Department of Physics and Astronomy
Heidelberg University

Bachelor Thesis in Physics
submitted by

Lea Bauer

born in Esslingen am Neckar (Germany)

April 2024

Performance and Error Analysis of Quantum Key Distribution Chip through Simulation

This Bachelor Thesis has been carried out by Lea Bauer at the
Kirchhoff-Institute for Physics in Heidelberg
under the supervision of
Prof. Dr. Wolfram Pernice

Abstract

Quantum Key Distribution (QKD) provides a robust solution to the security challenges posed by emerging quantum computers to traditional cryptographic systems. It enables the generation of secure and random cryptographic keys, safeguarding both current and future communications.
This thesis focuses on the development and analysis of a Monte Carlo simulation of an experimental realisation of a fully integrated photonic system employing three-state BB84 QKD protocol using time-bin encoding, alongside the implementation of the one-decoy state method. By incorporating hardware-specific parameters, the simulation replicates laboratory settings and allows for adjustment of the components. Therefore it can be utilized to optimize hardware settings to achieve a high secret key rate.
A first analysis is done by testing the influence of the attenuation on the secret key rate. With the current assumptions, the system can safely transmit secret keys for transmission distances of up to 100 km. Additionally, the impact of the variance of the wavelength stability on the secret key rate was found to be insignificant below variances in the heater voltage of 5.5 mV. The peak-to-peak modulation extinction ratios at 16.7 dB and 20.7 dB were analyzed, showing no clear trend in the secret key rate performance.

Zusammenfassung

Die Quanten-Schlüsselverteilung (Quantum Key Distribution, QKD) bietet eine robuste Lösung für die Sicherheitsprobleme, die durch aufkommende Quantencomputer für klassische kryptografische Systeme entstehen. Sie ermöglicht die Erzeugung sicherer und zufälliger kryptografischer Schlüssel und schützt so sowohl aktuelle als auch zukünftige Kommunikation.
Diese Arbeit beschäftigt sich mit der Entwicklung und Analyse einer Monte-Carlo-Simulation einer experimentellen Realisierung eines vollständig integrierten photonischen Systems, das das Drei-Zustand-BB84-Protokoll mit Zeitbin-Codierung sowie die One-Decoy-State-Methode verwendet. Durch die Einbeziehung hardwarespezifischer Parameter bildet die Simulation Laborbedingungen nach und erlaubt die gezielte Anpassung einzelner Komponenten. Dadurch kann sie verwendet werden, um Hardware-Einstellungen zu optimieren und eine möglichst hohe Secret-Key-Rate zu erzielen.
Eine erste Analyse erfolgte durch Untersuchung des Einflusses der Dämpfung auf die Secret-Key-Rate. Unter den aktuellen Annahmen kann das System sichere Schlüsselübertragungen über Distanzen von bis zu 100 km gewährleisten. Darüber hinaus wurde festgestellt, dass die Varianz der Wellenlängenstabilität bei Heizspannungs-Variationen unter 5,5 mV keinen signifikanten Einfluss auf die Secret-Key-Rate hat. Die analysierten Modulations-Auslöschungsverhältnisse (Extinction Ratios) von 16,7 dB und 20,7 dB zeigten keinen klaren Trend im Hinblick auf die Secret-Key-Rate.

Contents

Chapter 1

Introduction

In an increasingly interconnected world, secure communication is of critical importance. The field of cryptography has long sought to provide this security, in order to enable confidential communication between parties by preventing unauthorized access to messages. A variety of encryption methods has been developed over the years, each with its own strengths and weaknesses. However, many of these methods have, at some point, been compromised. In 1917, the one-time pad was invented, with its biggest advantage of it being theoretically unbreakable. Shannon later proved in 1949 that no encryption method can achieve security with a key shorter than the message itself, making the one-time pad optimal [1].

In cryptography, the two communicating honest parties are called Alice and Bob. Alice is assumed to want to transmit a secret message m of n bits to Bob. Using the one-time pad, Alice encrypts m by adding a key k of n bits to it, resulting in the encrypted message $m_e = m \oplus k$. Alice and Bob possess the key k, which allows Bob to decrypt m_e by adding k again, leaving Bob with $m_e \oplus k = m \oplus k \oplus k = m$. The security of the one-time pad is guaranteed as long as the key is used only once and is equal in length to the message [**Grasselli˙buch˙Quantum˙cryptography**]. The central challenge lies in securely distributing the key k to Alice and Bob.

Classical cryptography addresses this challenge by relying on assumptions about the adversary's computational power. It depends on the computational difficulty of certain mathematical problems, meaning that the schemes can be broken, but only with a substantial amount of power. Therefore, a security parameter can be set to a value, namely the amount of computational power needed to break the encryption, which must be more than what one thinks is available to an adversary. This value can be adjusted when the adversary's potential computational power increases with the advancement of technology. An example of such a problem that is deemed difficult to solve is the factorization of large numbers. In 1994 Peter Shor discovered that large numbers can be factorized in polynomial time assuming that one can make coherent manipulations on a lot of qubits [1]. However,

the rapid advancement of quantum computing threatens the security of current cryptographic systems [2]. This requires safe ways of key distribution and one way to do this is by utilizing quantum physics.
Quantum Key Distribution (QKD) is a specific task of quantum cryptography in which Alice and Bobestablish a shared secret key when connected by an insecure quantum channel and an authenticated public classical channel. The security of QKD originates in the fundamental principles of quantum physics. One argues that any adversary has to perform a measurement on some quantum state to gather any information, but a measurement always modifies the state of the measured system. Additionally, the states of Alice and Bob also cannot be copied as this is forbidden by the no-cloning theorem. The secret key can then be used with a one-time pad to ensure unconditionally secure communication, thus ensuring security without imposing restrictions on the power of the adversary. Theoretically, any quantum system can be used to implement quantum computing; however, employing light is the only practical choice for QKD as Alice and Bob are separated physically, so the quantum states need to be transmitted over distant locations without decoherence. One can achieve that with light as it does not easily interact with matter. A major issue with light is losses, as light scatters, which bounds the amount of keys that can be transmitted per second. Further, losses may lead to leakage of information, but this can be dealt with by adjusting the protocol used. [1]
This thesis explores the use of QKD to address the security challenges posed by advances in quantum computing. Specifically, it focuses on the development of a digital twin simulation of a three-state BB84-QKD-protocol. This protocol employs the one-decoy method and time-bin encoding, utilizing a 1550nm laser. The simulation models an on-chip implementation, featuring a sender and a receiver chip connected by an optical fiber on an Indium Phosphide substrate. Simulating the experimental setup enables including variances, which are difficult to calculate analytically and challenging to measure directly.
The thesis is organized as follows: Chapter 2 introduces the theory of QKD and the specific protocol used. Chapter 3 describes the simulation method, focusing on the implementation of components like the laser, Electro-Absorption Modulator, Delay Line Interferometer, detectors, and classification. Chapter 4 presents the simulation results, which are summarized in Chapter 5, along with an outlook on potential simulation improvements.

Chapter 2

Theory

2.1 Quantum Key Distribution

This chapter outlines the concept of Quantum Key Distribution, based on the first proposed QKD protocol by Bennett and Brassard [3]. Then, the specific implementation is explained and security aspects are discussed. The chapter concludes with an overview of the final simulation output parameters and how to evaluate them.

2.2 BB84 Protocol

The goal for this simulation is long-distance QKD, or discrete variable QKD (DV-QKD). This means that we rely on discrete observables like the polarization or discrete time-bins for encoding the information, and each bit of the key is transmitted by exactly one photon, which is prepared to span a set of different quantum states belonging to a two-dimensional Hilbert space $\mathcal{H}_2$. The alternative would be continuous variable QKD (CV-QKD). Here, field observables are used to encode the information [4].
There are several reasons, why we use DV-QKD instead of CV-QKD. Firstly, with CV-QKD it is more complex to analyze the security of the protocol. Secondly, because of the kind of detectors used, CV-QKD is far more susceptible to noise, which makes it difficult to extract a key over long distances, while for DV-QKD the error rate stays about constant with respect to losses. The constant error rates are due to the fact that in CV-QKD every measurement counts towards the final key calculation and in DV-QKD no detection events can simply be discarded.
One way to achieve the transmission of a key is a prepare-and-measure protocol. A quantum state is prepared by the sender Alice, sent in an optical fiber, and then measured by the receiver Bob.

As described in [5, pp. 92-95], in a standard prepare-and-measure protocol Alice and Bob have access to two channels: A quantum channel, where Alice can send Bob the quantum states she prepared, and an authenticated classical channel, where Alice and Bob can send classical messages. An eavesdropper, commonly called Eve, is able to listen in on the classical channel, but cannot change any messages being sent. In addition to that, she can interact with the quantum channel with no restrictions other than the laws of physics. This is shown in 2.1.

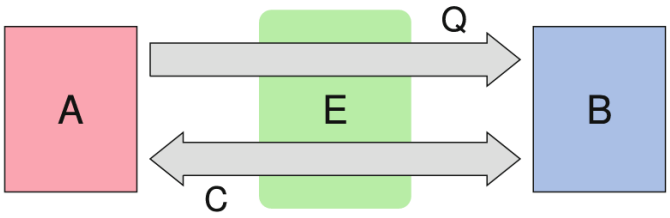


Figure 2.1: A schematic depicting the standard quantum key distribution (QKD) protocol. Alice (A) transmits quantum states to Bob (B) via a quantum channel (Q). They then use a classical channel (C) to coordinate their measurements and distill a shared secret key. Eve (E) may intercept and measure quantum transmissions and listen to classical communication in her attempt to gain information. Figure from [5, p.92]

The BB84 protocol is a well-established prepare-and-measure protocol that was suggested in 1984, making it the first protocol for quantum cryptography [1]. Each bit of the key is transmitted by exactly one photon, which is in a quantum state beloning to $\mathcal{H}_2$. For this to work, we need to prepare the photons to be in a pure qubit state, which can be described as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.2.1}$$

with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2+|\beta|^2 = 1$ [5, p. 19]. The qubit state is in a two-dimensional Hilbert space $\mathcal{H}_2$ with orthonormal basis states $|0\rangle$ and $|1\rangle$. The qubit can be any superposition of these two basis states. This basis is called the computational basis, whose basis vectors one can use to construct a mutually unbiased basis (MUB) to the computational basis. With two MUBs, a state prepared in one MUB will behave completely random and lose all its stored information when measured in another MUB. [5, p. 9] The easiest way to do this is to add and subtract the two basis vector resulting in four possible states:

$$|\psi_{Z_0}\rangle_A = |0\rangle_A \qquad |\psi_{Z_1}\rangle_A = |1\rangle_A \tag{2.2.2}$$

$$|\psi_{X_+}\rangle_A = \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right) \qquad |\psi_{X_-}\rangle_A = \frac{1}{\sqrt{2}}\left(|0\rangle_A - |1\rangle_A\right) \tag{2.2.3}$$

The BB84 protocol involves four main stages:

1. Quantum State Preparation: Alice prepares a sequence of $4n$ symbols. For each symbol i, she randomly chooses a bit $a_i \in \{0, 1\}$ and a basis $b_i \in \{0, 1\}$ (where 0 corresponds to the Z-basis and 1 to the X-basis). The prepared state $|\psi_{a_i b_i}\rangle_A$ is determined by these choices by convention (see Table 3.1 to look up the convention). The overall state sent by Alice is the composite system:

$$|\psi\rangle_A = \bigotimes_{i=1}^{4n} |\psi_{a_i b_i}\rangle_A, \tag{2.2.4}$$

   This quantum state is then transmitted through a quantum channel (Q).

2. Quantum Transmission and Measurement: The quantum channel, denoted by the operator $\mathcal{E}$, can be affected by Eve's eavesdropping attempts and inherent channel losses. Bob receives the state $\mathcal{E}(|\psi\rangle_A\langle\psi|)$ and acknowledges the reception via a classical channel (C). Bob independently chooses a random basis $b'_i \in \{0, 1\}$ for each received qubit and measures it in the chosen basis, obtaining a measurement outcome $a'_i \in \{0, 1\}$. Bob records these results in a classical bit string $a'_i = (a'_1, a'_2, ..., a'_{4n})$.

3. Sifting and Parameter Estimation: Alice announces her choice of basis b over the classical channel. Alice and Bob then compare their basis choices b and b'. They discard all the bits where $b_i \neq b'_i$ This sifting process leaves them with approximately $2n$ correlated bits. From these remaining bits, they use a subset of n bits for parameter estimation to assess the error rate in the quantum transmission, which can indicate Eve's presence. If the error rate exceeds a certain threshold, the protocol is aborted.

4. Classical Post-Processing: If the error rate is acceptable, Alice and Bob proceed with classical post-processing on the remaining n bits. This involves:

   - Error Correction: They apply error correction techniques to ensure their remaining bit strings a and a' become identical.
   - Privacy Amplification: They use privacy amplification methods to reduce Eve's potential information about their shared key, resulting in a shorter, more secure secret key of length $m < n$. This step often assumes the worst-case scenario where all observed errors are attributed to Eve's eavesdropping. [5, p. 108]

2.3 Three-State BB84 protocol

In the Three-State BB84 protocol, only the following states are utilized:

$$|\psi_0\rangle_A = |0\rangle_A \qquad |\psi_1\rangle_A = |1\rangle_A \tag{2.3.1}$$

$$|\psi_+\rangle_A = \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right) \tag{2.3.2}$$

In addition to this change, only the Z-basis states are used for the key generation and the X-basis is used for channel estimations to assess the overall characteristics of the communication channel, including loss, noise, and other imperfections. The unconditional security of the three-state protocol has been proven for the case of a single photon source and for the case of a phase-randomized coherent-state source under the condition that the decoy state method is used [6]. This will be explained in the next section.

2.4 Basis Implementation: time-bin QKD

Since the goal is long-distance QKD, working with single-mode fibers is preferred, as there are already existing and widespread fiber networks. Other types of encoding scheme like polarization encoding struggle with polarization drift which makes long-distance transmission more difficult. Single-mode fibers keep the shape of the light fairly stable, which is especially useful for time-bin encoding [7]. The lower the loss, the better it is suited for the protocol. Ultra-low loss fibers are preferred, but they are not as readily available as the standard fiber, which is what is available to the lab.

Instead of single photon sources weak coherent pulse lasers can be used. These have a few drawbacks, but more on that in Section 2.5. Weak coherent pulses can be described as:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.4.1}$$

where $\alpha \in \mathbb{C}$ and $|n\rangle$ a number state. $|n\rangle$ is a Fock state that represents the quantum state where the pulse contains n photons. Note that here $|0\rangle$ and $|1\rangle$ do not describe the orthonormal basis states of the computational basis [5, p. 131].

In time-bin encoding the basis states, $|0\rangle$ and $|1\rangle$ are encoded with early and late time-bins. This can be mathematically described by

$$|\psi_0\rangle = |\alpha\rangle_{\mathrm{E}} |0\rangle_{\mathrm{L}} \tag{2.4.2}$$
$$|\psi_1\rangle = |0\rangle_{\mathrm{E}} |\alpha\rangle_{\mathrm{L}} \tag{2.4.3}$$
$$|\psi_+\rangle = |\alpha\rangle_{\mathrm{E}} |0\rangle_{\mathrm{L}} + |0\rangle_{\mathrm{E}} |\alpha\rangle_{\mathrm{L}} \tag{2.4.4}$$

where $|\alpha\rangle$ is a coherent state as defined above [8].
Assuming the phase is unknown or totally randomized, the probability distribution for the number of photons in a state follows a Poisson distribution.

$$\rho = \sum_{n=0}^{\infty} P(n)|n\rangle\langle n| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!}|n\rangle\langle n| \tag{2.4.5}$$
$$P(n) = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} \tag{2.4.6}$$

Here $|\alpha|^2 = \mu$ describes the mean photon number in the signal [9, p. 132].

2.5 PNS-attack and One-Decoy State Method

In the BB84 protocol, it is assumed that single-photon sources are used, but suitable deterministic single-photon sources are not available yet. [10] states that experiments with a handful of photons are possible with single-photon sources and experiments with more than 15 imaginable. 15 is far from what would be needed for a QKD experiment, which is why weak coherent sources are used in practical quantum cryptography systems [11]. These have inherent imperfections, such as the probability of emitting multi-photon pulses which can be used by the eavesdropper Eve to perform the photon-number-splitting (PNS) attack. Here Eve blocks all single-photon pulses, keeps one of the photons from the multi-photon state and send the rest of the multi-photon photons to Bob. Now, under the right conditions and after the basis choices are announced by Alice and Bob, Eve could get the entire final key [12].
To illustrate this, here is a more concrete example: We assume the probability of the emission of a pulse containing multiphotons to be $p_{multi} = 10\%$ and the yield (the photons making it through the setup from sender to detector) $y = 10\%$. In addition, we assume that Bob uses a detector insensitive to photon numbers and that Eve has unlimited technological and computational power. This means that Eve can use every multiphoton pulse and use it for the PNS attack. On the one hand, Bob now observes that only 10% of photon pulses arrive at his detector, as he would expect. On the other hand, Eve can now get full information about the key by measuring all the photons she kept in the announced basis. If the yield y

is less than the probability of multiphotons in a pulse p_{multi}, then the scheme is totally insecure [13].
This framework is developed under the premise that loss is an inherent feature of practical BB84 QKD. The PNS attack has been experimentally demonstrated with a slightly modified version based on a beam splitter, which shows the practical danger of this attack and the need for a countermeasure [14]. This can be found in the decoy-state model. The only thing that changes to the three-state protocol is that we introduce decoy and signal states, which have different mean photon numbers. This means that we now have six possible states:

$$|\psi_{11,s}\rangle_A = |0\rangle_A \quad |\psi_{10,s}\rangle_A = |1\rangle_A \quad |\psi_{01,s}\rangle_A = \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right)$$
$$|\psi_{11,d}\rangle_A = |0\rangle_A \quad |\psi_{10,d}\rangle_A = |1\rangle_A \quad |\psi_{01,d}\rangle_A = \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right)$$

The subscript d stands for the decoy states and the subscript s for signal states. It is assumed that Eve cannot differentiate between the signal and the decoy state, so by doing a PNS attack, she would change the photon number in signal and decoy pulses, which in turn would change the yield and the error rate of the decoy states. These then affect the estimation of the single-photon detection gain and the error rate in signal states. In [8], good results were achieved when the following relation held: $\mu_s = \mu_d \cdot 2$. This is adopted in the following tests. The higher the mean photon number, the more it can interfere with the dead time of the detector, but if the mean photon number is too low only very little photons can be measured. Typical values that where used in [8] were $\mu_s = 0.06$, $\mu_s = 0.25$ or $\mu_s = 0.39$.
Originally, the decoy state method was proposed with infinitely many decoy intensities. One can also choose to implement two different decoy intensities (called the two-decoy method) or only one decoy-intensity (called one-decoy method). It has been shown that for practical block sizes of up to 10^8 bits that the one-decoy protocol achieves higher secret key rates than the two-decoy method for almost all experimental settings. In addition, it is also easier to implement, which is why it was chosen here [11].

2.6 Simulation Output

To precisely evaluate the security of Quantum Key Distribution (QKD), the calculation of the Secret Key Rate (SKR) is essential. This calculation requires various input values, such as the Quantum Bit Error Rate (QBER). However, since the experimental realization of QKD systems deviates from idealized assumptions, the simulation of events is necessary to account for these real-world conditions and

to determine an accurate SKR. The protocol chosen here follows the protocol description in [15]. When Bob randomly measures in one basis, he can measure the possible outcomes $\{0, 1, \emptyset, \perp\}$, where 0 and 1 are the bit values and $\emptyset$ and $\perp$ are the no-detection and double-detection events. If Bob measures one of the first three outcomes he assignes what he observes to his value string, but for a double-detection he assigns a random bit value to his value string. Events where there is a photon measured in the X-basis and in the Z-basis are discarded, as in the protocol Bob is only able to choose one basis to measure the photons.
In the next step called "basis reconciliation", Alice and Bob publicly announce their basis and whether the state is a decoy or a signal state over the authenticated channel. Now, after all basis are announced certain symbols can be grouped into sets. For the simulation, the four sets where the basis that is used to encode the bit and the one used to measure the bit are the same and the intensities are the same.

$$X_k = \{i : a_i = b_i = X \wedge k_i = k \wedge y_i = \emptyset\} \tag{2.6.1}$$

$$\text{and} \quad Z_k = \{i : a_i = b_i = Z \wedge k_i = k \wedge y_i = \emptyset\} \quad \forall k \in K, \tag{2.6.2}$$

where $k \in \{\mu_s, \mu_d\}$. Then, they check if they have collected enough detection events for every basis and intensity to gain sensible results. For example, the resulting key has to be big enough to encrypt the message. The concrete numbers depend on how the security parameters are chosen, but more on that later. If the condition is not satisfied the protocol is repeated up until.
The last step before the symbols can be post-processed is to determine the erroneous bits. When one strictly follows the protocol, one now has to use certain error correction schemes. In the simulation there are three cases that are detected as errors:

1. Measuring in Z-basis: Detection in late time-bin for Z_0 symbol sent.

2. Measuring in Z-basis: Detection in early time-bin for Z_1 symbol sent.

3. Measuring in the X-basis: Detection in late time-bin for X_+ symbol sent.

In all 3 cases the there shouldn't be a detection possible. The late time-bin of an X_+ symbol should always be empty because with the X-basis the destructive interference is measured. This can be seen in Figure 2.2, as the second time bin of the X_+ symbol is empty, the early time bin of the Z_0 symbol is empty and the late time bin of the Z_1 symbol is empty.

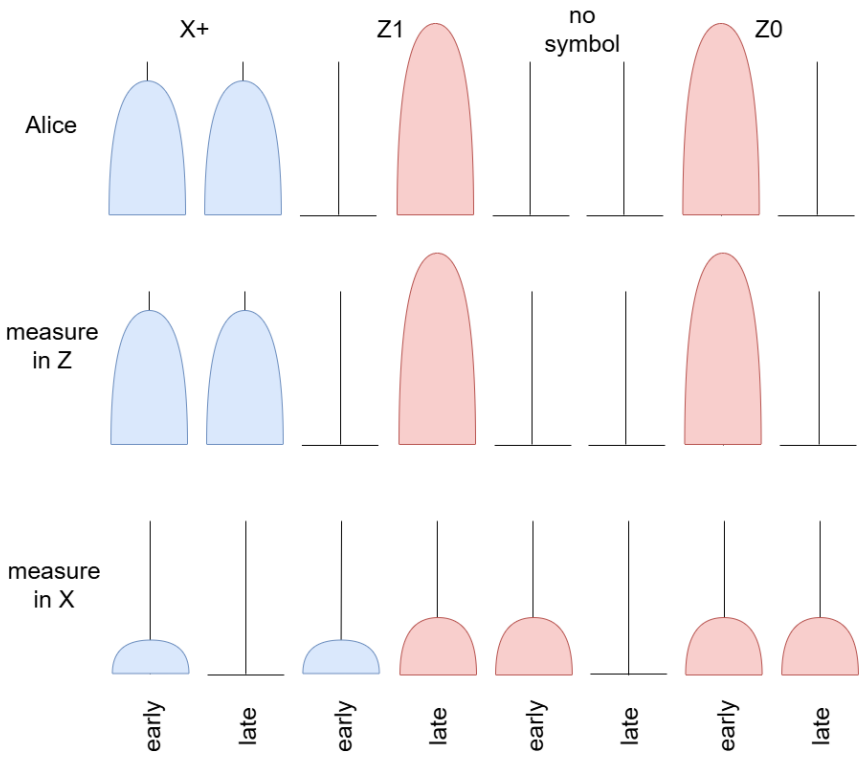


Figure 2.2: This figure pictures the measurement outcomes of perfectly prepared and measured states. Alice sends states and Bob measures them in either the Z or X basis. The results of Bob's measurements are dependent on the basis he chooses. The "no photon state" is just there for illustration purposes to prevent interference between the $Z1$ and the Z_0 state. It is not sent in the protocol.

This can again be done for decoy and signal states and the two bases, so four errors can be calculated. In total, together with the four diffferent measurements, we get eight quantities: $n_{Z,s}$, $n_{Z,s}$, $n_{Z,d}$, $n_{X,s}$, $m_{X,d}$, $m_{Z,d}$, $m_{X,s}$, $m_{X,d}$.
The number of observed events and the number of errors in the basis B for the intensity level $k \in \{\mu_s, \mu_d\}$ is denoted by $n_{B,k}$ and $m_{B,k}$. It is important to know that normally this has to be done without the knowledge of the value of the symbols as only the bases are communicated, but as this is a simulation the information was already available so it is easiest to do it this way.
Now, the results from the simulation can be calculated. For the QKD-chip that is replicated here, several parameters are of interest.
One of these is the QBER rate, which here is defined as the error rate of Alice's and Bob's bit strings on which the same quantum measurement is performed. This is shown in the supplementary material of [11].

$$QBER_{B,k} = \frac{m_{B,k}}{l_{B,k}} \tag{2.6.3}$$

$l_{B,k}$ is the number of prepared states in basis B and intensity k. One example of a pair of symbols that would count into the QBER is a state where both Alice and Bob measured in the Z-basis and Alice sent a Z_0 and Bob measured a Z_1 state. The QBER can be given for every intensity that photons are sent in and for signal and decoy states separately. Sometimes the QBERs for the decoy states are called phase error rates.
In the following, the calculation of the Secret Key Rate (SKR) is discussed. This consists of the repetition rate R of the key generating source, the secret key length l and is the total bit sequence length N.

$$SKR = R\frac{l}{N_{tot}} \tag{2.6.4}$$

The repetition rate being the symbol repetition rate, R is the number of symbols being sent per second. Because the total bit sequence length N_{tot} is also known, only the secret key length l has to be calculated. The finite-key effect are taken into account in the secret key length l. This formula can be taken from the supplementary material of [11].
This is done in Rusca et al. [11] which shows a security proof for the three state BB84 with a one-decoy method. This security proof follows the protocol for the two-decoy method in [15] closely, but adapted for the one-decoy method. An upper bound for the secret key length l is given by

$$l \leq s^l_{Z,0} + s^l_{Z,1}\left(1 - h\left(\phi^u_{Z,1}\right)\right) - \lambda_{\mathrm{EC}} - 6\log_2\left(\frac{19}{\epsilon_{\mathrm{sec}}}\right) - \log_2\left(\frac{2}{\epsilon_{\mathrm{cor}}}\right) \tag{2.6.5}$$

with $s^l_{Z,0}$ and $s^l_{Z,1}$ being the lower bounds of the vacuum and single photon events in the Z-basis respectively. The upper bound of the phase error of single photon events in the Z-basis is written as $\phi^u_{Z,1}$. ϵ_{cor} and ϵ_{sec} are correction and secrecy parameters. In the simulation these are chosen the same as in [11]. $h(x)$ is the binary entropy function described by

$$h(x) = -x\log(x) - (1-x)\log(1-x) \tag{2.6.6}$$

Lastly, the only open parameter λ_{EC} is the number of disclosed bits during the error correction phase. This can be estimated by

$$\lambda_{\mathrm{EC}} = f_{\mathrm{EC}} n_{Z,s} h(QBER_{Z,s}) \tag{2.6.7}$$

where f_{EC} is the error correction efficiency (assumed to be 1.19 here, as in [15]), $n_{Z,s}$ denotes the sifted key length from the signal Z basis states and $h(QBER_{Z,s})$ is the binary entropy of the QBER of the Z-basis signal states.
For the calculation of $s^l_{Z,0}$ and $s^l_{Z,1}$ the finite-key corrections are $n^{\pm}_{B,k}$ and $m^{\pm}_{B,k}$ which are for the counts and the errors of the respective bases. They are calculated as follows:

$$n^{\pm}_{B,k} = \frac{e_k}{p_k}\left(n_{B,k} \pm \sqrt{\frac{n_B}{2}\log \epsilon_1^{-1}}\right) \tag{2.6.8}$$

The ϵ_1 presented here is going to be part of ϵ_{sec}, but this will not be discussed further. In [15] ϵ_{sec} is chosen to be $\epsilon_{sec} = 19 \cdot \epsilon_1$ with $\epsilon_{sec} = 10^{-9}$.
The same formula can be used for $m^{\pm}_{B,k}$ if all n's are swapped for m's. Here, p_k with $k \in \{s, d\}$ is the probability to prepare a pulse as a decoy or a signal pulse. n_B is the total number of detection events in basis B. Thus, $n_B = n_{B,\mu_s} + n_{B,\mu_d}$. ϵ_{sec} is the security parameter which describes how the finite case differs from the asymptotic case.
Now, one can describe the lower bound on the vacuum event contributions $s^l_{Z,0}$ as:

$$s^l_{Z,0} = \frac{\tau_0}{\mu_s - \mu_d}\left(\mu_s n^-_{Z,\mu_d} - \mu_d n^-_{Z,\mu_s}\right) \tag{2.6.9}$$

τ_0 is the probability of generating a 0-photon state, or vacuum state. In general, τ_n is the probability of generating a n-photon state.

$$\tau_n = \sum_{k=\{\mu_s,\mu_d\}} p_k \frac{k^n e^{-k}}{n!} \tag{2.6.10}$$

The other lower bound in the calculation is the lower bound of the single detection events:

$$s^l_{Z,1} = \frac{\tau_1 \mu_s}{\mu_d(\mu_s - \mu_d)}\left(n^+_{Z,\mu_d} - \frac{\mu_d^2}{\mu_s^2} n^+_{Z,\mu_s} - \frac{\mu_s^2 - \mu_d^2}{\mu_s^2 \tau_0} s^u_{Z,0}\right) \tag{2.6.11}$$

Here, the upper bound on the contribution of vacuum events $s^u_{Z,0}$ is calculated with

$$s^u_{Z,0} = 2\left(\frac{\tau_0 e_k}{p_k}\left(m_{Z,k} + \sqrt{\frac{m_Z}{2}\log\left(\frac{1}{\epsilon_2}\right)} + \sqrt{\frac{n_Z}{2}\log\left(\frac{1}{\epsilon_1}\right)}\right)\right) \tag{2.6.12}$$

$k \in \{s, d\}$ is true here as well, so k can be chosen freely to refer to s (for signal) or to d (for decoy). Here, it is chosen to be the signal.
The phase error rate $\phi^u_{Z,1}$ is described with

$$\phi^u_{Z,1} = \frac{v^u_{X,1}}{s^l_{X,1}} + \gamma\left(\epsilon_{\text{sec}}, \frac{v^u_{X,1}}{s^l_{X,1}}, s^l_{X,1}, s^l_{Z,1}\right) \tag{2.6.13}$$

$v^u_{X,1}$ is the upper bound of error events in the X-basis from the single-photon states and gets calculated by

$$v^u_{X,1} = \frac{\tau_1}{\mu_1 - \mu_2}\left(m^+_{X,\mu_1} - m^-_{X,\mu_2}\right) \tag{2.6.14}$$

The lower bound of the contribution of single photon events $s^l_{X,1}$ is analogous to Eq. 2.6.11. γ is as follows

$$\gamma(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}\log\left(\frac{12(c+d)^2}{cd(1-b)a^2}\right)} \tag{2.6.15}$$

Now the SKR and the phase error can be calculated.
The gain is defined as

$$g_{B,k} = n_{B,k}/N_{B,k} \tag{2.6.16}$$

where $N_{B,k}$ is defined as the amount of symbols sent in the basis B and with a mean photon number of k.

2.7 Photonics

Conventionally, QKD devices have been built with discrete optical devices that are separately assembled with optical glasses and optical crystals which are then connected via free space or optical fibers. These traditional designs are difficult to make reliable, are costly to scale and not easy to package. In packaging the biggest problems are the high thermal and mechanical stabilities required to combat environmental influences like thermal fluctuations. Those are difficult to achieve in a big discrete optical system. This is where photonic integration plays a crucial role in advancing Quantum Key Distribution (QKD) technology. The systems by themselves are smaller, which makes them easier to package. Additionally, photonic chips are more scalable, because we all components are printed at once rather than being assembeled one by one. Furthermore, photonic chips are more stable. This is because the circuits are built on a solid platform, which minimizes the influence of vibrations or thermal influences. As an added bonus photonic chips can be mass-produced, which can lower the average cost per chip if the amount of chips fabricated is high enough. Integrating components onto a chip allows for the creation of scalable, stable and low cost devices [16].

The key difference is that [17] describes a receiver chip with 4 channels, each with its own laser at a different wavelength, allowing for the secret key rate per channel to be calculated and, under certain circumstances, multiplied by the number of channels. In contrast, this simulation calculates the secret key rate for a single channel.
The platform that the chip is on is made of Indium Phosphide. The choice of platform material is crucial in photonic integration. Indium Phosphide (InP) is a key material system for photonic integrated circuits (PICs), particularly in the 1550 nm wavelength region, which is important for optical fiber communications. InP is unique in its ability to provide a wide range of optical functionalities, making it a preferred choice for monolithic integration, where all photonic devices are integrated on a single chip using a single fabrication process [18]. This monolithic integration simplifies device fabrication and improves performance.

Chapter 3

Methods

3.1 Monte Carlo Simulation

Monte Carlo simulations are widely used to gain more information about how stochastic systems behave as here no exact results with a deterministic algorithm are available. This is done by random sampling to approximate some unknown quantity [19]. Due to the complexity of the examined systems not all physical processes are simulated, but only those that have the greatest impact on the unknown quantity. By varying the starting parameters, one can see how heavily the system relies on each parameter. In addition, variances in the starting parameters can directly be included, which yields results that are more closely tied to the experimental setup that the simulation is trying to replicate. Monte Carlo simulations are not only applicable in this specific case, but also in polarization-frame alignment schemes as in [20] or in multi-mode continuous-variable quantum key distribution, see [21]. An advantage of Monte Carlo simulations is that variations in, e.g., laser power can directly be implemented in the simulation. The resulting secret key rate (basically a parameter evaluating how many bits of key can be transmitted per second) includes detailed information about the physical setup. If one only calculates the secret key rate analytically, one has to assume a model of the physical setup where it is hard to take into account set system parameters like the specific calibration of Electro-absorption Module.

In this Monte Carlo simulation, the unknown quantity is the arrival time at the detector of the photons being sent. This quantity is not fixed as a photon could get lost at several points in the simulation (e. g., in the fiber or the detector). As discussed in 2.4 the probability distribution for the number of photons in a state follows a Poisson distribution which is inherently probabilistic. With these sampled photon times one can estimate important parameters like the QBER. The simulation is written in Python. This chapter describes the stages of the

simulation in chronological order, which closely follows Figure 3.1. Section 3.2 starts with the simulation of the laser characteristics, Section 3.3 outlines how the symbols are created by the EAM and the laser. To measure events in the X-basis, the Delay Line Interfermeter is described in Section 3.4 and the implementation of the detectors is covered in section 3.5.

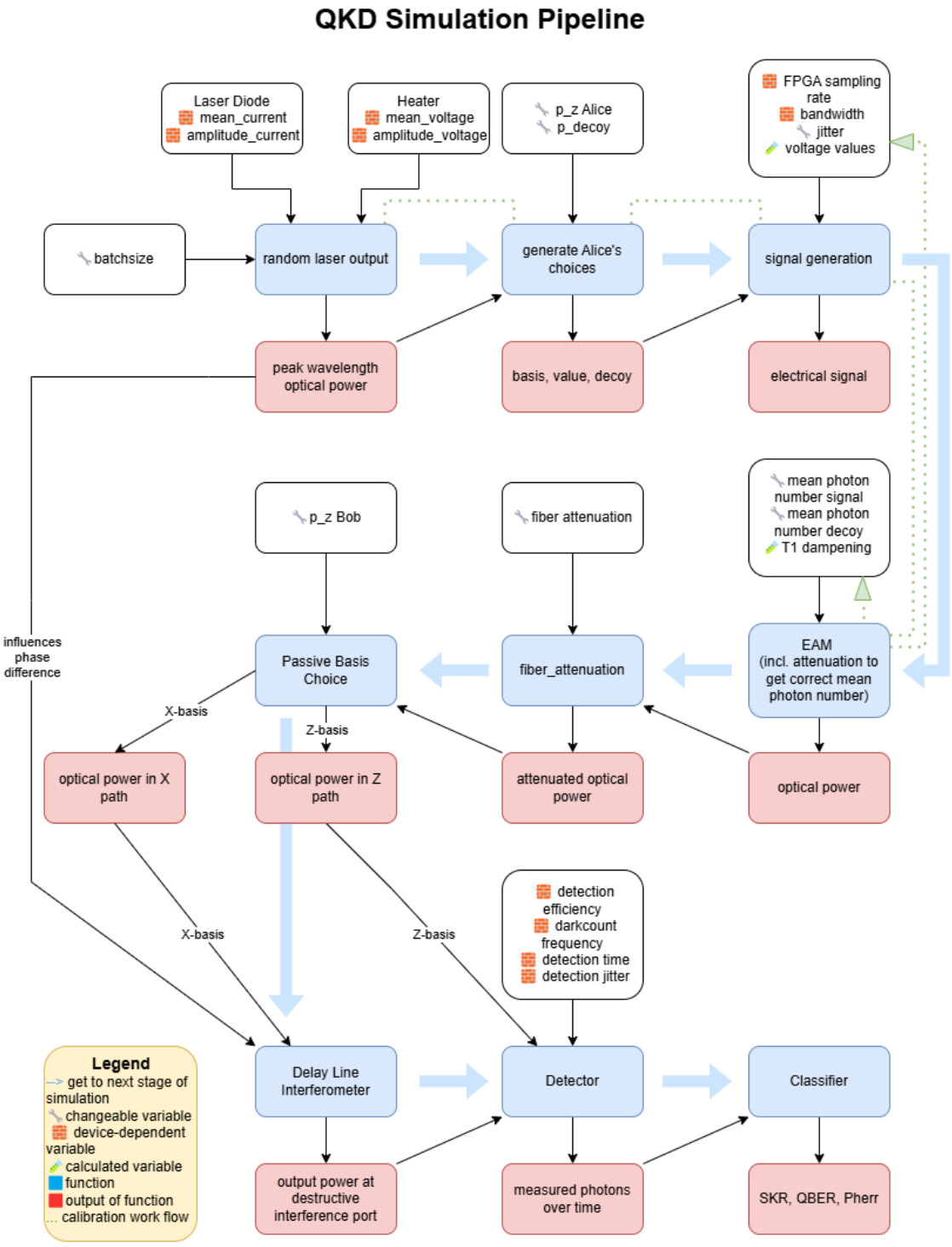


Figure 3.1: Flowchart depicting the sequential process of the code, from laser simulation to symbol creation, fiber attenuation, a passive basis choice, X-basis measurement, detector implementation and the classification in the end. The blue arrows depict the order of the stages of the simulation.

