Palacký University Olomouc
Faculty of Science

Department of Optics

Quantum key distribution using classical and non-classical light

Master's Thesis

Jiří Fadrný

Palacký University Olomouc
Faculty of Science

Department of Optics

Quantum key distribution using classical and non-classical light

Master's Thesis

Author:	Bc. Jiří Fadrný
Study programme:	N1701 Physics
Field of study:	Optics and Optoelectronics
Form of study:	Full-time
Supervisor:	RNDr. Miroslav Ježek, Ph.D.
Co-supervisor:	Mgr. Martina Nováková, Ph.D.

Thesis submitted on: .....

Univerzita Palackého
Přírodovědecká fakulta

Katedra optiky

Sdílení kvantového klíče s klasickými a kvantovými stavy světla

Diplomová práce

Autor:	Bc. Jiří Fadrný
Studijní program:	N1701 Fyzika
Studijní obor:	Optika a optoelektronika
Forma studia:	Prezenční
Vedoucí:	RNDr. Miroslav Ježek, Ph.D.
Konzultant:	Mgr. Martina Nováková, Ph.D.

Práce odevzdána dne: .....

Abstract

The goal of the Thesis is to develop a quantum cryptographic system based on the weak coherent states with the decoy-state technique. The intensity of the decoy states differs from the intensity of signal states, which allows secure key distribution with imperfect light sources over the long attenuating channel and prevents the photon-number-splitting attack. An experimental implementation of the polarization encoded decoy-state BB84 protocol has been designed. The states prepared by Alice are generated with vertical-cavity surface-emitting lasers (VCSELs), which are driven with a custom-made pulse box based on the microcontroller. The pulse box generates the signal and the decoy states at the maximal repetition rate around 19 MHz. I have also developed the software toolbox for the data analysis and estimation of the minimal secure key rate. The maximal channel attenuation which allows secure communication was estimated over 27 dB, which equals the distance in the standard telecommunication optical fiber of around 11.3 km at the wavelength of 850 nm and almost 130 km at the wavelength of 1550 nm. Moreover, I have studied the device-independent modification of E91 quantum cryptographic protocol, which provides more reliable security than prepare-and-measure QKD as it allows us to relax some assumptions that are usually made about the measurement devices of Alice and Bob. Two measured density matrices that describe the entangled Bell's states $\frac{1}{\sqrt{2}}(|H_1, H_2\rangle \pm |V_1, V_2\rangle)$ generated by the source of entangled photon pairs based on the spontaneous parametric down-conversion have been analyzed. The first high-quality entangled state would be suitable for QKD and can provide the secure key rate at least 0.92 bits/pair. However, the poor quality of the second state does not allow secure QKD.

Keywords

`Quantum key distribution, prepare-and-measure, BB84, decoy states, quantum entanglement`

Acknowledgments

I would like to express deep gratitude to RNDr. Miroslav Ježek, Ph.D. for the knowledge he passed on me, his help, and guidance through my experimental work. I would also like to acknowledge my co-supervisor Mgr. Martina Nováková, Ph.D., whose ideas were always inspiring. I am very grateful for the assistance with the pulse box proposal and the manufacture of the electronic circuits provided by Mgr. Michal Dudka. Moreover, I wish to thank Mgr. Radim Hošák for sharing his knowledge and experience with entangled-based QKD and for providing the measured density matrices. I am also grateful to Mgr. Ivo Straka, Ph.D. for sharing his laptop with me in times of need. Last but not least, I appreciate all the support and love given by my family and friends, especially I wish to thank for the love and encouragement given by my beloved girlfriend Martina.

Jiří Fadrný

Declaration

I hereby declare that I have written this Master's Thesis and performed all the presented research and experimental tasks by myself, while being supervised by RNDr. Miroslav Ježek, Ph.D. I also state that every resource used is properly cited. I agree with the Thesis being used for teaching purposes and being made available at the website of the Palacky University.

Signed in Olomouc on ....

