicable quantum technology, promises information theoretically secure communication. In the presented work the time-frequency (TF)-QKD protocol was examined, which uses time and frequency, namely pulse position modulation (PPM) in the time domain and frequency shift keying (FSK) in the frequency domain as the two complementary bases. Its security relies on the quantum properties of light and the time-frequency uncertainty relation.

TF-QKD can be implemented mostly with standard telecom-technology in the 1550 nm band. The PPM basis can be implemented with modulators and the FSK basis with help of wavelength-division multiplexing technology. The TF-QKD protocol is capable of providing an arbitrarily large alphabet enabling more than 1 bit/photon. Moreover, it is robust in the atmosphere making it suitable for transmission over the free-space channel.

In the present work the TF-QKD protocol is assessed theoretically, implemented with off-the-shelf components for 1 bit/photon and free-space transmission with optical tracking over a 388 m testbed is demonstrated in daylight. Using components at hand, secret key rates of 364 kbit/s back-to-back and 9 kbit/s over the free-space channel could be demonstrated.

Zusammenfassung

Die Quantenschlüsselverteilung (QKD), die erste anwendbare Quantentechnologie, verspricht informationstheoretisch sichere Kommunikation. In der vorliegenden Arbeit wurde das Zeit-Frequenz (TF)-QKD-Protokoll untersucht, das Zeit und Frequenz, nämlich Puls-Positionsmodulation (PPM) im Zeitbereich und Frequenzumtastung (FSK) im Frequenzbereich als die beiden komplementären Basen verwendet. Seine Sicherheit beruht den Quanteneigenschaften von Licht und auf der Zeit-Frequenz-Unschärferelation.

TF-QKD kann mit größtenteils Standard-Telekommunikationstechnologie im 1550-nm-Band implementiert werden. Die PPM-Basis kann mit Modulatoren und die FSK-Basis mit Hilfe der Wellenlängenmultiplex-Technologie realisiert werden. Das TF-QKD-Protokoll ist in der Lage, ein beliebig großes Alphabet bereitzustellen, was mehr als 1 bit/Photon ermöglicht. Darüber hinaus ist es robust gegenüber athmosphärischen Störungen und somit für die Übertragung über den Freiraumkanal geeignet.

In der vorliegenden Arbeit wird das TF-QKD-Protokoll theoretisch bewertet, mit Standardkomponenten für 1 bit/Photon implementiert und die Freiraumübertragung mit optischem Tracking über eine 388 m Teststrecke wird bei Tageslicht demonstriert. Unter Verwendung der vorhandenen Komponenten konnte eine sichere Schlüsselrate von 364 kbit/s back-to-back und 9 kbit/s über den Freiraumkanal demonstriert werden.

Contents

1. Introduction **1**

2. Essentials **5**
2.1. Quantum Key Distribution 5
2.1.1. The BB84 Protocol 7
2.1.2. The Time-Frequency QKD-Protocol 8
2.1.3. Decoy state protocols 9
2.2. Information and probabilities 10
2.2.1. Probabilities 10
2.2.2. Quantum bit and symbol error rate 13
2.2.3. Mutual information 13
2.2.4. Post processing 14
2.3. Free-space transmissions 16
2.3.1. Coupling of Gaussian beams 17
2.3.2. Influence of the atmosphere 18

3. Numerical Analysis of TF-QKD **21**
3.1. Pulse and bin relationships and basic definitions 21
3.2. One-level intercept/resend attack 26
3.2.1. Undisturbed QKD transmission 26
3.2.2. Leakage to the eavesdropper 28
3.2.3. Influence of eavesdropping on the receiver 30
3.2.4. Secret capacity 31
3.2.5. Conclusion on the one-level intercept/resend attack 32
3.3. two-level intercept/resend attack 33
3.3.1. Modification of the eavesdropping strategy 34
3.3.2. Additional information for the eavesdropper 34
3.3.3. Optimizing the symbol pulses 37
3.3.4. Optimize the conjugated pulses 39
3.3.5. Numerical Optimization Results 39
3.4. Secret key rate calculation for implemented systems 42
3.5. Conclusion on numerical analysis 44

4. Implementation of the QKD Setup **45**
4.1. TF-QKD setup 46
4.1.1. Alice's setup 46
4.1.2. Bob's Setup 51
4.2. Phase adjustment of control signals 53
4.3. Conclusion on the TF-QKD setup implementation 54

5. Experimental TF-QKD in a back-to-back configuration **57**
5.1. Procedure for TF-QKD transmissions 57
5.1.1. Preparatory procedure 57
5.1.2. TF-QKD transmission evaluation 60
5.2. Experimental back-to-back transmission of TF-QKD 62
5.2.1. Pulse parameters for the back-to-back experiment 62
5.2.2. Loss dependent distance measurement 63
5.2.3. Gate width optimization 66
5.3. Conclusion on TF-QKD in back-to-back configuration 72

6. Experimental Free-Space TF-QKD over a 388 Meter Link **73**
6.1. Implementing optical tracking for the TF-QKD setup 73
6.1.1. Optical tracking antennas 74
6.1.2. Beacon signal and filtering 75
6.1.3. The free-space test-bed 80
6.2. Experimental TF-QKD over a 388 m free-space link 82
6.2.1. Pulse parameters for TF-QKD over free-space 82
6.2.2. TF-QKD with tracking 82
6.2.3. TF-QKD performance over free-space 85
6.2.4. Comparison of free-space with back-to-back experiment . . . 90
6.3. Conclusion on the free-space TF-QKD transmission 92

7. Conclusion **93**

A. Appendix **97**
A.1. Properties of conditional probability for wrong basis measurement . 97
A.2. Towards a higher alphabet: Four symbols per basis 98
A.3. Free-space transmission: Additional calculations 100
A.3.1. Filtering calculations for separating QKD and beacon signal 100
A.3.2. Losses caused by windows transition 100

Acronyms **103**

Bibliography **105**

Relevant Own Publications **121**

Other Own Publications **122**

Supervised Master Theses **122**

List of Figures **125**

List of Tables **127**

Danksagung **129**

1. Introduction

In the modern interconnected world, secure communication becomes increasingly important. Nowadays, secure communication is mostly addressed by cryptographic algorithms or ciphers, which utilize certain problems, e.g. prime factorization or finding discrete logarithms, which a classical computer can only solve in a huge amount of time. Prime examples are on the one hand asymmetric ciphers like RSA [1], Diffie-Hellman [2] or Elliptic Curve Cryptography [3, 4] or on the other hand symmetric ciphers such as AES [5]. However, some of those cryptographic algorithms are threatened.

A fully functioning quantum computer [6] could be developed, which could use quantum algorithms, which outperform those running on classical computers in some applications. The most eminent of those algorithms is Shor's algorithm [7–10], which can perform prime factorization and find discrete logarithms in sub-exponential time and can thus break e.g. RSA, Diffie-Hellman and Elliptic Curve Cryptography. Symmetric cryptographic algorithms like AES might not be at danger directly by Shor's algorithm; however, the symmetric keys necessary are usually distributed via asymmetric ciphers.

Implementing a quantum computer is surely an ambitious undertaking, however, many research groups work on it at the moment, including groups in big companies such as IBM [11,12], Microsoft [12,13] and Google [14,15], which push the quantum computer further towards practical applications.

Even without a usable quantum computer, the assumptions cryptographic algorithms are based on might be flawed. New methods could be developed to break these algorithms, as has happened already in the past [16–18].

The only provable secure cryptography scheme – also in the presence of quantum computers – is the one-time pad method, also called Vernam cipher [19], where a random key (called the one-time pad), which is as long as the message and is only used once, encrypts and decrypts a secret message. When distributing keys in person is not an option, quantum key distribution (QKD) serves as a potentially unconditionally secure method to distribute the key. Together with the one-time pad method, QKD makes unconditionally secure communication possible.

The BB84 protocol named after its founders Bennett and Brassard and the year the protocol was published is historically the first proposed QKD-protocol [20]. Since the introduction of the BB84 protocol many more QKD protocols

were proposed, investigated and implemented, making QKD the most advanced quantum technology today.

One of the main challenges of QKD is, that the key rate diminishes with increased transmission loss, in other words with the transmission distance and cannot be amplified due to the no-cloning theorem. Loss over optical fibers goes exponential with the length of the fiber with approximately 0.2 dB/km for wavelength around 1550 nm. As of today, the longest fiber based QKD transmission was performed over 404 km of ultra-low loss fibers [21] and 303 km of standard telecom fibers [22], overcoming previous distance records [23–26].

To overcome the distance limit of a few hundreds of kilometers, there are two approaches, namely quantum repeaters and implementing satellite QKD. Quantum repeaters [27–29] work by entanglement swapping. By taking two entangled photon pairs, measuring one photon each by means of a Bell measurement and hereby leaving the remaining photons entangled, the bounds induced by loss [30] can be surpassed [31]. However, for quantum repeaters, quantum memories [32–35] are crucial, which are not technologically mature as of today.

Satellite-based QKD is attractive since most of the communication path is in vacuum, thus the losses are mostly geometric and thus scale quadratically. Further, satellite QKD is already viable with today's technology. Recently the first satellite QKD experiments were carried out with the satellite Micius. A prepare-and-measure scheme could be demonstrated from the satellite to the ground [36] as well as an experiment, where the satellite acted as a trusted node connecting two parties 7600 km apart [37] and an experiment where the satellite acted as an entangled photon pair source [38] connecting two parties 1200 km apart.

Free-space QKD is also expedient for other applications than satellite links, such as last-mile applications, where it is too complicated or too expensive to implement a fiber infrastructure or for scenarios, where one or both communication parties are mobile. QKD experiments over horizontal free-space links where demonstrated in [39–43] with the longest terrestrial link being 144 km in length [44–46] between the Canary Islands Tenerife and La Palma.

In order for QKD to be widely available, cost, size, and robustness are important factors. A lot of QKD experiments are still implemented on bulky optical tables and with exotic components. One way of solving this issues is to rely on off-the-shelf components, which are already in wide use. Those components are proven to work reliably in a lot of other applications and are relatively cheap due to high production output.

In the present work a QKD protocol is examined and implemented, which allows free-space transmission and is implemented with mainly off-the-shelf telecommunication components. This protocol is named time-frequency (TF)-QKD protocol and was proposed in [47, 48].

TF-QKD is a BB84 like protocol, which used time and frequency as the two orthogonal bases, namely pulse-position modulation (PPM) and frequency-shift keying (FSK), respectively. Its security relies on the time-frequency uncertainty relation, which forbids to measure time and frequency at the same time in an exact manner. These two bases are beneficial for the intended goal of utilizing off-the-shelf components since the technology necessary is already present in the form of optical modulators [49, 50] for the PPM basis and wavelength division multiplexing (WDM) technology [51, 52] for the FSK basis. Both technologies are already widespread in the world of classical communications. With respect to free-space QKD, PPM is already a common coding technique in classical free-space and satellite communication systems [53–57]. Furthermore, the PPM and FSK bases are capable of encoding a high number of symbols leading to a potentially high number of bits carried per photon. This is especially beneficial when detector saturation limits the key rates.

Many off-the-shelf components in optical communications are single-mode fiber (SMF) based. Since the declared goal of this work is to implement QKD over a free-space link, optical antennas capable of effectively coupling light in and out of SMF are crucial. Fortunately, such antennas were developed already at Fraunhofer Heinrich Hertz Institute (HHI), where the TF-QKD protocol was implemented. However, these antennas needed to be adapted for QKD transmissions. An advantage of using SMF based optical antennas is, that a lot of background light is already filtered spatially. Together with the high quality of off-the-shelf SMF-based spectral filters, this can enable QKD in daylight.

The goals of the presented project can be subdivided as follows: Firstly, the theoretical foundations of the TF-QKD protocol has to be developed. This is crucial for the second goal, which is to implement the TF-QKD protocol with off-the-shelf telecommunication components. The third goal is the QKD transmission over a free-space testbed in daylight. The structure of this thesis reflects on these goals and is presented in the following:

In Chapter 2 the essentials necessary for the subsequent work are introduced. The basics of QKD are summarized. Information and probability theory are introduced as far as it was necessary for the theoretical study. The necessary foundations of free-space transmissions with respect to single mode beams are stated.

In Chapter 3 the TF-QKD protocol is analyzed with the help of numerical calculations. Here close attention is paid to the effect of a high number of symbols, as one of the advantages of the TF-QKD protocol. Further, the influence of the pulse size is investigated. This is done by analyzing a intercept/resend (IR) attack, which exploits the weaknesses of the TF-QKD protocol. The chapter is closed with a guidance to calculate the secret key rate under the considered attack for the TF-QKD implementation.

Chapter 4 introduces the TF-QKD setup and how it is controlled by various control signals. In Chapter 5 the TF-QKD setup is experimentally evaluated in the back-to-back configuration. The chapter begins by addressing the experimental procedure to conduct and evaluate a TF-QKD transmission. Afterward, a detailed experimental evaluation in a back-to-back scenario is presented in order to evaluate the TF-QKD setup.

In Chapter 6 the experimental TF-QKD transmission over a 388 m free-space link is presented. The chapter begins by introducing the free-space optical antennas and the free-space testbed. Thereafter, the experimental free-space TF-QKD transmission is presented and discussed in detail.

Finally, the summary, conclusion, and outlook are given in Chapter 7.

2. Essentials

In this chapter, the essential foundations needed in the presented work are carried out. The chapter starts by introducing quantum key distribution (QKD) in Section 2.1, with a focus on the BB84 protocol, on which the time-frequency (TF)-QKD protocol is based on, the TF-QKD protocol itself, and the decoy state protocol. Further, in Section 2.2 the necessary basics of information and probability theory are presented, which will be crucial for the numerical assessment of the TF-QKD protocol later on. The chapter closes with Section 2.3 presenting some basics of free-space optics of Gaussian beams, which will become necessary later for the free-space TF-QKD transmission.

2.1. Quantum Key Distribution

QKD is the process of exploiting quantum physics to distribute a secret key between two parties. These two parties are commonly called Alice and Bob, where usually Alice is the sender and Bob the receiver. Alice and Bob want to obtain a coinciding secret key, which is only known to them and not to an eavesdropper commonly called Eve. Alice and Bob can use this key, e.g. for absolutely secure communication by means of the one-time pad method [19].

A raw key is distributed between Alice and Bob in the form of qubits (usually embodied by photons), which is later on used to create the secret key. There are a lot of different QKD-protocols, but all of them rely on basic principles of quantum physics.

Alice and Bob distribute qubits over an authenticated channel. For authentication, a pre-shared secret is necessary. This could, for example, be a part of the key from the last QKD transmission. The QKD-protocol is designed such, that if Eve interacts with the qubits she has to change them in a way that is detectable for Alice and Bob. This can be traced back to either of two principles of quantum physics [58]: One could state, that Eve needs to perform a measurement in a quantum mechanical meaning of the word, which will, in turn, alter the system she measures on. A different point of view is in consideration of the no-cloning theorem [59]. Eve wants to have a perfect copy of the system containing the qubits used for creating the secret key. This is of cause forbidden by the no-cloning theorem.

Regardless of which argument one uses, Alice and Bob need to set up their QKD system such that they can deduce how much information Eve has about the key. Only if their information on the key surpasses the information of Eve, they can distill a secret key from the transmitted qubits. Even if no secret key was distributed, Eve does still not get a hand on the secret message, since it was not sent up to this point.

A distinctive feature of QKD protocols is, whether single-photon detectors like in BB84 or coherent detection schemes are used. In the literature, the single-photon detector type of protocol is often referred to as discrete variable (DV)-QKD, whereas coherent detection type protocols are referred to as continuous variable (CV)-QKD [60–65].

However, both types of protocols can be set up with discrete or continuous modulations, which makes this definition misleading. The topic of the present work is a single-photon detector based TF-QKD protocol implemented with discrete modulations. During the course of this work, this protocol will be compared with a single-photon detector based TF-QKD protocol using continuous modulations, presented in [66]. Consequently the convention used in [66] will be used in this work: Single-photon detector based protocols with discrete modulations will be denoted as DV and single-photon detector based protocols with continuous variables are denoted as CV.

The difference here is not only technical but also conceptional. On the one hand Single photon based protocols use the particle properties of photons, e.g. in the polarization [20], phase [67] or time-frequency [68–70] space. On the other hand, coherent detection based schemes use the wave properties of photons, namely the quadrature of amplitude and phase of a weak coherent pulse [71–73].

Single-photon detector based QKD protocols can further be differentiated into three classes: Firstly prepare and measure QKD, where Alice prepares photons deterministically and sends them over to Bob, like the BB84 protocol or the TF-QKD protocol presented here.

Secondly entanglement based QKD [46, 70, 74, 75], where an entangled photon source not necessarily possessed by Alice or Bob sends the two partners of an entangled photon pair to Alice and Bob [76]. Since the photons are entangled, Alice's and Bob's measurements are correlated.

Thirdly measurement device independent QKD [77–79] where Alice and Bob prepare indistinguishable photons, send them to a Bell measurement station, which publicly announces the results. Alice can deduce the state Bob has prepared his photon in from the Bell measurement and the state she has prepared her photon in (and vice versa).

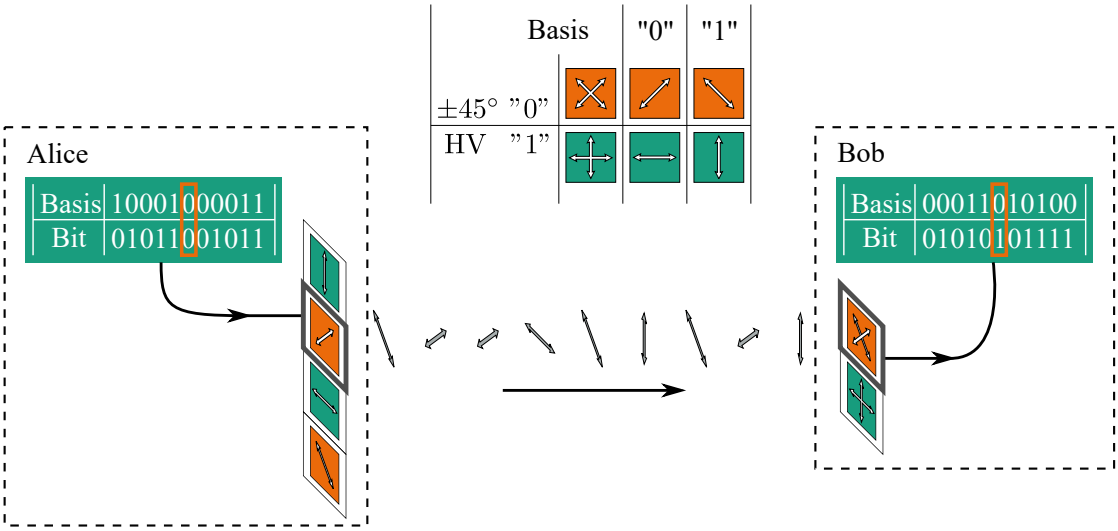


Figure 2.1.: Transmission scheme for the BB84 protocol. Alice randomly chooses one of two bases, either HV or ±45° and one of two symbols to encode the qubits. Bob measures them randomly in one of the two bases.

2.1.1. The BB84 Protocol

The BB84 protocol named after its founders Bennett and Brassard and the year their respective paper [20] was published is historically the first proposed QKD-protocol. Many other QKD-protocols – among others the TF-QKD-protocol – rely on similar principles. Thus, it seems obvious to start by explaining the BB84 protocol.

The BB84-protocol uses the polarization of single photons to form two non-orthogonal bases. A basis consists of two orthogonal states, which encodes the qubit and thus carry the qubits. The two bases being realized with non-orthogonal linear polarization are shown in Figure 2.1. The first basis consists of two states, namely horizontally (90°) and vertically (0°) linear polarization and is called HV-basis while the states of the other basis consist of 45° and −45° linear polarization and is called ±45°-basis. Bob has a measurement setup which can either measure in the HV or in the ±45°-basis. When the basis chosen by Bob differs from the basis of Alice, the measurement outcome and thus the measured symbol is random and uncorrelated to the sent symbol.

Alice now sends a stream of photons each coded with a random symbol in a random basis. Usually, she chooses the two bases and the two symbols all with equal probability. Bob measures the incoming photons also in a random basis with equal probability and will be in the correct basis with respect to Alice half of the time. After a sufficient amount of photons are sent over, Alice and Bob

communicate over a public channel which photons Bob detected and which basis they have chosen for each of those photons. From the arrived photons Alice and Bob only keep the photons where their bases coincide. This process is called sifting and the remaining key is called the sifted key.

Since it is not possible to measure the polarization of single photons with absolute certainty without knowledge of the basis, the photons were prepared in, Eve will necessarily induce detectable errors when she eavesdrops on the transmission and can consequently be detected.

2.1.2. The Time-Frequency QKD-Protocol

The TF-QKD-protocol is a BB84 like protocol with modulations in the time- and frequency domain as the two complementary bases, which was proposed by several authors [48, 69].

The security of the CV version of the TF-QKD protocol was discussed in the literature. In [66] it was shown, that the bases can be constructed such, that photons of both bases cannot be distinguished. It is stated, that together with the time-energy uncertainty relation the protocol can thus be made secure. The security of entanglement-based CV-TF-QKD in the presence of a IR attack is proven in [80], and in the presence of general attacks in [70, 81]. Security against general attacks is the strongest form of attacks, where Eve is only restricted by the laws of physics [58].

However, a security proof against general attacks for the DV version of the TF-QKD does not exist up to this date to the knowledge of the author. The DV version of the TF-QKD protocol in its prepare-and-measure [82] or entanglement [68] form was reported. An analysis of a certain IR attack was addressed in [83]. In Section 3.3 the IR attack discussed there will be revisited and compared to the IR attack discussed in the present work.

The main subject of this thesis is the DV embodiment of the TF-QKD. One of the main differences between TF-QKD in its DV version and BB84 is the imperfect complementary of the measurement bases. While in BB84 all information coded in one basis is completely deleted, if the information coded in the other is measured, this is not the case for DV version of the TF-QKD protocol, where some information remains, as will be examined in Chapter 3.

In the DV version of the TF-QKD-protocol discrete modulations in the time- and frequency domain are used, namely PPM in the time domain and FSK is the frequency domain. In the PPM (respectively FSK) modulation, information is coded in the distance to a reference point in time (respectively frequency). Thus, contrary to the polarization-bases in BB84, more than two symbols per basis can be encoded, which increases the number of bits per sent symbol and thus per sent

photon. In this case the modulations are called M-PPM and M-FSK with M being the number of symbols per basis. Ideally, up to $\log_2 M$ bits can be transmitted per photon measured by Bob.

Despite using PPM and FSK as the two bases, Alice and Bob perform the same steps as in the BB84-protocol, which will be given in the following:

1. Alice creates a random stream of symbols encoded randomly in the PPM or FSK basis and sends them to Bob.

2. Bob measures the photons randomly in the PPM or FSK basis. The bits carried by the measured symbols are called the raw key

3. Alice and Bob communicate over a public channel, for which symbols their basis coincides and discard all symbols, where their basis differ. This process is called sifting and the resulting key is called the sifted key

4. Alice and Bob share which symbol they have sent/measured for a small fraction of the sifted key and subsequently calculate the quantum symbol error rate (QSER) or quantum bit error rate (QBER) (See Section 2.2.2 for more information on QBER and QSER) of Bob's measurement with respect to Alice sent symbols. If the QBER or QSER is to high, they have to abort the transmission process and secure communication is not possible.

5. Alice and Bob perform post-processing, namely error correction and privacy amplification (see Section 2.2.4), depending on the measured QSER or QBER. The resultant key is called the secret key. The key of Alice and Bob is now coinciding and known only to them.

2.1.3. Decoy state protocols

While some QKD experiments are implemented with single photon sources [84–86], most are implemented with lasers where the mean photon number of each sent pulse is set to $\mu \ll 1$. This will inevitably lead to some pulses containing more than one photon.

The so-called photon number splitting (PNS) attack [87,88] exploits this in order for Eve to get additional information about the key. Eve can e.g. measure the photon number of each pulse, block all single-photon pulses and keep one photon of each multi-photon pulse, while the remaining photons of the multi-photon pulses are forwarded to Bob. Usually, the loss in a QKD transmission is high enough, that Eve can mimic the loss the transmission usually experiences entirely with photons from multi-photon pulses, thus fully compromising security.

However, the decoy state method [89–95] clothes this loophole. Different versions of the decoy state protocol were developed with the core principle being, that the photon numbers of the sent pulses are taken from a set $\{\mu_1, \mu_2, \dots\}$ of different mean photon numbers. Eve can only measure the number of photons a certain pulse contains, not with which mean photon number the pulse was prepared.

During post-processing, Alice, additionally to the basis choice, reveals the mean photon number each symbol measured by Bob was sent in. By analyzing the statistic of the measured photons depending on the chosen photon number, they can deduce the amount of information Eve possibly received due to PNS attacks.

2.2. Information and probabilities

In this section the essentials for assessing the TF-QKD protocol theoretically is given. Therefore, the relevant parts of probability theory is introduced, then QBER and QSER is introduced in terms of probabilities, followed by introducing mutual information, and lastly the effects of post-processing on the mutual information is discussed.

2.2.1. Probabilities

When talking about information some basics of probability theory need to be defined prior. That will be done in this section. For a more detailed introduction in the field of probability theory see for example [96].

Let $a \in A$ be a random event out of the Set A with M elements:

$$A = \{a_1, a_2, \dots, a_M\}. \tag{2.1}$$

The probability for the event $a \in A$ to occur is defined as $P_A(a)$ with

$$\sum_{a \in A} P(a) = 1. \tag{2.2}$$

In other words, the probability that any event a out of the set A happens is one. It will be useful to arrange all the M probabilities $\{P_A(a_1), P_A(a_2), \dots, P_A(a_M)\}$ as a vector with M entries, such that

$$\mathbf{P}_A = \begin{pmatrix} P_A(a_1) \\ P_A(a_2) \\ \vdots \\ P_A(a_M) \end{pmatrix}, \tag{2.3}$$

which will be called probability vector. As in (2.2), all probability vectors are defined such, that their elements sum up to one.

Let $b \in B = \{b_1, b_2, \ldots, b_N\}$ be another event from another set of size N with the according probabilities $P(b)$ and with

$$\sum_{b \in B} P(b) = 1. \tag{2.4}$$

The event, where a and b happen together can be written as $(a \cap b)$ and the joint probability for this can be written as $P_{A \cap B}(a \cap b)$. Similar to (2.3), where the probabilities of the events of one set can be arranged as a vector, the joint probabilities of two events out of two sets can be arranged as the $M \times N$ matrix

$$\mathbf{P}_{A \cap B} \equiv \begin{pmatrix} P_{A \cap B}(a_1 \cap b_1) & P_{A \cap B}(a_1 \cap b_2) & \cdots & P_{A \cap B}(a_1 \cap b_N) \\ P_{A \cap B}(a_2 \cap b_1) & P_{A \cap B}(a_2 \cap b_2) & & \vdots \\ \vdots & & \ddots & \vdots \\ P_{A \cap B}(a_M \cap b_1) & \cdots & \cdots & P_{A \cap B}(a_M \cap b_N) \end{pmatrix} \tag{2.5}$$

In this matrix the probability of every combination of events $a \in A$ and $b \in B$ is represented by one matrix entry. The probability, that any combination of events occur together is obviously

$$\sum_{a \in A} \sum_{b \in B} P(a \cap b) = 1. \tag{2.6}$$

If two measurements show a dependency, it makes sense to introduce the conditional probability $P_{B|A}(b|a)$, which is the probability of event b under the condition, that a occurs. The conditional probability can be written in terms of the joint probability as

$$P_{B|A}(b|a) \equiv \frac{P_{B \cap A}(b \cap a)}{P_B(a)} \tag{2.7}$$

Similar to 2.5, it can be arranged as a matrix, which will be called conditional probability matrix:

$$\mathbf{P}_{B|A} = \begin{pmatrix} P_{B|A}(b_1|a_1) & P_{B|A}(b_1|a_2) & \cdots & P_{B|A}(b_1|a_N) \\ P_{B|A}(b_2|a_1) & P_{B|A}(b_2|a_2) & & \vdots \\ \vdots & & \ddots & \vdots \\ P_{B|A}(b_M|a_1) & \cdots & \cdots & P_{B|A}(b_M|a_N) \end{pmatrix} \tag{2.8}$$

The probability of any event $b \in B$ occurring, for a given a, in other words the sum over one row of the conditional probability matrix sums up to one:

$$\sum_{b \in B} P_{B|A}(b|a) = 1 \tag{2.9}$$

If a probability $\mathbf{P}_A$ and the conditional probability $\mathbf{P}_{B|A}$ are both known, $\mathbf{P}_B$ can be expressed as

$$\mathbf{P}_B = \mathbf{P}_{B|A}\mathbf{P}_A \tag{2.10}$$

In the presented work, probability describes the processes during a QKD transmission and thus represent the probabilities for sending or measuring a symbol carrying information about the key. Equations such as (2.10) can describe one sending process of a symbol from Alice to Bob. Note, that in this context the Elements $a \in A$ and $b \in B$ are the set of used symbols, which in consequence results in the number of a and b being of the same length M and the joint/conditional probabilities being quadratic $M \times M$ matrices.

In a real QKD transmission of cause not every symbol gets detected. Quite the contrary, typically most symbols are either empty since the mean sent photon number is well below one, get lost during the transmission or do not get detected even when they reach the detectors due to a non-unity detection efficiency. In the evaluation described here, only the symbols, which are detected are taken into account. The effect of loss is detached from the probability-contemplation and is treated independently thereof.

In (2.10) $\mathbf{P}_A$ represents the probabilities for Alice to send each symbol with a certain probability and $\mathbf{P}_B$ represents Bob to measure those symbols with a certain probability. $\mathbf{P}_{B|A}$ describes the influence of the transmission channel and describes for every sent symbol, what the probability is to get either received as the correct symbol or as one of the $M-1$ wrong symbols.

Similarly, one can describe chains of transmissions involving more than two parties with this annotation. This can for instance be a transmission process not only including Alice and Bob but also a intermediate third party Eve with the probability vector $\mathbf{P}_E$ consisting of the M elements $P_E(e)$ with $e \in E = \{e_1, e_2, \ldots, e_M\}$ and $\sum_{e \in E} P_E(e) = 1$. This transmission process can be split into the transmission from Alice to Eve and from Eve to Bob as

$$\mathbf{P}_B = \mathbf{P}_{B|E}\mathbf{P}_E \tag{2.11}$$

and

$$\mathbf{P}_E = \mathbf{P}_{E|A}\mathbf{P}_A \tag{2.12}$$

which result in

$$\mathbf{P}_B = \mathbf{P}_{B|E}\mathbf{P}_{E|A}\mathbf{P}_A. \tag{2.13}$$

The transmission describing the whole process can thus be described by the conditional probability matrix

$$\mathbf{P}_{B|A} = \mathbf{P}_{B|E}\mathbf{P}_{E|A}. \tag{2.14}$$

which is composed of the conditional probability matrices describing the partial transmissions.

2.2.2. Quantum bit and symbol error rate

With the subsequent section in mind it makes sense to also define the quantum symbol error rate (QSER) at this point. The QSER is a measure for the occurring errors in a QKD transmission. It is defined as the fraction of all measured symbols, that where measured as a symbol different from the sent one. The fidelity F_M, namely the fraction of correctly received symbols out of all received symbols in terms of probabilities, is defined as

$$F_M = \sum_{a \in A} P_A(a)\, P_{B|A}(a|a), \tag{2.15}$$

which is the sum over all elements on the primary diagonal of the conditional probability matrix, each weighted by the probability of the symbol being sent by Alice. With this the QSER Q_M trivially follows as

$$Q_M = 1 - \sum_{a \in A} P_A(a)\, P_{B|A}(a|a). \tag{2.16}$$

Assuming Alice sends all symbols with the same probability $P_A = 1/M$, the QSER can be written in terms of the trace $\mathrm{tr}\,()$ of the conditional probability:

$$Q_M = 1 - \frac{1}{M}\mathrm{tr}\left(\mathbf{P}_{B|A}\right). \tag{2.17}$$

The quantum bit error rate (QBER) Q_2 is defined as the QSER for the case where a symbol carries exactly one bit of information, in other words $M = 2$. Since the bit is a common unit of information, it make sense to translate the QSER into the QBER [97]:

$$Q_2 = \frac{M}{2(M-1)} Q_M. \tag{2.18}$$

2.2.3. Mutual information

In order to describe the information of Alice and Bob about a shared and secret key, it has to be defined what information means in this context. Here the mutual information is a powerful tool. As the name suggests, it describes the coinciding information of two parties as a measurable quantity in bits. In the case of QKD Alice and Bob both have information about the transmission process, which is not completely coinciding yet, embodied by the defective sifted key. The mutual information describes the amount of coinciding information about the sifted key. Eve's knowledge of the sifted key can similarly be described by the mutual information of Alice and Eve.

For M symbols s out of the alphabet S sent by the sender and M symbols r out of R received by the receiver the mutual information follows as [98]

$$I'_{S,R} = \sum_{s=1}^{M} \sum_{r=1}^{M} P_{S\cap R}(s \cap r) \log_2 \left(\frac{P_{S\cap R}(s \cap r)}{P_S(s) P_R(r)} \right) \tag{2.19}$$

s out of S and r out of R will in the following be assigned to one of the involved characters by either replacing it by a out of A for assigning it to Alice, b out of B, for assigning it to Bob and e out of E for assigning it to Eve. A symbol carries up to $N = \log_2(M)$ bits or one qu-N-it. (2.19) can be rewritten with (2.8) to be dependent on the conditional probability instead of the joint probability

$$I'_{S,R} = \sum_{s=1}^{M} \sum_{r=1}^{M} P_{R|S}\left(r|s\right) P_S\left(s\right) \log_2 \left(\frac{P_{R|S}\left(r|s\right)}{P_R\left(r\right)} \right), \tag{2.20}$$

Considering the two bases used in TF-QKD, $2M$ symbols are used in total. Since only one basis is used at a time, the maximum amount of mutual information still is $N = \log_2 M = \log_2\left(2M\right) - 1$. (2.20) can be rewritten as

$$I_{S,R} = \sum_{s=1}^{2M} \sum_{r=1}^{2M} P_{R|S}\left(r|s\right) P_S\left(s\right) \log_2 \left(\frac{P_{R|S}\left(r|s\right)}{P_R\left(r\right)} \right) - 1. \tag{2.21}$$

In other words, one bit of information is subtracted, since only half of the symbols can be used at a time.

2.2.4. Post processing

As described above, Alice and Bob share mutual information about the sifted key, but they at this point do not have a coinciding key representing this mutual information. Thus, Alice and Bob need to use post-processing to create a secret key out of the defective sifted key. post-processing consists of two parts, error correction and privacy amplification.

In the following it is explained what error correction and privacy amplification is and what it does to the mutual information between Alice and Bob $I_{A,B}$ and between Alice and Eve $I_{A,E}$. A depiction of post-processing is shown in Figure 2.2 [99].

(a) $\log_2 M$ is the maximum of mutual information per arriving photon Alice and Bob can possess after the sifting process, assuming there is no eavesdropping and no errors occur. With eavesdropping $I_{A,B}$ has some value smaller than $\log_2 M$. Alice and Bob measure a variable (which one depends on the protocol, e.g. QBER or QSER) from which they can deduce how much information Eve holds about the key, described by $I_{A,E}$.

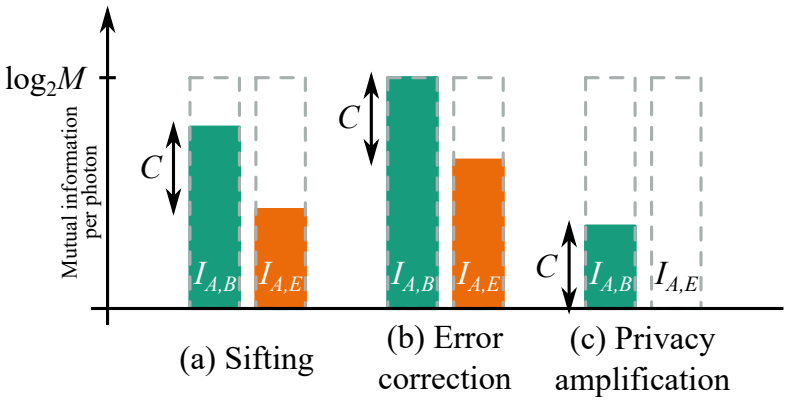


Figure 2.2.: Post processing and information. The mutual information of Alice and Bob, and of Alice and Eve is shown to illustrate the relation between mutual information and capacity C after sifting, error correction and privacy amplification respectively. Ideal error correction and privacy amplification algorithms are assumed. (a) After sifting, Alice and Bob compare some of their bits and observe a quantum bit error rate (QBER). From the QBER they deduce the knowledge Eve has on the sifted key. (b) Alice and Bob perform error correction to receive a coinciding key; Eve will also gain knowledge from this step, since Alice and Bob have to communicate over a public channel, here. (c) Alice and Bob use privacy amplification. With the knowledge of Eves information on the error-corrected key, they can make sure, that Eve no longer holds significant information about the resulting secret key.

(b) Alice and Bob perform error correction. The length of the secret key is bound by the information Alice and Bob possess about the sifted key, namely the mutual information $I_{A,B}$ [58, 100]. In order for them to both get the total information about the sifted key, they have to communicate about the remaining information. This is done publicly, consequently Eve can also get hand on this information. Assuming optimal error correction, Alice's and Bob's mutual information will be increased to $I_{A,B} = \log_2 M$ and Eve's mutual information will increase by the same amount.

(c) Subsequently Alice and Bob use privacy amplification [101]. Alice and Bob create a secret key out of the error corrected sifted key by means of certain algorithms, which reduces Eve's knowledge on the key to a point, where her mutual information is 0. During this process $I_{A,B}$ decreases by the same amount as $I_{A,E}$, effectively reducing the key length.

The first widespread [102] privacy amplification algorithm was the "Cascade" [103] algorithm, but work on more efficient privacy amplification has also been carried out [102, 104–107].

Following the reasoning above it is not possible for Alice and Bob to establish a secret key if $I_{A,B} \leq I_{A,E}$. Based on this the secret capacity C in bits per photon is defined, following the definition in [58] for the secret fraction to be

$$C = \begin{cases} I_{A,B} - I_{A,E} & \text{for } I_{A,B} > I_{A,E} \\ 0 & \text{for } I_{A,B} \leq I_{A,E} \end{cases} \tag{2.22}$$

For $M = 2$ the secret capacity is called secret fraction which is more common in the literature, as for example in [58]. C can become larger than one for $M > 2$ and thus represents the capacity of secret bits per photon. Thus, here it is called secret "capacity" rather than secret "fraction".

It is straightforward to also define the secret key rate at this point:

$$S = KC \tag{2.23}$$

where K is the sifted key rate, defined as the number of photons Bob manages to detect per time interval.

2.3. Free-space transmissions

In the present work, one of the declared goals is to transmit a QKD signal over a free-space testbed. Since the implemented QKD setup is purely SMF based, the transmitted beams are in first approximation Gaussian. In this section, the basics of free-space transmission for single mode beams is discussed. In Section 2.3.1 the geometric losses for coupling light in and out a SMF are discussed. In Section 2.3.2

other forms of free-space losses, such as absorption, scattering and turbulence are discussed.

2.3.1. Coupling of Gaussian beams

In the following the coupling two SMFs over free space links is discussed, following [108]. A beam coupled out of a SMF can with good accuracy be approximated with a Gaussian beam [109–111]. The field of a Gaussian beam is cylindrically symmetrical with its symmetry axis running along its direction of propagation. L is the distance along its axis and r the distance from the axis. The Gaussian field has the form

$$E_A(r, L) = \hat{E}_A \frac{W_0}{W(L)} \exp\left(-\frac{r^2}{W^2(L)}\right) \exp\left(-i\Phi(r, L)\right). \tag{2.24}$$

Half the beam width, namely the distance from the beam's central axis, where the field has fallen to $1/e$ (respectively the intensity of the field has fallen to $1/e^2$) is defined as

$$W(L) = W_0\sqrt{1 + L^2/z_R^2}, \tag{2.25}$$

which is depending on half the beam waist W_0, namely the half-width of the beam at its origin. z_R is the Rayleigh range,

$$z_R = \frac{\pi W_0}{\lambda}, \tag{2.26}$$

which is defined as the distance along the axis where the beam has the width $W(z_R) = \sqrt{2}W_0$ and is depending on the wavelength λ. z_R marks the point of transition between the near field ($L \ll z_R$) and the far field ($L \gg z_R$). $\Phi_A(r, L)$ is the phase of the Gaussian field.

The divergence angle in the far field θ_D depends on the beam waist W_0

$$\theta_D = \arctan\left(\frac{W(L)}{L}\right) \approx \frac{\lambda}{\pi W_0} \tag{2.27}$$

thus a larger beam waist makes the divergence angle θ_D smaller, which in turn increases the coupling efficiency at a distance L. Usually a collimator, a lens with a distance equal to the lens' focal length f, is used to create a wider collimated beam compared to the beam coming out of the SMF. The beam waist after the collimator $W_{0,C}$ can be calculated with (2.27) and becomes

$$W_{0,C} \approx f\theta_D = \frac{f\lambda}{\pi {W_0}^2}. \tag{2.28}$$

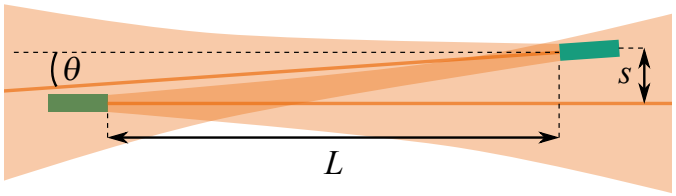


Figure 2.3.: Antenna mismatch definition. A sketch of the angular θ and lateral s mismatch of two Gaussian antennas with the separation L is shown.

If necessary the beam can be widened more by means of a beam expander.

In order for the Gaussian beam described in (2.24) to be coupled with a receiver, the Gaussian beam mode and the mode of the receiver need to be coupled. If the receiver also is a Gaussian antenna, e.g. a SMF, the coupling efficiency η_{point} is described by the overlap integral [112]

$$\eta_{\text{point}} = \frac{\int_A \|E_A^*(r,L)\| \, \|E_B(r,L)\| \, dA}{\int_A \|E_A(r,L)\|^2 dA \int_A \|E_B(r,L)\|^2 dA}, \tag{2.29}$$

where $E_B(r,L)$ is the Gaussian field of the receiver and $\|E(r,L)\|$ is indicating the normalization of the fields to $\int_A E(r,L)\, dA = 1$. In [112] the coupling efficiency η_{point} is shown to be

$$\eta_{\text{point}} = \frac{4z_R^2}{L^2+4z_R^2} \exp\left(-\frac{2z_R^2}{W_0^2}\frac{2s^2+2sL\sin\theta+(L^2+2z_R^2)\sin^2\theta}{L^2+4z_R^2}\right) \tag{2.30}$$

for angular θ and lateral s mismatch with the optical antennas being a distance L apart (see Figure 2.3). Assuming the optimal case without mismatch, where $\theta = 0$ and $s = 0$, the coupling efficiency becomes

$$\eta_{\text{point}} = \frac{4z_R^2}{L^2+4z_R^2}. \tag{2.31}$$

2.3.2. Influence of the atmosphere

Additionally to geometric losses, further losses can have an influence on free-space optical transmissions in the atmosphere, namely absorption, Rayleigh scattering and Mie scattering. The losses can be described by the Beer-Lambert law [113,114]

$$\eta_{\text{BL}}(L) = e^{-\delta(\lambda)L}, \tag{2.32}$$

where $\delta(\lambda)$ is optical attenuation coefficient and L describes the distance. The coefficient is composed of

$$\delta(\lambda) = \delta_A(\lambda) + \delta_R(\lambda) + \delta_M(\lambda), \tag{2.33}$$

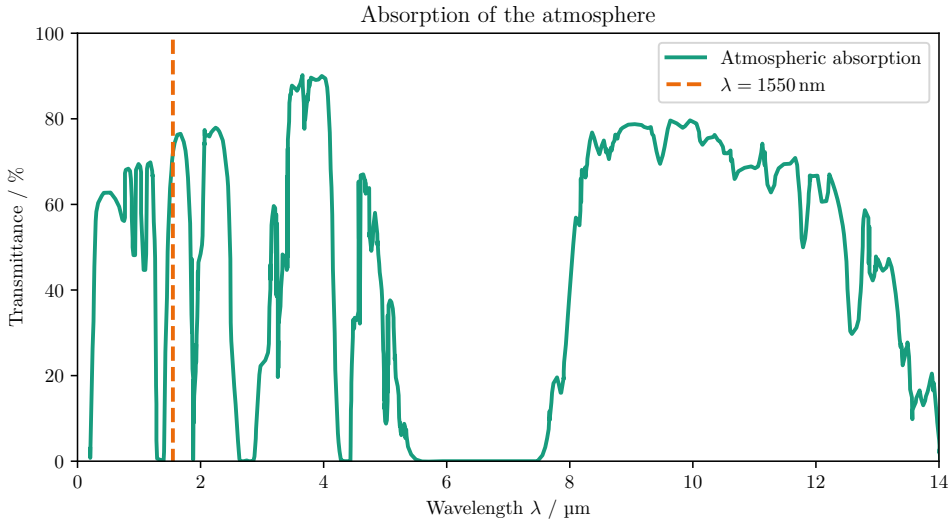


Figure 2.4.: Transmission in the atmosphere. As an example the transmission for a 1800 m horizontal path on see level is shown [114]. The transmission wavelength, chosen in the present work, namely 1550 nm, is in a wavelength-window with relative low absorption.

where $\delta_A(\lambda)$ is the attenuation coefficient caused by absorbtion, $\delta_R(\lambda)$ the attenuation coefficient caused by Rayleigh scattering and $\delta_M(\lambda)$ the attenuation coefficient caused by Mie scattering.

Absorption is caused by the molecules the atmosphere is composed off. The molecules contributing the highest amount to absorption, are O_2, O_3, H_2O, CO_2 and CO_2O_3 [114]. Rayleigh scattering is the elastic scattering at particles which are small compared to the wavelength, namely at the molecules the air consists of and other small particles. Mie Scattering, in turn, is elastic scattering at particles, which size is bigger than the wavelength of the scattered light, namely aerosols and fine particulates in the atmosphere.

$\eta_{\mathrm{BL}}(L)$ is highly dependent on the weather condition. At clear sky $\delta(\lambda) = 0.1$ corresponding to a loss of 0.43 dB/km. However, with rain or fog the attenuation coefficient can be at $\delta(\lambda) = 1$ or $\delta(\lambda) = 10$ respectively, corresponding to losses of 4.3 dB/km and 43 dB/km respectively [113]. A Measurement of the transmittance over a 1800 m long path can be seen in Figure 2.4. It can be observed, that 1550 nm light is in a window with low absorption, which was one of the reasons this wavelength was chosen in the present work.

The free-space QKD transmissions carried out in the present work has been done with clear sky weather conditions thus the losses due to absorption and scattering should be around 0.2 dB for the 388 m long free-space testbed, which

will be introduced in Section 6.1.3.

When SMFs are used for transmitting light, the turbulence of the air has a big effect on the coupling efficiency. Thermal and pressure induced fluctuations in the atmosphere lead to temporal local variations of the refractive index. This is called atmospheric turbulence and disturbs the phase and orientation of the beams wave front traveling through the atmosphere [114–116]. This degrades the spatial coherence of the beam and thus decreases the coupling efficiency tremendously [117]. Turbulence effects can be corrected with adaptive optics [114, 118]. The simplest and cheapest systems correct tip and tilt of the incident light [119, 120], more advanced and expensive systems additionally correcting wavefront mismatches with deformable mirrors [121–123].

3. Numerical Analysis of TF-QKD

In Section 2.1.2 the basic idea of the TF-QKD protocol was introduced. In this chapter, the DV version of the TF-QKD-protocol will be investigated with respect to different intercept/resend (IR)-attacks. Major parts of the results presented in this chapter were published in [124].

The TF-QKD protocol is conceptionally similar to the BB84 protocol. However, contrary to BB84 a measurement in one basis does not delete the information possibly contained in the other basis. An eavesdropper Eve could utilize this and extract at least some information about the key from both bases.

In this chapter, the characteristics of the TF-QKD protocol are addressed. This is done by introducing an IR eavesdropping strategy regarding the protocol's weaknesses. For this purpose, the framework for describing the transmission process and the IR-attack is given in Section 3.1. In Section 3.2 a standard IR-attack (referred to as one-level IR-attack) is applied which is then extended in Section 3.3 to a two-level IR-attack exploiting that Eve can get information from both bases. The results will be utilized to optimize the protocol in terms of pulse widths.

In Section 3.4 the analysis of the two-level IR-attack is translated into a method to calculate the possible secret key rate for an actual embodiment of the protocol. Finally, in Section 3.5 the numerical assessment carried out here is summarized and concluded. All calculations presented in the following were done with the numerical computing environment *MATLAB*.

3.1. Pulse and bin relationships and basic definitions

The modulations used as the two bases are M-PPM in the time domain and M-FSK in the frequency domain. Both modulations are shown in Figure 3.1 in the form of the energy density distribution of the respective pulses for $M = 4$. Here M symbol pulses in M different time (frequency) bins represent M different symbols. In the conjugate basis, namely the frequency (time) domain, the conjugate pulses should not contain any information about the key. Consequently, the conjugated pulses in the frequency (time) domain are all identical, regardless of which symbol was sent in the time (frequency) domain. Further, the conjugated pulse is centered to maximize the overlap with the symbol pulses.

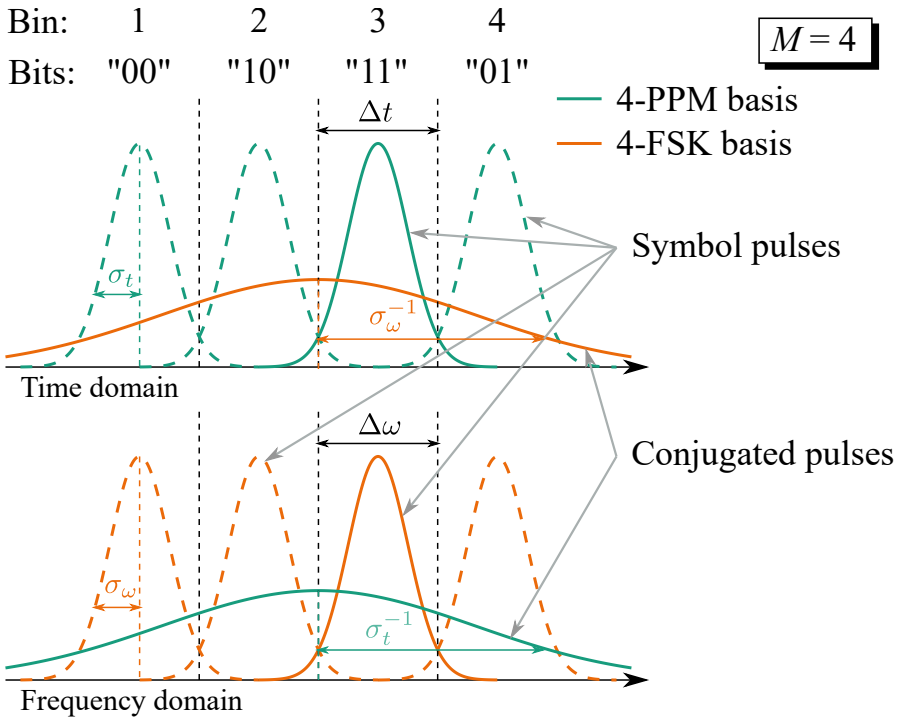


Figure 3.1.: Bases used in TF-QKD. The pulse-position modulation (PPM)- and frequency-shift keying (FSK)-basis for $M = 4$ symbols per basis is shown. The distribution of the PPM (FSK) basis in the time and frequency domain are drawn in green (orange). The symbol pulses carry the qubits while the conjugated pulses are uncorrelated to them. The pulses have Gaussian shapes, namely, have a Gaussian distribution for amplitude and intensity. The intensity is proportional to the probability distribution to measure a photon at a certain point in the time (frequency) domain.

In general, the conjugated pulse is broader than the symbol pulses and thus has a huge overlap with the symbol pulses. The energy of one pulse is assumed to exactly match the energy of one photon, such that the energy distribution also represents the probability distributions to measure a photon at a certain point in the time (frequency) domain. Fourier-limited Gaussian pulses are assumed. Each symbol can contain up to $N = \log_2 M$ bits, i.e. one qu-N-it.

σ_t (σ_ω) represents half the $1/e$ width of the energy density of a PPM (FSK) symbol pulse. Δt ($\Delta\omega$) is the symbol pulse separation in the time (frequency) domain. The central frequency (time) of the conjugated PPM (FSK) pulses is chosen such that they are centered with respect to the FSK (PPM) symbol pulses in the frequency (time) domain. The $1/e$ half-widths of the symbol pulses and conjugate pulses are reciprocal. The pulse energy density is given by

$$\rho_\sigma(z) \equiv |\psi_\sigma(z)|^2 \equiv \frac{\sqrt{2}}{\sigma}\phi\left(\sqrt{2}\frac{z}{\sigma}\right) \tag{3.1}$$

Here $\phi(z) = 1/(2\pi)^{1/2}\exp\{-z^2/2\}$ is the standard normal distribution, σ is equal to σ_t (σ_ω) for the PPM (FSK) symbol pulse and σ_ω^{-1} (σ_t^{-1}) for the conjugated FSK (PPM) pulse. Furthermore $z = t$ for time ($z = \omega$ for frequency) pulses.

Perfect overlap of both bases and information loss due to the measurement in the wrong basis cannot be perfectly achieved. However, with the following two pulse relations both can be approached:

(i) The full $1/e$ width of the PPM (FSK) symbol pulse is similar to the pulse distance:

$$\Delta t \approx 2\sigma_t \tag{3.2}$$

$$\Delta\omega \approx 2\sigma_\omega \tag{3.3}$$

(ii) The conjugated PPM (FSK) pulse is approximately as wide as all M FSK (PPM) symbol pulses combined:

$$2\sigma_t^{-1} \approx M\Delta\omega \tag{3.4}$$

$$2\sigma_\omega^{-1} \approx M\Delta t \tag{3.5}$$

From (i) the quantitative pulse relations for the symbol pulses can be distilled to be

$$\alpha \equiv \frac{2\sigma_t}{\Delta t} = \frac{2\sigma_\omega}{\Delta\omega} \tag{3.6}$$

and with (ii) the quantitative pulse relations for the conjugated pulses can be distilled to be

$$\beta \equiv \frac{2\sigma_{\omega}^{-1}}{M\Delta t} = \frac{2\sigma_{t}^{-1}}{M\Delta\omega}. \tag{3.7}$$

α is the normalized $1/e$ width of the intensity $\rho_{\sigma}(z)$ of the symbol pulses and β of the conjugated pulses. For simplicity, the pulse relations are assumed to be equal for PPM and FSK pulses in both domains. This results in time and frequency being interchangeable in the calculations carried out in this chapter.

$\alpha = 1$ and $\beta = 1$ would mean replacing the approximately-equal sines with equal signs in 3.6 and 3.7 respectively. Thus, following (i) and (ii) it is assumed, that optimal values for α and β will be near one.

At this point, it is assumed, that every pulse contains exactly one photon and noise is neglected. Typically, classical PPM systems have dead time between each symbol [125], thus inter-symbol interference is neglected as well.

It is assumed, that Bob and Eve filter the photons depending on their position in the time (frequency) domain and measure each filter bin by means of a single photon detector. In the following, the position of the filter bins with respect to the pulse positions will be defined. Figure 3.2 shows the bin and symbol pulse positions for $M = 4$. The part of the pulse, which spills in neighboring bins, is called spill region. The center position $c(i)$ of the i^{th} symbol pulse is defined as

$$c(i) = i - \frac{M+1}{2}, \tag{3.8}$$

normalized to Δt ($\Delta\omega$) and with $i = [1, M]$ numbering the PPM (FSK) symbol pulses in a ascending manner.

Rectangular filters are assumed for Bob and Eve, because it reduces complexity, but also because it is the preferred filter shape to prevent additional errors which would otherwise occur due to overlapping bins. Each bin is defined by its lower $f_{\text{low}}(j)$ and upper bound $f_{\text{up}}(j)$, again normalized to Δt ($\Delta\omega$) for time (frequency) basis:

$$f_{\text{low}}(j) = \begin{cases} -\infty & \text{for } j = 1 \\ j - \frac{1}{2}M - 1 & \text{for } j = 2, ..., M \end{cases} \tag{3.9}$$

$$f_{\text{up}}(j) = \begin{cases} j - \frac{1}{2}M & \text{for } j = 1, ..., M-1 \\ +\infty & \text{for } j = M \end{cases} \tag{3.10}$$

The outer bins (i.e. $j = 1$ or $j = M$) are chosen to be unbounded on their outer site (differently stated, the respective bounds are at $\pm\infty$). In this way it is assured, that every symbol is detected and the cumulative probability is always 1. If the time (frequency) domain would not be entirely defined in terms of measurement bins, additional losses would occur due to Gaussian pulses extending into infinity, which was explicitly detached from the probabilities in Section 2.2.1.

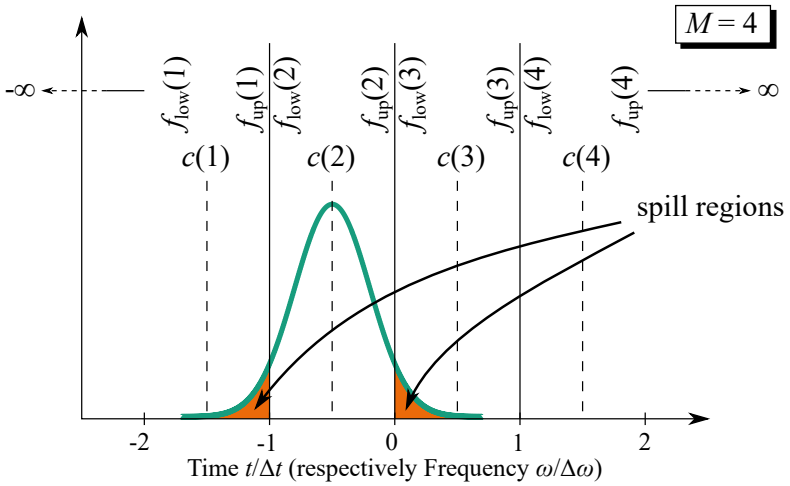


Figure 3.2.: Definition of bins for TF-QKD for $M = 4$. Each symbol is associated to a symbol pulse located in a given bin. Bins, are defined in the time and frequency domains by their lower and upper bounds $b_{\text{low}}(j)$ and $b_{\text{up}}(j)$. The centers of the symbol pulses sent by the sender Alice are given by $c(i)$. As an example a pulse sent in the second bin is shown. The regions, which spill in other bins, namely the spill regions, are also marked.

3.2. One-level intercept/resend attack

The present analysis starts with assuming Eve to perform a standard intercept/resend (IR)-attack [126], here called the one-level IR-attack in order to distinguish it from the two-level IR-attack, described later in Section 3.3. Eve will measure a fraction ε of the symbols sent by Alice randomly either in the PPM or in the FSK basis and forward the rest of the symbols unaltered to Bob. For each intercepted symbols she resends a symbol of her own. She will use the basis, in which she has performed her measurement and send the symbol she has measured to Bob.

With Section 3.1 the necessary tools to address the process from Alice partially over Eve to Bob are at hand. The conditional probability for the sending processes, both with and without Eve attacking on the photons and the corresponding probabilities of Alice, Bob and Eve are needed. Subsequently, with those probabilities, the mutual information can be calculated. In the following, it is assumed, that Alice and Bob do the steps specified in Section 2.1.2. Only photons detected by Bob's detectors are considered in the following, thus loss will not be part of the following analysis.

3.2.1. Undisturbed QKD transmission

For the case where Eve is not intercepting the symbols the transmission can be described by Alice sending symbols directly to Bob. Because of the sifting process Bob will be in the correct basis with respect to Alice in all relevant cases. Firstly, it is assumed, that both are in the PPM basis. The probabilities for Alice sending a symbol in the PPM basis and Bob also measuring it in the PPM basis is shown in Figure 3.3 (a) for $M = 4$. The conditional probability becomes

$$\begin{aligned} P_{B|A}^{\text{correct}}(b|a) &= \int_{(f_{\text{low}}(b)-c(a))\Delta t}^{(f_{\text{up}}(b)-c(a))\Delta t} \rho_{\sigma_t}(t)\, dt \\ &= \frac{\sqrt{2}}{\sigma_t} \int_{(f_{\text{low}}(b)-c(a))\Delta t}^{(f_{\text{up}}(r)-c(a))\Delta t} \phi\left(\sqrt{2}\frac{t}{\sigma_t}\right) dt. \end{aligned} \tag{3.11}$$

With the substitution $t = x\Delta t$ and (3.6), $P_{B|A}^{\text{correct}}(b|a)$ can be expressed by means of the normalized symbol pulse width α.

$$\begin{aligned} P_{B|A}^{\text{correct}}(b|a) &= \frac{\sqrt{2}\Delta t}{\sigma_t} \int_{f_{\text{low}}(b)-c(a)}^{f_{\text{up}}(r)-c(a)} \phi\left(\sqrt{2}\frac{x\Delta t}{\sigma_t}\right) dx \\ &= \frac{\sqrt{2}}{\alpha} \int_{f_{\text{low}}(r)-c(a)}^{f_{\text{up}}(b)-c(a)} \phi\left(\sqrt{2}\frac{2x}{\alpha}\right) dx. \end{aligned} \tag{3.12}$$

$P_{B|A}^{\text{correct}}(b|a)$, as described in Section 2.2.1, can be arranged as the $M \times M$-Matrix $\mathbf{P}_{B|A}^{\text{correct}}$. This expression is independent of basis or domain specific variables.

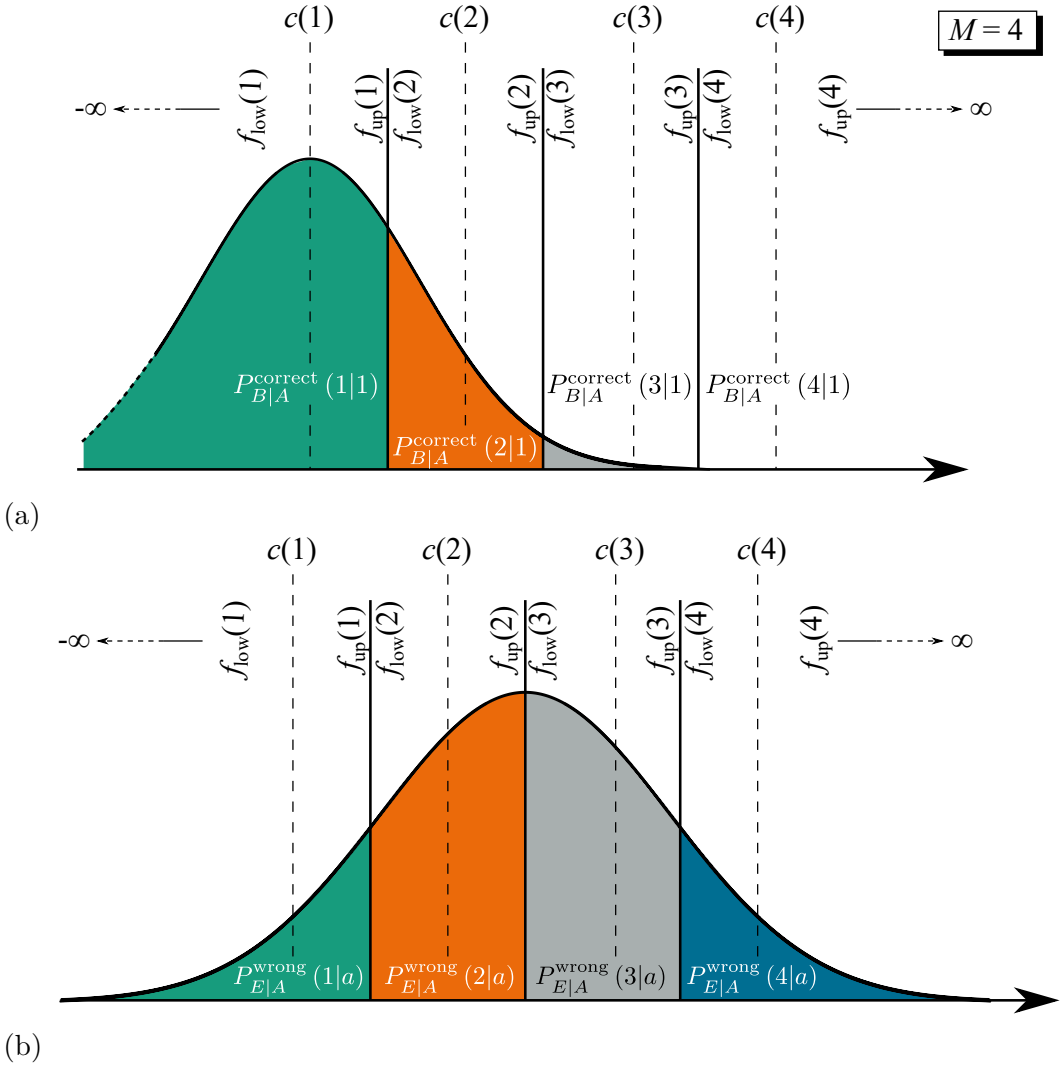


Figure 3.3.: Visualization of the conditional probability for symbol and conjugated pulses for $M = 4$ symbols per basis. (a) The first symbol is sent by Alice and measured by Bob in the pulse-position modulation (PPM) basis. (b) A symbol is sent by Alice in the frequency-shift keying (FSK) basis and measured in the PPM basis by Eve

It can easily be shown, that the same expression can be obtained by considering Alice sending in the FSK basis and Bob measuring in the FSK basis. This would result in calculations analogue to what was done above (by changing $\Delta t \to \Delta\omega$, $\sigma_t \to \sigma_\omega$, integrate over $dt \to d\omega$ and respectively change the substitution $t = x\Delta t \to \omega = x\Delta\omega$).

In order to describe the entire sending process, photons being encoded in both, the PPM and FSK basis have to be considered. Consequently the probability vectors and conditional probability matrices need to be merged to vectors of length $2M$ and $2M \times 2M$-matrices, respectively. The conditional probability matrices for for the whole process including the PPM an FSK basis becomes

$$\mathbf{P}_{B|A}^{\text{Bob}} = \begin{pmatrix} \mathbf{P}_{B|A}^{\text{correct}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \mathbf{P}_{B|A}^{\text{correct}} \end{pmatrix}, \tag{3.13}$$

in the case where no eavesdropping occurs. $\mathbf{0}_{M,M}$ describes a $M \times M$ zero matrix. It is assumed that Alice sends all symbols of both bases with the same probability. Thus her probability for sending a out of A is

$$P_A^{\text{Alice}}(a) = \frac{1}{2M}, \tag{3.14}$$

which can be arranged as the vector

$$\mathbf{P}_A^{\text{Alice}} = \frac{1}{2M} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \tag{3.15}$$

with $2M$ vector elements. With this the probability for Bob measuring the different symbols can be calculated by using (3.13) and (2.10). It follows

$$\mathbf{P}_A^{\text{Bob}} = \mathbf{P}_{A,B}^{\text{Bob}} \mathbf{P}_A^{\text{Alice}} \tag{3.16}$$

3.2.2. Leakage to the eavesdropper

After finding the conditional probability matrix for the transmission from Alice to Bob without Eve interfering, the same must be done for the case where Eve is interfering with the transmission. More precisely Alice sends symbols to Eve. Eve randomly switches her measurement basis, which will make her sometimes be in the correct and sometimes in the wrong basis.

In the case where Eve measures in the basis Alice sent in, analogue to (3.12) it follows

$$P_{E|A}^{\text{correct}}(e|a) = \frac{\sqrt{2}}{\alpha} \int_{f_{\text{low}}(r)-c(a)}^{f_{\text{up}}(e)-c(a)} \phi\left(\sqrt{2}\frac{2x}{\alpha}\right) dx, \tag{3.17}$$

with the according $M \times M$-Matrix $\mathbf{P}_{E|A}^{\text{correct}}$.

Contrary to Bob, Eve will measure the symbols in the wrong basis in some of the relevant cases. As shown in Figure 3.3 (b) for $M = 4$, when Alice sends in the FSK basis and Eve measures in the PPM basis, it follows that

$$\begin{aligned} P_{E|A}^{\text{wrong}}(e|a) &= \int_{f_{\text{low}}(e)\Delta t}^{f_{\text{up}}(e)\Delta t} \rho_{\sigma_\omega^{-1}}(t)\, dt \\ &= \frac{\sqrt{2}}{\sigma_\omega^{-1}} \int_{f_{\text{low}}(e)\Delta t}^{f_{\text{up}}(e)\Delta t} \phi\left(\sqrt{2}\frac{t}{\sigma_\omega^{-1}}\right) dt. \end{aligned} \tag{3.18}$$

This expression is independent of the symbol a, Alice sends. This is of cause deliberate in order not to have any correlation between the sent symbol and the conjugated pulse. With the substitution $t = x\Delta t$ and (3.7), $P_{E|A}^{\text{wrong}}(e|a)$ can be written in terms of the normalized conjugated pulse width β and the number of symbols per basis M and becomes

$$\begin{aligned} P_{E|A}^{\text{wrong}}(e|a) &= \frac{\sqrt{2}\Delta t}{\sigma_\omega^{-1}} \int_{f_{\text{low}}(e)}^{f_{\text{up}}(e)} \phi\left(\sqrt{2}\frac{\Delta t x}{\sigma_\omega^{-1}}\right) dx \\ &= \frac{\sqrt{2}}{\beta M} \int_{f_{\text{low}}(e)}^{f_{\text{up}}(e)} \phi\left(\sqrt{2}\frac{2x}{\beta M}\right) dx, \end{aligned} \tag{3.19}$$

which can be written as the $M \times M$ Matrix $\mathbf{P}_{E|A}^{\text{wrong}}$. Note, that $\mathbf{P}_{E|A}^{\text{wrong}}$ has the property, that it's matrix product with a probability vector always results in a vector which has the same elements as any of the (equal) rows of the matrix, see Appendix A.1.

If Eve measures in the PPM basis, the transmission for both cases, namely Alice sending in the PPM basis (Eve measuring in the correct basis with respect to Alice) and Alice sending in the FSK basis (Eve measuring in the wrong basis with respect to Alice) can be combined into one $2M \times 2M$ matrix

$$\mathbf{P}_{E|A}^{\text{Eve,PPM}} = \begin{pmatrix} \mathbf{P}_{E|A}^{\text{correct}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \mathbf{P}_{E|A}^{\text{wrong}} \end{pmatrix} \tag{3.20}$$

If Alice prepares all symbols in the FSK basis, it can similarly be found that

$$\mathbf{P}_{E|A}^{\text{Eve,FSK}} = \begin{pmatrix} \mathbf{P}_{E|A}^{\text{wrong}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \mathbf{P}_{E|A}^{\text{correct}} \end{pmatrix}. \tag{3.21}$$

With (3.20) and (3.21) respectively the probability vector of Eve for both cases can be calculated and becomes

$$\mathbf{P}_{E}^{\text{Eve,PPM}} = \mathbf{P}_{E|A}^{\text{Eve,PPM}} \mathbf{P}_{A}^{\text{Alice}}. \tag{3.22}$$

and

$$\mathbf{P}_{E}^{\text{Eve,FSK}} = \mathbf{P}_{E|A}^{\text{Eve,FSK}} \mathbf{P}_{A}^{\text{Alice}}. \tag{3.23}$$

Since the sifting process is public, Eve will have the knowledge of which basis Alice and Bob used after sifting. However, since the sifting will be done after all photons are sent and measured, she will not have this information, when she resends photons, as will be discussed next.

3.2.3. Influence of eavesdropping on the receiver

When Eve measures Alice's symbol, she will prepare a new symbol according to her measurement. In other words, she resends the symbol that she measured in the basis she measured it in. Initially, the two cases where Eve is in the PPM basis and where she is in the FSK basis are separated. Let us first consider the case where Eve is in the PPM basis.

The conditional probability matrix for the transmission process from Alice to Eve was calculated in (3.20). When Eve is in the correct (wrong) basis with respect to Alice, Bob is also in the correct (wrong) basis with respect to Eve, resulting in

$$\mathbf{P}_{B|E}^{\text{Eve,PPM}} = \begin{pmatrix} \mathbf{P}_{B|E}^{\text{correct}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \mathbf{P}_{B|E}^{\text{wrong}} \end{pmatrix}, \tag{3.24}$$

where $\mathbf{P}_{B|E}^{\text{correct}} = \mathbf{P}_{E|A}^{\text{correct}}$ and $\mathbf{P}_{B|E}^{\text{wrong}} = \mathbf{P}_{E|A}^{\text{wrong}}$, because it is assumed, that Eve uses the same filters as Bob and the same pulse relations as Alice. For the transmission from Alice over Eve to Bob, both matrices can be multiplied (as described in Section 2.2.1 resulting in (2.14)) and can be written as

$$\begin{aligned} \mathbf{P}_{B|A}^{\text{Bob,IR,PPM}} &= \mathbf{P}_{B|E}^{\text{Eve,PPM}} \mathbf{P}_{E|A}^{\text{Eve,PPM}} \\ &= \begin{pmatrix} \left(\mathbf{P}_{B|A}^{\text{correct}}\right)^2 & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \left(\mathbf{P}_{B|A}^{\text{wrong}}\right)^2 \end{pmatrix} \\ &= \begin{pmatrix} \left(\mathbf{P}_{B|A}^{\text{correct}}\right)^2 & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \mathbf{P}_{B|A}^{\text{wrong}} \end{pmatrix} \end{aligned} \tag{3.25}$$

as the conditional probability matrix for the transmission process from Alice over Eve to Bob. In Appendix A.1 the relation $\left(\mathbf{P}_{B|A}^{\text{wrong}}\right)^2 = \mathbf{P}_{B|A}^{\text{wrong}}$ is derived.

Analogue, when Eve measures in the FSK basis it follows that

$$\mathbf{P}_{B|A}^{\text{Bob,IR,FSK}} = \begin{pmatrix} \mathbf{P}_{B|A}^{\text{wrong}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \left(\mathbf{P}_{B|A}^{\text{correct}}\right)^2 \end{pmatrix}. \tag{3.26}$$

Because Eve randomly chooses one of the two bases, both transmission processes described by (3.25) and (3.26) have to be averaged. It follows that

$$\begin{aligned}\mathbf{P}_{B|A}^{\text{Bob,IR}} &= \frac{1}{2}\left(\mathbf{P}_{B|A}^{\text{Bob,IR,PPM}} + \mathbf{P}_{B|A}^{\text{Bob,IR,FSK}}\right) \\ &= \frac{1}{2}\begin{pmatrix} \left(\mathbf{P}_{B|A}^{\text{correct}}\right)^2 + \mathbf{P}_{B|A}^{\text{wrong}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \left(\mathbf{P}_{B|A}^{\text{correct}}\right)^2 + \mathbf{P}_{B|A}^{\text{wrong}} \end{pmatrix},\end{aligned} \tag{3.27}$$

from which the probability vector of Bob when Eve attacks can be calculated to be

$$\mathbf{P}_{B}^{\text{Bob,IR}} = \mathbf{P}_{B|A}^{\text{Bob,IR}}\mathbf{P}_{A} \tag{3.28}$$

If Eve attacks on a fraction ε of the symbols (represented by (3.27)) and leaves $(1-\varepsilon)$ untouched (represented by (3.13)), the conditional probability matrix $\mathbf{P}_{B|A}^{\text{Bob},\varepsilon}$ becomes

$$\mathbf{P}_{B|A}^{\text{Bob},\varepsilon} = (1-\varepsilon)\,\mathbf{P}_{B|A}^{\text{Bob}} + \varepsilon\mathbf{P}_{B|A}^{\text{Bob,IR}}. \tag{3.29}$$

Bob's probability vector can now be calculated to

$$\mathbf{P}_{B}^{\text{Bob},\varepsilon} = \mathbf{P}_{B|A}^{\text{Bob},\varepsilon}\mathbf{P}_{A} \tag{3.30}$$

In (2.17) the QSER was defined for one basis and $M \times M$-matrices. For the presented case of PPM and FSK basis, which result in $2M \times 2M$-matrices the QSER needs to be modified accordingly by writing

$$Q_M = 1 - \frac{1}{2M}\text{tr}\left(\mathbf{P}_{B|A}^{\text{Bob},\varepsilon}\right), \tag{3.31}$$

with Q_2 being the QBER for $M = 2$.

3.2.4. Secret capacity

With (2.21) the mutual information between Alice and Bob, when Eve attacks on a fraction ε of the symbols can be calculated:

$$I_{A,B} = \sum_{b=1}^{2M}\sum_{a=1}^{2M} P_{B|A}^{\text{Bob},\varepsilon}(b|a)P_A(a)\log_2\left(\frac{P_{B|A}^{\text{Bob},\varepsilon}(b|a)}{P_B^{\text{Bob},\varepsilon}(b)}\right) - 1. \tag{3.32}$$

The mutual information between Alice and Eve can be calculated with (3.20), (3.21), (3.22) and (3.23) and becomes

$$\begin{aligned} I_{A,E}^{\mathrm{1L}} = & \underbrace{\frac{\varepsilon}{2}\left[\sum_{e=1}^{2M}\sum_{a=1}^{2M} P_{E|A}^{\mathrm{Eve,PPM}}(e|a)\, P_A(a) \log_2\left(\frac{P_{E|A}^{\mathrm{Eve,PPM}}(e|a)}{P_E(e)}\right) - 1\right]}_{\text{Mutual information for Eve measuring in the PPM basis}} \\ & + \underbrace{\frac{\varepsilon}{2}\left[\sum_{e=1}^{2M}\sum_{a=1}^{2M} P_{E|A}^{\mathrm{Eve,FSK}}(e|a)\, P_A(a) \log_2\left(\frac{P_{E|A}^{\mathrm{Eve,FSK}}(e|a)}{P_E(e)}\right) - 1\right]}_{\text{Mutual information for Eve measuring in the FSK basis}} \end{aligned} \tag{3.33}$$

The "1L" as a superscript denotes the mutual information to the one-level IR-attack in order to distinguish it from the mutual information for the two-level IR-attack, which will be calculated in Section 3.3.

There is one summand for $I_{A,B}$ (3.32) and two summands for $I_{A,E}$ (3.44) which can be explained by the following: Bob does not know, which basis Eve has chosen (correct or wrong basis), thus the mean over both cases was taken to calculate his mutual information. In contrast, Eve knows Alice and Bobs basis choice after the sifting process thus can distinguish between them. Both cases do not blend together, consequently, the mutual information can be calculated separately and summing the results. Note that the mutual information for Eve is higher when her knowledge about Alice's and Bob's basis choice is taken into account.

Because of the basis symmetry, the two summands in Eve's mutual information are equal. (3.44) can be simplified resulting in

$$I_{A,E}^{\mathrm{1L}} = \varepsilon\left[\sum_{e=1}^{2M}\sum_{a=1}^{2M} P_{E|A}^{\mathrm{Eve,PPM}}(e|a)\, P_A(a) \log_2\left(\frac{P_{E|A}^{\mathrm{Eve,PPM}}(e|a)}{P_E(e)}\right) - 1\right]. \tag{3.34}$$

The secret capacity can finally be calculated with (2.22), which is depending on the fraction of photons ε Eve eavesdrops on:

$$C_{\mathrm{1L}} = \begin{cases} I_{A,B} - I_{A,E}^{\mathrm{1L}} & \text{for } I_{A,B} > I_{A,E}^{\mathrm{1L}} \\ 0 & \text{for } I_{A,B} \leq I_{A,E}^{\mathrm{1L}} \end{cases} \tag{3.35}$$

3.2.5. Conclusion on the one-level intercept/resend attack

The secret capacity C_{1L} from (3.35) is plotted over α and β in Figure 3.4 for the example of $M = 4$ and $\varepsilon = 0.5$. Regarding the normalized symbol pulses width, regarded by α, one can draw the conclusion, that indeed narrow pulses are preferable, as suggested in [83]. However, in the one-level IR-attack the information

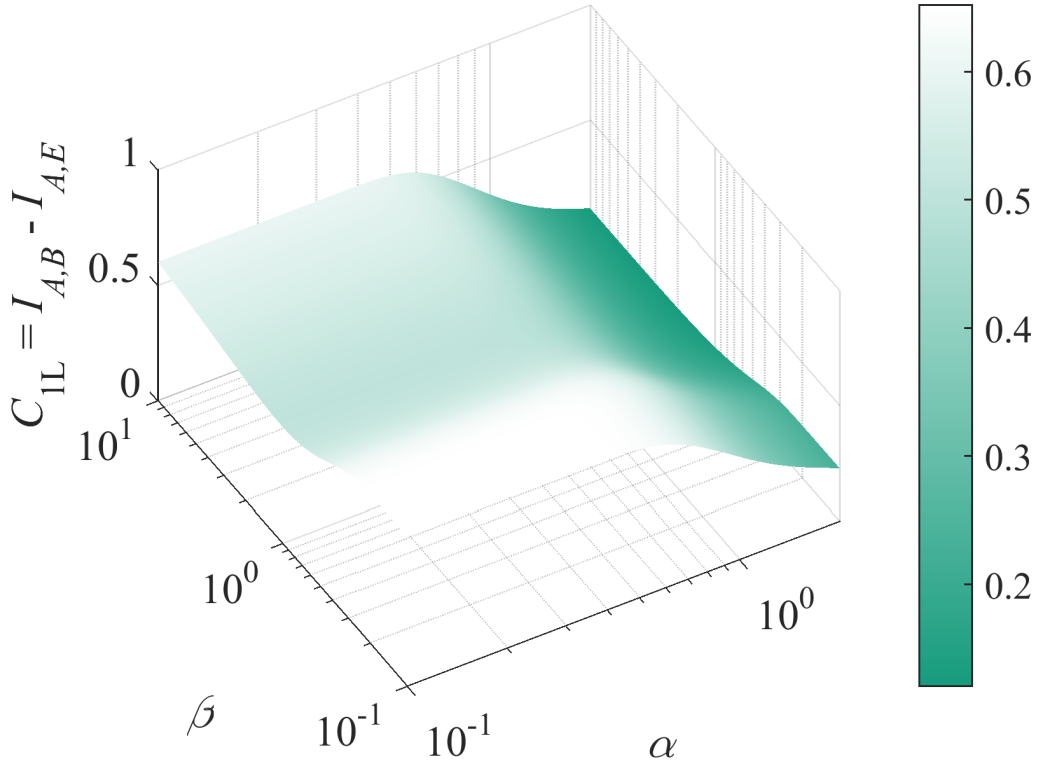


Figure 3.4.: Secret capacity C_{1L} in bits per symbol for the one-level intercept/resend (IR) attack. Here it is shown for the number of symbols per basis $M = 4$ and the fraction $\varepsilon = 0.5$ of sent photons Eve is eavesdropping on. The secret capacity is plotted over α and β, which are the normalized symbol and conjugated pulse width, respectively.

still present in the conjugated basis is ignored by Eve. Thus this attack did not consider one of the most important weaknesses of the TF-QKD protocol.

In the next section the two-level IR strategy, which considers this weakness, will be discussed. The results presented in this section are similar to the IR-strategy for protocols like the BB84 protocol, which does not hold this weakness and will serve as a comparison for the two-level IR-attack.

3.3. two-level intercept/resend attack

As mentioned in Section 2.1.2 measuring in one basis does not delete the entire mutual information possibly encoded in the other basis, contrary to other QKD

protocols, like e.g. BB84. Eve could utilize this to increase her mutual information. There are different strategies conceivable, Eve could use. One of which is explained in [83], where the performance of a prepare-and-measure TF-QKD using DV is investigated. The key assumption there is, that the pulses are very narrow compared to their distance, as was proposed in [66] for the CV based TF-QKD. In the attack described there, Eve exploits the small width of the pulses by measuring only a slice of the PPM (FSK) basis and forwarding all the photons, which are not inside the slices to the FSK (PPM) basis. The center of the slices and the center of the PPM (FSK) pulses are chosen by Eve to coincide. Towards the asymptotic case of indefinitely narrow pulses, the slices could become smaller, decreasing what is extracted from a hypothetical conjugated pulse.

Using narrow pulses was proposed in [66] for CV version of TF-QKD, not the DV version. There it was shown, that in the CV version of TF-QKD narrow pulses are preferable since there are no gaps between the pulses there. Thus both bases can be made indistinguishable. However, this is not the case for the DV version, thus narrow pulses might not be the optimal choice here. In the following wide pulses are taken into account for which in general only measuring slices is not beneficial anymore. Thus, a different IR-strategy is discussed in the following.

3.3.1. Modification of the eavesdropping strategy

In the IR-strategy presented here, referred to as the two-level IR-attack, Eve measures the photons either first in the PPM and then in the FSK basis or vice versa by cascading the filters as shown in Figure 3.5. Rectangular filters are assumed. Further, it is assumed, that Eve picks the first basis to be PPM or FSK equally likely. Eve uses PPM (FSK) filters of width Δt ($\Delta\omega$) where each filter output forwards the photons to a second set of M rectangular FSK (PPM) filters of width $\Delta\omega$ (Δt). Their outputs forward the photons to a total of $2M^2$ detectors.

Eve will only learn the used bases during the sifting process after the transmission, thus we assume she will resend photons according to the outcome of the first filter. Since the pulses are not yet broadened, there they thus contain more information. Consequently, Bob's mutual information does not change compared to the one-level IR. What does change is that Eve's mutual information increases due to the second filter.

3.3.2. Additional information for the eavesdropper

Initially, it is assumed, that Eve filters in the PPM basis first and subsequently in the FSK basis. She will thus measure in the correct basis with respect to Alice first, whenever Alice sends in the PPM basis. Eve will filter a second time in the FSK

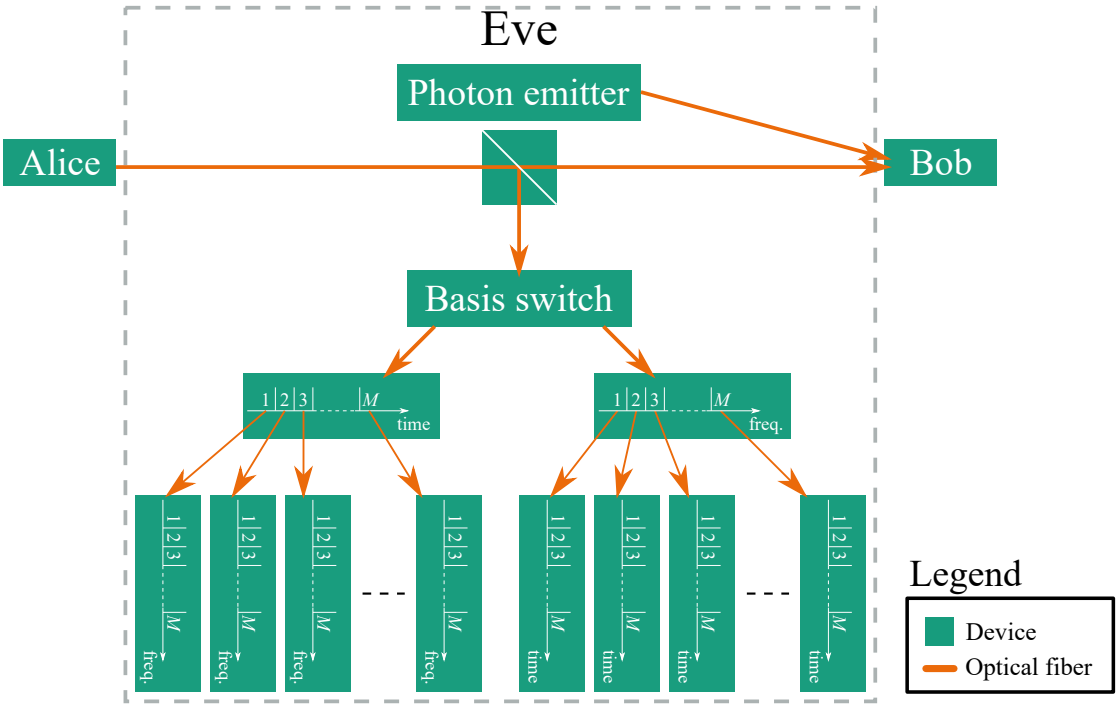


Figure 3.5.: Eves eavesdropping setup for the two-level intercept/resend attack. Eve randomly selects a fraction ε of the sent photons and forwards them to her measurement apparatus while leaving the rest untouched. Then she filters the photons firstly in the time domain (level one) and then in the frequency domain (level two) or vice versa. Thus she gets at least some information in both bases for every photon. After measuring the photons Eve resends a photon according to the first level.

basis, but she will discard the results there as soon as she learns Alice's and Bob's basis choice during the sifting process. For this case, the second filtering level does not change Eves mutual information, compared to the one-level IR-attack.

However, whenever Alice uses the FSK basis, Eve will first measure in the wrong basis with respect to Alice. In the one-level IR-attack, Eve would not get any information, whereas here she can still learn something about the key.

The truncating of the conjugated pulse in the FSK basis due to the first filter will reshape the symbol pulse in the PPM basis according to the Fourier transform denoted as $\mathcal{F}()(\omega)$. However, the center position of the symbol pulse in the FSK basis will not change. The modified pulse can be described by

$$\begin{aligned} g_f(\omega) &= \left| \mathcal{F}\left(\psi_{\sigma_\omega^{-1}}(t) H_f\left(\frac{t}{\Delta t}\right)\right)(\omega)\right|^2 \\ &= \frac{\sigma_\omega}{\sqrt{\pi}} \left| \int_{-\infty}^{+\infty} \phi\left(\frac{t}{\sigma_\omega^{-1}}\right) H_f\left(\frac{t}{\Delta t}\right) e^{-i\omega t} dt \right|^2 \end{aligned} \tag{3.36}$$

with the rectangular filter function being defined as

$$H_f\left(\frac{t}{\Delta t}\right) = \begin{cases} 1 & \text{for } b_{\text{low}}(f) < t/\Delta t < b_{\text{up}}(f) \\ 0 & \text{otherwise.} \end{cases} \tag{3.37}$$

With applying the substitutions $t = x\sigma_\omega^{-1}$ and $\omega = w\sigma_\omega$ the modified pulse can be written as

$$g_f(w) = \frac{1}{\sqrt{\pi}} \left| \int_{-\infty}^{+\infty} \phi(x) H_f\left(\frac{M\beta x}{2}\right) e^{-iwx} dx \right|^2. \tag{3.38}$$

Consequently, for the second filtering process the conditional probability follows to be

$$P_{E|A}^{2^{\text{nd}}\,\text{correct}}(e|a) = \sum_{f=1}^{M} \int_{(b_{\text{low}}(e)-c(a))\Delta\omega}^{(b_{\text{up}}(e)-c(a))\Delta\omega} g_f(\tilde{\omega})\, d\tilde{\omega} \tag{3.39}$$

which can be arranged as the conditional probability matrix $\mathbf{P}_{E|A}^{2^{\text{nd}}\text{correct}}(e|a)$. The conditional probability matrix for both bases thus becomes

$$\mathbf{P}_{E|A}^{\text{Eve,2L,PPM}} = \begin{pmatrix} \mathbf{P}_{E|A}^{\text{correct}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \mathbf{P}_{E|A}^{2^{\text{nd}}\text{correct}} \end{pmatrix} \tag{3.40}$$

for Eve measuring firstly in the PPM and secondly in the FSK basis. The superscript 2L ascribes the conditional probability matrix to the two-level IR-attack. Analogous, The conditional probability for the case where Eve first filters in the FSK basis and second in the PPM basis can be written as

$$\mathbf{P}_{E|A}^{\text{Eve,2L,FSK}} = \begin{pmatrix} \mathbf{P}_{E|A}^{2^{\text{nd}}\text{correct}} & \mathbf{0}_{M,M} \\ \mathbf{0}_{M,M} & \mathbf{P}_{E|A}^{\text{correct}} \end{pmatrix}. \tag{3.41}$$

Accordingly, the probability vectors become

$$\mathbf{P}_E^{\text{Eve,2L,PPM}} = \mathbf{P}_{E|A}^{\text{Eve,2L,PPM}} \mathbf{P}_A^{\text{Alice}}. \tag{3.42}$$

$$\mathbf{P}_E^{\text{Eve,2L,FSK}} = \mathbf{P}_{E|A}^{\text{Eve,2L,FSK}} \mathbf{P}_A^{\text{Alice}}. \tag{3.43}$$

With this the mutual information between Alice and Eve can finally be written analogue to 3.44 and 3.34 as

$$\begin{aligned} I_{A,E}^{\text{2L}} &= \frac{\varepsilon}{2} \left[\sum_{e=1}^{2M} \sum_{a=1}^{2M} P_{E|A}^{\text{Eve,2L,PPM}}(e|a)\, P_A(a) \log_2 \left(\frac{P_{E|A}^{\text{Eve,2L,PPM}}(e|a)}{P_E(e)} \right) - 1 \right] \\ &\quad + \frac{\varepsilon}{2} \left[\sum_{e=1}^{2M} \sum_{a=1}^{2M} P_{E|A}^{\text{Eve,2L,FSK}}(e|a)\, P_A(a) \log_2 \left(\frac{P_{E|A}^{\text{Eve,2L,FSK}}(e|a)}{P_E(e)} \right) - 1 \right] \\ &= \varepsilon \left[\sum_{e=1}^{2M} \sum_{a=1}^{2M} P_{E|A}^{\text{Eve,2L,PPM}}(e|a)\, P_A(a) \log_2 \left(\frac{P_{E|A}^{\text{Eve,2L,PPM}}(e|a)}{P_E(e)} \right) - 1 \right]. \end{aligned} \tag{3.44}$$

Consequently, the secret capacity becomes

$$C_{\text{2L}} = \begin{cases} I_{A,B} - I_{A,E}^{\text{2L}} & \text{for } I_{A,B} > I_{A,E}^{\text{2L}} \\ 0 & \text{for } I_{A,B} \leq I_{A,E}^{\text{2L}} \end{cases} \tag{3.45}$$

3.3.3. Optimizing the symbol pulses

With (3.44) the secret capacity C can be plotted over α and β, as can be seen in Figure 3.6 for $M = 4$ and $\varepsilon = 0.5$.

Comparing Figure 3.6 with Figure 3.4 it can be observed, that the two-level IR-attack first and foremost decreases the secret capacity for narrower pulses. This underlines that small α and therefore narrow symbol pulses are not the preferred choice for the DV version of the TF-QKD protocol. Since the two-level IR-attack regards more of Eves capabilities, it will be assumed from here on, that Eve is using the two-level IR-attack.

Note, that for $M = 2$ all entries of $\mathbf{P}_{E|A}^{\text{wrong}}$ become 0.5, independent of the value for β. looking at Figure 3.3 (b) the reason becomes obvious: If the pulse is split in it's middle, the probability for measuring a photon in one of the two bins is equal and thus need to be 0.5. Consequently C_{2L} (and also C_{1L}) is independent from β.

Moreover for $M > 2$, e.g. $M = 4$, as in Figure 3.4, the optimal normalized symbol pulse width α_{opt} and the optimal secret capacity $C_{\text{opt, 2L}}$ are not changed by the normalized conjugated pulses width β.

Arguments on how to find the optimal normalized conjugated pulse width β will be discussed in the next section.

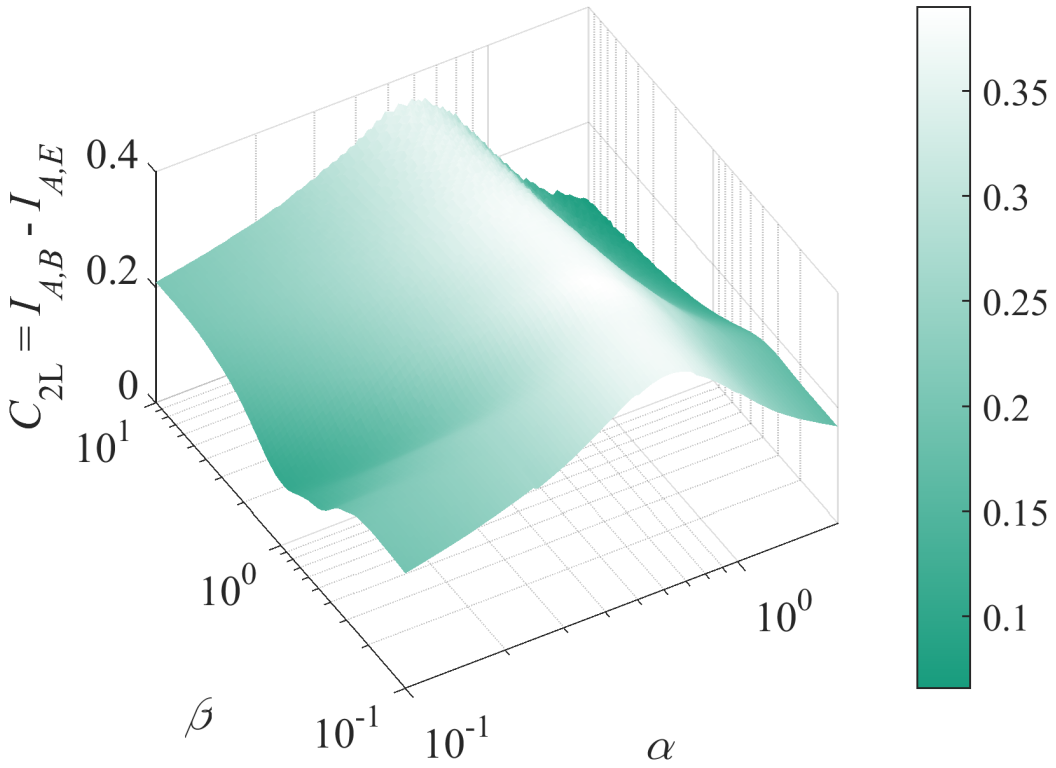


Figure 3.6.: Secret capacity C_{2L} per symbol in bits for the two-level intercept/resend (IR) attack. Here it is shown for the number of symbols per basis $M = 4$ and the fraction $\varepsilon = 0.5$ of sent photons Eve is eavesdropping on. The secret capacity is plotted over α and β, which are the normalized symbol and conjugated pulse width, respectively.

3.3.4. Optimize the conjugated pulses

Neither in the one-level nor in the two-level IR-attack, Eve exploits the imperfect overlap of conjugated and symbol pulses in the same domain. One example of such a strategy is described in [83]. The attack described there can be generalized to Eve performing a basis depending attack. By utilizing, that at certain areas in the time (or frequency) domain, it is more probable to measure a symbol pulse than a conjugated pulse or vice versa. Based on that knowledge, she either measures the pulse in the time (or frequency) domain or sends them further to a frequency (or time) measuring device. Rather than simulating this exact or a similar strategy, the focus will lie on minimizing the weakness of imperfectly overlapping symbol and conjugated pulses.

As mentioned before, a security proof for the CV version of the TF-QKD protocol was carried out in [66]. The key statement there was, that it is possible to bring symbol and conjugated pulses to perfect overlap, namely to show, that

$$\sum \rho_{\sigma_t}(t) = \sum \rho_{\sigma_\omega^{-1}}(t), \tag{3.46}$$

In [66] the symbol pulses are assumed to be asymptotically narrow. With a suitable probability distribution of the symbol pulses, matching the pulse form of the conjugated pulse, perfect overlap can be achieved. This is not possible if the symbols are not distributed continuously, as is the case for the DV TF-QKD protocol, which is the topic of the present work. However, a perfect overlap can at least asymptotically be approached.

In terms of the pulses, as they are defined in (3.1), the difference of the pulses defining the overlap function can be quantified

$$U_\alpha(\beta) \equiv \int \sum_{s=1}^{M} \left| \rho_{\sigma_t}\left(t + \left[s - \frac{M+1}{2}\right]\Delta t\right) - \rho_{\sigma_\omega^{-1}}(t) \right| dt \tag{3.47}$$

which is depending on the pulse forms and thus on the parameters α and β for the symbol and conjugated pulses, respectively. A visualization of $U_\alpha(\beta)$ can be seen in Figure 3.7. With α as an input β can now be varied numerically in order to find the minimum of $U_\alpha(\beta)$.

3.3.5. Numerical Optimization Results

Now, all the tools necessary to find the optimal symbol pulse α_{opt}, the optimal conjugated pulse β_{opt} and the optimal secret capacity $C_{\text{opt,2L}}$ are at hand. With this, two optimization processes were performed numerically. The optimization processes were performed with the numerical computing environment *MATLAB*. The two optimization processes were:

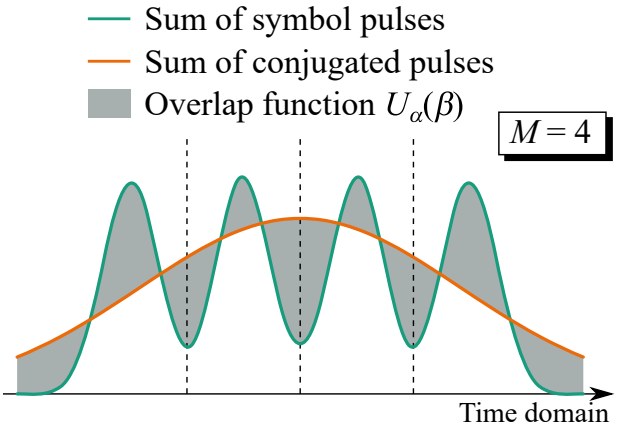


Figure 3.7.: Visualization of the overlap function. The sum of all symbol pulses and the sum of all conjugated pulses are displayed in the time basis, of which $U_\alpha(\beta)$ (3.47) is a measure for the overlap (namely, the overlap function).

1. To find the optimal symbol pulse α_{opt} and the respective optimal secret capacity $C_{\text{opt,2L}}$, $C_{\text{opt,2L}}$ was calculated for values of α in the range of 0.1 and 2, which, as can be seen from the results below, was sufficient. Subsequently the highest value for $C_{\text{opt,2L}}$ and the according α was picked.

2. To find the optimal conjugated pulse β_{opt}, $U_\alpha(\beta)$ from (3.47) was optimized numerically depending on β with $\alpha = \alpha_{\text{opt}}$ from the previous step. This was done by utilizing the function *fminsearch*, which uses the Nelder Mead Simplex algorithm [127].

The time for the optimization steps was Figure 3.6 indicated, that α_{opt} is constant for different value for β. That could be verified by again performing the optimization tasl 1. mentioned above with $\beta = \beta_{\text{opt}}$ as an input parameter. As expected, α_{opt} did not change.

α_{opt}, β_{opt} and $C_{\text{opt,2L}}$ are plotted in Figure 3.8 for different eavesdropping fractions ε. As a comparison the secret capacity for an ideal, error free transmission, namely $\log_2 M$ is shown.

It can be observed, that α_{opt} gets bigger with higher ε, in other words, when Eve attacks on a higher fraction of the transmitted photons. This can be understood, when the influence of α on the mutual information between Alice and Bob and between Alice and Eve is considered. A large α increases the spill regions and thus the QBER of Bob. On the other hand, it also decreases the mutual information between Alice and Eve. When ε is small, it is of higher weight for Alice and Bob

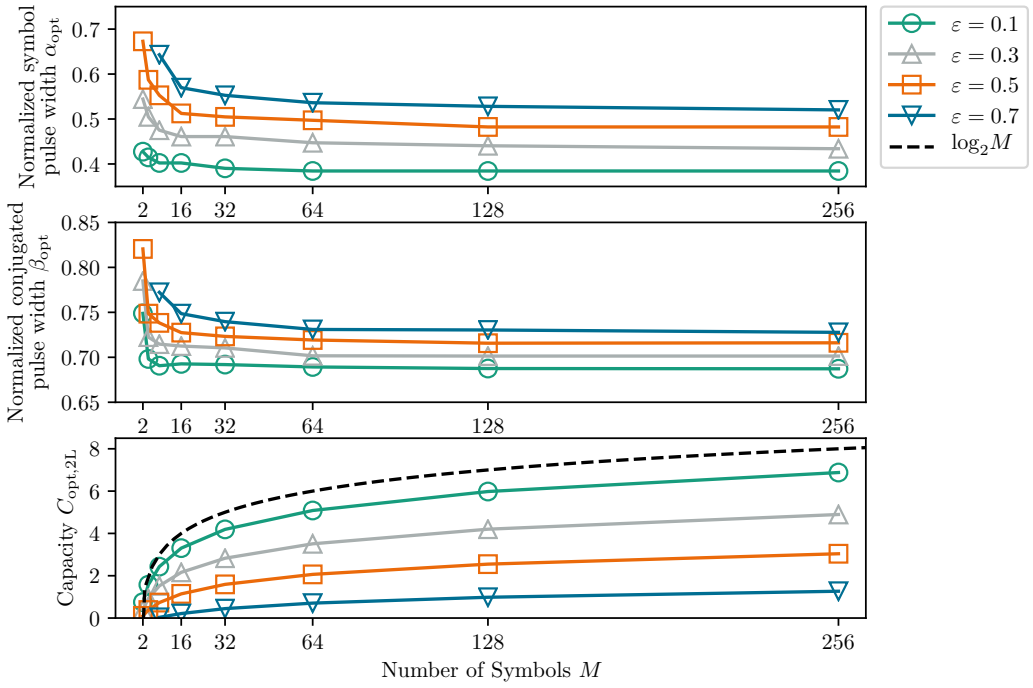


Figure 3.8.: Optimal normalized symbol pulse width α_{opt} (top), optimal normalized conjugated pulse width β_{opt} (middle) and the secret capacity $C_{\mathrm{opt,2L}}$ (bottom) for these optimal values over the number of symbols M per basis. $\log_2 M$ is also plotted in the bottom plot, as it represents the number of bits per photon for an ideal, error free transmission.

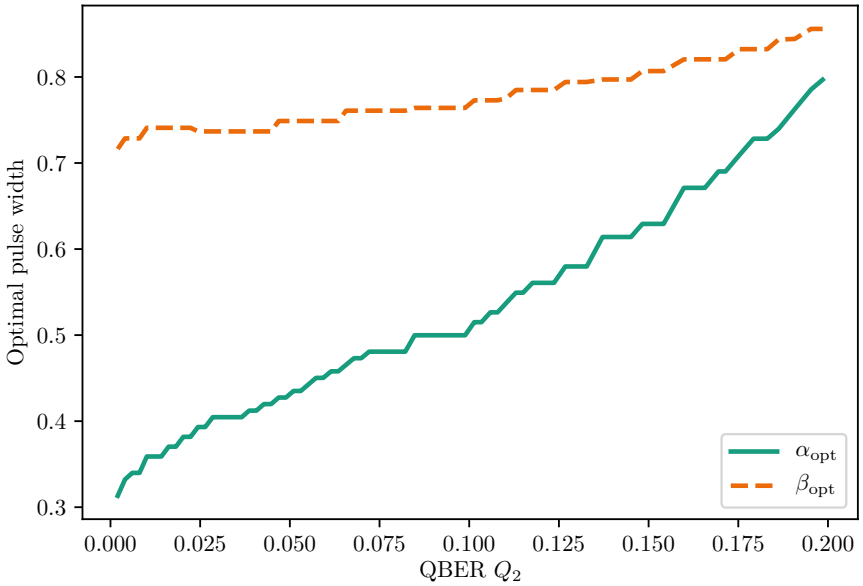


Figure 3.9.: Optimal pulse parameters for $M = 2$ symbols per basis. The optimal normalized symbol pulse width α_{opt} and the optimal normalized conjugated pulse width β_{opt} are plotted over the quantum bit error rate (QBER) Q_2.

to have a small error. With higher ε it becomes increasingly important, that Eves information on the sifted key decreases.

Since the experimental realization presented in this work is for $M = 2$ symbols per basis, the optimal pulse values depending on the QBER Q_2 is shown in greater detail in Figure 3.9. Note, that the step-like features of the graph are numerical artifacts caused by granularity.

3.4. Secret key rate calculation for implemented systems

In the previous parts of this chapter, the normalized pulse width of symbol and conjugated pulses were examined, optimal pulse widths where found and the secret capacity was calculated for the optimal values. The pulse widths are generally not exactly at their optimum in an implementation. In this section, it is shown how to calculate the secret capacity $C_{2\text{L}}$ and secret key rate S depending on measured values of the normalized symbol pulse width α, the normalized conjugated pulse

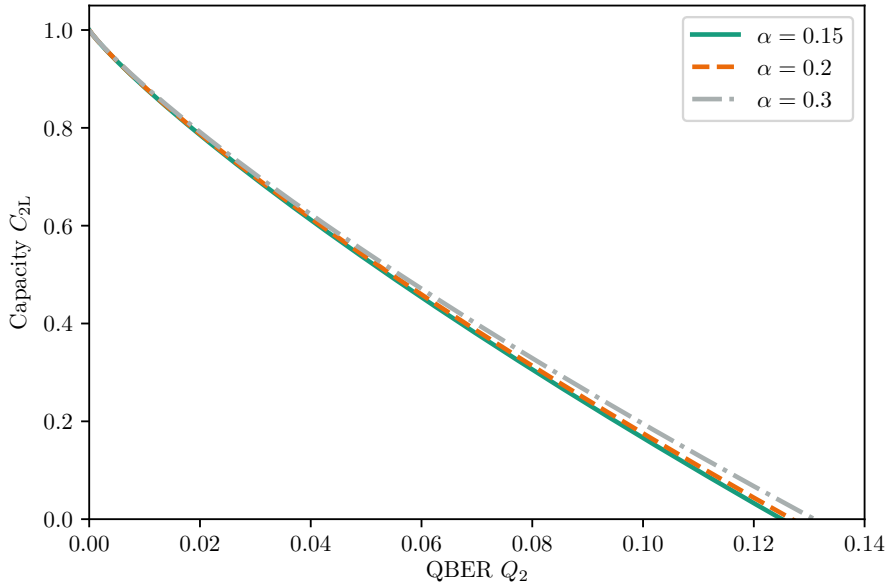


Figure 3.10.: Secret capacity C_{2L} over quantum bit error rate (QBER) for $M = 2$ symbols per basis for the pulse parameters set later in the present work, see Table 5.2.

width β, the sifted key rate R and the QSER Q_M (QBER Q_2).

For given α and β the correlation between the secret capacity C_{2L} and the QSER Q_M can be deduced with (3.45) and (3.31). However, C_{2L} can for $M = 2$ entirely be described by α, since β does not change the secret capacity for the considered IR-attack, as stated before. In Figure 3.10 the secret capacity C_{2L} is plotted over the QBER for the experimentally implemented values of α (The implemented pulse parameters are described later in Section 5.2.1 and Section 6.2.1 for the experimental back-to-back and free-space TF-QKD transmissions, respectively).

It can be observed, that the experimentally implemented parameters for α do not change the secret capacity C_{2L} by much. However, α and β will have a large effect on the measured QBER, as will be shown later in Section 5.2. The secret key rate can then be calculated by means of (2.23).

Note that in the derivation of the secret key rate it is assumed, that Alice sends all symbols with the same probability. In the experimental realization where the different symbols take different paths in Bob's system, this is not always given by default. Thus the settings need to be adjusted in order to ensure this is the case for each transmission, as will be discussed in Section 4.1.2.

Note further, that the different channels will still not be exactly equal, e.g. in

terms of the QBER originating from the two bases. This can not be prevented completely, especially, since the measurement in the time and in the frequency domain is conceptually very different. To regard additional asymmetries, such as this one, is beyond the scope of the present work.

3.5. Conclusion on numerical analysis

In this chapter, the TF-QKD protocol was analyzed numerically. Contrary to BB84, in TF-QKD, it is possible for an eavesdropper to access at least some of the information encoded in both bases. By examining an IR eavesdropping attack which exploits this loophole, the advantage an eavesdropper could get by this was shown. As a counter measure the optimal normalized pulse widths α and β of the used modulations were calculated by numerical optimization. This was done for symbol numbers per basis of up to $M = 256$. It could be shown, that narrow pulses, although leading to smaller overlaps between the symbols, are not the preferable choice, since they open up attack points an eavesdropper can exploit.

The maximum secret capacity $C_{2\mathrm{L}}$ in bits per photon was calculated for the optimal pulse widths depending on the fraction of eavesdropped photons ε. Additionally, the optimal pulse width depending on the QBER was shown for the case of two symbols per basis.

Since for an implementation of the setup it is not guaranteed, that the optimal pulse width can be implemented, the tools for calculating the secret capacity for arbitrary pulse widths were given, which will be needed in Chapter 5 and Chapter 6.

4. Implementation of the QKD Setup

The focus of this chapter is the experimental realization of TF-QKD setup. Parts of the setup were subject of previous publications [128–130]. Another publication about the setup is in preparation [131]. It was a targeted objective of the present work to implement a QKD system which is mostly implemented from standard telecommunication components and at the same time highly compatible with existing telecommunication infrastructure. Further, the QKD protocol was meant to be used not only over fiber but also over free-space optical links. To make use of existing off-the-shelf telecommunication components, the whole setup is SMF based. A wavelength around 1550 nm was chosen for the optical signal, since it does not only have a tremendously low loss in SMF but also in the atmosphere. Moreover, a lot of telecommunication components are optimized or only operational in the C-band.

Due to the components at hand, the repetition rate of the system is set to be $R_{\text{rep}} = 30\,\text{MHz}$, the pulse width and distance in the PPM basis is on the order of 100 ps to 1 ns and the FSK symbols in the order of 1 to 10 GHz, due to the existing components and to satisfy the pulse-width relations (3.6) and (3.7) being in the order of one.

The present setup is implemented with an attenuated laser as a photon source since real single-photon emitters are as of yet far away from being off-the-shelf components. Moreover, the decoy state protocol efficiently closes the loophole induced by occasional multi-photon pulses, embodied by the PNS attack (see Section 2.1.3).

The decoy state protocol (see Section 2.1.3) would be simple to implement in the present setup, without the need to change components. Since the symbol and conjugated pulses have a different intensity for the same number of photons anyway it would be trivial to implement multiple decoy states. For the decoy state protocol, the intensity of the pulses is usually set to a mean photon number of up to $\mu = 0.5$ [89]. This mean photon number is also set for the present setup. However, implementing the decoy state protocol was not a priority for the present work.

In Chapter 3 the influence of using different numbers of symbols M per basis

is one of the main subjects. However, the implementation as described in the following is only using $M = 2$ symbols per basis. First experiments with $M = 4$ symbols per basis and the occurring difficulties are described in Appendix A.2. To evaluate the presented implementation a simple and fixed pattern of symbols, e.g. $[F_0, T_0, F_1, T_1]$, is sent repeatedly. T_0 and T_1 represent the PPM-symbols and F_0 and F_1 the FSK-symbols.

This chapter starts with Section 4.1 introducing the general scheme of the DV-TF-QKD setup, after which the setup of Alice and Bob is unveiled in greater detail. Afterwards, the signals controlling the setup and their synchronization is described in Section 4.2. The chapter finishes with a conclusion in Section 4.3.

4.1. TF-QKD setup

A simplified scheme of the setup can be seen in Figure 4.1. Alice setup can be divided into two groups. The devices on the right-hand-site handle the optical signal: The tunable laser sends out a continuous wave (CW)-signal with the desired wavelength, the Mach-Zehnder modulator (MZM) creates the pulse forms and position in the time domain and the attenuator attenuates the signal to a desired mean photon number.

The devices on the left-hand-side, in turn, control the devices on the right-hand-site. The 30 MSa-AWG controls the tunable laser and thus the position of the pulses in the frequency domain, the 34 GSa-AWG controls the MZM and thus the shape and position of the pulses in the time domain and the clock synchronizes all other devices.

In Bob's setup, the receiving photons are forwarded by a 3 dB-coupler acting as the random basis choice either to the PPM basis or to the FSK basis. The PPM-basis is embodied by a DOMZM-filter forwarding the photons to two APDs. The FSK basis is embodied by a WDM-filter forwarding the photons to another set of two APDs. The clicks on the APDs thus indicate which basis was chosen and which symbol was measured.

4.1.1. Alice's setup

Alice setup can be seen in more detail in Figure 4.2. The tunable laser is a digital supermode distributed Bragg reflector (DBR) laser [132] (*Bookham TL 3000 DJC*), which is tunable over the whole C-band and has a linewidth of 1 to 5 MHz. Digital supermode lasers are especially well suited for fast wavelength tuning [133], which is crucial for the present application. The Laser is controlled on the one hand by a laser controller (five *PRO 8052 LD/TE Controller* embedded in a *Profile PRO*

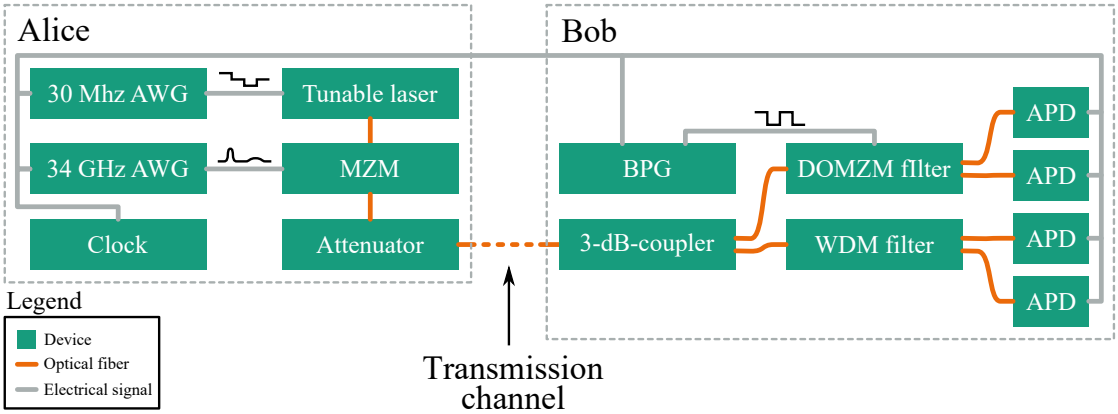


Figure 4.1.: Simplified depiction of the setup showing only the most important components. Alice part of the setup consists of two arbitrary waveform generators (AWGs) controlling the tunable laser's output wavelength and the AWG shaping the pulses in the time domain. An attenuator attenuates the signal to single-photon level. Bobs part of the setup consists of a 3 dB-coupler functioning as a passive basis choice, and subsequently a dual-output Mach-Zehnder modulator (DOMZM) controlled by a bit-pattern generator (BPG) and a wavelength division multiplexing (WDM) functioning as time and frequency filters. Depending on the filtered symbol, four avalanche photodiodes (APDs) measure the four symbols.

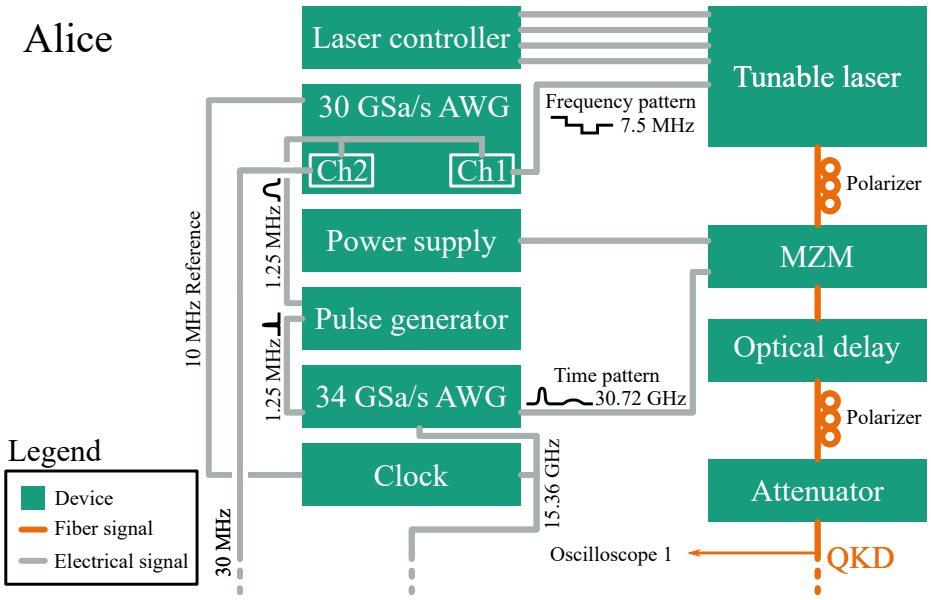


Figure 4.2.: Depiction of Alice's part of the setup. See text for a detailed description.

8000 Mainframe), which gives multiple constant currents to most sections of the laser.

On the other hand, the phase control section of the laser is controlled by a 30 MSa-AWG (*Rigol DG1032Z Arbitrary Waveform generator*). The 30 MSa-AWG tunes the signal wavelength according to the signal pattern, e.g. $[F_0, T_0, F_1, T_1]$. A pattern with three levels (two for F_0 and F_1 and one for both T symbols) and with a 7.5 MHz repetition rate (the frequency at which the four symbols repeat) is set. The signal is depicted in Figure 4.3 (a). Note, that Figure 4.3 only shows a principle illustration of the signals, without showing the correct scale. The 30 MSa-AWG gets a 10 MHz reference signal from a Clock (*HP 8341B Synthesized Sweeper*) in order to be synchronized to the rest of the setup.

The CW laser light is forwarded to a MZM (*Oclaro PowerBit SD-40 Intensity Modulator*) which has a extinction ratio bigger 20 dB and a bandwidth of 20 GHz, corresponding to 40 Gbit/s on-off keying for classical communication. The MZM is controlled by a 34 GSa-AWG (*HHI 34 GSa/s Arbitrary Waveform Generator* developed at HHI). It has 6 bit resolution, a 18 GHz bandwidth and a memory of 16 Mbit. The 34 GSa-AWG receives an 15.36 GHz clock signal by the external clock, which is doubled internally resulting in a 30.72 GHz symbol rate. A sample thus is $R_{\text{Sampl}} = 32.5$ ps long.

The 34 GSa-AWG shapes the pulses according to the time patter, embodied e.g. by $[F_0, T_0, F_1, T_1]$, which can be seen in Figure 4.3 b). Further, a constant voltage

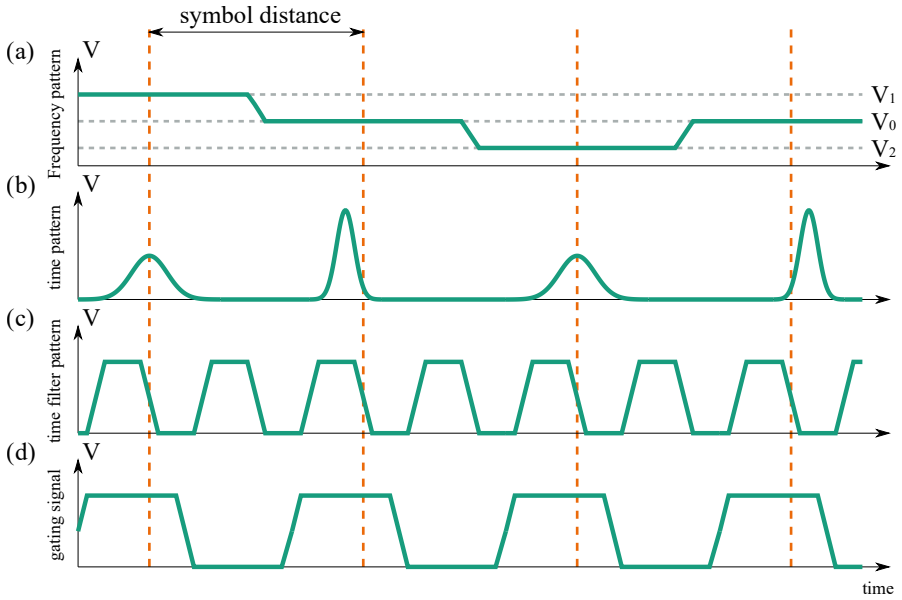


Figure 4.3.: Depiction of the four used patters steering the transmission for $[F_0, T_0, F_1, T_1]$. (a) shows the frequency pattern used for tuning the laser. (b) shows the time pattern used for shaping the pulses in the time domain. (c) shows the time filter symbol, which is used to control the dual-output Mach-Zehnder modulator (DOMZM)-filter. (d) shows the gating pattern for the avalanche photodiodes (APDs).

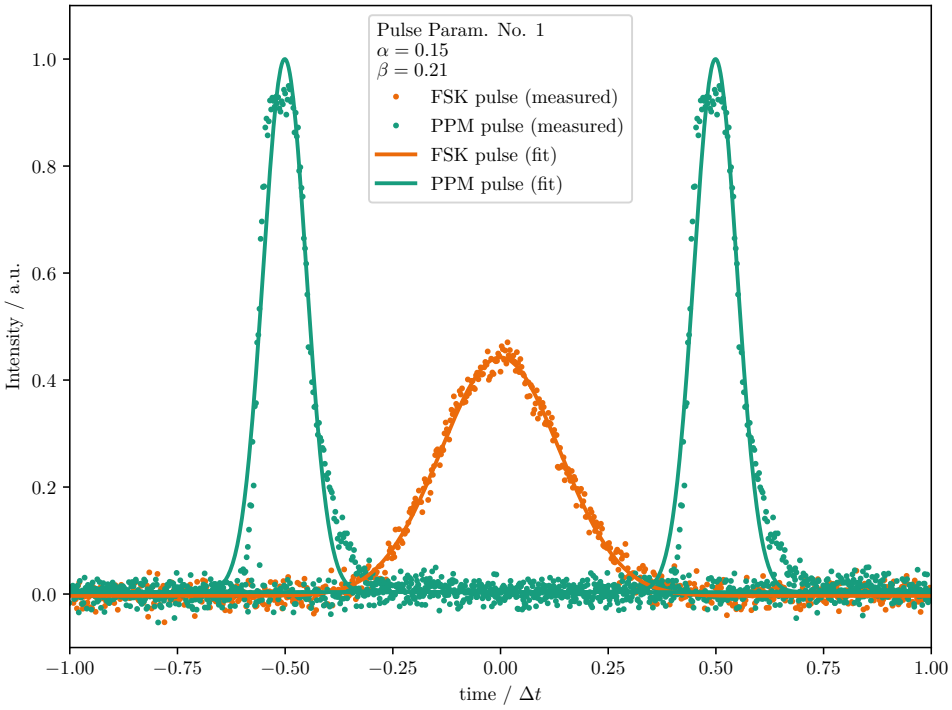


Figure 4.4.: Pulse shapes for the symbol and conjugated pulses in the time domain. As an example, pulse parameters No. 1 from Table 5.2 were used: $\Delta t = 40R_S$, $\sigma_\omega^{-1} = 10R_S$, $\sigma_t = 2R_S$ (were R_S is the sample length of the 34 GSa-AWG) and $\Delta\omega = 50.3$ GHz was set, resulting in pulse parameters $\alpha = 0.15$ and $\beta = 0.21$.

around 5 V is applied to the MZM to steer its operating-point. One example of the pulse shapes formed by the MZM can be seen in Figure 4.4.

In order to synchronize both AWGs in terms of the sequence of symbols, the 30 MSa-AWG is triggered by the 34 GSa-AWG. The trigger signal has a repetition frequency of 1.25 MHz corresponding to 24 successive symbols. The trigger signal of the 34 GSa-AWG is very narrow and can not be used directly as a trigger for the 30 MSa-AWG, which is why a *HP 8112A 50 MHz Programmable Pulse Generator*, measures the trigger and resends a wider signal with the same frequency.

After the MZM the signal is forwarded to a *JDS Fitel HD4 Optical Delay* which can delay the optical signal in a range of 350 ps with an accuracy of 0.002 ps. It is needed for precisely synchronizing Alice's and Bob's setups. Finally the signal

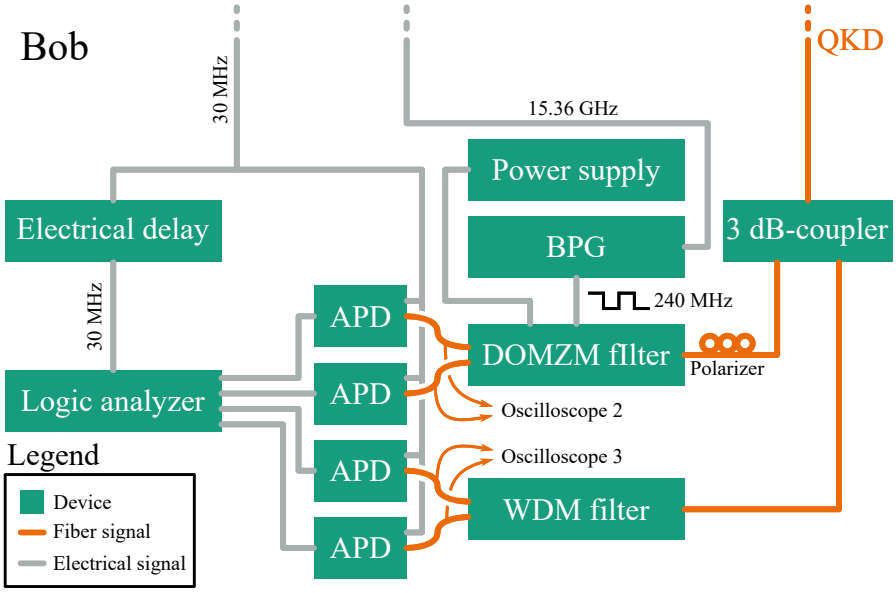


Figure 4.5.: Depiction of Bob's part of the setup. See text for a detailed description.

is attenuated by a *HP 8156A Attenuator* capable of up to 60 dB attenuation with a typical accuracy of 0.05 dB and only 0.02 dB of polarization dependent loss. Finally, the signal is sent over to Bob's system.

Polarization controllers are integrated where needed, namely before the polarization sensitive MZM and before the attenuator in order to change the polarization for the transmission between Alice and Bob. The clock providing the synchronization signals for both AWGs is also used to synchronize Bob's setup with Alice's, as will be described in the following section.

4.1.2. Bob's Setup

Bob's setup is shown in Figure 4.5. The QKD signal enters Bob's signal and is split up by a 3 dB-coupler which is acting as the random basis switch. Half of the signal is forwarded to a DOMZM filter representing the PPM basis filter and the other half to a WDM filter representing the FSK basis.

The DOMZM filter (*EOSPACE 1x2 Dual Output Modulator*), acts as a high bandwidth time filter. It has an insertion loss of 3.5 dB, an extinction ratio of 18 dB and a bandwidth of 20 GHz. It is controlled by a *SHF BPG 40A BPG* which has 20 GHz of bandwidth.

The DOMZM receives a constant voltage between 0 and 9 V for steering its operating-point. The constant voltage has to be re-adjusted from time to time

because the operating point drifts over time. This can happen on the order of hours and decreases the extinction ratio, namely the ratio between the active and the inactive output.

The BPG receives the 15.36 GHz clock signal from Alice's setup to synchronize the DOMZM filter with the MZM from Alice's setup. The BPG can be programmed with a bit sequence of 256 bit, whereof the first 128 were programmed to be 0 and the last 128 to be 1 forming a rectangular function with a frequency of 240 MHz. The pattern can be seen in Figure 4.3 c).

The WDM filter is a *Optoplex IL-CABFAS001 Interleaver*, based on the step-filter interferometer design [134]. It is commonly used for (de-)interleaving of signals, which are 12.5 GHz apart in the frequency domain. However, since it has a rather rectangular shape, signals, which are closer together can also be split or combined. Since this device is entirely passive, the position of the filter in the frequency domain cannot be changed, thus the signal frequencies have to be aligned to the filter instead. The insertion loss is 2 dB and the channel isolation 21 dB.

The outputs of the DOMZM and WDM filters are forwarded each to a pair of APDs (*IDQ ID210 NIR 100 MHz Gated Detector*), which measure the incoming photons. The APDs are InGaAs APDs, which operate in Geiger mode. They can be gated with a frequency up to 100 MHz which is necessary for InGaAs APDs to decrease the otherwise high dark count rate. The APDs receive a 30 MHz-Gating signal from the second channel of the 30 MHz-AWG in order to be synchronized with Alice's setup. The signal is depicted in Figure 4.3 d). The APDs have a tunable quantum efficiency of up to 25 %, where a tradeoff between efficiency and a low dark count rate need to be considered. For this work, an efficiency of 22.5 % was used.

Adjusting the gate width of the APDs is one way of optimizing a QKD transmission, as will be shown in Section 5.2.3. The gate width of the APDs can be controlled over a graphical interface. However, the displayed gate width differs from the real effective gate width. This can be seen on the one hand by comparing the dark counts of the APDs and on the other hand, when the same constant signal is given to different APDs. The real gate width can be estimated by measuring the shortest set gate width at which a signal can be measured, which corresponds to 200 ps of real gate width and can serve as an offset [personal communication with Bruno Sanguinetti (IDQuantique), 2015].

As stated in Section 3.4 all symbols need to occur with the same probabilities. Deviations can be compensated by slightly altering the gate width until all symbols occur equally likely. The set gate width G_W is assumed to be the average of all four gate width.

If an APD produces a click, a 5 ns long TTL signal is generated. The signals of

the four APDs are measured by an *ASIX Omega Logic Analyzer* which registers bit 1 for every click of the APDs. The logic analyzer can measure up to 16 TTL inputs, triggered by trigger signals of up to 99.95 MHz. It has 512 Mb of internal memory, which can efficiently be used by using RLE and Huffman coding [135] for compression, which is especially beneficial, when the data consists of mostly bit 0as in QKD transmissions. The logic analyzer could measure transmissions for intervals between 20 s and multiple hours depending on the number of recorded clicks.

The logic analyzer also receives the 30 MHz-gating signal, which is delayed by an electrical delay, namely a triggered pulse generator, to compensate differences in travel time of the trigger signal and the TTL signals of the APDs.

4.2. Phase adjustment of control signals

In the previous section Alice's and Bob's setup were introduced. There, four signals where introduced, which steer the sending and measuring process and where depicted in Figure 4.3. Summing up, the four control signals are:

- The **frequency pattern**, which controls the separation and position of the pulses in the frequency domain,
- the **time pattern**, which on the one hand controls the position in the time domain of the pulses and on the other hand determines the pulse width and intensity in the time- and the frequency domain,
- the **time-filter pattern**, which controls the time filter
- and the **gating signal**, which synchronize the gating of the APDs and the logic analyzer with the optical signal.

The four signals need to have the right relative phase. The frequency pattern is created at the 30 MSa-AWG and imprinted onto the frequency of the CV signal. At the MZM it is superposed with the time pattern. Here the frequency pattern $[F_0, T, F_1, T]$ and the time pattern $[F, T_0, F, T_1]$ need to be synchronous to form the PPM- and FSK-symbols correctly. Both, the time pattern and the frequency pattern can be shifted freely, with the precision of the respective APD. The frequency pattern is a step function which steps are constant for roughly 10 ns. Thus the precision of the phase between time and frequency pattern also needs to be that precise.

The optical signal is then attenuated and sent over to Bob, where it is split and redirected to the PPM- and FSK basis measurement. In the PPM measurement

basis, the time pattern needs to be synchronized with the time-filter pattern. For technical reasons, the time and frequency patterns are shifted with respect to the time-filter pattern rather than the other way around. The time pattern can only be shifted sample-wise by R_{Sampl}, thus an optical delay was integrated to increase the precision.

The optical signals need to be synchronous with the gating pattern for all four APDs. The APDs are capable of shifting the gate over 20 ns, which corresponds to roughly 6 m of optical fiber. Thus, as long as the fiber lengths behind the 3 dB-coupler do not differ by that much, synchronization is possible.

However, each click of the APDs is forwarded as a TTL signal to the logic analyzer, where each of the four TTL signals, as well as the gating pattern given to the logic analizer, need to be synchronized. The fiber and cable lengths between the 3 dB-coupler and the logic analyzer need to be such that all four TTL signals gets registered by the logic analyzer with 5 ns precision according to the TTL signal's duration.

This is achieved by choosing exactly the length of the cables between each of the APDs and the logic analyzer. To measure the potential offsets, a oscilloscope (*LeCroy Wave Pro 960*) with a bandwidth of 2 GHz and four electrical inputs measured the four TTL signals and the cable length was changed accordingly. Once the four APD signals where synchronous, the electrical delay could be used to correct for any phase difference between the TTL signal and the logic analyzer trigger.

4.3. Conclusion on the TF-QKD setup implementation

One of the declared goals of the presented work was to implement a QKD setup with SMF based off-the-shelf components. As described in this chapter, this was accomplished.

With the components at hand, the repetition rate was set to 30 MHz. Repetition rates far higher than that were already reported [21, 26, 136, 137]. The limiting device in the presented setup was the tunable laser, which could be tuned with a frequency up to about 30 MHz. The APDs gating frequency could not exceed 100 MHz, which would limit the repetition rate to 100 MHz. For an improved TF-QKD setup, the tunable laser could be replaced by multiple lasers with the desired wavelengths. The APDs could be replaced by superconducting nanowire single-photon detectors (SNSPDs) [138,139], which do not need to be gated. With SNSPDs it would further be possible to measure the time of arrival directly one detector. Hereby, one SNSPD can substitute the time filter and the successive

APDs. However, cryogenic cooling becomes necessary, which increases complexity.

Nevertheless, for a proof-of-principle experiment and for exploring the TF-QKD protocol, the implemented repetition rate was sufficient and the setup was suitable for the experiments carried out in this work.

5. Experimental TF-QKD in a back-to-back configuration

Arguably, the secret key rate S is the essential merit for validating a QKD transmission. For a given QKD setup, the secret key rate, in turn, is depending on the sifted key rate and the QBER. However, the sifted key rate and the QBER are depending on the conditions the QKD transmission experiences such as loss and how the QKD setup was adjusted, in the case of TF-QKD in terms of pulse forms and APD gate width G_W. In this chapter, the implemented TF-QKD setting is evaluated in terms of the sifted key rate, QBER and resulting secret key rate. Thereby the influence of loss, pulse width and gate width on this merits are emphasized and discussed. A publication about the presented results is in preparation [131].

The chapter is structured as described in the following: In Section 5.1 The procedure for performing a QKD transmission with the setup described in Chapter 4 is described. In Section 5.2 the experimental back-to-back QKD transmission is presented. Finally the back-to-back experiments are concluded in Section 5.3

5.1. Procedure for TF-QKD transmissions

This section will cover the necessary steps to perform a QKD transmission. Firstly the preparatory procedure before the transmission is introduced. Secondly, the subsequent steps for deducing the sifted key rate and QBER are presented.

5.1.1. Preparatory procedure

In the following, various parameters are measured by means of an oscilloscope. A *HP 83485B Optical/Electrical Plug-In Module* in a *Agilent Infinium DCA-J 86100C* mainframe was used, which provides a bandwidth of 20 GHz optically as well as electrically. The attenuation is set to 0 dB and if necessary amplified by an *IPG EAD-100-C* erbium doped fiber amplifier (EDFA) which can provide up to 27 dBm of output power.

First, the pulse parameters which will be used in the following QKD transmission will be set and calibrated with the oscilloscope connected at position "Oscilloscope 1" in Figure 4.2. With the pulse width parameters α and β, as defined in 3.6 and

Type	Set		Measured
	σ / R_{Sampl}	σ / ps	σ / ps
Symbol pulse (σ_t)	2	65	97, 6
Conjugated pulse (σ_ω^{-1})	10	325.5	269.6
Conjugated pulse (σ_ω^{-1})	20	651.0	510.2
Conjugated pulse (σ_ω^{-1})	30	976.6	695.8

Table 5.1.: The measured pulse widths σ_x are shown depending on the set pulse width displayed in units of the 30 MSa-arbitrary waveform generator (AWG)'s sample length R_S.

3.7, σ_t, Δt and σ_ω^{-1} define the pulses unambiguously. These three parameters can all be set by changing the time pattern accordingly. The parameters are all given in multiples of the sample rate R_{Sampl}.

Since the bandwidth of MZM and 34 GSa-AWG is limited, the real pulse widths σ_t and σ_ω^{-1} will differ from the set pulse intensity (see Figure 5.1, top and middle). For a given pulse width the set intensity (and thus mean photon number per pulse) was varied to find coinciding intensities for the symbol and conjugated pulses. the attenuation will later be set such, that $\mu_{\text{meas}} = 0.5$. To utilize the total resolution of the 34 GSa-AWG, the highest symbol pulse and a conjugated pulse with equal intensities were chosen. At this stage, it would in principle be possible to in the future choose multiple intensities to implement the decoy state protocol. The measured pulse width deviates from the set pulse width (see Figure 5.1 bottom), which needs to be taken into account in the next step.

From the measured pulse widths and pulse separation in the time domain, α and β are calculated. The pulse width in the frequency domain is determined by the pulse widths in the time domain. From this, the needed pulse separation in the frequency domain $\Delta\omega$ can be calculated with (3.6) and (3.7). The frequency pattern is set accordingly.

As mentioned in Section 4.2 the phase of the different patterns needs to be adjusted relative to each other. In order to adjust the phase between the time- and the frequency pattern, first the initial phase needs to be measured. This is done by sending $[F, 0, 0, 0]$ (where 0 stands for sending no pulse) as the time pattern and $[F_0, F_1, F_1, F_1]$ as the frequency pattern. The outputs of the WDM-filter are connected to the oscilloscope (at position "Oscilloscope 3" in Figure 4.2). When changing the phase between time pattern and frequency pattern, the pulse is visible in the output corresponding to F_0 25 % of the time and in the output of F_1 75 % of the time. The phase is correct when the pulse is visible in the output of F_0.

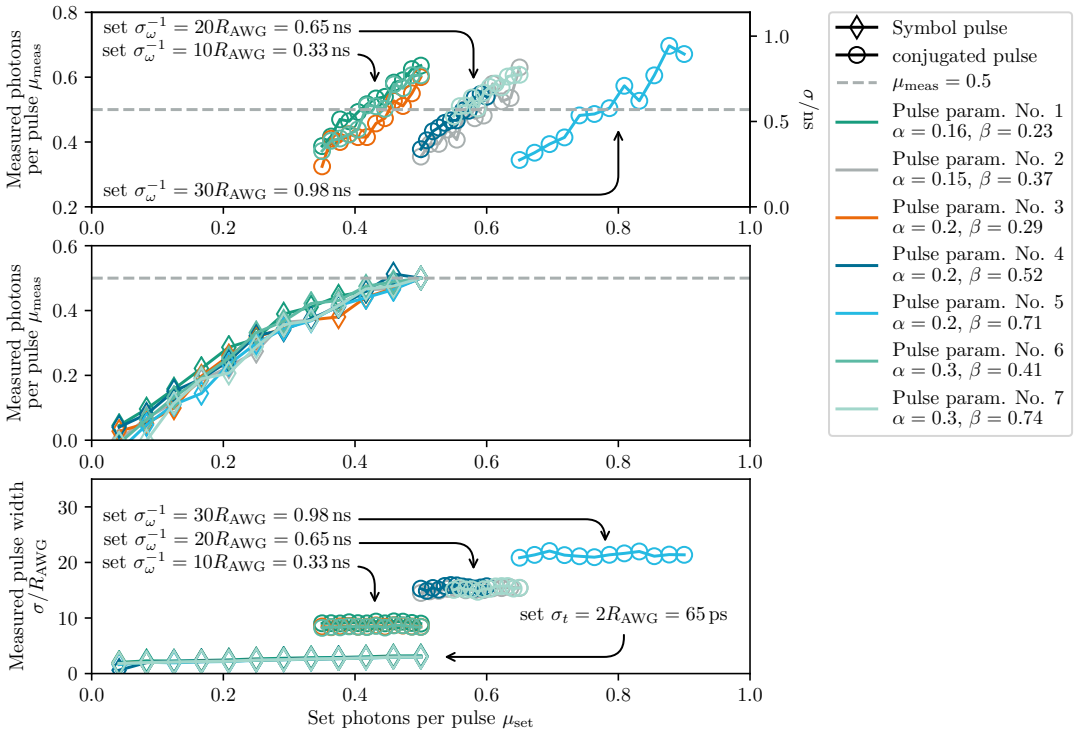


Figure 5.1.: Set and measured pulse widths in the time domain and pulse intensity in terms of photon number per pulse, depending on the set pulse width, for the pulse parameters later introduced in Table 6.2. R_{AWG} is the sample length of the 34 GSa arbitrary waveform generator (AWG). The measured pulse width and photon number differ from the set pulse width and photon number, due to the limited bandwidth of the 34 GSa-AWG and the Mach-Zehnder modulator (MZM). For a given pulse width the set photon number was varied to find coinciding photon numbers for the symbol and conjugated pulses. the attenuation will later be set such, that $\mu_{\text{meas}} = 0.5$. To utilize the total resolution of the 34 GSa-AWG, the highest symbol pulse and a conjugated pulse with equal intensity were chosen. The measured pulse width deviates from the set pulse width, which needs to be taken into account to calculate the pulse parameters and choose the correct pulse distance $\Delta\omega$ in the frequency domain.

To adjust the phase between the time and time filter pattern, the position of both need to be measured at position "Oscilloscope 2" in Figure 4.5. Both, the MZM and the DOMZM can be set to let pass the signal by switching off the 34 GSa-AWG or BPG respectively and tuning the applied constant voltage. If the MZM (respectively DOMZM) is set to let pass, the time filter signal (respectively time signal) can be measured with the oscilloscope.

As mentioned before, the working point of the DOMZM is drifting thus it has to be set as well at this point. If an EDFA was used before, it has to be removed from the setup since it adds additional noise to the system. The attenuator needs to be set according to the intensity measurement described above.

Now The gate position of the APDs need to be adjusted by sending the only one symbol at a time (e.g. $[T_0, T_0, T_0, T_0]$) and maximize the counts on the respective APD (e.g. the one for measuring T_0). Lastly, the electrical delay is adjusted such, that APD-clicks get registered from the logic analyzer.

5.1.2. TF-QKD transmission evaluation

After performing this preparatory steps, a QKD transmission is performed by setting the sending pattern to e.g. $[F_0, T_0, F_1, T_1]$ and starting a measurement with the logic analyzer.

In the following, the procedure of evaluating the transmission from the raw data measured by the logic analyzer is described. For each time-bin the logic analyzer saves a "1" for each APD which clicked and a "0" for each APD, that did not. This results in a quadruplet of bits. Together with a respective quadruplet of bits representing the sent symbols, the different kind of events can be categorized.

An illustrative example including all categories of events can be seen in Figure 5.2. All Events which contain more (1) or less (2) photons than one are rejected. Furthermore, photons measured in the wrong basis get rejected as well, representing the sifting. The remaining events sum up to the valid events V_{Valid}. The sifted key becomes

$$S = \frac{V_{\text{Valid}}}{t_{\text{meas. duration}}}, \tag{5.1}$$

where $t_{\text{meas. duration}}$ is the duration of the measurement. The valid events consist of correct symbols (4) and errors q (5), where the QBER can be calculated by

$$Q_2 = \frac{q}{V_{\text{Valid}}}. \tag{5.2}$$

The bit-wise phase between the measured and sent pattern is not known before the evaluation since the logic analyzer starts recording at a random position. Therefore the evaluation is first done with a subset of successive symbols for all

Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32		
Sent																																		
F_0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0		
T_0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0		
F_1	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0		
T_1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1		
Measured																																		
F_0	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0		
T_0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	1	1	0	0	0	1	0	1	0	0	0	0	0	0	1		
F_1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0		
T_1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0		
Valid Counts																																	Sum	
F_0	1								1				1																1				4	
T_0		1				1															1												3	13
F_1																											1						1	
T_1							1					1				1												1				1	5	
Errors																																		
F_0																													1				1	
T_0		1																			1												2	6
F_1																															1		1	
T_1												1																				1	2	
Mutli photons																		1				1											2	
Wrong basis				1			1				1								1	1					1					1			7	

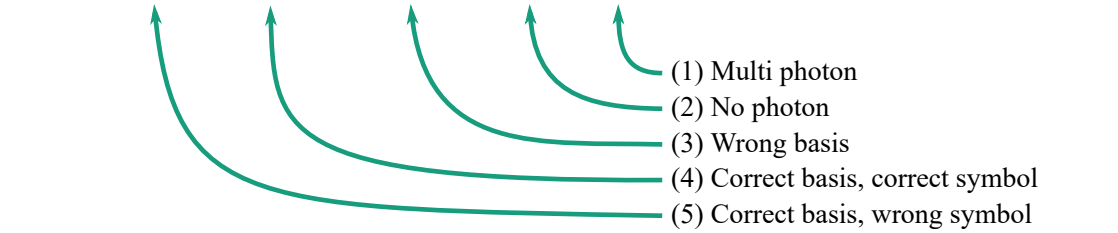


Figure 5.2.: Illustrative example of 32 sent symbols which contain all kinds of events, which can be categorized in five groups: (1) Multi photons, where multiple APDs have clicked; (2) no photon provokes a click; (3) a click is registered in the wrong basis; (4) The correct symbol was measured in the correct basis; (5) The wrong symbol was measured in the correct basis.

four possible phases. From the calculated secret key rate and QBER, the correct phase can be ascertained.

Additionally, the QBER and secret key rate are registered separately for each symbol, as can be seen in Figure 5.2. This is necessary for technical reasons, namely to measure the drift of the DOMZM and to measure if the probability for all symbols is equal.

5.2. Experimental back-to-back transmission of TF-QKD

In this section, the TF-QKD setup implemented in the present work is analyzed and optimized experimentally. The setup is analyzed for the back-to-back case, namely where Alice's output fiber and Bob's input fiber are connected directly.

To set up a QKD transmission, the steps described in Section 5.1.1 are executed. To evaluate the transmission, the measured raw data is interpreted in order to get the sifted key rate and QBER, as described in Section 5.1.2. From this, the secret key rate can be calculated, following Section 3.4.

The secret key rate is strongly dependent on the transmission distance which increases the loss a transmission experiences. In the following experiment, the variable optical attenuator integrated into Alice's setup is utilized to simulate additional losses. To extend the attenuation range of the variable optical attenuator, fixed optical attenuators were inserted to increase the loss by 30 dB. The setting parameters, which are varied are firstly the pulse parameters, as shown in Table 5.2. Secondly the APD gate width G_W is varied in order to find the loss dependent optimal value for each set of pulse parameters.

In Section 5.2.1 the used values for α and β and the resulting pulse width and distances in the time and frequency domain are presented. In Section 5.2 the TF-QKD protocol is evaluated for a back-to-back scenario. Here the focus will lie on the one hand on the transmission losses and on the other hand on the optimization of the setup by adjusting the APD gate width G_W and setting different pulse parameters α and β.

5.2.1. Pulse parameters for the back-to-back experiment

One of the key questions of the presented work is the influence, the pulse forms, namely the width of the symbol- and conjugated pulses have on the raw key rate and QBER and thus on the achievable secret key rate. After the theoretical work in Chapter 3, the experiment was carried out with different parameters for α and β. Since in the presented implementation of the TF-QKD system Bob's filters are not

No.	Set [R_S]		Pulse parameters		Time domain [ps]			Freq. domain [GHz]		
	Δt	σ_ω^{-1}	α	β	σ_t	σ_ω^{-1}	Δt	σ_ω	σ_t^{-1}	$\Delta\omega$
1	40	10	0.15	0.21	97	268	1302	3.7	10.3	50.3
2	40	20	0.15	0.37	95	483	1302	2.1	10.6	28.4
3	30	10	0.20	0.29	97	278	977	3.6	10.3	36.3
4	30	20	0.20	0.50	96	486	977	2.1	10.4	20.8
5	30	30	0.20	0.71	99	693	977	1.4	10.1	14.3
6	20	10	0.30	0.43	97	278	651	3.6	10.3	24.2
7	20	20	0.30	0.77	98	499	651	2.0	10.2	13.4

Table 5.2.: Pulse parameters for back-to-back transmission, used in Section 5.2. For all parameters $\sigma_t = 2R_S$, Δt and σ_ω^{-1} where set. Afterwards the real values of σ_t and σ_ω^{-1} where measured and α and β was calculated accordingly. From this the pulse widths σ_ω and σ_t^{-1} in the frequency domain could be deduced and the pulse separation $\Delta\omega$ could be calculated and set. For convenience the pulse parameters are numbered from No. 1 to No. 7.

exactly rectangular but have limited bandwidth, α and β will have a stronger effect on the QBER Q_2 and thus the secret key rate S as indicated by the theoretical assessment, carried out in Chapter 3.

During the curse of this work two measurement series where executed. In the first measurement series, which will be the topic of Section 5.2, the SMF leaving Alice's setup (see Figure 4.2) and entering Bob's setup Figure 4.5, were directly connected. With this setting QKD transmissions were performed with the parameters specified in Table 5.2. Two of the three set parameters were varied, namely the pulse distance Δt and width of the conjugated pulses σ_ω^{-1} in the time domain, all set in multiples of the rate R_S. The third value was the width of the symbol pulses in the time domain, which was set to $\sigma_t = 2R_S$ for all sets of parameters.

The pulses in the time domain where already shown in Figure 4.4 for pulse parameters No. 1 from Table 5.2. For the other sets of parameters, the pulses can be seen in Figure 5.3.

5.2.2. Loss dependent distance measurement

As an initiatory example a transmission is plotted in Figure 5.4 for pulse parameters No. 1 from Table 5.2. The sifted key rate K, QBER Q_2 and secret key rate S are plotted over the loss.

The values for the sifted key rate K and the QBER Q_2 are deduced as described in Section 5.1.2, marked with green circles and orange squares respectively. Each

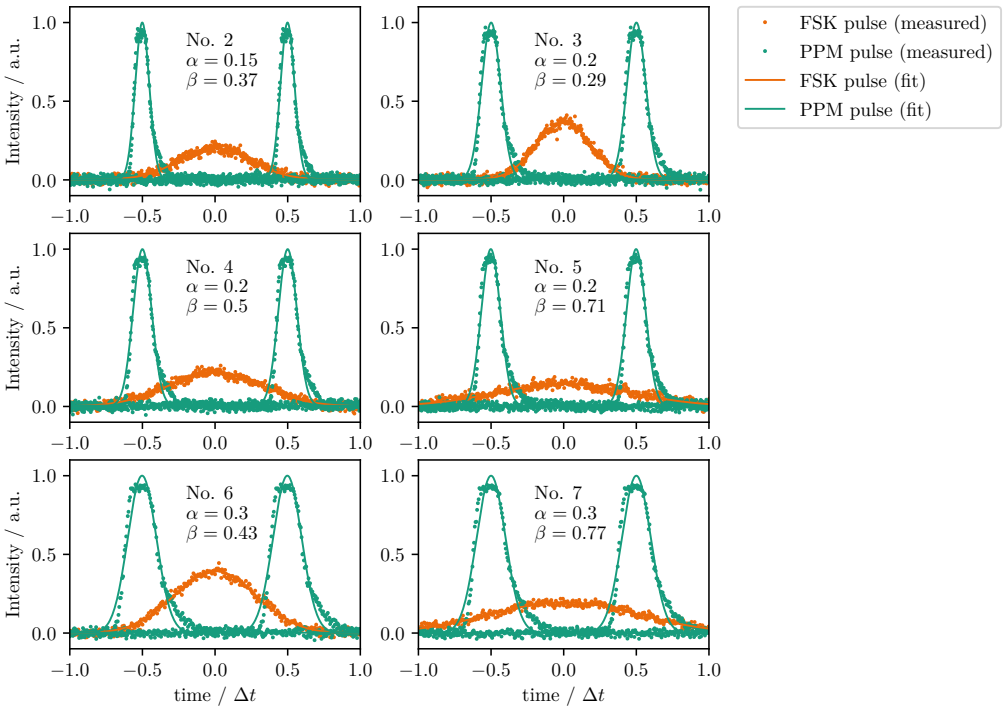


Figure 5.3.: Symbol and conjugated pulses in the time domain. For comparison, the pulses are all normalized to the pulse distance of the symbol pulse Δt. Both, the symbol as well as the conjugated pulses fit quite well to the ideal Gaussian pulses.

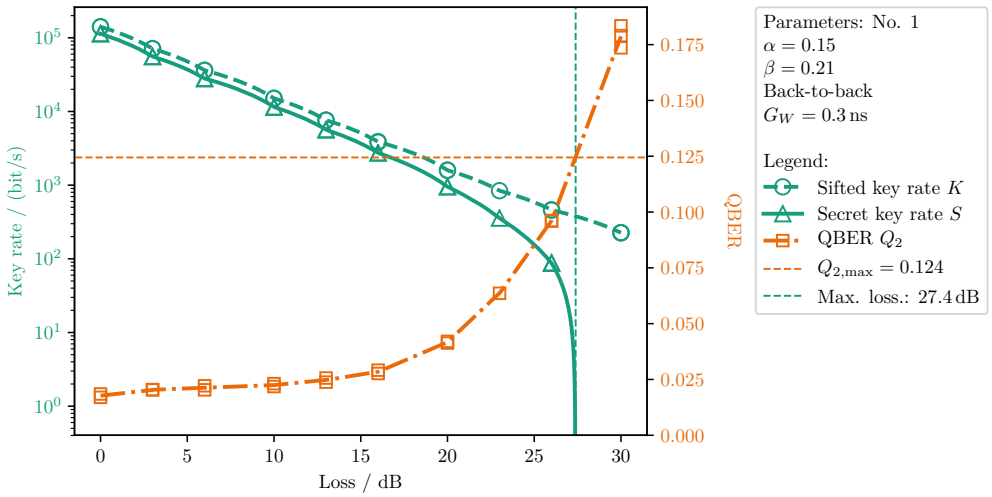


Figure 5.4.: Back-to-back Transmission for different transmission losses. Sifted key rate S, quantum bit error rate (QBER) Q_2 and secret key rate S plotted over loss for pulse parameters No. 1 (see Table 5.2) and a gate width of $G_W = 0.30ns$. For every value of loss, multiple measurements where performed. The measured values are shown as marks. For K and Q_2 the values between the measured values are extrapolated linearly (dashed and dash-dotted lines respectively). S is calculated for the measured values of K and Q_2 (marks) as well as for the linear fits (solid lines) The maximum QBER of $Q_M = 0.124$ above of which a QKD transmission is not possible is at 27.4 dB of loss. This happens to be the highest tolerable loss measured in the present work and corresponds to 137 km link distance over single-mode fiber (SMF).

transmission was carried out multiple times. For K and Q_2 the values in between the measured data points are interpolated linearly with respect to the mean of the measured points, plotted as a dashed and dash-dotted line respectively.

The secret key rate S is calculated with (2.23). The secret key rate calculated from the measured points for K and Q_2 are represented by green triangles. The secret key rate is also calculated for the interpolated values of K and Q_2, plotted as a solid green line.

It can be observed how the sifted key rate K is decreasing and the QBER is increasing. The QBER Q_2 is caused firstly by photons measured in the wrong bin due to overlapping symbols and imperfect filters and secondly from APD dark counts. The number of wrongly measured photons decrease the same way correctly measured photons do, thus changing the loss is not changing their share of the QBER. However, the dark counts are independent of the transmission losses, leading to an increasing QBER with loss. For the presented case QKD transmission is not possible anymore if the QBER surpasses 0.124, corresponding to a loss of 27.4 dB. Incidentally, this is also the highest maximum loss achieved in the present work and corresponds to a link distance of 137 km over SMF.

5.2.3. Gate width optimization

In Figure 5.5 the sifted key rate K (top) and QBER Q_2 (bottom) are plotted over the transmission loss for various gate width G_W for pulse parameters No. 1. It can be observed, that the sifted key rate, as well as the QBER, is increasing with increasing gate width. If the gate width is larger more photons coming from the signal pulses can be gathered, by measuring a larger slice of the pulses, which will increase the secret key rate. On the other hand, dark counts also have a higher chance of occurring, decreasing the secret key rate. Note, that the gate width should have a similar effect also in other QKD protocols when gated detectors are used.

The according secret key rate S is plotted over the loss in Figure 5.6. It can be seen, that there is a trade-off of high sifted key rate and low QBER, resulting in an optimal secret key rate S. It can be observed, that the optimal value for the gate width $G_{W,\mathrm{opt}}$ depends on the induced loss. Comparing e.g. the lowest gate width $G_W = 0.22\,\mathrm{ns}$ with the highest $G_W = 0.68\,\mathrm{ns}$ one can observe, that the higher gate width leads to a secret key rate roughly one order of magnitude higher compared to the lower gate width for 0 dB of loss. However, for the higher gate width, the secret key rate quickly falls until no key distribution is possible above 4.1 dB of loss. For the low gate width, a secret key can still be distributed up to 27 dB of loss.

This trend is also true for the other pulse parameters from Table 5.2, as can be

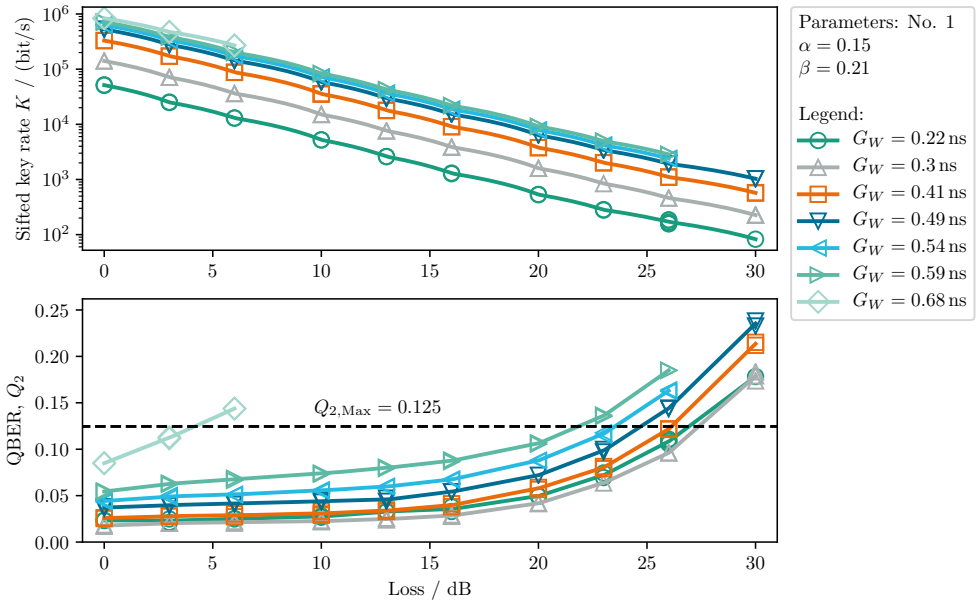


Figure 5.5.: Sifted key rate K and quantum bit error rate (QBER) Q_2 plotted for different gate widths G_W for the set parameters $\Delta t = 40R_S$ and $\sigma_\omega^{-1} = 10R_S$ corresponding to $\alpha = 0.15$ and $\beta = 0.21$ (pulse parameters No. 1 in Table 5.2). The marks are measured values while the solid lines are connecting the measured values in a linear manner. For every value of loss, multiple measurements where performed.

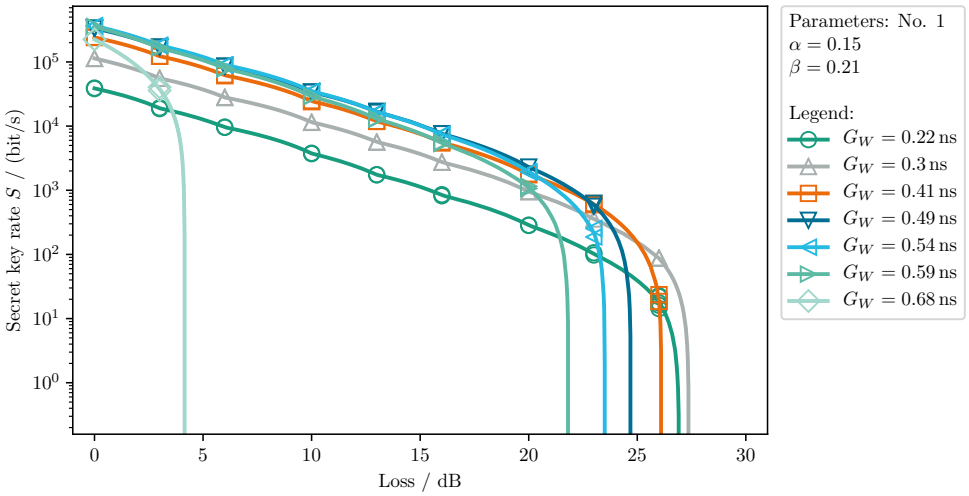


Figure 5.6.: Secret key rate over Loss for different gate widths for back-to-back configuration. Sifted key rate S corresponding to the sifted key rate K and quantum bit error rate (QBER) Q_2 plotted in Figure 5.5. S is calculated for the measured values of K and Q_2 (marks) as well as for the linear fits in between the marks (solid lines).

seen in Figure 5.7, where the maximum loss is plotted over the set gate width.

However, as mentioned above, the optimal gate width for lower loss transmissions is not the same as for high losses. To examine this further, the sifted key rate K, the QBER Q_2 and the secret key rate S are plotted over the gate width in Figure 5.8 for three different values of loss.

Contemplating the sifted key rate and QBER it can be seen, that the sifted key rate has a negative slope, while the QBER has a positive one. This can easily be understood by comparing the gate width with the pulse width: The number of photons gathered from the Gaussian pulses by widening the gate is increasing digressively. Meanwhile, the dark counts increase linearly. In total, the QBER thus increases more quickly with an increasing gate width.

Comparing the optimal gate width $G_{W,\mathrm{opt}}$ marked in the plots for different losses, it can be seen, that the optimal gate width is decreasing with higher loss. This is in agreement with the previous observation, that smaller gate widths are needed to maximize the transmission range. Incidentally, the optimal secret key rate $S = 364.6\,\mathrm{kbit/s}$ in the top of Figure 5.8 is the highest values for a back-to-back transmission without additional loss, achieved in the present work.

In Figure 5.9 the optimal gate width (top) together with the corresponding secret key rate S (bottom), depending on the occurring loss is plotted for all pulse

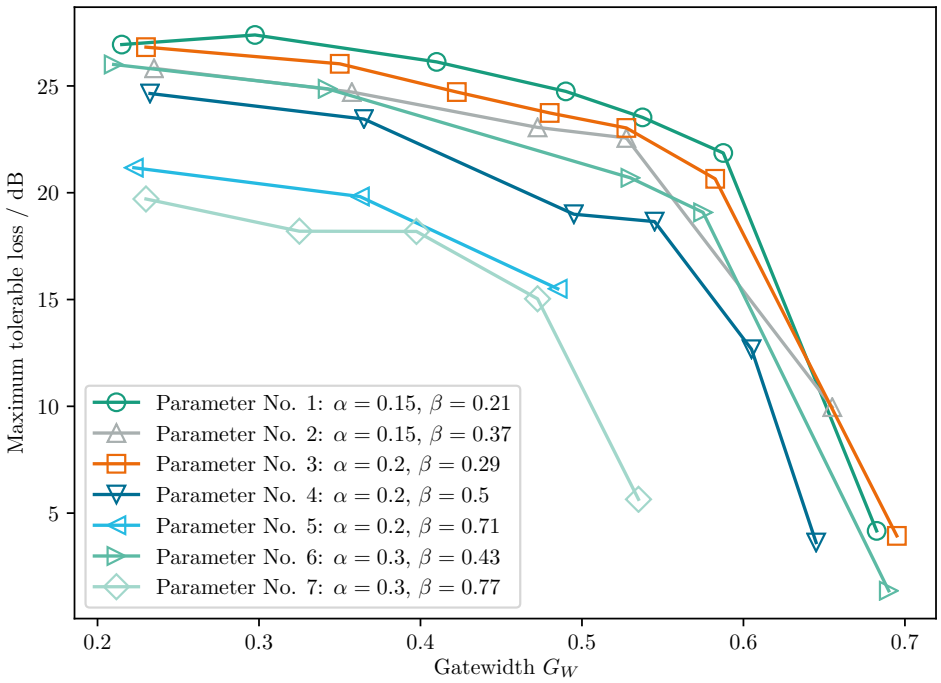


Figure 5.7.: Maximum tolerable loss plotted over gate widths for back-to-back configuration, above which a QKD transmission is not possible anymore, for the pulse parameters specified in Table 5.2.

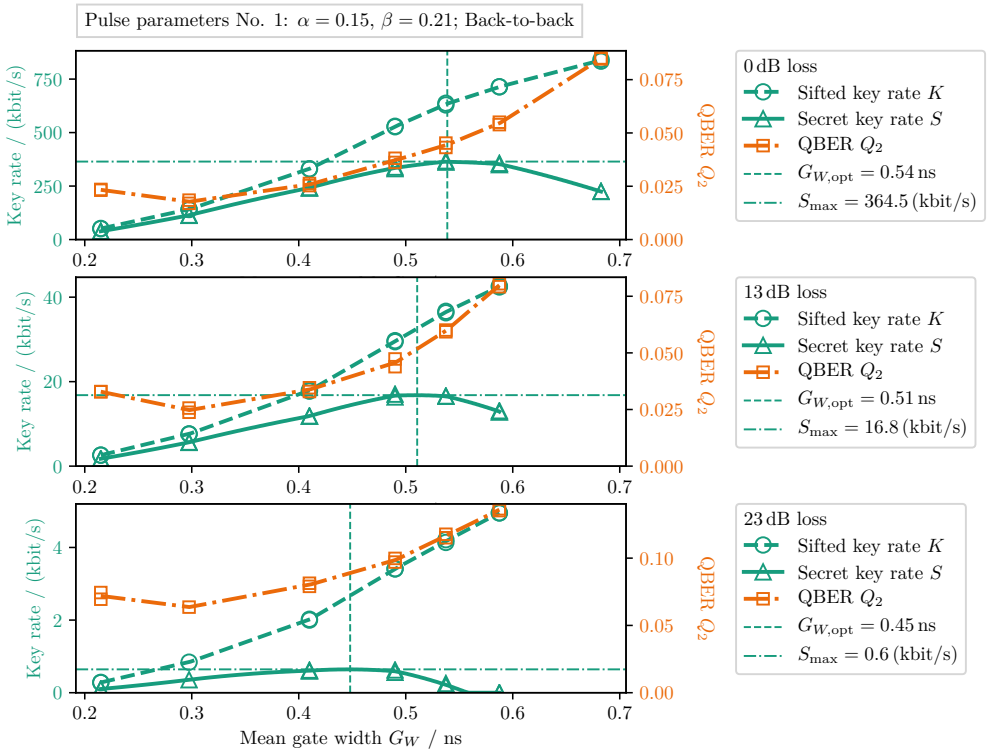


Figure 5.8.: Transmission depending on gate width for three different values of loss. The sifted key rate K, quantum bit error rate (QBER) Q_2 and secret key rate S plotted over the set gate width G_W for three values of loss. Pulse parameters No. 1 from Table 5.2) are set. For every value of gate width G_W, multiple measurements where performed. It can be observed, that the optimal gate width $G_{W,\mathrm{opt}}$, namely the gate width corresponding to the maximum secret key rate, is decreasing with increasing loss.

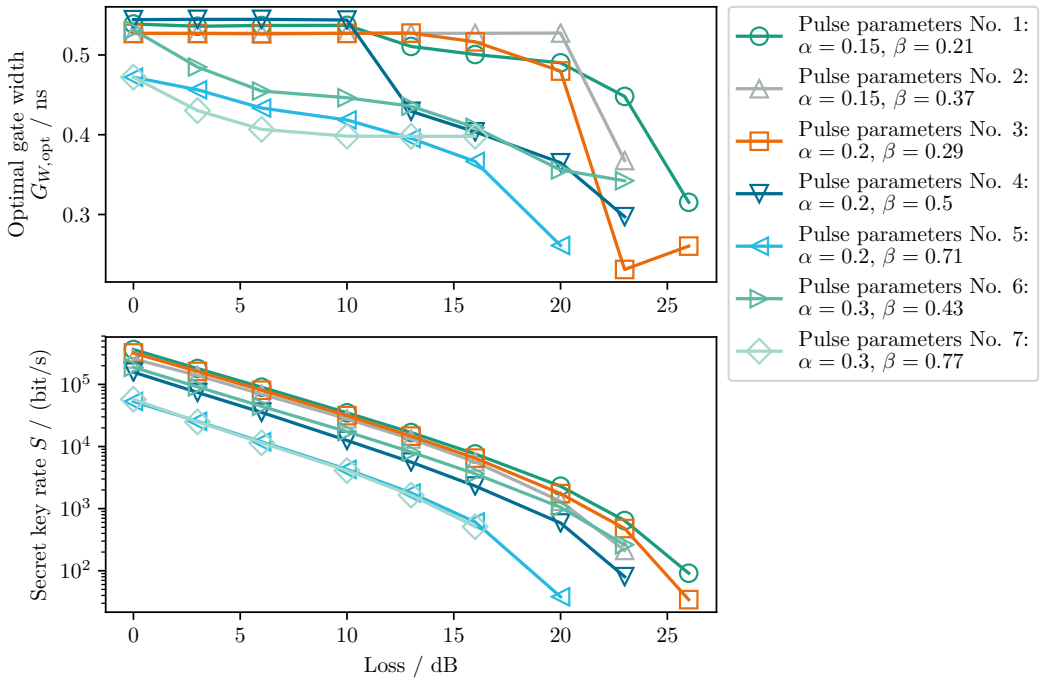


Figure 5.9.: Optimal gate width $G_{W,\mathrm{opt}}$ (top), namely the gate width corresponding to the maximum secret key rate S (bottom), for the pulse parameters specified in Table 5.2.

parameters from Table 5.2. It can be seen, that the secret key rate is highest for the pulse parameters No. 1 independently of the induced loss. Looking at Table 5.2 these pulse parameters account for pulse distances of $\Delta t = 1302\,\mathrm{ps}$ in the time domain and $\Delta\omega = 50.3\,\mathrm{GHz}$ in the frequency domain, which are both the highest values tested in the present work. Very close behind in secret key rate pulse parameters No. 3 are following, which account for the second widest pulse separation in the time and the frequency domain.

α_{opt} and β_{opt} are calculated numerically in Chapter 3 by assuming perfectly rectangular filters. Non-rectangular filters, as always present in real-world implementations like the present one, increase the QBER for Alice and Bob. For the considered IR attack, increasing Δt and $\Delta\omega$ decreases α and β moving them away from the theoretically deduced optimal value for the highest secret key rate. On the contrary, it also decreases the effect of the imperfect filters on the QBER, which increases the secret key rate.

5.3. Conclusion on TF-QKD in back-to-back configuration

In summary in this chapter, the optimal gate width depending on the normalized pulse parameters α and β as well as on the transmission loss could be deduced. From the set pulse parameters, the QKD performance was best for pulse parameters No. 1 corresponding to $\alpha = 0.15$ and $\beta = 0.21$, closely followed by pulse parameters No. 3 with $\alpha = 0.20$ and $\beta = 0.29$. The maximum transmission loss above of which QKD is not possible anymore could be shown to be 27.4 dB, equivalent to a link distance of 137 km over SMF, for pulse parameters No. 1. The highest back-to-back secret key rate, without additional induced loss, was also shown with these parameters to be 364.6 kbit/s.

Furthermore, the optimal gate width G_W was found depending on the pulse parameters and the transmission loss. Note, that optimizing the gate width is not only a possibility for the TF-QKD protocol but can always be done, when gated detectors with noise are present.

It could further be shown, that smaller normalized pulse parameters α and β are preferable for a real-world implementation than the optimal values predicted by the theoretical considerations, due to the imperfections of the implemented filters.

The presented TF-QKD setup is now characterized. It is possible to set up the TF-QKD setup with an optimal setting in terms of gate width, regardless of the transmission distance, as long as losses are below 27.4 dB.

6. Experimental Free-Space TF-QKD over a 388 Meter Link

The topic of this chapter is the implementation and experimental validation of the TF-QKD setup over a 388 m free-space link. The TF-QKD setup introduced in Chapter 4 and validated in Chapter 5 in a back-2-back scenario was adapted for free-space transmission. optical antennas capable of optical tracking, which were developed at HHI, were build and adapted for QKD. This evolved implementing suitable filtering between an optical beacon beam necessary for optical tracking and the QKD signal. The filtering also is needed to make daylight QKD transmission possible. A publication about the presented results is in preparation [131].

The structure of the chapter is as follows: The optical antennas are introduced, the beacon signal and filtering are discussed, and the free-space testbed is presented in Section 6.1. Afterwards, the experimental transmission over the 388 m link is presented and evaluated in Section 6.2. Here the performance of the tracking and TF-QKD system are discussed. Finally, the TF-QKD transmission over the free-space link is summarized and discussed in Section 6.3.

6.1. Implementing optical tracking for the TF-QKD setup

During the work described in the present work, a free-space link was implemented. This was done by means of two free-space optical antennas capable of precisely coupling a beam of light in and out of a SMF by means of optical tracking and tip/tilt correction. For the tracking to work, however, the QKD signal is to weak. Thus a beacon signal is superposed with the QKD signal. The QKD signal needs sufficient filtering in order to filter out the orders of magnitude strong beacon signal.

In the following, firstly, the antennas will be described in detail in Section 6.1.1. Secondly, the beacon signal and its filtering from the QKD signal will be addressed in Section 6.1.2. Thirdly, the characteristics of the free-space testbed will be described in Section 6.1.3. Thirdly superposing and filtering of a beacon signal with the QKD signal is described. One important subject of these three sections

Location	Component	Losses / dB
Alice's site	Fibers 10 to 9 floor	1.5†
	Add-drop-filter	5.7*
	Circulator	1.2*
	Antenna	0.4*
Transmission link	Windows	3.9†
	Geometric coupling efficiency	2.7
	Other free-space losses	10 to 16
Bob's site	Antenna	0.4
	Circulator	1.3
	Three add-drop-filters	2
	Fibers 9 to 10 floor	0.7†

Table 6.1.: Table of relevant losses occurring during transmission. The losses are divided into losses of Alice, of Bob and transmission losses. *All losses on Alice's site can be seen as part of Alice's QKD-setup and can thus be compensated for before sending. †Since neither the windows nor the fibers are an intrinsic part of the QKD setup, their effect was also compensated for in order to evaluate the QKD system sufficiently.

are the losses the QKD signal experiences. A summary of all relevant losses can be seen in Table 6.1.

6.1.1. Optical tracking antennas

As described above, the QKD setup is entirely SMF based. Thus optical antennas capable of efficiently coupling light in and out of SMF are crucial. Fortunately optical antennas with an active tracking system were developed at HHI [120]. These antennas are capable of initial signal acquisition and tracking. The optical antennas constructed during the course of the present work, are described in the following. A master thesis supervised within the frame of the presented work was done about the implementing the tracking antennas into the TF-QKD setup [140]

Two mainly identical antennas, one for Alice for sending the QKD signal and one for Bob for receiving it are used. A depiction of the antennas can be seen in Figure 6.1.

The antennas require bidirectional communication in order to work. The principle of the optical antennas is the following: A fraction of the received communication signal is measured by means of a quadrant detector (QD) in order to find the misalignment of the incoming beam. The knowledge of the misalignment is processed and corrected by means of a piezo controlled fine steering mirror. As

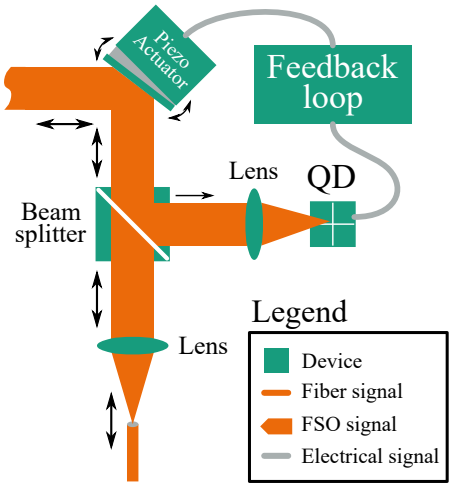


Figure 6.1.: Sketch of the tracking antennas. A fraction of the incoming signal is split off and used to measure the pointing mismatch with a quadrant detector (QD). A piezo controlled mirror corrects the mismatch accordingly.

stated in [141], single mode beams are reciprocal, even in a turbulent medium. Consequently, the measurement and subsequent correction of the incoming beam also corrects the sent beam.

The antenna emits a beam with a beam waist of $W_0 = 10.6\,\text{mm}$ and dissipates 8 % of the beam to measure the pointing error. The remaining 92 %, corresponding to 0.4 dB loss, is coupled into the SMF. Note, that the QKD system of Alice is defined to end after the optical antenna. Thus the loss of Alice's antenna can be compensated for by means of attenuating 0.4 dB less, compared to the back-to-back case. The antenna has a pointing error of below 10 µrad, which corresponds to a coupling efficiency of $\eta = -2.7\,\text{dB}$ only adding 0.3 dB of loss compared to the pointing-error free case ($\eta = -2.4\,\text{dB}$) for 388 m of distance.

6.1.2. Beacon signal and filtering

The QKD signal is superimposed with a beacon signal by means of WDM in order for optical tracking to be possible. A master thesis supervised within the frame of the presented work was done about the filtering setup [142].

In classical communication the sent beam is called Tx and the received beam Rx. This convention will be followed for the classical beacon beam. In Figure 6.2 the design for combining Alice's QKD signal with Rx and Tx is shown. Tx is superimposed with the QKD signal, by means of a 200 GHz-add-drop WDM filter (*oeMarket OAD-200-CH35-1-FA*) which induces 5.7 dB of loss for the QKD signal

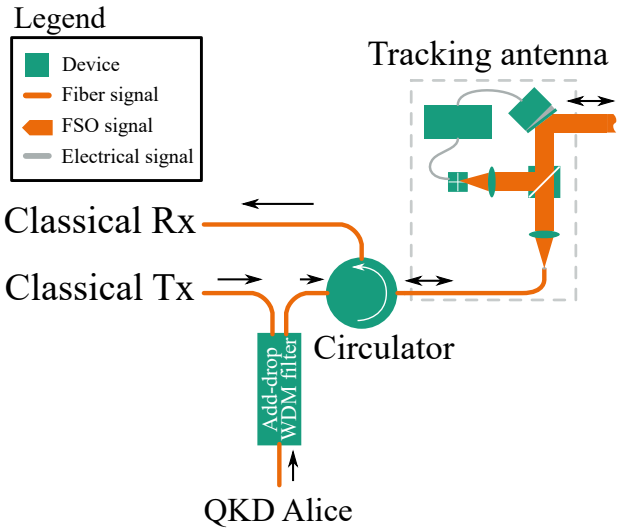


Figure 6.2.: Filtering system connected to Alice's QKD system. The weak QKD signal is combined with the classical Tx signal by means of a add-drop wavelength division multiplexing (WDM) filter. The Rx signal is separated direction-wise by means of a circulator.

in this direction. A circulator separates the signals directional-wise, namely the Rx from the combined QKD and Tx signal. Afterwards, the signal is coupled to the tracking antenna.

In Figure 6.3 the design for separating Tx and Rx from the QKD signal is shown. Tx is filtered out directional-wise by means of a circulator. Then Rx and the remaining Tx are filtered out with successive add-drop WDM filters. The circulator has a directivity of 50 dB. The sending power of both beacons is equal. Thus, Tx is the main source of noise at this point as long as the free-space loss for Tx is smaller than the circulators directivity.

In Appendix A.3.1 the needed filtering is estimated to be between 80 and 130 dB, depending on the transmission losses. Thus three add-drop WDM filters, each with a extinction ratio of around 50 dB and a insertion loss of between 0.5 to 0.9 dB from the common to the add-drop channel, where installed in the system.

The QKD signal is positioned around 1549.35 nm, corresponding to channel 35 of the dense wavelength division multiplexing (DWDM) frequency grid standardized by International Telecommunication Union (ITU) [143]. For the beacon beam, three WDM channels on the 200 GHz ITU frequency grid were analyzed, namely channel 31, 33 and 39. Channel 39 was tested to evaluate the influence of Raman scattering [144] which can have a effect on the QKD transmission [145, 146]. Channel 31 and 33 were chosen to analyze if the distance to the QKD channel has

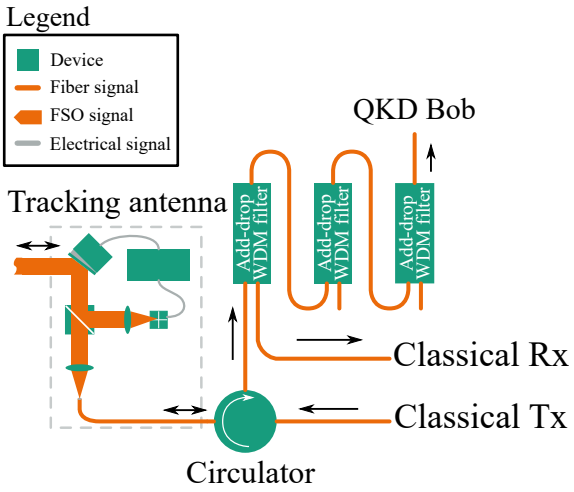


Figure 6.3.: Filtering system connected to Bob's QKD system. The weak QKD signal is separated from the classical Tx signal direction-wise by means of a circulator and with multiple add-drop wavelength division multiplexing (WDM) filters from the Rx signal. Hereby a filtering of 150 dB can be reached with an extinction ratio for the QKD signal of only 2 dB.

an influence on the noise.

In Figure 6.4 the noise is measured with the APDs (gate width set to $G_W = 0.30$ ns) over the free-space link. No QKD transmission was performed, thus the counts are purely caused by dark counts of the APDs, background photons, and photons coming from the beacon signal. The sent power is defined as the power leaving Alice's optical antenna. The received power defines the power just before 200 GHz-add-drop WDM filters. However, no influence of the beacon channel number could be observed. Channel 31 corresponding to 1552.52 nm was chosen for the beacon signal.

In addition to filtering out the beacon signal, the add-drop WDM filters also suppress background light as shown in Figure 6.5 (top). There, the total count rate without filters at day $R_{\mathrm{BG,Day}}$ and at night $R_{\mathrm{BG,Night}}$ and the count rate with two or three filters, respectively $R_{\mathrm{BG,Day,2F}}$ and $R_{\mathrm{BG,Day,3F}}$ are shown. To account for the sifting process all counts are divided by two. The count rates are plotted over the gate width G_W. In the bottom plot, the dark count rate is subtracted as an offset.

Without any filter, it can be observed, that the counts contributed by background light at Night $R_{\mathrm{BG,Night}}$ is negligible compared to the dark counts R_{DC}. It is hard to quantify the influence of the weather condition. However, multiple measurements were taken, when it was sunny and cloudy and for different solar

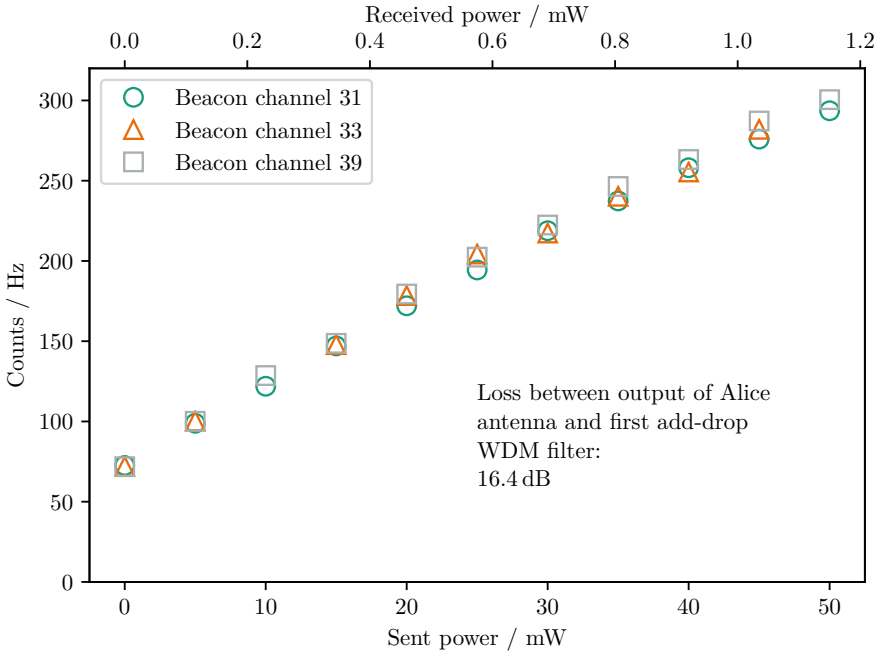


Figure 6.4.: Noise count influences by the beacon signal, depending on the position of the beacon signal in the International Telecommunication Union (ITU) frequency grid. Sent power: power leaving Alice's optical antenna. Received power: power before 200 GHz-add-drop wavelength division multiplexing (WDM) filters. The measurement was performed with the avalanche photodiodes (APDs), with a mean gate width of $G_W = 0.30\,\mathrm{ns}$.

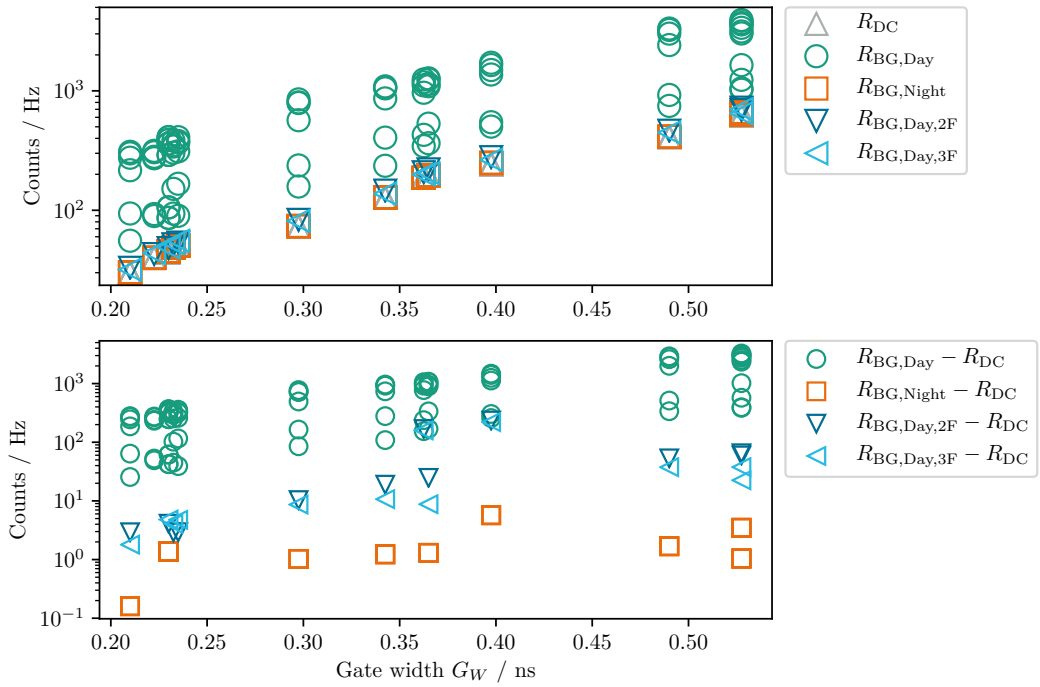


Figure 6.5.: Background photons measurement. Top: Dark count rate R_{DC}, background count rate without filters at daytime $R_{\mathrm{BC,Day}}$ and nighttime $R_{\mathrm{BC,Night}}$, and at daytime with two $R_{\mathrm{BC,Day,2F}}$ or three $R_{\mathrm{BC,Day,3F}}$ add-drop wavelength division multiplexing (WDM) filters, plotted over the gate width G_W. Bottom: Dark count rate R_{DC} subtracted as an offset from the remaining count rates.

altitudes to give an impression on what count rates can be expected. For the performed measurements the background counts in daylight $R_{\mathrm{BG,Day}}$ can be up to one order of magnitude higher than the dark count rate R_{DC}.

Integrating add-drop WDM filters reduces the number of background counts tremendously. The difference between two and three filters is negligible regarding background count rates. Usually, QKD experiments are carried out during night [39,45,46], because the background during the day is too high. With the presented setup, it is easily possible to perform QKD transmission regardless of the time of the day.

6.1.3. The free-space test-bed

In this section, the free-space testbed will be introduced and characterized. The testbed was also used for classical communication experiments, such as an experiment, where $2 \times 1.7\,\mathrm{Tbit/s}$ where transmitted eye-save, which was a world record at the time [120].

The free-space testbed is embodied by a link between two optical antennas described in the previous section located at HHI main building linked over a mirror on a HHI site branch 194 m apart from the antennas. The distance is hereby doubled to 388 m, as shown in Figure 6.6. Conveniently all crucial devices could stay in the same building.

The mirror is of circular shape with a diameter of 100 mm and its tip and tilt can be controlled remotely. The distance was measured by means of a time-of-flight measurement between Alice's to Bob's optical antenna. The QKD setup and the free-space optical antennas were in different labs connected with fibers. In the following the loss between the output of Alice's QKD setup, as depicted in Figure 4.2 and the input of Bob's setup as depicted in Figure 4.5 will be described.

The QKD system is located on the tenth floor of the HHI main building, whereas the antennas are located on the ninth floor. Fibers connecting both floors where used, which induced measured losses of 1.5 and 0.7 dB for both ways respectively. The antennas and the mirror are inside buildings, thus the link runs through windows repeatedly, which cause a loss of 3.9 dB, see Appendix A.3.2.

The present work should give a fair evaluation of how the QKD transmission generally performs. Thus parts not necessary for the QKD transmission are compensated for, by means of reducing the attenuation at Alice's setup respectively.

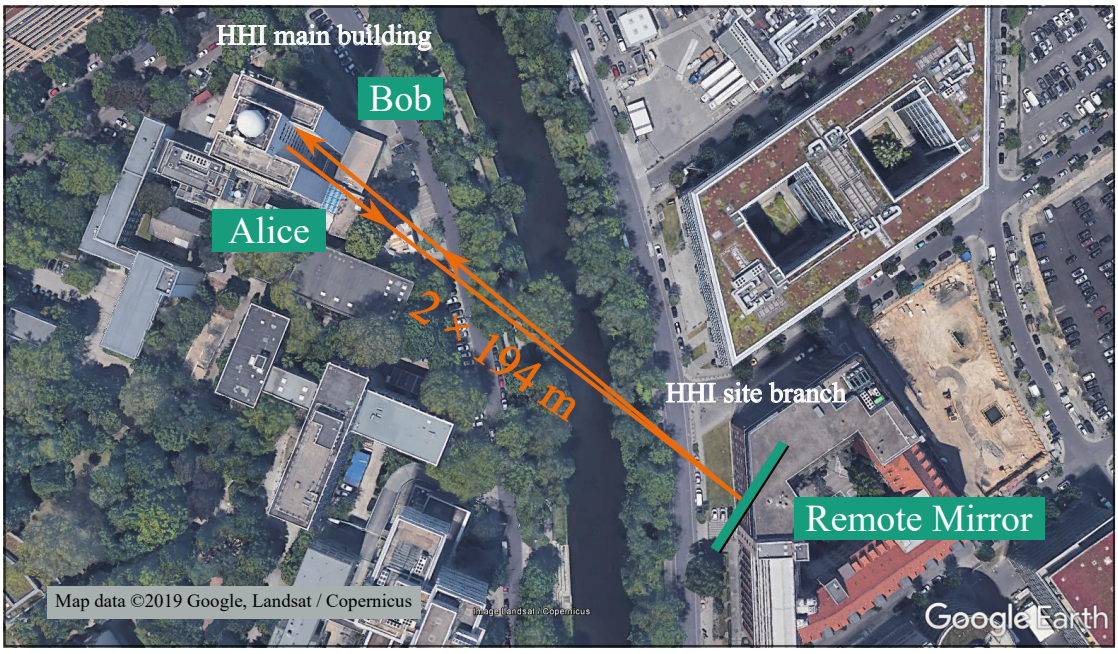


Figure 6.6.: Free-space testbed between Fraunhofer Heinrich Hertz Institute (HHI) main building to a site branch of HHI in the Berlin city center. The distance is doubled by a remotely controllable mirror. The distance is approximately 194 m one way, thus the total distance extended by the mirror is approximately 388 m.

6.2. Experimental TF-QKD over a 388 m free-space link

In this section the free-space transmission over the 388 m long testbed introduced in Section 6.1.3 is discussed. The link is implemented between two optical antennas capable of initial acquisition and tracking which were described in Section 6.1.1. Because the QKD signal consists of single photons it is too weak for the antennas to be used for tracking, the QKD signal is overlaid by a strong beacon signal, as was discussed in Section 6.1.2.

6.2.1. Pulse parameters for TF-QKD over free-space

In order to compare the results from the back-to-back and free-space transmissions, the same parameters were targeted for the free-space transmissions as for the back-to-back transmission. However, it was not possible to set the exact settings again, thus the parameters are slightly different, as can be seen in Table 6.2. Nevertheless, the parameters are similar enough for the two measurement series to be compared.

No.	Set [R_S]		Pulse parameters		Time domain [ps]			Freq. domain [GHz]		
	Δt	σ_ω^{-1}	α	β	σ_t	σ_ω^{-1}	Δt	σ_ω	σ_t^{-1}	$\Delta\omega$
1	40	10	0.16	0.23	104	295	1302	3.4	9.6	42.3
2	40	20	0.15	0.37	97	488	1302	2.0	10.3	27.5
3	30	10	0.20	0.29	97	281	977	3.6	10.3	35.7
4	30	20	0.20	0.52	99	510	977	2.0	10.1	19.3
5	30	30	0.20	0.71	96	696	977	1.4	10.5	14.7
6	20	10	0.30	0.41	98	270	651	3.7	10.2	24.7
7	20	20	0.30	0.74	96	479	651	2.1	10.4	14.1

Table 6.2.: Pulse parameters for free-space transmission, which is the topic of Section 5.2. The parameters slightly differ from the parameters shown in Table 5.2, since it was not possible to recall the exact settings used there. The numbering of the pulse parameters is consistent with the set parameters

6.2.2. TF-QKD with tracking

To evaluate how the TF-QKD protocol performs over free-space links, it is expedient to show the development over time. In Figure 6.7 a QKD transmission for the back-to-back case is shown as a reference for the free-space transmission plots

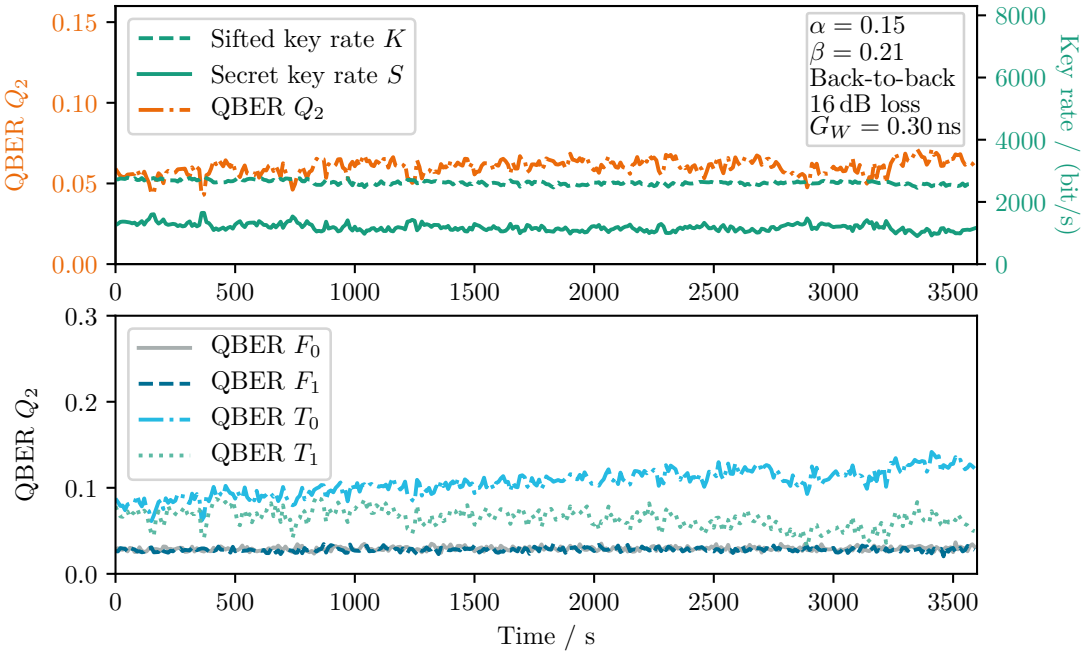


Figure 6.7.: Back-to-back QKD transmission over time. Pulse parameters No. 1 from Table 5.2 are set. Top: sifted key rate K, the quantum bit error rate (QBER) Q_2 and the secret key rate S for a back-to-back transmission with 16 dB loss and the gate width set to $G_W = 0.30$ ns. Bottom: QBER subdivided by symbols. A slight drift of the dual-output Mach-Zehnder modulator (DOMZM) can be observed.

shown later on. In the top of the figure the sifted key rate K, the QBER Q_2 and the secret key rate S is shown. in the bottom, the QBER is shown subdivided by symbols, as described in Section 5.1.2.

It can be observed, that the QBER corresponding to the symbols sent in the PPM basis is drifting over time. This is a typical example of the DOMZM-filter drift's influence on a QKD transmission. In Figure 6.8 a similar plot is shown for a free-space transmission. It can be seen that the QKD transmission stays stable with the exception of the DOMZM drift for at least 6000 s. The measurement was taken in the middle of the day at 13:59 on December 11$^{\text{th}}$ 2018, confirming, that daylight QKD is indeed possible with the implemented setup.

To compare how the QKD transmission performs with and without active optical tracking, measurements were performed, where tracking was initially switched on but switched off after some time. Four of those measurements can be seen in

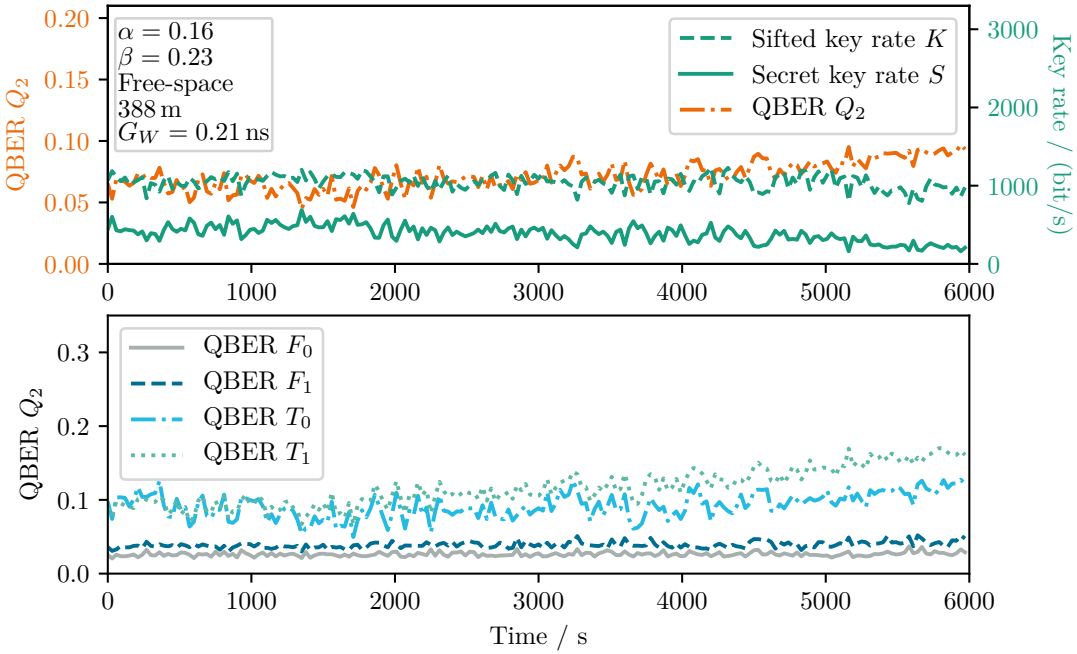


Figure 6.8.: QKD over 388 m free-space link. Pulse parameters No. 1 from Table 6.2 are set. The measurement was started at 13:59 on December 11$^{\text{th}}$ 2018 showing, that day light QKD is possible with the implemented setup. Top: sifted key rate K, quantum bit error rate (QBER) Q_2 and secret key rate S for a free-space transmission with the gate width set to $G_W = 0.30$ ns. Bottom: QBER sorted by which symbol was sent. The QKD transmission is mostly stable over the measured 6000 s with the exception of dual-output Mach-Zehnder modulator (DOMZM)-drift, which can be seen from the respective QBER in the bottom plot.

Figure 6.9 and Figure 6.10. In all cases the tracking algorithm was left on for 300 s and then was switched off for the remaining time period. For two of the measurements, the beacon signal was also switched off to evaluate its influence on the tracking. However, in compliance with the background measurements shown in Figure 6.4, there was no observable difference. The measurements where all performed during a week in December 2018 at different times during the day and evening. As was already shown in Section 6.1.2, especially with Figure 6.5, the time of the day had no influence on the QKD transmission.

In Figure 6.9 two measurements can be seen, where the coupling efficiency is getting worse relatively quickly after tracking is switched off due to misalignment. In the top plot, an instant decline in sifted key rate K and enhancement of QBER Q_2 can be seen, which in turn decrease the secret key rate S. However, after the initial decline, the transmission stays relatively stable. In the bottom plot, the misalignment is happening more slowly over a period of at least 700 s. 540 s after the tracking is switched off the QBER increased too much for a secret key to be created.

In Figure 6.10 both measurements stay relatively stable despite switching off tracking for a long time. The difference in how quick the misalignment takes place is influenced by a lot of factors, which are not under the control of the operator of the experiment. For example, sudden shocks caused by a vigorously closed door near the experiment can cause a rapid misalignment such as the one shown in Figure 6.9 (top). Slow misalignment as shown in Figure 6.9 (bottom), can happen, e.g. because the sun is no longer blocked by a cloud and slowly heats up the building causing it slowly shift. Sometimes nothing of impact happens for a period of time, such that the link stays intact, as shown in Figure 6.10. However, the tracking algorithm can easily compensate for all shown impacts on the coupling efficiency.

6.2.3. TF-QKD performance over free-space

Above it was shown, that the tracking enables stable QKD transmission over the free-space testbed. In the following the optimization as discussed for the back-to-back case in Section 5.2.3 is evaluated for the free-space transmission.

In Figure 6.11 the sifted key rate K, QBER Q_2 and secret key rate S are displayed for the two pairs of pulse parameters shown in Section 5.2.3 to lead to the best performance, namely pulse parameters No. 1 and No. 3 from Table 6.2.

Pulse parameters No. 3 lead to a secret key rate of $S = 8.9\,\mathrm{kbit/s}$ for the optimal gate width of $G_{W,\mathrm{opt}} = 0.52\,\mathrm{ns}$. The secret key rate for pulse parameters No. 1 is slightly lower with $S = 6.3\,\mathrm{kbit/s}$ for $G_{W,\mathrm{opt}} = 0.48\,\mathrm{ns}$. Both set of pulse parameters lead to the two best secret key rates for the free-space case,

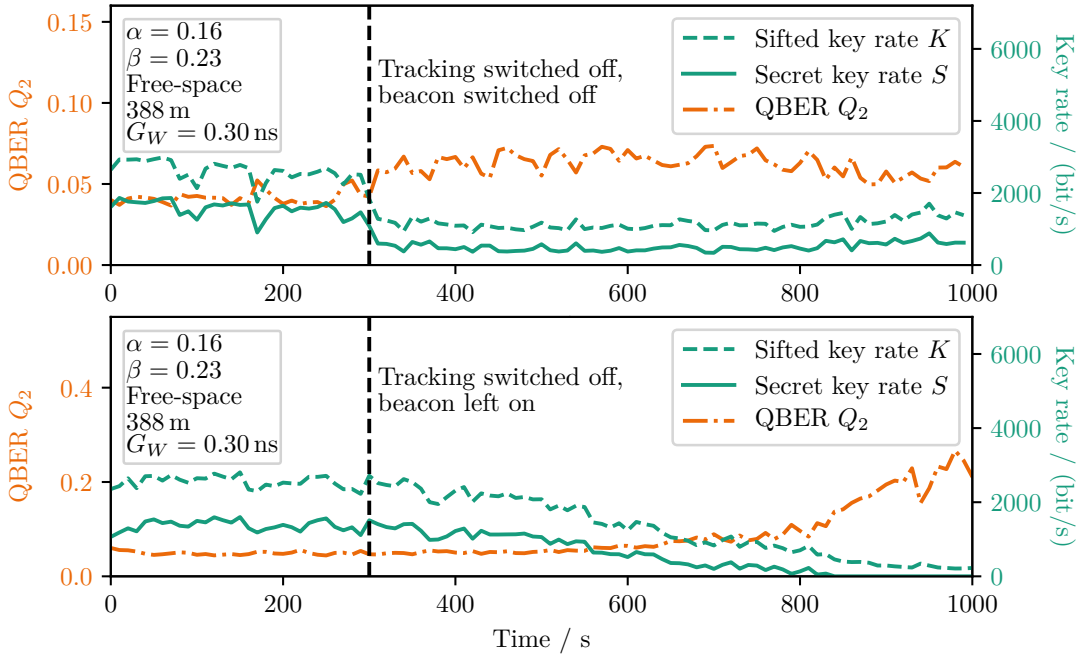


Figure 6.9.: QKD over 388 m free-space link with misalignment after switching off tracking. In both plots the link becomes worst after switching off tracking. Top: The measurement was started at 19:27 on December 11$^{\text{th}}$ 2018. The coupling efficiency becomes worse immediately, but is not lost entirely over the course of the measurement. Bottom: The measurement was started at 15:27 on December 12$^{\text{th}}$ 2018. The misalignment is slower compared to the top plot but the QKD transmission can not be maintained eventually. Pulse parameters No. 1 from Table 6.2 are set.

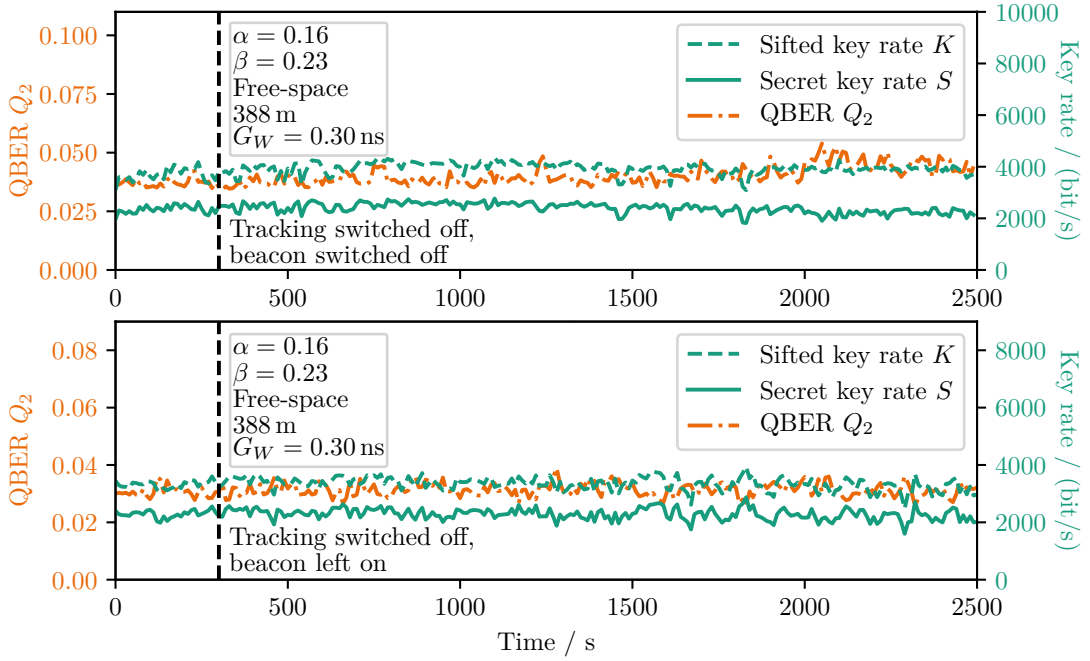


Figure 6.10.: QKD over 388 m free-space link without observable misalignment after switching off tracking. Here, despite switching off tracking, the link remains unchanged for at least 2500 s. Top: The measurement was started at 16:37 on December 12$^{\text{th}}$ 2018, Bottom: The measurement was started at 13:28 on December 13$^{\text{th}}$ 2018. Pulse parameters No. 1 from Table 6.2 are set.

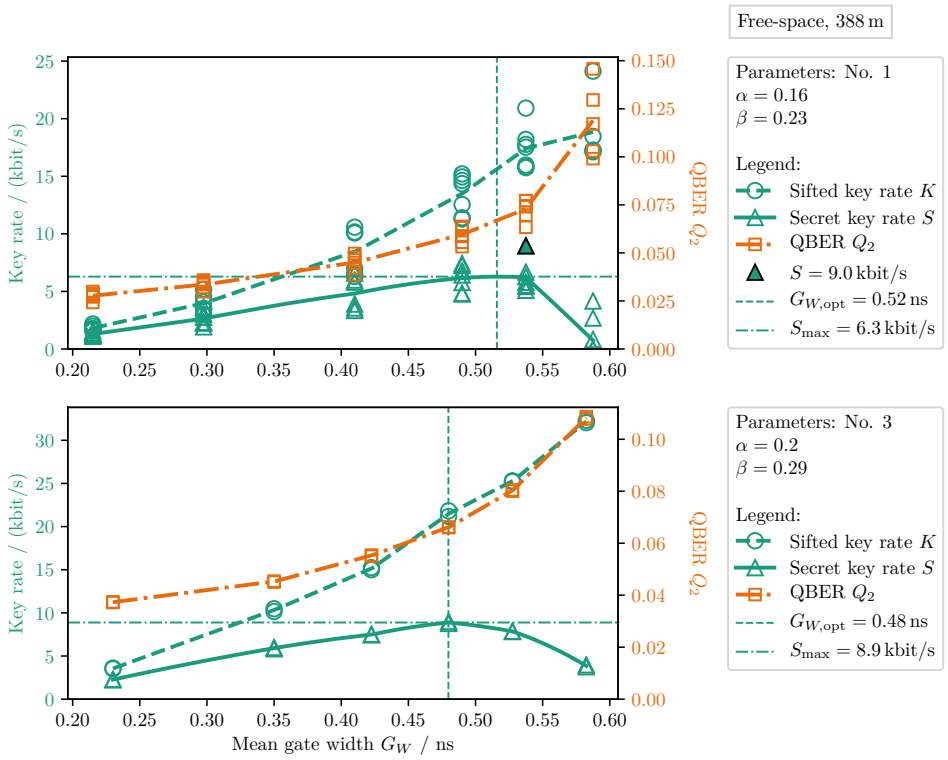


Figure 6.11.: QKD transmission over the 388 m free-space link for two sets of parameters. Measured sifted key rate K, quantum bit error rate (QBER) Q_2 and secret key rate S is plotted over the gate width G_W. The highest secret key rate $S_{\max}$ and the respective optimal gate width $G_{W,\mathrm{opt}}$ are denoted. The highest secret key rate for a single transmission over the 388 m free-space link can be seen in the top, where 9 kbit/s were achieved. Each QKD transmission was performed multiple times for the same value of gate width G_W. Over multiple transmissions, the highest mean secret key rate is slightly lower, with 8.9 kbit/s, which can be seen in the bottom plot.

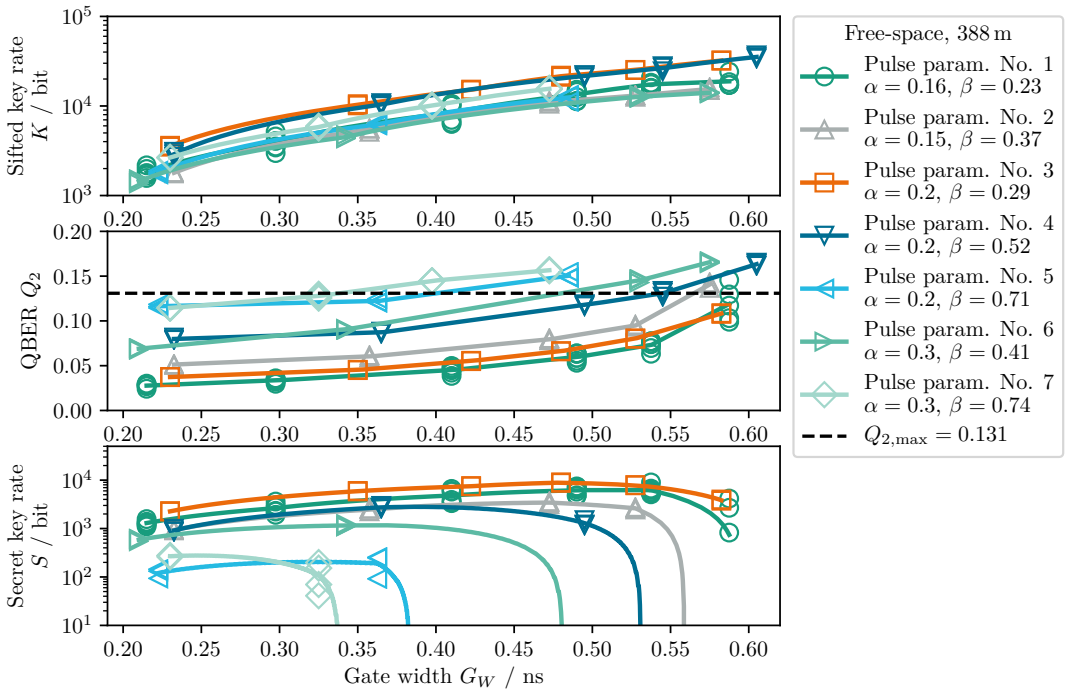


Figure 6.12.: Free-space transmissions for all set parameters and plotted over gate width. Sifted key rate K, quantum bit error rate (QBER) Q_2 and secret key rate S plotted over gate width G_W for pulse parameters No. 1 (top) and No. 2 (bottom).

as predicted, as can be seen in Figure 6.12. However for the back-to-back case pulse parameters No. 1 are slightly better in terms of secret key rate, while pulse parameters No. 3 are slightly better for the free-space case. The optimal gate width is roughly consistent with the optimal gate width found in Section 5.2.3.

However, from the top plot in Figure 6.11 it can be seen, that the values for the same gate width G_W are scattering quite a lot. One QKD transmission for pulse parameters No. 1 (top) shows a secret key rate of $S = 9.0\,\mathrm{kbit/s}$ (marked in the plot), which is higher than the highest secret key rate achieved with pulse parameters No. 3. Incidentally, this happens to be the highest secret key rate measured over the free-space testbed in the present work.

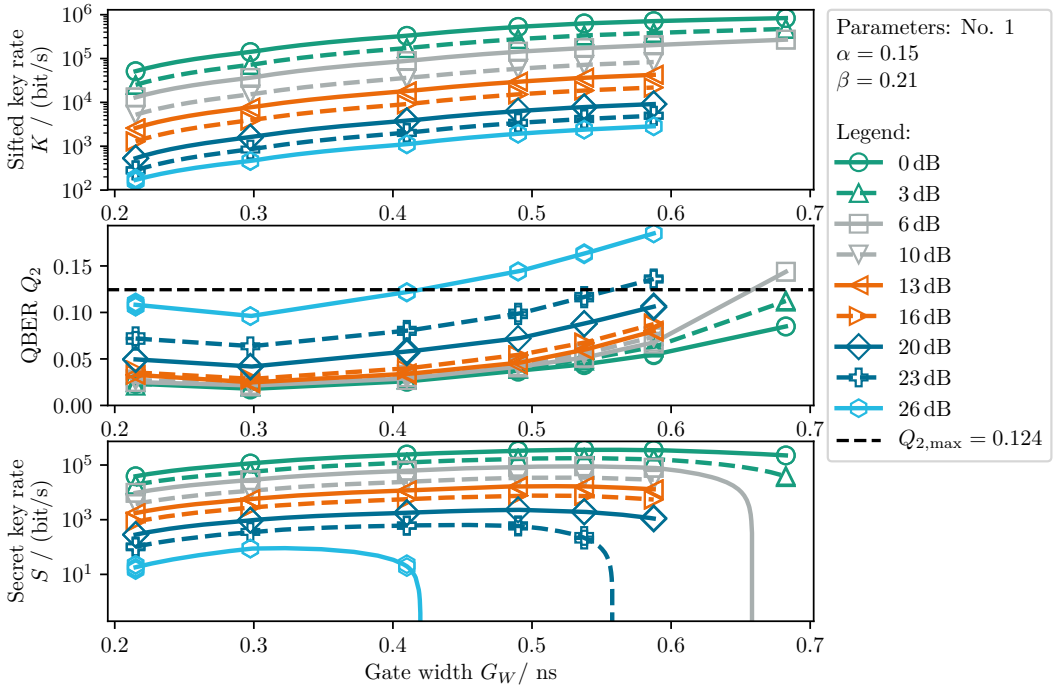


Figure 6.13.: Sifted key rate K, quantum bit error rate (QBER) Q_2 and secret key rate S plotted for the back-to-back case over the gate width for pulse parameters No. 1.

6.2.4. Comparison of free-space with back-to-back experiment

In the following the free-space QKD transmission is compared to the back-to-back case discussed in Section 5.2 for the example of pulse parameters No. 1. In Figure 6.13 the sifted key rate, QBER, and secret key rate is plotted over the gate width for the back-to-back case for all set losses.

To evaluate the free-space transmission, in Figure 6.14 the respective results are added to Figure 6.13. For better visibility the ordinate's scale is adapted according to the free-space transmission.

It can be observed, that the sifted key rate coincides quite good with the back-to-back measurement accounting for 16 dB of loss. However, looking at the QBER, one can see, that the QBER is worse than for the 16 dB back-to-back measurement for higher gate width.

For example at $G_W = 0.59\,\text{ns}$ the sifted key rate is at around 18 kbit/s for the free-space and back-to-back case. However, the QBER for the back-to-back case

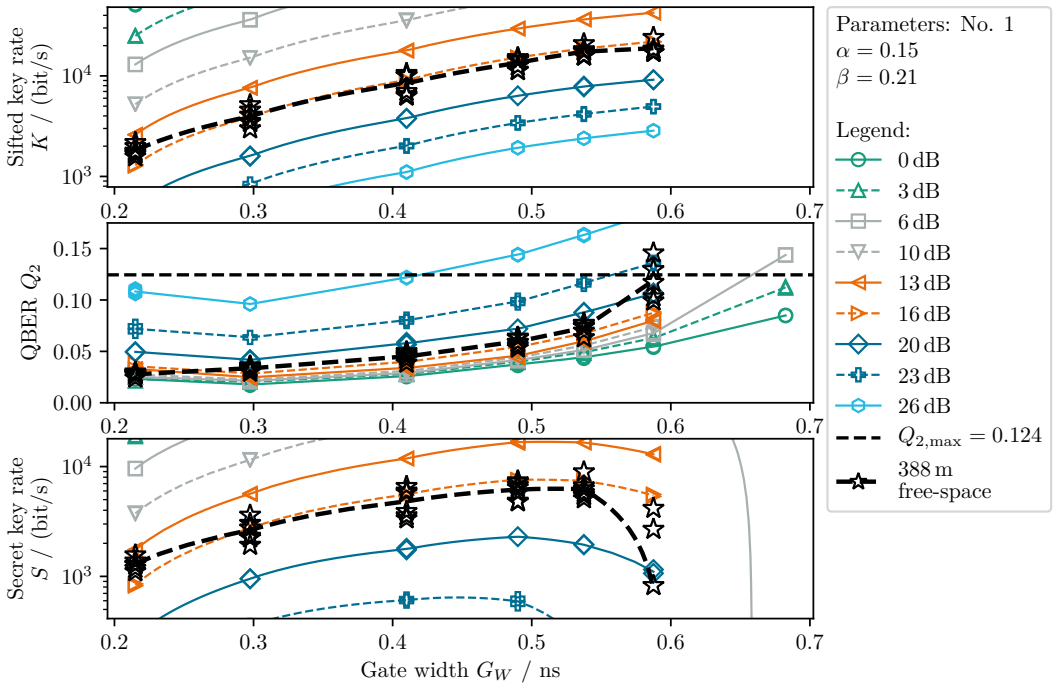


Figure 6.14.: Modification of Figure 6.13 with free-space QKD transmission for pulse parameters No. 1 added. The plot section is reduced for better visibility.

is at $Q_2 = 0.09$, whereas it is at $Q_2 = 0.12$ for the free-space case. The photons coming from the beacon and the environment are on the order of 100 Hz, which is enough for explaining the increased QBER.

6.3. Conclusion on the free-space TF-QKD transmission

In this chapter it was shown how a optical tracking system was implemented into the TF-QKD setup. With sufficient filtering two goals were achieved: A strong beacon beam can be superposed with the QKD signal, without disturbing it vitally, making optical tracking possible for the QKD system. Furthermore, stray light is successfully filtered out, which makes undisturbed day light QKD transmission possible. With long-time measurements over multiple hours, comparing transmission with and without tracking, the reliability of the tracking system could be shown.

However, it can be observed, that background counts from the environment and the beacon can result in a slightly higher QBER leading to a slightly lower Secret key rate, compared to the back-to-back case.

Finally A secret key rate of up to 9 kbit/s could be demonstrated over the 388 m test link, undisturbed by daylight and with optical tracking preserving the link.

7. Conclusion

Summary and discussion

In the presented work the TF-QKD protocol was assessed theoretically, implemented with off-the-shelf components and key distribution over a 388 m free-space testbed was demonstrated.

The theoretical assessment carried out in Chapter 3 was done with the motivation of finding the optimal parameters, namely the pulse widths, for the modulations in the time and the frequency domain. Further, the influence for a higher number of symbols per basis was elaborated. With the help of numerical optimization, optimal pulse parameters for the normalized symbol pulses α_{opt} and normalized conjugated pulse parameter β_{opt} were found. It could be shown, that narrow pulses, although leading to smaller overlaps between the symbols, are not the preferable choice, since they open up attack points an eavesdropper can exploit. Further, a tool for evaluating an implementation in terms of possible secret key rate was presented.

With the theoretical results in mind, the TF-QKD protocol was implemented in Chapter 4. It was a targeted goal of the present work to implement the protocol from off-the-shelf components and further purely single-mode fiber (SMF) based, which was successfully accomplished.

The setup was evaluated and optimized in terms of set pulse parameters and in terms of the set gate width in Chapter 5, which had a great influence on the achieved secret key rate. It could be shown, that the optimal settings (namely the APDs gate width) for the setup are depending on the transmission loss. This should always be the case for QKD protocols using gated detectors. A secret key rate of 364.6 kbit/s could be achieved back-to-back. It could further be shown, that a secret key can be distributed up to losses of 27.4 dB, which can be translated into a distance of 137 km over SMF.

Finally, the TF-QKD protocol was prepared for a free-space transmission and then demonstrated experimentally in Chapter 6 over a 388 m free-space testbed. Free-space optical antennas, which were developed at HHI, capable of precisely coupling light into SMFs were constructed and adapted for the QKD transmission. The antennas work by measuring the pointing error and correcting it accordingly. However, the QKD signal, only consisting of single photons, is not strong enough

for the antennas, which is why a beacon beam was superposed with the QKD signal. Sufficient filtering became necessary to suppress noise originating from the beacon in the QKD signal. Here wavelength division multiplexing (WDM) technology was used in order to separate beacon and QKD signal sufficiently. It was achieved that the beacon has almost no noteworthy influence on the QKD transmission. Furthermore, The QKD signal exists only in a single channel of the 200 GHz ITU grid. Both indicate, that classical communication in the remaining ITU grid channels would not be a problem for the QKD transmission, which is a whole topic of research on its own [145, 147–153].

It was also achieved, to filter out the majority of background light by means of massive spectral filtering and by filtering due to the single mode fields of the antennas. This makes QKD transmissions in daylight easily possible, which is a research topic of its own as well [40, 43, 154]. The QKD transmission could be shown to be stable for long periods of time. A secret key rate of 9 kbit/s could be demonstrated over the 388 m free-space testbed, independently of the time of day.

Outlook

A security proof against general eavesdropping attacks is still missing for the TF-QKD protocol. It could be shown in this work, that for such a proof to be carried out close attention needs to be paid to the exact pulse forms and overlap of the bases in order to prevent any leakage of information about the key to potential eavesdroppers. Security proofs against general attacks for other QKD protocols based on the time-energy uncertainty relation do exist [81, 155, 156], giving a hint, that such a proof for the TF-QKD protocol might be at the horizon.

As of today, the record in terms of secret key rate was demonstrated in [157] with 107 Mbit/s over 7.9 km of multi-core fiber, surpassing previous records [91, 155, 156, 158–160]. The presented secret key rates for the TF-QKD protocol cannot keep pace with this secret key rates, however, that was not the goal of this work after all. It was rather the goal to explore what the TF-QKD protocol was capable of with the components at hand and with only utilizing off-the-shelf SMF-based components. However, with existing off-the-shelf components, secret key rates in the state-of-the-art realm would be accessible.

The repetition rate of the presented setting was at only 30 MHz. Conceptually it would be feasible to increase the repetition rate to multiple GHz, which could increase the secret key rate to hundreds of Mbit/s or more. For that a few changes would be needed in the TF-QKD design: Tuning lasers in terms of wavelength is to slow. Instead, multiple lasers could be utilized which are switched on and off. With today's technology 100 GBit on-off-keying data rates are feasible for classical communication [161]. On the detector site superconducting nanowire single-

photon detector (SNSPD) [138, 139] could be utilized, which nowadays can have a time resolution as small as 3 ps [162]. Embedded in closed-cycle cryostats, these detectors become increasingly user-friendly [139, 163, 164]. With time-resolving detectors an arbitrarily high number of symbols could be used in the time domain, overcoming detector saturation by sending a huge number of bits per photon.

Summarizing, there is a lot of potential for the TF-QKD protocol. For TF-QKD to become a mature device which can be used in the real world, however, a few topics are still left in terms of research- and development effort to be attempted.

A. Appendix

A.1. Properties of conditional probability for wrong basis measurement

In the following it is shown, that it's matrix product of $\mathbf{P}_{E|A}^{\text{wrong}}$ with a probability vector always results in a vector which has the same elements as any of the rows in $\mathbf{P}_{E|A}^{\text{wrong}}$.

As can be seen in (3.19), $P_{E|A}^{\text{wrong}}$ is independent of a. Written as a matrix, each row of $\mathbf{P}_{E|A}^{\text{wrong}}$ is equal. Let $\mathbf{P}_A$ be a vector with the elements $a \in A$ which sum up to 1. By defining

$$P_{E|A}(e) \equiv P_{E|A}(e|a_1) = P_{E|A}(e|a_2) = \cdots = P_{E|A}(e|a_M), \tag{A.1}$$

for every $e \in E = \{e_1, \ldots, e_M\}$ it follows

$$\mathbf{P}_{E|A}^{\text{wrong}} = \begin{pmatrix} P_{E|A}(e_1) & \cdots & P_{E|A}(e_1) \\ \vdots & & \vdots \\ P_{E|A}(e_M) & \cdots & P_{E|A}(e_M) \end{pmatrix}. \tag{A.2}$$

To get $\mathbf{P}_A$, similar to (2.10) it can be written:

$$\begin{aligned} \mathbf{P}_B &= \mathbf{P}_{E|A}^{\text{wrong}} \mathbf{P}_A \\ &= \begin{pmatrix} P_{E|A}(e_1) & \cdots & P_{E|A}(e_1) \\ \vdots & & \vdots \\ P_{E|A}(e_M) & \cdots & P_{E|A}(e_M) \end{pmatrix} \begin{pmatrix} P_A(a_1) \\ \vdots \\ P_A(a_M) \end{pmatrix} \\ &= \begin{pmatrix} P_{E|A}(e_1) \overbrace{[P_A(a_1) + \ldots + P_A(e_M)]}^{=1} \\ \vdots \\ P_{E|A}(e_M) [P_A(a_1) + \ldots + P_A(e_M)] \end{pmatrix} \\ &= \begin{pmatrix} P_{E|A}(e_1) \\ \vdots \\ P_{E|A}(e_M) \end{pmatrix} \end{aligned} \tag{A.3}$$

Note, that no assumption about the elements of $\mathbf{P}_A$ was made, besides its elements summing up to one. Consequently the relation is true for all probability vectors.

It is incidental, that

$$\left(\mathbf{P}_{E|A}^{\text{wrong}}\right)^2 \mathbf{P}_A = \mathbf{P}_{E|A}^{\text{wrong}} \underbrace{\mathbf{P}_{E|A}^{\text{wrong}} \mathbf{P}_A}_{\text{probability vector}} = \mathbf{P}_{E|A}^{\text{wrong}} \mathbf{P}_A. \tag{A.4}$$

This can also phenomenologically be understood from the following example: Alice sends to Eve, while their bases differ. Bob is in the correct basis with respect to Alice in all relevant scenarios, thus he is in a different basis compared to Eve. Eve's measurement is uncorrelated to the symbol Alice sent and Bob's measurement is again uncorrelated to the symbol Bob sends. This finally means that what Eve has measured is irrelevant for Bobs measurement and he will just measure according to the conjugated pulse Eve sends.

A.2. Towards a higher alphabet: Four symbols per basis

During the course of this work the present TF-QKD implementation was explored with respect to using more symbols, namely $M = 4$ per basis. The implemented system can be seen in Figure A.1. For the FSK basis cascaded interleavers where used. A master thesis supervised within the frame of the presented work addresses the subject touched in this section [165].

For the PPM basis the DOMZM was used to distribute the odd and even time symbols. The symbols leaving one of the DOMZM outputs thus have a separation of $2\Delta t$. With a suitable huge Δt (in other words, a small α) it is possible to distinguish the symbols by means of the time resolution of the APDs. This is done by using a 3 dB-coupler and set up the gate position of the APDs such, that only one of the symbols is measured while the other one is occurring while the gate is closed.

However, with this setup the secret key rate decreases more due to additional errors and additional losses in Bob's system, than it increases by photons carrying two bits of information. Moreover the number of necessary APDs increase with the number of symbols M, while the number of carried bits only increase logarithmically with M. Consequently a different design where fewer detectors are needed is preferable.

For example time and frequency resolving detectors could be used. Detectors with a better time resolution are already on the market in the form of superconducting nano-wire single photon detectors, which reach a time-resolution in the ps

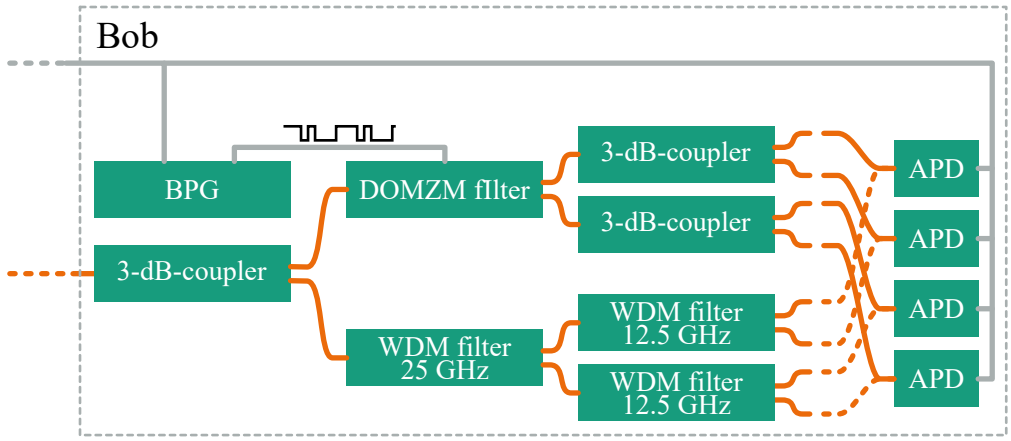


Figure A.1.: Bob's setup for $M = 4$ symbols per basis. See text for detailed explanation.

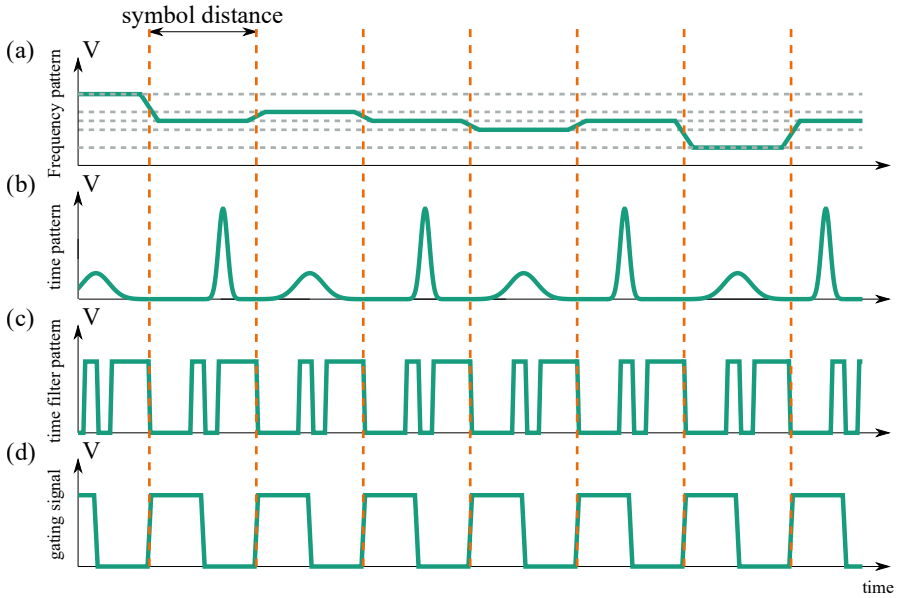


Figure A.2.: Patterns used in the $M = 4$ embodiment of the TF-QKD protocol. (a) shows the frequency pattern used for tuning the laser. (b) shows the time pattern used for shaping the pulses in the time domain. (c) shows the time filter symbol, which is used to control the dual-output Mach-Zehnder modulator (DOMZM)-filter. (d) shows the gating pattern for the avalanche photodiodes (APDs).

range. Without frequency resolving detectors one could dismantel the symmetry between PPM and FSK basis by using a large number of symbols in the PPM basis but only two in the FSK basis. In this way only three detectors would be needed, but the the advantages of using a high alphabet would still be present.

A.3. Free-space transmission: Additional calculations

A.3.1. Filtering calculations for separating QKD and beacon signal

In the following the needed filtering between the QKD and beacon signal is calculated. The power of the QKD signal leaving Alice's setup is

$$P_{\mathrm{QKD,A}} = R_{\mathrm{rep}} \mu E_{\mathrm{Photon}} \tag{A.5}$$

with R_{rep} being the systems repetition rate, μ the number of photons per pulse. The energy of a single photon is $E_{\mathrm{Photon}} = R_{\mathrm{rep}} \mu \frac{hc}{\lambda}$ with the Plank constant h, the speed of light c and the wavelength roughly being $\lambda = 1550\,\mathrm{nm}$. The beacon power needs to be such, that the power on the QD is sufficient for tracking. One has

$$P_{\mathrm{Beacon,QD}} = P_{\mathrm{Beacon,A}} \mu_L \mu_{\mathrm{BS}} \tag{A.6}$$

where in the present setup the QD power should be at least around $P_{\mathrm{Beacon,QD}} = -20\,\mathrm{dBm}$. The fraction of the signal forwarded to the QD is $\mu_{\mathrm{BS}} = -10\,\mathrm{dB}$. μ_L is the total transmission loss. The needed filtering F can with (A.5) and (A.6) be described as

$$F \geq \frac{G P_{\mathrm{QKD,A}}}{P_{\mathrm{Beacon,A}}} = \frac{G R_{\mathrm{rep}} \mu \mu_{\mathrm{BS}} hc}{\lambda P_{\mathrm{Beacon,QD}}} \mu_L. \tag{A.7}$$

Where $G = 10^3$ is the desired factor between the QKD signal and the noise photons originating from the beacon. In this way the effect of the beacon on the QBER should be negligible. One can observe, that the filtering depends on the free space link loss, as shown in Figure A.3. In the present work the free-space link loss is on the order of 20 dB, but in order for the setup to work also for higher distances with higher losses, e.g. up to 50 dB, a filtering of above 120 dB is targeted.

A.3.2. Losses caused by windows transition

The antennas and the mirror are inside buildings, thus the link runs trough multiple windows. In total, the beam passes two times trough triple glass windows

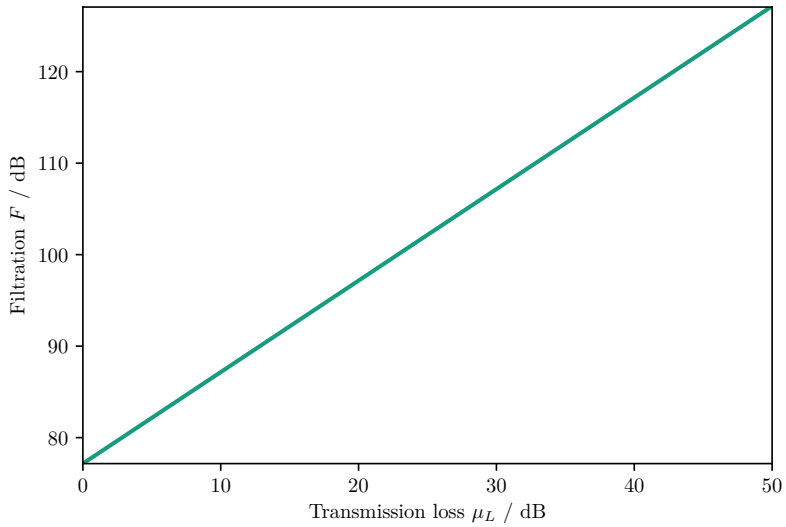
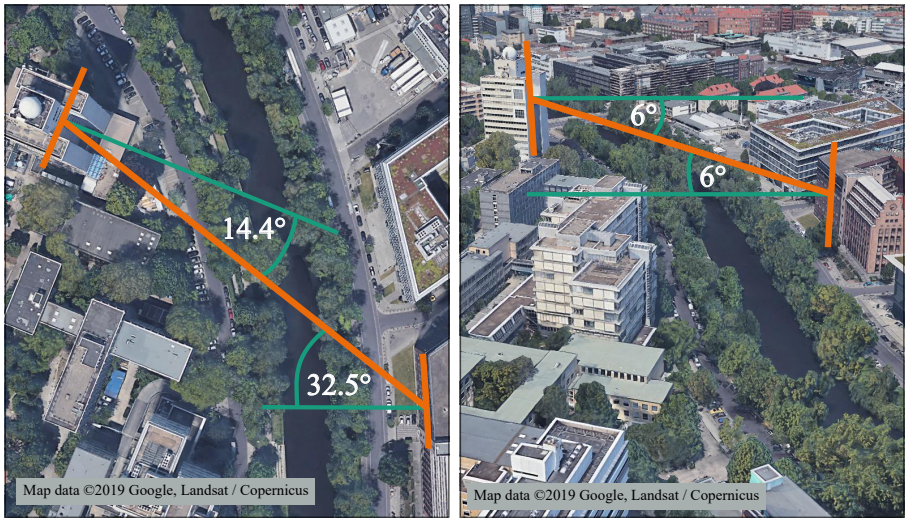


Figure A.3.: Needed filtering plotted over the transmission loss. For a certain QKD system, the filtering needed is mainly depending on the transmission loss, since the beacon beams power needs to increase the more loss it experiences in order for its signal to be detectable on the quadrant detector (QD).



(a) Azimuth (b) Elevation

Figure A.4.: Angle of the transmission beam with the windows it is passing through on its way from HHI main building to HHI site branch and back. The beam is two times passing through triple-glass windows (main building) and two times through double-glass windows (site branch). The angles are shown for azimuth (a) and elevation (b).

(at HHI main building) and two times through doublle glass windows (at HHI site branch). The refractive index of window glass is $n = 1.52$. With the Fresnel equations [118] it is possible to calculate the losses due to reflections depending on the incidence angles shown in Figure A.4. The Fresnel equations for transmission are

$$t_s = \frac{2n_1 \cos\theta_1}{n_1 \cos\theta_1 + n_2 \cos\theta_2} \tag{A.8}$$

$$t_p = \frac{2n_1 \cos\theta_1}{n_1 \cos\theta_2 + n_2 \cos\theta_1} \tag{A.9}$$

and with Snell's law

$$n_1 \sin\theta_1 = n_2 \sin\theta_2. \tag{A.10}$$

A total transmission of 0.41 is achieved which is equivalent to 3.9 dB of loss, assuming uniformly random polarization.

Acronyms

APD	avalanche photodiode
AWG	arbitrary waveform generator
BPG	bit-pattern generator
CV	continuous variable
CW	continuous wave
DBR	distributed Bragg reflector
DOMZM	dual-output Mach-Zehnder modulator
DV	discrete variable
DWDM	dense wavelength division multiplexing
EDFA	erbium doped fiber amplifier
FSK	frequency-shift keying
HHI	Fraunhofer Heinrich Hertz Institute
IR	intercept/resend
ITU	International Telecommunication Union
MZM	Mach-Zehnder modulator
PNS	photon number splitting
PPM	pulse-position modulation
QBER	quantum bit error rate
QD	quadrant detector
QKD	quantum key distribution

QSER	quantum symbol error rate
SMF	single-mode fiber
SNSPD	superconducting nanowire single-photon detector
TF	time-frequency
WDM	wavelength division multiplexing

Bibliography

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

[2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[3] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*. Springer, 1985, pp. 417–426.

[4] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[5] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, "Report on the development of the advanced encryption standard (aes)," *Journal of Research of the National Institute of Standards and Technology*, vol. 106, no. 3, p. 511, 2001.

[6] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, p. 45, 2010.

[7] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[8] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'brien, "Experimental realization of shor's quantum factoring algorithm using qubit recycling," *Nature Photonics*, vol. 6, no. 11, p. 773, 2012.

[9] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner *et al.*, "Computing prime factors with a josephson phase qubit quantum processor," *Nature Physics*, vol. 8, no. 10, p. 719, 2012.

[10] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, "Realization of a scalable shor algorithm," *Science*, vol. 351, no. 6277, pp. 1068–1070, 2016.

[11] M. Steffen, D. P. DiVincenzo, J. M. Chow, T. N. Theis, and M. B. Ketchen, "Quantum computing: An ibm perspective," *IBM Journal of Research and Development*, vol. 55, no. 5, pp. 13–1, 2011.

[12] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Experimental comparison of two quantum computing architectures," *Proceedings of the National Academy of Sciences*, vol. 114, no. 13, pp. 3305–3310, 2017.

[13] K. Svore, A. Geller, M. Troyer, J. Azariah, C. Granade, B. Heim, V. Kliuchnikov, M. Mykhailova, A. Paz, and M. Roetteler, "Q#: Enabling scalable quantum computing and development with a high-level dsl," in *Proceedings of the Real World Domain Specific Languages Workshop 2018*. ACM, 2018, p. 7.

[14] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, "Characterizing quantum supremacy in near-term devices," *Nature Physics*, vol. 14, no. 6, p. 595, 2018.

[15] C. Neill, P. Roushan, K. Kechedzhi, S. Boixo, S. V. Isakov, V. Smelyanskiy, A. Megrant, B. Chiaro, A. Dunsworth, K. Arya *et al.*, "A blueprint for demonstrating quantum supremacy with superconducting qubits," *Science*, vol. 360, no. 6385, pp. 195–199, 2018.

[16] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of gsm encrypted communication," in *Annual international cryptology conference*. Springer, 2003, pp. 600–616.

[17] O. Dunkelman, N. Keller, and A. Shamir, "A practical-time attack on the a5/3 cryptosystem used in third generation gsm telephony." *IACR Cryptology ePrint Archive*, vol. 2010, p. 13, 2010.

[18] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," *Journal of CRYPTOLOGY*, vol. 4, no. 1, pp. 3–72, 1991.

[19] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *AIEE, Journal of the*, vol. 45, no. 2, pp. 109–115, 1926.

[20] H. Bennett Ch and G. Brassard, "Quantum cryptography: public key distribution and coin tossing int," in *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, 1984, pp. 175–9.

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

[22] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical review letters*, vol. 117, no. 19, p. 190501, 2016.

[23] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography," *Japanese Journal of Applied Physics*, vol. 43, no. 9A, p. L1217, 2004.

[24] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, no. 7, p. 075003, 2009.

[25] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.

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

[27] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature communications*, vol. 6, p. 6787, 2015.

[28] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, p. 400, 2018.

[29] M. Pant, H. Krovi, D. Englund, and S. Guha, "Rate-distance tradeoff and resource costs for all-optical quantum repeaters," *Physical Review A*, vol. 95, no. 1, p. 012304, 2017.

[30] K. Azuma, A. Mizutani, and H.-K. Lo, "Fundamental rate-loss trade-off for the quantum internet," *Nature communications*, vol. 7, p. 13523, 2016.

[31] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, "Overcoming lossy channel bounds using a single quantum repeater node," *Applied Physics B*, vol. 122, no. 4, p. 96, 2016.

[32] T. Chaneliere, D. Matsukevich, S. Jenkins, S.-Y. Lan, T. Kennedy, and A. Kuzmich, "Storage and retrieval of single photons transmitted between remote quantum memories," *Nature*, vol. 438, no. 7069, p. 833, 2005.

[33] C. Simon, M. Afzelius, J. Appel, A. B. de La Giroday, S. Dewhurst, N. Gisin, C. Hu, F. Jelezko, S. Kröll, J. Müller *et al.*, "Quantum memories," *The European Physical Journal D*, vol. 58, no. 1, pp. 1–22, 2010.

[34] K. Heshami, D. G. England, P. C. Humphreys, P. J. Bustard, V. M. Acosta, J. Nunn, and B. J. Sussman, "Quantum memories: emerging applications and recent advances," *Journal of modern optics*, vol. 63, no. 20, pp. 2005–2028, 2016.

[35] F. Bussières, N. Sangouard, M. Afzelius, H. De Riedmatten, C. Simon, and W. Tittel, "Prospective applications of optical quantum memories," *Journal of Modern Optics*, vol. 60, no. 18, pp. 1519–1537, 2013.

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

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

[38] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[39] W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," *Physical Review Letters*, vol. 81, no. 15, p. 3283, 1998.

[40] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New journal of physics*, vol. 4, no. 1, p. 43, 2002.

[41] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, "Free space quantum key distribution: Towards a real life application," *Fortschritte der Physik: Progress of Physics*, vol. 54, no. 8-10, pp. 840–845, 2006.

[42] M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein *et al.*, "Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources – a proof of principle experiment," *New Journal of Physics*, vol. 16, no. 4, p. 043003, 2014.

[43] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photonics*, vol. 11, no. 8, p. 509, 2017.

[44] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007.

[45] T. Schmitt-Manderbach, "Long distance free-space quantum key distribution," Ph.D. dissertation, LMU München München, 2007.

[46] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, "Entanglement-based quantum communication over 144 km," *Nature physics*, vol. 3, no. 7, p. 481, 2007.

[47] S. F. Yelin and B. C. Wang, "A novel time-frequency quantum key distribution technique for optical fiber communication systems," in *Optical Fiber Communication Conference*. Optical Society of America, 2004, p. TuN1.

[48] Z. Chang-Hua, P. Chang-Xing, Q. Dong-Xiao, G. Jing-Liang, C. Nan, and Y. Yun-Hui, "A new quantum key distribution scheme based on frequency and time coding," *Chinese Physics Letters*, vol. 27, no. 9, p. 090301, 2010.

[49] K. Liu, C. R. Ye, S. Khan, and V. J. Sorger, "Review and perspective on ultrafast wavelength-size electro-optic modulators," *Laser & Photonics Reviews*, vol. 9, no. 2, pp. 172–194, 2015.

[50] E. L. Wooten, K. M. Kissa, A. Yi-Yan, E. J. Murphy, D. A. Lafaw, P. F. Hallemeier, D. Maack, D. V. Attanasio, D. J. Fritz, G. J. McBrien *et al.*,

"A review of lithium niobate modulators for fiber-optic communications systems," *IEEE Journal of selected topics in Quantum Electronics*, vol. 6, no. 1, pp. 69–82, 2000.

[51] A. Banerjee, Y. Park, F. Clarke, H. Song, S. Yang, G. Kramer, K. Kim, and B. Mukherjee, "Wavelength-division-multiplexed passive optical network (WDM-PON) technologies for broadband access: a review," *Journal of optical networking*, vol. 4, no. 11, pp. 737–758, 2005.

[52] S. Bhatt and S. Jhaveri, "A review of dense wavelength division multiplexing and next generation optical internet," *International Journal of Engineering Science and Innovative Technology*, vol. 2, pp. 404–412, 2013.

[53] K. Kiasaleh, "Performance of apd-based, ppm free-space optical communication systems in atmospheric turbulence," *IEEE transactions on communications*, vol. 53, no. 9, pp. 1455–1461, 2005.

[54] T. T. Nguyen and L. Lampe, "Coded multipulse pulse-position modulation for free-space optical communications," *IEEE Transactions on Communications*, vol. 58, no. 4, pp. 1036–1041, 2010.

[55] D.-s. Shiu and J. M. Kahn, "Differential pulse-position modulation for power-efficient optical communication," *IEEE transactions on communications*, vol. 47, no. 8, pp. 1201–1210, 1999.

[56] Z. Sodnik, B. Furch, and H. Lutz, "Free-space laser communication activities in europe: Silex and beyond," in *LEOS 2006-19th Annual Meeting of the IEEE Lasers and Electro-Optics Society.* IEEE, 2006, pp. 78–79.

[57] M. De Sanctis, E. Cianca, T. Rossi, C. Sacchi, L. Mucchi, and R. Prasad, "Waveform design solutions for ehf broadband satellite communications," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 18–23, 2015.

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

[59] M. Fox, *Quantum optics: an introduction.* OUP Oxford, 2006, vol. 15.

[60] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, p. 16025, 2016.

[61] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.

[62] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Scientific reports*, vol. 6, p. 19201, 2016.

[63] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Physical review letters*, vol. 114, no. 7, p. 070501, 2015.

[64] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015.

[65] A. Leverrier, "Security of continuous-variable quantum key distribution via a gaussian de finetti reduction," *Physical review letters*, vol. 118, no. 20, p. 200501, 2017.

[66] B. Qi, "Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation," *Optics letters*, vol. 31, no. 18, pp. 2795–2797, 2006.

[67] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.

[68] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," *Physical review letters*, vol. 98, no. 6, p. 060503, 2007.

[69] S. Yelin and B. C. Wang, "Time-frequency bases for bb84 protocol," *arXiv preprint quant-ph/0309105*, 2003.

[70] J. Nunn, L. Wright, C. Söller, L. Zhang, I. Walmsley, and B. Smith, "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," *Optics express*, vol. 21, no. 13, pp. 15 959–15 973, 2013.

[71] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations," *Physical Review A*, vol. 62, no. 6, p. 062308, 2000.

[72] M. Hillery, "Quantum cryptography with squeezed states," *Physical Review A*, vol. 61, no. 2, p. 022309, 2000.

[73] T. C. Ralph, "Continuous variable quantum cryptography," *Physical Review A*, vol. 61, no. 1, p. 010303, 1999.

[74] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review*, vol. 47, no. 10, p. 777, 1935.

[75] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," *Physical Review A*, vol. 63, no. 1, p. 012309, 2000.

[76] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[77] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[78] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li *et al.*, "Experimental measurement-device-independent quantum key distribution," *Physical review letters*, vol. 111, no. 13, p. 130502, 2013.

[79] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature communications*, vol. 2, p. 238, 2011.

[80] L. Zhang, C. Silberhorn, and I. A. Walmsley, "Secure quantum key distribution using continuous variables of single photons," *Physical review letters*, vol. 100, no. 11, p. 110504, 2008.

[81] Z. Zhang, J. Mower, D. Englund, F. N. Wong, and J. H. Shapiro, "Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry," *Physical review letters*, vol. 112, no. 12, p. 120506, 2014.

[82] M. Leifgen, R. Elschner, N. Perlot, C. Weinert, C. Schubert, and O. Benson, "Practical implementation and evaluation of a quantum-key-distribution scheme based on the time-frequency uncertainty," *Physical Review A*, vol. 92, no. 4, p. 042311, 2015.

[83] Y. Zhang, I. B. Djordjevic, and M. A. Neifeld, "Weak-coherent-state-based time-frequency quantum key distribution," *Journal of Modern Optics*, vol. 62, no. 20, pp. 1713–1721, 2015.

[84] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, "Experimental open-air quantum key distribution with a single-photon source," *New Journal of physics*, vol. 6, no. 1, p. 92, 2004.

[85] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, "Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors," *Scientific reports*, vol. 5, p. 14383, 2015.

[86] M. Leifgen, T. Schröder, F. Gädeke, R. Riemann, V. Métillon, E. Neu, C. Hepp, C. Arend, C. Becher, K. Lauritsen *et al.*, "Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution," *New journal of physics*, vol. 16, no. 2, p. 023021, 2014.

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

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

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

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

[91] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Optics express*, vol. 21, no. 21, pp. 24 550–24 565, 2013.

[92] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, "Decoy-state quantum key distribution with biased basis choice," *Scientific reports*, vol. 3, p. 2453, 2013.

[93] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Physical Review A*, vol. 89, no. 2, p. 022307, 2014.

[94] M. Lucamarini, J. F. Dynes, B. Fröhlich, Z. Yuan, and A. J. Shields, "Security bounds for efficient decoy-state quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 197–204, 2015.

[95] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Physical Review A*, vol. 95, no. 1, p. 012333, 2017.

[96] R. Meester, *A Natural Introduction to Probability Theory*. Birkhäuser, 2003.

[97] H. Hemmati, *Deep space optical communications*. John Wiley & Sons, 2006, vol. 11.

[98] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 1991.

[99] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[100] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Citeseer, 2005.

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

[102] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Information reconciliation for quantum key distribution," *Quantum Information and Computation*, vol. 11, no. 3&4, pp. 0226–0238, 2011.

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

[104] T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 83, no. 10, pp. 1987–1991, 2000.

[105] S. Liu, H. C. Van Tilborg, and M. Van Dijk, "A practical protocol for advantage distillation and information reconciliation," *Designs, Codes and Cryptography*, vol. 30, no. 1, pp. 39–62, 2003.

[106] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. Nickel, C. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A*, vol. 67, no. 5, p. 052303, 2003.

[107] J. S. Johnson, M. R. Grimaila, J. W. Humphries, and G. B. Baumgartner, "An analysis of error reconciliation protocols used in quantum key distribution systems," *The Journal of Defense Modeling and Simulation*, vol. 12, no. 3, pp. 217–227, 2015.

[108] E. Voges and K. Petermann, *Optische Kommunikationstechnik: Handbuch für Wissenschaft und Industrie*. Springer, 2002.

[109] D. Marcuse, "Gaussian approximation of the fundamental modes of graded-index fibers," *JOSA*, vol. 68, no. 1, pp. 103–109, 1978.

[110] A. Sharma, S. Hosain, and A. Ghatak, "The fundamental mode of graded-index fibres: simple and accurate variational methods," *Optical and Quantum Electronics*, vol. 14, no. 1, pp. 7–15, 1982.

[111] A. Ankiewicz and G.-D. Peng, "Generalized gaussian approximation for single-mode fibers," *Journal of lightwave technology*, vol. 10, no. 1, pp. 22–27, 1992.

[112] S. Nemoto and T. Makimoto, "Analysis of splice loss in single-mode fibres using a gaussian field approximation," *Optical and Quantum Electronics*, vol. 11, no. 5, pp. 447–457, 1979.

[113] I. I. Kim, B. McArthur, and E. J. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," in *Optical Wireless Communications III*, vol. 4214. International Society for Optics and Photonics, 2001, pp. 26–38.

[114] M. Bass, C. DeCusatis, J. Enoch, V. Lakshminarayanan, G. Li, C. Macdonald, V. Mahajan, and E. Van Stryland, *Handbook of Optics, Third Edition Volume V: Atmospheric Optics, Modulators, Fiber Optics, X-Ray and Neutron Optics*, 3rd ed. New York, NY, USA: McGraw-Hill, Inc., 2010.

[115] H. Willebrand and B. S. Ghuman, *Free space optics: enabling optical connectivity in today's networks*. SAMS publishing, 2002.

[116] R. Ramirez-Iniguez, S. M. Idrus, and Z. Sun, *Optical wireless communications: IR for wireless connectivity*. Auerbach Publications, 2008.

[117] Y. Dikmelik and F. M. Davidson, "Fiber-coupling efficiency for free-space optical communication through atmospheric turbulence," *Applied Optics*, vol. 44, no. 23, pp. 4946–4952, 2005.

[118] E. Hecht, *Optics*. Pearson Education, Incorporated, 2017.

[119] M. E. Grein, A. J. Kerman, E. A. Dauler, O. Shatrovoy, R. J. Molnar, D. Rosenberg, J. Yoon, C. E. DeVoe, D. V. Murphy, B. S. Robinson *et al.*, "Design of a ground-based optical receiver for the lunar laser communications demonstration," in *2011 International Conference on Space Optical Systems and Applications (ICSOS)*. IEEE, 2011, pp. 78–82.

[120] N. Perlot, J. Rödiger, and R. Freund, "Single-mode optical antenna for high-speed and quantum communications," in *Photonic Networks; 19th ITG-Symposium*. VDE, 2018, pp. 1–4.

[121] T. Bifano, "Adaptive imaging: Mems deformable mirrors," *Nature photonics*, vol. 5, no. 1, p. 21, 2011.

[122] S. Cornelissen, A. Hartzell, J. Stewart, T. Bifano, and P. Bierden, "Mems deformable mirrors for astronomical adaptive optics," in *Adaptive Optics Systems II*, vol. 7736. International Society for Optics and Photonics, 2010, p. 77362D.

[123] P.-Y. Madec, "Overview of deformable mirror technologies for adaptive optics and astronomy," in *Adaptive Optics Systems III*, vol. 8447. International Society for Optics and Photonics, 2012, p. 844705.

[124] J. Rödiger, N. Perlot, R. Mottola, R. Elschner, C.-M. Weinert, O. Benson, and R. Freund, "Numerical assessment and optimization of discrete-variable time-frequency quantum key distribution," *Phys. Rev. A*, vol. 95, p. 052312, May 2017.

[125] S. Constantine, L. E. Elgin, M. L. Stevens, J. A. Greco, K. Aquino, D. D. Alves, and B. S. Robinson, "Design of a high-speed space modem for the lunar laser communications demonstration," in *SPIE LASE*. International Society for Optics and Photonics, 2011, pp. 792 308–792 308.

[126] C. Kollmitzer and M. Pivk, *Applied quantum cryptography*. springer, 2010, vol. 797.

[127] D. M. Olsson and L. S. Nelson, "The nelder-mead simplex procedure for function minimization," *Technometrics*, vol. 17, no. 1, pp. 45–51, 1975.

[128] J. Rödiger, N. Perlot, and R. Freund, "Quantum cryptography over the FSO channel with PPM and FSK modulations," in *Broadband Coverage in Germany. 9th ITG Symposium. Proceedings*. VDE, 2015, pp. 1–5.

[129] J. Rödiger, N. Perlot, O. Benson, and R. Freund, "Benefits of time-frequency coding for quantum key distribution," in *International Conference on Space Optics – ICSO 2016*, vol. 10562. International Society for Optics and Photonics, 2017, p. 105623N.

[130] F. Beutel, J. Rödiger, N. Perlot, R. Freund, and O. Benson, "Quantum key distribution over free space," in *Advanced Study Institute on NATO ASI on Quantum Nano-Photonics*. Springer, 2017, pp. 357–359.

[131] J. Rödiger, N. Perlot, F. Beutel, R. Freund, and O. Benson, "Time-frequency QKD over the free-space channel with optical tracking in daylight (tbd)," *in preparation*, 2019.

[132] A. J. Ward, D. J. Robbins, G. Busico, E. Barton, L. Ponnampalam, J. P. Duck, N. D. Whitbread, P. J. Williams, D. C. Reid, A. C. Carter *et al.*, "Widely tunable ds-dbr laser with monolithically integrated soa: Design and performance," *IEEE Journal of selected topics in quantum electronics*, vol. 11, no. 1, pp. 149–156, 2005.

[133] J. Buus and E. J. Murphy, "Tunable lasers in optical networks," *Journal of Lightwave Technology*, vol. 24, no. 1, p. 5, 2006.

[134] Y.-C. Hsieh, "Application of a step-phase interferometer in optical communication," 2003, uS Patent 6,587,204.

[135] M. Sharma, "Compression using huffman coding," *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, no. 5, pp. 133–141, 2010.

[136] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, "Quantum key distribution system clocked at 2 ghz," *Optics Express*, vol. 13, no. 8, pp. 3015–3020, 2005.

[137] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 ghz time-bin quantum key distribution," *Applied Physics Letters*, vol. 112, no. 17, p. 171108, 2018.

[138] E. A. Dauler, M. E. Grein, A. J. Kerman, F. Marsili, S. Miki, S. W. Nam, M. D. Shaw, H. Terai, V. B. Verma, and T. Yamashita, "Review of superconducting nanowire single-photon detector system design options and demonstrated performance," *Optical Engineering*, vol. 53, no. 8, pp. 081 907–081 907, 2014.

[139] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," *Superconductor science and technology*, vol. 25, no. 6, p. 063001, 2012.

[140] F. Beutel, "Implementation and evaluation of time-frequency quantum key distribution over free space," Master's thesis, Humboldt-Universität zu Berlin, 2017.

[141] J. H. Shapiro and A. L. Puryear, "Reciprocity-enhanced optical communication through atmospheric turbulence–part i: Reciprocity proofs and far-field power transfer optimization," *Journal of Optical Communications and Networking*, vol. 4, no. 12, pp. 947–954, 2012.

[142] S. Sharma, "Quantum cryptography over free-space with active optical tracking," Master's thesis, Humboldt-Universität zu Berlin, 2019.

[143] ITU-T Rec, "G. 694.1," *International Telecommunications Union-Standardization Sector [ITU-T]*, 2012.

[144] C. V. Raman, "A new radiation," *Indian Journal of physics*, vol. 2, pp. 387–398, 1928.

[145] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[146] K. Patel, J. Dynes, I. Choi, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Physical Review X*, vol. 2, no. 4, p. 041010, 2012.

[147] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada *et al.*, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels," *Communications Physics*, vol. 2, no. 1, p. 9, 2019.

[148] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao *et al.*, "Integrating quantum key distribution with classical communications in backbone fiber network," *Optics express*, vol. 26, no. 5, pp. 6010–6020, 2018.

[149] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable qkd with intense dwdm classical channels," *New Journal of Physics*, vol. 17, no. 4, p. 043027, 2015.

[150] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, p. 051123, 2014.

[151] A. Tanaka, M. Fujiwara, K.-i. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki *et al.*, "High-speed quantum key distribution system for 1-mbps real-time key generation," *IEEE Journal of Quantum Electronics*, vol. 48, no. 4, pp. 542–550, 2012.

[152] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New Journal of Physics*, vol. 12, no. 10, p. 103042, 2010.

[153] N. Peters, P. Toliver, T. Chapuran, R. Runser, S. McNown, C. Peterson, D. Rosenberg, N. Dallmann, R. Hughes, K. McCabe *et al.*, "Dense wavelength multiplexing of 1550 nm qkd with strong classical channels in reconfigurable networking environments," *New Journal of physics*, vol. 11, no. 4, p. 045012, 2009.

[154] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," *New Journal of Physics*, vol. 11, no. 4, p. 045007, 2009.

[155] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," *Science advances*, vol. 3, no. 11, p. e1701491, 2017.

[156] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits *et al.*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," *New Journal of Physics*, vol. 17, no. 2, p. 022002, 2015.

[157] B. Da Lio, D. Bacco, D. Cozzolino, F. Da Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai *et al.*, "Record-high secret key rate for joint classical and quantum transmission over a 37-core fiber," in *2018 IEEE Photonics Conference (IPC)*. IEEE, 2018, pp. 1–2.

[158] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, "High-rate field demonstration of large-alphabet quantum key distribution," *arXiv preprint arXiv:1611.01139*, 2016.

[159] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami *et al.*, "10-mb/s quantum key distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[160] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photonics*, vol. 10, no. 5, p. 312, 2016.

[161] S. Wolf, H. Zwickel, W. Hartmann, M. Lauermann, Y. Kutuvantavida, C. Kieninger, L. Altenhain, R. Schmid, J. Luo, A. K.-Y. Jen *et al.*, "Silicon-organic hybrid (soh) mach-zehnder modulators for 100 gbit/s on-off keying," *Scientific reports*, vol. 8, no. 1, p. 2598, 2018.

[162] B. Korzh, Q. Zhao, S. Frasca, J. Allmaras, T. Autry, E. Bersin, M. Colangelo, G. Crouch, A. Dane, T. Gerrits *et al.*, "Demonstrating sub-3 ps temporal resolution in a superconducting nanowire single-photon detector," *arXiv preprint arXiv:1804.06839*, 2018.

[163] R. Radebaugh, "Cryocoolers: the state of the art and recent developments," *Journal of Physics: Condensed Matter*, vol. 21, no. 16, p. 164219, 2009.

[164] R. H. Hadfield, M. J. Stevens, S. S. Gruber, A. J. Miller, R. E. Schwall, R. P. Mirin, and S. W. Nam, "Single photon source characterization with a superconducting single photon detector," *Optics Express*, vol. 13, no. 26, pp. 10 846–10 853, 2005.

[165] R. Mottola, "Implementation and characterization of large alphabet time-frequency quantum key distribution," Master's thesis, Humboldt-Universität zu Berlin, 2016.

Relevant own publications

[P1] J. Rödiger, N. Perlot, and R. Freund, "Quantum cryptography over the FSO channel with PPM and FSK modulations," in *Broadband Coverage in Germany. 9th ITG Symposium. Proceedings*. VDE, 2015, pp. 1–5.

[P2] J. Rödiger, N. Perlot, O. Benson, and R. Freund, "Benefits of time-frequency coding for quantum key distribution," in *International Conference on Space Optics–ICSO 2016*, vol. 10562. International Society for Optics and Photonics, 2017, p. 105623N.

[P3] J. Rödiger, N. Perlot, R. Mottola, R. Elschner, C.-M. Weinert, O. Benson, and R. Freund, "Numerical assessment and optimization of discrete-variable time-frequency quantum key distribution," *Phys. Rev. A*, vol. 95, p. 052312, May 2017.

[P4] F. Beutel, J. Rödiger, N. Perlot, R. Freund, and O. Benson, "Quantum key distribution over free space," in *Advanced Study Institute on NATO ASI on Quantum Nano-Photonics*. Springer, 2017, pp. 357–359.

[P5] N. Perlot, J. Rödiger, and R. Freund, "Single-mode optical antenna for high-speed and quantum communications," in *Photonic Networks; 19th ITG-Symposium*. VDE, 2018, pp. 1–4.

[P6] S. Sharma, N. Perlot, J. Rödiger, and R. Freund, "Tracking challenges of qkd over relay satellite," in *Proceedings of ICSO 2018*, 2018.

[P7] O. Benson, T. Kroh, C. Müller, J. Rödiger, and N. Perlot, *Semiconductor Nanophotonics – Materials, Models, Devices*. Springer, 2020, ch. Quantum networks based on single photons.

[P8] J. Rödiger, N. Perlot, R. Mottola, M. Leifgen, R. Elschner, O. Benson, and R. Freund, "Large-alphabet Time-Frequency QKD," in *QCrypt, 5th International Conference on Quantum Cryptography*, (Poster), Tokyo, Japan, 2015.

[P9] J. Rödiger, N. Perlot, M. Leifgen, R. Elschner, R. Mottola, O. Benson, and R. Freund, "Large-alphabet time-frequency quantum key distribution," in *DPG Frühjahrstahung 2016*, (Talk), Hannover, Germany, 2016.

[P10] F. Beutel, J. Rödiger, N. Perlot, O. Benson, and R. Freund, "Evaluation of time-frequency QKD over different transmission channels," in *QCrypt, 6th International Conference on Quantum Cryptography*, (Poster), Washington, USA, 2016.

[P11] F. Beutel, J. Rödiger, N. Perlot, R. Freund, and O. Benson, "Time-frequency quantum key distribution over free space," in *DPG Frühjahrstahung 2017*, (Talk), Mainz, Germany, 2017.

[P12] J. Rödiger, N. Perlot, R. Freund, and O. Benson, "Time-frequency quantum key distribution for satellite communication," in *COST Action CA15220, Quantum Technologies in Space*, (Talk), Valletta, Malta, 2017.

[P13] J. Rödiger, N. Perlot, R. Freund, and O. Benson, "Time-frequency QKD over free-space and fiber channels," in *QCrypt, 7th International Conference on Quantum Cryptography*, (Poster), Cambridge, United Kingdom, 2017.

[P14] J. Rödiger, N. Perlot, F. Beutel, R. Freund, and O. Benson, "Time-frequency QKD over the free-space channel with optical tracking in daylight (tbd)," *in preparation*, 2019.

Other own publications

[O1] N. Kukharchyk, S. Pal, J. Rödiger, A. Ludwig, S. Probst, A. V. Ustinov, P. Bushev, and A. D. Wieck, "Photoluminescence of focused ion beam implanted er3+: Y2sio5 crystals," *physica status solidi (RRL)–Rapid Research Letters*, vol. 8, no. 10, pp. 880–884, 2014.

[O2] J. Rödiger, N. Perlot, and M. Rohde, "Freistrahloptische turbulenzschlüsselverteilung," in *Research Day 2016 Tagungsband*, Beuth Hochschule für Technik Berlin, 2016, pp. 80–85.

[O3] T. Lühmann, N. Raatz, R. John, M. Lesik, J. Rödiger, M. Portail, D. Wildanger, F. Kleißler, K. Nordlund, A. Zaitsev *et al.*, "Screening and engineering of colour centres in diamond," *Journal of Physics D: Applied Physics*, vol. 51, no. 48, p. 483002, 2018.

Supervised master theses

[M1] R. Mottola, "Implementation and characterization of large alphabet time-frequency quantum key distribution," Master's thesis, Humboldt-Universität zu Berlin, 2016.

[M2] S. Sharma, "Quantum cryptography over free-space with active optical tracking," Master's thesis, Humboldt-Universität zu Berlin, 2019.

[M3] F. Beutel, "Implementation and evaluation of time-frequency quantum key distribution over free space," Master's thesis, Humboldt-Universität zu Berlin, 2017.

List of Figures

2.1. BB84 protocol 7
2.2. Post processing and information 15
2.3. Antenna mismatch definition 18
2.4. Transmission in the atmosphere 19

3.1. Bases used in TF-QKD 22
3.2. Definition of bins for TF-QKD 25
3.3. Visualization of the conditional probability for symbol and conjugated pulses 27
3.4. Secret capacity for the one-level intercept/resend attack 33
3.5. Eves eavesdropping setup for the two-level intercept/resend attack . 35
3.6. Secret capacity for two-level intercept/resend attack 38
3.7. Visualization of the overlap function 40
3.8. Results for optimal normalized symbol pulse width, optimal normalized conjugated pulse width and the secret capacity 41
3.9. Optimal pulse parameters for $M = 2$ symbols per basis 42
3.10. Secret capacity $C_{2\mathrm{L}}$ over QBER for $M = 2$ symbols per basis 43

4.1. Simplified TF-QKD setup 47
4.2. Alice's setup 48
4.3. Patters steering the transmission 49
4.4. Pulse shapes in the time domain 50
4.5. Bob's setup 51

5.1. Set and measured pulse widths in the time domain and pulse intensity in terms of photon number per pulse 59
5.2. Transmission evaluation measurement and categorization 61
5.3. Measured pulse width for set parameters 64
5.4. Back-to-back Transmission for different transmission losses 65
5.5. Sifted key rate and QBER over Loss for different gate widths (back-to-back) 67
5.6. Secret key rate over Loss for different gate widths for back-to-back configuration 68

5.7. Maximum tolerable loss plotted over gate widths for back-to-back configuration . . . 69
5.8. Transmission depending on gate width for three different values of loss . . . 70
5.9. Optimal gate width and maximum secret key rate depending on transmission loss (back-to-back). . . . 71

6.1. Sketch of the tracking antennas . . . 75
6.2. Filtering design Alice . . . 76
6.3. Filtering design Bob . . . 77
6.4. Noise count influences by the beacon signal . . . 78
6.5. Background photons measurement . . . 79
6.6. Free-space testbed . . . 81
6.7. Back-to-back QKD transmission over time . . . 83
6.8. QKD over 388 m free-space link . . . 84
6.9. QKD over 388 m free-space link with misalignment after switching off tracking . . . 86
6.10. QKD over 388 m free-space link without observable misalignment after switching off tracking . . . 87
6.11. QKD transmission over the 388 m free-space link for two sets of parameters . . . 88
6.12. Free-space transmissions for all set parameters and plotted over gate width . . . 89
6.13. Back-to-back: Sifted key rate, QBER and secret key rate over loss for one set of pulse parameters . . . 90
6.14. Modification of Figure 6.13 with free-space QKD transmission added 91

A.1. Bob's setup for $M = 4$ . . . 99
A.2. Steering patterns for $M = 4$ . . . 99
A.3. Needed filtering plotted over the transmission loss. . . . 101
A.4. Angle of transmission through windows . . . 102

List of Tables

5.1. Measured pulse widths depending on set pulse width 58
5.2. Pulse parameters for back-to-back transmission 63

6.1. Relevant losses occurring during transmission 74
6.2. Pulse parameters for free-space transmission 82

Danksagung

Für die Betreuung meiner Dissertation möchte ich mich zunächst Prof. Dr. rer. nat. Oliver Benson Dr.-Ing. Nicolas Perlot und Prof. Dr.-Ing. Ronald Freund bedanken, die das Arbeiten an meiner Promotion erst möglich gemacht haben. Die Anleitung und vielen fruchtbaren fachlichen Diskussionen haben mir in den letzten Jahren sehr geholfen und haben wesentlich zu den Ergebnissen, die ich in der vorliegenden Arbeit vorstelle, beigetragen.

Außerdem möchte ich mich bei den vielen Kollegen und Mitstreitern, sowohl am Fraunhofer HHI als auch in der Nanooptik AG an der Humboldt Universität zu Berlin bedanken, die dazu beigetragen haben eine angenehme, kooperative und produktive Arbeitsatmosphäre zu schaffen. Besonders zu erwähnen sind hier Dominic Schulz, Christian Schmidt, Tim Kroh, Chris Müller, Roberto Mottola und Fabian Beutel.

Natürlich möchte ich mich auch bei meiner Frau Johanna Rödiger für ihren Einsatz, ihr Verständnis, ihre Geduld und ihre Unterstützung bedanken. Besonderer Dank gilt auch meinen Eltern, nicht nur für die moralische Unterstützung bei der Promotion, sondern auch schon in den Jahren davor und dafür, dass sie immer an mich geglaubt haben.

Zuletzt geht mein Dank noch an alle Freunde und Verwandte und an all die Menschen, die ich nicht genannt habe, die aber in kleinen oder großen Teilen direkt oder indirekt Anteil an dem Erfolg der vorliegenden Arbeit haben.