As mentioned earlier, to investigate the performance and security of our Quantum Key Distribution (QKD) system, a comprehensive simulation framework was developed. This framework, visually represented in Figure 3.1, models the key stages of the QKD experiment carried out here, including state preparation, transmission through a quantum channel, detection, and subsequent data processing for secret key distillation. The simulation allows us to analyze the impact of various experimental parameters and imperfections on the final secret key rate and quantum bit error rate (QBER). Notably, the brick symbol in the diagram denotes signal parameters that are inherently fixed due to the characteristics of the specific hardware chip being simulated, representing constraints imposed by the physical implementation. These can be values that have been previously measured on a similar chip and then implemented like optical transmission depending on the input voltage in the EAM. Other parameters are set by design like the 6.5 GS/s (Giga samples per second) symbol rate. Conversely, the wrench symbol indicates signal parameters that can be deliberately varied and adjusted within the simulation environment. The ability to tweak these adjustable parameters allows for a systematic exploration of their influence on the final secret key rate, enabling optimization strategies to enhance the performance of the QKD system under different operational conditions. The code infrastructure and plotting was supported with suggestions from ChatGPT [22].

3.2 Laser

For the simulation, a distributed feedback laser is used, which is a specific type of semiconductor laser. These are used in integrated photonics because of their spectral purity, wavelength stability and compactness [23]. The specific laser used in the simulation is on Indium Phosphide and emits light at around 1550 nm. The output of is the laser is in the mW range with a line width of approximately 5 MHz. The laser is controlled with a setup developed in [24], where a current is applied in at the Laser Diode and a voltage is applied at the local heater, which are both specifically designed to tune the wavelength. This is done with an electronic laser driver.

The base wavelength of the laser is regulated to stay at 1550 nm and the heater is used to modulate the peak wavelength by +1.5nm on top of that. This can be seen in Figure 3.2.

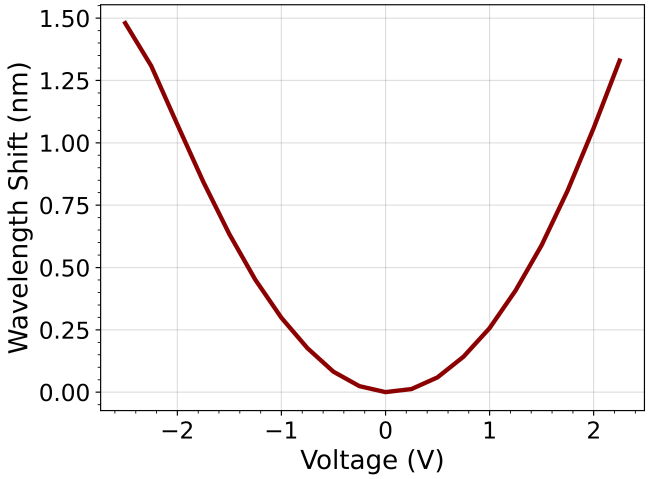


Figure 3.2: Wavelength shift as a function of applied voltage to the heater. The plot highlights the tunability of the laser's output wavelength through voltage adjustments, which is how the wavelength is controlled in this optical systems.

Similarily, the optical power of the laser is influenced by current applied to the laser diode, which is described by Figure 3.3.

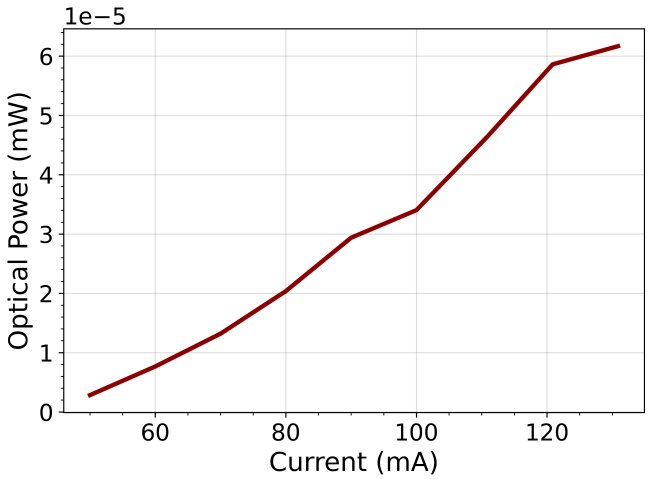


Figure 3.3: Optical power as a function of laser diode current. The plot illustrates the relationship between the driving current and the resulting optical power output of the laser diode.

In the simulation, for each symbol, a voltage for the heater and a current for the laser diode are assumed. In previous tests, the control electronics show fluctuations over time which can be seen in Figures 3.4 and 3.5.

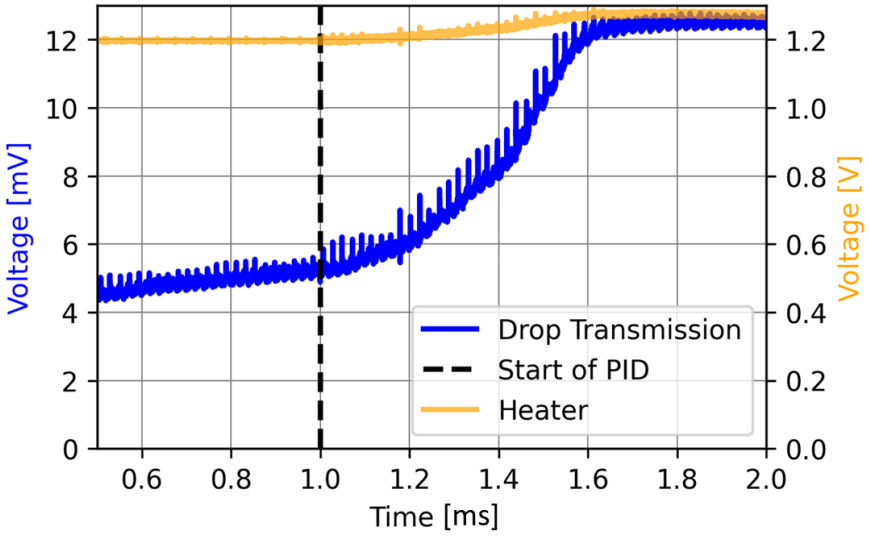


Figure 3.4: This figure shows the control signal of the heater (yellow) and the output of the heater (blue) locked to a resonator feedback. The yellow curve is This figure is taken from [24] Figure 4.26.

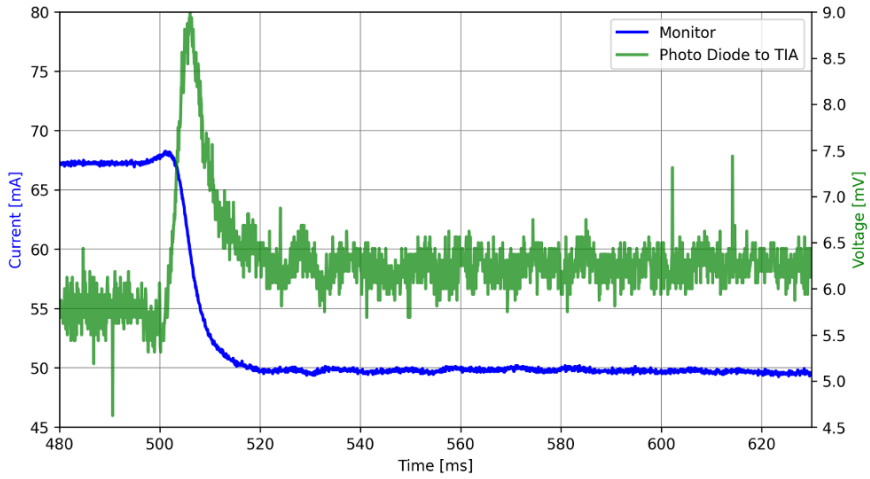


Figure 3.5: This figure shows in green the photo diode voltage which is linear to the output power of the laser. The line in blue is the monitoring current of the laser driver. The laser driver is supposed to keep the output power constant, but even after 540 ms when the system is stable, one can see fluctuations. This figure is taken from [24] Figure 4.13.

For both Figures 3.4 and 3.5, it is important to look at the system after the fluctuations remain constant. In Figure 3.5 the variance can be observed after

approximately 530 ns and in Figure 3.4 after 1.6 ms.

One can observe a 50 Hz fluctuation in the monitoring current (blue) in Figure 3.5 and a 20 Hz fluctuation in the voltage of the heater (yellow) in Figure 3.4. The observed behavior can be simulated as sine waves with a current amplitude of $I_{amp} = 0.41mA$. The amplitude of the voltage is $V_{amp} = 0.011V$. In the simulation, the mean current of the laser diode $I_{mean} = 82.11mA$ and the mean voltage applied to the heater $V_{mean} = -1.755V$ are chosen from Figure 3.2 and Figure 3.3, among other factors. These will be elaborated for I_{mean} in Section 3.3 and for V_{mean} in Section 3.4.

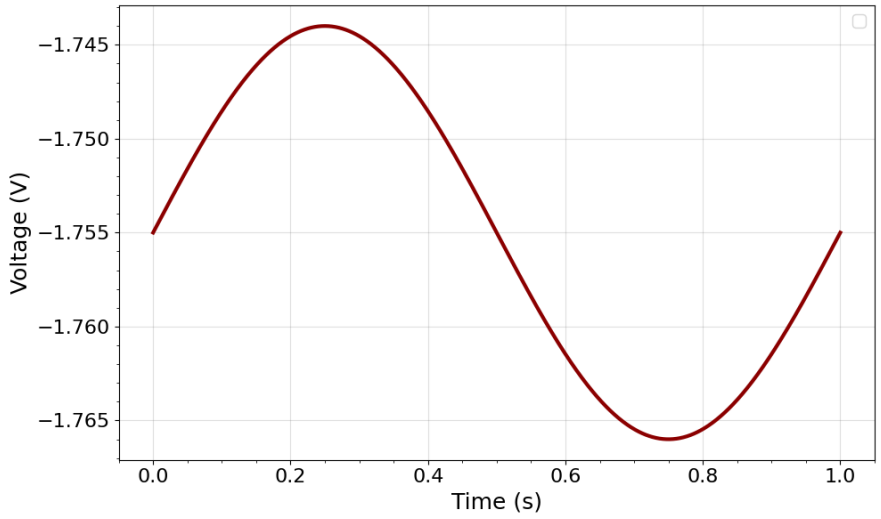


Figure 3.6: Sinusoidal simulated heater voltage signal oscillating over time, captured between 0 and 1 second. The heater voltage varies between approximately -1.743 V and -1.747 V.

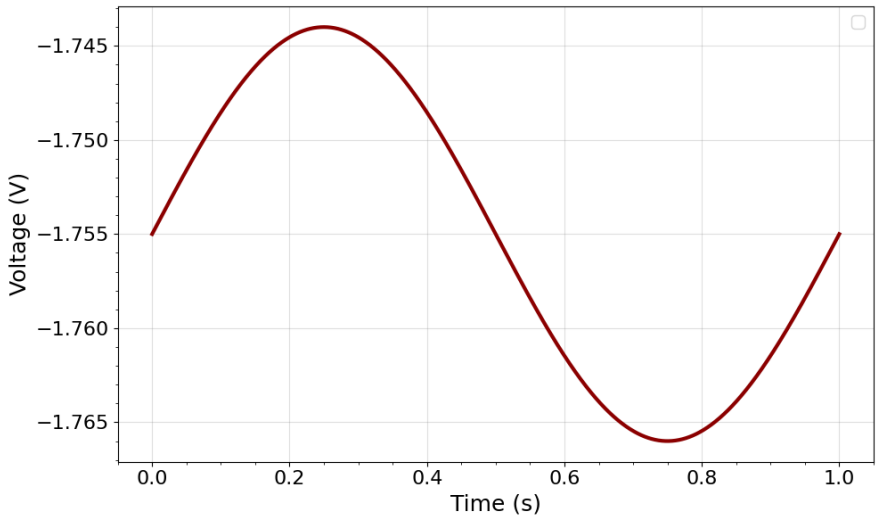


Figure 3.7: Sinusoidal laser diode current signal, measured in milliamperes (mA), fluctuating over a one-second interval. The current oscillates between roughly 82.08 mA and 82.14 mA.

It is essential to now determine in which frequency the voltage of the heater and the current of the laser diode change. The simulation has a symbol rate $\frac{6.5}{4}GHz = 1.625GHz$ (also see Section 3.3.1). In Figure 3.5, the control electronics showed sinusoidal fluctuations in the 100 Hz-range. This means that the voltage and the amplitude fluctuate much slower than symbols are being sent, so in the simulation groups of symbols are assigned the same chosen voltage and the same chosen current. These groups of symbols are batched together, the batch size is chosen to be 1000.

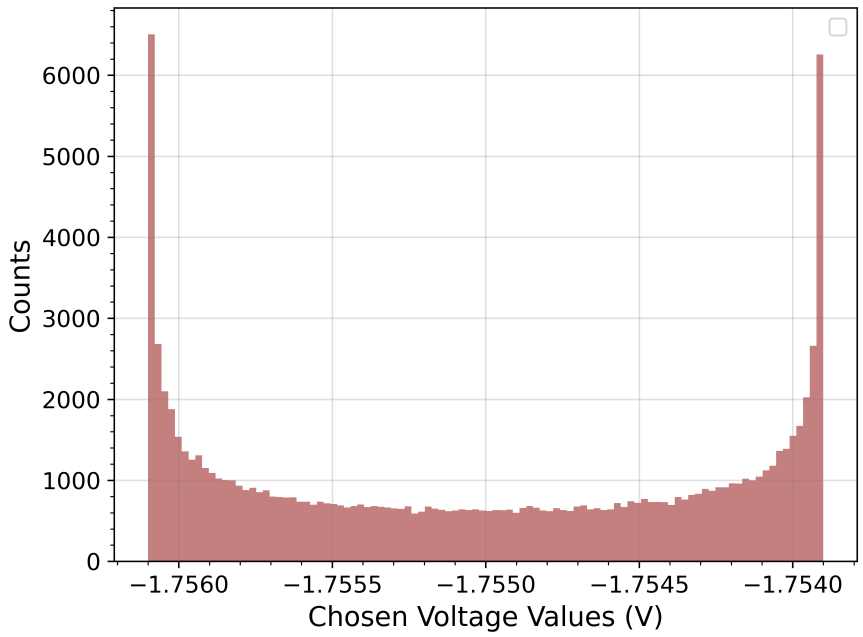


Figure 3.8: Distribution of chosen voltage values (V) showing a U-shaped pattern with higher counts at the extremes (-1.7560 V and -1.7540 V).

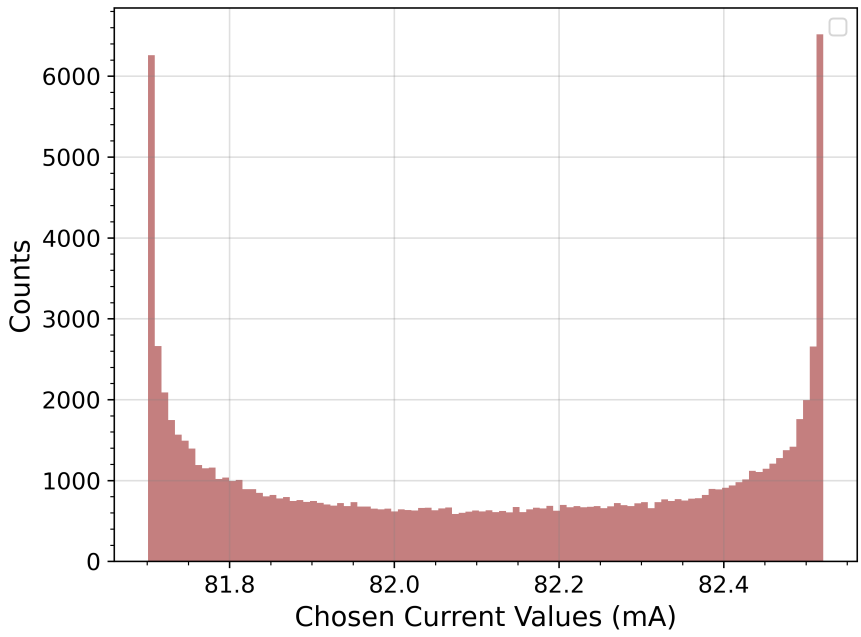


Figure 3.9: Histogram of chosen current values (mA) exhibiting a U-shaped distribution, with peaks around 81.75 mA and 82.5 mA.

With this, the optical power and the peak wavelength are controlled. The applied current to the laser diode and the voltage of the heater have errors, the actual applied voltage and applied current are sinusoidal also seen in Figure **??** where the mean voltage and mean current are the vertical offsets that can be observed. The amplitudes of the sines are fixed and can be seen in Table 3.3. For each batch of symbols a wavelength and a current is randomly chosen, which now influence the optical power and the peak wavelength.

For the protocol to be 100% accurate, the laser pulses have to be phase randomized, to ensure that the weak coherent pulse can be described as the sum of Fock states. This is left out in the simulation, because it does not influence the simulation, as only in the Delay Line Interferometer the phase plays a role. When the laser pulses are phase-randomized, they don't interfere with each other and there is only interference in-between a symbol. For the simulation, this influence is disregarded as it is beyond the scope of this thesis.

3.3 Electro-Absorption Module

3.3.1 Electrical Signal Generation

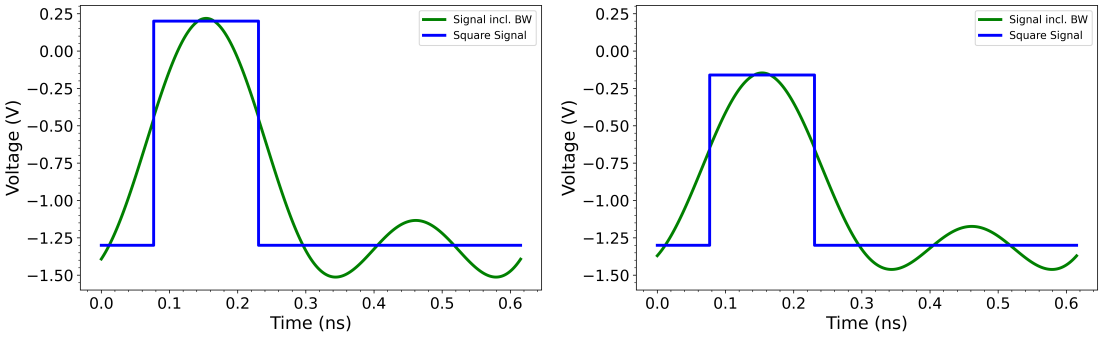
Next, the electrical signal for the Electro-Absorption modulator is created, where the symbols that are being sent are already encoded. Alice's choice of basis, value (for information encoding), and decoy state are then probabilistically generated based on $p_{z,Alice}$ and p_{decoy}. The variables basis, value, and decoy can all be either 0 or 1. If the X-basis (0) gets chosen, then value is set to -1 regardless of what it was set to, because in the X-basis there is only the X_+ state available. The states corresponding to the variables basis, value, and decoy can be looked up in Table 3.1.

Title	**Basis**	**Value**	**Decoy**
State: $Z_{0,signal}$	Z (1)	1	No (0)
State: $Z_{1,signal}$	Z (1)	0	No (0)
State: $X_{+,signal}$	X (0)	-1	No (0)
State: $Z_{0,decoy}$	Z (1)	1	Yes (1)
State: $Z_{1,decoy}$	Z (1)	0	Yes (1)
State: $X_{+,decoy}$	X (0)	-1	Yes (1)

Table 3.1: Quantum states used in the QKD simulation, including basis, value, and whether the state is a decoy.

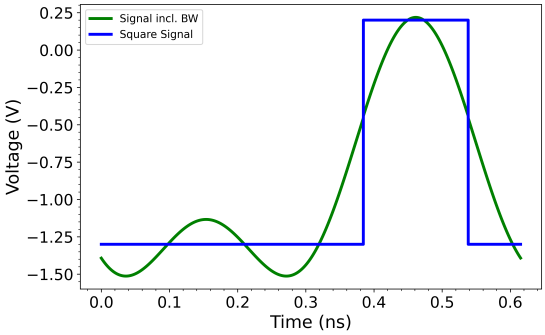
Based on the variables basis, value and decoy for each symbol a square-shaped electrical pulse gets created. There are five different voltages that can be set. There is the non-signal voltage at which the EAM absorbs most laser light. The four other voltage are the four combinations possible when one can choose the variables basis and decoy, see Table 3.2.
As discussed in Section 2.4, the state Z_0, for example, corresponds to a pulse in the early time bin. To differentiate later where a pulse is present and where no pulse is, each symbol is divided into four samples. The maximum sampling rate for simultaneous operation of the RF-DACs is 6.5 GS/s. Since at least two samples are required per symbol, and to avoid signal overlap between successive time bins one sample must be set to an absorbing (non-signal) state. This results in a division into four samples per symbol, corresponding to a symbol rate of 1.625 $\frac{GBaud}{s}$.
Within one symbol, the second and fourth samples are always set to the non-signal voltage, while the first and third samples are set according to the required signal voltage as listed in Table 3.2.
How exactly these voltages are set depends on the calibration of the EAM, which will be discussed in more detail in Section 3.3.3. For the state Z_0, this means

that the first quarter (first sample) of the symbol carries the signal voltage for the Z-basis, while the remaining three quarters are set to the non-signal voltage. An illustration of this voltage scheme can be seen in Figure 3.10.
Additionally, the symbol is shifted by 1/8 of a symbol time for improved visibility. This shift does not affect the results, as all symbols are transmitted sequentially in time.

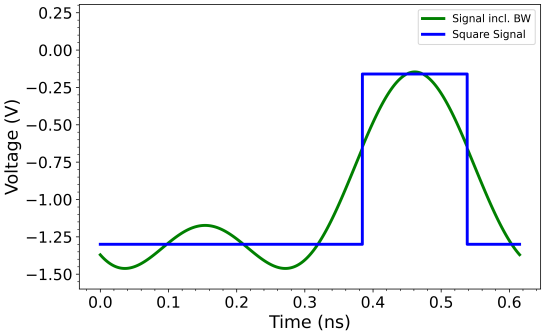


(a) Z_0

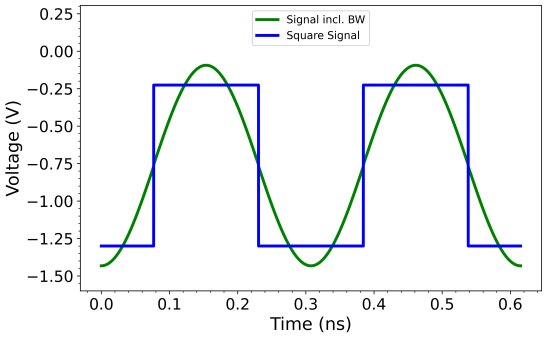
(b) $Z_{0,decoy}$



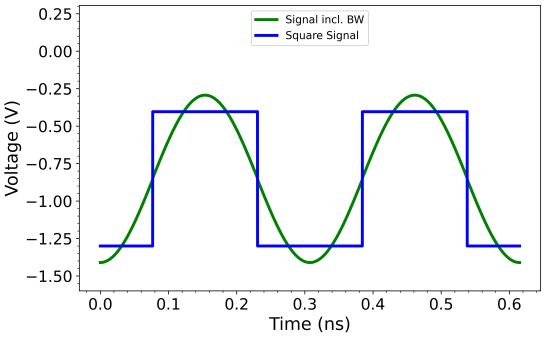
(c) Z_1



(d) $Z_{1,decoy}$



(e) X_+



(f) $X_{+,decoy}$

Figure 3.10: These plots illustrate the temporal voltage signal (green line) resulting from an intended square voltage pulse (blue line), when passed through a system with limited bandwidth of 4 GHz. The finite bandwidth causes the sharp transitions of the ideal square wave to become rounded.

The electrical signal is generated by a Field Programmable Gate Array (FPGA)

board, a device composed of configurable logic blocks that allow for precise timing control of electrical signals. In particular, the FPGA board used here is the AMD Zynq UltraScale+ RFSoC, which integrates 16 radio frequency Digital-to-Analog Converters (RF-DACs) directly onto the chip. This architecture enables the digital data streams to be prepared and processed directly on the chip, without needing to buffer the large data volumes in external RAM. This is a necessity, given the extremely high data rates involved.
The RF-DACs convert digital signals into analog signals and have an analog bandwidth limited by the physical characteristics of the DAC circuitry. For the RF-DACs used here, the analog bandwidth is 4 GHz, meaning they can reproduce signal frequencies up to 4 GHz with a power loss of no more than 3 dB [25]. The direct integration of high-speed DACs with programmable logic greatly simplifies system architecture and ensures minimal latency between data preparation and signal output.
In the simulation this is done by applying a frequency-domain filter to the signal to attenuate frequencies outside the desired range. By transforming the signal into the frequency domain using Fast Fourier Transform (FFT), it selectively scales the Fourier coefficients based on a smooth, interpolated frequency response. For this, the two arrays $freq\_x$ and $freq\_y$ are defined:

```
S_fourier = fft(signal)
frequencies = fftfreq(len(signal), d=1 / sampling_rate_fft)

freq_x = [0, bandwidth * 0.8, bandwidth, bandwidth * 1.2, \\
    sampling_rate_fft / 2]
freq_y = [1, 1, 0.7, 0.01, 0.001]  # Smooth drop-off

np.multiply(S_fourier, np.interp(np.abs(frequencies), freq_x, freq_y)
    , out=S_fourier)

signal = np.real(ifft(S_fourier))
```

The frequency response of the filter is defined by the arrays $freq\_x$ and $freq\_y$. The $freq\_x$ array specifies key frequency points, and the $freq\_y$ array defines the corresponding gain values at those points. Specifically, at 0 Hz, the gain is set to 1. At $0.8 \cdot bandwidth$, the signal is also still fully preserved with a gain of 1, ensuring that frequencies up to 80% of the desired bandwidth are unaffected by the filter. The gain decreases gradually at the bandwidth, where it is set to 0.7, introducing a slight attenuation to the signal at the upper edge of the desired bandwidth. At $1.2 \cdot bandwidth$, the gain drops to 0.01, marking the point where the filter attenuation becomes more pronounced, and higher frequencies start to be suppressed. Finally, at sampling-rate-fft / 2, the Nyquist frequency, the gain is reduced to 0.001, ensuring that frequencies close to the Nyquist limit are effectively suppressed.

The Nyquist frequency is the highest frequency that can be accurately sampled. This goes back to the Sampling Theorem, which states the following:
We assume a flat frequency response up to $0.8 \cdot \textit{bandwidth}$ with full gain (1.0). The 3 dB point, corresponding to approximately 70% in voltage (or 50% in power), is reached at the bandwidth (e.g., 4 GHz). Beyond that, the gain decreases further, dropping to 0.01 at $1.2 \cdot \textit{bandwidth}$ and finally to 0.001 at the Nyquist frequency (*sampling rate*/2, effectively suppressing high-frequency components.
The frequency response is defined by two arrays: $freq\_x$ specifies key frequency points and $freq\_y$ the corresponding gains. This setup ensures that the signal remains undistorted up to the bandwidth while attenuating unwanted high-frequency components according to the Sampling Theorem.
Suppose a signal is bandlimited. Let B be the maximum frequency in its frequency spectrum. If the signal is sampled at rate $f_s > 2B$, then it can be reconstructed exactly from its samples. $2B$ is called the Nyquist rate and the condition $f_s > 2B$ required for reconstruction is called the Nyquist condition.
This means that the filter will progressively attenuate frequencies approaching this point, ensuring that higher frequencies over the selected bandwidth are effectively suppressed [26]. The use of a smooth, gradual transition in the filter's response ensures that there are no sharp cutoffs.
The linear interpolation performed by np.interp(np.abs(frequencies), $freq\_x$, $freq\_y$) is crucial to achieving a smooth frequency response. By linearly interpolating the values in $freq\_y$ across the frequency points defined in $freq\_x$, the filter ensures a continuous, gradual transition between the preserved and attenuated frequency ranges. This helps avoid harsh cutoffs, which could introduce unwanted artifacts such as the Gibbs effect. This effect arises from the non-uniform convergence of the partial sums of a Fourier series in the vicinity of non-removable, or jump, discontinuities within the approximated function. [27, p. 105] This approach provides fine control over the filter's behaviour, allowing it to balance the preservation of important signal components within the desired bandwidth while progressively attenuating higher frequencies to simulate the influence of the RF-DAC.
This results in a voltage signal that is adjusted to account for the bandwidth of the RF-DAC. The laser light is then attenuated in accordance with these voltage levels.

3.3.2 Modulation of the Light with the Electro-absorption Module

To attenuate the laser light, an Electro-absorption Modulator (EAM) is included, which attenuates the optical power to achieve the desired signal patterns. For the simulation, an already calibrated EAM is taken and the optical transmission

depending on the input voltage is measured and used to determine the laser pulse after the EAM. The data used for this can be seen in Figure 3.11.

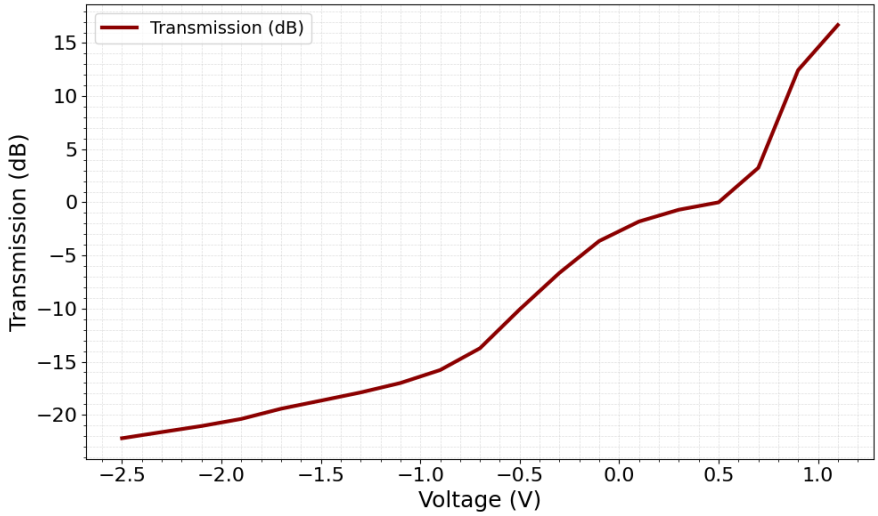
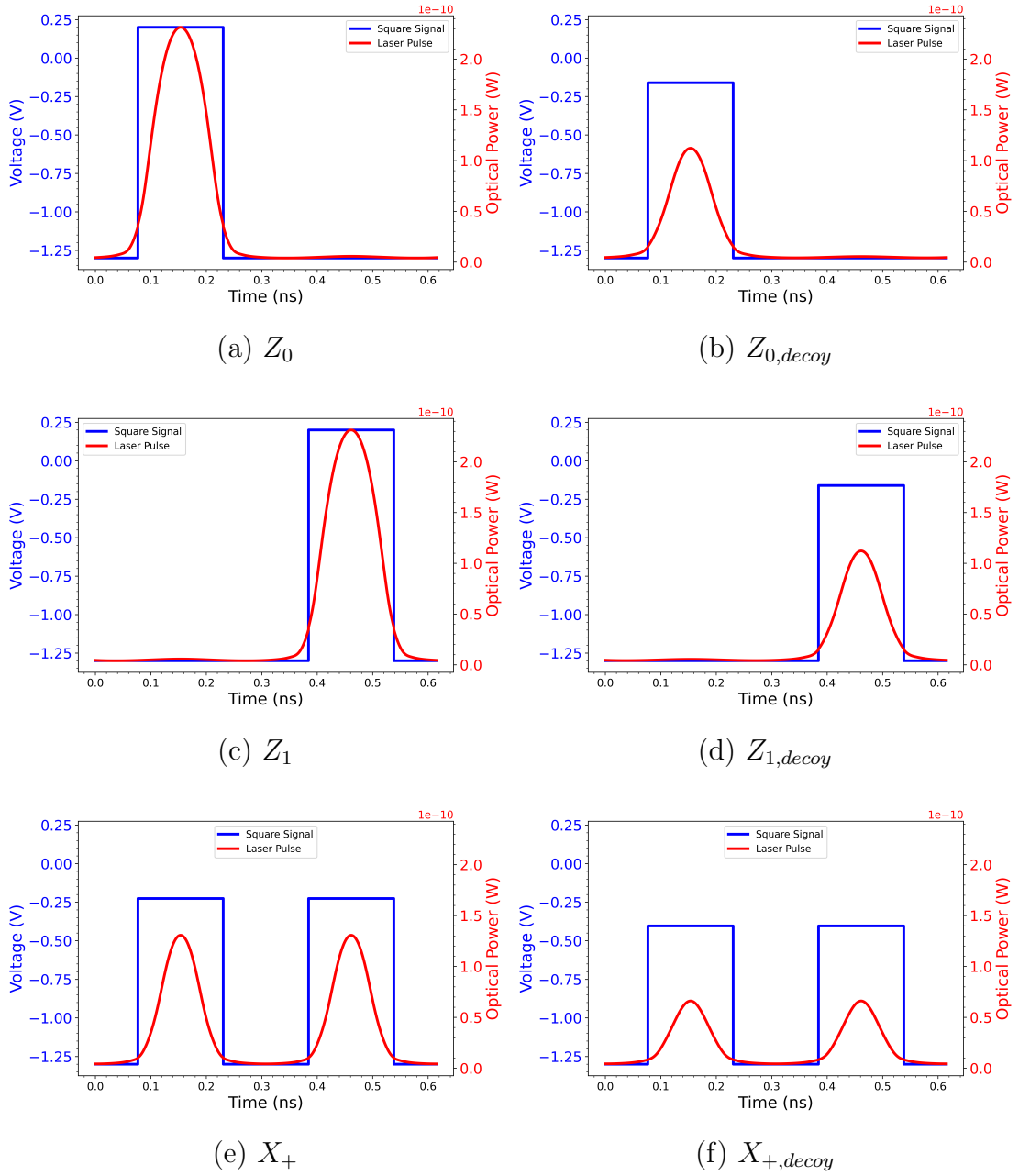


Figure 3.11: Electro-absorption modulator (EAM) transmission as a function of applied voltage. The plot shows how the optical transmission through the EAM varies with the applied voltage, demonstrating the modulator's ability to control light intensity for signal modulation. This is used to create the states Z_0, Z_1 and X_+.

The transmission is then multiplied by the peak optical power to get the power over time. The laser pulse of all symbols are displayed in Figure 3.12.
After the EAM, the signals are attenuated to achieve the desired mean photon numbers. In Figure 3.1 this dampening is called T_1 attenuation. The signal state is attenuated to the mean signal photon number μ_{signal} and the decoy state is attenuated to the mean decoy photon number μ_{decoy}. This attenuation is a global attenuation that is the same for all the states. To achieve the different desired photon numbers, the voltage values that get fed into the EAM are different for Z_{signal}, Z_{decoy}, X_{signal} and X_{decoy} values. This is also the reason why five different voltage values are required.
In the following section, the calibration of the voltages and the dampening are explained.

3.3.3 Calibration

The dashed green lines in Figure 3.1 depict a detailed calibration process designed for fine-tuning the generated signals. This process begins with calibrating the T_1 attenuation which is the last attenuation step before the light exits the chip. This



(a) Z_0 (b) $Z_{0,decoy}$

(c) Z_1 (d) $Z_{1,decoy}$

(e) X_+ (f) $X_{+,decoy}$

Figure 3.12: These plots illustrate the square voltage pulse (green line) and the resulting optical power of the pulse (red line) after the EAM where a bandwidth of 4 GHz has been applied.

attenuation is done to achieve the mean photon number for the corresponding kind of signal, where the mean photon number is always in the sub single-photon

level. Typical values for this are a signal mean photon number $\mu_s = 0.182$ and a mean decoy photon number $\mu_d = 0.1$. For this, it is the easiest to use a Z_0-state as the difference between the higher signal voltage and the non-signal voltage is biggest, which means it has the highest extinction ratio. For all other states the extinction ratio is smaller which is then easily adjusted with the starting voltages. This assures that the calibration of the other voltage values is possible after the T_1 calibration is successful. In physical set-ups, the calculation of the mean photon number is performed right at the point where the photon leaves the chip. Any losses on the chip itself will not influence the light after the attenuation as these are accounted for as long as the losses don't result in a mean photon below the desired one. These calibrations have to be done before the system is put into operation.
To achieve accurate calibration, we start at the very beginning by choosing the voltage for the heater to achieve a wavelength shift on the laser. Here, the mean voltage is chosen to prevent further fluctuations in the calibration batch and make the calibration as accurate as possible. Same goes for the current for the . This is done to get a stable calibration. In the following the symbol is set to Z_0 and two voltage values for the square signal are assumed. The two assumed voltages for the Z_0 signal are set in the beginning and they define the extinctions ratio of the EAM, see 3.11. After the EAM the mean photon number of the signal is calculated by integrating the power over time. The final dampening is calculated as follows:

$$T_1 = \frac{\mu_{calculated}}{\mu_{desired}} \tag{3.3.1}$$

Once the T_1 attenuation is accurately set, the other voltage values within the system are carefully adjusted to produce the intended average photon numbers. This adjustment is carried out using a binary search method, which continues until the error is small (less than 10^{-7}). This high level of precision allows for accurate adjustments to the voltage levels, leading to optimized signal generation.
To achieve an extinction ratio of $16.7dB$, the non-signal voltage $V_{nosignal}$ and the signal voltage for the Z-basis $V_{Z,signal}$ were set to $V_{nosignal} = -1.3$ and $V_{Z,signal} = 0.2$. An example of the calibrated voltage values can be seen in Figure 3.2.
Now, the sender is complete and the optical signal gets transmitted through a fiber of a certain length to the receiver. This is modelled by a fiber attenuation as the optical fiber used has a constant loss of 0.16 dB/km at 1550 nm[28]. In the simulation a fiber length of 10 km was used which corresponds to a loss of 1.6 dB. This is the point where the mean current of the laser diode I_{mean} is once calibrated. I_{mean} directly influences the peak optical power of the laser pulse. Because of the final attenuation to the mean photon number with $T1_{dampening}$, I_{mean} has to be high enough so the calculated mean photon number $\mu_{calculated}$ is high enough for T_1

Parameter	Symbol	Value (V)
non-signal voltage $V_{nosignal}$	-	-1.3
Signal voltage Z-basis $V_{Z,signal}$	$Z_{0,signal}$, $Z_{1,signal}$	0.2
Signal voltage X-basis $V_{X,signal}$	$X_{+,signal}$	-0.2262
Decoy voltage Z-basis $V_{Z,decoy}$	$Z_{0,decoy}$,$Z_{1,decoy}$	-0.0648
Decoy voltage X-basis $V_{X,decoy}$	$X_{+,decoy}$	-0.3345

Table 3.2: Calibrated voltage values used for signal and decoy states in both standard and superposition bases for $\mu_s = 0.25$ and $\mu_d = 0.175$.

to be positive. T_1 is the attenuation necessary to achieve the desired mean photon number. In a device this is directly done with the EAM calibration, but because the voltage to transmission curve for the EAM is set to the same curve in the simulation, regardless of the mean photon number μ that one wants to achieve, this parameter has to be calibrated once per simulation run. The chosen mean current value $I_{mean} = 0.08211A$ satisfies this condition, as in the simulation T_1 is calibrated to $T_1 = 19.583$.

3.4 Delay Line Interferometer

After the fiber at Bob's end, a passive basis choice is implemented based on Bob's probability of choosing the Z-basis (p_{z_Bob}) by for the Z-basis path the power is multiplied by $p_{z_{Bob}}$ and for the X-basis path the power is multiplied by $1-p_{z_{Bob}}$. For measurements in the X-basis, the signal passes through a Delay Line Interferometer (DLI), which enables the necessary interference for distinguishing non-orthogonal states.

The DLI is used to measure phase differences between consecutive signals by splitting an incoming light pulse into two paths, introducing a controlled time delay of one time bin, and subsequently recombining them. The splitting and recombining is done with directional couplers and the delay is introduced by making the path between the two directional couplers longer. This can be seen in Figure 3.13. The interference at the output ports allows for phase-sensitive detection, which is used to detect symbols in the X-basis.

Figure 3.13: A Delay Line Interferometer (DLI) setup, illustrating the splitting and recombination of optical paths to measure phase differences. The spiral element represents the delay line. The illustration of the DLI is taken from [17].

Two of the three components of this Delay Line Interferometer are directional couplers. These consist of two parallel waveguides in an integrated photonic device.
ToDo: mehr directional coupler
The couplers are simulated to be a 50:50 coupler where any loss is disregarded. The waveguide loss for the delay line amounts to $(0.60 \pm 0.10)\frac{dB}{cm}$, which is a loss of approximately $2.7dB$. One can now assume that the two couplers aren't split 50:50, but in a way that the splitting ratio perfectly accounts for the loss in the delay line, making the loss only half, so $1.35dB$.
The coupler introduces a π phase shift, which can be seen in the i on the cross-diagonal. (Quelleee?? Koppler vllt Photonicsbuch?)
Up until now, the simulation worked with the power spectrum over time which was enough for now, but this isn't sufficient anymore as the phase of the electrical field has to be introduced to simulate destructive and constructive interference of the combined fibers. Later it will be sufficient to only look at the power again, because the detectors respond to the optical intensity and are therefore insensitive to the phase.[29, p.138]
The electrical field is simulated as follows:

$$E_{in}(t) = \sqrt{P(t)} \cdot e^{i\omega_0 n_{eff} t} = E_0(t) \cdot e^{i2\pi n_{eff} f_0 t} \tag{3.4.1}$$

Here f_0 is the carrier frequency, so the peak wavelength of the laser that was determined in the laser output function. (Ref??) For this, $P(t)$ is upsampled to a frequency of 10^{14} Hz to simulate the optical field evolution with high precision.

$$Q = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} T \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{3.4.2}$$

Here $\Delta\phi$ is the phase shift. This can be described like this:

$$\Delta\phi = \frac{2\pi f_0 n_{\text{eff}} \Delta L}{c} = \frac{2\pi f_0 n_{\text{eff}}}{c} \cdot \left(\tau \cdot \frac{c}{n_g}\right) = 2\pi f_0 \cdot \frac{n_{\text{eff}}}{n_g} \cdot \tau = 2\pi \frac{c}{\lambda_0} \cdot \frac{n_{\text{eff}}}{n_g} \cdot \tau \quad (3.4.3)$$

Δ L is the effective length difference of the two arms. λ_0 is the peak wavelength calculated at the laser. n_{eff} is the effective refractive index, this is material and geometry dependent. Mode simulations using Ansys lumerical of an uncladded SiN waveguide on SiO_2 with a width of $1.2\mu m$ and a height of $330nm$ yield the effective index $n_{eff} = 1.5543$.
The Matrix T respresents the delay line itself, which shifts $t \mapsto \tau$ which looks like this:

$$T \begin{pmatrix} E_{in,1}(t) \\ E_{in,2}(t) \end{pmatrix} = \begin{pmatrix} E_0(t) e^{i\omega_0 t} \\ E_0(t-\tau) e^{i\omega_0 (t-\tau)} \end{pmatrix} \quad (3.4.4)$$

The electrical field vector, when putting it into the coupler, only has one component, as the other component is empty because the coupler is splitting the light from one port into two ports.

$$\vec{E} = \begin{pmatrix} E_{in} \\ 0 \end{pmatrix} \quad (3.4.5)$$

With this, one can calculate the output electrical field after the DLI.

$$\begin{aligned}
\vec{E_{out}} = \begin{pmatrix} E_{out,1} \\ E_{out,2} \end{pmatrix} &= Q \cdot \begin{pmatrix} E_{in} \\ 0 \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} T \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \cdot \begin{pmatrix} E_{in} \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} T \frac{1}{\sqrt{2}} \begin{pmatrix} E_{in} \\ iE_{in} \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} T \frac{1}{\sqrt{2}} \begin{pmatrix} E_0(t) \cdot e^{i\omega_0 t} \\ E_0(t) \cdot e^{i(\omega_0 t + \frac{\pi}{2})} \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} E_0(t) \cdot e^{i\omega_0 t} \\ E_0(t-\tau) \cdot e^{i(\omega_0 (t-\tau) + \frac{\pi}{2})} \end{pmatrix} \\
&= \frac{1}{2} \begin{pmatrix} E_0(t) \cdot e^{i\omega_0 t} + E_0(t-\tau) \cdot e^{i\omega_0 (t-\tau) + \pi)} \\ E_0(t) \cdot e^{i\omega_0 t + \frac{\pi}{2})} + E_0(t-\tau) \cdot e^{i(\omega_0 (t-\tau) + \frac{\pi}{2})} \end{pmatrix} \\
&= \frac{1}{2} \begin{pmatrix} e^{i\omega_0 t}(E_0(t) - E_0(t-\tau) \cdot e^{-i\omega_0 \tau}) \\ ie^{i\omega_0 t}(E_0(t) + E_0(t-\tau) \cdot e^{-i\omega_0 \tau}) \end{pmatrix}
\end{aligned} \quad (3.4.6)$$

To model the delayed version of the input optical field E_{in}, the code needs to compute the field at time points shifted by the delay τ. These shifted time points may not align with the original time array t, so interpolation is used to estimate the values of the optical field at these new time points. The whole electrical field gets transformed by the two couplers and the delay line like this.
The second coupler will have a destructive and a constructive port, because both couplers introduce a $\phi/2$ phase shift between the two output ports, totally in a π phase shift, if the light gets cross-coupled twice. Depending on how the wavelength is tuned, either $E_{out,1}$ is the destructive port and $E_{out,2}$ is the constructive port or the other way around. Here the wavelength is tuned in a way where $E_{out,1}$ is the destructive port. On the chip, only the constructive interference port is measured, so in the following the simulation will continue working only with the constructive port.
The tuning can be done by looking at a peak that would experience destructive interference, measuring its height and sweeping over the wavelength. This is done in Figure 3.14. From this figure one can also see that the height of the peak is at its minimum at the -1.755 V, which was chosen for V_{mean}.

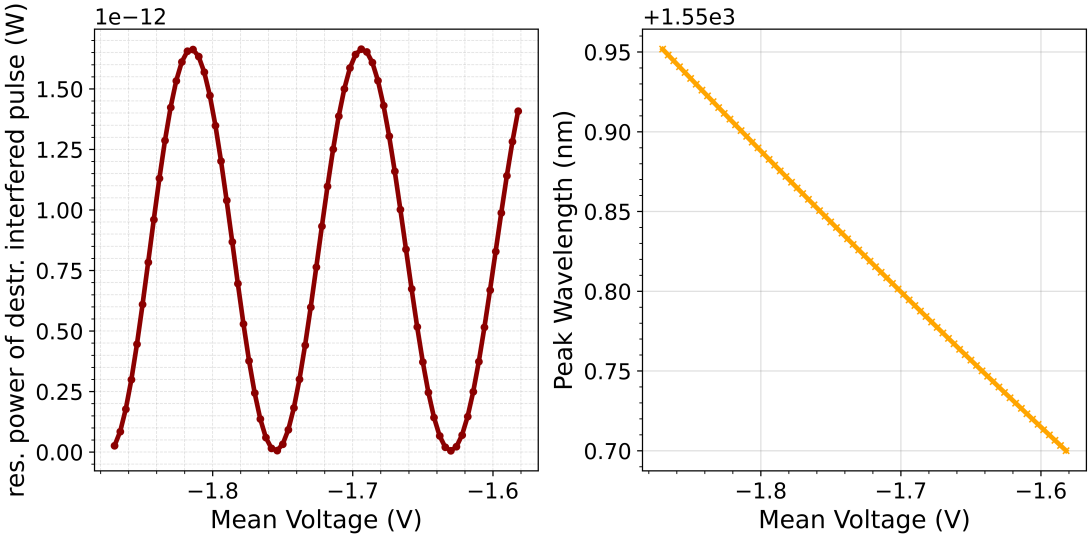


Figure 3.14: The two plots show a sweep of the mean voltage V_{mean} which directly translates to a sweep over the wavelength. This relationship can be seen in the right figure. The figure on the left shows the residual power of a destructively interfered pulse. One can observe a period of 50 pm. μ_s was chosen to be 0.25, μ_d to be 0.175.

To calculate the power out of the phase and amplitude of the optical field the square magnitude of the respective field is taken.

$$P_{destructive} = |E_{\text{destructive}}|^2 \tag{3.4.7}$$

This is done for the output port $E_{out,1}$ to yield

$$P_{out,1} = |E_{out,1}|^2 \tag{3.4.8}$$

$$= \frac{1}{4}(E_0(t)^2 + E_0(t-\tau)^2 - 2E_0(t)E_0(t-\tau)cos(\omega t) \tag{3.4.9}$$

One can now see the requirements for destructive interference. For it to occur, the phase difference $\Delta\phi$ has to be 0 if modulo 2 is applied.

$$\Delta\phi = 0, \pm 2\pi, \pm 4\pi, ... \tag{3.4.10}$$

This is the reason why the chosen mean voltage for the heater is calibrated once at this point as the voltage directly influences the peak wavelength λ_0.

In the simulation, because of the interpolation, the first peak of the simulation is set to 0. If this would not be done, the first peak would be way to high. In the following batches this is solved by taking a symbol more per batch from the beginning and then discarding it again so the first peak per batch after the first one looks normal. In Figure 3.15 one can see the power over time of the first 20 symbols of a simulation. The first symbol is set to 0.

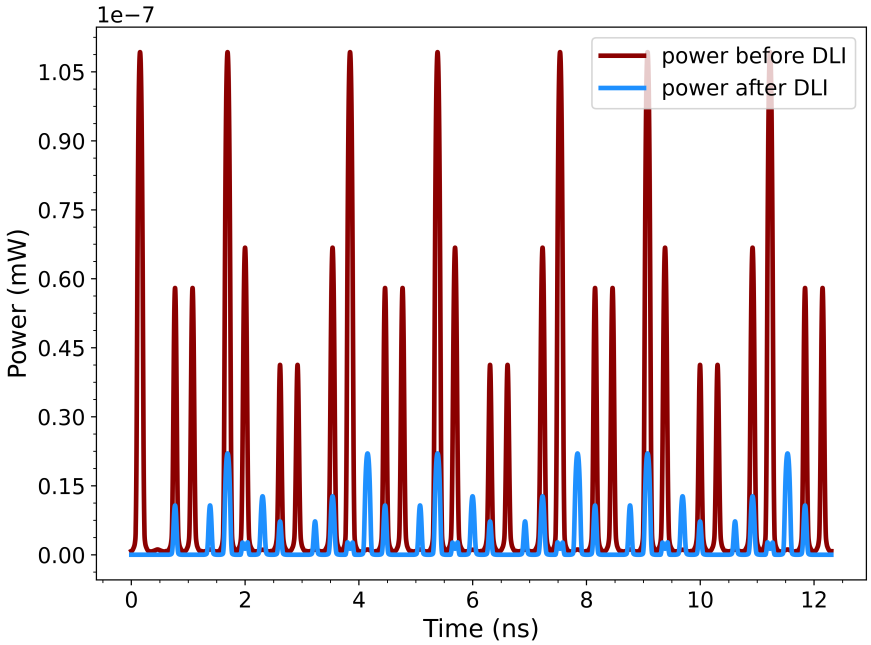


Figure 3.15: This Figure shows the power over time of 20 symbols before (red) and after (blue) the DLI. One can see that for the power after the DLI (blue) the power of the first symbol is set to 0.

This is now fed into the detector.

3.5 Detectors

Photon detection is simulated by the "Detector" module which does several thing. First it select photons based on the dampened optical power, includes the detector efficiency and its probabilistic nature, the timing jitter due to detector imperfection and the inclusion of dark counts.
The first step is the photon selection. This is done by integrating over the power of every symbol separately to get the energy of the symbol at this point. Then the mean photon number is calculated as follows:

$$\mu_{calculated} = \frac{E_{symbol}}{E_{photon}} = \frac{E_{symbol} \cdot \lambda_{laser}}{hc} \tag{3.5.1}$$

Here λ_{laser} is the peak wavelength of the laser determined earlier. As explained in Section 2.4, the amount of photons follows a Poisson statistic with the mean photon number being the mean. Because the simulation has a sufficient amount of counts, this Poisson statistic can be emulated by choosing a number of photons

based on this statistic. After normalizing $P(t)$ by $\mu_{calculated}$ it can be used as a probability density function for the arrival times of the photon(s). This ensures that parts of the symbol where the power is higher, the probability of there being a photon is higher as well. The wavelength of the photon is set to λ_{laser}.
After this, the detector specific properties are applied. The detection efficiency of the detector is estimated to be 30%. This is implemented by discarding 70% of the photons that were just chosen. In addition to this, the detector is assumed to have a dead time of 25 ns. This is applied to the photons by going through the whole array of detected photons and at the i-th photon deleting the $i+1$-th photon if the time between the detections of the i-th and the $i+1$-th photon doesn't exceed the detector dead time. Then it is deleted to account for the dead time. The last thing to be taken into account is the detection jitter.
To simulate the effect of detection jitter, timing variations are introduced to the detected times of the photons. Specifically, these times got shifted by random amounts drawn from a Gaussian distribution. The standard deviation of this distribution was derived from the specified jitter value of 5 ps, where it is assumed that this value represents the Full Width at Half Maximum (FWHM) of the jitter distribution. The FWHM is related to the standard deviation (σ) by the equation

$$FWHM = 2\sqrt{2ln(2)} \cdot \sigma, \tag{3.5.2}$$

which was rearranged to calculate σ. This approach is useful because it models the realistic, statistical nature of jitter. The jitter observed in the system is likely the cumulative result of numerous small, independent sources of variation (e.g., thermal noise and timing fluctuations) and thus primarily random. Therefore, by the Central Limit Theorem, such a summation of independent random variables tends toward a normal distribution, justifying the assumption of Gaussian behaviour. [30]
Here, a jitter value of $5ps$ is assumed.
Next the dark counts are calculated. With a dark count frequency of 1000 dark counts per second, there is a probability of $6.15 \cdot 10^{-5}\%$ that a dark count will happen in a symbol. The simulation will be dealing with block sizes of about 10^8, because up to there the one-decoy method protocol used here outperforms the two-decoy method [11]. This will give me an expected amount of dark counts of 62 counts. This part of the simulation then finally outputs the time, number and wavelength of the detected photons for the X-basis and for the Z-basis separately.

3.6 Classifier

This raw detection data is then processed by the classifier to identify relevant events and perform necessary post-processing.

The first step in the post-processing is the sifting step. In this, Bob announce the bases he has chosen to measured the photons Alice has sent. Alice compares Bob and says which he has chosen correctly and they discard all other bits. This is implemented in the code by only keeping detections where both Alice and Bob chose the right basis.
Because the aim of the whole simulation is the calculation of the secret key rate (SKR), the measured photons now need to be classified, into which detections are measured symbols and which are errors. For this, the photon detection time is taken and it is analyzed if it is in the late or the early time bin. A symbol sent in the Z basis, so Z_0 or Z_1 are correctly identified as such, when there is a measured photon in the corresponding time-bin (for e.g. Z_0 it is the early bin) and in the X basis no symbols are measured in the late bin. This is to exclude the case where we have measurements in the Z and in the X basis which can happen because of the passive basis choice but this isn't allowed in the protocol.
In the X basis, to detect an X_+ symbol, all events where there is a simultaneous detection in Z are discarded. Because the destructive interference port of the DLI is measured, it is not as simple as counting detections. As mentioned in [8] only symbols with a special symbol order can be taken into account, which can be seen in Figure 3.16 and 3.17.
As one can see in Figure 3.16 and Figure 3.17, to be able to measure the total detections in the X basis, the time bins where the photons are counted in have to be guaranteed to be uncorrelated from the symbol before, which is both guaranteed when a X_+ symbol is preceded by a Z_0 or when a Z_1 symbol is preceded by a X_+ symbol. The total number of photons in these constellations are described by $n_{X side}$.

$$n_{X,side} = n_{X_+Z_1} + n_{Z_0X_+} \tag{3.6.1}$$

The total amount of detections in X n_X can be calculated based on the probability $p_{Z,Alice}$.

$$n_X = \frac{n_{X side}}{\frac{1}{4} \cdot p_{Z,Alice}} \tag{3.6.2}$$

When measuring the destructive port of the DLI, only 25 % of the signal power of one peak can be measured, the other 75 % exit through the constructive output port of the interferometer as explained in Section 3.4. The factor $\frac{1}{4}$ accounts for this when calculating how many X detection there are. If there is an X_+ symbol, the probability of there being a X_0 preceding the X_+ is $\frac{1}{2}p_{Z,Alice}$ and the probability of there being a X_1 after the X_+ is also $\frac{1}{2}p_{Z,Alice}$, because the probability to choose Z_0 or Z_1 when the symbol has to be in the Z basis is $\frac{1}{2}$.

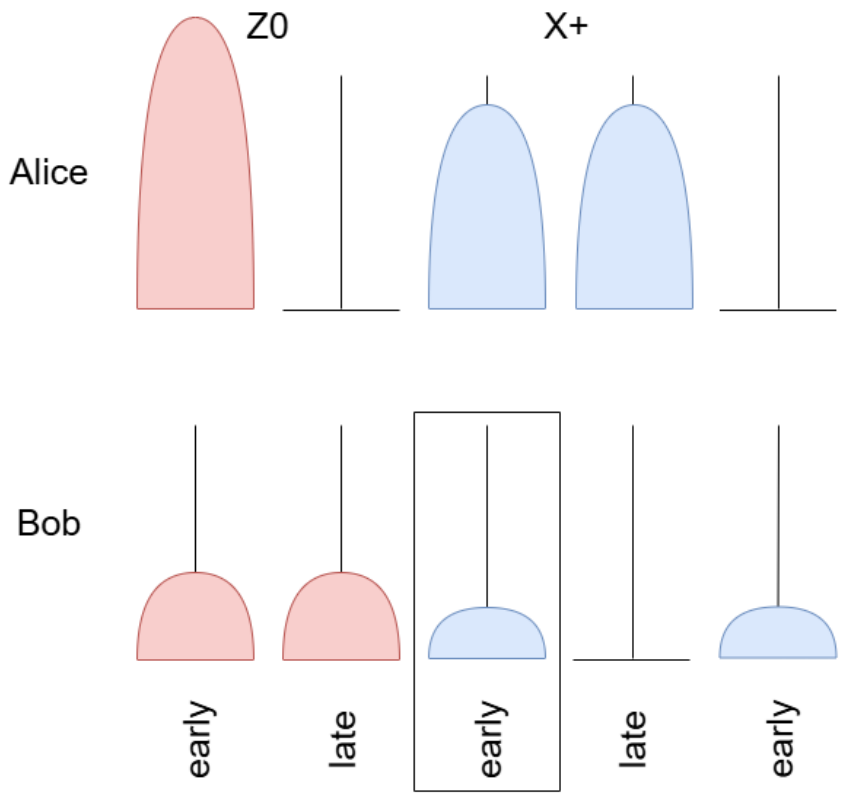


Figure 3.16: Example of the symbol combination that can be used to calculate the total number of detections in X n_X. Here the two signal states Z_0 and then X_+ are shown. The early time bin of the X_+ symbol is used to measure n_X, as they are uncorrelated with the pulse in the symbol before. The marked positions is where the photons are counted, giving the quantity $n_{Z_0X_+}$. This illustration is a recreation, based on [8].

This is filtering for $n_{X,side}$ can be done for both signal and decoy states to get the probability of X_+ signal detections and X_+ decoy detections.

Finally, the simulation outputs key performance metrics, including the Secret Key Rate (SKR) and the Quantum Bit Error Rate (QBER). These metrics allow for a quantitative evaluation of the simulated QKD system's performance under various conditions.

What now follows is an overview of all variables that are fixed in the system. In Table 3.3 lists all variables that are fixed by the system.

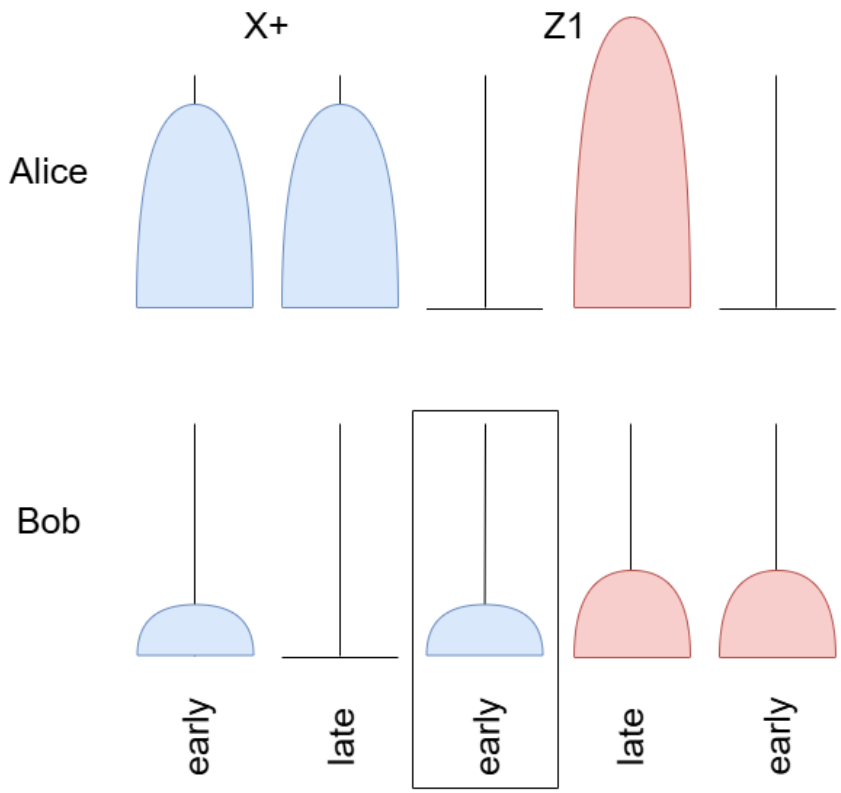


Figure 3.17: Example of the symbol combination that can be used to calculate the total number of detections in X n_X. Here the two signal states X_+ and then Z_1 are shown. The early time bin of the X_+ symbol is used to measure n_X, as they are uncorrelated with the pulse in the symbol before. The marked positions is where the photons are counted, giving the quantity $n_{X_+Z_1}$. This illustration is a recreation, based on [8].

Table 3.3: Fixed Signal Parameters Due to Chip Characteristics

Parameter Name	Fixed Value
FPGA sampling rate FPGA sampling bandwidth	4 GHz
mean current amplitude current	0.0005 A
mena voltage amplitude voltage	0.002 V
$p_{z,Bob}$	0.5
detector jitter	5 ps
detector efficiency	30%
darkcount frequency	1000 Hz
detection time	25 ns

Chapter 4

Results

In this section, the results of the simulation are presented.

4.1 Histograms of Z-detector and X-detector

As a first proof of concept, the simulation excludes the classification. Starting at the laser, EAM, DLI and both detectors are simulated, which yield the detected photon times. The detected photon times are sorted into 60 bins per symbol and displayed in a histogram. It is important to note that for the construction of the histogram, a fixed order of symbols is fed into the simulation. Taking a fixed symbol order ensures that all differences in normalized photon counts are attributed to lower mean photon numbers in the signal. A histogram of a random symbol order is created. One can also take a random symbol order and then sort it, but to make the peaks in the histogram comparable, one must fine-tune $p_{Z,Alice}$ and p_{decoy} correctly for every symbol to appear in the histogram evenly.
For all the symbols, the photon time counts in the X-basis get normalized by the highest count in the X basis, the photon time counts in the Z-basis are dealt with accordingly. This enhances readability. One has to keep in mind that the counts in the X-basis are always lower than the counts in the Z-basis. As an example, one can look at the Z_0 symbol. Here, the one pulse in the early time-bin gets split up into one pulse in the early time-bin and one pulse in the late time-bin by the DLI, which is also what one measures in the X-basis. Because the optical power is split up into two time-bins, the mean photon number in one time-bin is now halved. The amount of photons per pulse can be described by a Poisson statistic with the mean photon number being the mean, which directly translates into half the amount of photons over time. Depending on how Bob's passive basis choice $p_{Z,Bob}$ is chosen, this can skew the ratio of Z to X detections even more.
In the histogram the signal states are labeled Z_0, Z_1 and X_+ and the decoy states

as Z_0^*, Z_1^*, and X_+^* for spacing reasons. In the following figures, the following parameters were set: $\mu_{signal} = 0.7$, $\mu_{signal} = 0.1$

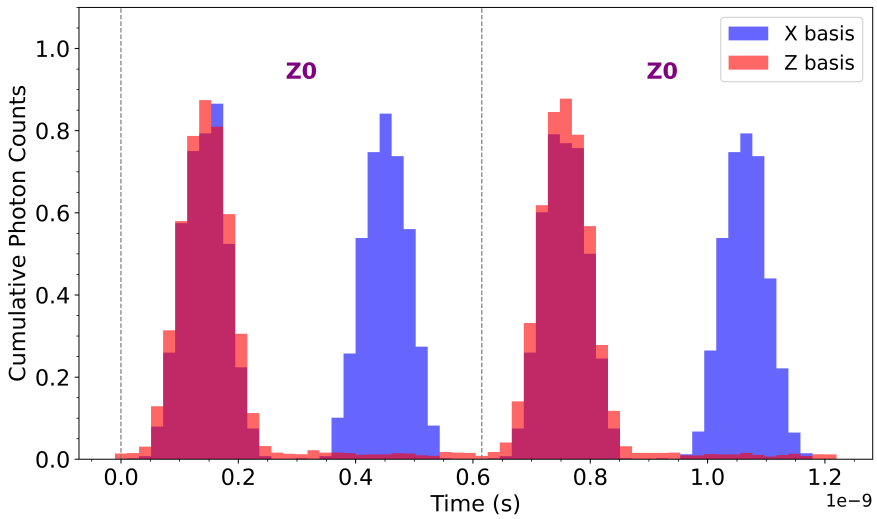


Figure 4.1: In this Figure, one can see for the Z_0 symbol most photon counts being measured in the Z basis (red) are in the early time-bin as expected. Those early time-bin counts can either be the photons that were sent at the start or they are dark counts. Either way, they are later classified as correct and count toward the correct count in the Z basis n_Z. In the late time-bin, there are also detections, which are either false detections or dark counts. Those count towards the errors in the Z basis m_Z. Keeping in mind that the dark count rate is 1000 Hz. Most of the counts in the late time-bin are errors. Because the pulses of the Z symbols have a time-bin in-between them they don't interfere and one can see counts in the X basis for all 4 bins.

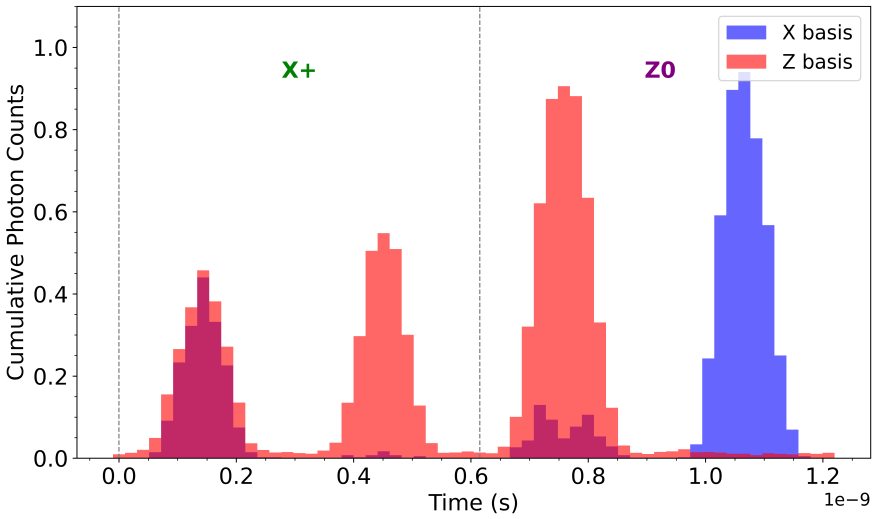


Figure 4.2: In this Figure one can see that the bins per counts are lower for the X_+ symbol, which is because for the two pulses for an X symbol are calibrated to yield the same photon number as the single pulse when a Z symbol is sent. One can also see the early time-bin of the X_+ symbol interfering with the late time-bin of the X_+ symbols resulting in barely any detections except for errors.

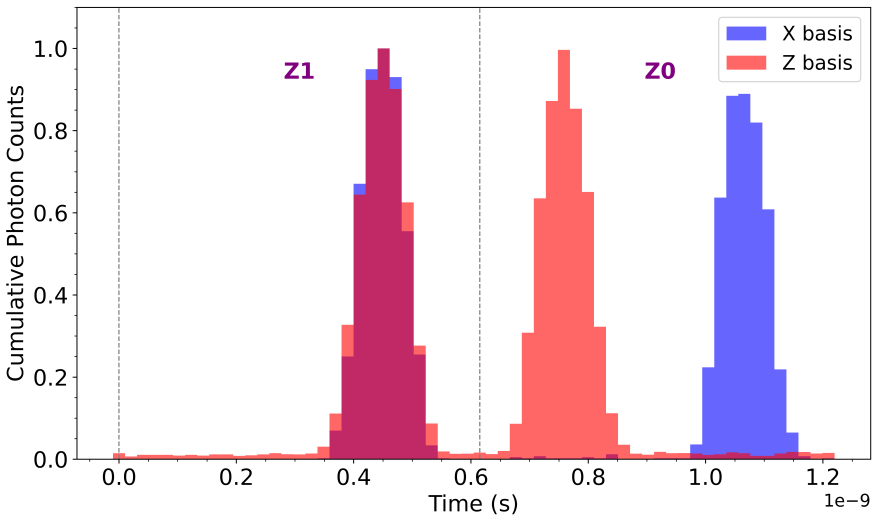


Figure 4.3: The late time-bin of the Z_1 symbol interferes with the early time-bin of the Z_0 symbol, leaving the first time-bin of the X basis for Z empty. The late time-bin of the Z_0 symbol has significant counts in the X basis, because the delayed pulse from the early time-bin is now in the late time-bin

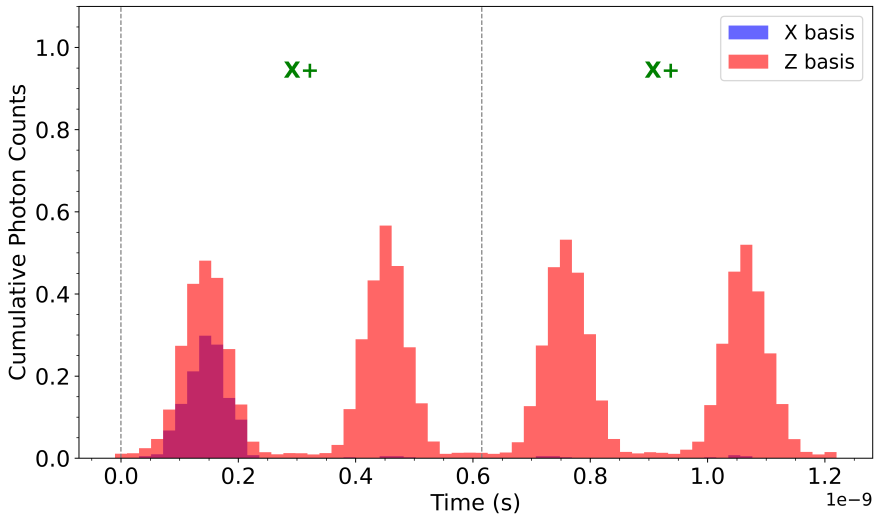


Figure 4.4: In this Figure one can see the first pulse in the first symbol not interfering with the preceding pulse. Because the pulses being sent are both X_+ pulses, they have approximately the same mean photon number, yielding nearly perfect destructive interference in the three following time-bins. In the Z basis, one can see the the two characteristic pulses per symbol.

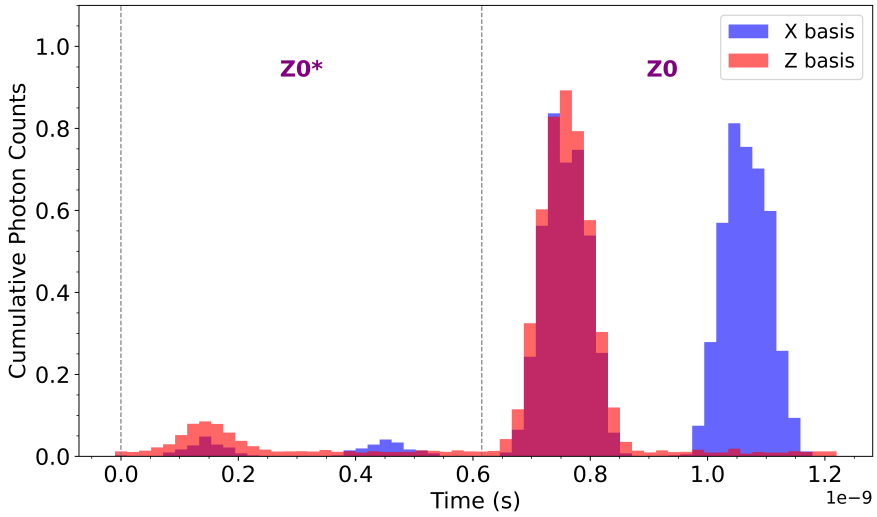


Figure 4.5: In this Figure one can see how the $Z_{0,decoy}$ (in the diagram Z_0^*) pulses differs from the $Z_{0,signal}$ pulse (in the diagram Z_0). This is because the decoy mean photon number μ_d is chosen to be $\frac{1}{7}$-th of the signal mean photon number μ_s.

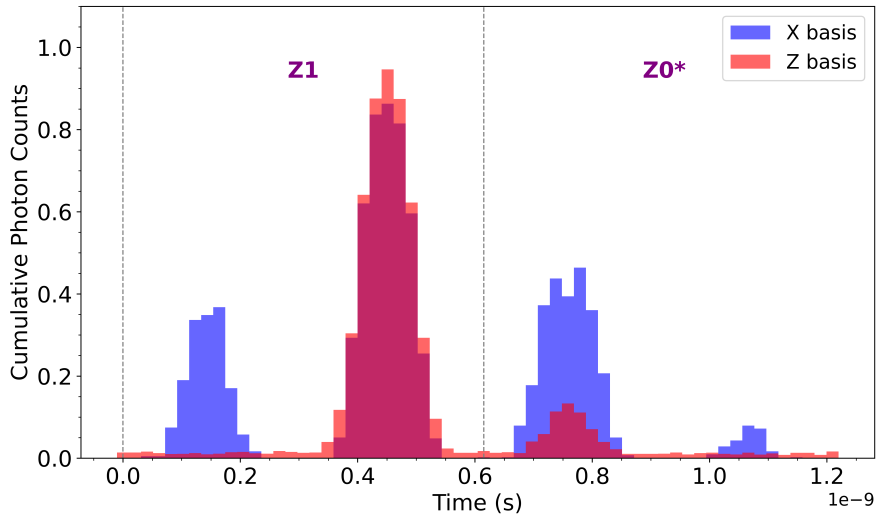


Figure 4.6: In this Figure one can see how two pulses don't completely destructively interfere when the pulses don't have the same mean photon number. The mean photon number of the $Z_{1,signal}$ state is 0.7 and the mean photon number of the $Z_{0,decoy}$ state is 0.1. This means the delayed late time-bin pulse from the $Z_{1,signal}$ state experiences some interference with the non-delayed pulse of the early time-bin of the $Z_{0,decoy}$ state. The delayed part of the $Z_{0,decoy}$ pulse can be seen in the late time-bin of the $Z_{0,decoy}$ symbol.

4.2 Calculation of SKR over Attenuation

In a next section the Secret Key Rate is plotted over the attenuation. For this, the attenuation and the mean photon number is adjusted in between each simulation run and the it is calculated for which probabilities p_{decoy} and $p_{Z,alice}$ the secret key rate is optimal. The total channel attenuation is more than the fiber attenuation, the fiber attenuation is what is adjustable in the simulation. The channel attenuation can be estimated based on all input parameters. As a first step, a suitable balance between μ_s and μ_d has to be found. One can define the ration between μ_s and μ_d as $\mu_s = r \cdot \mu_d$. In [8] the ratio used was $r = 2$, which is cited as close to the optimum value for almost all distances. In contrast to this, in [17] ratios between $r = 2.5$ and $r = 3.3$ were used. The measurement parameters for the SKRs for [17] can be found in [31] in Figure 4.1. The determination of this ratio is done by trial and error. In the simulation, no SKR could be calculated for $r = 2$ or $r = 3.33$, but SKRs could be calculated with $r = \frac{10}{7}$, which is used in all of the following simulations unless said otherwise.

In Table 4.1, one can see an overview of the starting parameters used in the

simulation.

Parameter	**Values**
$p_{z,Alice}$ for the simulation	0.5
p_{decoy} for the simulation	0.5
ϵ_{sec}	10^{-15}
ϵ_{cor}	10^{-9}
$V_{nosignal}$	-1.3
$V_{Z,signal}$	0.2
block size $n_{Z,s}$ is scaled to	10^9

Table 4.1: Parameters for SKR over attenuation, consistent across all attenuation values. The block size $n_{Z,s}$ gets scaled to is 10^9, all other counts are scaled accordingly. $p_{z,Alice}$ and p_{decoy} are only chosen like this for the simulation. For the weighted counts later other $p_{z,Alice}$ and p_{decoy} are optimal.

In Figure 4.1, that p_{decoy} and $p_{Z,Alice}$ are also input parameters in the simulation, just like μ_s and μ_d. Simulating every event with different ratios r and varying over p_{decoy} and $p_{Z,Alice}$ is very computationally expensive which is why a short cut is used here. In the simulation p_{decoy} and $p_{Z,Alice}$ are set to $p_{decoy} = 0.5$ and $p_{Z,alice} = 0.5$ to generate the events and errors $n_{B,k}$ and $m_{B,k}$ where B is the basis and $k \in \{\mu_s, \mu_d\}$ the intensity level. After $n_{B,k}$ and $m_{B,k}$ were simulated, the counts $n_{B,k}$ and $m_{B,k}$ were weighted for all possible probabilities for p_{decoy} and $p_{Z,alice}$ from 0.02 to 0.98 and the SKR was calculated. Then the maximum secret key rate is noted in Table 4.3 together with the assumed p_{decoy} and $p_{Z,alice}$ that the maximum SKR was measured at. This guarantees that the SKR is optimized in terms of p_{decoy} and $p_{Z,alice}$.

The weighing of the counts is illustrated in Table 4.2. The factor 4 is in the calculation to keep the number of counts constant before and after the weighing.

Variable	Basis & State	Expression
n_{Z,μ_s}	Z, Signal	$4 \cdot n_{Z,\mu_s} \cdot p_{Z,Alice} \cdot (1 - p_{decoy})$
n_{Z,μ_d}	Z, Decoy	$4 \cdot n_{Z,\mu_d} \cdot p_{Z,Alice} \cdot p_{decoy}$
n_{X,μ_s}	X, Signal	$4 \cdot n_{X,\mu_s} \cdot (1 - p_{Z,Alice}) \cdot (1 - p_{decoy})$
n_{X,μ_d}	X, Decoy	$4 \cdot n_{X,\mu_d} \cdot (1 - p_{Z,Alice}) \cdot p_{decoy} \cdot \text{factor}_{X,\mu_d}$
m_{Z,μ_s}	Z, Signal	$4 \cdot m_{Z,\mu_s} \cdot p_{Z,Alice} \cdot (1 - p_{decoy})$
m_{Z,μ_d}	Z, Decoy	$4 \cdot m_{Z,\mu_d} \cdot p_{Z,Alice} \cdot p_{decoy}$
m_{X,μ_s}	X, Signal	$4 \cdot m_{X,\mu_s} \cdot (1 - p_{Z,Alice}) \cdot (1 - p_{decoy})$
m_{X,μ_d}	X, Decoy	$4 \cdot m_{X,\mu_d} \cdot (1 - p_{Z,Alice}) \cdot p_{decoy}$

Table 4.2: Weighted expressions for different basis and signal/decoy combinations using $p_{Z,Alice}$ and p_{decoy}.

As a final step, the counts get scaled, so the counts in $n_{Z,s}$ are either 10^7, 10^8 or 10^9 counts and all the other counts and the total symbols are scaled with the same factor. The SKR was highest for $n_{Z,s}$ being scaled to 10^9. This is documented in Table4.1 as factorized $n_{Z,s}$.

The simulation results are displayed in Figure 4.3. When looking at 4.3, it is obvious that the calculation of p_{decoy} and $p_{Z,alice}$ was needed. With $p_{decoy} = 0.5$ and $p_{Z,alice} = 0.5$ the errors in the Z basis $m_{X,s}$ and $m_{X,d}$ were under 5 counts. With the probabilities chosen as extrem as in Table 4.3, the resolution for the errors in the X basis would have been bad and the simulation would have counted 0 counts in these areas. Then the SKR cannot be calculated. The SKR is observed to go down, the higher the attenuation is, with the only outlier being the SKR at 9 dB for $\mu_s = 0.5$ and $\mu_d = 0.35$.

In Table 4.4, the QBER for the X and Z basis and the decoy or signal states $QBER_{Z,s}$, $QBER_{Z,d}$, $QBER_{X,s}$ and $QBER_{X,d}$ were calculated according to Section 2.6. One can observe that for 19 dB and 25 dB, some counts for the X basis are zero, which is not ideal for the calculation of the SKR or the QBER as then the counts are 0 regardless of how they get weighed. The overall measured counts decreases, for higher attenuations. The amount of detections for $n_{Z,s}$ decreases from 6660 counts to 5353 counts when the fiber attenuation is increased from 1 dB to 9 dB. In general, one can observe an increase in the $QBER_{Z,s}$ and in $QBER_{Z,d}$ with an increase in fiber attenuation. For 25 dB, the $QBER_{Z,s}$ and in $QBER_{Z,d}$ have approximately doubled in comparison to the $QBER_{Z,s}$ and in $QBER_{Z,d}$ for 1 dB up to 5.16% and 10.46%. For the $QBER_{X,s}$ and the $QBER_{X,d}$ no such trend is clearly observable, both QBERs seem to vary randomly.

Att. (dB)	μ_s	μ_d	**calc.** p_{decoy}	**calc.** p_{Z_Alice}	**SKR** ($\frac{Bit}{s}$)
1	0.1	0.07	0.06	0.98	12,71
3	0.125	0.075	0.04	0.98	9,72
6	0.25	0.175	0.08	0.92	7,84
9	0.5	0.35	0.08	0.92	10,58
12	0.6	0.42	0.04	0.98	4,99
17	0.7	0.49	0.06	0.98	1,70
19	0.7	0.49	0.86	0.98	0,60
25	0.7	0.49	-	-	-

Table 4.3: Parameters for the SKR measurement. The fiber attenuation in dB is given to the simulation. μ_s and μ_d are the mean photon numbers for the signal and the decoy states which are sent with a probability of p_{decoy} and 1 - p_{decoy}, respectively. Max. SKR is the maximum SKR that can be achieved with the corresponding probabilities calculated p_{decoy} calculated p_{Z_Alice}.

Att. (dB)	$QBER_{Z,s}$	$QBER_{Z,d}$	$QBER_{X,s}$	$QBER_{X,d}$	**counts**	**symbols**
1	3.38	5.66	0.45	1.09	11805	2 million
3	3.22	5.93	0.179	0.52	9373	2 million
6	3.61	6.09	0.96	6.25	9325	2 million
9	3.07	7.20	2.08	4.46	9295	2 million
12	3.90	6.33	1.07	1.10	28460	10 million
17	4.56	7.06	0.96	0.63	10537	10 million
19	4.39	8.01	0.00*	1.79	6643	10 million
25	5.16	10.46	1.25	None **	1660	10 million

Table 4.4: Quantum Bit Error Rates (QBER) for signal and decoy states across different fiber attenuation values. Counts indicates the total counts measured is the sum of all $n_{B,k}$ and $m_{B,k}$ for the case $p_{decoy} = p_{Z,Alice} = 0.5$ and symbols are the total symbols that were being sent. In the field * the error counts for the X signal states $m_{X,d}$ (for the case $p_{decoy} = p_{Z,Alice} = 0.5$) is 0, which yields a $QBER_{X,s}$ of 0. In the field ** both $m_{X,d}$ and n_{X_d} are 0, which yields a $QBER_{X,d}$ that is not calculable.

4.3 Variation of the Heater Voltage Amplitude

In this section, the variation in the heater voltage amplitude V_{amp} is looked at. The same procedure as in Section 4.2 is used. The starting parameters are listed in Table 4.5. The SKRs are optimized for p_{decoy} and $p_{Z,Alice}$ again. The only difference

to Section 4.2 is that the fiber attenuation is constant at 3 dB and $\mu_s = 0.25$ and $\mu_d = 0.175$. Again the best result is given for $n_{Z,s}$ factorized to 10^9 counts, with the other counts being scaled by the same factor.

Parameter	**Value**
$p_{z,Alice}$ for the simulation	0.5
p_{decoy} for the simulation	0.5
ϵ_{sec}	10^{-15}
ϵ_{cor}	10^{-9}
μ_s	0.25
μ_d	0.175
$V_{nosignal}$	-1.3
$V_{Z,signal}$	0.2
Fiber attenuation (dB)	6 dB
block size $n_{Z,s}$ is scaled to	10^9
Symbols sent	2 million

Table 4.5: Parameters for SKR over variation of heater voltage amplitude V_{amp}, consistent across V_{amp} values. The block size $n_{Z,s}$ gets scaled to is 10^9, all other counts are scaled accordingly. $p_{z,Alice}$ and p_{decoy} are only chosen like this for the simulation. For the weighted counts later other $p_{z,Alice}$ and p_{decoy} are optimal.

The results are summarized in Table 4.6. For the variation of heater voltage amplitude V_{amp} chosen to be $V_{amp} = 11mV$, no SKR was observable. For V_{amp} between $V_{amp} = 5.5mV$ and $V_{amp} = 1.1mV$ one cannot observe a clear trend. In an attempt to keep the variations as small as possible for the rest of the simulations a V_{amp} of $V_{amp} = 0.0011V$ was chosen. ToDo: write more with new values.

V_{amp} **(mV)**	**calc.** p_{decoy}	**calc.** p_{ZAlice}	**SKR** ($\frac{MBit}{s}$)
11	-	-	-
5.5	0.04	0.98	9,72
4.4	0.08	0.98	9,89
3.3	0.08	0.98	9,32
2.2	0.04	0.98	9,93
1.1	0.14	0.96	8,34

Table 4.6: Parameters for the SKR measurement. The fiber attenuation in dB is given to the simulation. μ_s and μ_d are the mean photon numbers for the signal and the decoy states which are sent with a probability of p_{decoy} and 1 - p_{decoy}, respectively. The dashes represent non-existent results for the respective V_{amp} value.

In Table 4.7, the QBER for X and Z basis and decoy or signal states were calculated. One can observe fairly stable total counts, with only the total counts for $V_{amp} = 11mV$ being higher. The $QBER_{X,s}$ and the $QBER_{X,d}$ decrease for V_{amp} being smaller, while the $QBER_{Z,s}$ and $QBER_{Z,d}$ remain fairly constant. ToDo: neu schreiben mit weiteren Daten

V_{amp} **(mV)**	$QBER_{Z,s}$	$QBER_{Z,d}$	$QBER_{X,s}$	$QBER_{X,d}$	**counts**	**symbols**
0.011	0.0358	0.0648	0.2656	0.4400	9576	2 million
0.0055	0.0344	0.0635	0.1140	0.1172	9286	2 million
0.0044	0.0364	0.0532	0.1065	0.1103	9306	2 million
0.0033	0.0386	0.0585	0.0491	0.0583	9316	2 million
0.0022	0.0348	0.0514	0.0076	0.0227	9269	2 million
0.0011	0.0361	0.0609	0.0096	0.0625	9325	2 million ??

Table 4.7: Quantum Bit Error Rates (QBER) for signal and decoy states across different assumed amplitude of the heater voltage values V_{amp}. Counts indicates the total counts measured is the sum of all $n_{B,k}$ and $m_{B,k}$ for the case $p_{decoy} = p_{Z,Alice} = 0.5$ and symbols are the total symbols that were being sent.

4.4 SKR with different extinction ratio

In this section, the extinction ratio is changed and compared to the extinction ratio used in Section 4.2 and Section 4.3. With the previous setting of $V_{nosignal} = -1.3$ and $V_{Z,signal} = 0.2$ together with Figure 3.11, one gets an extinction ratio of 16.7

dB from $V_{nosignal}$ to $V_{Z,signal}$. In this section, $V_{nosignal}$ and $V_{Z,signal}$ are changed to $V_{nosignal} = -2.1$ and $V_{Z,signal} = 0.4$, which yields an extinction ratio of 20.7 dB.

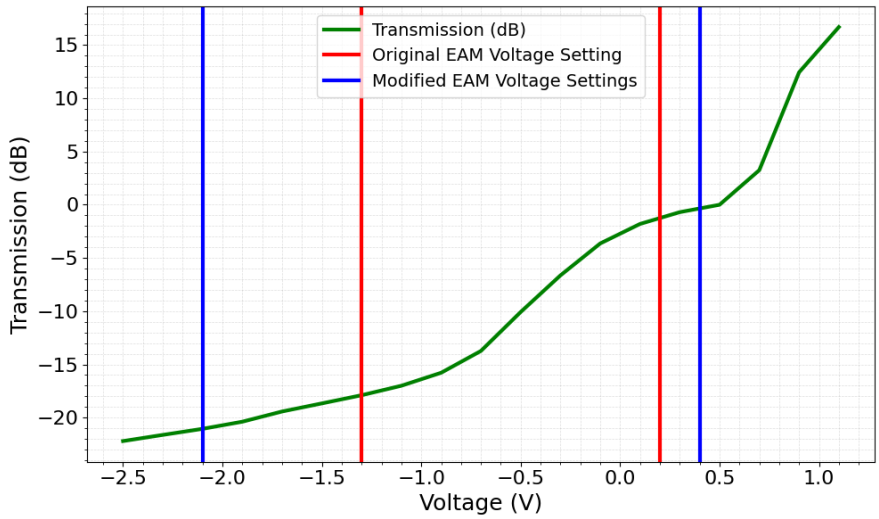


Figure 4.7: Electro-absorption modulator (EAM) transmission (green) as a function of applied initialization voltage for the modulation of the laser light at the EAM. The plot shows how the optical transmission through the EAM varies with the applied initialisation voltage, demonstrating the modulator's ability to control light intensity for signal modulation. This is used to create the states Z_0, Z_1 and X_+. The vertical red lines represent the original initialization voltage settings, which are $V_{nosignal} = -1.3$ and $V_{Z,signal} = 0.2$. The vertical blue lines represent the modified initialization voltages at the EAM $V_{nosignal} = -2.1$ and $V_{Z,signal} = 0.4$.

For comparability reasons, all the simulation runs in this section are the same as in Section 4.2. Table 4.8 shows the input parameters of the simulation, that are the same for all runs. Again, the best results were achieved for the scaling the $n_{Z,s}$ counts to 10^9, adjusting all other values $n_{B,k}$ and $m_{B,k}$. The assumed voltage amplitude for the heater is chosen to be 1.1 mV to be safe, that a secret key rates can be obtained.

Parameter	**Values**
$p_{z,Alice}$ for the simulation	0.5
p_{decoy} for the simulation	0.5
ϵ_{sec}	10^{-15}
ϵ_{cor}	10^{-9}
$V_{nosignal}$	-2.1
$V_{Z,signal}$	0.4
Fiber attenuation (dB)	3
Symbols sent	2 million
block size $n_{Z,s}$ is scaled to	10^9
V_{amp} (V)	0.0011
I_{amp} (A)	0.00041

Table 4.8: Parameters for SKR over attenuation, consistent across V_{amp} values. The block size $n_{Z,s}$ gets scaled to is 10^9, all other counts are scaled accordingly. $p_{z,Alice}$ and p_{decoy} are only chosen like this for the simulation. For the weighted counts later other $p_{z,Alice}$ and p_{decoy} are optimal. The block size $n_{Z,s}$ gets scaled to is 10^9, all other counts are scaled accordingly.

The results and the comparison is shown in Table 4.9. One can approximately see the same outlier SKR value as for 9 dB in the modified 20.7 dB extinction ratio simulation run. In general, the modified case yields a slightly lower secret key rate.

Att. (dB)	μ_s	μ_d	**Original (16.7 dB)**			**Modified (20.7 dB)**		
			p_{decoy}	$p_{Z,Alice}$	SKR ($\frac{Mbit}{s}$)	p_{decoy}	$p_{Z,Alice}$	SKR ($\frac{Mbit}{s}$)
1	0.10	0.07	0.06	0.98	12,71	0.04	0.98	13,62
3	0.125	0.075	0.04	0.98	9,71	0.06	0.98	1,60
6	0.25	0.175	0.08	0.92	7,84	0.1	0.98	9,46
9	0.50	0.35	0.08	0.92	10,58	0.16	0.96	9,48

Table 4.9: Comparison of original and modified configurations across fiber attenuation levels. The original run is for 16.7 dB and the new modified run is at 20.7 dB.

Att. (dB)	$QBER_{Z,s}$		$QBER_{Z,d}$		$QBER_{X,s}$		$QBER_{X,d}$	
	Orig.	**Mod.**	**Orig.**	**Mod.**	**Orig.**	**Mod.**	**Orig.**	**Mod.**
1	0.0338	0.0173	0.0566	0.0294	0.0045	0.0075	0.0109	0.0313
3	0.0322	0.0161	0.0593	0.0361	0.0179	0.0388	0.0052	0.0417
6	0.0361	0.0169	0.0609	0.0288	0.0096	0.0152	0.0625	0.0446
9	0.0307	0.0181	0.0720	0.0262	0.0208	0.0167	0.0446	0.0515

Table 4.10: Comparison of QBERs in Z and X bases for signal and decoy states between original and modified simulation runs across fiber attenuation values.

The comparison of total counts is shown in Table 4.11. One can see that the overall counts go down with increasing fiber attenuation.

Att. (dB)	**Symbols**		**Counts**	
	Orig.	**Mod.**	**Orig.**	**Mod.**
1	2 million	2 million	11805	13629
3	2 million	2 million	93973	10082
6	2 million	2 million	9325	10760
9	2 million	2 million	9295	10953

Table 4.11: Comparison of total symbols sent and total detection counts between original and modified simulations across various fiber attenuation values. "Counts" is the total number of detection events (sum of all $n_{B,k}$ and $m_{B,k}$), and "Symbols" refers to the total number of symbols sent per run, with $p_{decoy} = p_{Z,Alice} = 0.5$.

Chapter 5

Conclusion

5.1 Discussion

The following discussion will address the experimental results obtained in Section 4.

The simulated histogram looks as expected, with observable destructive interference in the X basis. One can nicely see the decoy states, yielding partial destructive interference between, for example, a $Z_{1,signal}$ state and a $Z_{0,decoy}$ state.

One has to keep in mind that with the simulation runs that were done for this thesis, the ratio r between μ_s and μ_d could not be perfectly calibrated for every attenuation, which is a big part of optimizing the SKR. This means that the SKRs at different attenuations cannot be perfectly compared, as the fixed ratio of $r = \frac{10}{7}$ is for some attenuations more optimal than others. In Rusca et al. [11] the ratio of μ_s and μ_d was swept as well, which leads to a SKR that continually decreases with an increasing attenuation (see Figure 2 in [11]).

When looking at the SKR over the attenuation at an peak to peak extinction ratio of 16.7 dB the obtained SKRs displayed in Table 4.3 are realistic with the SKR being between $0.06\frac{MBit}{s}$ and $12.71\frac{Mbit}{s}$. This can be compared to Beutel et al. [17], where SKRs of 12.17 $\frac{Mbit}{s}$ at 10 dB channel attenuation were demonstrated. As mentioned in Section 2.7, the receiver chip in [17] has four channels. This means that the SKR is calculated for four parallel channels, which allows one to send four times the amount of photons per second. Because of this, the SKR is expected to be 4 times as high as in the simulation. In [17] in Figure 2a), one can see detection efficiencies for the Z basis of 17 % which is about half of what is assumed in the simulation. In addition to this, with the simulation not all potential error sources are included, e. g. the delay line loss is missing in the simulation. In an experiment, all errors sources are included, which worsens the result. The higher key rate in the simulation could stem from the fact that the

channel attenuation in the paper is not the same as the fiber attenuation in the simulation. In addition, a trend of a decreasing key rate for an increasing fiber attenuation can be observed for attenuations between 1 and 19 dB, with only one outlier at 9 dB. One reason for that could be that the ratio between μ_s and μ_d is not finely calibrated for the fiber attenuations 1 to 6. One could assume that if they were to be perfectly tuned, they would yield higher SKRs.

The simulated QBER rates are relatively small with the highest being 7.2% in the Z basis. This is to be expected, as no fabrication error for the DLI is assumed, which would reduce the visibility. In general, reducing the dead time increases the maximum count rates but also increases the after-pulse probability and hence the QBER [8]. The dead time influences the count rates more at lower attenuation, as there more counts are measured at low attenuations. This is why increasing the attenuation simulates an increase in the dead time, because less photons per seconds get detected. As expected, the QBERs increase with an increase in attenuation in Table 4.3.

To evaluate the significance of wavelength stabilization, a sweep over the voltage amplitude V_{amp} was carried out. Key rates up to $9.8\frac{Mbits}{s}$ were obtained and noted in Table 4.6. No clear trend in the SKR can be observed with key rates between $9,32\frac{Mbit}{s}$ and $9.93\frac{Mbit}{s}$. This indicates that the fluctuations are statistical and below a V_{amp} of $V_{amp} = 5.5mV$, one can freely choose V_{amp}. This choice was set to $V_{amp} = 1.1mV$. It is important to note that the previously assumed $V_{amp} = 0,011V$ did not yield a SKR. For the simulation to yield results, it had to be adjusted. This indicates that for stable results in this specific measurement setup a precise voltage control is necessary for the setup to work.

Lastly, the SKR with a different extinction ratio (ER) was analyzed to the modulator performance. One expects for higher extinction ratios, smaller QBERs, as the difference between no pulse being sent and a pulse being sent is better. This trend is mostly not observed in Figure 4.10. One can also see in Figure 4.9 that the overall SKR is decreasing when looking at the simulation matches with the 20.7 dB extinction ratio in comparison to the 16.7 dB extinction ratio. This is not expected. A reason for that could be that the peak-to-peak ER was adjusted by adjusting the voltage peak values. However, the change in signal shape due to the non-linearity of the EAM response has not been taken into account.

There are several reasons why the SKRs obtained in the simulation are only upper bounds for realistic SKRs on devices. Firstly, multiplexing isn't included in the simulation. Multiplexing can introduce crosstalk, which would elevate the error counts and lead to a worse result. Secondly, for the simulation fabrication variations for the passive basis choice for Bob and the DLI are not accounted for. Thirdly, the polarization is not included at all in the simulation. The polarization stability of the symbols being sent influences the detection efficiency of the detec-

tors and the visibility. In this case, vibration and temperature changes in the fiber become significant. Fourthly, because the sender and receiver chip is connected with a fiber, there can be stray light, that goes into the system which isn't simulated. Lastly, an aspect worth it to mentioning is dispersion, which can lead to a pulse broadening in the fiber.

5.2 Summary

The objective of this thesis was to develop and analyze a Monte Carlo simulation of a three-state BB84 quantum key distribution (QKD) protocol utilizing time-bin encoding and incorporating the one-decoy state method. The simulation was designed to closely emulate conditions expected in a photonic QKD chip. The core focus of the work involved constructing the simulation environment and integrating hardware-specific parameters. This included setting up the software infrastructure and modeling key features relevant to the operation of a photonic QKD chip.
Using this simulation, secret key rates were evaluated over varying levels of attenuation, and the influence of key hardware variances, such as fluctuations in heater voltage, was systematically analyzed. Additionally, the effect of the peak-to-peak extinction ratio on system performance was investigated.
The thesis began with an introduction to Quantum Key Distribution, highlighting the BB84 protocol as a foundational example. The implementation details of the three-state BB84 protocol, particularly the choice of time-bin encoding, were presented. The vulnerability posed by photon-number-splitting (PNS) attacks and the corresponding mitigation strategy through the one-decoy state method were discussed. Furthermore, the calculation methods for SKR and QBER were detailed, and the suitability of photonic platforms for QKD applications was briefly outlined.
Subsequently, the key components of a photonic QKD chip were examined, and the operation of the simulation was demonstrated using histograms. The simulation was capable of calculating SKRs over transmission distances up to 100 km. In terms of heater voltage variance, a significant reduction in SKR was observed at $11mV$ variance, whereas no consistent trend could be identified between $5.5mV$ and $2.2mV$. A minor decrease in SKR at $1.1mV$ may be attributed to imperfect choice of the mean heater voltage.
The analysis of the peak-to-peak extinction ratio, comparing values of $16.7dB$ and $20.7dB$, showed no clear trend in SKR performance. This could potentially be explained by the omission of nonlinear effects in the electro-absorption modulator response within the current simulation model.
In summary, the simulation developed in this thesis proves to be a versatile tool. It supports parameter optimization and can be adapted to closely reflect experi-

mental constraints, making it well-suited to study the experimental conditions for QKD.

5.3 Outlook

Following this bachelor thesis, several things can be addressed regarding the implementation and analysis of the simulation. Multiplexing could have been implemented to get even closer to the chip design the simulation is trying to simulate. This can include crosstalk between the channels and possible correlations. This would make the error rate and the privacy amplification worse. In addition to that, the phase randomization could have been implemented together with the polarization stability. This would worsen the secret key rate, as the detection efficiency would be worse, leading to fewer detections for the overall symbols that are being sent. Even with the existing simulation, the simulation can be analysed more deeply. In the simulation, the passive basis choice of Bob $p_{Z,Bob}$ is set to $p_{Z,Bob} = 0.5$, but $p_{Z,Bob}$ can also be changed to any value between 0 and 1. In addition to that, in Section 4 the probabilities $p_{Z,Alice}$ and p_{decoy} are swept in 0.02 increments. Doing a finer sweep could yield a higher SKR. The most effective step would be to properly optimize the ratio between μ_s and μ_d, here called r independently for all attenuations. This guarantees that the SKRs are more comparable between attenuations. This can be done by going through the attenuation and sweeping μ_s and μ_d independently.

Appendix A

Acknowledgement

First and foremost, I would like to thank Julius Römer for supervising me throughout the process of working on this thesis. You were always available, listened patiently and provided valuable feedback. Thank you for the hours you spent, so this all could work.
A big thank you to Prof. Dr. Wolfram Pernice for being my primary examiner and to Prof. Dr. Lauriane Chomaz for being my second examiner.
Furthermore, I would like to thank Philipp and Frank, who were always available for questions and provided me with more inside into the theory behind all different components.
Additionally I would like to thank Simon Thamm for the discussions and the time piecing the puzzle pieces together.
Thank you to my family at home, my boyfriend and my friends who have supported me, whether it be by providing emotional support, welcome distraction, when I needed it and proofreading the thesis. I am so grateful to have you in my life and you have made this journey so much easier.

Bibliography

[1] Valerio Scarani et al. "The security of practical quantum key distribution". In: *Reviews of modern physics* 81.3 (2009), pp. 1301–1350.

[2] Lily Chen et al. *Report on post-quantum cryptography*. Vol. 12. US Department of Commerce, National Institute of Standards and Technology ..., 2016.

[3] Charles H Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical computer science* 560 (2014), pp. 7–11.

[4] Davide Rusca and Nicolas Gisin. "Quantum cryptography: an overview of quantum key distribution". In: *arXiv preprint arXiv:2411.04044* (2024).

[5] Ramona Wolf. *Quantum Key Distribution. An Introduction with Exercises*. eng. Springer eBook Collection. Cham: Springer International Publishing, 2021, 1 Online–Ressource (XI, 229 p.) ISBN: 978-3-030-73991-1. DOI: 10.1007/978-3-030-73991-1.

[6] Chi-Hang Fred Fung and Hoi-Kwong Lo. "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry". In: *Physical Review A* 74.4 (Oct. 2006). ISSN: 1094-1622. DOI: 10.1103/physreva.74.042342.

[7] Ilaria Vagniluca et al. "Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution". In: *Physical Review Applied* 14.1 (July 2020). ISSN: 2331-7019. DOI: 10.1103/physrevapplied.14.014051.

[8] Alberto Boaron et al. "Simple 2.5GHz time-bin quantum key distribution". In: *Applied Physics Letters* 112.17 (Apr. 2018), p. 171108. ISSN: 0003-6951. DOI: 10.1063/1.5027030. eprint: https://pubs.aip.org/aip/apl/article-pdf/doi/10.1063/1.5027030/19753557/171108_1_online.pdf.

[9] Federico Grasselli. *Quantum Cryptography. From Key Distribution to Conference Key Agreement*. eng. Springer eBook Collection. Cham: Springer, 2021, 1 Online–Ressource (XVII, 152 Seiten). ISBN: 978-3-030-64360-7. DOI: 10.1007/978-3-030-64360-7.

[10] Evan Meyer-Scott, Christine Silberhorn, and Alan Migdall. "Single-photon sources: Approaching the ideal through multiplexing". In: *Review of Scientific Instruments* 91.4 (Apr. 2020), p. 041101. ISSN: 0034-6748. DOI: 10.1063/5.0003320. eprint: https://pubs.aip.org/aip/rsi/article-pdf/doi/10.1063/5.0003320/19771655/041101_1_online.pdf.

[11] Davide Rusca et al. "Finite-key analysis for the 1-decoy state QKD protocol". In: *Applied Physics Letters* 112.17 (Apr. 2018), p. 171104. ISSN: 0003-6951. DOI: 10.1063/1.5023340. eprint: https://pubs.aip.org/aip/apl/article-pdf/doi/10.1063/1.5023340/13995801/171104_1_online.pdf.

[12] Anqi Huang et al. "Quantum key distribution with distinguishable decoy states". In: *Physical Review A* 98.1 (2018), p. 012330.

[13] Won-Young Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Phys. Rev. Lett.* 91 (5 2003), p. 057901. DOI: 10.1103/PhysRevLett.91.057901.

[14] Wei-Tao Liu et al. "Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution". In: *Phys. Rev. A* 83 (4 2011), p. 042326. DOI: 10.1103/PhysRevA.83.042326.

[15] Charles Ci Wen Lim et al. "Concise security bounds for practical decoy-state quantum key distribution". In: *Phys. Rev. A* 89 (2 2014), p. 022307. DOI: 10.1103/PhysRevA.89.022307.

[16] Wei Luo, Liang Cao, Yichi Shi, et al. "Recent progress in quantum photonic chips for quantum communication and internet". In: *Light: Science & Applications* 12.1 (2023), p. 175. DOI: 10.1038/s41377-023-01173-8.

[17] Fabian Beutel et al. "Fully integrated four-channel wavelength-division multiplexed QKD receiver". In: *Optica* 9.10 (2022), pp. 1121–1130.

[18] M. Baier et al. "Integrated transmitter devices on InP exploiting electro-absorption modulation". In: *PhotoniX* 1.1 (2020), p. 4. DOI: 10.1186/s43074-020-0003-4.

[19] Reuven Y. Rubinstein. *Fast sequential Monte Carlo methods for counting and optimization*. eng. Ed. by Radislav [MitwirkendeR] Vaisman. Wiley Series in probability and statistics. Includes bibliographical references and index. - Description based on print version record. Hoboken, N.J.: J. Wiley Sons, 2014, 1 online resource (1 v.) ISBN: 978-1-118-61235-4 and 1-118-61235-3.

[20] Brendon L. Higgins, Jean-Philippe Bourgoin, and Thomas Jennewein. "Numeric estimation of resource requirements for a practical polarization-frame alignment scheme for quantum key distribution (QKD)". In: *Advanced Optical Technologies* 9.5 (Aug. 2019), 253–261. ISSN: 2192-8576. DOI: 10.1515/aot-2020-0016.

[21] W. Zhao et al. "Monte Carlo-based security analysis for multi-mode continuous-variable quantum key distribution over underwater channel". In: *Quantum Information Processing* 21.186 (2022). DOI: 10.1007/s11128-022-03533-6.

[22] OpenAI. *ChatGPT: AI assistant used for code scaffolding, plotting, and infrastructure suggestions*. Accessed April 29, 2025. 2024.

[23] Weng W. Chow and Stephan W. Koch. *Semiconductor-laser fundamentals. physics of the gain materials*. eng. Includes bibliographical references and index. Berlin ; Heidelberg [u.a.]: Springer, 1999. ISBN: 3-540-64166-1 and 978-3-540-64166-7.

[24] Filip Jonathan Imielowski. *Development of Laser Driver Circuits for Wavelength-Multiplexing Application*. Bachelor's thesis. 2024.

[25] AMD (Advanced Micro Devices). *RF-DAC Electrical Characteristics. Zynq UltraScale+ RFSoC Data Sheet: DC and AC Switching Characteristics*. https://docs.amd.com/v/u/en-US/ds926-zynq-ultrascale-plus-rfsoc-data-sheet. Accessed April 12, 2025. AMD Technical Information Portal.

[26] Ayfer Ozgur. *Lectures 9-10: Sampling Theorem*. ENGR76 lecture notes. Stanford University. 2024.

[27] *Mathematical Physics II*. eng. Basel, Switzerland: MDPI - Multidisciplinary Digital Publishing Institute, 2020, 1 Online–Ressource (182 p.) ISBN: 978-3-03943-495-4 and 978-3-03943-496-1.

[28] Corning Inc. *SMF-28® ULL Optical Fiber Datasheet*. https://www.fionec.com/wp-content/uploads/Corning_SMF-28-ULL_2020-03.pdf. Accessed: 2025-04-14. 2020.

[29] Bahaa E. A. Saleh and Malvin Carl Teich. *Fundamentals of photonics*. eng. Second edition. Wiley series in pure and applied optics. Hoboken, New Jersey: Wiley-Interscience, 2007, 1 Online–Ressource (XIX, 1177 Seiten). ISBN: 978-1-118-58581-8.

[30] Ransom Stephens. "Jitter analysis: The dual-Dirac model, RJ/DJ, and Q-scale". In: *Agilent Technical Note* (2004).

[31] Fabian Beutel. "High Key-Rate On-Chip Quantum Key Distribution with Waveguide-Integrated Single-Photon Detectors". Doctor rerum naturalium (Dr. rer. nat.) in Physics. Inaugural-Dissertation. Münster, Germany: Westfälische Wilhelms-Universität Münster, 2022.

Appendix B

Declaration

I confirm that I have written this thesis independently and have not used any sources or aids other than those specified.

Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Heidelberg, den 30. April 2024

Lea Bauer