



MASTERARBEIT | MASTER'S THESIS

Titel | Title

Fast laser carving for a three-state BB84 protocol
implementation with time-bin encoding and decoy states

verfasst von | submitted by

Pascal Léon Thiele B.Sc. MSc

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of
Master of Science (MSc)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree
programme code as it appears on the
student record sheet:

UA 066 876

Studienrichtung lt. Studienblatt | Degree
programme as it appears on the student
record sheet:

Masterstudium Physics

Betreut von | Supervisor:

Univ.-Prof. Dipl.-Ing. Dr. Philip Walther

Acknowledgements

Many thanks to Prof. Philip Walther, my academic supervisor, for the support and freedom I received in performing and writing this thesis. Many thanks to Dr. Hannes Hübel for the opportunity to develop a quantum key distribution prototype in the optics lab of the Austrian Institute of Technology (AIT), for his pragmatic, although rigorous, guidance and heartwarming laughs. A big thanks to all of my AIT colleagues, in particular to Dr. Marie-Christine Slater and Florian Prawits, for the theoretical discussions and for helping with a lot of software and hardware debugging, from which I learned a lot. Thank you all for creating a nice work environment and for the dragon boat races.

As with my first master's thesis, I relied on the support of those around me in performing and completing this thesis, especially Chloé and my family – thank you.

This work received funding by the project *Development of an encryption system based on quantum key distribution* (project number 881112) of the program *Quantum research and technologies* from 2019 supported by the Austrian Research Promotion Agency (FFG).

Abstract

Quantum Key Distribution (QKD) can provide random and secure keys for information-theoretically secure cryptographic protocols, thereby ensuring the privacy of both current and future communications. This master's thesis presents the implementation of a simplified three-state BB84 protocol with time-bin encoding and the one-decoy method, whose security against collective attacks was proven by Rusca et al. in 2018. The optical transmitter setup consists of a continuous wave laser with a wavelength at 1550 nm, modulated by a phase randomizer and a primary intensity modulator used for fast laser carving. This intensity modulator generates 400 ps-wide pulses with an intra-symbol pulse separation of 1 ns in the classical optical regime. A second intensity modulator selects among three intensity levels for the Z and X basis states and their corresponding decoy state counterparts. These pulses are then attenuated to the quantum level to match the respective photon number occupancy of the states, with a targeted mean photon number of 0.1 for signal states. The receiver's side includes a beam splitter for passive basis selection, two single-photon detectors, and an unbalanced interferometer. With this setup, a quantum bit error rate (QBER) below 2 % was achieved for attenuations up to 19 dB. The quantum visibility of the setup was found to be 94 %. A QKD exchange was performed, and using a corrected estimate for the decoy mean photon number, a secret key rate of 1.7 kHz was extracted. The presented results demonstrate the successful implementation of the setup and the potential of fast laser carving in QKD experiments.

Kurzfassung

Die Quanten-Schlüsselverteilung (quantum key distribution, QKD) kann zufällige und sichere Schlüssel für informationstheoretisch sichere kryptografische Protokolle bereitstellen und so die Vertraulichkeit sowohl der aktuellen als auch zukünftiger Kommunikation gewährleisten. Diese Masterarbeit präsentiert die Implementierung eines vereinfachten Three-State BB84-Protokolls mit Time-Bin Kodierung und der One-Decoy Methode, dessen Sicherheit gegen kollektive Angriffe von Rusca et al. im Jahr 2018 bewiesen wurde. Der Aufbau des optischen Senders besteht aus einem Dauerstrichlaser mit einer zentralen Wellenlänge von 1550 nm, der von einem Phasenrandomisierer und einem primären Intensitätsmodulator moduliert wird, der für schnelles Laser Carving verwendet wird. Dieser Intensitätsmodulator erzeugt 400 ps breite Pulse mit einem Intra-Symbol-Pulsabstand von 1 ns im klassischen optischen Bereich. Ein zweiter Intensitätsmodulator wählt zwischen drei Intensitätsstufen für die Z und X Basiszustände sowie deren entsprechenden Decoy Zustände. Diese Pulse werden dann auf das Quantenlevel abgeschwächt, um die jeweilige Photonenanzahlbesetzung der Zustände zu erreichen, wobei eine mittlere Photonenanzahl von 0.1 für die Signal Zustände angestrebt wird. Die Empfängerseite umfasst einen Strahlteiler zur passiven Basisauswahl, zwei Einzelphotonendetektoren und ein verzögertes Interferometer. Mit diesem Aufbau wird eine Quantenbitfehlerrate (quantum bit error rate, QBER) unter 2 % für Dämpfung bis zu 19 dB erreicht. Die Quantenvisibilität des Aufbaus betrug 94 %. Ein QKD-Austausch wurde durchgeführt, und unter Verwendung einer korrigierten Schätzung für die Photonenanzahl der Decoy Zustände wurde eine Geheimschlüsselrate von 1.7 kHz extrahiert. Die präsentierten Ergebnisse demonstrieren den erfolgreichen Aufbau und das Potenzial von schnellem Laser Carving in QKD-Experimenten.

Contents

Acknowledgements	i
Abstract	iii
Kurzfassung	v
List of Tables	ix
List of Figures	xi
1. Introduction	1
2. Quantum Key Distribution	5
2.1. Concept of QKD - the original BB84 protocol	5
2.2. QKD Protocols and Implementations	9
2.2.1. Time-Bin Encoding of a Three-State BB84 Protocol with Decoy States	12
2.2.2. Coherent States, Annihilation and Creation Operators	14
2.2.3. Time-Bin Encoding with Weak Laser Pulses	15
2.2.4. Attacks and Security	16
2.2.5. The Photon Number Splitting Attack and the Decoy State Method	19
3. Experimental Setup	21
3.1. Proposed QKD Protocol	21
3.2. The Lab Demonstrator	24
3.3. Alice's Setup - Transmitter	27
3.4. Bob's Setup - Receiver	34
4. Quantum Key Distribution Experiment	39
4.1. Pattern and Symbol Encoding	39
4.1.1. Sampling of Patterns	41
4.1.2. Mean Photon Number Estimation	42
4.2. QKD Experiments	42
4.2.1. QBER over Attenuation	43
4.2.2. Visibility Measurement	45
4.2.3. Secret Key Discussion	47
5. Conclusion	51

Contents

Bibliography	53
A. Appendix	59
A.1. The No-Cloning Theorem	59
A.2. Algorithm - Plateau Analysis in Step Signal	60
A.3. Calculation of the SKR	60

List of Tables

3.1. Phase Modulation Values	31
3.2. Optical AM levels	33
4.1. Errors and Counts in Z and X basis	48
4.2. SKR Protocol Parameters	49

List of Figures

2.1. Concept of QKD	6
2.2. Polarization Vector in Z and X Basis	7
2.3. Illustration of BB84 Protocol	9
2.4. QKD Classification	11
2.5. Bloch Sphere	13
2.6. Eve's Attacks	17
3.1. Structure and Timing of a Symbol	22
3.2. Prepared States	23
3.3. Setup Block Diagram	26
3.4. Transfer Function of Intensity Modulator	29
3.5. Carver Signal	30
3.6. Phase Scrambler Signal	31
3.7. AM Signal	32
3.8. Amplitudes of the Modulated Laser	33
3.9. Width of Modulated Laser Pulses	34
3.10. Setup Block Diagram Bob	35
3.11. Delayed MZI	37
3.12. Setup of MZI Characterization	37
3.13. Visibility Measurement	38
4.1. Frame Stream	40
4.2. State Distribution	41
4.3. QBER over Attenuation	44
4.4. Visibility	46

1. Introduction

Information exchange has ever been fundamental to human interaction. Undeniably, without language, and later literacy, humanity would have not evolved into such complex societies (as we know them today). Hand in hand with human development, communication methods have become more diverse and complex. In parallel, with the development of communication technologies and methods, the requirement for secure transmission arose, to guarantee privacy of information, exchanged between natural or legal persons. Cryptography is the study of securing this privacy of communication between two parties. The field of cryptography is nearly as old as human civilization itself. An essential part of cryptography is the deliberate replacing of symbols with other symbols, thus morphing the text, with the earliest occurrence dating back some 4000 years to the time of the Pharaohs ^[1]. Cryptography has since then dramatically evolved, here we give a very brief discussion on cryptography, its application and the necessity for quantum key distribution which motivates this thesis.

Every good story has protagonists ^[1] in this thesis, the main protagonists are called Alice and Bob, who take the roles of the transmitter and receiver respectively. In all generality, the privacy of Alice's message is established by mapping her message m to an *a priori* nonsensical, in the most secure case a random, symbol sequence called the encrypted message e (the cryptogram). It is this (random) sequence that is then sent to Bob. This process is called encryption. Secure communication refers to a scenario in which an eavesdropper, whom we will refer to as Eve henceforth, might successfully intercept the encoded message, yet remains incapable of extracting any meaningful information from the intercepted signal.

Not every encrypted message constitutes a random symbol sequence. For instance, the well-known Caesar cipher is not random but algorithmic. Here, one uses a one-to-one mapping of every letter in the Roman alphabet to another letter. In particular, the encrypted message is only obtained by a shift in letters in this alphabet. Even though trivial, it fulfills the requirements of an *a priori* nonsensical ^[2] message and is therefore an encryption method. Such a method is for obvious reasons weak, compared to an encryption scheme that yields a completely (truly) random cryptogram. In any case, the specific encryption is entirely described by an (encryption) key, k and/or the encryption algorithm denoted by $E(m; k)$ used by Alice to encrypt her message. Based on the specific encryption protocol, the receiving party, Bob, can then decode (decrypt) the message with a corresponding (decryption) key \tilde{k} and algorithm $\tilde{E}(e; \tilde{k})$ and thus a secure communication can be established ^[3]. Alice and Bob need to agree previously on an

¹And every studying field it's traditions and customs.

²In the sense, that it is not a clear text.

³In symmetric encryption, both keys are up to transformation identical. In asymmetric encryption,

1. Introduction

encrypting and decryption protocol such that $m = \tilde{E}(E(m, k), \tilde{k})$.

With the previously exchanged random key of the same length, Alice and Bob can achieve *unconditional security* of the secret message. Unconditionally secure, also known as information theoretically secure, means that not even a computationally omnipotent entity can do more than guess the content of the secret message. Attaining this level of security necessitates the fulfillment of specific conditions. First, the encryption key needs to be at least as long as the message. Second, the key is drawn from a uniform distribution of all possible keys, where special emphasis should be given to the fact that perfect (true) randomness is required. Third, the key is used only once, i.e. it is never, not even part-wise, reused for another (encryption) purpose. Fourth, the key itself is kept secret and is only known by Alice and Bob.

The most well known example of an information theoretically secure protocol is the one-time pad (OTP) scheme. An OTP is the symmetrical encryption scheme, in which Alice employs the secret key to encrypt her message, while Bob uses the same key to decipher the message. In an OTP the message is mapped to a bit string, m . This string is XORed, denoted by \oplus , with the key k . The resulting, encrypted message e , is completely random. Bob can retrieve the original message by XORing again the cipher with the same key k . As an example, the following encryption of the binary representation of the ASCII encoded "P":

$$\begin{aligned} m &= 01010000 \\ k &= 10111001 \\ e &= m \oplus k = 11101001 \\ e \oplus k &= 01010000 = m := \text{P (ASCII)} \end{aligned}$$

In OTPs it is consequently imperative that Alice and Bob not only reach consensus on the shared key, but also maintain its secrecy under all circumstances. Furthermore, since Alice and Bob are separated by a physical distance⁴, the key needs to be previously exchanged, which poses ultimately the key distribution problem [2, 3]. How could such a key safely and efficiently be distributed?

In the information age, with the necessity to exchange large amounts of (sensitive) data rapidly, more practical schemes than OTPs are employed to circumvent this key distribution problem. These encryption schemes require necessarily some information exchange between the communicating parties, but its amount is kept to a minimum and other encryption algorithms are used. These algorithms are not necessarily unconditionally

different keys are used.

⁴Which is to say that they are not in the same room, otherwise Alice and Bob could potentially agree on an easier, but still secure, communication method.

secure, but rather rely on computational assumptions that certain (decoding) operations are computationally too costly and thus inefficient. The prime example thereof is the prime number factorization, which would be required to break the popular RSA encryption method [4, 5]. With technological advancements on the soft- and hardware side, these encryption schemes may become vulnerable to eavesdropping. One possible technological advancement is, for example, the development of a functional quantum computer⁵. Such a quantum computer would lower considerably the computational effort it takes to decrypt a message [2, 3]. With a quantum computer, Shor's algorithm can be used to factorize any non-prime integer efficiently, i.e. it takes only polynomial time, which is considerably faster than any other known (classical) factorizing algorithm [6].

Encryption methods based on "computational hardness" might consequently lose their security, and the confidentiality of previous messages can no longer be assured, as Eve could potentially have archived any intercepted messages. Currently discussed are mainly two ways out of this issue. On the one hand, one can rely on so-called post-quantum encryption, which are classical encryption algorithms, but still secure despite the menace of quantum computers. However, these encryption methods have one major drawback: they make assumptions about classical or quantum algorithms that have not yet been developed. With this in mind, post-quantum algorithms are secure only to the extent that there is no *known* way to compromise the security. On the other hand, one can use the approach of quantum key distribution (QKD). As the name suggests, QKD focuses only on the key distribution part of an encryption scheme. QKD exploits fundamental laws of (quantum) physics to ensure the generation of a secret key, which could be used, but not exclusively, for an OTP scheme, thereby ensuring unconditionally secure communication.

This thesis studies a novel experimental implementation of a particular QKD protocol, a variation of the well-known BB84 protocol [7]. While the standard BB84 protocol utilizes four states, here only three states are required, reducing the complexity of the system. Three-state BB84 implementations have already been demonstrated, notably in [8, 9, 10]. The QKD implementation discussed in this thesis of a three-state BB84 protocol is performed with time-bin encoding, a state-of-the-art encoding method, and with a standard near-infrared wavelength of 1550 nm. To account for one of the most discussed loopholes in practical QKD implementation, decoy states are used to prevent photon number splitting attacks [11]. The minimal approach of the one-decoy method is chosen to facilitate the experimental setup [11, 12].

In this time-bin encoding scheme, a continuous-wave laser is used to generate the quantum states. In contrast to [8, 9], which require an interferometer for the state preparation, we use fast laser carving for the state generation as in [10]. This should ultimately allow for a simpler and cheaper implementation of a three-state BB84 protocol. The aim of this master thesis is to perform a proof of principle that fast laser carving can be used for a time-bin encoded three-state BB84 protocol. An emphasis is also made on a comprehensive description of the laboratory setup and components, as well as the data analysis to generate the results. This laboratory demonstration aims to provide an estimate of the attainable secret key rate.

⁵Sometimes called the "Quantum Menace", and is taken very seriously by private and public actors.

1. Introduction

This thesis is structured as follows: First, in Chap. 2, general theoretical and practical concepts of QKD systems are discussed, notably the first proposed QKD protocol, the standard (four-state) BB84 protocol and the related three-state protocol. A particular focus is made on the description of the time-bin encoding and the photon number splitting attack. Second, Chap. 3 describes in detail the general experimental setup with its relevant components. This includes the hardware description and evaluation of the electrical signals used to control the relevant components. Third, Chap. 4 treats state and pattern encoding and the performed experiments, including their analysis. We detail how the mean photon number can be obtained from the experiments, and we give a first estimation of the obtainable secret key rate and the related security parameter estimation. A summary of the thesis is presented in Chap. 5, including an outlook on further improvements of the setup.

2. Quantum Key Distribution

This chapter outlines the core concept of Quantum Key Distribution (QKD), primarily based on the first proposed QKD protocol from Bennett and Brassard in 1984 [7]. Different approaches and implementations of QKD, as well as security aspects, are discussed to give a more general overview of QKD and what it has grown into. This chapter concludes with a description of a state-of-the-art QKD implementation with time-bin encoding and the decoy-state method relevant to the implementation described in this thesis.

2.1. Concept of QKD - the original BB84 protocol

The first formally proposed QKD protocol is from Bennett and Brassard in 1984 (BB84) [7]. Here, we introduce the general concepts and power of QKD illustrated by the BB84 protocol, which belongs to the family of the "prepare-and-measure protocols". All prepare-and-measure QKD protocols assume two communication channels between Alice and Bob: a classical public channel and a quantum channel. The public channel is authenticated¹ and serves as a communication link between Alice and Bob. Since it is a public channel, any information shared there is supposedly also available for Eve. The second channel is quantum, i.e. it is used to transmit quantum states. Due to the quantum nature of the states (random) quantum effects may affect the states. This channel is possibly corrupted by Eve, she can intercept, and in particular, modify any quantum signal transmitted via this channel. The general concept of QKD, in the prepare-and-measure spirit, is sketched in Fig. 2.1, with both the bidirectional classical and the unidirectional quantum channel. One should further note that QKD assumes strong walls for both Alice and Bob's laboratories, i.e. no information, besides information transmitted over the two dedicated channels, passes these walls. The interior of the respective labs is free from manipulation from the outside world.

In the original BB84 protocol, qubits, the quantum analog to a (classical) logical bit, are sent through the quantum channel. The general form of a qubit is

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (2.1)$$

with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. This condition ensures that the state is well-normalized. To be more precise, Eq. (2.1) is only the form of a *pure state*, opposed to a statistical mixture which are called mixed states. Mixed states are described by their density operator or density matrix, but since we will not further discuss mixed states in this

¹Meaning that any messages sent by Alice to Bob are guaranteed to be from Alice and uncorrupted, and vice versa.

2. Quantum Key Distribution

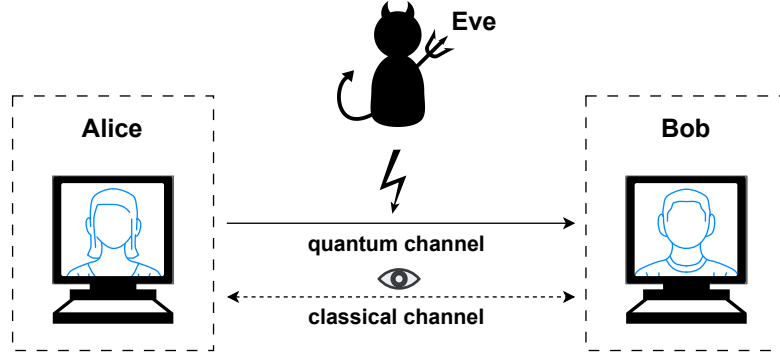


Figure 2.1.: General concept of QKD. Alice uses a quantum channel to send a key to Bob. This channel can be corrupted by an eavesdropper, Eve. After the transmission, Alice and Bob communicate over a public classical channel to estimate Eve's knowledge of the transmitted key.

thesis, we omit here their introduction. In any case, the qubit state is embedded in a two-dimensional Hilbert space² with the two orthonormal basis states $|0\rangle$ and $|1\rangle$. A qubit is therefore nothing but a two-level system in a quantum superposition between $|0\rangle$ and $|1\rangle$. This superposition is kept until measurement when the wave function ψ collapses and the qubit gets projected on one of the (measurement) basis states³. Associating the measurement outcome, and therefore the two basis states, with the classical bit values "0" and "1", one can retrieve one bit of information from the measurement process. The projection probabilities are $|\alpha|^2$ and $|\beta|^2$ for the states $|0\rangle$ and $|1\rangle$, respectively. Different physical objects or systems can be described as being a qubit, the polarization of a photon being one of them. Taking the standard vector notation $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, it becomes apparent that the polarization state lying in the physical space plane

$$|\psi\rangle = \cos \theta e^{i\phi_x} |0\rangle + \sin \theta e^{i\phi_y} |1\rangle \quad (2.2)$$

can be indeed described as a qubit. Here, $\theta \in [0, 2\pi]$ describes the polarization with respect to the x-axis (in the direction given by $|0\rangle$), $\phi_x, \phi_y \in [0, 2\pi[$ are the phase angles and i is the imaginary unit. In the case of linearly polarized photons, the phase angles are equal, setting them arbitrarily to zero one obtains

$$|\psi\rangle = \cos \theta |0\rangle + \sin \theta |1\rangle, \quad (2.3)$$

which is a specific case of Eq. (2.1). A polarization state is visualized in Fig. 2.2

Passing the photon through a horizontal-vertical polarization filter or splitter corresponds to a projection measurement on their basis states. This measurement basis is commonly called the Z basis. Here, the probability *amplitudes* $\cos \theta$ and $\sin \theta$ define the

²A Hilbert space is a real or complex vector space endowed with an inner product which is also complete w.r.t. the induced norm.