Jiří Fadrný

Contents

Chapter 1

Introduction

Quantum cryptography (QC) is a promising application of quantum optics and information theory which offers secure communication between the two remote parties. There is a classical symmetrical cipher called the Vernam cipher that was proven absolutely secure. However, it incorporates a secret key a priori known only to the two participants of the communication (traditionally known as Alice and Bob), which makes the cipher unpractical in conventional cryptosystems. However, QC offers a way to distribute such a secret sequence of bits (key) between them and provides the ability to reveal eavesdropping [1]. The first quantum-cryptographic protocol was introduced by C. Bennett and G. Brassard in 1984 [2].

The general process of quantum key distribution (QKD) consists of quantum communication part over a physical channel and classical post-processing. During quantum communication, Alice sends bits as quantum states according to a specific QKD protocol. Bob measures the incoming states and obtains a string of bits correlated to Alice's one. Classical post-processing via an authenticated public channel is essential to extract the secret key from the raw data. First, sifting is applied to obtain maximally correlated data strings. Although, Bob's and Alice's bit sequences are correlated only up to a certain point due to decoherence in the channel or eavesdropper's interaction. The errors between their strings are repaired by the information reconciliation protocol. The last step of post-processing is so-called privacy amplification which decreases knowledge of the key which an eavesdropper (commonly known as Eve) might have to an arbitrarily low value.

There are two general approaches to QKD. It can be performed in discrete variables (DV-QKD), which utilize the particle-like behavior of light. This approach is followed in this thesis. The key is distributed with quantum bits (qubits), which are, in general, vectors in the two-dimensional Hilbert space. The qubits are carried by photons and are transmitted via the quantum channel. There is just one single photon in every single pulse in the ideal DV-QKD protocol. Such a photon carries exactly one bit of information, while all the potential losses in the channel lead to a decrease in the transmission rate of the key. However, perfect single-photon sources are not yet available, hence they are being replaced with different emitters. DV-QKD protocols utilize single photons

avalanche diodes (SPADs) as detectors, which have their limitation in repetition frequency, efficiency, and excess noise due to dark counts and dead time of the detectors. Nevertheless, even with imperfect devices, which are often utilized, the DV-QKD is in general easy to implement.

Before going into detail, it is worth mentioning the second option which is the continuous variables quantum key distribution (CV-QKD). CV-QKD protocols operate in infinite-dimensional Hilbert space and usually utilize so-called Gaussians states to carry the information. The classical information is encoded into the phase space of the x and p quadratures of the light. The main advantage over DV-QKD is that such encryption allows us to transmit more than one classical bit of information in a single pulse. CV-QKD protocols utilize homodyne detectors, which work also as efficient background filters as the phase and the frequency of a local oscillator is locked to the signal. That makes it applicable in free-space QKD (Earth to satellite) even during the day, which is extremely difficult with DV-QKD. Homodyne detectors require phase and amplitude control of the local oscillator but provide a high repetition rate. However, these protocols are in general sensitive to losses and noise in the channel. A certain level of attenuation in the channel can break the security of some basic CV-QKD protocols while attenuation only lowers the key rate in DV-QKD.

Both approaches face different challenges but both can provide secure key distribution. As mentioned before, this thesis is focused on DV-QKD. Therefore, from now on, I will discuss the DV-QKD only and I will refer to it just as QKD.

Despite its promise, it is not trivial to ensure unconditional security for real implementations of QKD. Experimental QKD faces many imperfections of real-life components. The absence of a perfect single-photon source or existence of detection loss can break the security of some QKD protocols [3, 4]. Another difficulty is to distribute the secret key over long distances. The distance on which it is still possible to distribute the secret key is limited by the attenuation in the quantum channel and the quantum bit error rate (QBER) of the transmission. Moreover, long-distance QKD may be also insecure because of the photon-number splitting attack (PNS, will be discussed later). Thus, if these characteristics of real-life devices are not taken into account, the protocol security is not assured. Actually, the most severe attacks to the QKD systems often profit form features that are not incorporated in the security proofs. They are called side-channel attacks and they usually employ classical tools to gain any information from the imperfect device rather than some quantum-mechanics based attacks.

QKD was designed [5]. The security proofs of DI QKD protocols do not make any assumptions on the quantum devices used by Alice and Bob as they may be noisy, its parameters and measurement directions may vary in time or as mentioned before it may have some uncontrolled side channels. To introduce the idea of DI QKD in a nutshell, Alice and Bob share the entangled pair of photons (it should be noted that DI QKD does not have to necessarily involve entanglement). Each of them possesses a quantum measurement device which we can imagine as a black box addressed with binary inputs (that may refer to

their choices of measurement basis) and which provides binary outputs. Note that no assumptions on how the measurement is done are not made. Alice and Bob generate random input for their quantum device and according to it, each of them performs measurements on halves of the entangled photon pairs. The input-output behavior of their devices is then tested and if they behave honestly, Alice's and Bob's data should be correlated in a non-local way which may be verified by a violation of Bell-type inequalities as Clauser, Horne, Shimony, and Holt (CHSH) test. If the correlations are bellow classical limit no secret key can be distilled [6]. It should be stressed that even local correlations may be misinterpreted as non-local ones if the detector efficiencies are not high enough which is sort of a drawback in Bell experiments.

Even though DI QKD can provide reliable security, it is not easy to distribute the entanglement over long distances. Additionally, with low detectors efficiencies, no secret key might be distillable in the end. Thus, a more general approach of measurement device-independent (MDI) QKD was designed. Its main idea is that Alice and Bob generate states from one of two bases and send it to the receiver party, often called Charlie, who performs the Bell's measurement on the incoming states. Charlie may be entirely under the control of Eve, but it has to publicly announce the output of the Bell's measurement. In this case, no assumption on the employed detectors used is made. Moreover, the entangled pairs are no longer required and Alice and Bob can utilize the decoy-state method to prevent PNS attack. The key is produced if Alice and Bob use the same basis. Charlie knows only the results of the Bell's measurement but not the encoded bit.

Current research pushes the limits of experimental QKD to achieve reasonable secure key rates over long distances as well as analyze the security of the experimental implementation under realistic conditions and with only finite-size data samples transmitted [7]. The basic scheme of BB84 with decoy states is still a powerful tool to accomplish that goal [8, 9]. Even though the original BB84 is being recently slightly simplified and optimized to obtain the best performance. Such a scheme allowing secure QKD over the maximal distance of 421 km was presented in 2018 in [10] utilizing ultra low-loss optical fibers and superconducting detectors. Almost the same distance was achieved earlier in 2016 with the MDI scheme in [11]. The secret key was distributed over 311 km with standard optical fiber and over 404 km with ultra low-loss optical fiber.

The attenuation in the optical fibers will not allow quantum communication for much longer distances. Therefore, QKD is also being tested in free space. The secret key was distributed between the Canary islands [12, 13]. Two faraway places on the Earth can be also connected with the quantum channel utilizing a satellite. At first, a satellite was operated only as a reflector reflecting the photon states back to the Earth [14]. Most of the satellites operate in the low-Earth-orbit (LEO), which is up to 2000 km above the Earth's surface. Currently, the satellites are equipped with photon sources capable of generation of classical and non-classical states as well as performing measurements. Among others, the Chinese Micius satellite performs QKD from the LEO to Earth. It can establish a secret key of kHz rate utilizing the decoy-state method between itself and several ground stations and it can then act as a Charlie so that

the remote laboratories may generate the key with each other. This way, the QKD was achieved between the places separated on Earth by 7600 km [15]. The longest distance of quantum communication utilizing the CV states was recently performed over 38600 km between the Alphasat satellite in the geostationary orbit and the ground laboratory [16]. Even though most of the free-space QKD takes place during the night, also the communication in the daylight is being studied. The satellite-based QKD accompanied with the fiber-based quantum cryptosystems is a promising way to achieve the global QC network.

The aim of my work is to develop a QKD system based on the weak coherent states with the decoy-state technique, which represents the current state-of-the-art in secure communication due to its relatively easy implementation. For that purpose, I employ the BB84 protocol with the polarization encoding. I have dealt with all the experimental challenges that accompany the construction of any QKD system based on the weak coherent states such as the choice of the light source and developing the electronics circuits to control and modulate the optical signals. It also includes ensuring the indistinguishability of the states in their unused degrees of freedom. Additionally, I have built the detection system, dealt with its synchronization with the clock signal, and data evaluation using custom-made software. I have analyzed the performance of the developed QKD system and estimated the minimal secure key rate that could be achieved after the information reconciliation and the privacy amplification.
In the second part of the thesis, I have also analyzed the possibility of QKD with the source of entangled photon pairs. I emulated high and low-quality entangled photon source by using different coincidence window widths, the obtained states were characterized by density matrices. Based on the modification of the Ekert's E91 protocol I have estimated the achievable secure key rate such sources can provide.

The structure of the thesis is as follows. In chapter 2, I will first introduce the theory of the prepare-and-measure QKD with weak coherent states. Then in section 2.2, I will describe my implementation of the BB84 protocol. Later in 2.3, I will discuss the issues of selecting appropriate light sources. In section 2.4, I will go through the experimental setup and finally, in section 2.5 I will explain how the experiment is controlled and synchronized. Chapter 3 covers the classical postprocessing of the raw key, which includes the information reconciliation and privacy amplification. I will also go through the theory that is needed to estimate the secure key rate.
In chapter 4, I will discuss the experimental methods that precede the actual quantum state transmission. Then I will describe the process of data acquisition, analysis, and at the end also the results of the test state transmission.
Chapter 5 deals with the QKD based on entangled photon pairs. I will introduce an entanglement-based protocol and I will estimate the secure key rate of the provided sample density matrices. Finally, I will conclude my work and discuss further plans and possible improvements.

Chapter 2

Weak coherent-state based QKD

2.1 Prepare-and-measure DV-QKD

Here I would like to describe the idea of DV-QKD using the well-known BB84 proposed by C. H. Bennett and G. Brassard in 1984 [2] as an example, which is the quintessential example of prepare-and-measure DV-QKD protocol. A qubit is represented as one of the four states in two non-orthogonal bases. Let us denote $\mathbb{Z}$ basis as

$$\begin{aligned} |+z\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |-z\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned} \tag{2.1}$$

and $\mathbb{X}$ basis as

$$\begin{aligned} |+x\rangle &= \frac{1}{\sqrt{2}}(|+z\rangle + |-z\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ |-x\rangle &= \frac{1}{\sqrt{2}}(|+z\rangle - |-z\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \end{aligned} \tag{2.2}$$

Alice randomly prepares one of the states and sends it to Bob over a quantum channel. Bob for each instance randomly and independently on Alice chooses his measurement basis. If the quantum channel is not affected by Eve, Bob will get correlated data for the instances in which he has chosen the right basis as

$$\begin{aligned} \langle \pm x| \pm x\rangle &= 1, \\ \langle \pm z| \pm z\rangle &= 1. \end{aligned} \tag{2.3}$$

In other cases, Bob's outcome will be random because of the

$$\begin{aligned} \langle \pm x| \pm z\rangle &= \frac{1}{\sqrt{2}}, \\ \langle \pm z| \pm x\rangle &= \frac{1}{\sqrt{2}}. \end{aligned} \tag{2.4}$$

The security of the BB84 is based on the fact that the presence of Eve would increase the quantum bit error rate of Alice's and Bob's communication QBER $e = \frac{n}{N_d}$, where n stands for the number of bits in which Alice's and Bob's key differs. N_d is the number of bits detected by Bob. The protocol is designed to resist the most basic individual attack, the intercept-resend attack. Because Alice chooses the bases randomly, Eve does not know in which basis she should measure. Her best choice is to guess and switch the bases randomly too. Accordingly to her measurement Eve generates a new state and sends it to Bob. However, her information gain with this type of attack will only be 0.5 as she will guess the correct basis only in half of the cases on average. Moreover, the non-orthogonality of the bases will provide Bob with random results in the instances in which Eve's basis has not matched with Alice's one. Thus, Eve's interference induces noise to quantum communication and reveals her presence. Apart from the non-orthogonality, the security of QKD relies on the so-called no-cloning theorem which means that Eve cannot make a perfect copy of the transmitted state as a consequence of the linearity of quantum mechanics [17].

It is worth mentioning other possible prepare-an-measure protocols such as two-state and six-state protocols. The BB84 protocol can be extended by adding one more basis to reach the six-state protocol. The bits are being encoded to three non-orthogonal bases which makes it even more difficult for Eve to correctly guess the measurement basis. Her increased uncertainty leads to more induced noise while she measures in the wrong basis. It can be shown that in general, the six-state protocol allows secure QKD for higher values of QBER in comparison with standard four-state BB84.

In 1992, C. H. Bennett proposed his so-called B92 protocol which utilizes only two non-orthogonal states as the most minimalistic system capable of QKD [18]. He pointed out that two non-orthogonal states are sufficient for QKD. However, a positive operator-valued measure (POVM) can be performed to unambiguously discriminate non-orthogonal states in most of the instances, which when executed by Eve can threaten the security of B92. Even though, it has been shown that the B92 is secure [19] and it is being implemented in some cryptosystems such as [20] or its entanglement-based version in [21]. These implementations benefit from its easy implementation, yet B92 does not perform as good as the BB84 as it is more noise dependent in general. It should be noted that noise is always present in realistic systems due to the imperfection of real-life components even if Eve does not interfere. Therefore, for the sake of security one must assume that all the noise is generated by Eve as we are not able to distinguish its source.

As mentioned earlier single-photon source is more demanding for experimental implementation than attenuated laser, particularly when deployed in a common telecommunication network. However, the current technology does not provide that. Therefore attenuated laser is being implemented in real-life QKD instead. Such a laser provides weak coherent states which have the Poisson distribution of photon number of each pulse. The density matrix of a coherent state is given by

$$\rho_C = \sum_{n=0}^{\infty} \frac{\mu^n}{n!} e^{-\mu} |n\rangle\langle n|, \tag{2.5}$$

where μ stands for intensity and n stands for photon number. This imperfection in the practical implementations of QKD protocols makes them vulnerable to certain types of attacks. Namely, the photon number splitting (PNS) attack, which exploits the fact that imperfect photon sources emit in some pulses more than one photon. Let us assume that Eve operates with unlimited technology. Then she can proceed for example as follows. Eve nondestructively measures the number of photons in a pulse that is being transmitted from Alice to Bob. If there is only one photon in the pulse, Eve will block it. However, she will split the multiphoton pulses, keep one photon in her quantum memory, and send the rest of the pulse to Bob via an ideal noiseless channel. Therefore she can compensate for the channel losses she induces by the blocking of single photons. After listening to the classical public communication between Alice and Bob, Eve will learn in which bases she has to measure the photons to obtain the whole secure key. This attack is extremely dangerous as there is no error increase caused by Eve (so-called zero-error security break).
It should be noted that the zero-error security break can, in general, occur in long and noisy channels. QKD with imperfect sources may be secure in shorter scales. Let us consider a photon source that emits a vacuum state with a probability of 90%, single-photon state with a probability of 9%, and multiphoton state with a 1% probability. Let us also say that the attenuation of the channel is 99%. In this situation, Eve can block all the single photons and deliver all the split multiphoton pulses to Bob. In this scenario, she will obtain the whole secret key with the photon number splitting attack. However, if the channel is shortened or noise is decreased (channel attenuation reduced to 95% for instance), she can no longer block all the single photons because that would affect the channel transmittance and reveal her presence.

We see, that realistic prepare-and-measure implementation of DV-QKD such as BB84 protocol with weak laser pulses is exposed to the dangerous PNS attack. There are some ways to prevent it. One can reduce Eve's ability to gain information with the PNS attack by different coding. In 2004 Scarani, Acin, Ribordy, and Gisin proposed the SARG04 protocol for this purpose [22]. It utilizes the very same technology as BB84, four states ($|\pm x\rangle$ and $|\pm z\rangle$) in two non-orthogonal bases are incorporated, only the bits are encoded into the bases rather than into the states. The main difference though is in the shifting phase in the classical communication part of the protocol. Instead of the basis used for encoding Alice announces a pair of states $\mathbb{A}_{\omega,\omega'}$ for each run of the protocol, where ω stands for a state from $\mathbb{X}$ basis and ω' for the one from $\mathbb{Z}$. One of the states was actually sent by Alice and the other is chosen randomly. For example one can read $\mathbb{A}_{+,-}$ as Alice sends either $|+x\rangle$ or $|-z\rangle$. As a successful run one can assume only such in which Bob's measurement does not match with Alice's announced pair of state. For clarity let us suppose that Alice has sent $|-z\rangle$ state and she announces $\mathbb{A}_{+,-}$. Then the bit was successfully transmitted only if Bob measures in $\mathbb{X}$ basis and obtains result " $-$ " which stands for $|-x\rangle$ state. All the other possible outcomes would match with Alice's announcement,

thus has to be discarded. In other words, Bob can be sure what state Alice has sent only for the described result of his measurement. Bob can read it as follows; Right, my result differs from the states announced by Alice, so I must have measured in the wrong basis which means Alice has actually sent $|-z\rangle$ state.

Alice sends		Bob can detect	
State	$\mathbb{A}_{\omega,\omega'}$	$\mathbb{X}$	$\mathbb{Z}$
$\|+x\rangle$	$\mathbb{A}_{+,-}$	" $+$ "	" $\oplus$ " or " $-$ "
$\|+x\rangle$	$\mathbb{A}_{+,+}$	" $+$ "	" $+$ " or " $\ominus$ "
$\|-x\rangle$	$\mathbb{A}_{-,+}$	" $-$ "	" $+$ " or " $\ominus$ "
$\|-x\rangle$	$\mathbb{A}_{-,-}$	" $-$ "	" $\oplus$ " or " $-$ "

Table 2.1: Possible codewords Alice announces when transmitting states in $\mathbb{X}$ basis and Bob's possible measurement outcomes.

For clarity, let us take a look at all the possible codewords Alice can announce during the public discussion with Bob when she transmits a state from $\mathbb{X}$ basis. As shown in table 2.1 there are two options for each state. The two last columns refer to states that Bob detects for his choice of basis. The instances, in which his result is conclusive, are circled.

In general SARG04 protocol increases Eve's uncertainty about the state that is being transmitted which provides higher security of the protocol in comparison with BB84. However, even if Bob chooses the correct basis, he obtains a bit only in half of the instance. The higher security of the SARG04 is obtained at the cost of a lower secret key rate.

Another strategy to prevent PNS attack is to use a so-called decoy-state protocol that utilizes additional photon sources on Alice's side. These decoy sources are indistinguishable from the signal ones in all the degrees of freedom except for the expected photon number in a pulse. The first proposal of this protocol by Whang [23] considers decoy-state sources with a higher intensity than the signal one. Signal pulses are randomly exchanged for the decoy pulses which are more likely to consist of multiple photons. If Eve blocked all the single-photon pulses (mostly from the signal source), the loss of the decoy states would be much smaller in comparison with the signal states which Alice and Bob can expose during the public communication while they estimate the parameters of the channel. Therefore, Alice and Bob only need to monitor the transmittance of both sources and reveal the PNS attack this way.

However later decoy-state implementations utilize strong signal state and two decoy states rather than following Whang original proposal as shown in [24]. The decoy states are vacuum one, which is used to estimate dark counts of the detectors, and the weak coherent decoy-states are applied to reveal the PNS attack. The expected photon number of the signal state is typically higher than the one of the weak decoy-state as it offers a higher key generation rate. Obviously, Eve cannot distinguish which pulses are decoy and which are signal, she can no longer efficiently perform PNS attack while Alice and Bob only

have to watch over the transmittance of the quantum channel. The decoy-state scheme significantly prolongs the distance over which QKD can be executed.

We have seen that one can make the protocol more robust by inducing additional uncertainty in the public communication part of the protocol. Alternatively, the PNS attack can be prevented by adding more states to the protocol and then monitor the behavior of the transmitted states at various levels of optical intensity, which is an approach followed in this thesis.

2.2 BB84 protocol implementation

In this thesis, we adopt the basic and well known BB84 protocol with its original polarization encoding. Let us implement $\mathbb{Z}$ basis as horizontal and vertical polarizations

$$\begin{aligned} |+z\rangle &= |H\rangle \\ |-z\rangle &= |V\rangle \end{aligned} \tag{2.6}$$

and $\mathbb{X}$ basis as diagonal and antidiagonal polarizations

$$\begin{aligned} |+x\rangle &= |D\rangle \\ |-x\rangle &= |A\rangle. \end{aligned} \tag{2.7}$$

Let us now go through our implementation of the decoy-state assisted BB84 protocol proposal in detail. For each pulse, Alice has to determine whether she sends a decoy or a signal state. One way to do so is by generating three bits with her true random number generator as visualized in Fig. 2.1.

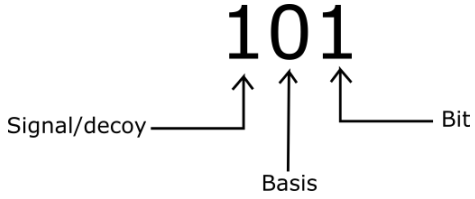

Figure 2.1: Three random bits determine Alice's state. She generates either decoy or signal state according to the first bit, basis choice is determined by the second one, and the last bit represents the classical bit that is being transmitted.

The scheme of the protocol is shown in table 2.2. Alice generates a 3-bit long random number for each pulse as illustrated by line 1a. According to it, she generates polarization state from the set $\{\mathrm{H}, \mathrm{V}, \mathrm{D}, \mathrm{A}\}$ with appropriate intensity as can be seen in lines 1b and 1c (S and D stand for signal and decoy state, respectively). At the same time, Bob randomly chooses his measurement basis only (line 2). However, his choices have to be independent of Alice's ones. If Bob chooses the same basis as Alice for the particular pulse he can detect the correct result. Such instances are marked with *yes* in line 3. This covers the whole quantum communication part of the protocol. The rest of the QKD

process continues via an authenticated classical public channel.

The rest of the QKD process continues via an authenticated classical public channel. Let us follow the direct reconciliation, i.e. Bob will post-process his data to match Alice's key. First, Bob publicly announces in which basis he measured, for each transmitted photon. Alice tells him in which instances he chooses correctly and whether she transmits a signal or a decoy state. Then they keep only the bits corresponding to these events and discard the rest. This process is called sifting and the sifted key Alice and Bob obtain is illustrated in line 4a. The line 4b represents transmitted decoy states, which are all revealed to check the transmittance and QBER of the decoy states.
In the next step, Alice and Bob have to estimate the transmittance and QBER of the signal states. Thus, they agree on a sub-set of the sifted key (illustrated as a mask applied to the sifted key in line 5a) and reveal it. If the bit value of Alice and Bob matches, the instance is marked with *yes* (line 5b). Last line 6 then represents the final raw key, which has to go through the information reconciliation and privacy amplification.

1a	101	100	011	101	110	100	110	011	010	100	001	111	110	001	110	100	011
1b	$\|A\rangle$	$\|D\rangle$	$\|V\rangle$	$\|A\rangle$	$\|H\rangle$	$\|D\rangle$	$\|H\rangle$	$\|V\rangle$	$\|H\rangle$	$\|D\rangle$	$\|A\rangle$	$\|V\rangle$	$\|H\rangle$	$\|A\rangle$	$\|H\rangle$	$\|D\rangle$	$\|V\rangle$
1c	S	S	D	S	S	S	S	D	D	S	D	S	S	D	S	S	D
2	$\mathbb{X}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{X}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{X}$	$\mathbb{Z}$	$\mathbb{X}$	$\mathbb{Z}$	$\mathbb{X}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{X}$	$\mathbb{X}$	$\mathbb{Z}$	$\mathbb{X}$
3	yes	no	yes	yes	yes	no	no	yes	no	no	yes	yes	yes	yes	no	no	no
Bob calls Alice																	
4a	1	-	-	1	0	-	-	-	-	-	-	1	0	-	-	-	-
4b	-	-	0	-	-	-	-	1	-	-	1	-	-	1	-	-	-
5a	1	-	-	0	0	-	-	-	-	-	-	1	0	-	-	-	-
5b	yes	-	-	-	-	-	-	-	-	-	-	yes	-	-	-	-	-
6	-	-	-	1	0	-	-	-	-	-	-	-	0	-	-	-	-

Table 2.2: Decoy-state BB84 protocol, lines 1a are bits generated by Alice, 1b and 1c show states Alice sends, line 2 represents bases in which Bob measures, line 3 tells whether Alice and Bob used the same basis, line 4a is the sifted key, 4b shows transmitted decoy states, 5a is a verification mask, 5b presents the result of the verification, and line 6 shows the final raw key.

In this illustrative protocol example, there was used signal generating probability of 50 % as well as for the probability of decoy states. However, in typical cryptosystems, the probability of the signal states is set much closer to 100 %, and thus maximalizing the secure key rate as the secret key is extracted only from the signal states.

2.3 Discussion of light sources

Before going through the experimental setup, I would like to highlight the importance of an appropriate light source choice. The particular emitter should fulfill several technical requirements, which might not seem important at first

sight. The desired features may be achieved with several semiconductor light sources such as laser diode (LD), a vertical-cavity surface-emitting laser diode (VCSEL), or a superluminescent light-emitting diode (SLED) for instance.

Obviously, one would like to have a high modulation speed of the light source. As the mean photon number in a pulse is typically very low, the carried states may not reach the end of the attenuated quantum channel. The repetition frequency of the transmitter is extremely important as the final secret key rate is proportional to, and it often limits the repetition rate of the whole system. Therefore, the particular light source should be capable of modulation speed in GHz range. The response of a light source is typically determined by the rise time, which is a time during which optical signal rise from 10 % to 90 % (or from 20 % to 80 % alternatively) when a voltage is applied across the device. Here, the operating current which is needed to drive the emitter is also worth mentioning. It may be beneficial to choose sources that need low drive current (driven with voltage bellow 5 V) as they can be controlled by a larger range of electronics. Additionally, low drive current typically does not produces much heat.

I would like to stress the importance of having enough optical power in the setup which is essential to build and then adjust the experimental setup. Even though quantum communication runs with intensities bellow one photon per pulse, the system has to be adjusted with strong signals. Thus, the optical power is wanted to be in a single spatial mode and narrow spectral mode.

Our BB84 implementation involves four quantum polarization states, which can be produced by a single source and a polarization modulator, or as in our case, with four separate light emitters. Not surprisingly, in such a case, they all have to be spectrally indistinguishable. Therefore, the same frequency spectra of the emitters are required.
It is fairly easy to ensure spectral indistinguishability for broad-spectrum (in range of tens of nm) sources such as LED or SLED. Their spectra typically overlap very well. However, an issue with broad-spectrum sources is that they suffer from chromatic dispersion when propagating in an optical medium. The photon from the weak optical pulse stretched in time due to dispersion may arrive at a detector in a different time window than that in which it is expected. As the repetition frequency of the emitter should be as high as possible, the arrivals of photons have to be well defined so that the synchronization of communication would not be broken.
It is always possible to use a narrow band-pass interference spectral filter which would transmit light only in a small range of wavelengths. Though, there are other technical difficulties to overcome. If the spectra are broad enough, one may incorporate a band-pass filter before all the sources are coupled into the quantum channel. However, selecting only a narrow band of the spectra brings another difficulty as it is very power ineffective.

An alternative option is to incorporate narrow-spectrum sources. However, central wavelength (CWL) of LDs or VCSELs with a very narrow spectral line (units of nm or less) may differ from piece to piece even if one gets the component from a single batch. The positions of the central peak in the spectrum

vary typically more than the width of the peak. However, we have the ability to control the CWL by changing the temperature of the source or current going through it. Moreover, no intensity is lost because of the filter.

Now we see that the convenient sources should be spectrally indistinguishable in an intense narrow spectrum. Also, the spatial indistinguishability is required, which is essential particularly for the free-space QKD. It is easy to secure the spatial indistinguishability by filtering the signals with single-mode optical fiber. However, we also expect all the power to be in a single spatial mode so that the system may be tested and adjusted with the intense optical signal. There are various technologies designed to achieve an intense single spatial mode. