Handheld Quantum Key Distribution

Jannik Luhn

München 2017

Handheld Quantum Key Distribution

Jannik Luhn

Master's Thesis
Faculty of Physics
Ludwig-Maximilians-Universität
Munich

Supervised by
Prof. Dr. Harald Weinfurter

Submitted on
May 17th, 2017

Mobiler Quanten-Schlüsselaustausch

Jannik Luhn

Masterarbeit
Fakultät für Physik
Ludwig-Maximilians-Universität
München

Betreut von
Prof. Dr. Harald Weinfurter

Eingereicht am
17. Mai 2017

Contents

1. Introduction

The ability to speak is one of the most important characteristics of humankind. It enables efficient transfer of information between different individuals, boosting the ability to learn and making the collaborative development of complex ideas possible. The historical influence of speech is illustrated by the observation that advances in communication technologies are often accompanied by major sociological revolutions. For instance, the development of writing in Mesopotamia in the 4th millenium BC occurred simultaneously to the emergence of state societies [1]. Likewise, the invention of the printing press in the 15th century coincides with Europe's transition from the Medieval Period to the Renaissance [2].

More recently, the idea to use electromagnetic signals in order to transmit information enabled communication over long distances without serious delay. This culminated in the development of the Internet, a network capable of connecting essentially any two persons on the planet.

While the ability to easily transmit messages over long distances brings about substantial benefits, at least one problem is essentially unavoidable: It is practically impossible to physically shield the channel between sender and receiver against eavesdroppers. However, secrecy of messages is often a crucial desire. Therefore, efficient encryption techniques have been developed that try to encode the message in such a way that an adversary who intercepts it is unable to extract its meaning. Only the designated receiver should be able decode the message properly, often achieved by means of some pre-shared secret.

However, the most widely used encryption techniques are fundamentally insecure, as are the preparation protocols that establish shared secrets to begin with: They are susceptible to brute force attacks and—more importantly—in some cases breakable by quantum computers. Efficient attacks using classical computers have not been found yet, but their nonexistence remains to be proven. Thus, the security of such protocols relies on technological and financial limitations of the attacker.

As an alternative, quantum key distribution (QKD) has been proposed in 1984 [3] and, independently, in 1991 [4]. In combination with the One-Time-Pad, a classical encryption scheme, it allows for unconditionally secure communication [5, 6], i.e., its security can be proven even under the assumption that the eavesdropper is capable of carrying out any physically possible operation on the transmitted signals. Sender and receiver are able to detect eavesdropping attempts and can and estimate the amount of information the attacker has extracted. With this knowledge,

secrecy can either be reestablished by classical post-processing steps or the protocol can safely abort without having leaked any confidential information.

Unfortunately, a variety of technical challenges hinder mainstream adoption of QKD. In particular, QKD requires the transmission of quantum states between sender and receiver, usually carried by photons. Thus, electrical conductors, which are typically employed in conventional communication systems, do not constitute viable channels. Instead, free space or optical fiber connections have to be used. Furthermore, transmission losses limit the maximally achievable distance.

A large fraction of the QKD experiments performed in the last decades was aimed at increasing the distance between sender and receiver. Beginning with the first experimental realization over a distance of 30 cm [7], the current distance record is a key exchange over 404 km of fiber [8]. A multitude of impressive free-space experiments demonstrated the versatility of QKD, including long-distance connections between islands [9, 10] as well as key exchanges between ground-station and aircraft [11], hot-air balloon [12], and truck [13]. Today, a goal aspired by many is to achieve a key exchange with a satellite [14]. Many experiments were already performed to pave the way to this end [15–18].

At the same time, miniaturized QKD devices that are optimized for short distances promise to serve a range of use-cases as well. For instance, both mobile devices and the Internet of Things rely on the ability to communicate securely but do not tolerate large form factors. Our experiment addresses this space. A miniaturized sender was designed and assembled by Mélen [19]. A suitable receiver featuring active beam tracking and thus enabling handheld operation was set up by Vogl [20]. Both were characterized scrutinizingly by Freiwang [21]. Building on these results, this project develops an analysis procedure, undertakes a sequence of handheld key exchange measurements, and assesses the performance of the system.

The present thesis is organized as follows: Chapter 2 introduces the problem of key distribution using the example of a classical algorithm. Chapter 3 describes the idea behind quantum key distribution, addressing the BB84 protocol in particular. Chapter 4 reviews the experimental setup, Chapter 5 the analysis procedure. In Chapter 6, measurement results are presented and discussed. Chapter 7 provides a conclusion and suggests future improvements.

2. Classical Key Distribution

Before investigating quantum key distribution, in this chapter its classical counterpart is described. The basic idea behind the protocol is discussed and illustrated using the example of the well known Diffie-Hellman scheme. Finally, the assumptions made on the adversary are evaluated.

2.1. Motivation

Assume that a sender ("Alice") wants to transmit a message to a remote receiver ("Bob"). The channel through which the message is communicated can also be accessed by an eavesdropper ("Eve"), from whom Alice and Bob want to keep the message secret.

To solve this problem, Alice transforms the message in such a way that only Bob but not Eve can revert this operation to recover the so-called plaintext. This process of disguising the message is called encryption, its reverse decryption, and the intermediary result a cyphertext [22].

According to Kerckhoffs' principle [23], cryptographic algorithms should be considered publicly known. The only secrets Alice and Bob are allowed to have are keys, i.e., parametrizations of the encryption algorithms randomly chosen for each use.

The most straightforward cryptographic algorithms are symmetric, i.e., the same key is used for encryption and decryption. Examples are the One-Time-Pad [23] and the Advanced Encryption Standard (AES) [24] which will briefly reviewed in the following.

One-Time-Pad (OTP) The OTP requires a key K of the same length as the plaintext M. Then, the cyphertext $C = M \oplus K$, where $\oplus$ denotes the bitwise XOR operation, and $M = C \oplus K$. Despite their simplicity, OTPs are unbreakable in the sense that it is mathematically impossible to recover M from C without knowledge of K. Still, they are rarely used for practical reasons.

Advanced Encryption Standard (AES) The key for AES has a length of 128, 192 or 256 bits. First, the message is split into 128 bit blocks. Subsequently, each block is modified in several rounds of substitution (replacing bytes using a lookup table), permutation (changing the byte order) and mixing (bytes are

correlated with each other using matrix multiplication). Additionally, blocks are XORed with a round key that is derived from the original key but changes after each round.

For decryption, the inverse of each operation is applied to the encrypted block. This can be done in an efficient way if the key is known.

In order to use symmetric encryption to secure their communication, Alice and Bob need to agree on a secret key in advance. Often, they desire to do this repeatedly for each communication session. This is to minimize the required time to securely store the key and therefore mitigate the risk of compromising its security [22]. In case of the OTP, a new key for every message is even obligatory.

In summary, techniques are necessary with which Alice and Bob can securely and efficiently generate shared secret data, having no or few secrets in the beginning. Such protocols are called key agreement, key distribution, or key exchange protocols. If they rely on quantum mechanics they are called quantum, otherwise classical protocols.

2.2. Example: Diffie-Hellman Key Exchange

The first key exchange protocol, named Diffie-Hellman after its inventors, was proposed in 1976 [25]. It is an example for an asymmetric algorithm because each party has their own private key as well as a public one shared with every other party.

In order to exchange a secret key, Alice and Bob first have to generate their private keys—a random large number, x at Alice and y at Bob. The protocol specifies a large prime number n and an integer $g < n$. With these, they can calculate their public keys X and Y as follows:

$$X = g^x \mod n, \tag{2.1a}$$
$$Y = g^y \mod n, \tag{2.1b}$$

where $\mod n$ indicates calculation in the multiplicative group modulo n. X and Y are publicly communicated to the other party and any interested eavesdropper. To finally arrive at a shared secret

$$k = g^{xy} \mod n \tag{2.2}$$

Alice and Bob compute, respectively,

$$k_A = Y^x \mod n, \tag{2.3a}$$
$$k_B = X^y \mod n. \tag{2.3b}$$

Since

$$\begin{aligned} k_A &= Y^x \mod n \\ &= (g^x \mod n)^y \mod n \\ &= g^{xy} \mod n \\ &= k \end{aligned} \tag{2.4}$$

and similarly for k_B, Alice and Bob have aggreed on the key k. In contrast, an attacker ideally is unable to retrack this computation.

2.3. Security Assumptions

In the Diffie-Hellman protocol, Alice's and Bob's private keys are, of course, not published explicitly. However, the public keys contain exactly the same information, just in conceiled form. An adversary capable of reversing Equation 2.1, i.e., finding x for a given X, can recover the private key from the public key. This possibility breaches the security of the system.

Therefore, to successfully argue that Diffie-Hellman and other classical key exchange protocols are indeed secure, some assumption on the attacker's powers must be made. A widely used approach consists in defining the so called computational security [24]. It allows attackers to only employ feasible strategies that have a non-negligible success probability.

Feasibility can be formalized further as the condition of having a runtime (measured in, e.g., computer cycles) polynomial in n, where n is a security parameter such as the key length. An exemplary attack prohibited by this definition is to simply test every possible private key: There are 2^n different n-bit keys. Plugging all of them into Equation 2.1 thus takes a time proportional to 2^n. As this expression is not polynomial but exponential in n, such a "brute force" strategy is not allowed under the definition of computational security.

The final necessary assumption made for the Diffie-Hellman protocol is, that inverting Equation 2.1 or, more generally, calculating discrete logarithms is hard for the attacker, i.e., she does not have access to algorithms that are polynomial in n.

Both of these assumptions may be dubious, depending on the application. Computational security is broken if the attacker simply has enough time and resources.

If the trend of exponentially growing computational power over time predicted by Moore's law [26] continues, this issue becomes even more severe.

What is more, the hardness of the discrete logarithm using classical computation has not been proven. On the contrary, quantum computers can efficiently solve this problem using Shor's algorithm [27]. The same is true for integer factorization, on which the widely used RSA protocol is based [28]. A practical general quantum computer is not believed to be developed in the next decade, but progress is made fast and, considering the commercial interest, will likely continue in the future [29].

3. Quantum Key Distribution

In light of the notion of computational security and the resulting limited usefulness of classical key distribution schemes, the question arises if such assumptions are necessary. As first conjectured by Bennet and Brassard [30] and later proven by, among others, Shor and Preskill [31] as well as Mayers [5], this is not the case, if one takes a step from classical protocols to schemes utilizing quantum mechanics: So called quantum key distribution (QKD) protocols do not rely on any assumptions limiting the power of the adversary. In conjunction with the one-time-pad, they thus allow for unconditionally secure communication.

In this chapter, the fundamental principles of quantum mechanics enabling QKD are reviewed. Next, the BB84 protocol, which we implement in our experiments, and its decoy state extension is described. Finally, side-channels as potential attack vectors are discussed.

3.1. Properties of Quantum States

QKD relies on two fundamental principles of quantum mechanics: The destructive nature of measurements and the unclonability of quantum states. We focus the discussion of the consequences of these principles to qubits, which are, analogous to the classical bits, the atomic units of quantum information.

A qubit is a quantum state living in a two dimensional Hilbert space. As an orthonormal basis for this space, we define the states $|0\rangle$ and $|1\rangle$ employing Dirac's bra-ket notation. Therewith, any qubit $|\psi\rangle$ can be expressed as a superposition of the form

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{3.1}$$

where α and β are complex numbers satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. The included global phase factor is physically irrelevant. In vector notation, one can equivalently write

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{3.2}$$

which avoids to explicitly mention the chosen basis.

For photons as carriers of qubits, $|0\rangle$ might be associated with horizontal, $|1\rangle$ with vertical polarization. Diagonal and anti-diagonal polarization (±45°) would then be represented by $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, and left/right circular polariztion by $|L,R\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)$.

3.1.1. Measuring Quantum States

Observables, loosely defined as properties of a system that one can measure, are represented by self-adjoint linear operators A acting on elements of the Hilbert space. Such operators fulfill equations of the form

$$A|a_i\rangle = a_i\,|a_i\rangle\,, \tag{3.3}$$

where $|a_i\rangle$ and a_i are the so called eigenstates and eigenvalues of the operator.

Quantum mechanics postulates that, when a measurement is carried out, the numerical outcome will be equal to one of the eigenvalues. Furthermore, the state of the system will collapse onto the corresponding eigenstate. Which outcome and which final state is chosen can, in general, not be predicted with certainty. Results will merely follow a probability distribution

$$p_i = \left|\langle a_i|\psi\rangle\right|^2, \tag{3.4}$$

where $\langle a_i| = |a_i\rangle^\dagger$ is the eigenstate corresponding to outcome i and $|\psi\rangle$ is the state on which the measurement is performed.

Three well known operators in a two dimensional Hilbert space are the Pauli matrices σ_z, σ_x, and σ_y:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{3.5}$$

As can easily be verified, the eigenstates of σ_z are $|0\rangle$ and $|1\rangle$ with eigenvalues ±1. Therefore, σ_z is the operator responsible for polarization measurements in the horizontal/vertical (H/V) basis. Similarly, σ_x corresponds to diagonal/anti-diagonal (+/-) and σ_y to left/right-circular (L/R) polarization.

As an example, suppose that two parties, Alice and Eve, play a game: Alice prepares a photon in some state and sends it to Eve. Eve wins if she can tell Alice the original state, otherwise she loses.

In the first round Alice is restricted to the states $|0\rangle$ and $|1\rangle$. Therefore, Eve can simply measures with σ_z: As $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 1|0\rangle = \langle 0|1\rangle = 0$ she will, according to Equation 3.4, always get outcome $+1$ if Alice sends $|0\rangle$ and -1 if Alice sends $|1\rangle$. Eve can, thus, perfectly distinguish Alice's challenges and wins the game.

In the next round, Alice is additionally allowed to prepare diagonal and anti-diagonal photons: $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. If Eve would apply the same strategy and measure those states with σ_z, her result would be completely indecisive:

$$p_{+1}(|\pm\rangle) = \left|\langle 0| \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\right|^2 = \frac{1}{2}\left|\langle 0|0\rangle \pm \langle 0|1\rangle\right|^2 = \frac{1}{2},$$
$$p_{-1}(|\pm\rangle) = \left|\langle 1| \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\right|^2 = \frac{1}{2}\left|\langle 1|0\rangle \pm \langle 1|1\rangle\right|^2 = \frac{1}{2}. \tag{3.6}$$

(3.7)

In other words, for those photons that Alice prepared with diagonal polarization she would get outcome $+1$ and -1 with equal probability, no matter if Alice's state originally was diagonal or anti-diagonal. She would get the same results if she would simply throw a coin.

Another strategy for Eve might be to measure in σ_x. As the eigenstates of this operator are $|+\rangle$ and $|-\rangle$, it would enable her to distinguish those two states. However, now Eve is unable to learn anything about the horizontally and vertically polarized photons:

$$p_{\pm 1}(|0\rangle) = \left|\frac{1}{\sqrt{2}}(\langle 0| \pm \langle 1|)|0\rangle\right|^2 = \frac{1}{2}\left|\langle 0|0\rangle \pm \langle 1|0\rangle\right|^2 = \frac{1}{2},$$
$$p_{\pm 1}(|1\rangle) = \left|\frac{1}{\sqrt{2}}(\langle 0| \pm \langle 1|)|1\rangle\right|^2 = \frac{1}{2}\left|\langle 0|1\rangle \pm \langle 1|1\rangle\right|^2 = \frac{1}{2}, \tag{3.8}$$

Since, as was shown, σ_z can be used to distinguish between $|0\rangle$ and $|1\rangle$, and σ_x between $|+\rangle$ and $|-\rangle$, Eve might think that chaining those two measurements might help. But, after the first of these operations, the state will have collapsed to the eigenstate of the applied operator corresponding to the measurement result. This means that it carries no more information about the original state, rendering any additional measurement useless.

In summary, Eve cannot win this game all the time: Sometimes her best guesses will be wrong. Measurements give only a conclusive result if the states to distinguish are different eigenstates of the operator. The more they deviate from this ideal, the less informative is the outcome. In the most extreme case the measurement gives no information at all.

This is the fundamental principle exploited by quantum key distribution: The honest parties, Alice and Bob, encode their information in eigenstates of a randomly

selected basis unknown to the adversary, Eve. Thus, she will carry out her attack—some kind of measurement—using the wrong operator sometimes. This gives, first, meaningless results and, second, alters the states. This trace left by Eve can then be detected by Alice and Bob, estimating the severity of her attack.

3.1.2. Cloning Quantum States

If it is not possible to measure the same quantum system multiple times, one might suggest the following alternative: First, make several copies of the state and then measure each of those. Effectively, this would circumvent the former restriction.

However, perfectly cloning an arbitrary quantum state is prohibited by the no-cloning theorem, which can be proven for both pure [32, 33] and mixed [34] states. Some loopholes remain, though: For most, if not all, QKD protocols, the adversary has some prior knowledge about the sent state. In the case of BB84, for instance, only four different states are used. Thus, a machine designed to only copy a limited number of states might be sufficient to break the system, but is not ruled out by the general statement above.

Secondly, also an attack with an imperfect cloning apparatus must be considered. As shown by Bužek et al. [35], such a device could operate with a fidelity as high as $\sqrt{5/6}$. As it turns out, with such a quality an attacker cannot extract more information from the copied than from the original state, but this is not immediately apparent from the no-cloning theorem directly.

These examples illustrate the high amount of caution and carefulness one has to display when arguing for the security of QKD protocols, dictated by the goal of unconditional security. Despite all the necessary qualifications, though, the principle stated by the no-cloning theorem neatly condenses the essence of why QKD is secure.

3.2. The BB84-protocol

The first quantum key distribution (QKD) protocol was proposed by Bennet and Brassard in 1984 [3]. After its inventors and the year of publication, it was named BB84. Despite many more recent developments it is still widely used today, not only due to its simplicity but also because its performance is by no means inferior to its more recent descendants. As it is also implemented in our setup, this section is dedicated to describing the different steps in the protocol, an extension with decoy states to improve the protocol's practicality, and the formulas with which one can estimate the resulting secret key rate.

3.2.1. Original Protocol

Consider the same situation described in Chapter 2: Two honest parties, Alice and Bob, seek to establish a secret key between each other. They are connected via a quantum channel, over which Alice can send qubits to Bob. In practice, the states are usually encoded in photons and the channel may be free space or an optical fiber. The channel is assumed to be fully controlled by an eavesdropper, Eve: She can block signals, measure them, modify them, let them pass untouched, and even launch additional ones, at her discretion. She is not bound by any further restrictions, but only the laws of physics.

In addition to the quantum channel, Alice and Bob can exchange classical messages between each other. In contrast to its quantum counterpart, this channel is required to be authenticated: While Eve can read those messages (passive eavesdropping), she cannot impersonate Alice or Bob and send messages in their name (active eavesdropping).

Before the key exchange procedure starts, Alice and Bob agree on a common frame of reference. They name the eigenstates of σ_z $|H\rangle$ and $|V\rangle$, and the eigenstates of σ_x $|+\rangle$ and $|-\rangle$. Finally, they assign bit values to the four states: 0 to $|H\rangle$ and $|+\rangle$, 1 to $|V\rangle$ and $|-\rangle$.

The protocol proceeds as follows.

Preparation. Alice transmits a sequence of qubits over the quantum channel to Bob, each randomly chosen from the set $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$. The corresponding bases and bit values constitute her so called raw key.

Detection. Bob measures each of the received qubits in either σ_z or σ_x. The chosen bases and the measurement results are Bob's raw key.

Sifting. Bob announces over the classical channel, which qubits he detected and in which basis he has measured them. Alice announces her preparation bases. The bit values on both sides, in contrast, remain secret.

They discard all parts of their raw keys in which Bob did not detect anything or in which Alice's and Bob's basis choice differ. What remains on both sides are the sifted keys.

Post-processing In the final stage, Alice and Bob publicly estimate the error between their sifted keys—the quantum bit error rate (QBER). Subsequently, they perform two classical post-processing steps: Error correction removes the differences between Alice's and Bob's key. Privacy amplification squeezes out any information Eve might have about the key. Both steps reduce the key length.

In the final stage, Alice and Bob perform two classical post-processing steps: First, they correct differences in their sifted keys (error correction). As a byproduct, this gives them the quantum bit error rate (QBER), with which they can estimate the maximal amount of information Eve could have about the key. In the second step, called privacy amplification, the key is compressed such that the attacker's knowledge vanishes. Both steps reduce the final key length.

The idea behind the protocol is, that Eve is ignorant of the basis in which an individual state is prepared. If she tries to guess, she will guess wrong half of the times. Thus, her measurements will modify the state, which will result in an increased QBER. This in turn alerts Alice and Bob, who can therewith estimate the amount of knowledge Eve has about the key. In case they conclude that there is still some information about Alice's key that Bob but not Eve has, they continue with post-processing. Then, the step of privacy amplification is able to compress the key such that all of Eve's information is eliminated. However, if Eve is more knowing than Bob, this is not possible, but the protocol can safely abort. As BB84 is only a protocol to merely generate a key, but not to transmit a message, no secret data is compromised. Thus, in the end Alice and Bob either share a secure symmetric key or know that they do not.

3.2.2. Implementation with Weak Coherent Pulses

In the original BB84 protocol, the transmitted quantum states are supposed to be qubits carried by single quantum systems. Hence, in a physical implementation one would have to employ single photon emitters. While this technology is rapidly progressing, it still comes with a variety of limitations, including low repetition rates [36]. Therefore, in order to achieve higher key rates, our experiment as well as many others use laser pulses instead. They can be attenuated to such a degree that each pulse contains on average less than one photon.

Still, lasers do not emit single photons. Regardless of attenuation, they exhibit a Poissonian statistics:

$$P_\mu(n) = \frac{\mu^n}{n!} e^{-\mu}. \tag{3.9}$$

Here, $P_\mu(n)$ describes the probability of having n photons in a laser pulse with mean photon number per pulse μ. Only with probability $P_\mu(1) = \mu e^{-\mu}$ a pulse is ideal in the sense that it contains exactly one photon. With probability $P_\mu(n \geq 2) = 1 - e^{-\mu} - \mu e^{-\mu}$, however, a multi-photon pulse occurs. In those cases, an eavesdropper could pass only one photon to Bob and extract information from all the others. As this would not affect Bob's photon, the attack would not be detected. Only for photon

numbers approaching zero, this attack is negligible, but then the fraction of empty pulses $P_\mu(0) = e^{-\mu}$ increases, reducing the overall key rate.

This eavesdropping strategy is called photon number splitting (PNS) attack [37, 38]. To increase its effectiveness even further, Eve performs a quantum nondemolition measurement of the photon number, not modifying the polarization state. If the pulse contains more than one photon, she stores one and forwards the rest to Bob. If instead it is a single-photon pulse, she either blocks it or lets it pass with a chosen probability. Once Alice announces the preparation bases, Eve can measure the qubits in her memory and learn the bit values without introducing errors.

Blocking of single photon-pulses would result in a reduced channel transmission, which can be easily and accurately estimated by Alice and Bob. However, some absorption is inevitable in realistic systems, e.g., due to optical coupling losses or imperfect detection efficiencies. Eve is able to, in principle, replace those technical absorption loss mechanisms with her strategic filtering, and this change cannot be detected. Therefore, Alice and Bob have to assume that any reduced channel transmission is induced by an attack and increase the amount of privacy amplification accordingly, resulting in secret key rates scaling very unfavorably with e^{-T^2}.

Thus, the possibility of PNS attacks reduces the secure key rate significantly, especially when the transmission is low. In fact, in case of a transmission lower than the probability of single photon pulses detected by Bob, every single photon pulse might have been blocked and all detected ones are insecure, preventing any secret key distillation.

3.2.3. Decoy State Extension

As the PNS attack threatened to make the BB84 protocol impractical, a countermeasure was developed [39, 40]. Decoy state quantum key distribution is an easy to implement extension to BB84. The idea is to send, in addition to the normal signals, so called decoy pulses, characterized by a different intensity. As coherent states with different mean photon numbers are not orthogonal to each other, an attacker cannot distinguish between the two classes and has to treat both equivalently. When suppressing single photon pulses, she will then introduce different transmission values for decoy and for signal pulses, due to the different single-photon probability. This then enables Alice and Bob to distinguish between genuine losses and a PNS attack.

The effort necessary to extend an existing BB84 setup with decoy states is often small: One has to tune the intensity of the laser sources, which is usually required for calibration and stabilization anyways. In practice, it is favorable to have not only two intensity levels, but also to use the vacuum state as a third one [41]. For this, one has to turn the source off completely.

In our setup, sending decoy states is not as straightforward, as the developed electronics allow only to switch between high (signal) and low (vacuum) brightness. A solution proposed by Harrington et al. [42] is to send two different polarization states generated in individual sources simultaneously, resulting in a pulse with twice as much intensity. While this approach sounds promising, its security is questionable: Decoy pulses might be distinguishable in the polarization degree of freedom, violating a crucial assumption in the security proofs. For low enough intensities, however, indistinguishability is likely restored. A more in-depth assessment is undertaken by Höhn [43].

3.2.4. Secret Key Rate

After having achieved a general understanding of the BB84 protocol and its security, it is imperative to obtain a quantitative estimate of the resulting secret key rate. First, it allows an objective comparison between different systems. Second, the calculated parameters are important inputs for the error correction and privacy amplification algorithms.

A prerequisite for such calculations is a model for the system. Following [40, 41], we assume that our source emits phase randomized weak coherent pulses ρ_A with mean photon number μ:

$$\rho_A = \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} |i\rangle \langle i| . \tag{3.10}$$

Furthermore, the receiver is modeled as a threshold detector: It can only distinguish between zero and non-zero photon pulses, but not resolve the photon number. Thus, we define the transmittance of an i-photon state, i.e., the probability that an i-photon state produces a click in the detector, as

$$\eta_i = 1 - (1 - \eta)^i, \tag{3.11}$$

where η is the total transmission, incorporating channel losses, non-unity detection efficiencies, and time filtering. Then, the yield of an i-photon state is the probability of getting a click under the condition that an i-photon state is present at the detector. With the yield of zero-photon pulses Y_0, i.e., the darkcount rate, it is given by

$$Y_i = Y_0 + \eta_i - Y_0 \eta_i \approx Y_0 + \eta_i, \tag{3.12}$$

with good approximation for typical low noise and low transmission conditions. Then, the probability of registering a detection and having sent an i-photon state

is, according to the definition of conditional probability, the product of Y_i and the propability of an i-photon state

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}, \tag{3.13}$$

which is called the gain of i-photon states. Finally, the overall gain Q_μ of a pulse with mean photon number μ can be calculated via the law of total probability:

$$Q_\mu = \sum_{i=0}^{\infty} Q_i \approx Y_0 + 1 - e^{-\eta\mu} \tag{3.14}$$

and represents the probability of detecting something if a pulse has been emitted. Note that Alice and Bob can only estimate Q_μ directly. All quantities specific to a specific photon number, in particular Q_i, are hidden, enabling photon number splitting attacks.

As shown by Gottesman et al. [44], a BB84 system modeled as above is capable of generating secret keys at the rate

$$S_{\text{sec}} = \frac{Q_\mu}{2}\left[-f(\delta_\mu)H_2(\delta_\mu) + \frac{Q_1}{Q_\mu}[1 - H_2(\delta_1)]\right], \tag{3.15}$$

displayed in a form similar to the one used by Lo et al. [40]. Here, δ_μ denotes the average QBER, δ_1 the QBER of single-photon states, and $f(\delta_\mu)$ the efficiency of the error correction algorithm. H_2 is the binary Shannon entropy, defined as $H_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$

For an intuitive understanding of this essential formula, note that it is proportional to Q_μ, which is the probability to detect a pulse and can, thus, be associated with the raw key rate. The factor of $1/2$ expresses that half of the raw key is discarded during sifting. In the remaining sum, the first term quantifies losses due to error correction. The rest represents key compression during privacy amplification: Only a fraction Q_1/Q_μ of all pulses is resilient against PNS attacks, and of this a fraction $H_2(\delta_1)$ is still insecure due to measurements performed by Eve.

Since both Q_1 and δ_1 cannot be measured directly by Alice and Bob, they have to find worst case estimates. In the following, two of those are presented, one with and one without decoy states.

3.2.4.1. According to GLLP

Gottesman et al. [44] (GLLP) found approximations for the original BB84 protocol. They observe that in the worst case, only single photon pulses are blocked by the PNS attacker and every (presumably insecure) multi-photon pulse is detected. Therefore,

they bound the fraction of multi photon detections, or in their therminology the number of tagged bits Δ, by

$$\Delta = 1 - \frac{Q_1}{Q_\mu} \leq \frac{P_\mu(n \geq 2)}{Q_\mu} = \frac{1 - e^{-\mu} - \mu e^{-\mu}}{Y_0 + 1 - e^{-\mu\eta}}. \tag{3.16}$$

Ignoring background and expanding up to second order in μ, this simplifies to

$$\Delta \approx \frac{\mu}{2\eta}. \tag{3.17}$$

They also recognize, that in the worst case the QBER of multi-photon pulses is zero, such that all contributions to the average δ come from single-photon pulses. Thus, they estimate

$$\delta_1 \leq \frac{\delta}{1 - \Delta}. \tag{3.18}$$

In summary, their upper and, respectively, lower bounds for Q_1 and δ_1 are

$$Q_1^L = Q_\mu(1 - \Delta), \tag{3.19a}$$

$$\delta_1^U = \frac{\delta_\mu}{1 - \Delta} \tag{3.19b}$$

3.2.4.2. Using Decoy States

If also decoy states with mean photon number $\nu \neq \mu$ are being sent, Alice and Bob have also the parameter Q_ν available, allowing a much better approximation. Since the corresponding calculations are lengthy and little illuminating, we restrict ourselves to only show the results from [41]:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \tag{3.20a}$$

$$\delta_1^U = \frac{\delta_\mu Q_\mu - Y_0 e^{-\mu}/2}{Q_1^L}. \tag{3.20b}$$

As is illustrated in figure Figure 3.1, the resulting secrecy of the bits in the sifted key does not depend strongly on the transmission. This leads to much higher key rates in practical scenarios compared to the original BB84 protocol.

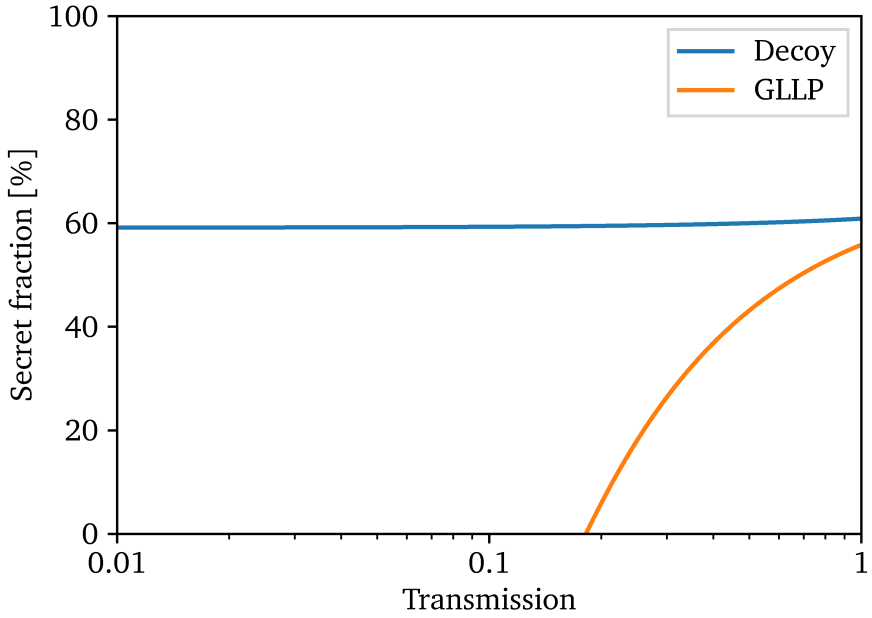


Figure 3.1.: Comparison between GLLP and decoy formulas. Plotted is the secret fraction, i.e., the secret key rate divided by the sifted key rate. A detector efficiency of 38 % and mean photon number of 0.1 has been assumed.

3.3. Classical Post-processing

After key sifting, Alice and Bob share a sequence of bits. However, for two reasons it is not yet usable as a key for symmetric encryption: First, Alice's and Bob's version differ slightly because of measurement errors and, possibly, attempts of eavesdropping. Second, an adversary might have gained some knowledge about the key in an attack. To distill a both symmetric and secure key, Alice and Bob therefore apply error correction and privacy amplification algorithms in the post-processing phase.

3.3.1. Error Correction

Error correction, also called reconciliation, aims to remove any errors between Alice's and Bob's sifted keys in order to obtain the same result at both sides. For this process, the two parties have to collaborate and exchange some information about their keys via the classical channel. To account for this loss of secrecy, the key length needs to be reduced appropriately. In this respect, error correction algorithms are limited according to Shannon [45], who states that keys with QBER δ must be shrinked by

at least a factor of $1-H_2(\delta)$, where $H_2(\delta) = -\delta\log_2(\delta)-(1-\delta)\log_2(1-\delta)$ refers to the binary Shannon entropy.

A variety of error correction algorithms has been developed, including Cascade [46], Winnow [47], and LDPC [48]. They differ in how close their efficiency is compared to the theoretical limit at different error rates. However, all of them are based on some variant of parity checking: Both Alice and Bob split up their sifted keys in blocks. For each block, the parity, i.e., the number of 1-bits, is computed and published. If the parities disagree, an error is found. By repeating the process on smaller and smaller subblocks the error is further and furher isolated and, eventually, can be corrected.

3.3.2. Privacy Amplification

After error correction, Alice and Bob share a common key, but they must assume that it is at least partially known to Eve. The amount of information Eve maximally has can, however, be estimated from QBER and transmission during the key exchange. With these figures and the expressions discussed in Section 3.2.4, Alice and Bob can calculate by how much they have to compress the key in order to make it secure, i.e., completely unknown to Eve.

For this so called privacy amplification step [49, 50], they express their key as a vector with n binary entries. To reduce its length to k, they multiply it modulo 2 with an $n \times k$ matrix, filled with random bits. This mixes the key in such a way, that one would need to know more than k bits of the original key in order to predict any bit in the result.

As knowing the used matrix already during the key exchange stage of the protocol would open up some attack avenue for Eve, Alice and Bob have to agree on the matrix only after all qubits have been measured. In general, this is inefficient, as they have to exchange on the order of $nk \propto n^2$ bits. Instead, they usually select from a so-called two-universal subset of linear functions. Two-universality ensures that, although the set does not contain every binary matrix, its elements are random enough such that Eve cannot profit from this restraint.

3.4. Side-channels

In the description above it has been implicitly assumed that the bit information is only encoded in a single degree of freedom—in our case the polarization. In practice, however, it is inevitable to leak some information via a different channel as well. Such imperfections can be exploited by an attacker by a simple measurement, known as side-channel attack. As Bob examines only one degree of freedom, this would remain undetected, breaking the security of the specific implementation.

For photons as information carriers three possible side-channels need to be considered: The spatial mode, the wavelength, and the timing of the pulses, which are all continuous variables. In order to quantify the attack potential, at least two methods are available.

The first one is to calculate the quantum mechanical overlap of the respective wavefunctions $\psi_i(x)$, where x can be position, wavelength, or time, and i labels the four BB84 states. In experiments, one typically has access to only the associated probability distribution $p_i(x) = |\psi_i(x)|^2$. But with the assumption of perfect overlap of the conjugated degree of freedom, the complex contributions to the integral cancel each other out. Then, the overlap $o_{i,j}$ between state i and state j can be calculated as

$$o_{i,j} = \int \psi_i^*(x)\,\psi_j(x)\,\mathrm{d}x = \int \sqrt{p_i(x)\,p_j(y)}\,\mathrm{d}x. \tag{3.21}$$

If the overlap is 1 for all combinations, the probability distributions are equal and the side-channel is closed. If it is zero, the states can be perfectly distinguished by the attacker.

A second method closer to the information theoretic point of view is to estimate the mutual information I [51, 52] between a side-channel regarded as a random variable A and the bit value $B = \{0, 1\}$:

$$I_\beta = 1 + \int_A \mathrm{d}x \sum_{b\,\in\,B} \frac{p_\beta(x|b)}{2} \log_2\left(\frac{p_\beta(x|b)}{2\,p_\beta(x)}\right). \tag{3.22}$$

In this expression, β denotes one of the two bases and, accordingly, $p_\beta(x|0)$ and $p_\beta(x|1)$ are the probability distributions for the considered degree of freedom, conditioned on the bit value. As both bases are equally likely, the mutual information between bit value and side-channel is on average $I = (I_{H/V} + I_{+/-})/2$.

Note that both approaches are only indicators and cannot be used directly to quantify effects on the secret key rate. One circumstance that makes it difficult to incorporate such side-channels into security proofs is that the attacker is allowed to block some of the signals. Therefore, she could filter in such a way, that the remaining probability distributions overlap much poorer than the originally measured ones.

4. Experimental Setup

The purpose of our experiment is to demonstrate a key exchange between a handheld sender and a stationary receiver over free space. To this end, devices for both of the two parties have been developed, with detailed descriptions provided by Mélen [19] and Vogl [20], respectively. Exhaustive characterizations have been performed by Freiwang [21]. This chapter reviews the setup.

4.1. Handheld Transmitter ("Alice")

The central design goal [53] of the sender is a small form factor such that it can be effortlessly be held in the user's hand. Future integration in other devices, as, for instance, mobile phones, should be feasible with only little modification. At the same time, it should enable key exchanges with secret key rates sufficient for practical applications, requiring a high repetition frequency of the laser sources.

4.1.1. Design

Our transmitter produces the four linear polarization states necessary for the BB84 protocol with four independent emitters. The alternative—having only one source and modulating the polarization afterwards—typically requires bulk optical components and is therefore not suitable for our goal of miniaturization. We use near-infrared vertical-cavity surface-emitting lasers (VCSELs) as light source. As their emission is unpolarized, polarizers in four different orientations prepare the signal states. A waveguide chip guides the initially non-overlapping beams into a single spatial output mode. In addition to this signal, the device also emits a visible beacon beam used for synchronization purposes and to assist the user in aiming.

Figure 4.1 shows a schematic view of Alice's design, Figure 4.2 a photograph of the assembled optics. The images demonstrate that miniaturization has been successful: The optics fit in a volume of only $35 \times 20 \times 8\,\mathrm{mm}^3$. The whole device, including the associated electronics, was mounted in a rather spacious box of $19.4 \times 8.8 \times 4.8\,\mathrm{cm}^3$. These dimensions allow handheld operation without any problems.

In the following, the different components are presented in more detail.

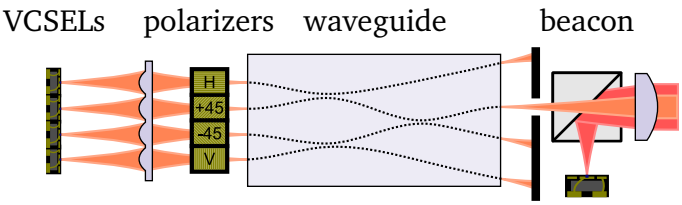


Figure 4.1.: Schematic depiction of the sender. Components from left to right: The VCSEL array, a micro-lens array coupling light into the waveguide, the polarizer array, the waveguide circuit, the beacon laser, a dichroic beam splitter overlapping beacon and signal beam, and a collimating lens.

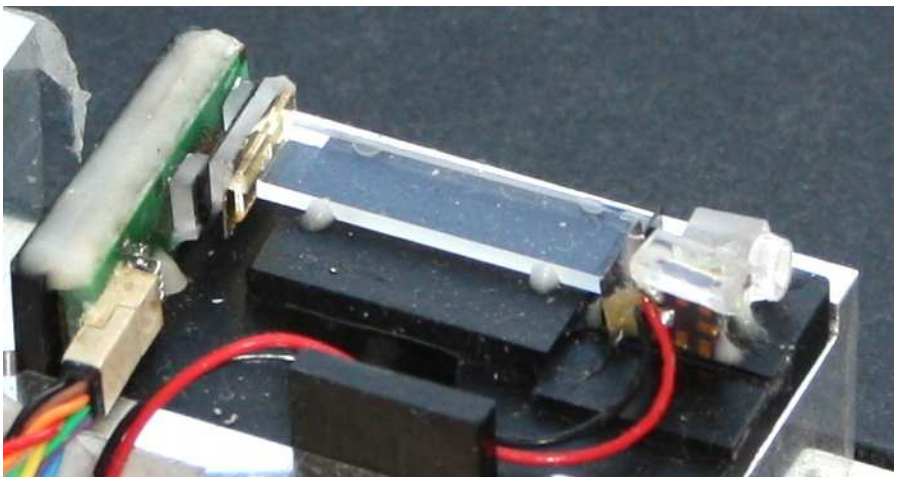


Figure 4.2.: Photograph of Alice's optics.

VCSEL array

As light sources we use a commercial VCSEL array emitting at a wavelength of 850 nm with a pitch of 250 µm. As we need four diodes for our application, this translates into a minimum width of only 750 µm. A modulation speed of up to 28 Gbit s^{-1} allows for precise timing control required to close the corresponding side-channel. Due to their symmetric construction, VCSELs should have no intrinsic polarization direction [54], which, in our sample, leads to unpolarized emission, at least for short pulses [19]. Therefore, polarizers are effective means to prepare the signal states.

Driving electronics

To create short pulses, sophisticated driving electronics is required. An electronic oscillator runs at a frequency of 100 MHz, which determines the pulse repetition rate of the device. For each of the four lasers, two such clock signals are provided. They can independently be shifted in time with a resolution of 5 ps by two delay lines. An electronic AND gate combines the two signals, leading to electrical pulses with a length determined by the difference between the two delay values, which can be as short as the resolution. Finally, a laser driver converts the voltage pulses to a current with a low (bias) and a high (modulation) level. Which diode is turned on in each cycle is determined by an FPGA that also configures the two delay parameters as well as the bias and modulation current for each channel. The FPGA's storage allows for a maximal raw key length of 131072 Bits, which are cyclically repeated during a key exchange.

Polarizer array

Four wire-grid polarizers filter the unpolarized light from the VCSELs to produce the linear polarizations required by BB84. For their production, the technique of focused ion beam (FIB) milling is applied [55]: It carves a pattern of parallel stripes into a solid gold layer on a transparent substrate, with a period smaller than the wavelength. Such a structure blocks polarizations orthogonal to the stripe axis, whereas parallel polarization is at least partially transmitted.

In our design, all four polarizers are written as an array on the same substrate, simplifying assembly as much as possible. We achieve extinction ratios of more than 1/1000, which does not limit the device's performance.

Waveguide chip

To establish spatial indistinguishability, a single-mode waveguide circuit [56] is employed. It is fabricated by femtosecond laser writing, which uses the high intensity in the focus of a femtosecond laser to locally increase the index of refraction in a carrier material. By moving the position of the laser relative to the substrate, a one dimensional path can be written. Two such guides in close proximity comprise a beam splitter, by virtue of evanescent coupling.

The sophisticated design depicted in Figure 4.3 couples light from four input modes into one output mode. The other three exits are blocked. The structure is optimized for polarization independence and low birefringence. To limit losses, large bending radii have to be chosen. Therefore, the waveguide contributes with 2.5 cm by far the most to the length of the optics.

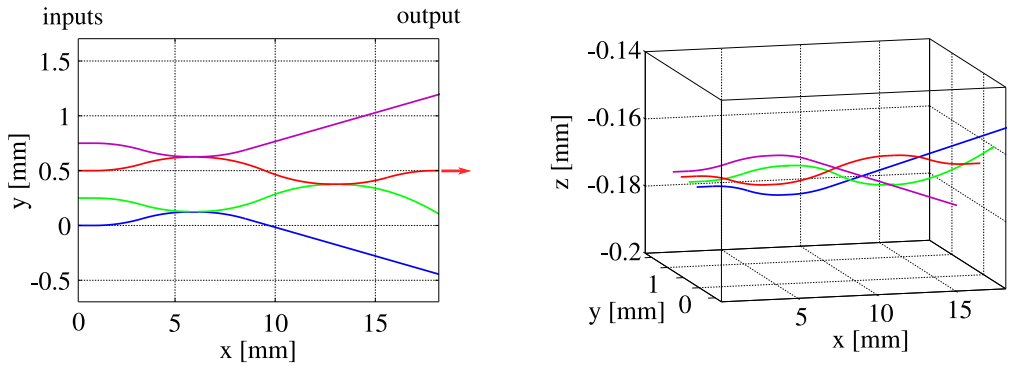


Figure 4.3.: Design of the waveguide circuit (taken from [19]). Left: Top view, right: 3D view.

Beacon laser

The beacon laser [20] operates at a wavelength of 680 nm, which to the human eye appears as red. In its spectrum, there is also a weak broad peak at the signal wavelength of 850 nm, which is blocked with a longpass filter. A dichroic mirror in the signal path, which reflects the beacon but is trasmissive for near infrared, overlaps signal and beacon, before an outcoupling lens approximately collimates both beams.

For synchronization between sender and receiver, the beacon is modulated with a rectangular signal at half of Alice's 100 MHz clock frequency. In principle, it can also transmit data by imprinting a more complex pattern, e.g., to encode block numbers, but besides some preliminary tests this has not been implemented yet.

4.1.2. Characterization

After a device has been assembled, one must make sure that it satisfies all requirements. In the case of a BB84 transmitter two aspects are crucial: The quality of the polarization states and its susceptibility to side-channel attacks. Both are characterized in the following.

4.1.2.1. Polarization States

To measure the four polarization states emitted by the device, quantum state tomography is performed. However, as is extensively discussed by Freiwang [21], the results drift slightly over time on the order of hours, likely due to temperature fluctuations. Therefore, the procedure is repeated before each key exchange and, thus, its description in this thesis is postponed to Section 6.1.3.

Here, only typical values for two quantities summarizing the states' quality shall be given, beginning with the source intrinsic QBER after optimal compensation. This number is the error rate which one would get in a key exchange if all other components would work flawlessly and no attack is carried out. Alternatively, one could also see it as the source's contribution to the final QBER. Typically, it is between 0.5 and 1.5 %.

Second, the preparation quality [57]

$$q = -\log_2 \max \left| \langle \psi_x | \psi_z \rangle \right|^2, \tag{4.1}$$

where the maximization finds the largest (read: worst) overlap between two states in different bases. In the optimal case of perfectly conjugated bases, $q = -\log_2 1/2 = 1$, in the worst case of overlapping bases $q = -\log_2 1 = 0$. Due to the steepness of the logarithm below 1, even slight changes in the states cause large variations of q. Therefore, we find that our states achieve values in the range between 70 and 90 %.

4.1.2.2. Temporal Side-channel

Similar to the polarization states, the temporal profile of the pulses emitted by Alice also varies from day to day. What is more, it is actively calibrated by tuning the configuration parameters of the delay lines and the laser drivers, likely causing a different shape for each measurement. Thus, we again refer the reader to Section 6.1.1 in the results chapter.

4.1.2.3. Spectral Side-channel

The four polarization states might have differing wavelengths, as they are produced by four different laser diodes. To confirm this, the four spectra have been recorded with a grating and a single-photon resolving charge-coupled device (CCD). Each diode was measured individually with typical settings for bias, modulation, and delays (see, for instance, Table 6.2). Exposure time was 1 s. The result is shown in Figure 4.4.

As expected, the states are distinguishable and the spectral side-channel is not closed. If the project were to outgrow the state of a proof-of-principle experiment, this issue would have to be resolved. One proposed solution is to use VCSELs with a tunable wavelength, which is possible by, e.g., controlling the diode's temperature [58] or inducing mechanical stress [59]. Also, one could employ another kind of light source with a broader spectrum, such as an LED, but this comes with other disadvantages. Finally, the most promising approach, especially for production in larger quantities, is to preselect diodes with overlapping spectra.

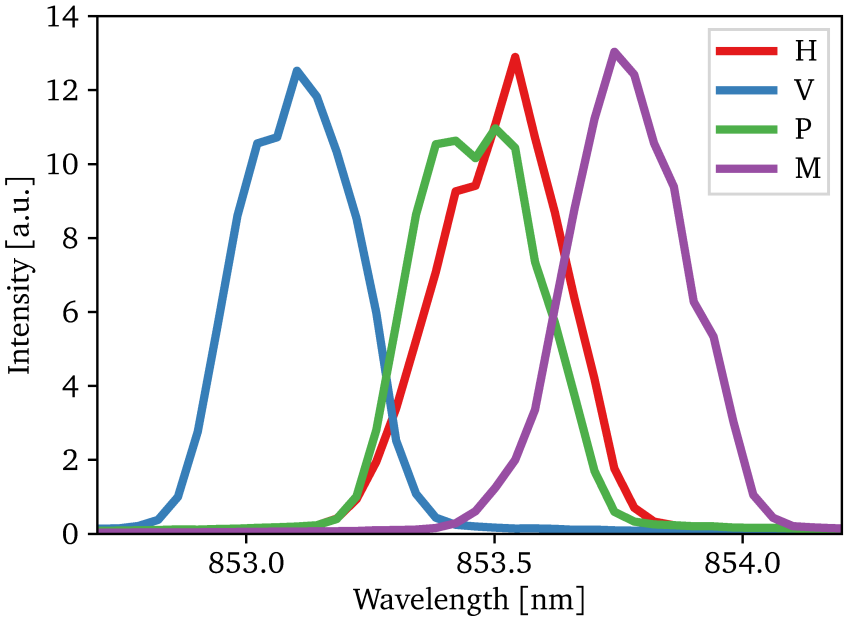


Figure 4.4.: Spectra of the four VCSELs at typical driving parameters.

4.1.2.4. Spatial Side-channel

Finally, the spatial mode side-channel is studied. Supposedly, it is closed by the waveguide chip. As it is single-mode, non-unity overlap would be suprising, but is not ruled out: For instance, the length of the waveguide might be too short to perfectly extinguish all non-guided modes, or the guided mode could be polarization dependent.

In order to be sure, the overlap has to be measured. To this end, photographs of the beam profiles have been taken at different distances for each of the four channels. Due to the very low intensity of the signal, a low-noise camera with high quantum efficiency had to be used (PCO Sensicam em). See Figure 4.5 for an example image set.

For each of the distances, the mutual information between bit value and spatial mode has been calculated (see Equation 3.22). This resulted in suprisingly high values between 1.4 and 3.4 %, growing with distance. As visually the pictures do not differ considerably, the most likely explanation is the pronounced noise, which, being random, reduces the apparent overlap. This also agrees with the observation that larger distances yield worse values, as there the beam intensity and thus the signal-to-noise ratio, becomes smaller.

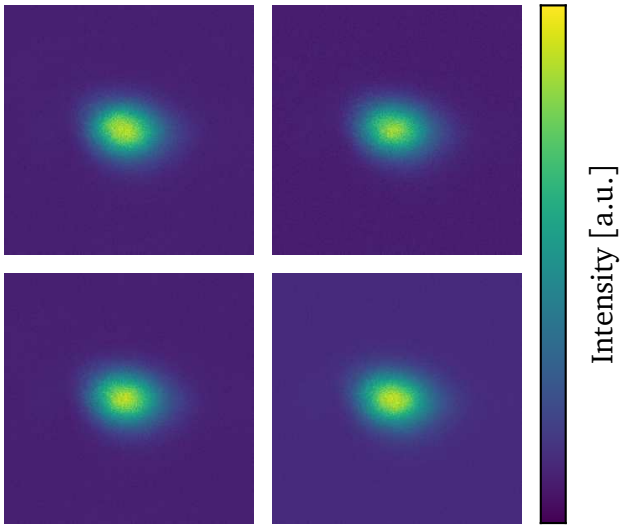


Figure 4.5.: Beam profiles at a distance of 46 cm from the outcoupling lens for the four different channels. Clockwise starting top-left: Horizontal, vertical, −45°, 45°. Each quadratic image consists of 300×300 pixels corresponding to $2.4 \times 2.4\,\mathrm{mm}^2$.

To confirm this assumption, Gaussian beams have been fitted to the four image sequences. Using the results, the mutual information was calculated analytically for each distance. At worst, this resulted in a mutual information below 0.01 %. Since the beams appear to be not perfectly Gaussian, the significance of the exact value is uncertain. Still, this confirms the hypothesis, that the results above are in fact due to noise, to which the fits are resistant, and also suggests a very good overlap.

4.2. Stationary Receiver ("Bob")

The task of a BB84 receiver is to measure the incoming polarization states in a randomly selected basis. Additionally, our specific application scenario of handheld communication requires beam tracking and basis alignment capabilities. In this section, the design of the receiver is presented by first describing the polarization measurement scheme and then detailing the components facilitating the interface to the sender. A schematic overview is shown in Figure 4.6.

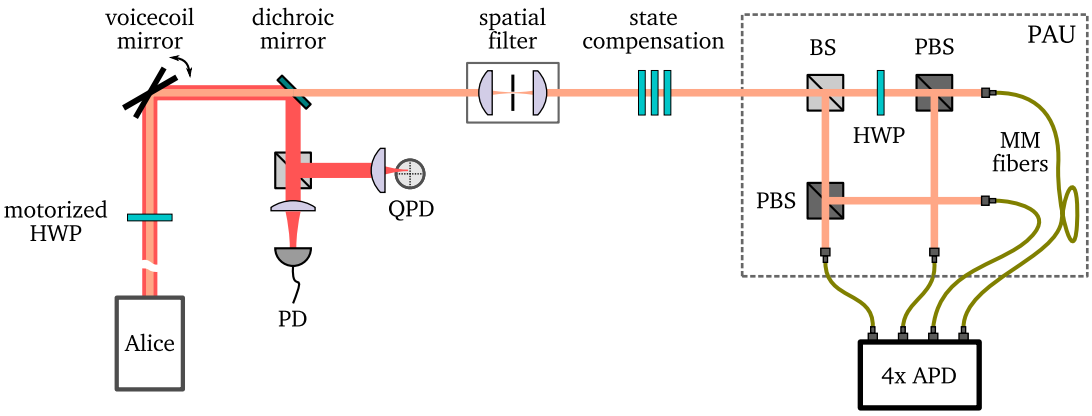


Figure 4.6.: Schematic depiction of the receiver. HWP: half wave plate, PD: photodiode, QPD: quadrant photodiode, PAU: polarization analysis unit, BS: beam splitter, PBS: polarizing beam splitter, MM fibers: multi-mode fibers, APD: avalanche photodiode.

4.2.1. Polarization Measurement

The state measurement is performed by the detection unit. But before the projection takes place, it is useful to correct polarization rotations in the receiver and imperfections in the sender, for which a compensation apparatus was designed.

4.2.1.1. Detection Unit

As is common for BB84 receivers, a 50/50 beam splitter is used to select the measurement basis in a passive fashion: In one of the two output arm the state is measured in σ_z, in the other in σ_x. The σ_z measurement is performed by a polarizing beam splitter, which separates horizontal and vertical polarization, and two fiber-coupled silicon avalanche photo diodes connected to a timestamping unit. The other arm is similar in structure, but an additional half-wave plate rotates the measurement basis to σ_x. At our signal wavelength, the single photon detectors (PerkinElmer DTS SPCM-AQ4C) feature a detection efficiency of 38 % according to specification.

4.2.1.2. State Compensation

The optical path in the receiver that a signal pulse has to pass in order to arrive at the detection unit comprises a variety of optical components such as mirrors and lenses. Those modify the polarization state, leading to misaligned reference frames between state preparation and analysis and, thus, an increased QBER and decreased

secure key rate. Fortunately, as long as they are polarization independent they can be regarded as unitary and thus invertible by compensating components.

In addition, a compensation is already beneficial considering the polarization states emitted by Alice alone: Birefringence in the waveguide and the dichroic mirror changes the polarization states, which are only originally defined by the polarizer array. Mainly, this affects all four states equally, allowing the compensation to succeed even after the spatial modes have been unified.

Polarization state rotations can experimentally be implemented by wave plates. As it turns out, two quarter waveplates and one half waveplate can, when rotated accordingly, apply any unitary operation to the polarization state of a transmitted photon. Therefore, such a structure is placed directly in front of the polarization analysis unit.

For a given set of polarization states (see Section 6.1.3 for the measurement method), one then can calculate the appropriate waveplate angles by optimizing the resulting QBER. As a local minimization often fails to find the global minimum, we employ a combination of rough global [60] and precise local [61] optimization algorithm, both from the SciPy library [62], to this task.

4.2.2. Spatial Mode Filter

If an adversary is capable of modifying the different detection efficiencies of the four detectors, the BB84 protocol becomes vulnerable [63, 64]. In the worst case of complete control a concrete strategy could look like this: Eve measures the state emitted by Alice in a randomly selected basis, and produces the corresponding detection result for Bob. Then, she has the same information as Bob about the key, without having to introduce any errors, and the key's secrecy is broken.

One way of inducing a detection efficiency mismatch possible in a freespace system is to alter the beam path, resulting in different coupling efficiencies to the detectors. To prevent this in our setup, a spatial filter limits the range of possible incoming modes [65]. By scanning the remaining mode space, one can quantify that the remaining detection efficiency mismatch and confirm that it is close to zero [66].

4.2.3. Interaction with Alice

The remaining components in the receiver enable an efficient interplay with the handheld sender. Three obstacles need to be overcome: Misaligned reference frames due to a tilted orientation of the transmitter, bad coupling efficiencies caused by inaccurate aiming, and drifting clocks.

4.2.3.1. Basis Alignment

It is crucial that Alice and Bob share a common frame of reference, i.e., agree on definitions of “horizontal”, “vertical”, “diagonal”, and “anti-diagonal”. If not, the receiver’s measurement bases would not match the transmitted states, which results in enhanced QBERs and diminished secret key rates.

During a handheld key exchange, one has to expect that the user tilts the transmitter and, as seen from the receiver’s point of view, rotates her reference frame around the beam axis. To realign the bases again, Bob has a half-wave plate at his disposal, whose angle he can control using a stepping motor. Alice, on the other hand, measures her orientation in space using the attitude sensor of a smartphone, placed on top of the device. An Android app continuously sends the current angle over Wi-Fi to Bob’s computer, who rotates the waveplate accordingly.

As was observed at least with the smartphone used during development, the reported angle flips back and forth between two values, even when the device does not move. In order to avoid transmitting this noisy data, the program therefore first collects 10 values at an interval of 10 ms and then only sends the average of those. As a result, the refresh rate of the basis alignment amounts to 10 Hz. This is likely too slow to counter trembling, which typically shows similar oscillation frequencies [67], but these motions cause only very small angle offsets. In contrast, the main source of errors—constant misalignment and continuous steady drifts—are resolved.

4.2.3.2. Beam Tracking

Besides tilts, handheld operation would, if untreated, also lead to coupling efficiencies close to zero. This is mainly caused by the spatial filter, which limits the acceptance angle of the incoming beam to only $\pm 1.4\,\text{mrad} = \pm 0.08^\circ$ or, in other words, to a window of 2.7 mm diameter at a distance of 1 m. Therefore, active beam tracking is required.

A voicecoil mirror in the beam path, which can be tilted up to $\pm 3^\circ$ from its resting position in both axes, is able to correct wrong incoming angles. To provide an error signal, the beacon beam emitted by the sender is separated from the signal by a dichroic mirror. Then, it is guided to a quadrant photo diode, which resolves if the beam hits the center or is off into a certain direction. This signal is fed back to the voicecoil mirror, setting up a control loop.

To mark the enhanced cone of acceptance, two pinholes with a distance of rougly 15 cm are placed in front of the voicecoil mirror. Once a user sees that the beacon beam is not blocked by one of the two pinholes, she knows that she likely couples to the photo detectors. To further aid her estimate, an acoustic feedback has been implemented: A sharp sound (square wave) signals loss of coupling, a soft one (sine) operation of the beam tracking. When coupling is restored, a high pitch indicates a

large angle of the voicecoil mirror, a deep one a only small displacement from zero. This guides the user closer to the center, giving her a greater margin of error.

4.2.3.3. Clock Synchronization

As with most communication systems, quantum key distribution needs clock synchronization because Bob assigns pulse numbers based on detection timestamps. If this fails because his clock ticks different from Alice's, they will not be able to agree on a key.

Clock synchronization utilizes the beacon beam, which Alice has modulated with a 50 MHz square signal. It is coupled to an amplified photo diode with a bandwidth of 150 MHz. The electrical output signal is passed on to a commercial clock recovery chip, which converts it to a clean square signal with defined amplitude and twice the frequency. Then, an FPGA counts the oscillations and emits a signal every thousand pulses, effectively reducing the frequency to 100 kHz. This value is low enough to be counted by the same timestamping unit that also records the signal pulses, but large enough to not suppress too much information about clock drifts.

While this design is sufficient for clock synchronization, it leaves some things to be desired. Most importantly, it breaks down as soon as the clock recovery signal is lost, which happens frequently during handheld key exchanges. Improved electronics could try its best to continue the output signal even if no input is present, based on the frequency in, say, the last 100 ms. Furthermore, it synchronizes only "locally", but not "globally": The system ensures that Alice's and Bob's clock tick at the same frequency, but not that they show the same absolute time. A solution would be to transmit block numbers using the beacon modulation, marking the start of a new batch of bits. Those issues, however, are not crucial, as they can also be solved in post-processing during analysis (see Section 5.2.2 and Section 5.2.3).

5. Data Analysis

This chapter describes how we estimate a secret key rate given a file of detection events recorded during a key exchange. First, we give an overview on the procedure as a whole and its software implementation. Then, we present the most important steps in greater detail: Pre-processing, synchronization, filtering, and calculation of the secret key rate. To conclude, we make suggestions for an improved future version.

5.1. Overview

Bob infers which detection at the receiver belongs to which emitted signal by means of the recorded timestamps. However, at the outset Bob's clock is independent from Alice's, necessitating synchronization as the first task of the analysis. This is done in two steps: First, a "local" synchronization ensures that both clocks tick in phase. Second, a "global" synchronization sets a common reference point.

Subsequently, all events recorded outside a certain detection window around the expected arrival time of the pulses are removed. Those most likely are random noise due to detector darkcounts, stray light, or background emission by Alice's VCSELs. Thus, they carry no information and would only increase the error rate. An additional step of filtering discards events in periods of very low transmission, in which even most events inside the detection window stem from background.

Then, sifting takes place (see Section 3.2). Finally, Alice's and Bob's sifted keys are compared with each other to estimate the QBER. Together with the transmission inferred from the sparseness of Bob's raw key, secure key rates are calculated. An actual secret key is not extracted.

A particularity of our setup is that Alice's key is available at Bob's computer performing the analysis, obviating the need for any classical communication. Furthermore, as Alice's storage space is limited, her raw key is looped infinitely. Those deficiencies would need to be resolved in a practical device, but for our proof-of-principle experiment they only reduce the required complexity.

5.2. Major Tasks

5.2.1. Data Preprocessing

The raw files containing the detection events of a key exchange measurement can become very large: A repetition rate of 100 MHz, mean photon number of 0.1 , transmission of 40 %, and detector efficiency of 38 % leads to a detection rate of about 1.5 MHz. The timestamps are measured with picosecond resolution and are encoded in plaintext decimals, thus taking 13 Byte already after 10 s. Two more ASCII-characters are used as delimiter and to store which detector has clicked. In total, for a typical static key exchange of 60 s, a file larger than 1 GB is produced.

While this size fits in the memory of typical modern computers, it becomes unwieldy to work with. Typically, many copies of the same or similar datasets stay in memory during processing, soon reaching the machine's limit. The easiest way to deal with this problem is to split the detection file into small chunks right at the beginning of the analysis process, which is done by the `split_chunks` command.

`split_chunks` iterates over the lines, each representing a single detection event, in the given input file and stores them in memory. Once a configurable number of lines (`CHUNK_SIZE` $= 10^7$ by default) has been read, it continues until it finds the next clock recovery signal. Only then, the detections are written to a new chunk file. Then, the process repeats, but also including the previous clock signal in the next chunk. Eventually, the detection file will have been split into small chunks with a reasonable size of about 170 MB (for the default `CHUNK_SIZE`).

The motivation for the duplication of clock recovery signals at the chunk borders is to minimize the need of carrying over detections from one file to the next during analysis. This way, each file can be easily examined individually, without needing to ignore detections before the first or after the last clock recovery signal. And more importantly, it gives an anchor point to seamlessly synchronize between two consecutive files.

5.2.2. Local Clock Synchronization

Only in perfect conditions Bob would detect every pulse sent by Alice without additional noise, allowing him to construct his raw key simply by stringing together his detector clicks. In practice, due to the use of weak coherent pulses instead of perfect single photon sources, imperfect transmission and detection efficiencies, background and darkcounts, as well as the possible presence of an adversary in the channel, this simplistic approach does not succeed.

Instead, Bob has to infer the pulse index from the time at which each detection event has occurred. If he sets the expected arrival time of the first qubit to 0 (see Section 5.2.3), the next pulses are due at T, $2T$, $3T$, ..., where T is the inverse

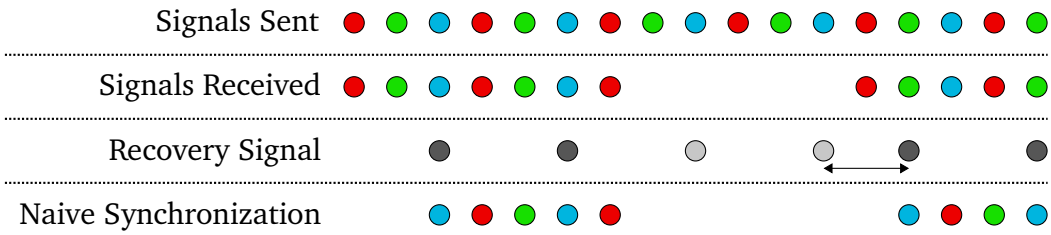


Figure 5.1.: Simplified illustration of the clock recovery scheme. Alice sends a stream of signals, of which Bob detects only some. His recovery electronics clicks every three detections (dark dots). A naive synchronization scheme might thus assign pulse numbers 0, 3, 6, ... (blue dots) to each recovery signal. This approach fails as phase matching between pre- and post interrupted signal is not guaranteed.

of Alice's repetition rate. Therefore, dividing the detection timestamp by T and rounding to the nearest integer yields the detection's index in the raw key.

Two requirements on Bob's timestamping unit follow from this: It needs an accuracy of at least T, which in our setup is 10 ns, and it needs to stay in sync with Alice's clock over the period of a key exchange (typically between 10 and 60 s). While the first requirement is easily satisfied out of the box by Bob's single photon detectors (resolution of 400 ± 50 ps [68]) and the time to digital converters (about 80 ps), synchronization has to be achieved in software, drawing on data from Bob's clock recovery electronics described in Section 4.2.3.3.

The clock recovery electronics outputs one signal to the timestamping unit each time 1000 cycles of Alice's 100 MHz beacon modulation are counted. During a key exchange, this results in a signal with a frequency in Alice's time units of 100 kHz. The recorded timestamps are measured with Bob's clock, enabling him to convert between the two time scales.

In a handheld scenario, though, coupling of the beacon beam onto Bob's photo diode might be periodically lost due to shaking of the transmitter. Then, the counter will halt until coupling is restored, leading to a large gap between two recovery timestamps. The resumed signal is then still phase matched with Alice's clock, but not necessarily with the previous recovery signal (see Figure 5.1).

Synchronization is performed by the function `sync_clocks`. It takes a chunk as input containing detection events and their timestamps t_B, as measured with Bob's clock. Assuming an uninterrupted beacon signal, it then assigns to each clock recovery event at Bob's time t_B^{sync} a timestamp t_A^{sync} in Alice's time units: 0 µs to the first, 10 µs to the second, and so on, given by the known frequency of Alice's recovered 100 kHz signal. The pairs $(t_B^{\text{sync}}, t_A^{\text{sync}})$ are considered sampling points of a function mapping between the two clocks. Consequently, all other detection timestamps are

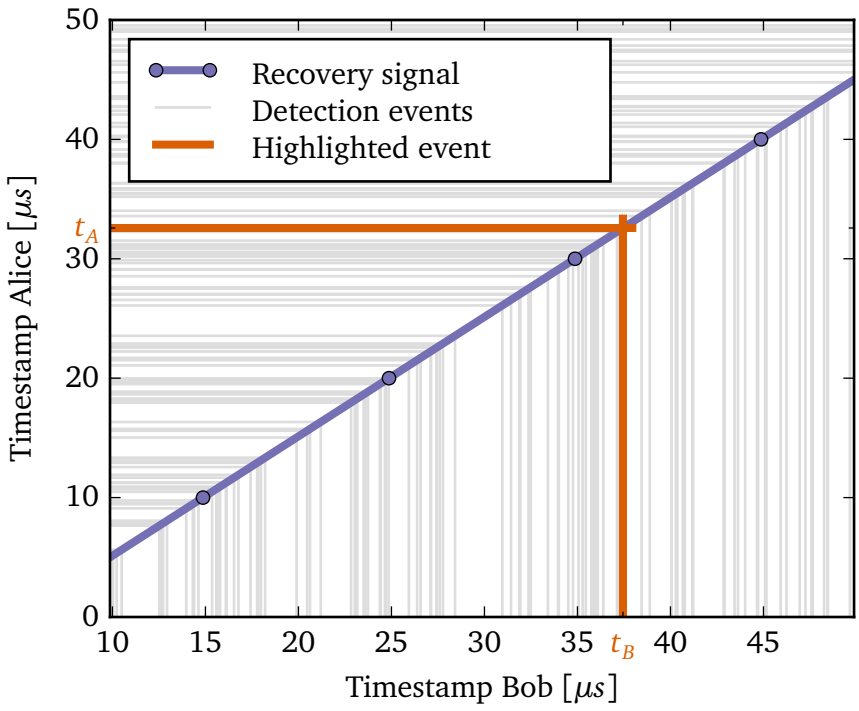


Figure 5.2.: Exemplary synchronization data. Using the interpolated clock recovery signal (blue dots) as reference, detection timestamps are converted from Bob's to Alice's clock.

converted to Alice's clock using a linear interpolation of the acquired data (see Figure 5.2).

When the coupling of the beacon laser to the photo diode is lost, however, the recorded timestamps of clock recovery signals display a more complicated behavior, which is shown in Figure 5.3. During regular operation, the difference between consecutive timestamps is roughly constant at the expected 10 µs, varying by less than 0.5 ns (50 ppm). When the coupling is lost, the first output signal of the clock recovery is late by about 3 ms, followed by 115 to 120 signals with a time difference 3.3 µs shorter than 10 µs. This cycle repeats until coupling is regained with few dead times in the order of a few 100 ms in between. The cause for these peculiarities has not been investigated further but rests likely in the unspecified behavior of the clock recovery chip when the input level is low.

To work around these issues, `sync_clocks` ignores recovery pulses which are much closer to their predecessor than the expected 10 µs as well as their direct surroundings (nearest and, to be on the safe side, next-nearest neighbors). As those

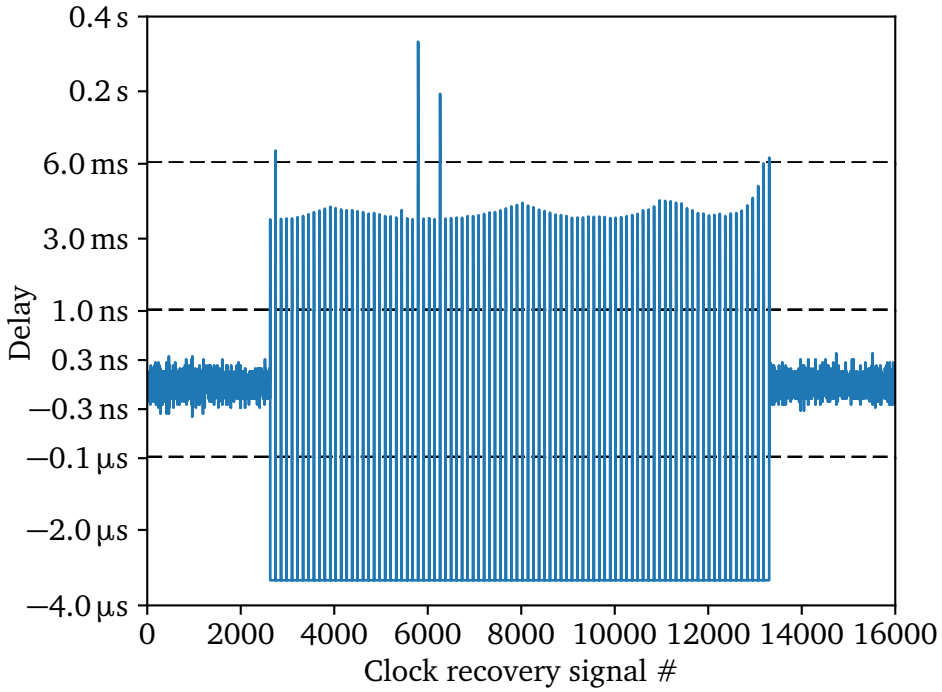


Figure 5.3.: Delay of clock recovery signals during loss of signal. For each clock recovery signal, the time difference to the previous one is measured and its delay (i.e., difference to the expected value of 10 µs) is plotted. Instead of a single or few outliers, bizarre behavior on four different timescales, separated by dashed lines, is observed.

appear to be only electronic artifacts not carrying any actual timing information, no useful data is discounted.

To bridge the resulting gap δ_B^{gap}, an estimate for the passed time on Alice's clock δ_A^{gap} has to be found, in place of the usual 10 µs. For that, a time conversion factor $f = \delta_A/\tilde{\delta_B}$ is defined, where $\delta_A = 10\,\mu\text{s}$ is Alice's clock period multiplied by 1000 and $\tilde{\delta_B}$ denotes the median time difference between consecutively detected recovery signals. Then, δ_A^{gap} is approximated by multiplying δ_B^{gap} with f and rounding to the nearest multiple of δ_A.

The idea behind this approach is to assume a linear relation between Alice's and Bob's clock that does not change over the course of a chunk. The median is used in favor of the mean because of its resilience against outliers, which, as shown above,

are plentiful when the beacon coupling is lost . Lastly, rounding to multiples of δ_A ensures that δ_A^{gap} is a multiple of 10 µs. This incorporates the observation that the clock recovery signal is, if present, always in phase with Alice's clock.

In summary, after `sync_clocks` has been executed, each detection event has two timestamps attached: One—measured—refering to Bob's clock and another one—estimated—refering to Alice's. This allows time filtering and setting up the raw key.

5.2.3. Global Clock Synchronization

The synchronization scheme described in Section 5.2.2 makes sure that Alice's and Bob's clocks tick in phase with each other, allowing the receiver to extract a proper raw key. A global offset, however, with respect to Alice's raw key due to different absolute time zeros is still present. Furthermore, such a global offset might change multiple times during a handheld key exchange when the clock signal is lost and the local synchronization method fails.

The most elegant solution to this problem is to let Alice split her raw key in blocks. Then, she can transmit a serial number each time a new block starts using her beacon modulation (see Section 4.1.1 and Section 4.2.3.3 for the necessary components in the sender and the receiver, respectively). In our setup, the key is cyclically repeated already after about 1 ms due to Alice's storage size. Therefore, only one block and, thus, a single start marker instead of a number would suffice.

This scheme, while implemented, was not used for the key exchanges discussed in this thesis. Instead, the global offset was determined by publically comparing parts of the raw keys of the two parties utilizing the fact that the number of possible offsets is limited by the key length. In a straightforward manner, the correlations for all possible offsets are tested. All but one will show negligible correlation, uniquely identifying the correct offset.

The number n of bits to compare should be chosen as small as possible, as it reduces the effective raw key length. Additionally, less comparison bits result in a faster analysis. If, on the other hand, the number is too low, the probability of erroneously selecting the wrong offset becomes prohibitively large. To find a sensible compromise, we calculate the expected overlap for the correct offset. For a raw key with QBER δ, the number of correct bits is given by

$$n_{correct} = \frac{n}{2}(1-\delta), \tag{5.1}$$

disregarding the half of the bits measured in the incorrect basis.

Now, we are interested in the probability of finding by chance a better correlation at one of the N wrong offsets. For a single offset, the probability to find k matching bits is given by the binomial distribution with success probability 1/2:

$$p(k) = \binom{n}{k}\frac{1}{2^n} \tag{5.2}$$

Summing for all $k \geq n_{correct}$ yields the probability p_0 to erroneously exceed the correlation found at the correct offset. Then,

$$p = 1-(1-p_0)^N \tag{5.3}$$

is the propability to do this at least once for the N different offsets, which is the probability for the algorithm to fail.

A numerical analysis displayed in Figure 5.4 shows that a few tens of comparison bits are more than sufficient to reliably find the correct offset. Taking into account that during a handheld measurement the signal is lost and regained usually about once per 10 s and raw key rates of, depending on the protocol, at least 100 kHz are achieved, the number of lost bits due to this type of synchronization can safely be ignored.

Global synchronization as described above is performed by the `find_key_offset` method. It takes Alice's and Bob's raw keys as parameters and returns the offset with the highest correlation. Comparison bits are selected from a period with high key rate to ensure a low QBER and, thus, high success probability of the algorithm. `find_key_offset` is called once at the beginning of the key exchange and again each time the clock signal is lost, since there the local clock synchronization scheme tends to fail, warranting a fresh start.

5.2.4. Signal-to-Noise Ratio Filtering

During a handheld key exchange the transmission varies rapidly between zero and the maximum achievable value. As described in detail in Section 3.2.4, low transmission values substantially reduce the resulting secret key rate. Furthermore, in times of low transmission the QBER is enhanced as there the signal-to-noise ratio is larger, assuming an equal background countrate. This has a negative effect on the secret key rate as well.

One might wonder whether the case of non-constant transmission is covered in QKD security proofs, given that in their secret key rate formulas the transmission appears as a number instead of a probability distribution. To answer this question consider two attacks, both optimal for the two different tranmissions they result in. If the eavesdropper switches back and forth between those two strategies quickly enough, Alice and Bob are fundamentally unable to recover the two transmission values, as this requires integrating over some time interval. Instead, to them the key exchange is indistinguishable from a static one, and they would apply the standard proven formulas. For the attacker, on the other side, the frequency at which she

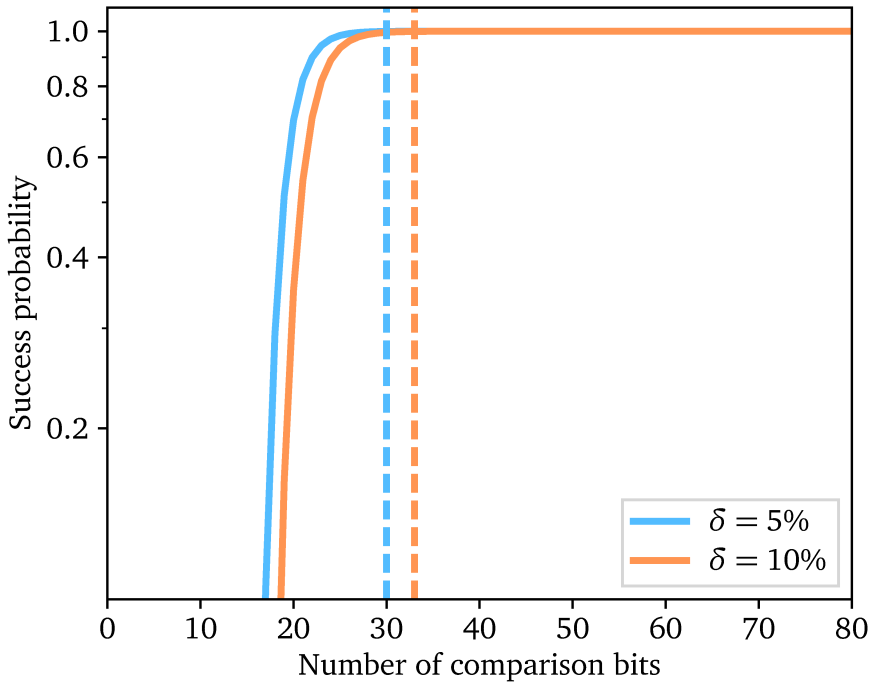


Figure 5.4.: Success probability of our global synchronization scheme as function of the chosen number of comparison bits. Numerical evalation of Equation 5.3 with our key length of $N = 131072$ in two bad case scenarios with high QBERs. Vertical dashed lines mark 99.9 % success probability.

changes her strategy does not matter, as the amount of extracted information does not change (it should only depend on the number of affected bits, not at which time they have have been transmitted or what happened in between). Therefore, if standard QKD security proofs allow seemingly static key exchanges, they must also allow key exchanges with varying transmissions.

A natural approach to handle varying channel transmissions would be to group the detections into time bins and calculate the secret key rate for each bin separately, based on the current QBER and transmission. However, this appears to be dangerous, as in short time bins the necessary parameters can only be estimated with large variances. Finite key analyses, which take them into account, could be applied to quantify how this affects the secret key rate but are not used in this thesis. Furthermore, it likely reduces the total secret key rate. Therefore, we refrained from doing such a time resolved analysis.

Instead, we apply a technique proposed and tested by Erven et al. [69] called signal-to-noise ratio (SNR) filtering. Here, data measured with high SNR, signaled by a low raw key rate, is discarded. The remaining parts are effectively recorded in a shorter timespan and, thus, have a higher averaged transmission.

Before applying the filter, a cutoff value or threshold has to be defined, which we express as a transmission (as it is proportional to the raw key rate). A high threshold would have the advantage of high average transmission and low QBER, a low threshold would result in better raw key rates. Another free parameter to choose is the used binsize. The optimal choices will depend on the transmission distribution in the specific key exchange and, for our datasets, will be discussed in Section 6.3.2.

We find optimal values for threshold and binsize by maximizing the secret key rate. For this, first a global brute force optimization of both parameters is performed. Next, the best threshold is further approached using SciPy's implementation of Nelder-Mead's Simplex algorithm [62, 70, 71]. In this second step the binsize is left unchanged, as at this point in the analysis for reasons of performance of the program the data is already prebinned to 10 ms blocks. Consequently, only integer multiples of this value are possible to evaluate, ruling out many good optimization algorithms that are only applicable to continuous functions. From experience, however, the binsize does not have a significant effect on the secret key rate, justifying this compromise.

5.2.5. Secret Key Rate Estimation

Once a signal-to-noise filter has been applied, raw keys have been sifted, and QBER as well as transmission have been determined, the resulting secret key rate can be estimated. In Section 3.2.4 two suitable formulas for two different protocols, BB84 in plain form and with the decoy extension, have been presented. While a complete implementation of the decoy state method for our system is still pending (see Chapter 7), we are nevertheless able to estimate corresponding rates. This is because both formulas depend, apart from predetermined system properties, on the very same parameters.

To reiterate the results of Section 3.2.4, the following expression has to be evaluated:

$$S_{\text{sec}} = \frac{Q_\mu}{2}\left[-f(\delta_\mu)H_2(\delta_\mu) + \frac{Q_1}{Q_\mu}\left[1 - H_2(\delta_1)\right]\right] \tag{5.4}$$

Q_1 and δ_1 are not directly accessible in the experiment and have to be estimated in the most pessimistic way. For plain BB84

$$Q_1 \geq Q_1^L = Q_\mu(1-\Delta), \tag{5.5a}$$

$$\delta_1 \leq \delta_1^U = \frac{\delta_\mu}{1-\Delta} \tag{5.5b}$$

and for decoy

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2} Y_0\right), \tag{5.6a}$$

$$\delta_1 \leq \delta_1^U = \frac{\delta_\mu Q_\mu - Y_0 e^{-\mu}/2}{Q_1^L}. \tag{5.6b}$$

Parameters that are fixed for a given test run are the mean photon number μ, the ensuing fraction of tagged bits Δ (see Equation 3.17), and the darkcount yield Y_0. Not a priori known but extracted from a specific key exchange are the QBER δ_μ and the transmission dependant gain Q_μ. A typical value for the classical error correction efficiency of $f(\delta_\mu) = 1.22$ is assumed [72]. For the decoy analysis, we expect the same transmission to determine Q_ν and a secondary mean photon number $\nu = 2\mu$. This value for ν would emerge if decoy states would be produced by turning on two diodes at the same time, as proposed by Harrington et al. [42].

The sifted key rate R_{sift} does not appear directly in Equation 5.4, so it might be unclear how to use this experimentally measured parameter. That is because usually proportional to the transmission, which appears in the formula via the gain Q_μ. In our case, however, due to the application of a SNR filter, the relationship between those two quantities is not so simple: A higher threshold will, e.g., decrease the sifted key rate but at the same time increase the average transmission. Of course, it would be possible to redefine one of these parameters and restore their direct dependence. But this would deprive us from at least one of the useful intuitions that larger sifted key rates mean more transmitted bits and less transmission means less secure keys.

Instead, we disregard SNR filtering for now and assess that in this case the factor $Q_\mu/2$ in Equation 5.4 denotes the probability that a sent pulse appears in the sifted key. Then, the remainder of the expression r_{sec} is the secret fraction, i.e., the probability that a bit survives proper post-processing. Thus, we can write

$$R_{\text{sec}} = R_{\text{sift}} \frac{S_{\text{sec}}}{Q_\mu/2} \equiv R_{\text{sift}} r_{\text{sec}}, \tag{5.7}$$

where we also changed from rates measured in "bits per pulse" (denoted by S) to "bits per unit time" (R). In this equation we can finally plug in quantities evaluated

after SNR filtering without problems: A larger threshold increases r_{sec} and decreases R_{sift}, but any mathematical coupling between the quantities is eliminated.

5.3. Future Improvements

While the implementation of the analysis software works reasonably well for the purposes of this thesis, some aspects could be improved. Likewise, some features may become relevant for a future version.

The most apparent deficiency is the long time required to analyze one key exchange, usually 5 to 10 min, depending on the measurement's duration and how often the synchronization has to be reestablished. A simple improvement concerns the global synchronization algorithm, which at the moment tests any possible offset starting at an arbitrary constant value. However, quitting as soon as a reasonably large correlation has been found would suffice, reducing the runtime on average by a factor of two. Moreover, when trying to regain synchronization, we propose to look in the vicinity of the previous offset first, as the time difference should pile up only slowly. Combined, those two provisions should speed up the process considerably.

Another weakness is the apparent complexity of the program, resulting from the choice of Python as programming language. Due to its dynamic nature, it can in some cases be slow compared to static languages, which makes, e.g., a simple iteration over all detection events practically impossible. Therefore, for performance critical code, third party libraries such as NumPy [73] are used, which outsource computation to precompiled machine code. This however is only efficient if the problem at hand can be expressed as an operation acting on a large array of data (e.g., summing over a sequence of numbers or squaring each element). Unfortunately, for the task of a key exchange analysis, this often requires quite elaborate and unintuitive reexpressions of the problems with correspondingly detrimental effects on code readability. A rewrite of the program in a static programming language would allow a more intuitive approach and, likely, even result in a faster program.

Finally, if our system is to be developed further into a practical device, some additional requirements arise. Firstly, the analysis would have to be done "live", i.e., at the same time as the physical key exchange procedure. Then, the user could be notified once a secret key of a prespecified length had been generated. Secondly, a secret key would have to be actually generated, instead of only estimating at which rate this would be possible. Lastly, Alice and Bob need their own physically separated key extraction devices, connected only by the quantum and a classical channel required by the BB84 protocol.

6. Results

The preceding chapters described how our experiment works in principle—from the underlying theory to the data analysis procedure. In this last part of the thesis, a selection of actual key exchange measurements is discussed. After presenting the calibration procedure, we display the chosen conditions and conclude with a thorough analysis of the performed handheld key exchanges.

6.1. Calibration

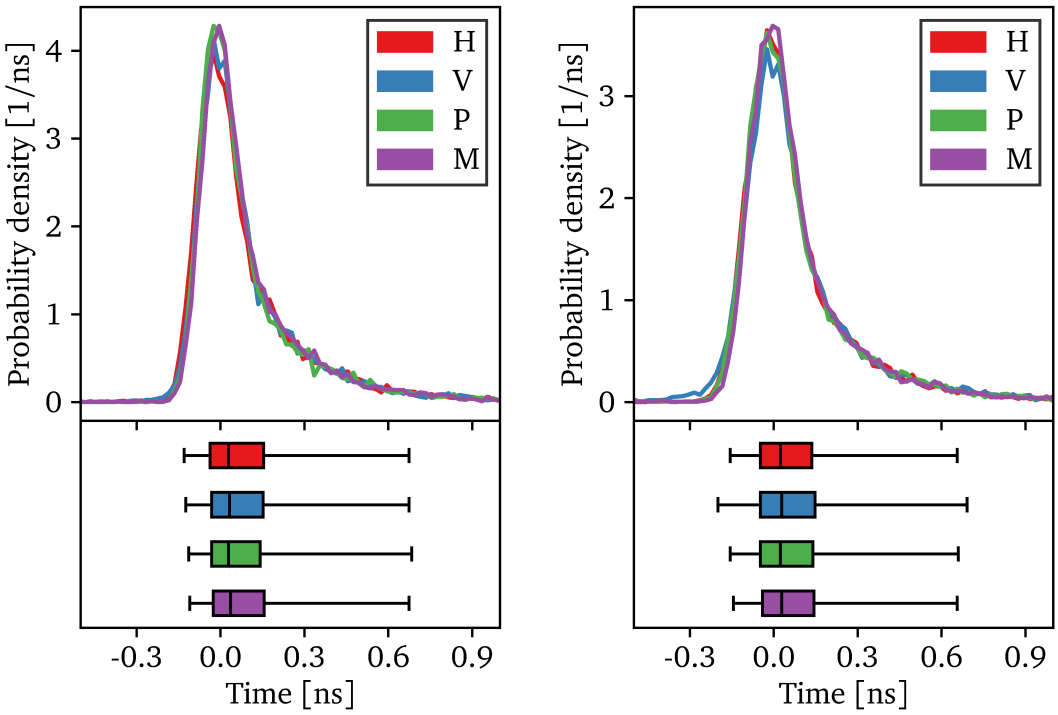
Several tasks are necessary before a key exchange can be performed: It must be made sure that Alice's pulses overlap temporally, the intensity has to be set accurately and equal for the four diodes, and, for proper compensation, the polarization states need to be tomographed.

6.1.1. Temporal Overlap

The shape of the signal pulses in the temporal domain is depicted in Figure 6.1. 10 000 and 20 000 detections, respectively, have been recorded for two sets of key exchanges—one with low and one with high intensity pulses. For convenience, we define pulse length as the duration in which 95 % of the events have been detected. This quantity is more meaningful as, e.g., the full-width-half-maximum (FWHM), which strongly depends on only a few values and, therefore, reveals little on the rest. For the high intensity key exchange, this pulse length was 610 ps, for the low intensity key exchange 641 ps. This difference could be caused by the changed pulse settings or by different temperatures in the laboratory.

The quantum mechanical overlap (see Equation 3.21), assuming a perfect correspondence in the frequency domain, evaluates to 98.4 % and 98.9 %, respectively, averaged over all pulse combinations (see Table 6.1 for a full analysis). Due to Poissonian noise in each time bin even a perfect overlap would, at the number of detections taken, yield only overlaps of 99.0 % and 99.3 %, respectively (note that noise can make the overlap only worse). Therefore, we consider the pulses close to indistuinguishable.

Both subjectively and objectively, the vertically polarized pulse of the low intensity measurement appears to overlap relatively poorly with the three other ones. This



(a) High intensity key exchange (b) Low intensity key exchange

Figure 6.1.: Temporal pulse shapes for the two pulse settings. For each of the four sources, the probability time-density and a corresponding boxplot is shown. The boxes enclose 50 %, the whiskers 95 % of the data points. Vertical lines mark the median.

defect is caused by a short and shallow run-up phase before the actual rising slope only featured only by this channel, as well as a slightly lower peak intensity. A higher modulation current, as was used for instance in the high intensity measurement, might have addressed this issue.

6.1.2. Mean Photon Number

Once the pulses overlap in time domain, their intensity needs to be chosen. For this, an expected QBER and transmission is predicted. Optimizing the secret key rate expressions discussed in Section 3.2.4 then yields, depending on the applied protocol, a target value (see Figure 6.2).

	H	V	P	M
H	100	98.5	98.3	98.2
V	98.5	100	98.3	98.2
P	98.3	98.3	100	98.6
M	98.2	98.2	98.6	100

(a) High intensity key exchange

	H	V	P	M
H	100	98.9	99.2	99.1
V	98.9	100	98.7	98.5
P	99.2	98.7	100	99.1
M	99.1	98.5	99.1	100

(b) Low intensity key exchange

Table 6.1.: Quantum mechanical overlaps of the time degree of freedom between each pulse pair in percent.

While the intensity has to be set roughly already during the calibration of the pulse shape, it is fine-tuned at a later point in time by controlling only the modulation current. This ensures that the brightness is determined as shortly before the key exchange as possible, allowing little room for change by, e.g., ambient temperature fluctuations. At the same time, the pulse shape stays essentially the same as only slight variations of a single parameter are performed.

All key exchanges discussed in this thesis have been performed with one of two mean photon numbers: $\mu_{\text{low}} = 0.05$ and $\mu_{\text{high}} = 0.15$. μ_{low} is, at our system parameters and for handheld operation, optimal according to GLLP. Key exchanges with μ_{high} are intended for a decoy analysis. Here, even larger intensities would be desirable. These are, however, prohibited by a beginning degradation of our transmitter's laser sources. None the less, key rates multiple times higher than for GLLP can be expected.

The mean photon number has been measured using the receiver's polarization analysis unit. To this end, Alice has been mounted in front of Bob's entrance pinhole and the coupling efficiency has been maximized using two mirrors. In this configuration, the coupling efficiency to each detector is known [21]. Also taking into account the specified detector efficiency and the pulse repetition rate, the measured count rates are converted to a mean photon number per pulse.

The intensities of the four laser sources are matched with each other by individually tuning the modulation current of the channels. Likely due to crosstalk, the mean photon number increases unpredictably when all channels are turned on in an alternating fashion (as it is the case during a key exchange). Therefore, multiple steps of matching the channels and checking the resulting total intensity are performed.

The final pulse parameters are shown in Table 6.2.

6.1.3. Polarization State Tomography

Section 4.2.1.2 described Bob's ability to compensate for inevitable polarization rotations. This task requires knowledge of the initial states prepared by the transmitter.

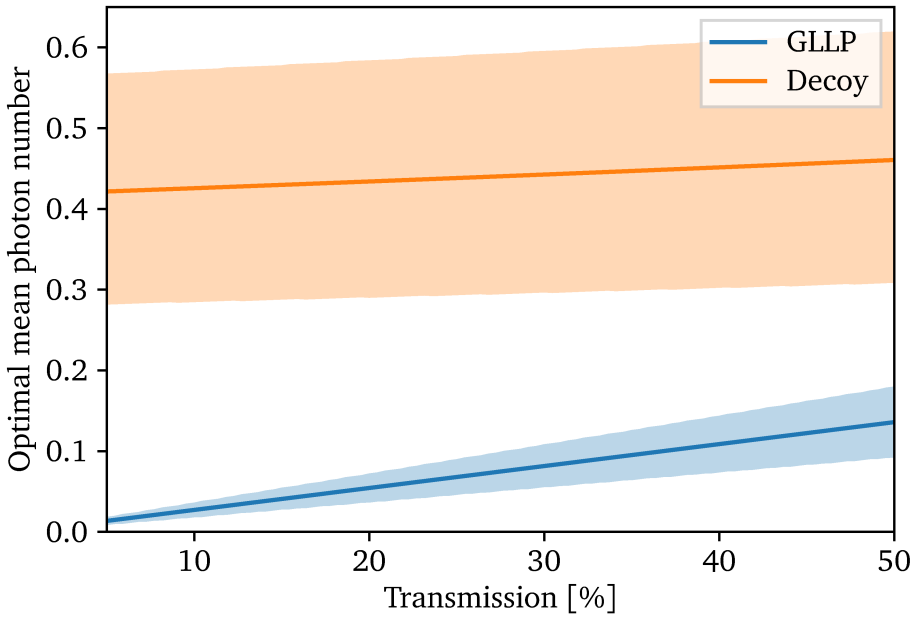


Figure 6.2.: Optimal mean photon number as a function of transmission. For GLLP lower mean photon numbers than for the decoy protocol have to be chosen. The highlighted region around each curve marks less than 10 % deviation of the secret key rate from its optimal value. A QBER of 2 % and detector efficiency of 38 % (not included in the transmission) have been assumed.

As those have been observed to change over time, e.g., due to temperature drifts, we measure them right before a key exchange. To this end, two different methods have been applied, which have already been described individually by Freiwang [21]: A complete tomography and a partial one.

For the complete tomography the setup depicted in Figure 6.3a is used. A quarter waveplate and a polarizer, both mounted on stepping motors, project the incoming light onto one of the six Pauli eigenstates: horizontal, vertical, diagonal, and anti-diagonal as well as left- and right-circular polarization, depending on the angle settings. The remaining optical power is measured and, ultimately, the full state can be retrieved.

The partial tomography as seen in Figure 6.3b is performed using our receiver's polarization analysis unit. After some unitary transformation caused by Bob's optical components such as mirrors and lenses, the projections on the four BB84 states are measured. This scheme has the advantage of being fast, because there is a dedicated

Channel	Bias	Modulation	Delay A	Delay B
0 (V)	5	225	32	95
1 (P)	5	254	30	125
2 (M)	1	196	94	137
3 (H)	2	253	64	94

(a) Settings for the high intensity key exchange.

Channel	Bias	Modulation	Delay A	Delay B
0 (V)	2	191	29	89
1 (P)	6	238	40	137
2 (M)	1	149	89	133
3 (H)	4	235	82	110

(b) Settings for the low intensity key exchange.

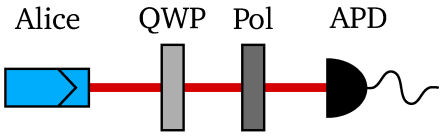
Table 6.2.: Pulse parameters ensuring overlap and equal intensities used during the two key exchanges. The numbers are parameters passed to the laser driver and delay lines, representing currents and time offsets, respectively.

detector for each projection while no mechanical components have to be moved. However, the information about the circular component of the state remains unknown. Furthermore, Bob's transformation would have to be characterized in order to reconstruct the original states.

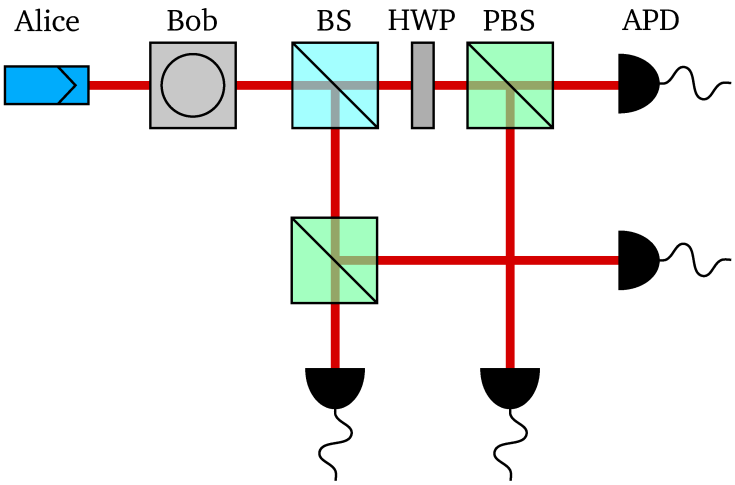
To benefit from the advantages of both schemes, we combine them: First, we extract the degree of polarization of each of the individual states from the results of a full tomography. Subsequently, we perform a partial tomography. The circular component can then, up to a sign, be calculated from the two measured components and the degree of polarization. The sign can simply be guessed, as a mistake would become clearly apparent in a failing state compensation. Bob's rotation does not have to be taken into account separately, as it needs to be compensated for as well.

For comparison between the full and partial tomographies, we mathematically apply an optimal, unitary compensation operation to both measurement results (see Section 4.2.1.2). This way, the polarization effects induced by Bob have no influence as long as they are unitary, but also any other unitary difference is disregarded. To quantify the agreement between the two schemes, we use the fidelity

$$F(\rho,\sigma) = \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \tag{6.1}$$



(a) Full tomography setup.



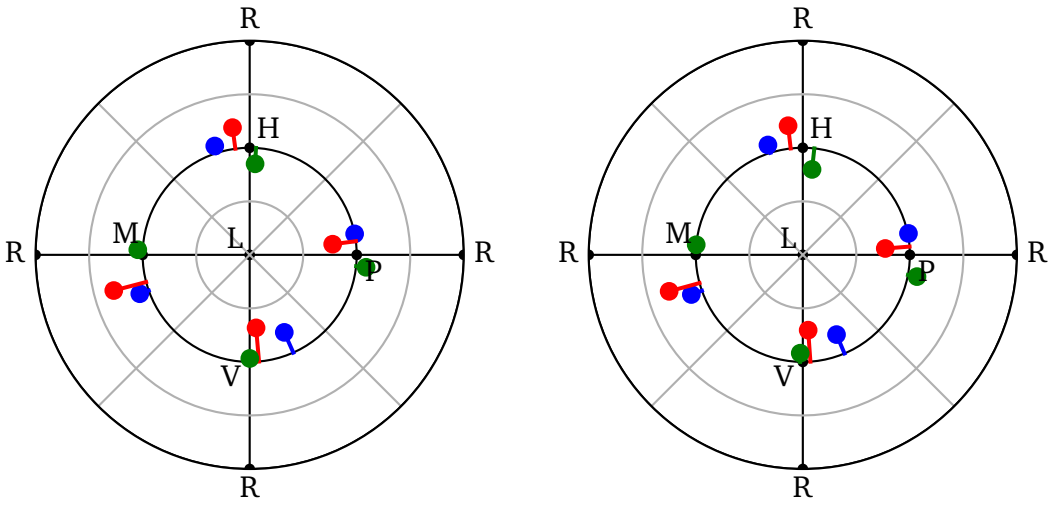
(b) Partial tomography setup.

Figure 6.3.: Pictorial representation of the two tomography setups. Alice: transmitter, QWP: rotating quarter wave plate, Pol: rotating polarizer, APD: avalanche photo detector, Bob: arbitrary polarization state rotation, BS: 50/50 beam splitter, HWP: half wave plate, PBS: polarizing beam splitter.

defined for two quantum states given by their density matrices ρ and σ. On average over the four BB84 polarization states, it evaluates to 0.9998 in both the high and the low intensity key exchange.

The essential results of the tomography are detailed in Figure 6.4, Table 6.3, and Appendix A. Two key coefficients describing the imperfections are the source intrinsic QBER after optimal compensation δ_A and the state preparation quality q (see Equation 4.1). δ_A amounts to 0.9 % and 0.8 %, q to 72.6 % and 75.3 % for the high and low intenisty key exchange, respectively.

Apparent are the large differences on the order of 10 % in the preparation quality factor determined with the different tomography schemes. One reason for this may be changes of the polarization states over time. Due to the steepness of the curve of q, even small distortions can have such severe effects. In addition, non-unitary components in the receiver such as mirrors with different reflection coefficients for



(a) High intensity key exchange. (b) Low intensity key exchange.

Figure 6.4.: Polarization states for the two key exchanges. Depicted is a Poincare sphere in azimuthal equidistant projection: The linear polarization angle is read off the azimuthal angle, the circular component off the radial distance from the equator. Original states in blue, states inside of Bob in red, compensated states in green.

horizontal and vertical polarization could have similar consequences. Therefore, we consider the value determined by the full tomography to be most accurate. This value being also the lowest one ensures that we do not overestimate our setup.

Finally, the unitary compensation operation calculated earlier was implemented in the experiment by turning the designated waveplates in the receiver accordingly (see Section 4.2.1.2). A partial tomography was performed with these settings, showing QBERs of 1.1 % and 1.6 % (Table 6.3 and Appendix A). The minor increase from the values estimated earlier could be explained by a slight misaligned reference axes of the waveplates. The fidelity of the compensation, calculated between the measured compensated states and the states from the partial tomography after optimal compensation, was 99.9 % and 99.6 %.

	H	V	P	M	avg
S_1	0.94	−0.85	0.19	−0.33	−0.01
S_2	−0.30	0.38	0.97	−0.93	0.03
S_3	0.11	−0.31	0.00	0.14	−0.02
DOP [%]	99.6	98.1	98.8	99.5	99.0
δ_{comp} [%]	0.5	1.5	1.1	0.4	0.9
q [%]			72.6		

(a) Full tomography of emitted states.

	H	V	P	M	avg
S_1	0.94	−0.86	0.12	−0.22	−0.01
S_2	−0.13	0.08	0.92	−0.85	0.01
S_3^*	0.31	−0.47	−0.33	0.47	−0.01
δ_{comp} [%]	0.4	1.3	1.0	0.5	0.8
q^* [%]			82.8		

(b) Partial tomography of states inside receiver.

	H	V	P	M	avg
S_1	0.97	−0.98	−0.10	0.05	−0.02
S_2	0.06	0.00	0.97	−0.99	0.01
S_3^*	−0.23	−0.05	0.14	0.07	−0.02
δ [%]	1.6	1.0	1.4	0.5	1.1
q^* [%]			86.4		

(c) Partial tomography after compensation.

Table 6.3.: Comparison of different polarization state tomographies for the high intensity key exchange. Each table breaks down the Stokes vector S of the horizontal (*H*), vertical (*V*), diagonal (*P*), and anti-diagonal (*M*) state as well as its degree of polarization (*DOP*) and its contribution to the quantum bit error rate (δ). Averages over all four states are in column *avg*. The row named *q* contains the extracted state preparation quality. For tables (a) and (b), the QBER after an optimal (calculated) compensation is specified (δ_{comp}). Values labeled with a star depend on the DOP acquired in the full tomography.

6.2. Experimental Setting

As implied in Section 3.2, the intensity of Alice's signal laser sources is a critical parameter for the final secret key rate that can be chosen freely by the experimenter. As the setup's performance under two distinct protocols (BB84 with and without decoy states) is ought to be studied, two respective optimal intensities arise. Thus, two similar key exchange runs differing essentially only in the signal beam power have been performed.

Furthermore, the final secret key rate does not only depend on properties of the setp but also on the person holding it: The steadiness of their hands has a considerable effect on the transmission. For this reason, multiple persons were asked to do multiple trials each.

During such a measurement, the user was sitting on a stool, whose height was adjusted at their convenience. The transmitter device was held in both hands close to the body, but without resting on anything. The laboratory was dimly lit, such that both the entrance pinholes and the beacon beam were clearly visible. The distance to the voicecoil mirror, defining the receiver's entrance, was roughly 30 cm.

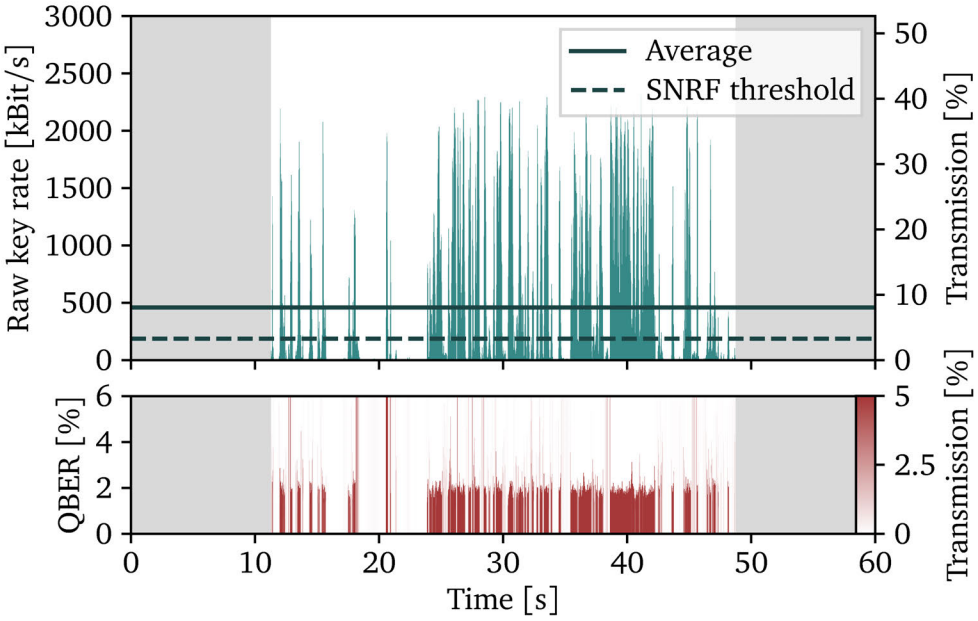
6.3. Analysis

After the setup had been calibrated with the satisfying results presented above and the key exchanges had been performed, the recorded data has been analyzed following Chapter 5. In the interest of meaningful comparability, the recorded data has been cropped such that it starts once coupling has been achieved for the first time and stops once the user willingly quits. We emphasize, though, that between the such defined beginning and end, no data was discarded. This resulted in exchange durations between roughly 15 and 55 s.

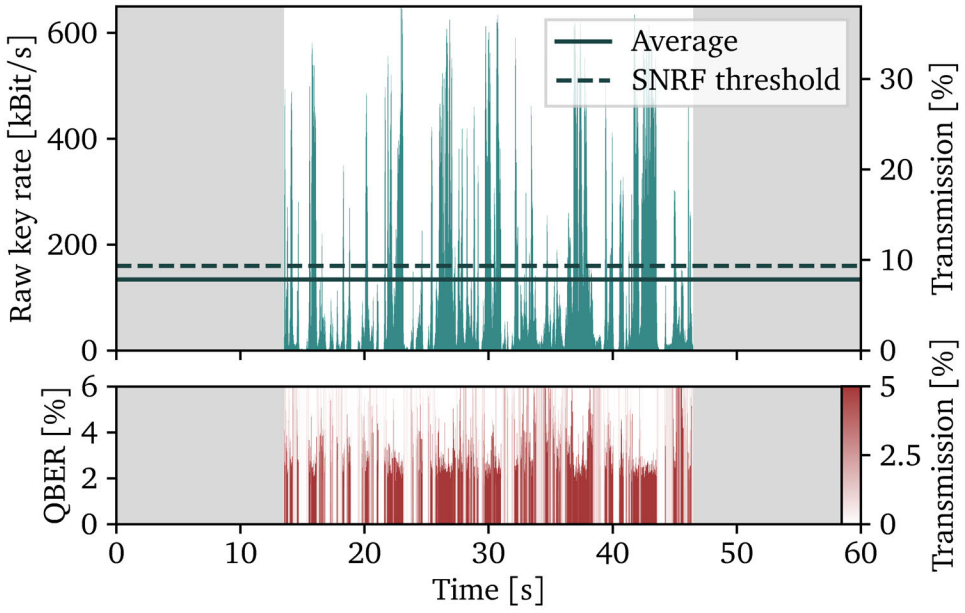
Figure 6.5 plots transmission and QBER over time for two exemplary measurements. For the complete set we refer to Appendix B. The main results are listed in Table 6.4. In the following, the course of the transmission over time, the impact of signal-to-noise filtering, the error rates, and the resulting key rates are studied in more detail.

6.3.1. Transmissions

The most obvious feature apparent in all trials is that the intensity fluctuates rapidly between zero and a maximum value. This is to be expected given that only perfect beam tracking would result in a constant transmission. Some imperfections have to be accepted, as our system can only correct for angles but not for displacement, is limited to a range of ±3°, and reacts with a finite delay.



(a) Key exchange X (high intensity).



(b) Key exchange XV (low intensity).

Figure 6.5.: Raw key rate, transmission and QBER over time for two exemplary trials, before SNR filtering. Raw key rate and transmission are proportional to each other and, thus, label the same plot. The solid line denotes the transmission and raw key rate average before SNR filtering, the dotted line the SNR threshold (detections below this line are discarded). QBERs at low transmissions are plotted in faint colors as they do contribute little to the overall average. For ease of comparison, both figures span 60 s, although the actually analyzed range is shorter.

Trial	Duration [s]	Key rate [kbit s^{-1}]			Total [Mbit]
		Raw	Sifted	Secret	
I	17.0	362	181	100	1.7
II	49.0	530	267	158	7.7
III	37.7	332	166	90	3.4
IV	36.5	421	212	47	1.7
V	32.0	293	147	42	1.3
VI	45.5	375	189	112	5.1
VII	39.5	298	139	52	2.0
VIII	14.5	241	123	69	1.0
IX	38.5	891	445	267	10.3
X	37.5	442	222	106	4.0
XI	31.5	193	97	56	1.7
XII	43.7	899	453	261	11.4

(a) Results of high intensity key exchanges with decoy analysis.

Trial	Duration [s]	Key rate [kbit s^{-1}]			Total [Mbit]
		Raw	Sifted	Secret	
XIII	30.5	203	100	39	1.2
XIV	26.5	63	31	10	0.3
XV	33.0	106	51	20	0.7
XVI	23.5	121	59	19	0.4
XVII	49.0	96	47	17	0.8
XVIII	41	133	66	19	0.8
XIX	39.5	128	63	23	0.9
XX	51.5	82	40	14	0.7

(b) Results of low intensity key exchanges with GLLP analysis.

Table 6.4.: Main results of key exchanges. Column “Rates” contains rates extracted after SNR filtering. “Total” is the product of duration and secret key rate.

For these reasons, the system cannot fully compensate shaking of the device in handheld operation. Due to physiological differences, this affects some users more strongly than others, resulting in different transmission averages for different trials: They vary almost by a factor of three.

The three worst trials conducted—VII, VIII, and IX—are characterized by long periods of negligible transmission, presumably caused by a simple misalignment. A system with a higher acceptance angle, which is currently under development [74], would be able to narrow such periods and might thus significantly improve secret key generation rates under similar conditions.

Two examples of very high transmission are trial IX and XII. These differ from many average trials only in the frequency with which transmission spikes are reached as well as in the local minima in between. However, the transmission maxima are similar in value. These results suggest that the tracking system is in principle capable of compensating hand motions extremely efficiently. Thus, minor speed improvements might already show compelling effects.

Despite all possibility for improvement, even for the least satisfactory key exchanges the transmission was sufficient to extract secret keys at practical rates—both for GLLP and decoy analysis.

6.3.2. SNR Filter

As discussed in Section 5.2.4, signal-to-noise filtering discards periods of the raw key that have a low transmission. This improves QBER and transmission averaged over the rest of the exchange time at the expense of the raw key rate. It proved itself as a crucial tool in handling the low intensity key exchanges, which were analyzed according to GLLP. As their secret key rate formulas depend strongly on the transmission, no keys can be extracted from the unfiltered data sets. Filtering increases the transmission value up to a level at which this is possible again.

When decoy formulas are used, which is the case for the high intensity data set, only minor gains could be achieved. Here, the transmission only marginally affects the secret fraction (see Figure 3.1) and thus the raw key rate is the more dominant factor. SNR filtering, however, reduces the raw key rate with consequentially negative effects on the secret key rate. But filtering can still be favorable in these cases because it reduces the QBER: During the discarded periods of weak signal, proportionally more detections are caused by random background having an error rate of 50 %.

The effects of SNR filtering as well as their optimal thresholds are compiled in Table 6.5. Here, thresholds are expressed on the same scale as the channel transmission, excluding detector efficiencies. Thus, time bins with transmissions lower than this threshold are discarded. The in principle equivalent alternative—quoting

a raw key rate threshold—would make comparisons between measurements with different mean photon numbers more difficult.

While it is generally true that a higher threshold results in a higher number of discarded bits, this does not necessarily hold when comparing unrelated data sets, as they may show different transmission distributions. This can, e.g., be seen at trials XIII and XV which both cutoff at 9.3 % transmission, but discard 10 and 21 % of bits respectively. Comparing their plots in Appendix B confirms, that in one case simply more time bins are affected by the filter.

For the GLLP key exchanges large thresholds are chosen by the optimization algorithm: On average they amounted to 9.3 %, leading to roughly 20 % of raw key bits to be sacrificed. Intriguingly, for all the low intensity trials, after SNR filtering, the transmission rose to similar values around 20 %, although the initial transmission varied by more than a factor of two. This indicates that the performance in this regime is indeed limited by bad transmission: Only once a certain, high transmission is reached, the secret fraction becomes positive. At this point, raising the threshold by even a little higher reduces the raw key rate significantly already, since the affected time bins have many detections in them. Therefore, the maximum found by the optimization algorithm lies in a very narrow region.

For the trials analyzed with decoy formulas, much smaller thresholds are used, which also span a larger range from 0.7 to 6.7 %. Even for very small transmissions, the contribution by background counts to the QBER is negligible, explaining the low thresholds. The wide range is due to the steep flanks of the high transmission peaks: They allow the threshold to change greatly with only little effect on both transmission and raw key rate. Trial V and VII stand out by a large number of discarded bits. In those measurements, however, the QBER was exceptionally high for reasons discussed in the next section, which makes them a special case and a comparison with the rest not particularly meaningful.

6.3.3. Error Rates

The quantum bit error rates (QBERs), i.e., the rates of wrong bits in the sifted key were in most cases on average 1.6 % for the high and 2.4 % for the low intensity key exchange. SNR filtering, reduced them from 1.8 % and 2.8 %, respectively (see Table 6.5).

Considering the predictions from the calibration measurements of 1.1 % and 1.6 % (see Section 6.1.3) this might appear disappointing. However, those numbers only incorporate imperfections in the polarization state and detector darkcounts. In practice, additional sources of background detections are present, each resulting in an error with probability of 50 %: First, the beacon laser is not blocked completely by the interference filter inside the receiver. While it is linearly polarized and, therefore,

Trial	Threshold [%]	Discarded [%]	QBER [%]	Transmission [%]
I	1.8	3	2.2 ↘ 1.7	6.4 ↗ 14.3
II	4.7	6	2.1 ↘ 1.4	9.6 ↗ 19.6
III	1.8	3	2.1 ↘ 1.8	5.9 ↗ 13.3
IV	2.2	3	5.1 ↘ 4.9	7.5 ↗ 18.5
V	5.8	12	6.8 ↘ 4.3	5.7 ↗ 19.4
VI	1.1	1	1.5 ↘ 1.4	6.5 ↗ 13.1
VII	6.7	12	4.4 ↘ 3.4	5.4 ↗ 18.3
VIII	3.4	6	2.0 ↘ 1.6	4.4 ↗ 16.1
IX	0.7	0	1.4 ↘ 1.4	15.3 ↗ 23.0
X	3.3	4	2.7 ↘ 2.4	7.9 ↗ 18.1
XI	0.9	2	1.6 ↘ 1.4	3.4 ↗ 12.1
XII	1.1	0	1.6 ↘ 1.5	15.5 ↗ 19.1

(a) High intensity key exchange

Trial	Threshold [%]	Discarded [%]	QBER [%]	Transmission [%]
XIII	9.3	10	2.4 ↘ 2.3	13.2 ↗ 21.9
XIV	9.7	27	3.2 ↘ 2.6	5.0 ↗ 20.4
XV	9.3	21	2.6 ↘ 2.3	7.9 ↗ 21.6
XVI	9.4	18	3.0 ↘ 2.7	8.6 ↗ 19.2
XVII	9.5	20	3.1 ↘ 2.4	7.0 ↗ 20.0
XVIII	9.5	17	2.9 ↘ 2.4	7.8 ↗ 19.8
XIX	8.7	16	2.5 ↘ 2.3	8.9 ↗ 19.4
XX	9.0	17	2.7 ↘ 2.5	5.8 ↗ 19.5

(b) Low intensity key exchange

Table 6.5.: Effects of the SNR filtering on performance defining quantities. The transmission threshold below which detections are discarded can be read off of column “Threshold”. The number of discarded detections is expressed under “Discarded” as a percentage of detections in the raw key.

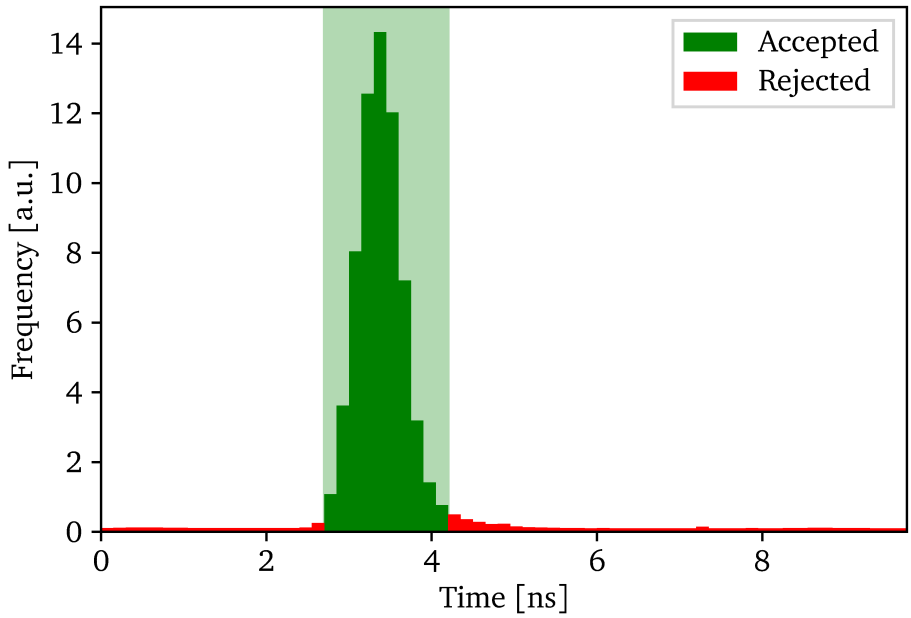


Figure 6.6.: Time histogram of detection events. Detections outside the detection window of 1.5 ns around the expected arrival time (light green) are rejected.

might couple to some detectors preferentially, it is, still, not correlated to the sent qubit. Second, during the key exchanges all four laser diodes are constantly biased and therefore emit some radiation even when no pulse is stimulated.

Furthermore, during a handheld key exchange, the transmission is on average lower than during the carefully coupled calibration measurement. Therefore, dark-counts by the detector and clicks from ambient light have a proportionally larger effect.

As mentioned in Section 5.2.2, a detection window of length 1.5 ns around the expected arrival time of the pulses filters most of the background clicks: Since those are evenly distributed over the pulse interval of 10 ns, only 15 % of the detections survive (see Figure 6.6). The window has to be larger than the pulse length characterized in Section 6.1.1 as the receiver's detector has a time jitter of 400 ± 50 ps [68] leading to a seemingly broader pulse. Additional spreading might be caused by the limited time resolution of the timestamping unit as well as phase fluctuations of the clock recovery output signal.

A final source of errors is the sender device's rotation. While an appropriate active alignment solution is in place (see Section 4.2.3.1), it only works for sufficiently slow changes due to its limited repetition rate of 10 Hz and cannot, e.g., make up for

trembling hands which oscillate at similar frequencies [67]. However, the expected amplitudes should be small and the induced errors thus little. In trial IV, V, and VII, the basis alignment control software had stopped unnoticed explaining the measured high QBERs and illustrating the importance of the compensation.

It is striking that the QBER for the low intensity key exchange is larger than for the high intensity one. This stems from the fact that the polarization states emitted by the source are slightly different, expressing itself in the two different values for the source intrinsic QBER. Additionally, a low signal intensity results in a more sparse raw key. The background, on the other hand is equally bright and, thus, while the absolute number of wrong bits stays the same, its fraction increases.

6.3.4. Raw, Sifted, and Secret Key Rates

The ultimate quantity assessing the performance of a quantum key distribution system is its secret key rate. It is a function of transmission and QBER, which have been discussed earlier already (see Section 3.2.4), and the raw key rate after SNR filtering, all averaged over the whole exchange time. Being proportional to the transmission without filtering, the raw key rate differed significantly between the different trials (see Table 6.4). For the high intensity key exchange, it varied between about 200 and 900 kbit s^{-1} with an average of 440 and a median of 370 kbit s^{-1}. Raw key rates for the low intensity trials fell into a range between 60 and 200 kbit s^{-1} with median 110, averaging to 120 kbit s^{-1}.

The raw key rate and mean photon number per pulse should—neglecting the improbable multi-photon pulses—be proportional to each other. As the mean photon number during the high intensity key exchange was about three times as large as during the low intensity one (see Section 6.1.2), the raw key rates in the low intensity trials appear slightly too low (or, alternatively, the high intensity ones too high). The differences are, however, small compared to fluctuations in transmission, such that they can easily be explained by the different user's form of the day.

It is suspicious that the sifted key rate for many trials is not exactly half of the raw key rate. To have a mismatch here, two factors have to come together: The sender has to send states from one basis more often or with higher intensity than the states from the other basis, and the receiver's detectors have to have unequal efficiencies. While the latter issue is known to exist for our setup [21], the former one is suprising. The sent keys as loaded into Alice's memory have been checked, but their qubit distribution was found to be even. Therefore, the cause must lie in Alice producing different mean photon numbers for the different states.

While the intensites of the sender's four laser sources have been matched during the calibration sequence (Section 6.1.2), this was done only individually. During the key exchanges themselves, however, all four diodes were biased at the same time,

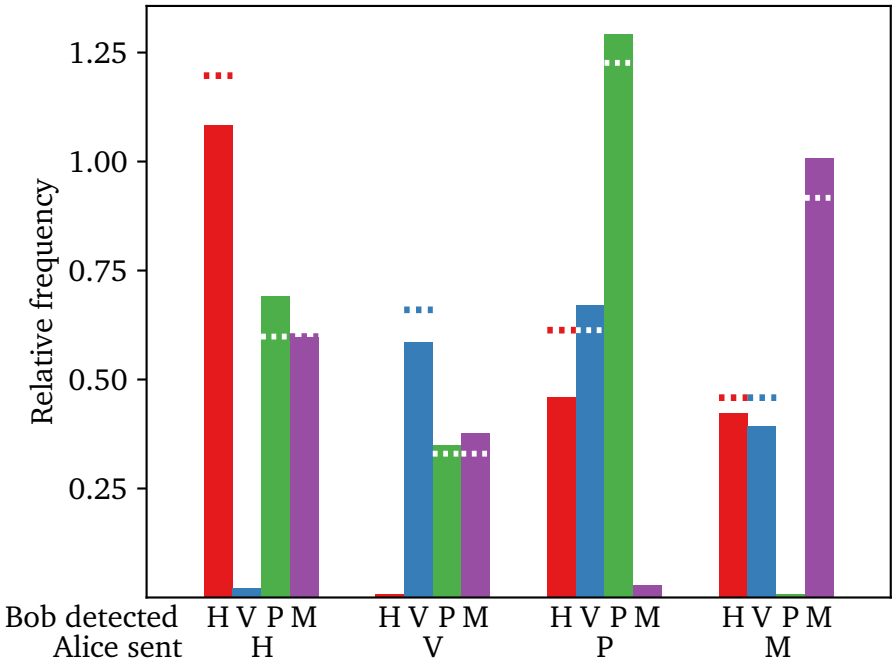


Figure 6.7.: Frequencies of sending and detecting states for all sixteen combinations. Dotted lines mark the frequencies expected for ideal states during an exemplary key exchange. Data is normalized such that in the ideal case the bars would have heights of 1, 0, 0.5, and 0.5

opening up the possibility of an intensity change. A calibration procedure more careful in this regard can likely solve this problem.

For further investigation, the clicks of each detector have been counted conditioned on the sent state and plotted for one examplary trial in Figure 6.7. As can clearly be seen, pulses with vertical and anti-diagonal polarization are detected less often. This issue is even more pronounced than the differences between the two bases, that become noticable in the deviating sifting rate. While this should affect the secret key rate negatively, no security proof incorporating different mean photon numbers for different states have been found. Therefore, we have to leave it unaddressed in the analysis.

Finally, the estimated secret key rates calculated with the formulas discussed in Section 3.2.4 follow a distribution similarly broadly scattered as the raw key rate: Between 42 and 267 kbit s^{-1} for the high and between 14 and 39 kbit s^{-1} for the low

intensity key exchange, with averages of 113 and 20 kbit s^{-1} as well as medians of 95 and 19 kbit s^{-1}, respectively. The large superiority of the high intensity key exchange is caused mainly, besides the slightly better QBER, in the decoy protocol: It allowed the usage of a higher intensity, which lead to larger raw key rates, and in addition to that estimated the eavesdropper's knowledge tighter—the secret fraction is larger, less bits need to be sacrificed in postprocessing at privacy amplification.

Multiplying each secret key rate with the duration of the corresponding measurement gives a number of secretly transmitted bits. For the high intensity trials this amounted to around 5 Mbit and to slightly less than 1 Mbit for the low intensity ones. Given the exchange times of only about 30 s both numbers testify the sufficiency of our setup in many practical application scenarios.

7. Conclusion

In this thesis, quantum key distribution between a handheld sender device and a stationary receiver was successfully demonstrated. We built upon preceding works designing and assembling transmitter [19] and receiver [20], as well as their thorough characterization [21]. Alongside few changes in the the experimental setup, we contributed the data analysis procedure described in Chapter 5 in order to complete the experiment. Finally, as discussed in Chapter 6, we performed measurements and estimated secret key rates for two protocols: BB84 with and without the decoy state extension.

The Secret key rates amounted to values between 10 and 39 $\mathrm{kbit\,s^{-1}}$ (BB84) and between 40 and 267 $\mathrm{kbit\,s^{-1}}$ (decoy). Signal to noise ratio filtering was found to be extremely beneficial to the analysis of handheld key exchanges, due to their typically featured strongly fluctuating transmission. Both temporal and spatial pulse shape were ruled out as possible side-channels, in contrast to the spectral degree of freedom, which was confirmed to be not yet overlapping.

To develop the system to a level of market-readiness, a number improvements at the hardware level are still necessary. At the sender side, the open spectral side-channel has to be closed. This can be faciliated by replacing the employed VCSELs by wavelength-tunable ones or by preselection of the installed diodes. To ensure a pleasant user experience, we suggest to automize the calibration procedure or even render it superfluous by enhancing the stability of the electronics. Long-term challenges include the industrialization of the manufacturing process and the integration into existing hard- and software.

On the receiving end, the active beam tracking mechanism is a promising starting point for improvement. Both a larger acceptance angle and faster tracking will substantially increase the achievable transmission rates as well as the maximum distance between sender and receiver in handheld operation. Depending on the application scenario, miniaturization might be beneficial here as well.

To increase the maximum key length, enhanced synchronization capabilities are needed. To this end, the already existing beacon laser can be used to periodically transmit block serial numbers. This merely requires software modifications at both sender and receiver. Similarly, we propose to extend the analysis program by routines actually extracting secret keys from the detected material instead of just estimating corresponding rates. Also, effects of finite statistics on the secret key rate have to be considered.

In summary, quantum key distribution between a handheld sender and a stationary was demonstrated in a laboratory setting. Based on the insights gained during this project, we predict that real-world applications are feasible as well. This will make the transmission channel of freespace communication systems unconditionally secure, rendering a variety of attack vectors ineffective.

Looking further ahead, many additional application scenarios may benefit or even require miniaturization similar to the handheld use case investigated here. Those scenarios include the integration of QKD devices into existing optical point-to-point communication links. Due to the lack of hand motions in such systems, long distances could be bridged with essentially the same hardware. With improved beam tracking and customized optics, even ground-to-satellite and inter-satellite quantum key distribution seems viable, providing a formidable challenge for future endeavors.

A. Tomography Data

In this appendix, we show detailed results of the various quantum state tomographies discussed in Section 6.1.3.

	H	V	P	M	avg
S_1	0.94	−0.85	0.19	−0.33	−0.01
S_2	−0.30	0.38	0.97	−0.93	0.03
S_3	0.11	−0.31	0.00	0.14	−0.02
DOP [%]	99.6	98.1	98.8	99.5	99.0
δ_{comp} [%]	0.5	1.5	1.1	0.4	0.9
q [%]			72.6		

(a) Full tomography of emitted states.

	H	V	P	M	avg
S_1	0.94	−0.86	0.12	−0.22	−0.01
S_2	−0.13	0.08	0.92	−0.85	0.01
S_3^*	0.31	−0.47	−0.33	0.47	−0.01
δ_{comp} [%]	0.4	1.3	1.0	0.5	0.8
q^* [%]			82.8		

(b) Partial tomography of states inside receiver.

	H	V	P	M	avg
S_1	0.97	−0.98	−0.10	0.05	−0.02
S_2	0.06	0.00	0.97	−0.99	0.01
S_3^*	−0.23	−0.05	0.14	0.07	−0.02
δ [%]	1.6	1.0	1.4	0.5	1.1
q^* [%]			86.4		

(c) Partial tomography after compensation.

Table A.1.: Comparison of different polarization state tomographies for the high intensity key exchange (same as Table 6.3).

	H	V	P	M	avg
S_1	0.94	−0.87	0.20	−0.33	−0.01
S_2	−0.30	0.37	0.97	−0.92	0.03
S_3	0.12	−0.29	0.01	0.16	0.00
DOP [%]	99.8	98.7	98.9	98.7	99.0
δ_{comp} [%]	0.3	1.1	1.0	0.9	0.8
q [%]			75.3		

(a) Full tomography of emitted states.

	H	V	P	M	avg
S_1	0.94	−0.88	0.07	−0.23	−0.03
S_2	−0.11	0.06	0.92	−0.85	0.01
S_3	0.33	−0.44	−0.35	0.44	0.00
δ_{comp} [%]	0.3	0.8	1.0	0.8	0.7
q [%]			79.7		

(b) Partial tomography of states inside receiver.

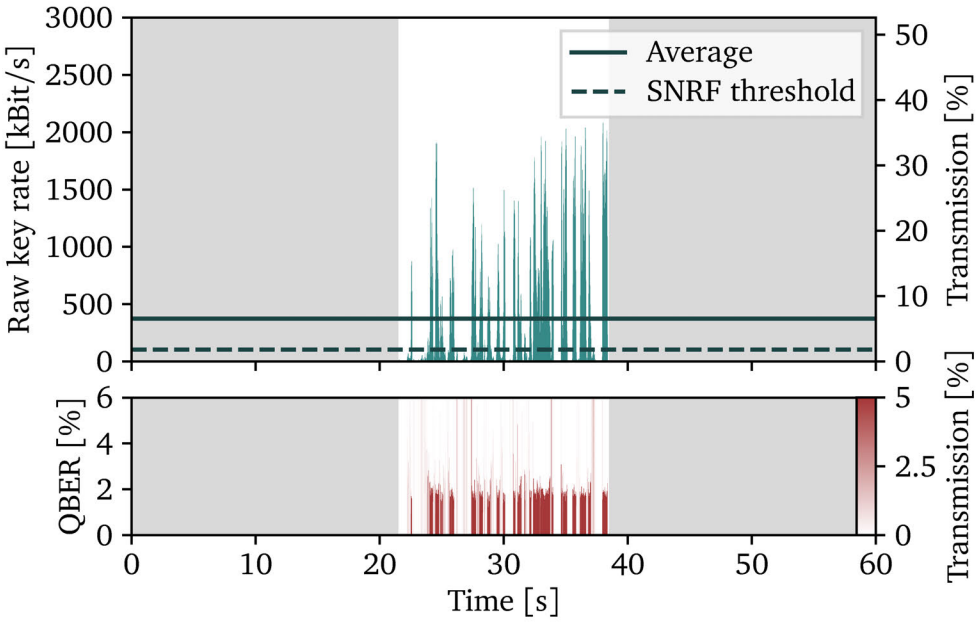
	H	V	P	M	avg
S_1	0.94	−0.98	−0.18	0.09	−0.03
S_2	0.10	−0.03	0.96	−0.99	0.01
S_3	−0.30	−0.13	0.13	0.00	−0.07
δ [%]	2.8	1.1	1.9	0.7	1.6
q [%]			80.9		

(c) Partial tomography after compensation.

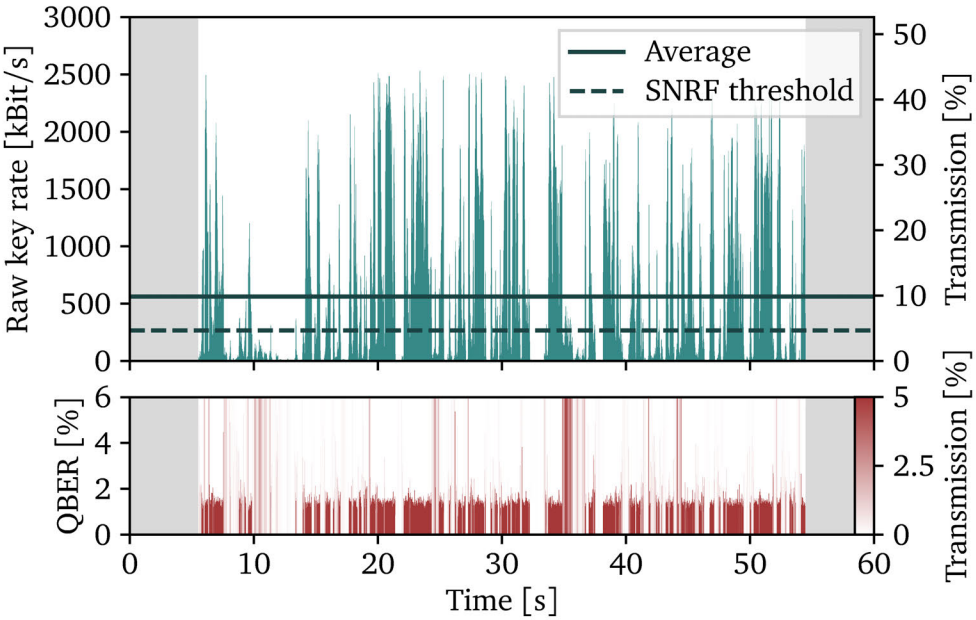
Table A.2.: Comparison of different polarization state tomographies for the low intensity key exchange.

B. Key Exchange Figures

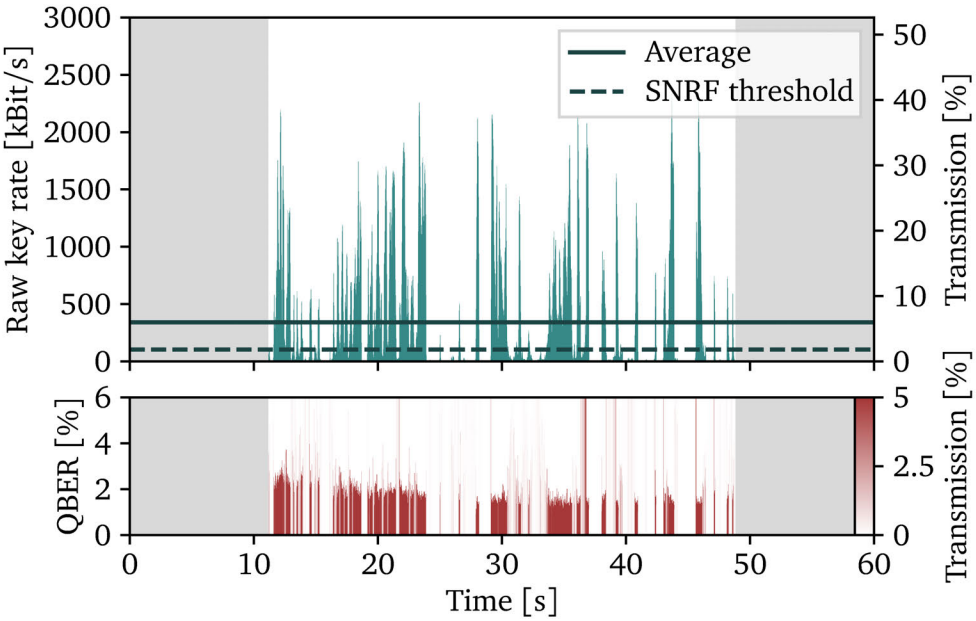
This appendix is a list of key exchange plots for all measurements discussed in this thesis. See the caption of Figure 6.5 for details about the visualization method and Section 6.3 for an interpretation of the data.



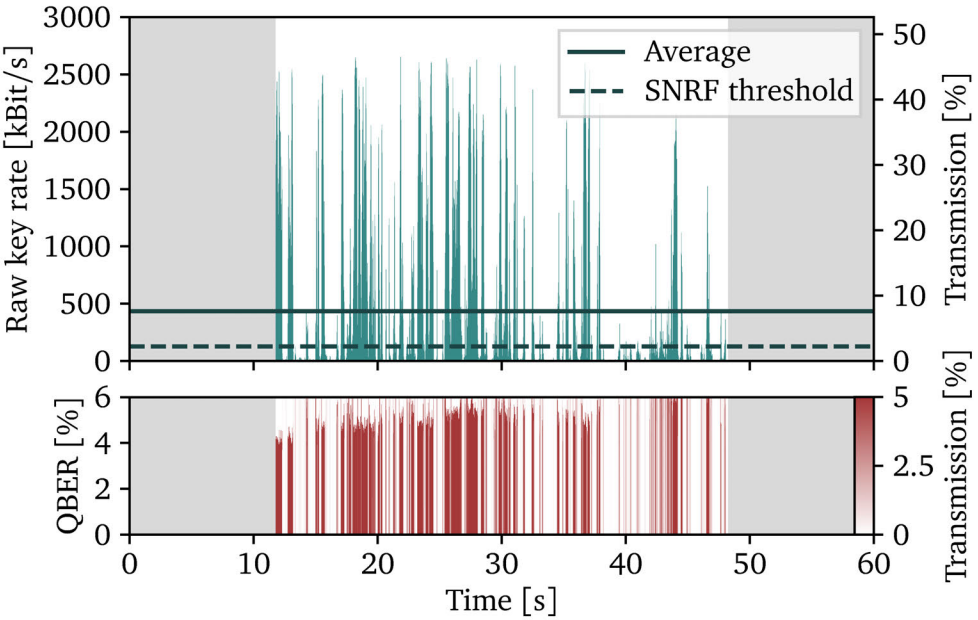
(a) High intensity key exchange I.



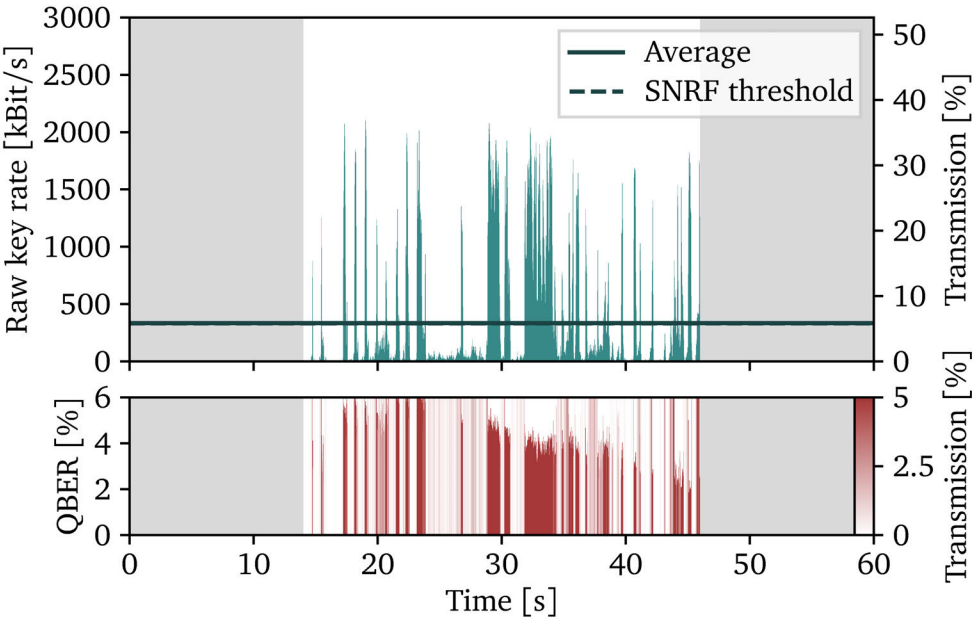
(b) High intensity key exchange II.



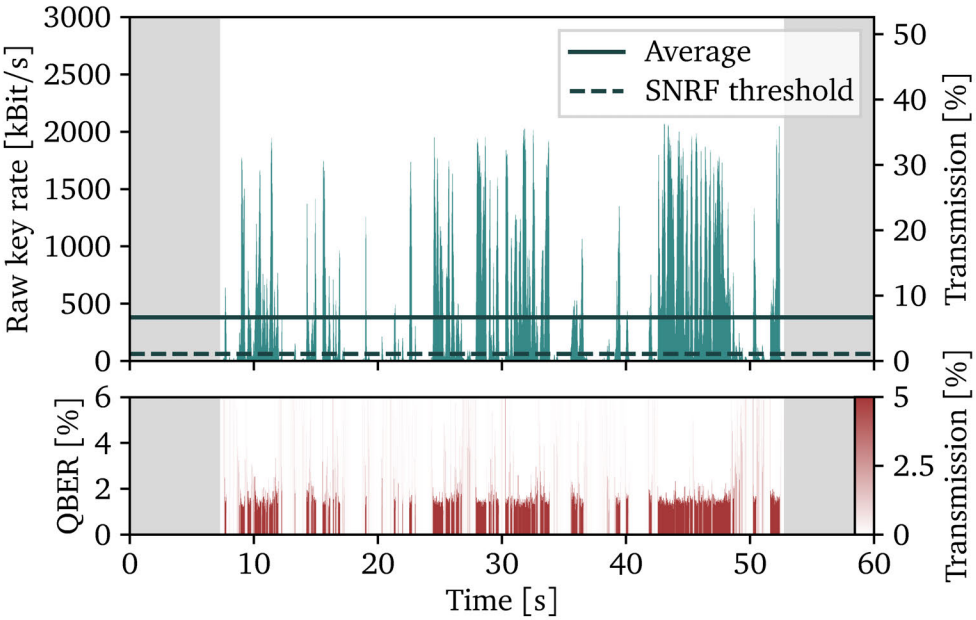
(c) High intensity key exchange III.



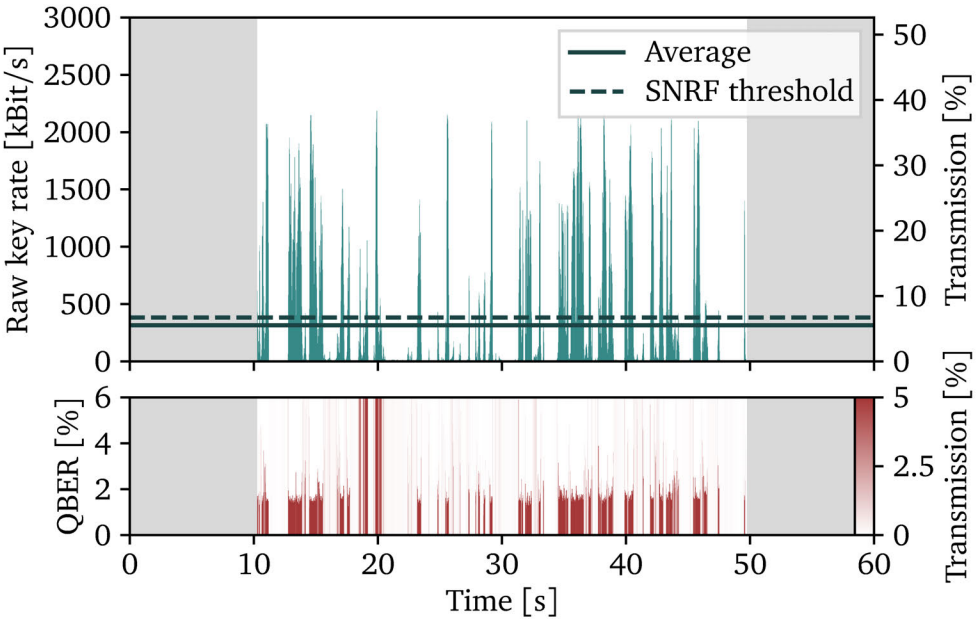
(d) High intensity key exchange IV.



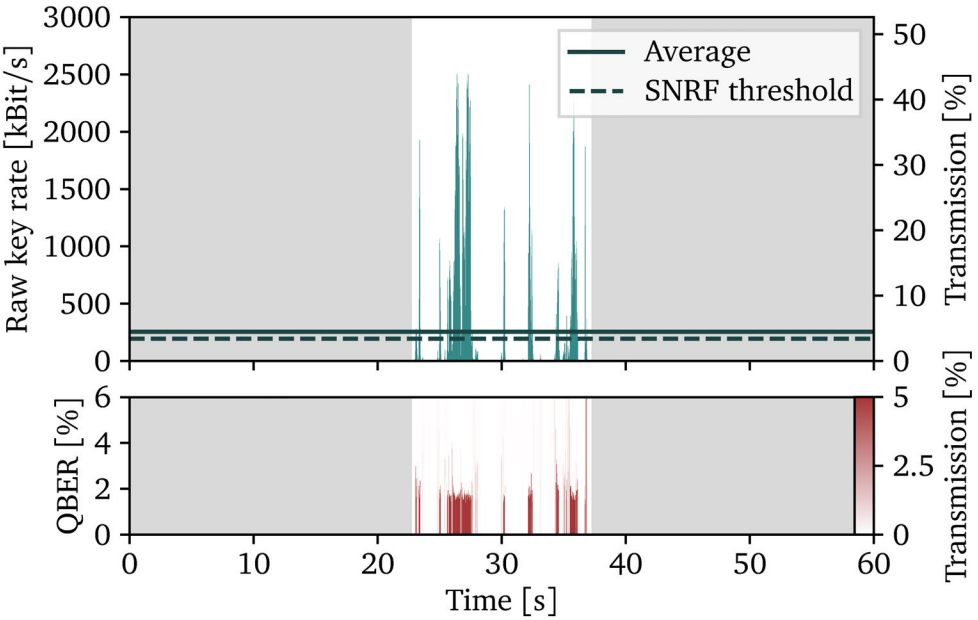
(e) High intensity key exchange V.



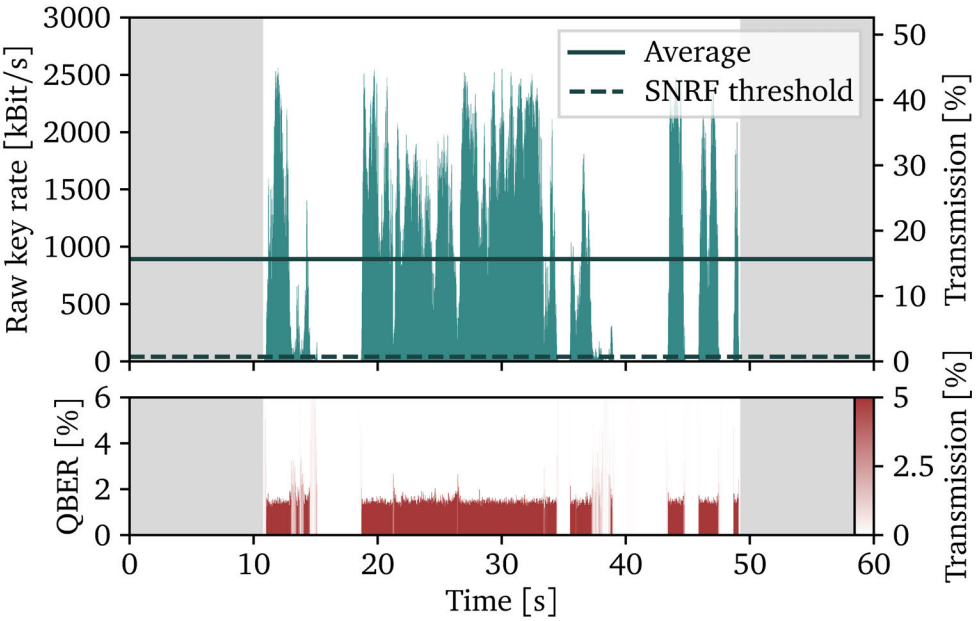
(f) High intensity key exchange VI.



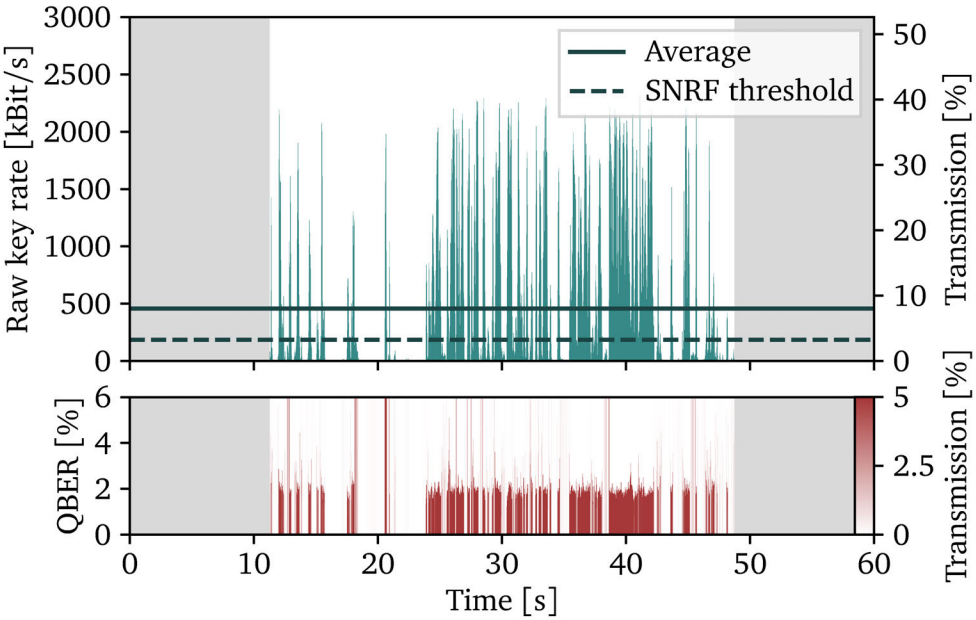
(g) High intensity key exchange VII.



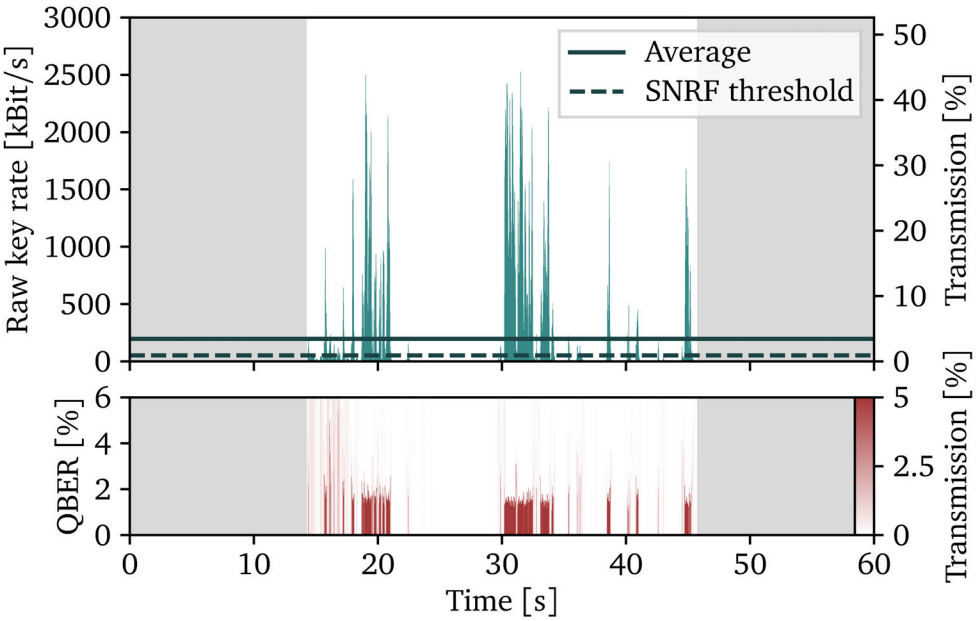
(h) High intensity key exchange VIII.



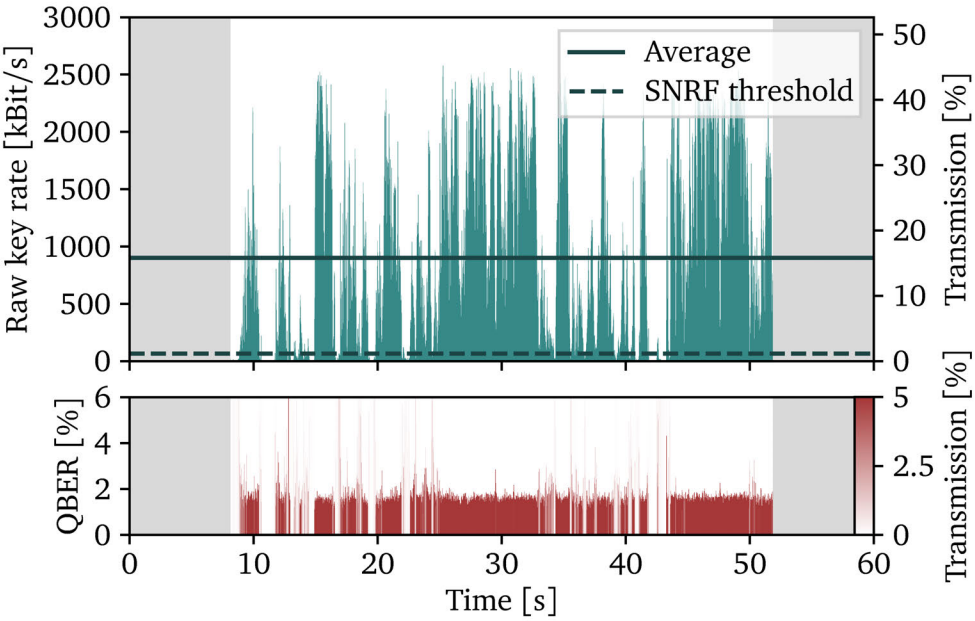
(i) High intensity key exchange IX.



(j) High intensity key exchange X.

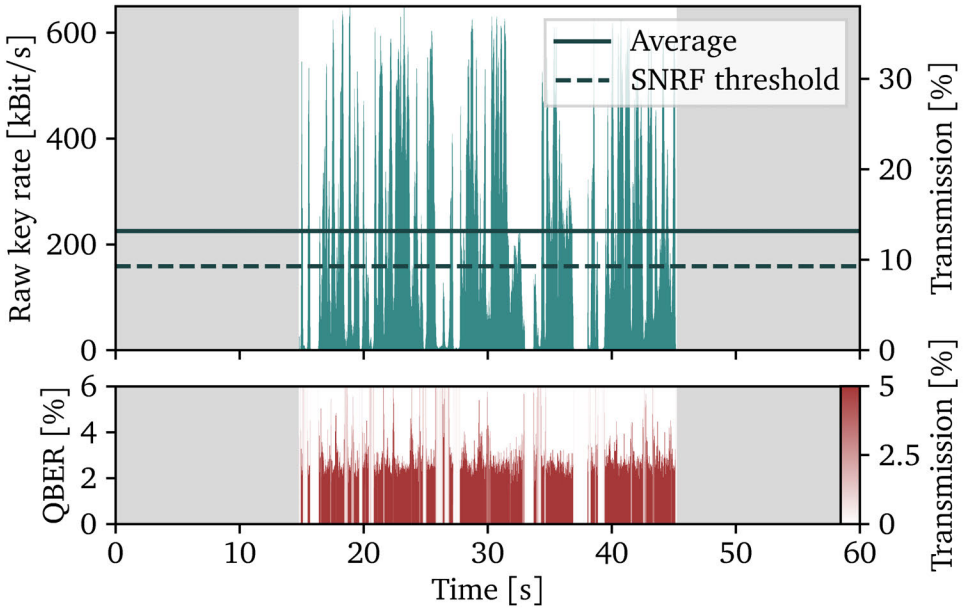


(k) High intensity key exchange XI.

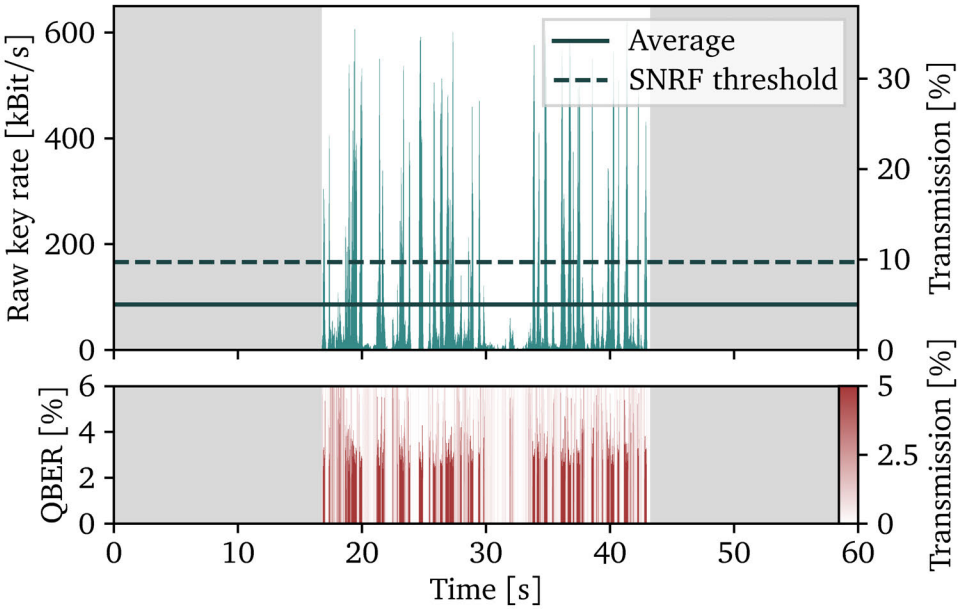


(l) Low intensity key exchange XII.

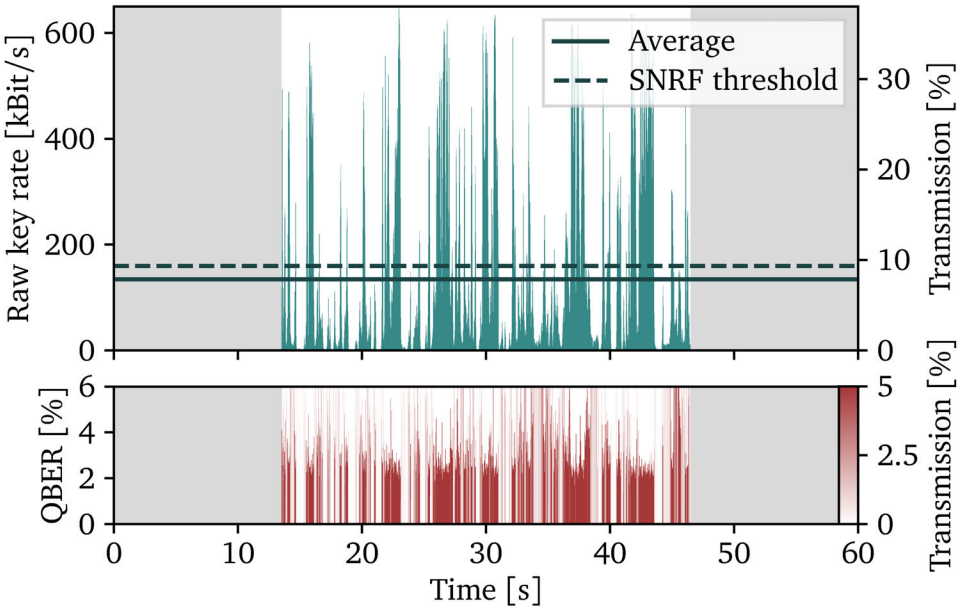
Figure B.1.: Raw key rate and QBER for all trials from the high intensity data set.



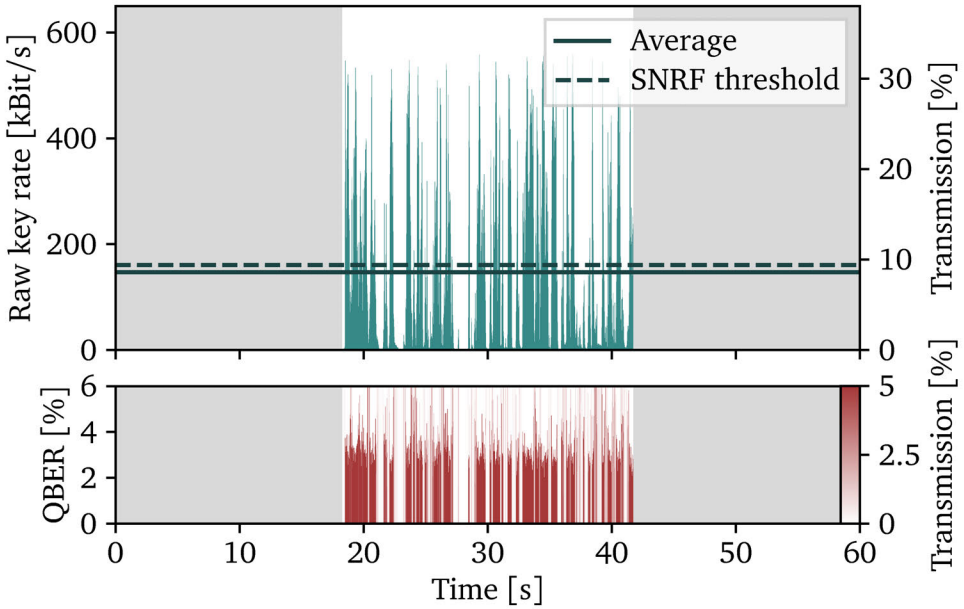
(a) Low intensity key exchange XIII.



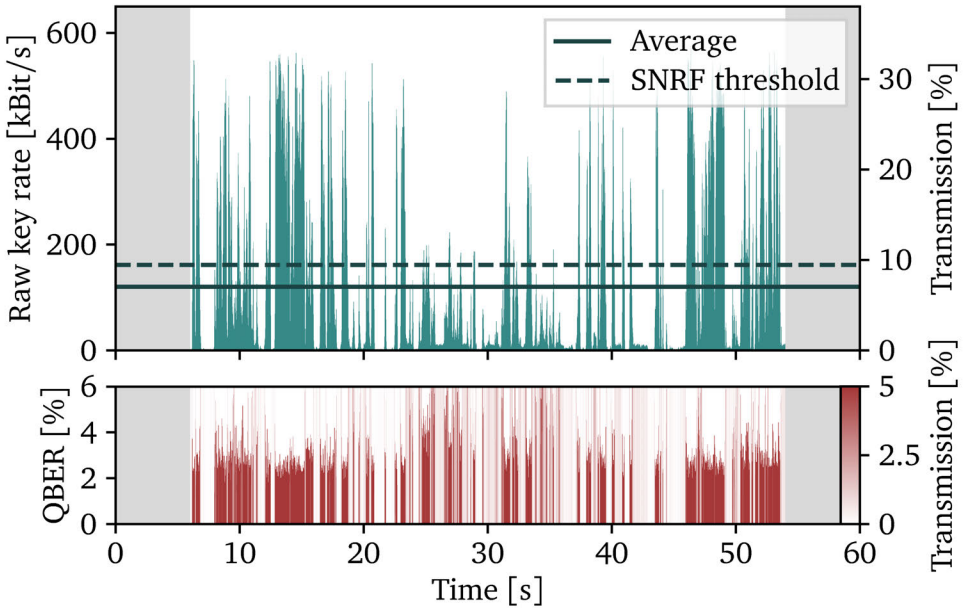
(b) Low intensity key exchange XIV.



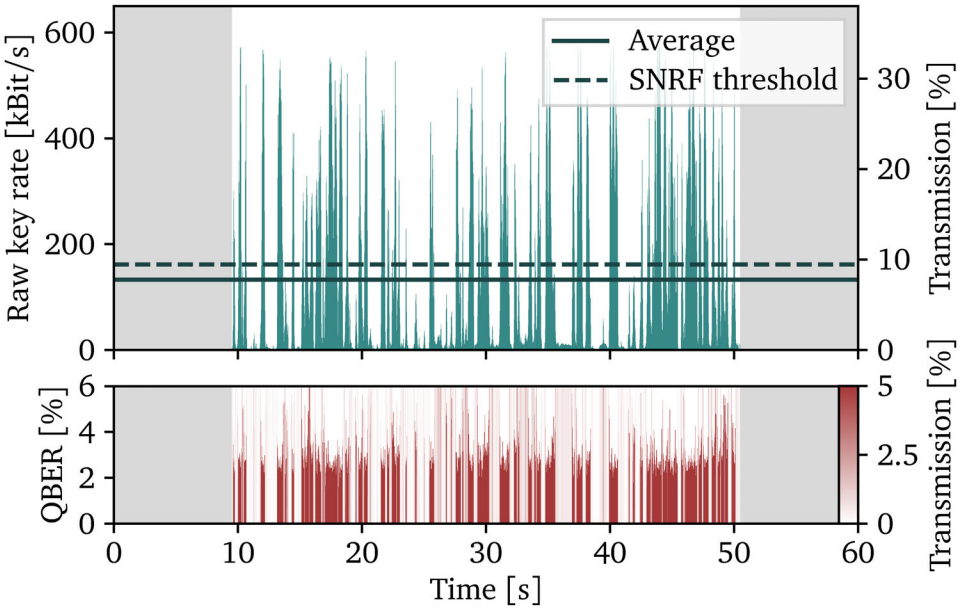
(c) Low intensity key exchange XV.



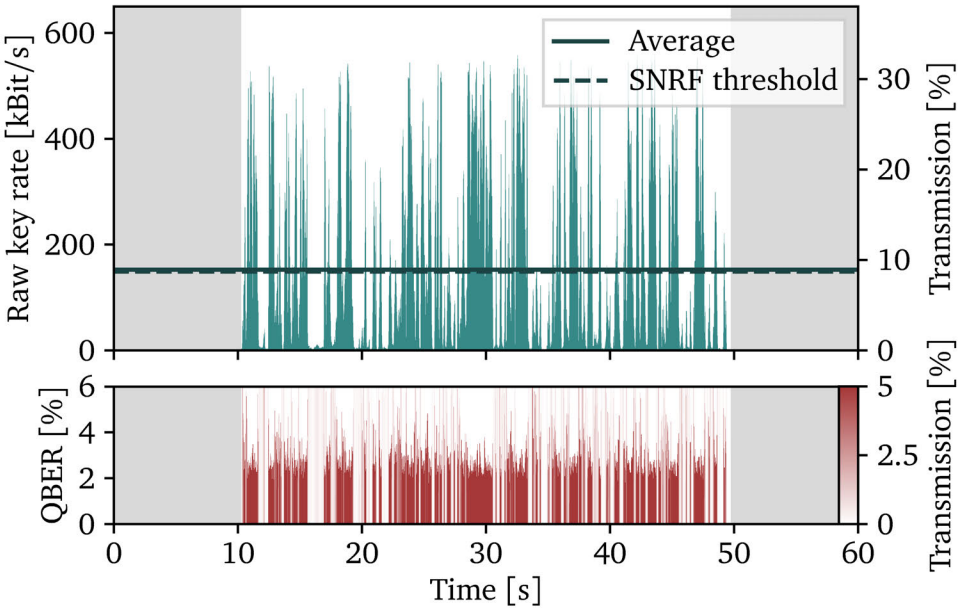
(d) Low intensity key exchange XVI.



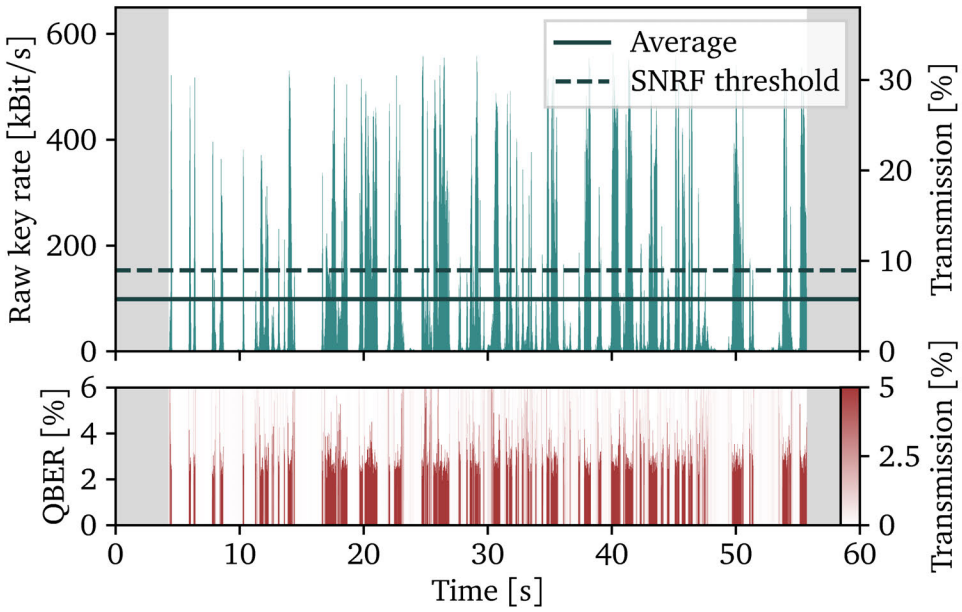
(e) Low intensity key exchange XVII.



(f) Low intensity key exchange XVIII.



(g) Low intensity key exchange XIX.



(h) Low intensity key exchange XX.

Figure B.2.: Raw key rate and QBER for all trials from the low intensity data set.

Bibliography

[1] Christopher Woods, editor. *Visible Language: Inventions of Writing in the Ancient Middle East and Beyond*. The Oriental Institute of the University of Chicago, 2010.

[2] Elizabeth L Eisenstein. *The printing press as an agent of change*, volume 1. Cambridge University Press, 1980.

[3] Charles H Bennet and Gilles Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proc. IEEE International Conf. on Computer, Systems and Signal Processing, New York, 1984*, volume 175, 1984.

[4] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[5] Dominic Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, May 2001.

[6] Hoi-Kwong Lo and Hoi Fung Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *science*, 283(5410):2050–2056, 1999.

[7] Charles H Bennett and Gilles Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM Sigact News*, 20(4):78–80, 1989.

[8] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, 117(19):190501, 2016.

[9] Rupert Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, Thomas Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature physics*, 3(7):481–486, 2007.

[10] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[11] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7(5):382–386, 2013.

[12] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, Liang Zhang, Qi Shen, Xiao-Fang Hu, Jin-Cai Wu, Shi-Ji Yang, Hao Jiang, Yan-Lin Tang, et al. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photonics*, 7(5):387–393, 2013.

[13] Jean-Philippe Bourgoin, Brendon L Higgins, Nikolay Gigov, Catherine Holloway, Christopher J Pugh, Sarah Kaiser, Miles Cranmer, and Thomas Jennewein. Free-space quantum key distribution to a moving receiver. *Optics express*, 23(26):33437–33447, 2015.

[14] Thomas Jennewein and Brendon Higgins. The quantum space race. *Physics World*, 26(03):52, 2013.

[15] Juan Yin, Yuan Cao, Shu-Bin Liu, Ge-Sheng Pan, Jin-Hong Wang, Tao Yang, Zhong-Ping Zhang, Fu-Min Yang, Yu-Ao Chen, Cheng-Zhi Peng, et al. Experimental quasi-single-photon transmission from satellite to earth. *Optics express*, 21(17):20032–20040, 2013.

[16] Tang Zhongkan, Rakhitha Chandrasekara, Yau Yong Sean, Cliff Cheng, Christoph Wildfeuer, and Alexander Ling. Near-space flight of a correlated photon system. *arXiv preprint arXiv:1404.3971*, 2014.

[17] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Physical review letters*, 115(4):040502, 2015.

[18] Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Luo Sha, Goh Cher Hiang, Daniel KL Oi, and Alexander Ling. Generation and analysis of correlated pairs of photons aboard a nanosatellite. *Physical Review Applied*, 5(5):054022, 2016.

[19] Gwenaelle Mélen. *Integrated Quantum Key Distribution Sender Unit for Hand-Held Platforms*. PhD thesis, Ludwig-Maximilians-Universität München, 2016.

[20] Tobias Vogl. Mobile free space quantum key distribution for short distance secure communication. Master's thesis, Ludwig-Maximilians-Universität München, 2016.

[21] Peter Freiwang. Towards hand-held quantum key distribution. Master's thesis, Ludwig-Maximilians-Universität München, 2017.

[22] Bruce Schneier. *Applied Cryptography (2nd Ed.): Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc., New York, NY, USA, 1995.

[23] Wade Trappe and Lawrence C. Washington. *Introduction to Cryptography with Coding Theory (2nd Edition)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2005.

[24] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.

[25] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[26] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8), April 1965.

[27] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. 26(5):1484–1509, October 1997.

[28] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[29] Masoud Mohseni, Peter Read, Hartmut Neven, Sergio Boixo, Vasil Denchev, Ryan Babbush, Austin Fowler, Vadim Smelyanskiy, and John Martinis. Commercialize quantum technologies in five years. *Nature*, 543(7644):171–174, March 2017.

[30] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.

[31] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[32] William K. Wooters and Wojciech H. Zurek. Quantum no-cloning theorem. *Nature*, 299:802, 1982.

[33] Dennis Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

[34] Howard Barnum, Carlton M Caves, Christopher A Fuchs, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15):2818, 1996.

[35] Vladimir Bužek and Mark Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844, 1996.

[36] Igor Aharonovich, Dirk Englund, and Milos Toth. Solid-state single-photon emitters. *Nature Photonics*, 10(10):631–641, 2016.

[37] Miloslav Dušek, Ondřej Haderka, and Martin Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Optics communications*, 169(1):103–108, 1999.

[38] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330, 2000.

[39] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[40] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[41] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1):012326, 2005.

[42] Jim W Harrington, J Mark Ettinger, Richard J Hughes, and Jane E Nordholt. Enhancing practical security of quantum key distribution with a few decoy states. *arXiv preprint quant-ph/0503002*, 2005.

[43] Tim Höhn. Bachelor's thesis, Ludwig-Maximilians-Universität München, 2017.

[44] Daniel Gottesman, H-K Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 136. IEEE, 2004.

[45] Claude E Shannon and Warren Weaver. The mathematical theory of information. 1949.

[46] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 410–423. Springer, 1993.

[47] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A*, 67:052303, May 2003.

[48] Robert Gallager. Low-density parity-check codes. *IRE Transactions on information theory*, 8(1):21–28, 1962.

[49] Charles H Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM journal on Computing*, 17(2):210–229, 1988.

[50] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[51] Sebastian Nauerth, Martin Fürst, Tobias Schmitt-Manderbach, Henning Weier, and Harald Weinfurter. Information leakage via side channels in freespace bb84 quantum cryptography. *New Journal of Physics*, 11(6):065001, 2009.

[52] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 1991.

[53] Gwenaelle Vest, Markus Rau, Lukas Fuchs, Giacomo Corrielli, Henning Weier, Sebastian Nauerth, Andrea Crespi, Roberto Osellame, and Harald Weinfurter. Design and evaluation of a handheld quantum key distribution sender module. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):131–137, 2015.

[54] Rainer Michalzik. *VCSELs: fundamentals, technology and applications of vertical-cavity surface-emitting lasers*, volume 166. Springer, 2012.

[55] Gwenaelle Mélen, Wenjamin Rosenfeld, and Harald Weinfurter. Impact of the slit geometry on the performance of wire-grid polarisers. *Optics express*, 23(25):32171–32178, 2015.

[56] Giuseppe Della Valle, Roberto Osellame, and Paolo Laporta. Micromachining of photonic devices by femtosecond laser pulses. *Journal of Optics A: Pure and Applied Optics*, 11(1):013001, 2009.

[57] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3:634, 2012.

[58] Seong-Seok Yang, Jeong-Kwon Son, Young-Kyu Hong, Yong-Ho Song, Ho-Jin Jang, Seong-jun Bae, Yong-Ho Lee, Gye-Mo Yang, Hyun-Sung Ko, and Gun-Yong Sung. Wavelength tuning of vertical-cavity surface-emitting lasers by an

internal device heater. *IEEE Photonics Technology Letters*, 20(20):1679–1681, 2008.

[59] HA Davani, Benjamin Kögel, P Debernardi, C Grasse, C Gierl, K Zogal, Åsa Haglund, J Gustavsson, Petter Westbergh, T Gründl, et al. Polarization investigation of a tunable high-speed short-wavelength bulk-micromachined mems-vcsel. In *SPIE OPTO*, pages 82760T–82760T. International Society for Optics and Photonics, 2012.

[60] David J Wales and Jonathan PK Doye. Global optimization by basin-hopping and the lowest energy structures of lennard-jones clusters containing up to 110 atoms. *The Journal of Physical Chemistry A*, 101(28):5111–5116, 1997.

[61] Stephen Wright and Jorge Nocedal. Numerical optimization. *Springer Science*, page 136, 2006.

[62] Eric Jones, Travis Oliphant, Pearu Peterson, et al. SciPy: Open source scientific tools for Python, 2001–. Version 0.17.1.

[63] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006.

[64] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A*, 78(4):042333, 2008.

[65] Markus Rau, Tobias Vogl, Giacomo Corrielli, Gwenaelle Vest, Lukas Fuchs, Sebastian Nauerth, and Harald Weinfurter. Spatial mode side channels in free-space qkd implementations. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):187–191, 2015.

[66] Tobias Vogl. Security of a free space qkd-receiver module with angle-dependent detection efficiency mismatch. Bachelor's thesis, Ludwig-Maximilians-Universität München, 2014.

[67] John Marshall and E Geoffrey Walsh. Physiological tremor. *Journal of Neurology, Neurosurgery & Psychiatry*, 19(4):260–267, 1956.

[68] Tobias Schmitt-Manderbach. *Long distance free-space quantum key distribution*. PhD thesis, Ludwig-Maximilians-Universität München, 2007.

[69] C Erven, B Heim, E Meyer-Scott, JP Bourgoin, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, 2012.

[70] John A Nelder and Roger Mead. A simplex method for function minimization. *The computer journal*, 7(4):308–313, 1965.

[71] Margaret H Wright. Direct search methods: Once scorned, now respectable. *Pitman Research Notes in Mathematics Series*, pages 191–208, 1996.

[72] C Gobby, ZL Yuan, and AJ Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84(19):3762–3764, 2004.

[73] Stefan van der Walt, S. Chris Colbert, and Gael Varoquaux. The numpy array: A structure for efficient numerical computation. *Computing in Science and Engg.*, 13(2):22–30, March 2011.

[74] Christian Eckel. Bachelor's thesis, Ludwig-Maximilians-Universität München, 2017.

Acknowledgements

Zum Schluss dieser Arbeit möchte ich all denen danken, die zu ihrem Gelingen beigetragen haben:

- Prof. Dr. Harald Weinfurter, der mir die Gelegenheit gab, in seiner Arbeitsgruppe an einem spannenden Projekt mitzuarbeiten.
- Meinem Kollegen Peter Freiwang, mit dem ich das letzte Jahr Labor, Experiment, Rückschläge und Erfolgserlebnisse teilen durfte.
- Dr. Wenjamin Rosenfeld für seine ständige Hilfsbereitschaft bei allen aufkommenden Problemen und die interessanten Nach-Mittagessens-Diskussionen.
- Dr. Gwenaelle Mélen, die trotz neuer Verpflichtungen immer noch Zeit für ihr altes Projekt gefunden hat, wenn wir nicht mehr weiter wussten.
- Dem Rest der Weinfurter-Gruppe für die Schaffung einer entspannten Atmosphäre, insbesondere meinem Schreibtischnachbarn Martin Zeitlmair für die gut gemeinten, aber zwecklosen Versuche, mich zum Kaffeetrinken zu verführen.
- Meinen Eltern Achim und Renate sowie meinen beiden Schwestern Clara und Karoline.
- Und zuletzt Alice und Bob, die trotz aller Schwierigkeiten bis zum Ende durchgehalten haben.

Erklärung

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

München, den 17. Mai 2017

Jannik Luhn