³In the described context, the measurement can be performed by a suitable projection operator.

2.1. Concept of QKD - the original BB84 protocol

probabilities $\cos^2 \theta$ that the photon is horizontally polarized and $\sin^2 \theta$ vertically polarized after measurement (after filters). Immediately after the measurement, the polarization is unambiguously aligned to one of these orthogonal directions⁴.

Instead of using the Z basis, the same polarization state can also be measured and described in the orthonormal X basis. This X basis is achieved by rotating the Z basis by 45° in physical space in the counterclockwise direction, earning it the alternate name of "diagonal basis". The X basis is spanned by $\{|+\rangle, |-\rangle\}$, with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. A visual representation of an arbitrary linear polarization vector $|\psi\rangle$ with angle θ in the Z basis and the same polarization state in the X basis is shown in Fig. 2.2.

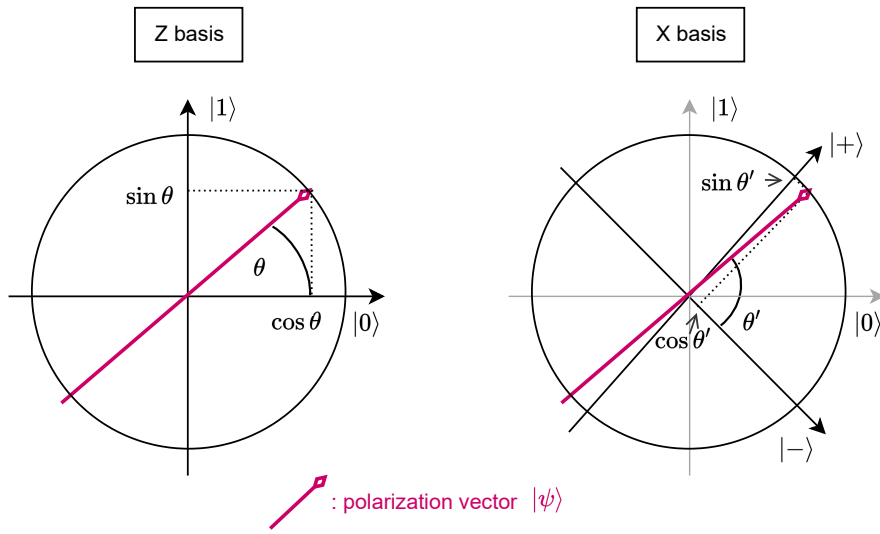


Figure 2.2.: Polarization vector with angle θ in the Z basis and angle $\theta' = \theta + 45^\circ$ in the X basis. The projection on the two respective basis vectors yields the probability amplitude. With an angle of $\theta \approx 45^\circ$, the projection probability on the horizontal/vertical axis is almost completely random ($\cos^2 \theta \approx \sin^2 \theta \approx \frac{1}{2}$), while a projection onto the diagonal axis described by $|+\rangle$ is almost certain ($\sin^2 \theta' \approx 1$).

These two bases are said to be mutually unbiased bases (MUBs) of the underlying Hilbert space. Particular about a MUB is that every basis vector of one basis has equal projection probability to all other basis vectors of another MUB [7, 13]. This implies that no information can be retrieved from a state that has components exclusively along one basis vector of a MUB, if it is measured in the another MUB. We will readdress the qubit representation and measurements with MUBs in Sec. 2.2.1.

⁴Such a photon, traveling through space without interaction with any other particles and fields, should maintain this polarization state until the end of time.

2. Quantum Key Distribution

Besides the uncertainty of the measurement outcome coming with the measurement in MUBs, another principle ensures the security of QKD protocols: the no-cloning theorem. This theorem states that it is impossible to copy an arbitrary unknown quantum state. A proof of the non-cloning theorem can be found in App. A.1. This is utterly important because, in its absence, Eve could copy any intercepted qubit, and extract information from the duplicate without altering the original state. This scenario would corrupt the protocol's integrity since no eavesdropping could ever be detected. Exploiting these properties is at the heart of the BB84 protocol.

The BB84 protocol is illustrated in Fig. 2.3 and goes as follows: Alice generates a random bit string. For each bit she uses randomly her basis, Z or X basis, to encode the bit value into the photons' polarization with an appropriate filter or waveplate. In the Z basis, she encodes a logical 0 (1) with $|0\rangle$ ($|1\rangle$), and in the X basis with $|+\rangle$ ($|-\rangle$). On the receiver side, the arriving photons are measured by Bob in a random basis (Z or X), independent of Alice's choice. Bob obtains binary values, given by the measurement outcomes. In half of the cases Bob will have chosen the same basis as Alice, in these cases the encoded bit value corresponds necessarily to the measured bit value if noiseless transmission is assumed. If Bob measures however in the complementary basis, he obtains randomly a logical 0 or 1. After the transmission of all qubits, Alice and Bob compare their bases over the public channel, disregarding all instances with different basis choices, yielding a shared key for their encryption protocol, this is the raw key. This process of basis reconciliation is referred to as "sifting", which is illustrated in Fig. 2.3. We introduce now Eve into this scenario, who is confronted with the same issue as Bob.

If Eve measures in the complementary basis (X) as $|\psi\rangle$ was prepared in (Z) and resends⁵ a photon in her basis with polarization corresponding to her measurement outcome, two cases need to be considered. The interesting case is when Bob measures in the original basis (Z) used by Alice during the state preparation. In this case, Bob obtains random outputs, which leads to disagreements in the bit values upon comparison of a sufficiently large bit string, which should have been identical due to the agreement on the basis choices. This test for eavesdropping by comparing a (random) subset of the sifted bit stream is crucial. On average, Alice and Bob should disagree in $\frac{1}{4}$ of the cases on the bit value, even though they had used the same basis⁶. However, this is only approximately true when finite key sizes are transmitted and statistical effects are accounted for.

Since the comparison of bit values to detect eavesdropping is public, the subset used there is lost for the secret key generation. The size of this subset has to be chosen in such a way that almost certainly eavesdropping can be excluded. If Alice and Bob agree on all bit values in the subset, they can exclude the (meaningful) presence of Eve. In a noiseless scenario with perfect measurement devices, any disagreement on the measurement outcome would immediately reveal the presence of Eve. In a realistic scenario, some bit values get flipped (bit flip) or are lost altogether during the transmission. The quantum

⁵In some way or another, Eve needs to resend a photon. This is because, if she does not, no key can be established, and therefore no secret can be revealed.

⁶The $\frac{1}{4}$ because in half of the cases, the opposite basis is chosen by Eve and in half of the cases Bob measures then a bit value opposite to what Alice initially sends.

2.2. QKD Protocols and Implementations

bit error rate (QBER) estimates the amount of disagreement between Alice's and Bob's bit streams. The QBER can be due to either too much noise or to the presence of Eve. In any case, the protocol is aborted if the QBER is estimated to be too high.

For secure key generation purposes, the raw key is subject to error correction and privacy amplification, after which the users yield the secure key, which is used to encrypt the secret message. Supplementary authentication steps are performed as well to ensure that Alice and Bob operate on correlated bit strings [14]. The secrecy rate of a given transmission is often quantified by the secret key rate (SKR). The processing steps of error correction and privacy amplification are all part of classical post-processing and are not quantum anymore. Unless a security proof is specifically formulated for a particular QKD protocol, the assurance of unconditional security cannot be guaranteed in principle. Theorists put a lot of effort in proving the security for various QKD protocols. Unconditional security for the BB84 QKD protocol, even in realistic scenarios, can be proven [15], meaning that as long as Eve's abilities are restricted by the laws of nature, the key is secure and therefore the encrypted message too. Section 2.2.4 elaborates more on the security aspects of QKD.

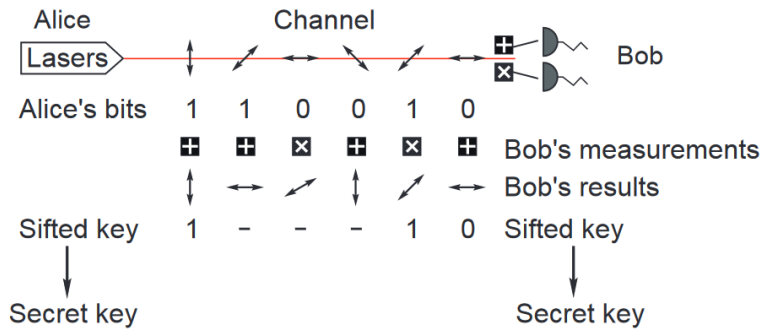


Figure 2.3.: Illustration of BB84 protocol. Alice sends logical bits, encoded in the photon's polarization, in either the vertical (Z) or the diagonal (X) basis. Bob measures in one of the two bases. In the absence of Eve, Alice and Bob necessarily agree on Bob's measurement outcomes if they keep only those qubits with identical preparation and measurement basis. Figure from [2].

2.2. QKD Protocols and Implementations

The original BB84 protocol suggested the polarization of photons to encode information. Nothing prevents the use of any other degree of freedom of a photon. Theoretically, Alice can also use any other quantum mechanically describable object, like electrons or ions, in a QKD implementation, and is additionally not even restricted to a qubit systems [16]. However, the choice of light (photons) has practical reasons. Light is suitable to transmit information over long (macroscopic) distances, which are always considered (or at least targeted) in QKD protocols, since otherwise, the whole encryption necessity would become somewhat obsolete. For these reasons, it is implicitly assumed,

2. Quantum Key Distribution

while discussing QKD protocols, that electromagnetic radiation/photons are used. The light's propagation medium is either fiber or air/vacuum (free space propagation). Even though QKD protocols in free space have been successfully implemented [17], the fiber variant seems to be the natural choice to assure maximum flexibility over the transmission line, especially allowing for QKD transmissions during daytime. Besides polarization, one could use the light's spectral properties to encode qubits in the photon's frequency [18, 19]. Another encoding scheme is phase/time-bin encoding, which has been successfully implemented in QKD protocols [8, 9, 10]. The mathematical description of a time-bin encoding of a BB84 protocol will be discussed in more detail at the end of this chapter.

Independently of the concrete encoding scheme, e.g. polarization, time-bin encoding, the protocols are usually implemented with highly attenuated laser pulses (coherent states) instead of single photon sources, as they are more costly and more difficult to control. The involved quantum states need to be described accordingly. The state description is left for Sec. 2.2.2, whereas its security loophole and the appropriate countermeasure are discussed in Sec. 2.2.5.

The examples of polarization or time-bin encoding are standard discrete variable QKD (DV-QKD) implementations. Complementary to DV-QKD, there exists the continuous variable pendant called CV-QKD. Besides the distinction between DV- and CV-QKD, one can argue for another broad categorization of QKD systems: there can also be the distinction between prepare-and-measure-based and entanglement-based schemes. A visual overview of a possible QKD classification is shown in Fig. 2.4.

The described BB84 protocol in Sec. 2.1 belongs to the prepare-and-measure DV-QKD category. Another prominent protocol of this category is the distributed-phase-reference (DPR) protocols [20] which uses a mixture of time and phase encoding of laser pulses. One example is the coherent one-way (COW) protocol. In the COW protocol, weak laser pulses are prepared in a time-bin train and transmitted to Bob. The coherence of the laser pulses between adjacent time bins is monitored to detect potential attacks from Eve [21, 22]. An advantage of COW over other QKD protocols is its relatively easier experimental setup, both on Alice's as well as on Bob's side of the transmission line.

Entanglement-based DV-QKD is based on the fact that observing or intercepting one quantum particle disturbs also its entangled pendant⁷. The first entanglement-based QKD protocol is the E91 protocol [23] proposed by A. Ekert in 1991 in which a photon source sends entangled photon pairs to Alice and Bob. Bob uses three different bases for his measurement and tests for violations of Bell's inequality to ensure the generation of a secret key. The BBM92 protocol is as well as E91 entanglement-based, but does not require the Bell test for its security [24] and utilizes only two measurement bases [2]. In fact, the apparent analogy to the BB84 protocol was already pointed out in the original paper [24], and paved the way to the interchangeability of preparation and measure-based schemes with entanglement ones, which is often exploited in the security proofs [2]. Although entanglement can be hard to realize experimentally, it has one considerable advantage, over the measurement-and-prepare scheme, namely making no assumption of the trustworthiness of the entanglement source. This makes entanglement-based QKD

⁷Welch "spukhafte Fernwirkung"! - nach Albert Einstein

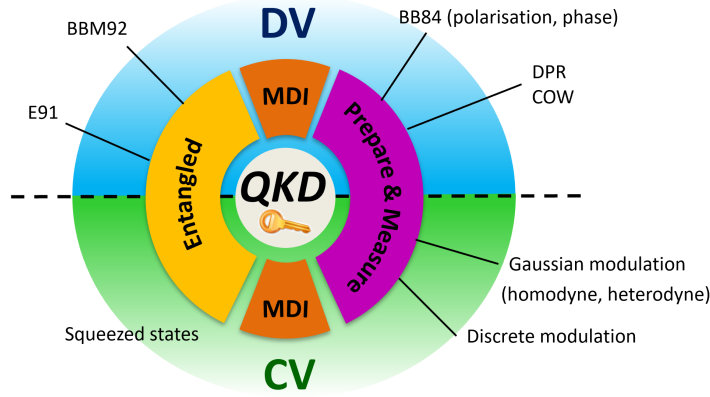


Figure 2.4.: QKD classification overview with example protocol types. DV-QKD can be seen as the opposite of CV-QKD and form a broad and general categorization of QKD. Prepare-and-measure QKD and entanglement-based QKD form together with MDI QKD another classification category. BB84-type protocols belong to the DV prepare-and-measure category, while QKD implementations relying on squeezed states belong to the family of CV entanglement-based QKD. It's important to note that this chart is by no means exhaustive, or claims ultimate accuracy, as other (sub)categories could also be defined.

potentially a good candidate for a satellite-based QKD network - with the orbiting satellite being the entanglement source. Such satellite-based QKD schemes have already been implemented, allowing a key change between two parties, separated by over 1200 km [25].

Besides entanglement and prepare-and-measure protocols, it is worth mentioning the measurement-device-independent (MDI) scheme. In this scheme, Alice and Bob are both preparing states and send them to a relay station, let's call this third, and untrusted, party Charlie. Charlie might be an alias for Eve, who is still present and might corrupt Charlie's measurements/announcements or the quantum link to Charlie. The power of MDI relies on the fact that no assumptions on any measurement devices are made, and therefore all attacks, side-channel attacks, targeting the trustfulness of these devices can be ruled out [26, 27, 2, 13]. Having introduced other schemes, it becomes clear now that the general QKD concept sketched in Fig. 2.1 sketches only the prepare-and-measure category, in which Alice prepares quantum states, and Bob measures them.

The above described schemes were all based on a discrete encoding of the quantum state. Discrete-variable and continuous-variable QKD are well recognized as being two fundamentally different approaches to QKD. The main reason for this comes from the fact that the DV-QKD security proofs consider states in finite-dimensional Hilbert space, while CV-QKD deals with states that live in an infinite-dimensional Hilbert space. The detection schemes of DV and CV-QKD are also very different.

In contrast to that, CV-QKD implementations are motivated mainly by two factors. First, CV-QKD schemes are more cost-efficient, since they do not require single-photon

2. Quantum Key Distribution

detectors, or even single photon generating sources [28]. Second, CV-QKD can theoretically achieve higher bit rates than DV-QKD [2]. The first CV-QKD protocols encoded information into the uncertainty of the light quadratures [29, 30]. Nowadays, the symbols are directly encoded into the light's quadrature via an appropriate modulation scheme of the amplitude and phase of coherent states. These schemes are usually based on Gaussian or discrete modulation constellations. Bob performs a coherent measurement either with homodyne or heterodyne detection to demodulate the encoded information. The heterodyne detection allows measuring both quadratures simultaneously at the cost of a 3 dB lower signal intensity [31]. The homodyne and heterodyne measurements needed in this setup are considerably easier and cheaper to implement than the measurements in DV-QKD (where the aforementioned single photon detectors are required) [2]. However, besides a shorter effective transmission distance, the major downside of CV-QKD is the lack of well-developed security proofs in the finite key size limit, which are for the time being more advanced for DV-QKD [13, 31]. The different levels of security of QKD systems are discussed in Sec. 2.2.4. It is expected that DV and CV-QKD will play a non-mutual exclusive role in the future, where CV-QKD is used in roles fitting its profile, e.g. as QKD link in metropolitan area networks, and DV-QKD in situations of long-distance and high-fidelity transmissions, e.g. inter- and intra-nation wide distant communication.

With different categories and implementation schemes in mind, the rest of this thesis treats DV prepare-and-measure QKD implementation. Before going into some security aspect of QKD systems, we specify the implemented BB84 protocol in more detail.

2.2.1. Time-Bin Encoding of a Three-State BB84 Protocol with Decoy States

Recall a general qubit state $|\psi\rangle$, with an equivalent formulation⁸ of Eq. (2.1)

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle, \quad (2.4)$$

with $\theta, \phi \in \mathbb{R}$ and $|0\rangle$ and $|1\rangle$, being the spanning states of bi-dimensional Hilbert space. The parameter θ tunes the probability amplitudes of the basis states, while conserving normalization of the state, and ϕ indicates the relative phase difference⁹. If one restricts that $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi[$, then it becomes more clear that Eq. (2.4) can be viewed as a representation of a sphere, the famous Bloch sphere cf. Fig. 2.5, with the basis states being at the two poles. Any pure quantum two-level system can be represented by a unique point on this sphere. A statistical mixture of such quantum states is called a mixed state, such a mixed state is described by a point in the interior of the sphere. The maximally mixed state, yielding the highest entropy, is the origin point of this sphere. If one considers the case of $\theta = 0, \pi$ and $\phi = 0$, one obtains back the basis states of the Z basis.

⁸Remember the trigonometric identity: $\cos^2 x + \sin^2 x = 1, \forall x \in \mathbb{R}$

⁹The global phase of the qubit is not an observable and can therefore be omitted without loss of generality.

2.2. QKD Protocols and Implementations

$$\begin{aligned}\theta = 0 : & \quad |\psi_{0Z}\rangle := |0\rangle \\ \theta = \pi : & \quad |\psi_{1Z}\rangle := |1\rangle\end{aligned}\tag{2.5}$$

Choosing the vector notation $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ of the Hilbert space, the states in Eq. (2.5) are easily recognized as being the eigenstates of the Z Pauli operator

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\tag{2.6}$$

For this reason, we call the basis formed by the eigenstates of Eq. (2.5) the Z basis.

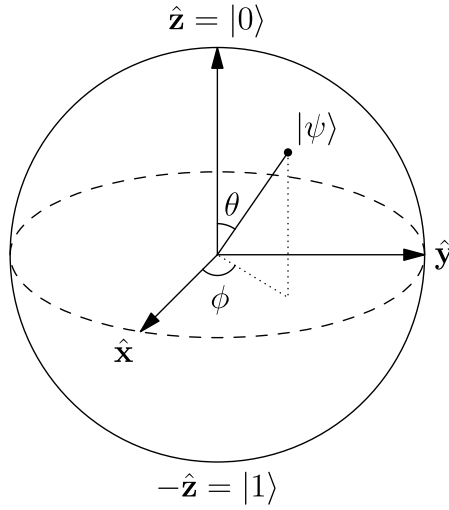


Figure 2.5.: The Bloch sphere is a visual representation of any two-dimensional Hilbert space. The two poles of the sphere represent the two basis states $|0\rangle, |1\rangle$; in our case associated either with bit value 0 or 1. All states living on the surface of the sphere are pure states. The interior of the sphere represents mixed states, with the origin of the sphere being the most entropic state. Figure from [32].

A state being with equal probabilities in $|0\rangle$ and $|1\rangle$ is described by the case $\theta = \pi/2$, in this case the qubit becomes

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\phi} |1\rangle \right),\tag{2.7}$$

which is nothing but a state on the equator of the Bloch sphere. Any basis on the equator would be unbiased w.r.t. the Z basis. One basis choice is the X basis formed by

$$\begin{aligned}\phi = 0 : & \quad |\psi_{0X}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ \phi = \pi : & \quad |\psi_{1X}\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)\end{aligned}\tag{2.8}$$

2. Quantum Key Distribution

which are the eigenstates of the X Pauli matrix

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2.9)$$

Another basis choice would be the Y basis, which is formed by the eigenstates of the Y Pauli matrix, which reads in the suggested notation as $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. In fact, there exist only three MUBs for any two-dimensional Hilbert space. With Z and X selected, no other basis would satisfy the requirement of maximal uncertainty which was demanded in Sec. 2.1. For our considerations, it is sufficient to consider only measurements in the Z and X basis.

Again, measuring the qubit state in the Z basis (X basis), if either $|\psi_{0Z}\rangle$ or $|\psi_{1Z}\rangle$ ($|\psi_{0X}\rangle$ or $|\psi_{1X}\rangle$) was prepared, yields the bit value 0 or 1. In the four-state BB84 protocol, both bases can be used for the key generation. A simplified version of this protocol is to restrict oneself to only three-states, yielding the three-state BB84 protocol. In a three-state BB84 protocol, the Z basis is used for the key generation and one state from the X basis for the monitoring of the QKD link. The monitoring state is called $|\psi_+\rangle$. Dropping the basis subscripts, one is left with,

$$|\psi_0\rangle, |\psi_1\rangle, |\psi_+\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle + |\psi_1\rangle). \quad (2.10)$$

For the reasons outlined in Sec. 2.2, the practical implementation of a three-state BB84 protocol (with and without time-bin encoding), and most other DV-QKD protocols, is performed with weak laser pulses. The states prepared by Alice are therefore coherent states $|\alpha\rangle$. Some notations on coherent states are reviewed before introducing the time-bin encoding.

2.2.2. Coherent States, Annihilation and Creation Operators

The quantum state generated by a laser can be described as a coherent state $|\alpha\rangle$. A coherent state can be written in the Fock basis (number basis) as

$$|\alpha\rangle = e^{-\frac{\|\alpha\|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (2.11)$$

where $\alpha \in \mathbb{C}$ and $|n\rangle$ a number state¹⁰. The number states $|n\rangle, n \in \mathbb{N}$ describe the presence of exactly n photons. The Eq. (2.11) is therefore just a superposition of all possible number states.

Number states can be generated from the vacuum state $|0\rangle$ via the bosonic creation operator \hat{a}^\dagger . Photons are bosons, i.e. integer valued spin particles. Starting from the vacuum, one has, $\hat{a}^\dagger |0\rangle = |1\rangle$. More generally, the creation operator applied on a number

¹⁰The states $|0\rangle, |1\rangle$ in the now adopted notation are not anymore the eigenstates of Z, but the number states with zero and one photon, respectively.

state gives $\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle$. The hermitian conjugate (adjoint) of the creation operator, is called the annihilation operator \hat{a} . It causes the reduction of the number state, which gives then $\hat{a} |n\rangle = \sqrt{n} |n-1\rangle$. From there, it is easy to verify that they satisfy the commutation relation:

$$[\hat{a}, \hat{a}^\dagger] = 1, \quad (2.12)$$

yielding the identity operator.

Both \hat{a} and \hat{a}^\dagger can be derived from the generalized position and momentum operators found in the Schrödinger equation of a quantum harmonic oscillator, probably the most studied and most important morphology of the famous Schrödinger equation. With the notation of the operators \hat{a} and \hat{a}^\dagger one can conveniently define the number operator $\hat{n} \equiv \hat{a}^\dagger \hat{a}$, which fulfills the eigenequation $\hat{n} |n\rangle = n |n\rangle$, i.e. an operator on number state yielding as eigenvalue the number of bosons (in our case photons). The annihilation has also the particularity that it has coherent states as eigenstates

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle, \quad (2.13)$$

this is because

$$\begin{aligned} \hat{a} |\alpha\rangle &= \hat{a} \left(e^{-\frac{\|\alpha\|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \right) = e^{-\frac{\|\alpha\|^2}{2}} \sum_{n=1}^{\infty} \frac{\alpha^n \sqrt{n}}{\sqrt{n!}} |n-1\rangle \\ &= e^{-\frac{\|\alpha\|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^{n+1} \sqrt{n+1}}{\sqrt{(n+1)!}} |n\rangle = e^{-\frac{\|\alpha\|^2}{2}} \sum_{n=0}^{\infty} \alpha \frac{\alpha^n}{\sqrt{n!}} |n\rangle \\ &= \alpha |\alpha\rangle, \end{aligned}$$

exploiting linearity and using that $\hat{a} |0\rangle = 0$.

As we defined coherent states in Eq. (2.11), they are normalized states, but, not orthogonal because the inner product, $\langle \beta | \alpha \rangle = e^{\alpha \beta^* - \frac{1}{2}(|\alpha|^2 + |\beta|^2)} \neq \delta(\alpha - \beta)$ for $\forall \alpha, \beta \in \mathbb{C}$. Coherent states have the property that they minimize Heisenberg's uncertainty relation¹¹

$$\Delta \hat{q} \Delta \hat{p} = \frac{\hbar}{2}, \quad (2.14)$$

but unlike squeezed coherent states, they also satisfy additionally $\Delta \hat{q} = \Delta \hat{p}$. Here, \hat{q} and \hat{p} are the phase-space coordinate operators. and Δp and Δq the associated standard deviations of the observables.

2.2.3. Time-Bin Encoding with Weak Laser Pulses

Time-bin encoding is a state-of-the-art encoding technique for QKD protocols. The main reason for this is that the coherence of states is maintained over long distances since one does not have to deal with polarization drifting, which is a common problem in optical fiber transmissions. In time-bin encoding, the state $|\psi_0\rangle$ is associated to the

¹¹die Heisenbergsche Unschärferelation

2. Quantum Key Distribution

early temporal mode denoted by (E) and the state $|\psi_1\rangle$ the later temporal mode (L). Mathematically, this is described by

$$\begin{aligned} |\psi_0\rangle &= |\alpha\rangle_E |0\rangle_L \\ |\psi_1\rangle &= |0\rangle_E |\alpha\rangle_L \end{aligned} \quad , \quad (2.15)$$

with $|\alpha\rangle$ a coherent state with mean photon number $\mu = |\alpha|^2$. The mean photon number is calculated from the expectation value of the number operator \hat{n} ,

$$\mu = \langle \hat{n} \rangle_\alpha = \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = |\alpha|^2, \quad (2.16)$$

simply by exploiting the eigenequation Eq. (2.11).

The coherent superposition, in the early and late time bin, of the monitoring state,

$$|\psi_+\rangle = \frac{1}{\sqrt{2}} (|\psi_0\rangle + |\psi_1\rangle) = |\alpha'\rangle_E |\alpha'\rangle_L, \quad (2.17)$$

has the fixed phase relation of $\phi = 0$. Here, both time slots yield the same photon occupation expectancy of

$$\mu' = |\alpha'|^2 = \frac{|\alpha|^2}{2} = \frac{\mu}{2}. \quad (2.18)$$

The monitoring state is usually generated via an interferometer and phase control, as in [8] with an unbalanced Michelson interferometer. Since the phase control between the early and late time bins is crucial, time-bin encoded protocols are sometimes referred to as time-bin phase encoding protocols. The specific implementation of the time-bin encoded qubits and their detection scheme is presented in Chap 3. Before doing so, however, we will dwell a bit into attack strategies and the security aspect of QKD.

2.2.4. Attacks and Security

So far, as in the case of the description of the BB84 protocol in Sec. 2.1, Eve's attack was described as intercepting and resending a single quantum state; this is an example of an opaque individual attack. Opaque attacks, also called intercept and resend attacks, destroy Alice's signal by measuring it. The original state is completely obscure to Bob since Eve masquerades Alice's states with her own. Another possible attacking strategy is composed of ancilla states which interact via a unitary transformation with Alice states, without destroying them. After the interaction, Alice's states are still forwarded to Bob. These attacks are called translucent attacks. Two of such attack types are described in [33], with one being an example of an entanglement-based attack.

Categories of Attacks

One can also categorize attacking strategies by the tools at Eve's use. These attacks are, in increasing power¹², individual, collective, and coherent attacks. These different

¹²Meaning Eve is more powerful, she has more possibilities to corrupt the secrecy of the key exchange.

strategies are sketched in Fig. 2.6. In all of these cases, Eve prepares ancilla states which interact via a unitary transformation with Alice states. In the case of individual attacks, Eve's ancillas are individually prepared and interact one at a time with the signal state. After the interaction, the ancilla state is immediately and individually measured. In the case of collective attacks, the ancilla state preparation happens as well individually, but Eve has access to a quantum memory¹³, giving her further possibilities [14]. In particular, Eve can wait until the post-processing, communicated over the public channel, is done, which could hint here towards the best possible individual measurement of all her ancilla states. The most general, and strongest form of attack are coherent attacks. In a coherent attack, Eve possesses not only a quantum memory, but her ancilla states are collectively prepared and are collectively measured.

In the best-case scenario, one can propose for a given QKD implementation a security proof valid for coherent attacks. Such security proof would assure, with the given constraints of the hard-wall assumption, the incorruptibility of Alice and Bob's secret key generation, because Eve's presence can be with certainty excluded. Security proofs can also be formulated in a weaker form, e.g. the protocol holds only for collective attacks, this gives at least the theoretical possibility of a security loophole.

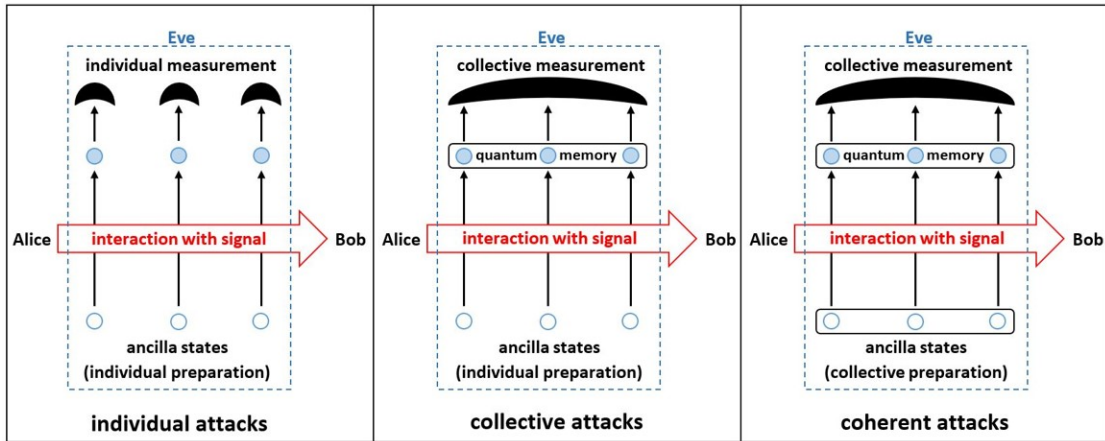


Figure 2.6.: Eve's attacks, categorized from left to right in increasing power. The security proof we utilize in this thesis to estimate a secret key models collective attacks. Although not information-theoretically secure, it provides Eve with ample possibility to corrupt the protocol as she can collectively measure all her individual prepared ancilla states after the transmission from Alice to Bob was completed. Figure from [31], many thanks to Florian Kanitscher.

Since coherent attacks are strong, and the security analysis for such states turns out to be rather complicated, not every security proof considers the same level of attack.

¹³A quantum memory is able to store quantum states, in particular, these states do not collapse or decohere over time. As of today, no practical quantum memory exists.

2. Quantum Key Distribution

Side Channel Attacks

In addition to this classification of attack types, one can exploit the (physical) implementation of the QKD system. These attacks are gathered under the name side channel attacks. Some attacks can be countered, others need to be accounted for, but they are always implementation-dependent. For instance, the photon number splitting attack, discussed in more detail in Sec. 2.2.5, does not need to be considered for obvious reasons if Alice possesses a single photon-generating source. CV-QKD does also elegantly circumvent this attack [28]. Some attacks do not even require any interaction with the transmitted state, but target the measurement devices, e.g. the single photon detector, by blinding them [34]. Various other hacking methods exist; some are more general, and others are implementation-dependent, an overview can be found in [35]. Different attack strategies need to be considered to ensure the security of the protocol. And every QKD protocol needs its own security proof. These security proofs need to consider any flaws and imperfections of the measurement apparatus and the transmission line itself. These effects need to be modeled appropriately to guarantee the security of an experimental QKD implementation. In realistic physical implementations, finite-size effects and related statistical fluctuations need to be considered as well.

Composability

Generally speaking, one demands two essential properties of the transmitted key. First, the key needs to be identical to Alice's key, otherwise, no shared encryption can be generated. Second, the key needs to be kept secret. It is allowed, to some ϵ extent, that these conditions are slightly relaxed, one speaks then of an ϵ -secure key, where ϵ is composed of a deviation in the correctness and privacy of the key. Evaluating the ϵ -security of a transmitted key, based on parameters obtained from the experiment, is at the heart of the security proofs¹⁴. Another requirement for security is composability. Composability means that the composition of different realizations, protocols, and algorithms is necessarily secure, if each component of this composition is secure itself [36]. This allows one to combine different realizations with cryptographic protocols without the necessity to prove the security of the combined setup.

Security Proofs

Lo and Chau proved in [37] the security of an entanglement-based QKD system. The proof is based on entanglement distillation, i.e. extraction of only truly entangled states, and perform then the security analysis. Through this work, the security of the BB84 protocol was shown in [38, 39]. Important quantities for the security bound are the *quantum bit error rate*¹⁵ (QBER) Q and the *phase error rate* induced by a bit-flip and

¹⁴Note that, if the channel is found to be insecure, the protocol is aborted, implying that the secrecy of Alice's message is guaranteed, because it is never transmitted.

¹⁵Formerly the QBER is not a rate: it is the ratio of bit errors over the key length, cf. Eq. (4.4). Thus, the phrasing *quantum bit error ratio*, would be more appropriate, but the formulation quantum bit error rate is the norm.

phase-flip. Based on these previous works, the famous GLLP security proof [15] for the BB84 protocol was proposed. A secret key was derived in the asymptotic regime for a realistic (experimental) QKD implementation. This security analysis extends to basis-dependent attacks and various model sources and detectors.

The security proof of a three-state BB84 protocol was proposed in [40]. The security proof invoked finite-key size effects as well as the use of decoy states to prevent the photon number splitting attack, cf. Sec. 2.2.5 [41]. Even though only collective attacks are modeled, i.e. not the most general form of Eve's attacking strategy, the authors claim that the presented work might still be sufficient to prove enough security, if further progress is made in the detection scheme security. An upper bound of the achievable key rate is provided. One derives from measurable quantities parameters, which bound the secret key length. An important part of the proof is that phase error in the Z basis is not obtained directly, but rather derived from the error rate in the monitoring line, i.e. the X basis in this case, cf. Sec. 2.2.1. The measured quantities and their discussion and influence on the SKR is dealt within Sec. 4.2.3.

The relevant security proof [40] assumed phase randomized coherent states, this is because [42] showed that phase randomization is required to maintain incorruptibility. There, a continuous phase randomization of $\phi \in [0, 2\pi[$ was assumed. However, [43] showed, that a relatively small number (10) of discrete but uniformly distributed phase angles suffice to cover this security loop-hole. Discrete phase randomization is also implemented in the thereafter presented experimental setup.

One prominent attack strategy was not yet discussed, namely the photon number splitting attack. This attack strategy, and remedy to it, will be discussed in the following.

2.2.5. The Photon Number Splitting Attack and the Decoy State Method

It was already pointed out in the beginning of this section that QKD implementations usually rely on coherent states instead of single photons. Lasers are coherent light sources, which can be used to generate short laser pulses. The number of emitted photons per pulse can be described by Poissonian statistics. The Poisson distribution is

$$\text{Pois}(n; \mu) = \frac{\mu^n e^{-\mu}}{n!}, \quad (2.19)$$

with $\mu \in \mathbb{R}^+$ describing the expectation value of the distribution. The laser pulse is a, no- ($n = 0$), one- ($n = 1$), or a multi-photon pulse ($n > 1$). These multi-photon pulses can be exploited by Eve using the photon number splitting (PNS) attack¹⁶ [11, 12]. In the terminology used in [33], we could call this a transparent attack. It is transparent from Eve and Bob's point of view, since Eve gets full knowledge of Alice's state, e.g. the polarization, if she separates one photon from the multi-photon signal and forwards the rest to Bob. Bob cannot use this signal alone to determine if Eve used the PNS

¹⁶In older literature referred to as beam splitter attack

2. Quantum Key Distribution

attack because the rest of the signal is not altered in any way. Eve exploits in PNS attack the accessible noise, in contrast to the intrinsic noise¹⁷, of the quantum channel. In this attacking strategy, Eve blocks all or a fraction of single photon signals, these states are then registered by Bob as vacuum states. This fraction of blocked photons is optimized for the underlying mean photon number and transmission efficiency, such that Bob obtains his expected vacuum count. To masquerade her attack, Eve mimics ideally a Poissonian distribution. She can do so by selectively destroying a certain number of photons in higher-order photon number signals. If, depending on the mean photon number and quantum efficiency, PNS attacks are possible, the protocol gets corrupted, and unconditional security can not be assured anymore [44, 12]. It was found that the use of decoy states in the protocol enables the recovery of unconditional security [11, 45, 44]. Since the proposed implementation also makes use of decoy states, we briefly outline the idea of the decoy state method. Originally, the one-decoy state method was proposed in [11], where Alice produces randomly two types of signals, the proper *signal states* and the *decoy states* with different mean photon number. Since Eve has no knowledge of whether a particular signal is a decoy or not, she needs to intercept either of them. By comparing and estimating the yield, which is to say the counting rate, of the signal and decoy states alike, they can obtain a condition of the security of their transmission. The decoy method was further improved and analyzed to improve the performance of QKD, notably by employing possibly more than one decoy state [45, 46] and by optimizing the expected photon number in the decoy states [47]. Relevant for the security discussion of this thesis are the decoy state methods as they were considered in [40, 41]. Both security analyses use the one-decoy method, where both decoy and signal states alike are used for the key generation¹⁸, implying the use of two intensity levels of the laser, i.e. two mean photon numbers. The one-decoy state protocol is also used as part of the experimental implementation described in the next chapter.

¹⁷Like detection inefficiencies

¹⁸The term decoy state is thus only of historical nature, since in the development of decoy protocols, decoy states were exclusively used to detect PNS attacks.

3. Experimental Setup

This chapter provides a detailed account of the assembly of the experimental setup and the lab demonstrator. It encompasses the description of the components and some necessary calibration/tuning procedures of the hardware. First, the state preparation of the time-bin encoded one-decoy state protocol is presented. Second, an overview of the general setup is provided, including a detailed explanation of the signal modulation and measurement process. Third and fourth, Alice's and Bob's respective components will be described. It is important to note that, as a lab demonstrator, the setup may deviate from a more mature QKD implementation, and significant differences will be highlighted throughout.

3.1. Proposed QKD Protocol

This master thesis propose a three-state BB84 protocol similar to [8, 9, 10] employing time-bin encoding and coherent states in the state preparation as they were introduced in Eq. (2.15). To prevent PNS attacks, the one-decoy method is used. Security for such a three-state BB84-like protocol with the one-decoy state method has been proven in the finite-key regime [48, 40].

An attenuated laser pulse is used to generate coherent states. A pulse in the early time bin, with an empty late time bin, is defined as logical 0, whereas an empty early time bin with a filled later time bin is considered logical 1. The monitoring states of the X basis occupy both early and late time bins. The time bin separation τ is chosen to be 1 ns and identical time bin pairs of consecutive symbols are separated by 10 ns. Since the symbol separation is considerably larger than the time bin separation, inter-symbol interferences, unlike in [8, 9], can be ruled out, it comes at the cost of a purely theoretical upper bound on the raw key rate of about 100 MHz. A detailed description of a symbol train and the symbol eigentimes is presented in Fig. 3.1. The smallest time increment, determined by the computer (FPGA, cf. Sec. 3.3) architecture and the software design, is 125 ps, which corresponds to one GTH¹ sample and is further discussed in Sec. 3.3.

As we utilize a one-decoy state method, we introduce an additional subscript s and d to distinguish between signal and decoy states in the BB84 states. It is important to note that the terms "signal" and "decoy" may lead to some confusion, as both are used for key generation. What holds significance is that these two types of states have distinct average photon numbers, i.e. intensities. The intensity of the signal state is labeled as μ_1 and the intensity of the decoy state as μ_2 , where $\mu_1 > \mu_2$. The following discussion drops the discriminating subscript when it generalizes to signal and decoy states alike. The

¹We use the acronym GTH, as it is also adopted by Xilinx, the manufacturer of the FPGA. While the exact meaning is not explicitly defined, it likely stands for Gigabit Transceiver High.

3. Experimental Setup

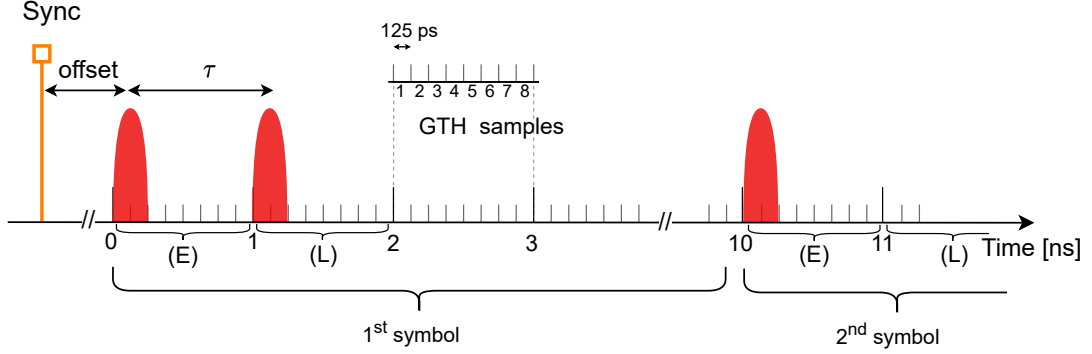


Figure 3.1.: The GTH samples are the sampling and output times of the computer (FPGA, cf. [3.3]), on which all other times are built on. One GTH sample has the duration of 125 ps, eight GTH sample form a time bin, i.e. a time bin is 1 ns long. A total of ten time bins form a single symbol. Each symbol has an early time bin (E) and a late time bin (L), separated by $\tau = 1$ ns. In this example, the first symbol consists of a double pulse (a $|\psi_+\rangle$ state) with intra-symbol pulse separation τ . The second symbol is a single pulse in the early time bin (a $|\psi_0\rangle$ state). The beginning of the symbol train, and thus of the QKD transmission, is determined by the known and constant offset (in units of GTH samples) between the synchronization signal (sync) and the first symbol. Since the sync signal can be deterministically detected, we can always find the beginning of the first and consecutive symbols.

individual pulses of the monitoring state have half the intensity of the respective signal state, as indicated in Eq. (2.18). Another intensity that needs consideration corresponds to the absence of a prepared state, i.e. the vacuum state with $\mu = 0$. The exact value of μ_1 and, μ_2 , as well as their ratio, is subject to the SKR optimization². The work presented in [8] puts an additional constraint on the intensity levels justified by a parameter analysis in [41], which states that $\mu_2 = \mu_1/2$ is almost optimal for a wide range of transmission distances. Adopting the same reasoning, the set of implemented intensities³ is

$$\left\{ \mu_1, \mu_2, \frac{\mu_2}{2} \right\}, \quad (3.1)$$

which bears the additional, and non-negligible, advantage that fewer intensities need to be generated, thereby facilitating the experimental implementation. A summary of the implemented states can be found in Fig. [3.2].

²As some other quantities, e.g. state preparation probabilities.

³As already mentioned earlier, the mean photon number μ of each pulse is the quantity of interest. In the context of this thesis, the term intensity of the pulses is used interchangeably with μ . This is because it gives a direct, more visual understanding of the pulses and because the intensity is directly proportional to the energy of the pulse, which is proportional to μ .

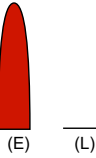
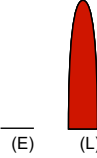
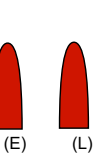
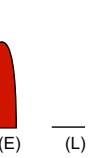
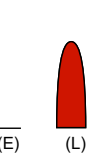
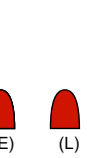
State	$ \psi_{0s}\rangle$	$ \psi_{1s}\rangle$	$ \psi_{+s}\rangle$	$ \psi_{0d}\rangle$	$ \psi_{1d}\rangle$	$ \psi_{+d}\rangle$
Basis, Bit	Z, 0	Z, 1	X	Z, 0	Z, 1	X
Intensity	μ_1	μ_1	$\frac{\mu_1}{2}$	μ_2	μ_2	$\frac{\mu_2}{2}$
Sketch						

Figure 3.2.: The states of a three-state BB84 protocol with time-bin encoding and one-decoy state. The table provides the ket notation of the states, the basis together with the carried bit value (if applicable), the intensity of an individual pulse, and a sketch of the pulses in the respective time bin. In our implementation, we have the additional constraint $\mu_2 = \mu_1/2$.

The novelty of our implementation w.r.t. the implementation proposed in [8, 9] lies in the generation of the four different intensities. The one there described approach utilizes an unbalanced Michelson interferometer on Alice's side to split a single pulse into early and later time bins, followed by an intensity modulator to create the states depicted in Fig. 3.2. Our implementation proposes a combination of two intensity modulators. One intensity modulator functions as pulse carver. The carver determines the occupied time bins, deciding whether to send a signal at all, corresponding to either $|\psi_0\rangle$ or $|\psi_1\rangle$ (both Z basis states), or to prepare a monitoring state (from the X basis). The second intensity modulator adjusts the photon number occupancy across three intensity levels for the Z and X basis states and their corresponding decoy state counterparts. The generation of the individual states is discussed in the next section.

3. Experimental Setup

3.2. The Lab Demonstrator

The experimental setup of the lab demonstrator is visualized in Fig. 3.3 and consists of the following key components:

- A continuous-wave laser
- A Field Programmable Gate Array (FPGA)
- A phase modulator (PM)
- Two intensity modulators (IM)
- Two single photon avalanche detectors (SPAD)
- A delayed Mach-Zehnder interferometer (MZI)
- A time tagging module (TTM)

which will be readdressed in the following.

The central control unit in this Alice's setup is the FPGA, overseen by her PC. The FPGA produces seven logical signals, or also called channels, which are converted with the FPGA Mezzanine Card (FMCARD), and the help of electrical amplifiers and digital to analogue converters (DACs) to four electronic signals (depicted by dotted lines in the block diagram) to modulate the specific components. We use an electrical signal for the PM (ϕ), one for the first and one for the second IM in the optical arrangement. Furthermore, FMCARD generates a synchronization pulse, denoted as *sync*, which is directly sent to Bob's TTM. This essentially encapsulates the modulation aspect of Alice's setup.

The optical line in Alice's part of the setup is the solid line originating from the laser source. The laser generates continuous wave laser (cw laser) with a center wavelength of 1550 nm and approximately 13 dBm power. The light passes first through the phase scrambler for phase randomization, cf. Sec. 2.2.4. The phase scrambler is followed by two consecutive IMs. The first IM is referred to as the *carver*, it shapes the signal by fully obstructing the laser, except in specific narrowed regions corresponding to the (if occupied) early and late time bins. The second IM, referred to as the *amplitude modulator* or AM, selects one of the possible intensities, $\mu_1, \mu_2, \mu_2/2$, and modulates the laser signal accordingly. We should point out that this nomenclature is slightly misleading, as we are not necessarily interested in the amplitude of a pulse, but in its intensity, i.e. the area of the pulse which is proportional to the energy, and thus to the mean photon number of the respective pulse. This latter quantity is a protocol parameter used in the calculation of the SKR, see A.3 and 4.2.3. The term AM first emerged from development-historic reasons and has been maintained throughout the subsequent development of the QKD system.

After passing through the AM, the signal goes through a variable optical attenuator (VOA), followed by a 99:1 beam splitter (BS). The 1% branch represents the signal line and includes an additional fixed attenuator α of 10 dB, serving as the final component in

Alice's assembly, signifying the departure of the signal from "Alice's lab", the transmitter output. The 99% branch of the BS is utilized to monitor the optical power through a Power Meter (PM). By adjusting the VOA appropriately, one can achieve the desired occupation distribution of the laser pulses. Additionally, it allows for simulating different losses corresponding to longer transmission distances. This concludes the description of Alice's experimental setup.

Bob's setup comprises a Beam Splitter (BS), a Mach-Zehnder Interferometer (MZI), two Single-Photon Avalanche Diodes (SPADs), and a Time-Tagging Module (TTM). The 90:10 BS is responsible for passive measurement basis selection, with the 90% and 10% branches associated with the Z and X basis, respectively. In the Z basis, incoming photons are detected by the SPAD, generating an electric signal subsequently recorded by the TTM. The precise mapping of the photon's time of arrival to a symbol in the symbol sequence enables the extraction of a bit sequence in the case of data states. This precise mapping of the expected time of arrival is enabled by the aforementioned sync pulse, as shown in Fig. 3.1. Since the sync pulse is classical, it can be reliably detected, allowing the beginning of the symbol train to be inferred based on a known offset.

The branch linked to the X basis includes an additional delay-line interferometer before reaching the SPAD. The MZI's delay matches the intra-symbol pulse separation of τ . We adjusted slightly the wavelength of our laser by tuning the driving current to achieve a phase shift of exactly π , causing destructive interference between coherent states in the early and late time bins. This method, compared to the thermal adjustment of the phase delay in the MZI, is faster, more precise and introduces no hysteresis effects. If a valid $|\psi_+\rangle$ state was initially prepared and arrived at Bob's setup, the state exiting the MZI should result in a no-detection event in the single photon detector if coherence is maintained. States from the Z basis should trigger detection events in the SPAD, but they are discarded later since they do not correspond to the correct measurement basis. Similarly, this SPAD is connected to the TTM.

In total, the TTM monitors three channels: one signal from the Z basis measurement, one signal from the X basis measurement, and the synchronization signal. The time tags of events in these channels are written to a file and preserved for later analysis on Bob's computer. The utilization of these files and the related processing are discussed in Sec. 4.

Two major differences to our setup compared to a high TRL⁴ QKD system should also be mentioned. First, no post-processing is performed, i.e. no error correction and no privacy amplification. The entire raw key generation is performed offline, together with the parameter estimation afterward for the security analysis. This implies the absence of a classical communication channel, between Alice and Bob, as depicted in Fig. 2.1 and in the setup description in Fig. 3.3. Even the distinction between Alice and Bob is an euphemism, as we had only one PC at our disposal being the controlling component on the transmitter and receiver side. The entire raw key is revealed and used in the calculation of the QBER. Alice plays an exclusively active role, involving state preparation, while Bob assumes a passive role by performing measurements and subsequent key processing. Second,

⁴Technology Readiness Level, DIN EN 16603-11:2020-02

3. Experimental Setup

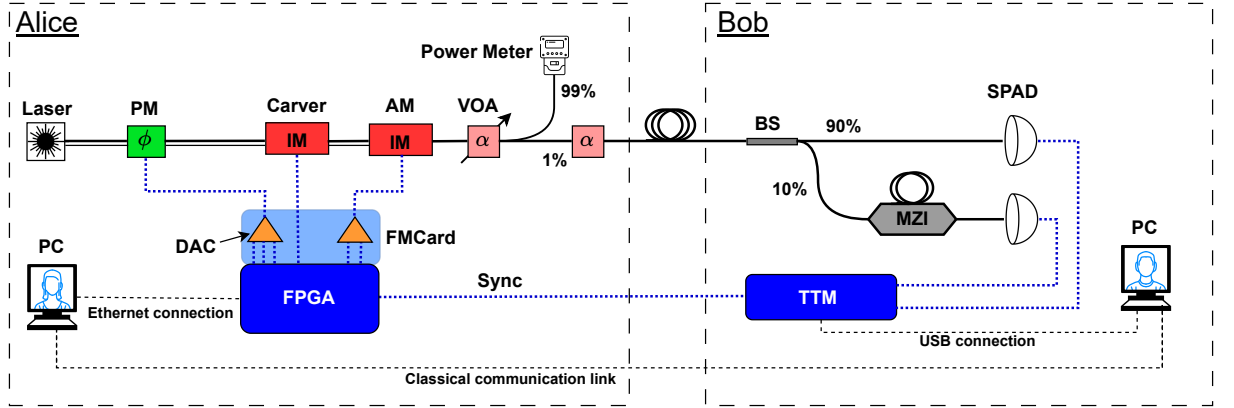


Figure 3.3.: Block diagram of the setup, with the black solid lines representing optical fibers, with double lines standing for polarization maintaining fibers, and dotted blue lines representing electrical transmission lines. Alice controls the FPGA on her side. The FPGA outputs seven logic channels which are converted (with DACs in some cases) to four analog (electrical) signals on the FMCARD (light blue area). One signal is the sync signal, used as a time reference for the measurement. The other signals control the electro-optical components to modulate the laser light in Alice's setup. Out of which, three are used for the phase randomization with the phase modulator (PM), and three are used for the generation of the six pulse forms with the two intensity modulators (IM). On Bob's side, the arrival time of the incoming photons is performed with two SPADs and a TTM corresponding to the two measurement bases, which are selected passively. One arm of the BS has an additional imbalanced MZI. This setup is the idealized version of the final experimental setup. In our experiment, Alice and Bob had the same PC, i.e. there was only one computer and therefore no classical communication channel. With this in mind, this block diagram describes the final state of the experiment detailed in Sec. 4.2.3.

the transmission is facilitated by having effectively two unidirectional communication links for the transmission: the quantum channel and the electrical classical sync channel. This extra transmission line ensures the continuous tracking of time alignment, i.e. localization of any detected photon events and the possibility to attribute them unambiguously to a specific symbol in the pattern. Unlike the classical communication link, this link is not free from Eve's manipulations, but can in the worst case only result in a denial of service. Typically, a classical synchronization signal is introduced into the quantum channel, and precautions must be taken to avoid significant interference with the quantum signal, such as through techniques like frequency multiplexing [49]. Various other methods exist to ensure time alignment; reliable external clock references provided by global navigation satellite systems (GNSS) or specific preambles encoded in the pattern can also be used.

3.3. Alice's Setup - Transmitter

This section is dedicated to a more detailed description and characterization of Alice's setup.

The optical line begins with a cw single-mode distributed feed-back laser from [Boxoptronics⁵](https://www.boxoptronics.com/) with high output power (10 mW). The laser is temperature-stabilized by a TEC (thermoelectric cooling) element. The laser's center wavelength is 1550 nm, which is a standard transmission wavelength for telecommunication technologies. Developing QKD systems for such wavelengths has the advantage of an already existing infrastructure. The linewidth of the laser is below 3 MHz. The following electro-optical components modulate the laser and are set up in the respective order: the PM, the carver, and the AM. Up to the AM, the output is not polarization-maintaining anymore. Therefore, polarization-maintaining fibers are used up to AM and regular single-mode fibers from there on.

FPGA and FMCARD

Field Programmable Gate Arrays (FPGA) are a computer type that is based on configurable logic blocks. This allows for a "quick" reprogramming in the field, i.e. in the lab, of the device. The main reason to use an FPGA lies in the fact that it allows for timewise well-controlled, and undelayed outputs of logical and phase locked signals. As time-bin QKD requires precise timing, FPGAs are a good choice for our setup. In the lab demonstrator, a 10 GHz FPGA from AMD Xilinx [\[50\]](#) has been selected. Hardware description languages are employed to manipulate circuits to fit the specific application. The FPGA is utilized to generate well-synchronized logical outputs at a high frequency. These logical outputs are translated to analog signals by a FPGA Mezzanine Card (FMC or FMCARD). The logical channels of the FPGA encode voltage levels as specified by the electronic design of the FMCARD. The FMCARD incorporates two integrated DACs. The electric signal then has 2^n voltage levels for a n -bit DAC. We built an image for the FPGA that will generate our desired encoding. The internal master clock of the FPGA runs at 200 MHz which generates via a phase-locked loop a GTH sampling frequency of 8 GHz. One GTH sample has therefore a duration of 125 ps, which is the time basis for all the output signals, i.e. signal lengths are calculated in multiples of GTH samples, cf. Fig. [3.1](#).

In the presented design, three logical channels are employed to specify one of the six states illustrated in Fig. [3.2](#). One logical channel is utilized to carve the laser light, i.e. to select pulses. Two logical channels are needed to select among three amplitude levels which translate in a first approximation to the mean photon numbers $\mu_1, \mu_2, \mu_2/2$. The conversion to a three-voltage analog signal is performed by a 2-bit DAC. The absence of a pulse, corresponding to the fourth intensity $\mu = 0$, is generated by the carver signal. In addition to that, one logical channel of the FPGA output is dedicated to the synchronization signal, which is sent directly to Bob. Furthermore, to generate the eight

⁵<https://www.boxoptronics.com/>

3. Experimental Setup

possible phases, three digital channels are required. The corresponding analog conversion is achieved by a 3-bit DAC on the FMCard. The specific mapping of digital channels to the BB84 states in the image design is detailed in Sec. 4.1.1

The carver signal should only be active when a certain pulse is carved, making it the fastest signal in the setup. In contrast, the other modulating signals (intensity and phase) can stay active for an extended duration; it is only necessary for them to cover both time bins for the $|\psi_+\rangle$ states. For practical implementation, these signals remain active for the entire "symbol duration", which is the early-to-early time separation, i.e. 10 ns. The carver signal can be freely positioned within these 10 ns for optimal timing. The relevant time scales involved in the symbol generation and how the beginning of a pattern train is configured are displayed in Fig. 3.1.

Once configured, the FPGA establishes a connection to Alice's PC via an Ethernet connection. The FPGA is then controlled by custom-made C++ FlexIO-based module software with a text user interface, enabling interactive playback and option settings to specify the FMCard outputs. This includes determining the specific pattern played or applying delays to specified logical outputs.

The sync is crucial to determine the beginning of the symbol train and by inference to find the positioning of all subsequent symbols in the playback. The exact setup and configuration of such playbacks are detailed in Sec. 4.1. The sync signal is repeated regularly with period T_{fr} and stays active for 200 ns at ~ 1 V. Setting the trigger level of a TTM or an oscilloscope at 500 mV one can confidently detect the presence of the sync under all circumstances⁶. As we can reliably detect the sync signal and have knowledge of the constant offset between the beginning of the pattern and sync, we can time align all symbols in the pattern. The other electrical signals drive the electro-optical components, directly influencing the shape of the optical signal. The characteristics of these signals are examined in the following. All electrical signals are transmitted through standard RF-SMA cables.

Carver

Intensity modulators are optoelectronic devices that allow light transmission based on an applied voltage V . The transmission is described by the corresponding transmission function $G : \mathbb{R} \rightarrow [0, 1]$, which is approximately defined by,

$$G(V) = \frac{1}{2} - \frac{1}{2} \cos \left(\frac{\pi V}{V_\pi} - \pi \right), \quad (3.2)$$

with \cos being the cosine function and V_π half of the period of G . An illustration of a transfer function can be found in Fig. 3.4.

⁶This is to say, we have never lost a single sync!

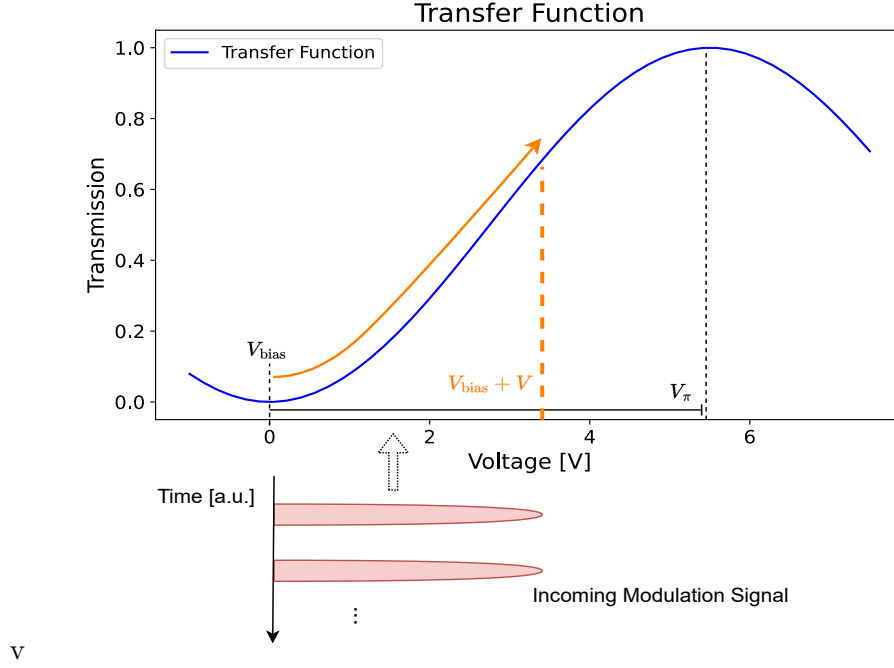


Figure 3.4.: Transfer function for an intensity modulator with period of $2V_\pi$. In this case, a bias voltage V_{bias} is applied to stabilize the IM in one of its null points, applying then a voltage V changes the transmission behavior and more light exits the IM.

The points at which the transmission is minimized are called null points. For the intended purposes, and with the chosen design of our modulation signals, both IMs should be stabilized at these null points. Stabilization is achieved through a micro bias controller (MBC) that adjusts the applied bias voltage V_{bias} based on an integrated optical-power feedback loop, ensuring that $T(V_{\text{bias}})$ becomes minimal. Applying a voltage V to an IM results in a change in its transmission to T' .

Two IMs are required to create the six states. The carver selects only the time bins of interest and "carves" therefore the pulses. The carver, a lithium niobate IM manufactured by [ixblue](https://www.ixblue.com/)⁷ is capable of fast modulation and creates pulses at a 1 GHz rate. The duration of the carver signal is set to two GTH samples, equivalent to 250 ps, cf. Fig. 3.1. Unlike the phase and amplitude signals, the carver signal is inverted, meaning its neutral (base) level is at a high voltage, and the active times of the carver are marked by a decrease in voltage. The carver signal directly modulates the IM from zero to full transmission because the IM is stabilized at the null point and V_π is applied.

⁷<https://www.ixblue.com/>, model MX-LN-20

3. Experimental Setup

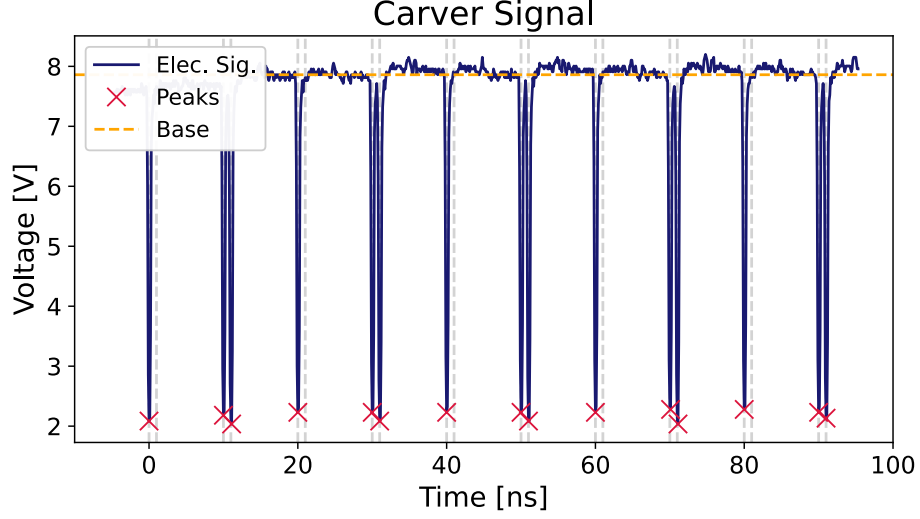


Figure 3.5.: The electrical carver signal (violet) of a repeated pattern of single pulses ($|\psi_0\rangle$) and double pulses ($|\psi_+\rangle$). The time separation between the early time bin of two consecutive symbols is 10 ns, and intra-symbol pulse separation is 1 ns. The baseline (idle voltage) in orange is the median of the entire electrical signal. The gray grid indicates the two time bins separated by 1 ns and each pair separated by 10 ns.

To characterize the carver signal, a pattern of repeated single and double pulses was played continuously, in this case we chose $|\psi_0\rangle$ and $|\psi_+\rangle$. The measured signal can be found in Fig. 3.5.

Peak analysis was conducted to characterize the pulse form and the pulse separation. Based on the chosen underlying pattern, the expected peak separations were 10 ns, 9 ns, and 1 ns. The averaged separation times of the peaks were found to be $10.02 \text{ ns} \pm 0.04 \text{ ns}$, $8.95 \text{ ns} \pm 0.5 \text{ ns}$, and $1.02 \text{ ns} \pm 0.04 \text{ ns}$, where the error estimate is the associated standard deviation (STD) of the mean. Considering that the sampling resolution of the oscilloscope used for this measurement was limited to 100 ps, it can be concluded that all peaks are well placed, allowing for precise time-bin encoding.

Given that only a few measurement samples constitute a single peak, the median of the signal was used to obtain an approximation of the idle voltage of the carver. The median was found to be 7.86 V. With respect to this baseline, the average modulation depth could be calculated, and it was found to be 5.688 V with an STD of 0.084 V. Although this modulation depth is smaller than V_π , it still allows for a relatively good extinction ratio, as will be discussed in the following. Furthermore, the full width at half maximum (FWHM) of each pulse was calculated and found to be 400 ps.

Phase Scrambler

As the laser operates continuously and is temperature-controlled, the phase stability of the laser is at least maintained for the duration of one symbol due to the laser linewidth of 2 MHz according to the laser datasheet. However, for security reasons, phase randomization (scrambling) is necessary, see Sec. 2.2.4 for the related discussion. In this lab demonstrator, the 3-bit DAC on the FMCARD can generate eight discrete phase values. Each unique bit-string maps to a different voltage applied to the PM manufactured by iXBlue⁸. The electrical signal, used to assess the modulation levels, is displayed in Fig. 3.6, where a periodic step pattern addressing each level was played. The respective levels are determined by the algorithm described in App. A.2 which retrieves the mean voltage of each modulation level, are summarized in Tab. 3.1.

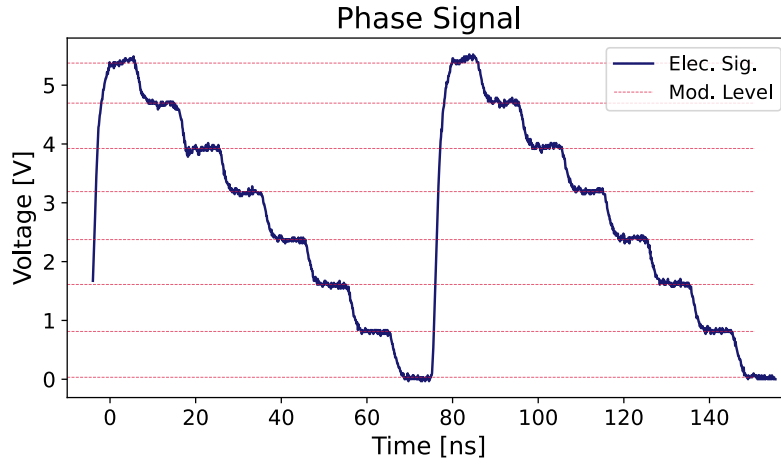


Figure 3.6.: The phase signal is generated by three bits, yielding eight approximately equispaced voltages. The different levels are uniformly distributed. For the analysis, a deliberately chosen descending pattern was played and the first two periods were recorded for the analysis.

Level	1	2	3	4	5	6	7	8
Mean Voltage [V]	0.034	0.813	1.611	2.375	3.191	3.924	4.696	5.375
STD [V]	0.033	0.043	0.058	0.063	0.040	0.061	0.050	0.069

Table 3.1.: Voltages applied to the PM for the phase scrambling. The voltages are on average separated by 0.768 V.

The mean distance between any two levels normalized to the level separation, calculated over all pairs, is 0.768 V with a STD of 0.026 V. With 5.375 V the FMCARD is only able to deliver up to V_π of modulation voltage, translating to a phase modulation in the range

⁸Model MPZ-LN-01

3. Experimental Setup

$[0, \pi]$. Although this does not cover the entire range of $[0, 2\pi]$ in the phase space, and thus, does not satisfy the requirements for the phase randomization, it may not be of significant concern for the proof-of-concept study of the setup.

Amplitude Modulator

In contrast to the carver, the output voltages for the AM need to be selected with more care, as three different intensity levels with well-defined ratios between them are required.

Calculating the inverse function of Eq. (3.2) gives

$$\tilde{V}(G) = \frac{V_\pi}{\pi} \left(\frac{V_\pi}{2} - \arccos(2G - 1) \right), \quad (3.3)$$

where the inversion domain of \cos was taken to be $[0, \pi]$. The intensities $\mu_1, \mu_2, \mu_2/2$ of the individual peaks of the states in Fig. 3.2, normalized w.r.t. μ_1 have relative ratios of 1, 1/2, and 1/4 w.r.t. μ_1 . Associating the peak point with the highest intensity, one can infer with Eq. (3.3) and $V_\pi \approx 5.5$ V the desired voltages for the modulation scheme. Figure 3.4 displays the transfer function and the targeted modulation levels 5.5 V, 2.75 V and 1.83 V.

Similar to the phase signal, the AM signal was measured over multiple symbol durations. The measured signal is displayed in Fig. 3.7 and analyzed in the same way as the phase signal, cf. App. A.2. The lithium niobate IM from Thorlabs⁹ was used for the generation of the three amplitudes, corresponding to the three mean photon numbers.

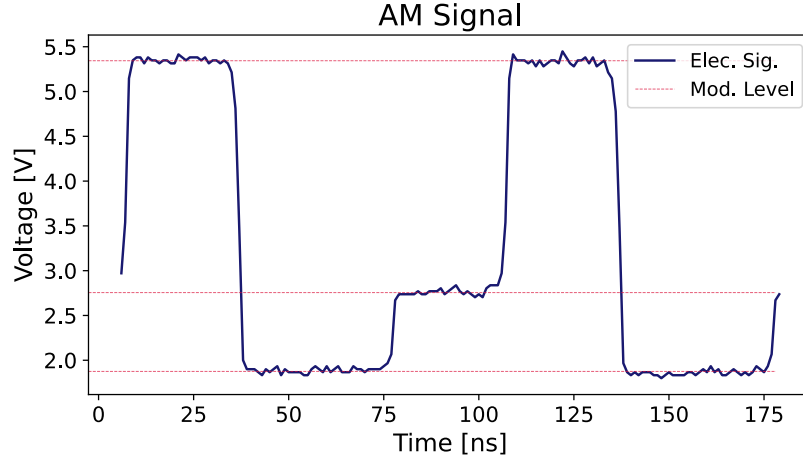


Figure 3.7.: The AM signal, measured over multiple symbol durations, generates the three intensity levels. The highest AM level is used to generate the states $|\psi_{0s}\rangle$ and $|\psi_{1s}\rangle$, the 2nd modulation level is used to generate the states $|\psi_{+s}\rangle$, $|\psi_{0d}\rangle$ and $|\psi_{1d}\rangle$. The last and lowest modulation level is only necessary to create $|\psi_{+d}\rangle$.

⁹<https://www.thorlabs.com/>, model LN81S-FC

The measured AM levels were found to be $1.87 \text{ V} \pm 0.03 \text{ V}$, $2.76 \text{ V} \pm 0.04 \text{ V}$ and $5.34 \text{ V} \pm 0.03 \text{ V}$. Since V_π is not exactly known, the AM's transfer function is only approximately known. This required an analysis of the configured modulation levels. For this measurement, no phase modulation was applied, however, the PM remained in the setup, and the laser light was modulated by the carver and the AM and then measured by a 10 GHz photodiode in the classical power regime ($\sim -10 \text{ dBm}$). A specific calibration pattern¹⁰ was played, cf. Fig. 3.8 for the measurement, and analyzed with peak detection, cf. Tab. 3.2. The height assessment of the AM-modulated pulses should correspond to the target mean photon numbers after attenuation.

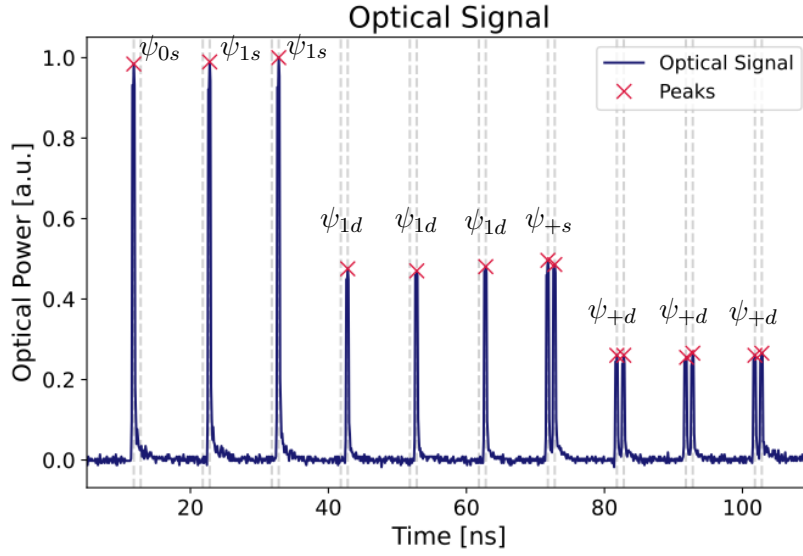


Figure 3.8.: Playback of the calibration pattern to assess the three amplitude levels of the pulses, and in a first approximation the related intensities. The signal was normalized w.r.t. the maximum recorded power. The three intensities should be $\mu_2/2 = 0.25$, $\mu_2 = 0.5$ and $\mu_1 = 1$. The gray grid indicates the first time and the second time bin of each symbol.

The peak detection algorithm found one peak per pulse as expected. The mean height and STD of the pulses belonging to the same amplitude are displayed in Tab. 3.2 and are compared to the expected (desired) amplitudes.

Normalized Amplitude	$\mu_2/2$	$\mu_2 = \mu_1/2$	μ_1
Expected	0.25	0.5	1
Measured	0.26 ± 0.04	0.48 ± 0.01	0.99 ± 0.01

Table 3.2.: Normalized optical power levels, measured and expected.

¹⁰See Sec. 4.1.1 for pattern playback and pattern creation.

3. Experimental Setup

The average agreement between measured and expected optical peak power is therefore 3.8%, 4.2%, and 1% for the level $\mu_2/2, \mu_2, \mu_1$ respectively. As we conditioned the levels on the calibration of μ_1 , it was expected that the agreement here is the greatest. It can be concluded that about 4.2% error in the height modulation of the pulse needs to be accounted for.

The FWHM width of each pulse in the calibration pattern sequence was found to be 400 ps. Figure 3.9 displays a zoom on the symbols 3, 7, and 8 (one-indexed) of Fig. 3.8 and contains all three intensity levels. The shaded areas correspond to durations of exactly 400 ps.

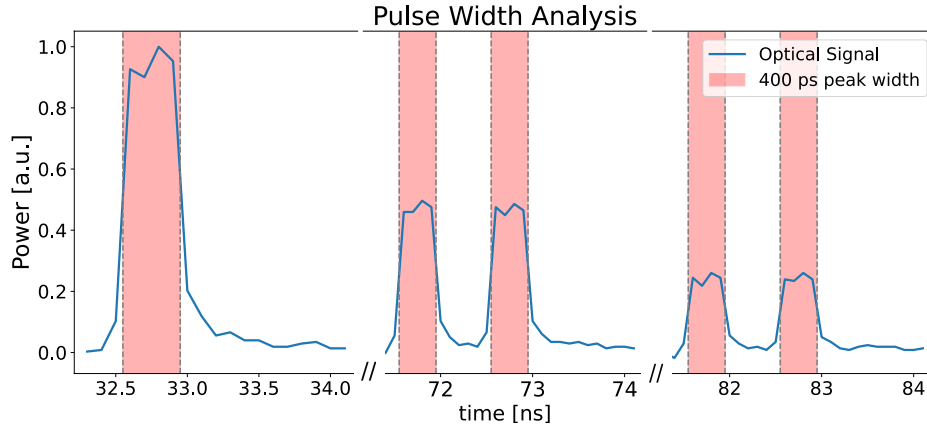


Figure 3.9.: Close-up of laser pulses in the optical regime with different heights. These pulses are the pulse (pairs) number 3, 6 and 7 in Fig. 3.8.

3.4. Bob's Setup - Receiver

The receiver setup, shown in Fig. 3.10, is considerably less complex than Alice's setup and requires little to no tuning. The first component is the BS, which has a splitting ratio of 90% and 10% and corresponds to the state generation probabilities, cf. Sec. 4.1.1. The 10% arm is associated with a measurement in the X basis, and the other is associated with a measurement in the Z basis. The 90% arm leads to a photon detector, signaling via a specific output signal to the TTM when a photon is measured. This photon detector-TTM combination is, therefore, a time-of-arrival measurement of any incoming optical signal, which is sufficient to decode the time-encoded signal bits. The TTM employed in this setup, manufactured by [qutools GmbH](https://qutools.com/)¹¹, has a digital time resolution of 1 ps with a timing jitter of less than 20 ps. The overall time jitter is greater, since the SPADs come with their own jitter of < 200 ps.

¹¹<https://qutools.com/> - quTAG MC with 8 channels

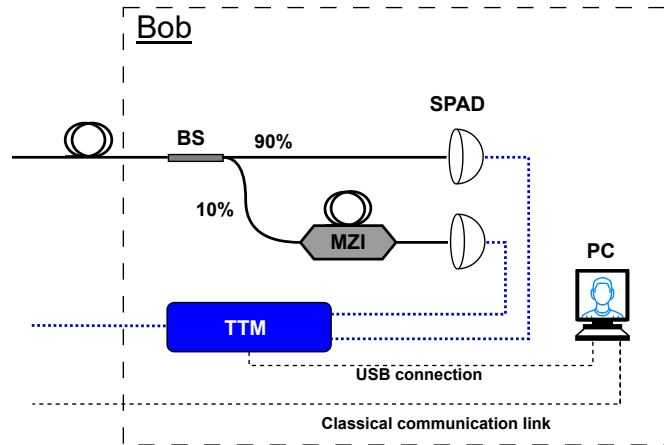


Figure 3.10.: Block diagram of Bob's setup, a closeup of the general experimental setup. Bob's has a passive basis selection with a 90:10 beam splitter (BS). In each basis, a detection time of the incoming photons is performed with two single photon avalanche detectors (SPADs). The X basis has an imbalanced Mach-Zehnder interferometer (MZI), to achieve destructive interference (for $|\psi_+\rangle$ states). As previously discussed, the classical communication link was missing as we used only one shared PC between by Alice and Bob.

Single Photon Avalanche Detectors

The employed SPADs from AUREA¹² are compact devices suitable for integration into racks and well suited for the near-infrared wavelength regime, and thus for the employed wavelength of 1550 nm. Single photon avalanche detectors are p-n junction semiconductors with applied reversed biases. This reversed bias voltage causes an electron-hole depletion zone in the p-n junction, which ultimately also causes a strong electric field. This zone is called the multiplication zone. If an incoming photon is absorbed in this region by the material it can generate an electron-hole pair, as described by the photo-electric effect [51]. The resulting electron (or hole) is accelerated by the present electric field, which can then result in impact ionization of other atoms. This impact ionization frees new electrons (holes), which are them self now accelerated and can generate, again, via impact ionization, new electron-hole pairs, etc. This cascading effect explains the "A" for avalanche in SPAD. This process leads to a short, strong, and measurable electrical signal. The initial configuration of the depletion zone is then quickly restored to allow the detection of a newly incoming photon. One denotes by dead time, the time it takes for a detector to be operational again. Shorter dead times increase the probability of after pulsing since the multiplication zone is not yet fully depleted of free electrons (holes). The detection of different wavelengths requires different materials. A typical semiconductor compound for the absorption of photons in the near-infrared regime is InGaS (Indium Gallium Silicon), as its bandwidth corresponds to these photon energies. The AUREA

¹²<https://www.aureatechnology.com/en/>, model SPD OEM NIR

3. Experimental Setup

detector also employs InGaS.

An essential characteristic of SPADs is its dark count rate, this is the count rate if no optical signal is applied. The dark counts are inherent to the device and the environmental conditions¹³. In our experiment, the dark count rate was about 470 Hz with a dead time of 25 μ s.

Delayed Mach-Zehnder Interferometer

The other detection line of the setup consists of a SPAD of the same fabricate and an additional delayed interferometer. The interferometer is used in this monitoring line to detect decoherence between the consecutive pulses of the $|\psi_+\rangle$ states. The setup utilizes Kyria's¹⁴ delay line interferometer, whose conceptual design is that of an MZI. This MZI has only one input port and the two output ports are associated with destructive and constructive interference, respectively. If a double pulse enters the MZI both pulses are split by a 50:50 BS, since one arm induces a time delay of exactly $\tau = 1$ ns, three time bins are obtained. The two side time bins should together contain half of the entered power of the early and late pulse. The central time bin contains the interference between the (E) and (L). Tuning the phase accordingly, one obtains in this central time bin constructive and destructive interference in the two output ports, respectively. This process is illustrated in Fig. 3.11. As mentioned earlier, only the port with destructive interference is monitored, corresponding to the X basis measurement. If we observe any non-destructive interference in the dark port, in the case a $|\psi_+\rangle$ was prepared, we can attribute this to a perturbation of the phase, i.e. a candidate of an eavesdropping attempt.

We performed a characterization measurement, the related setup is summarized in Fig. 3.12, to assess the obtainable visibility with this interferometer. The visibility, or fringe visibility, characterizes the contrast in the constructive/destructive interference of an interferometer. The visibility ranges from 0% to 100%, 100% indicating a perfect interference.

We injected laser light into the interferometer and monitored the optical power on both exit ports simultaneously. The standard deviation of the monitored power consecutive power measurements provided us with an error estimate. Tuning the phase delay through nearly the entire range of 2π yields the characteristic interference pattern displayed in Fig. 3.13. The phase delay was adjusted by applying a voltage. We determined the visibility V by looking at the minimum measured power of port 1 and the corresponding output

¹³At some point during the experiment, it was in early Spring, the environmental conditions in the lab became not only exhausting for the fellow scientists but also for the equipment. Due to a malfunctioning temperature regulation, the room temperature reached temperatures above 34 °C, which eventually resulted in the AUREA detectors failing to work, as the cooling mechanism of the detectors was overwhelmed. As the temperature rose, one could observe a rise in the dark counts, due to thermal radiation, which saturated in about 35 kHz. This is also the saturation level of the detector, for the specified settings.

¹⁴<https://kyria.com/delay-line-interferometers>, model MINT-band C-1GHz. In 2021, Kyria was acquired by iXblue.

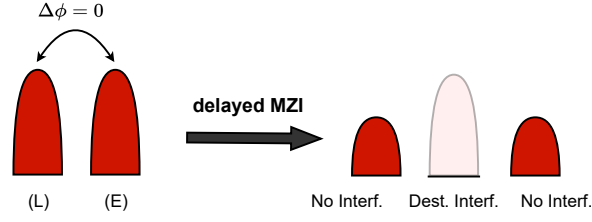


Figure 3.11.: The delay line interferometer delays in one arm the optical signal by $\tau=1$ ns, which corresponds to the separation distance between the early (E) and late (L) time bin. With the right phase difference of $\Delta\phi = \pi$, this results in destructive interference in the central time bin in one of the output ports, whereas the side time bins experience no interference.

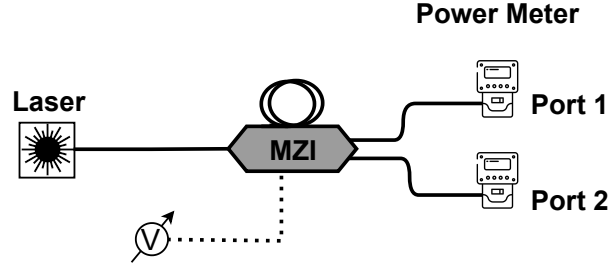


Figure 3.12.: Setup of the MZI characterization. We injected unmodulated cw laser light into the interferometer and monitored the power at both output ports. We tuned the voltage applied to the MZI, which changes the phase delay $\Delta\phi$ to go over the range of destructive and constructive interference in both ports.

power of port 2 (left dip in Fig. 3.13 at around 1.5 V.). The visibility is determined with

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} \quad (3.4)$$

with I_{\max}, I_{\min} the respective powers of port 2 and port 1. With conversions to SI units and appropriate chain rule, we calculated a visibility of $98.4\% \pm 0.8\%$. Accounting for device losses and imperfections, this is regarded as sufficient for our application.

3. Experimental Setup

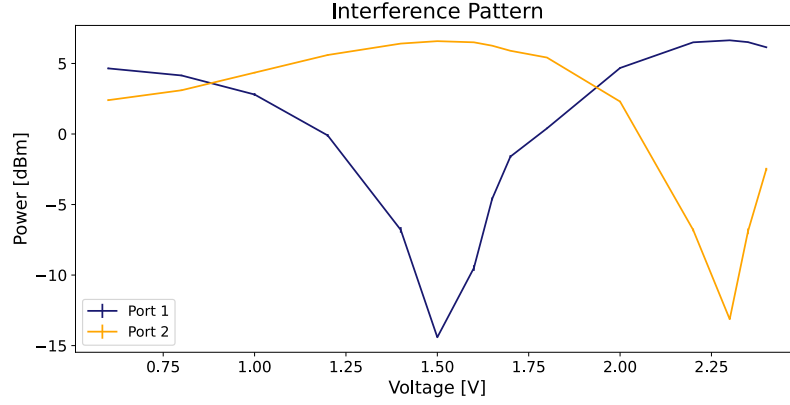


Figure 3.13.: Interference pattern of the MZI when applying a voltage to the MZI, which changes the phase difference. The point of interest for the visibility measurement are the extremal interference points. The error bars are estimated with the power measurement fluctuation (standard deviation), but are very small, and barely noticeable.

This chapter elaborated on the setup assembly, and in particular about the signal modulation. First, a laser light undergoes phase randomization, second, short laser pulses are created by carving the laser light. Third, the amplitude of the pulses was modulated such that, in a first approximation, the pulses will eventually contain the desired mean photon number. It also briefly described Bob's components of the receiver assembly, consisting essentially of a MZI, two SPADs, and a TTM.

4. Quantum Key Distribution Experiment

The chapter focuses on state sampling, data encoding for the state, and pattern creation in the context of quantum key distribution (QKD). This lays the foundation for the practical implementation of QKD transmission. Once outlined, the chapter describes the performed quantum measurements and subsequently analyzes them.

4.1. Pattern and Symbol Encoding

As discussed in Sec. 3.3, two bits are required for the amplitude modulation, and one bit is needed for the carrier. A total of three bits are used to specify the six states depicted in Fig. 3.2. Because the FPGA processes bytes, entire bytes are utilized to encode and store information for a symbol. To optimize storage efficiency, one byte encodes two symbols, with one symbol in the most significant nibble¹ and another symbol in the least significant nibble. Each nibble follows the '.BSP' encoding, where the most significant bit '.' is ignored. The 'B' bit encodes the basis, the 'S' bit encodes the strength of the pulse (low or high), and together with 'B', they map bijectively to the amplitude levels outlined in Eq. 3.1. The 'P' bit encodes the payload, representing the sampled bit value. For the three-state protocol, the 'P' is ignored if an X basis state is encoded. This encoding allows for easy extension to the four-state version of the protocol.

A sequence of such bytes is termed a *payload pattern*. Due to FPGA memory constraints, the size of a payload pattern is limited to about 120 MiB. Various side constraints on the byte count multiplicity exist but will not be emphasized further. The number of symbols in a payload pattern is therefore $2N$, with N being the byte size of the pattern.

For calibration and key distribution, different payload patterns are generated. Recall that, in order to satisfy the requirements of the one-time pad, the payload pattern needs not only to be sampled randomly but can only be used once. This implies that the transmitted payload sequence is limited by the byte count of the payload pattern, or multiple patterns need to be played subsequently to generate a sufficiently large key. For demonstration purposes, the former approach is the employed one. All payload patterns are generated in advance and are only uploaded to the FPGA upon request.

Similar to the payload pattern, the phase scrambler pattern encodes, on a byte-wise basis, the randomized phase for two symbols. The most significant bit of each nibble is discarded, and the remaining three bits map one-to-one to the eight voltage levels outlined in Tab. 3.1. Unlike the payload pattern, this pattern is generated on the fly for each QKD playback and is not stored, as the global phase of a single or double pulse is

¹A nibble is a half-byte, i.e. a four-bit string.

4. Quantum Key Distribution Experiment

irrelevant in the key generation. The pattern is uniformly sampled from a pseudo-random generator for the purpose of this thesis.

As already outlined in Sec. 3.3, continuous tracking of the position inside a transmitted symbol stream is crucial for the basis reconciliation and all other post-processing steps necessary to extract a secret key. This is achieved by subdividing the transmitted symbol stream into *frames*. The beginning of each frame is marked by the sync pulse, after which a specified number of symbols, sym_{fr} , is played. Similar to the payload pattern size, some side constraints apply, and sym_{fr} can not be set arbitrarily. With a chosen frame period of $P_{\text{fr}} = 1.1 \text{ ms}$ and $\text{sym}_{\text{fr}} = 96336$ one achieves a duty cycle of 87.6%. The number of symbols played in one frame is linked to the payload pattern size. For all patterns discussed in this thesis, $N = 120420 \text{ kiB}$ ². These values were chosen to maximize the transmission rate, while also respecting all boundary conditions, as well as to allow for an integer playback of frames³. With the selected parameters, a playback of exactly 2560 frames corresponds to the playback of the entire pattern without repetition. The conceptual design of the pattern with additional sync pulses as reference is sketched in Fig. 4.1.

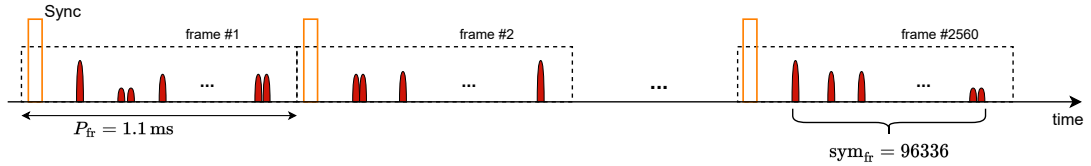


Figure 4.1.: The playback of a pattern is subdivided into frames. Each frame is marked by a classical sync pulse, which allows the mapping of the following time tags to symbols in the pattern. The frame period P_{fr} was chosen to be 1.1 ms and contained $\text{sym}_{\text{fr}} = 96336$ symbols, where the symbols are spaced 10 ns apart. With these choices and a pattern length of 120420 kiB, 2560 frames are required to play the entire pattern exactly once.

Not only does the subdivision into frames allow for easier handling and assessment of the pattern position, but it also enables temporal corrections. During playbacks, it was observed that the sync pulses were not separated by P_{fr} , but rather by $(1 + \epsilon) P_{\text{fr}}$, with $\epsilon \approx 10^{-5}$. This behavior was noticed not only in the sync signal but also in all other signals. The most likely explanation for this behavior is a slightly off FPGA clock. Therefore, all recorded time tags were scaled by a correction factor $1/(1 + \epsilon)$, determined by the ratio of the average sync-to-sync spacing and the expected P_{fr} of 1.1 ms.

²Note that the decimal prefixes should not be confused with the binary ones.

In binary, $1 \text{ kiB} = 2^{10} \text{ B} = 1024 \text{ B}$ and similarly, $1 \text{ MiB} = 2^{20} \text{ B}$.

³This is essentially a convenience factor for the analysis.

4.1.1. Sampling of Patterns

Different payload patterns, which are simply referred to as patterns for the following, were created via a dedicated Python script. For the discussion and analysis presented in this thesis, only three patterns are of interest. The first one is referred to as double pulse pattern ξ_+ , the second pattern is referred to as calibration pattern ξ_c , and the last one is called the random pattern, ξ_r . The former pattern ξ_+ consists solely of $|\psi_{+s}\rangle$ states and is used to characterize the X basis. The ξ_c pattern is employed to find the delay between sync and the beginning of the QKD transmission and to assess the amplitude levels, as described in Sec. 3.3. The ξ_r pattern is used to simulate a QKD transmission, i.e. generate a raw key, and eventually, a secret key.

While the payload bits must be sampled uniformly, the amount of monitoring states is subject to an optimization problem to maximize the SKR. The fraction of decoy states to signal states is also a free parameter and is ideally optimized for a specific transmission. For all experiments, the probability of preparing a signal state (Z basis) was chosen to be $p_Z = 0.9$ (and $p_X = 0.1$). The decoy state probability was set to $p_d = 0.3$ (and $p_s = 0.7$). The payload bits, in case the Z basis was selected, were obtained from a uniform distribution. The sampling was performed based on pseudo-random number generator⁴. Figure 4.2 visualizes the state occurrence frequency in ξ_r .

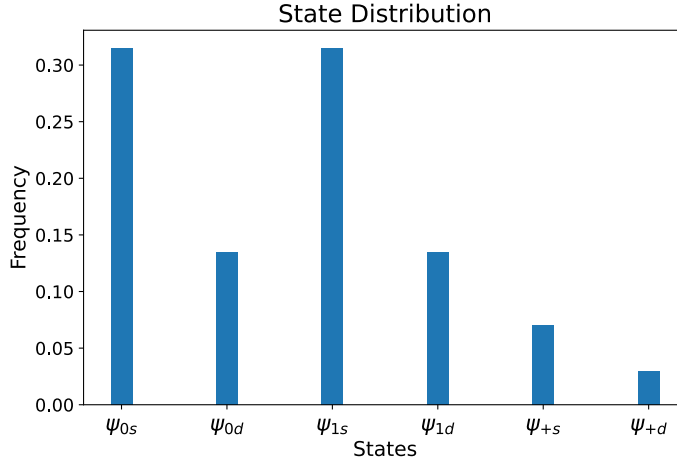


Figure 4.2.: Occurrence frequency of all states in the random pattern ξ_r of the QKD. The sampling probabilities were $p_Z = 0.9$ and $p_s = 0.7$.

The calibration pattern has the particularity that it is frame periodic, meaning the pattern repeats itself every sym_{fr} symbols. This frame periodicity enables the observation of a pulse at a specific time bin while averaging over different frames. The pattern is sampled in the same way as the random pattern, except for the first ten symbols, which are defined manually and serve as marker symbols. This does not significantly affect the

⁴Note that, this is not secure w.r.t. the requirements of an OTP, as discussed in Chap. 1.

4. Quantum Key Distribution Experiment

overall distribution of the states. This marker sequence is

$$|\psi_{0s}\rangle, |\psi_{1s}\rangle, |\psi_{1s}\rangle, |\psi_{1d}\rangle, |\psi_{1d}\rangle, |\psi_{1d}\rangle, |\psi_{+s}\rangle, |\psi_{+d}\rangle, |\psi_{+d}\rangle, |\psi_{+d}\rangle, \quad (4.1)$$

and was already shown in Fig. 3.8.

4.1.2. Mean Photon Number Estimation

Essential to the security consideration of the QKD implementation is the estimation of the mean photon number of the pulse, i.e. μ_1 . By design of the implementation, μ_2 can be directly inferred from the side constraint $\mu_1 = 2\mu_2$. As we will see later, this assumption will be challenged. The mean photon numbers are (optimization) parameters in the SKR. The mean photon number is estimated using the power measurement at the PM in the setup, cf. Fig. 3.3, as described in the following.

On the one hand, the power P is defined as the total (optical) energy E delivered over the time T

$$P = \frac{E}{T}. \quad (4.2)$$

On the other hand, the energy of a pulse containing \hat{n} photons, is just the sum of all single photon energies $E_{1\text{photon}} = hf$ contained in that pulse, f is the photon's frequency and h is Planck's constant. During the playback \hat{n} is the sum of $n_{\text{QKD}} + n_{\text{leak}}$. The former summand describes the photons from the QKD transmission, and the latter one, the laser leakage photons. The leakage photons are those photons that leak through, when all IMs are supposedly shut and should block a maximum of laser light, i.e. in the inter-symbol transmission times.

Consider now one frame period, in this case, one has exactly sym_{fr} pulses. The average photon number for signal and decoy states is μ_1 and μ_2 . The respective distribution in the pattern is given by the generation probabilities p_s and p_d . Therefore,

$$\hat{n} = n_{\text{leak}} + y \text{sym}_{\text{fr}} (p_s \mu_1 + p_d \mu_2), \quad (4.3)$$

with y being the duty cycle of the playback. The leakage photon rate can be found easily by monitoring the count rate at the SPAD and correcting for the dark count rate.

Using the above equations and applying the constraint $\mu_1 = 2\mu_2$, one can determine μ_1 from the measured power P_m at the power meter. The power of the QKD transmission, i.e., the power of the laser beam prepared by Alice, is simply $P_{\text{QKD}} = P_m - 30$ dBm. This accounts for a loss of -20 dBm due to the beamsplitter (BS) on Alice's side and an additional -10 dBm from the inline attenuation α , as illustrated in Fig. 3.3.

4.2. QKD Experiments

Since the system was built up sequentially, different measurements were performed to assess, first, the system integrity, and second, to develop the analysis scripts. In the following, three experiments are presented.

4.2.1. QBER over Attenuation

In the first experiment, the ability to associate reliable clicks in the SPAD to an occupied time bin, and thus to a payload sequence, was demonstrated. In other words, the bit error rate of the Z basis is measured, this QBER is denoted by Q . Since this experiment was successful, it was then expanded to a larger scope, namely, to assess the QBER over different attenuations, which shall be presented here. At this stage of the setup, the entire X basis measurement branch was missing. This should, however, not affect the measurement outcome and discussion w.r.t. the full system, cf. Fig. 3.3. Different attenuations were achieved by tuning the VOA, this simulates different fiber lengths, i.e. transmission distances.

Before starting the analysis, one needs to determine the exact beginning of the first time bin. This was done by repeatedly playing ξ_c . Building a histogram over frames reveals the position of the first time bin. This time offset between the sync and the first time bin, i.e. the beginning of the active playback, could therefore be inferred. The exact location of the time bins was then found by a QBER optimization. Here, subsampling of the two time bins was also employed to improve further the QBER. Subsampling is a technique in which not the entire time bin of (E) and (L) is considered, but only by a smaller window. This is considered to improve the QBER as fewer photons leak into the (L) from (E). The downside lies in less viable photons, which diminishes the raw and thus the secret key rate. The subsampling of the respective early and late time windows was kept for all attenuations.

Once the time alignment is found, one can map the recorded time tags to a payload and pattern index sequence. After sifting, one can calculate the Q , by comparing the sifted measured bit string to the initially prepared pattern. For this, one needs to consider the size L of the payload subset of the pattern, i.e. the number of prepared $|\psi_0\rangle$ and $|\psi_1\rangle$ states. Dividing the number of miss-matched bit values, m over L ,

$$Q = \frac{m}{L}, \quad (4.4)$$

yields the QBER.

Taking the statistical significance of the payload subset size into account, one can estimate an error for each QBER. This is done by calculating a symmetric confidence interval around Q of size $2\beta\sigma$, with $\beta = 1.96$ the confidence factor⁵ and σ the standard error of the distribution. The standard sampling error can be approximated with

$$\sigma = \sqrt{\frac{(Q(1-Q))}{L}}, \quad (4.5)$$

since the sampling process can be modeled as a binomial experiment, assuming each bit has an equal probability to be erroneous.

For the measurement, ξ_r was uploaded to the FPGA. In this first experiment, we selected a transmission power $P_{\text{QKD}} = -89 \text{ dBm}$ which corresponds to a mean photon

⁵Choosing $\beta = 1.96$ is a common choice to approximate 95%-tile of a normal distribution.

4. Quantum Key Distribution Experiment

number of $\mu_1 = 0.016$, cf. Sec. 4.1.2. We then simulated different attenuations by tuning the power of the QKD transmission, which was measured by continuously playing the loaded pattern. Once the power was measured, the data acquisition of the TTM was started and the pattern was played for exactly 2560 frames. This process was repeated for different simulated attenuations. Figure 4.3 summarizes the obtained results.

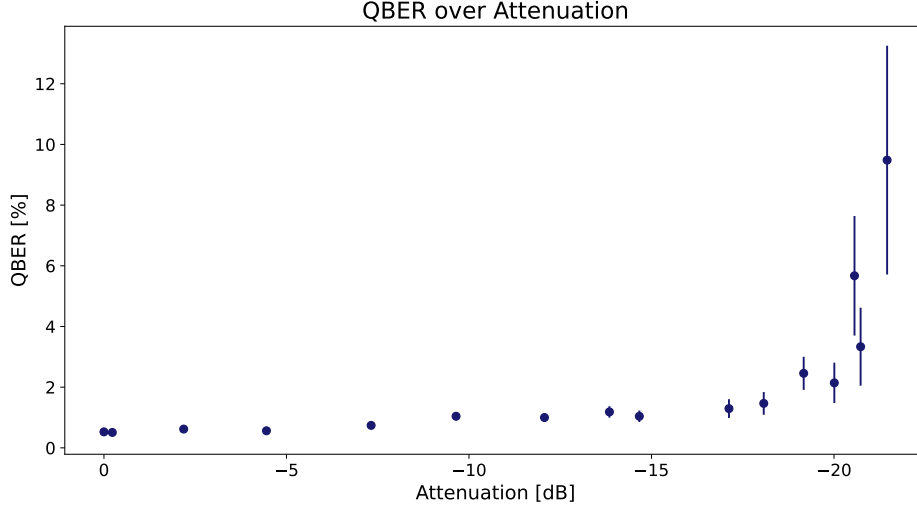


Figure 4.3.: QBER over different attenuation, simulating different transmission distances. The QBER is around 1% for small attenuations and starts to rise at around -19.2 dB.

The QBER remains low, at around 1%, which is typical value for QKD [41]. This QBER is maintained for attenuations up to 19.2 dB, with a very small estimated sampling error and key length of about 4000 bits. One observes an increase in the QBER from thereon, reaching 10%. Likewise, the size of L decreases, adding to the uncertainty of these QBERs. One should note that the power meter was at the edge of its resolution capacity for such low optical powers. This experiment showed that a QBER can be reliably inferred, even for lower attenuations. With reliable, we mean that the QBER is around 1% and raises only for high attenuations (which is to be expected) but remains under 13% within the error bars boundaries.

In our experiment, in which we want to extract a key, we target the pulse occupation $\mu_1 \approx 0.1$ to guarantee secrecy. With $\mu_1 = 0.1$, the probability of a pulse containing at least two or more photons is reduced to below 0.5%, reducing exposure to PNS attacks. This targeted mean photon number is closely achieved for a prepared QKD transmission power without (or slight) attenuation. This experiment shows that Alice can prepare states with a pulse occupation of $\mu_1 = 0.1$, and maintain a low QBER $< 2\%$ over different attenuations up to -19 dB. This QBER is comparable to experimental results in [8].

4.2.2. Visibility Measurement

A second experiment was performed to characterize the X basis. As discussed in Sec. 3.4 we aim for total destructive interference in the cases where $|\psi_+\rangle$ states are prepared. In the quantum case, the interference visibility was estimated with

$$V = 1 - \frac{N_{\text{int}}}{N_{\text{non}}} \frac{p_{\text{non}}}{p_{\text{int}}}, \quad (4.6)$$

in the work presented in [52], where N_{int} and N_{non} are the count in the interfering and non-interfering bins. The ratio $\frac{p_{\text{non}}}{p_{\text{int}}}$ express the amount of transmitted non-interfering to interfering sequences. In the case that only double pulses are prepared, and ignoring the effects of an unequal split ratio of the BS in the MZI, the proportion in the non-interfering time bins should be equal to that of the interfering time bin. Therefore, $\frac{p_{\text{non}}}{p_{\text{int}}} = 1$. The visibility is then estimated with

$$V = 1 - \frac{k_c}{2(k_e + k_l)} \quad (4.7)$$

where k_c is the number of counts in the central time bin and k_e and k_l are the respective counts in the early and late side bins. The factor of two in the denominator comes from the fact that we observe only one (the dark) port, but the visibility is calculated w.r.t. the total light incoming (and outgoing) to the MZI. Irrespective of the dark or bright port, in a perfect 50:50 BS only half of the light is observed in either of the ports.

For this measurement, the setup already had its final form, depicted in Fig. 3.3. The pattern ξ_+ was uploaded to the FPGA to achieve the same occupation number in (E) and (L) time bins. The experiment was performed as a back-to-back experiment with a QKD transmission power of -90 dBm. By playing the pattern continuously for 200 s one can achieve an estimate of V over a longer time, the results are summarized in Fig. 4.4.

Similarly, for Z basis measurements, the starting point of the transmission, i.e. the first time bin, was determined through the construction of a histogram. Once this offset was identified, subsampling of the three target time bins in the X basis was performed. The upper image in Figure 4.4 displays the counts in the early, central, and late time bins, along with a background estimation. The background count estimation is derived from the no-symbol bins, which lie between the later time bin of a symbol and the early time bin of the next symbol, excluding a 1 ns guard to reduce leakage. The background window lasts longer and accumulates, therefore, more counts as in a comparable window of 1 ns. Thus, we had to scale the background window appropriately for comparability with the other windows.

The average visibility throughout the measurement is 94.0%. Repeating the same experiment without phase randomization yields an average visibility of 97.7%. The difference can be attributed to the potential misalignment of the phase scrambler signal w.r.t. the carver signal. The intra-level voltage fluctuations of the phase scrambler cause only a negligible shift in visibility. Nonetheless, around 2.3% of contrast is lost in the system, even with a phase-stable state preparation. This may be attributed to several

4. Quantum Key Distribution Experiment

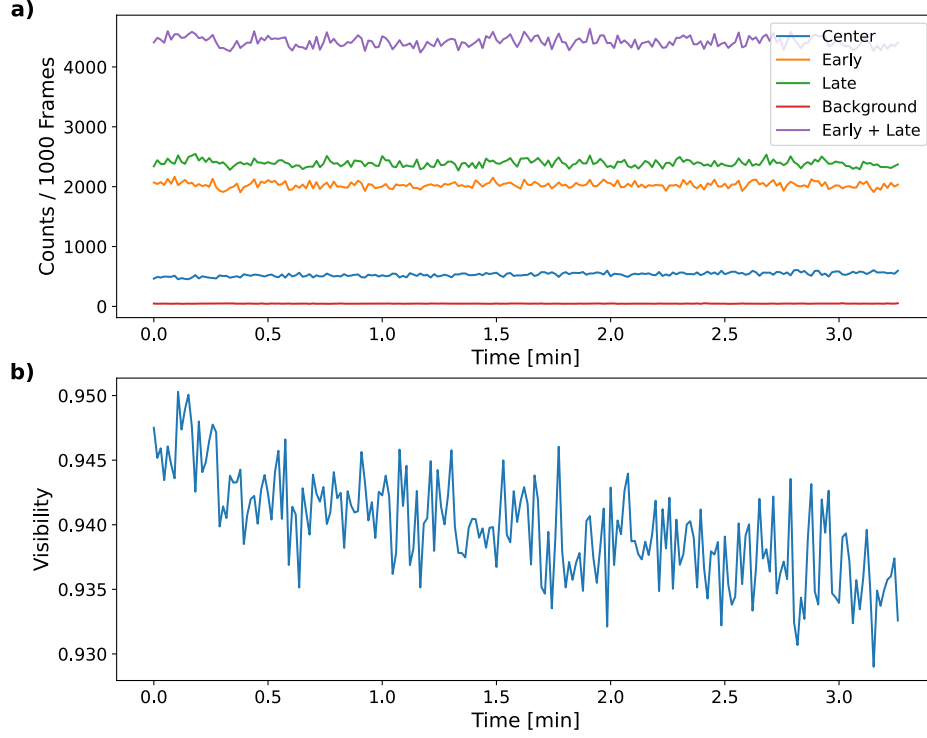


Figure 4.4.: Visibility measurement over approx. 3 min. Count sampling, (a), was performed every 1000 frames, i.e. 1.1 s over a period of 3 min. One can observe an overall increase of the center bin counts, which correlates with the decrease observed in the visibility (b), characterizing the X basis.

factors. First, unequal splitting coefficients in the BS may be present, as indicated by the observation of more counts in the late time bin than in the early time bin. Second, the MZI could be misadjusted, i.e. the phase shift in the long arm of the MZI is not precisely π . Third, non-ideal pulse formation during state preparation could also contribute to imperfect destructive interference, either due to double pulses not being separated by exactly 1 ns or variations in pulse amplitudes between the early and late time bins. Fourth, drifts during the running setup in the laser current or clock misalignment of the FPGA and the Kyla, i.e. $1 \text{ ns}_{\text{FPGA}} \neq 1 \text{ ns}_{\text{Kyla}}$. The hypothesis of drifting laser light can be supported by the argument that we performed first the experiment without phase randomization and only second the experiment with phase randomization.

In both experiments, with and without phase randomization, visibility decreases over time due to a slight increase in the central time bin counts. The maximum difference in visibility was 2% in the case of phase randomization over a measurement period of 3 min.

Due to generally low visibility combined with long-term stability issues, a high error rate in the X basis is anticipated, especially in the absence of periodic readjustments during extended measurements.

4.2.3. Secret Key Discussion

In this third and last experiment, we demonstrate the ability to measure the quantities of interest in order to derive a SKR. The experiment is set up as shown in the block diagram in Fig. 3.3. Recall from the discussion in Sec. 2.2.4 that the SKR is essentially bounded by the following quantities: the lower bound of the vacuum events in the Z basis $s_{Z,0}^l$, the lower bound of the single-photon events in the Z basis $s_{Z,1}^l$, and the upper bound of the phase error rate in the Z basis associated to the single-photon events $\phi_{Z,1}^u$. The secret key length l is bounded

$$l \leq s_{Z,0}^l + s_{Z,1}^l (1 - h(\phi_{Z,1}^u)) - \lambda_{\text{EC}} - 6 \log_2(19/\epsilon_{\text{sec}}) - \log_2(2/\epsilon_{\text{cor}}), \quad (4.8)$$

with $\epsilon_{\text{sec}}, \epsilon_{\text{cor}} > 0$ being the secrecy and correction parameter and λ_{EC} the number of disclosed bits during the error correction phase [41]. We denote here with $h(\cdot)$ the binary entropy function

$$h(x) = -x \log(x) - (1-x) \log(1-x). \quad (4.9)$$

The measurable quantity in the Z basis is the QBER, and the on the signal and decoy states conditioned QBERs, these two latter quantities give the bounds to $s_{Z,0}^l$ and $s_{Z,1}^l$. These bounds are also dependent on other, experiment-dependent quantities, e.g. mean photon numbers and state generation probabilities. The security analysis takes care to only include estimated single photon detection events in the calculation of the secret key to avoid leakage by the PNS attack.

The bound to the phase error $\phi_{Z,1}^u$ can itself be estimated from the error rate of the monitoring line [53]. Again, the error rates for the signal and decoy events are entered separately in the calculation of the upper bound [54, 41]. These error rates are calculated as the QBER in Eq. (4.4). Errors are accounted for in the cases in which $|\psi_+\rangle$ was prepared and the TTM registered a detection event in the central time bin. Conversely, a detection event in one of the side bins is considered to be a no-error event. The implemented equations to calculate the SKR l are given in a concise form in App. A.3.

As in 4.2.1, ξ_r was uploaded to the FPGA and played only once, i.e. for 2560 frames to simulate a key exchange. The power of the transmission was $P_{\text{QKD}} = -90.7$ dBm and the occupation number was consequently estimated to be 0.102. The experiment was performed in a back-to-back setting, meaning that the signal experienced no additional attenuation, apart from minimal unavoidable losses, before reaching Bob's measurement apparatus. The experimentally obtained raw key lengths in both bases and the respective error rates are summarized in Tab. 4.1.

With a subsampling window length of 200 ps for the time bins, we were able to push the QBER down to 0.67% this is comparable to the results obtained in Sec. 4.2.1. The error rate in the X basis is considerably worse at 12.53%, and even for 13.27% if one

4. Quantum Key Distribution Experiment

	Errors [%]			Events		
	total	μ_1	μ_2	total	μ_1	μ_2
Z	0.67	0.69	0.58	26936	21028	5908
X	12.53	12.31	13.27	423	325	98

Table 4.1.: The error percentages and the detection events, specified for basis Z and X, as well as for the signal (μ_1) and decoy (μ_2) states. We denote with n_Z the total number of detection events (bits) in the Z basis, from which we will eventually distill a secret key.

considers only other decoy error rate. From visibility measurement discussed in Sec. 4.2.2 this was already expected.

We identify two issues with the number of retrieved events. First, due to the short recording time of 2560 frames, and the resulting low number of detection events, statistical fluctuations may have affected the error rates. However, these effects are minor compared to another problem related to the insufficient number of detections events. These finite-key size effects might be more severe. Finite-key size corrections can only be applied for a sufficiently large number of detection events. For comparison, target blocking sizes, which are also designed to maximize the SKR, are about 10^7 or 10^9 [41], which is two to four orders of magnitude higher than the total number of detection events in the Z basis. To overcome this issue of small sample size, we artificially scale all detection and error events by a factor of 1000, to match a reasonable block size of $N_Z \approx 10^8$, in which we can apply safely finite-key corrections. The QBERs are not affected by this scaling. Events for both bases are scaled identically to maintain the relative ratio between them.

Second, by analyzing the counts more carefully, one finds a discrepancy in the expected detection ratio of signal-to-decoy states. This mismatch can be explained by poor sampling of the decoy states' amplitudes, which was assumed to be $\mu_1/2$, deviating from the classical analysis presented in Sec. 3.3. We relate this discrepancy to μ_2 because we have confidently estimated μ_1 through the analysis presented in Sec. 4.1.2. To account for this mismatch, we present a brief analysis to find an estimate of μ_2 . To retrieve μ_2 , we first need to determine the channel parameter $\eta < 1$. This channel parameter accounts for attenuation, detector efficiency, and other effects and is highly dependent on the setup.

We assume that the number of measured signal states $N_{\mu_1}^{\text{meas}}$ can be expressed as

$$N_{\mu_1}^{\text{meas}} = N_{\mu_1}^{\text{prep}} \text{Pois}(k \geq 1; \mu'_1), \quad \text{with } \mu'_1 = \eta \mu_1, \quad (4.10)$$

and with $N_{\mu_1}^{\text{prep}} = N p_s$ being the number of prepared signal states and $\text{Pois}(k \geq 1; \mu_1)$ the probability that a prepared signal state is a non-vacuum state and reaches the detector, cf. Eq. (2.19). Only pulses containing photons can cause clicks in the SPAD and thus contribute to $N_{\mu_1}^{\text{meas}}$. The probability that a pulse is a non-vacuum state can be rewritten as $\text{Pois}(k \geq 1; \mu'_1) = 1 - e^{-\mu'_1}$. We obtain η by rearranging Eq. (4.10) and inserting all known quantities.

The number of measured decoy states is modeled analogously to Eq. (4.10). Therefore,

we have

$$\mu_2 = -\log\left(1 - \frac{N_{\mu_2}^{\text{meas}}}{N_{\mu_2}^{\text{prep}}}\right)/\eta, \quad (4.11)$$

which evaluates to $\mu_2 = 0.065$, this updated estimate of μ_2 is used in the further calculation, cf. Tab. 4.2.

Having addressed and discussed our results, we can finally distill a secret key using the corrected protocol parameter μ_2 , applying the event scaling and finite-key corrections. An intermediate result of the SKR calculation is the estimation of the phase error rate, which is calculated with Eq. (A.10). In our experiment, we calculated $\phi_{Z,1}^u = 20.6\%$. We attribute this high phase error to an ongoing drift in the laser which resulted in worse visibility than in the experiments in Sec. 4.2.2. For the sake of simplicity, since we aim for a proof-of-concept calculation, we do not perform any error-correcting methods, however, account for the loss of usable key material. The number of disclosed bits during the error correction follows the formula $\lambda_{\text{EC}} = f_{\text{EC}} n_Z h(Q)$, with f_{EC} being the error correction efficiency, n_Z denoting the sifted key length, i.e. retrieved counts from the Z basis, and the binary entropy $h(Q)$ of the QBER in the very same basis. We set the error correction efficiency to 1.16. Table ref. 4.2 summarizes all protocol parameters used in calculating the SKR [55].

μ_1	μ_2	p_s	ϵ_{sec}	ϵ_{cor}	$\phi_{Z,1}^u[\%]$
0.102	0.065	0.7	10^{-5}	10^{-9}	20.6

Table 4.2.: Overview of SKR protocol parameters and estimation of the upper bound of the phase error rate in the Z basis. The mean photon number of the signal states (μ_1) was retrieved from the measurement of the laser power during the experiment. The decoy mean photon number (μ_2) was calculated with μ_1 and an estimate of the channel parameter η . The probability of generating a signal state is p_s , with the counter probability of generating a decoy state of $p_d = 1 - p_s$. The epsilon security and correctness parameters were retrieved from the SKR discussion [41]. It is important to note that the basis selection probability, active during state preparation and passive during the measurement, plays no role in the SKR estimation.

With a secret and reconciled key, the SKR can be calculated with

$$\text{SKR} = R \frac{l}{N_Z}, \quad (4.12)$$

with R the repetition rate of the key generating source and N_Z the length of the raw key. In our setup $R = 75.6$ MHz, and is calculated from the multiplication of symbol frequency, duty cycle, and Z basis preparation probability, the latter factor is included, because the Z basis contributes solely to the secret key. Note that the limiting factor in the SKR is not R , but rather the SPADs saturation level, which bounds the possible achievable key rate. As a reminder, the employed detectors saturated at about 35 MHz. We used the entire key, i.e. the total amount.

4. Quantum Key Distribution Experiment

The found SKR evaluates to 1.7 kHz, i.e. 1700 bits per second of secret information. This secret key rate is severely limited by the considerably high phase error rate of 20%, compared to the experimental values of other three-state BB84 experiments with time-bin encoding, which ranges from 2% to 7% [8, 9]. One should also note that the experiment for the SKR retrieval was performed in conditions that did not account for additional global attenuation, i.e. did not consider any meaningful transmission distances, i.e. Bob's lab was situated right beside Alice's lab. Despite being limited by errors and poor sampling, with careful analysis, we were able to extract a maximum achievable secret key rate.

In the conclusion of this chapter, we presented the pattern design with the specific byte-wise encoding, which translates to a symbol sequence. We detailed how it is possible to retrieve the mean photon number, i.e. occupation number, of a signal state pulse. We further performed three distinct experiments, first, we performed a QBER measurement over different attenuations in a simplified setup. We showed reliable performances, in the sampling, and measurement retrieval on both the hardware and software side. Second, we characterized the visibility measurement to demonstrate the ability to obtain a phase error rate. Third and finally, we performed a simultaneous measurement in Z and X basis, mimicking a life QKD transmission. Despite the high phase error rate, we were able to extract a non-zero secret key from this measurement. In the presented discussion, we addressed the main issue of our setup design and experiment, the most prominent being the poor estimation of the decoy state occupation number.

5. Conclusion

This master thesis discussed in Chap. 2 the general concept of QKD experiments, more particularly the three-state BB84 protocol with one-decoy state encoded with time-bin encoding, which falls under the category of measurement-and-prepare QKD protocols. In the three-state protocols, one basis is sacrificed entirely for the secrecy estimation and allows generally for a simpler setup design. The state-of-the-art time-bin encoding scheme was implemented in a novel way for this protocol. The proposed setup design, presented in Chap. 3, allows for a relatively simple state generation by employing fast laser carving to select the time bin slots. This was performed by a fast amplitude modulator, called the carver. An additional amplitude modulator was used to generate three distinct amplitude levels, thus implementing the one-decoy state protocol. These amplitude modulators, as well as a phase modulator for phase randomization, were all controlled by carefully designed electrical signals. We designed and analyzed these signals and found that, given a certain tolerance, they are well-fitted for our implementation. We created and registered a stream of pulses in the classical domain. While the time-bin encoding, the shaping/carving of the pulses, was performed with high accuracy, the pulse height, i.e. amplitude was only matched in accounting for standard error interval. Bob's measurement setup, consisting of two SPADs and interferometer and a time tagging module, was also described. The pattern design, playback design and the symbol encoding were described in Chap. 4. The pattern length and the frame size were optimized to exploit on the one hand the full memory capacity of the FPGA, and on the other hand to allow for an even playback of frames. Based on the byte-wise processing of the FPGA, two symbols were encoded per byte, one per nibble, with straightforward mapping to the six protocol states and possible extension to the four-state variant. We described how three different patterns were sampled, in particular, from which probability distribution the random pattern was drawn from. The retrieval of the mean photon number μ_1 is utterly important as it is an important protocol parameter for the calculation of the SKR. A method to retrieve μ_1 as part of the measurement routine was detailed. These preparatory experiments, their analysis and discussion led to the three experiments on quantum level: First, we performed QBER measurement over different attenuations, simulating different transmission distances. This experiment, focussing exclusively on the bit retrieval in the Z basis, demonstrated that a key can be successfully extracted and that the associated error rate remained low at 1% with high confidence up to attenuations of 19 dB with QKD transmission power of $P_{\text{QKD}} \approx -90$ dBm. Second, we characterized the X basis by sending $|\psi_+\rangle$ states and monitoring the visibility. The visibility was found to be at a maximum of 97.7%, but deteriorated over time, it was therefore expected that this degrades the phase error rate. This is especially true because we took the measurements for the visibility assessment and noticed already here a drift deteriorating the visibility, and only then

5. Conclusion

performed the final measurement with both detectors. Third, we performed a full QKD run with pulse occupancy of $\mu_1 = 0.102$ on two SPADs and passive basis selection. In the Z basis, we obtained a QBER below 1% and in the X basis an error rate at around 12% to 13%. With scaled detection events and estimation of $\mu_2 (= 0.065)$ we were able to follow closely the underlying security analysis of Rusca et al. [41]. Even though the upper bound on the phase error was estimated to border 20.6%, we were ultimately able to extract a positive SKR of about 1.7 kHz and demonstrated the potential of the setup design.

The aim of this master thesis was to build and test a prototype of a three-state BB84 protocol with time-bin encoding and the one decoy-state method. A modification towards existing implementation lays in the generation of the X state, which was in our experiment directly carved into the laser stream, instead of a beam splitting and recombination method. During this master thesis, we showed that cw-laser carving with an intensity modulator is a viable and simple method to generate pulses. We provided theoretical understanding, before detailing on software and hardware design all relevant aspects of our implementation. This allows for easy reproducibility and the possible extension to the four-state variant of the protocol.

Bibliography

- [1] Kahn D. The codebreakers : the story of secret writing. London: London : Weidenfeld I& Nicolson; 1966.
- [2] Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. Rev Mod Phys. 2020 May;92:025002. Available from: <https://link.aps.org/doi/10.1103/RevModPhys.92.025002>.
- [3] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dusek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009 Sep;81:1301-50. Available from: <https://link.aps.org/doi/10.1103/RevModPhys.81.1301>.
- [4] ISO/IEC 14888-2:2008; 2008. Current norm in 2022. Technical Committee: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection.
- [5] RONALD R, ADI S, LEONARD A. Cryptographic communications system and method; 1983. United States Patent 4,405,829. MASSACHUSETTS INST TECHNOLOGY.
- [6] Bouwmeester D, Ekert AK, Zeilinger A. The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation. 1st ed. Springer Publishing Company, Incorporated; 2010.
- [7] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: International Conference on Computers, Systems & Signal Processing. Bangalore, India; 1984. p. 175-9.
- [8] Boaron A, Korzh B, Houlmann R, Boso G, Rusca D, Gray S, et al. Simple 2.5 GHz time-bin quantum key distribution. Appl Phys Lett. 2018;112.
- [9] Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, et al. Secure Quantum Key Distribution over 421 km of Optical Fiber. Phys Rev Lett. 2018 Nov;121:190502. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.121.190502>.
- [10] Vagniluca I, Da Lio B, Rusca D, Cozzolino D, Ding Y, Zbinden H, et al. Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution. Phys Rev Appl. 2020 Jul;14:014051. Available from: <https://link.aps.org/doi/10.1103/PhysRevApplied.14.014051>.
- [11] Hwang WY. Quantum Key Distribution with High Loss: Toward Global Secure Communication. Phys Rev Lett. 2003 Aug;91:057901. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.91.057901>.

Bibliography

- [12] Lütkenhaus N, Jahma M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*. 2002 jul;4:44-4. Available from: <https://doi.org/10.1088/1367-2630/4/1/344>.
- [13] Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, et al. Advances in quantum cryptography. *Adv Opt Photon*. 2020 Dec;12(4):1012-236. Available from: <https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012>.
- [14] Kollmitzer C, Pivk M. *Applied Quantum Cryptography*. London: Springer; 2010.
- [15] Gottesman D, Lo HK, Lütkenhaus N, Preskill J. Security of Quantum Key Distribution with Imperfect Devices. *Quantum Info Comput*. 2004 sep;4(5):325–360.
- [16] Gröblacher S, Jennewein T, Vaziri A, Weihs G, Zeilinger A. Experimental quantum cryptography with qutrits. *New Journal of Physics*. 2006 may;8(5):75. Available from: <https://dx.doi.org/10.1088/1367-2630/8/5/075>.
- [17] Shengkai L, Yong HL, Liu C, Shentu GL, Dong-Dongli, Lin J, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *ACS Nano*. 2017 01:24.
- [18] Bloch M, McLaughlin SW, Merolla JM, Patois F. Frequency-coded quantum key distribution. *Opt Lett*. 2007 Feb;32(3):301-3.
- [19] Shi BS, Jiang YK, Guo GC. Quantum key distribution using different-frequency photons. *Applied Physics B*. 2000 06;70.
- [20] Bacco D, Christensen J, Usuga Castaneda M, Ding Y, Forchhammer S, Rottwitt K, et al. Two-dimensional distributed-phase-reference protocol for quantum key distribution. *Scientific Reports*. 2016 06;6.
- [21] Lavie E, Lim CCW. Improved Coherent One-Way Quantum key Distribution for High-Loss Channels. *Phys Rev Appl*. 2022 Dec;18:064053. Available from: <https://link.aps.org/doi/10.1103/PhysRevApplied.18.064053>.
- [22] Gao RQ, Xie YM, Gu J, Liu WB, Weng CX, Li BH, et al. Simple security proof of coherent-one-way quantum key distribution. *Opt Express*. 2022 Jun;30(13):23783-95. Available from: <https://opg.optica.org/oe/abstract.cfm?URI=oe-30-13-23783>.
- [23] Ekert A. Quantum cryptography based on Bell's theorem. *Physical review letters*. 1991;67 6:661-3.
- [24] Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. *Phys Rev Lett*. 1992 Feb;68:557-9. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.68.557>.
- [25] Yin J, Li YH, Shengkai L, Yang M, Cao Y, Zhang L, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*. 2020 06;582:1-5.

- [26] Braunstein SL, Pirandola S. Side-Channel-Free Quantum Key Distribution. *Phys Rev Lett.* 2012 Mar;108:130502. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.108.130502>.
- [27] Lo HK, Curty M, Qi B. Measurement-Device-Independent Quantum Key Distribution. *Phys Rev Lett.* 2012 Mar;108:130503. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.108.130503>.
- [28] Pereira D. Analysis and Optimization of Continuous Variables Quantum Cryptographic Systems. Instituto de Telecomunicações: Universidade de Aveiro; 2023.
- [29] Hillery M. Quantum cryptography with squeezed states. *Phys Rev A.* 2000 Jan;61:022309. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.61.022309>.
- [30] Ralph TC. Continuous variable quantum cryptography. *Phys Rev A.* 1999 Dec;61:010303. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.61.010303>.
- [31] Kanitschar F. Finite-size Security Proof for Discrete-Modulated CV-QKD Protocols. TU Wien and University of Waterloo; 2022.
- [32] Glosser. Bloch Sphere; 2012. United States Patent 4,405,829. Wikimedia. Available from: https://commons.wikimedia.org/wiki/File:Bloch_Sphere.svg.
- [33] Ekert AK, Huttner B, Palma GM, Peres A. Eavesdropping on quantum-cryptographical systems. *Phys Rev A.* 1994 Aug;50:1047-56. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.50.1047>.
- [34] Weier H, Krauss H, Rau M, Fürst M, Nauerth S, Weinfurter H. Quantum Eavesdropping without Interception: An Attack Exploiting the Dead Time of Single Photon Detectors. *New Journal of Physics - NEW J PHYS.* 2011 07;13.
- [35] Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. *Rev Mod Phys.* 2020 May;92:025002. Available from: <https://link.aps.org/doi/10.1103/RevModPhys.92.025002>.
- [36] Ben-Or M, Horodecki M, Leung D, Mayers D, Oppenheim J. The Universal Composable Security of Quantum Key Distribution; 2005. p. 386-406.
- [37] Lo HK, Chau H. Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances. *Science.* 1998 03;283.
- [38] Shor PW, Preskill J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys Rev Lett.* 2000 Jul;85:441-4. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.85.441>.
- [39] Lütkenhaus N. Security against individual attacks for realistic quantum key distribution. *Physical Review A.* 1999 10;61.

Bibliography

- [40] Rusca D, Boaron A, Curty M, Martin A, Zbinden H. Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol. *Phys Rev A*. 2018 Nov;98:052336. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.98.052336>.
- [41] Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H. Finite-key analysis for the 1-decoy state QKD protocol. *Appl Phys Lett*. 2018;112.
- [42] Lo HK, Preskill J. Phase randomization improves the security of quantum key distribution. *arXiv: Quantum Physics*. 2005 05. Available from: <https://api.semanticscholar.org/CorpusID:119058314>.
- [43] Cao Z, Zhang Z, Lo HK, Ma X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New Journal of Physics*. 2015 05;17.
- [44] Wang XB. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys Rev Lett*. 2005 Jun;94:230503. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.94.230503>.
- [45] Lo HK, Ma X, Chen K. Decoy State Quantum Key Distribution. *Phys Rev Lett*. 2005 Jun;94:230504. Available from: <https://link.aps.org/doi/10.1103/PhysRevLett.94.230504>.
- [46] Attema T, Bosman J, Neumann N. Optimizing the decoy-state BB84 QKD protocol parameters. *Quantum Information Processing*. 2021 04;20.
- [47] Ma X, Qi B, Zhao Y, Lo HK. Practical decoy state for quantum key distribution. *Phys Rev A*. 2005 Jul;72:012326. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.72.012326>.
- [48] Fung CHF, Lo HK. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. *Phys Rev A*. 2006 Oct;74:042342. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.74.042342>.
- [49] Wang LJ, Chen LK, Ju L, Xu ML, Zhao Y, Chen K, et al. Experimental multiplexing of quantum key distribution with classical optical communication. *Applied Physics Letters*. 2015 02;106(8):081108. Available from: <https://doi.org/10.1063/1.4913483>.
- [50] Xilinx; 2023. Available from: <https://www.xilinx.com/>.
- [51] Einstein A. Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt. *Annalen der Physik*. 1905;322(6):132-48. Available from: <https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19053220607>.
- [52] Walenta N, Burg A, Caselunghe D, Constantin J, Gisin N, Guinnard O, et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New Journal of Physics*. 2014 jan;16(1):013047. Available from: <https://dx.doi.org/10.1088/1367-2630/16/1/013047>.

- [53] Fung CHF, Ma X, Chau HF. Practical issues in quantum-key-distribution postprocessing. *Phys Rev A*. 2010 Jan;81:012318. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.81.012318>.
- [54] Lim CCW, Curty M, Walenta N, Xu F, Zbinden H. Concise security bounds for practical decoy-state quantum key distribution. *Phys Rev A*. 2014 Feb;89:022307. Available from: <https://link.aps.org/doi/10.1103/PhysRevA.89.022307>.
- [55] Wei K, Li W, Tan H, Li Y, Min H, Zhang WJ, et al. High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics. *Phys Rev X*. 2020 Aug;10:031030. Available from: <https://link.aps.org/doi/10.1103/PhysRevX.10.031030>.
- [56] Wootters WK, Zurek WH. Single quantum cannot be cloned. *Nature*. 1982 Oct;299.

A. Appendix

A.1. The No-Cloning Theorem

The following proof follows closely the proof from [56] (1982). This is a proof by contradiction and simply exploits the linearity of quantum operators.

Theorem 1. *No arbitrary unknown quantum state can be copied or cloned.*

Proof. Let be $|\psi\rangle, |b\rangle \in \mathcal{H}$, two quantum states living both in the Hilbert space \mathcal{H} . Assume now the existence of a linear cloning operator¹ \hat{C} , which is able to copy the state $|\psi\rangle$ onto the blank state $|b\rangle$,

$$\hat{C}(|b\rangle \otimes |\psi\rangle) = |\psi\rangle \otimes |\psi\rangle. \quad (\text{A.1})$$

Without loss of generality, $|\psi\rangle$ is decomposable into some basis $\{|\psi_i\rangle\}$ and can be written as a linear combination of these basis states: $|\psi\rangle = \sum_i a_i |\psi_i\rangle$, with $a_i \in \mathbb{C}$. One should therefore get on the one hand

$$\hat{C}(|b\rangle \otimes |\psi\rangle) = |\psi\rangle \otimes |\psi\rangle = \sum_j a_j |\psi_j\rangle \otimes \sum_i a_i |\psi_i\rangle = \sum_{i,j} a_i a_j (|\psi_j\rangle \otimes |\psi_i\rangle), \quad (\text{A.2})$$

but on the other hand,

$$\begin{aligned} \hat{C}(|b\rangle \otimes |\psi\rangle) &= \hat{C}\left(|b\rangle \otimes \sum_i a_i |\psi_i\rangle\right) \\ &= \sum_i a_i \hat{C}(|b\rangle \otimes |\psi_i\rangle), \\ &= \sum_i a_i (|\psi_i\rangle \otimes |\psi_i\rangle) \end{aligned} \quad (\text{A.3})$$

where linearity was exploited.

However, cloning the arbitrary state $|\psi\rangle$ leads to a contradiction upon comparison of the result obtained in Eq.(A.2) and Eq.(A.3), since $\sum_{i,j} a_i a_j (|\psi_j\rangle \otimes |\psi_i\rangle) \neq \sum_i a_i (|\psi_i\rangle \otimes |\psi_i\rangle)$, for any arbitrary state. Therefore, no cloning operator \hat{C} exists. \square

¹In quantum mechanics, the (time) evolution of quantum states, or observables, is described by unitary transformations, and these are linear.

A.2. Algorithm - Plateau Analysis in Step Signal

The algorithm utilized for characterizing modulation levels in the phase and amplitude modulator is outlined below. These "levels" correspond to the flat segments observed in the step signal.

The algorithm applied on the measured signal V operates as follows: First, V is sorted, resulting in \tilde{V} . This is crucial since V may address certain levels multiple times but at different instances. This sorting not only smoothens out the levels but also arranges them in a monotonically ascending order. Second, \tilde{V} is hashed into subarrays of varying sizes, some containing the levels and others containing the rising segments of \tilde{V} . These respective subarrays, a , were generated according to the following procedure: The initial subarray starts at the beginning of \tilde{V} and contains only the first element. The subarray grows iteratively, by appending the next element in \tilde{V} , until a stop criterion is met. In this case, a is considered complete, and a new subarray is initiated, containing the last non-appended element. This process is repeated until \tilde{V} is entirely hashed into subarrays. The stop criterion is triggered, if the next value is outside the threshold $s = \min(\text{STD}(s), k)$, where k is some predefined value, set to 2% of V_π (= half of the period of transfer function G).

Third and finally, subarrays a composed of a sufficient number of samples are retained, while others are discarded. This step is done because a subarray without enough samples cannot adequately represent a modulation level. This method resulted in three or eight subarrays, respectively, each comprising values corresponding to a distinct modulation level.

A.3. Calculation of the SKR

This section presents the implemented formulas for the calculation of the SKR. As outlined thoroughly, the QKD protocol is a three-state BB84 type with the one-decoy method. The derivation for the calculation of the SKR can be found in Rusca et al. [41]. Rusca's security proof follows the finite key analysis as in [54], which was presented for the two-decoy variant.

The upper bound for the secret key length l , cf. Eq. (4.8), is given by

$$l \leq s_{Z,0}^l + s_{Z,1}^l (1 - h(\phi_{Z,1}^u)) - \lambda_{\text{EC}} - 6 \log_2(19/\epsilon_{\text{sec}}) - \log_2(2/\epsilon_{\text{cor}}), \quad (\text{A.4})$$

with $s_{Z,0}^l$ and $s_{Z,1}^l$ representing the lower bounds of the vacuum and single photon events in the Z basis respectively, and $\phi_{Z,1}^u$ denoting the upper bound of the phase error of the single photon events in the Z basis. These quantities are calculated from measurable quantities acquired from the experiment. As expressed in the main text, $h(\cdot)$ is the binary entropy, cf. Eq. (4.9).

Let's denote, by $n_{B,k}$, $m_{B,k}$ the number of observed events and the number of errors in the basis B for the intensity level $k \in \{\mu_1, \mu_2\}$. The used notation in this section differs slightly from the one used in the rest of the thesis, this is to ensure on the one hand a more compact and consistent formulation of the formulas and on the other hand a better

A.3. Calculation of the SKR

comparability with the source [41]. Furthermore, $n_{B,k}^\pm$ and $m_{B,k}^\pm$ denote the finite-key corrections of $n_{B,k}$ and $m_{B,k}$ respectively. They are calculated with

$$n_{B,k}^\pm = \frac{e^k}{p_k} \left(n_{B,k} \pm \sqrt{\frac{n_B}{2} \log \epsilon^{-1}} \right), \quad (\text{A.5})$$

idem for $m_{B,k}$, with p_k being the probability to prepare a pulse with $\mu = k$ (in the main text, these probabilities were denoted by p_s and p_d) and \log the natural logarithm. The total number of detection events in basis B is $n_B = n_{B,\mu_1} + n_{B,\mu_2}$. The parameter ϵ is the security parameter describing with which probability the observed statistics differ from the asymptotic case, i.e. the finite-key approximation.

The lower bound on the single photon contributions is calculated with

$$s_{Z,0}^l = \frac{\tau_0}{\mu_1 - \mu_2} \left(\mu_1 n_{Z,\mu_2}^- - \mu_2 n_{Z,\mu_1}^+ \right), \quad (\text{A.6})$$

with τ_n the probability of generating a n photon state, i.e. in this case a vacuum state. Having only two intensity levels, τ_n is easily calculated from the Poisson distribution Eq. (2.19) and the generation probabilities with

$$\tau_n = \sum_{k=\{\mu_1, \mu_2\}} p_k \frac{k^n e^{-k}}{n!}. \quad (\text{A.7})$$

The main contribution to the secret key comes from the single photon detection events, it is computed with

$$s_{Z,1}^l = \frac{\tau_1 \mu_1}{\mu_2 (\mu_1 - \mu_2)} \left(n_{Z,\mu_2}^+ - \frac{\mu_2^2}{\mu_1^2} n_{Z,\mu_1}^+ - \frac{(\mu_1^2 - \mu_2^2)}{\mu_1^2 \tau_0} s_{Z,0}^u \right), \quad (\text{A.8})$$

with $s_{Z,0}^u$ the upper bound on the contribution of vacuum events, which is calculated in this implementation with

$$s_{Z,0}^u = 2 \left(\tau_0 \frac{e^k}{p_k} \left(m_{Z,k} + \sqrt{\frac{1}{2} m_Z \log(1/\epsilon_1)} + \sqrt{\frac{1}{2} n_Z \log(1/\epsilon_1)} \right) \right). \quad (\text{A.9})$$

The phase error rate is estimated with

$$\phi_{Z,1}^u = \frac{v_{X,1}^u}{s_{X,1}^l} + \gamma \left(\epsilon_{\text{sec}}, \frac{v_{X,1}^u}{s_{X,1}^l}, s_{X,1}^l, s_{Z,1}^l \right), \quad (\text{A.10})$$

where $v_{X,1}^u$ describes the upper bound of error events in the X basis from the single-photon states, $s_{X,1}^l$ is the X basis analog to Eq. (A.8). The ominous γ function is

$$\gamma(a, b, c, d) = \sqrt{\frac{(c+d)(1-b)b}{cd \log 2} \log \left(\frac{(c+d) 21^2}{cd(1-b)a^2} \right)}, \quad (\text{A.11})$$

and takes a security parameter ϵ_{sec} . The term $v_{X,1}^u$ is calculated with

$$v_{X,1}^u = \frac{\tau_1}{\mu_1 - \mu_2} \left(m_{X,\mu_1}^+ - m_{X,\mu_2}^- \right). \quad (\text{A.12})$$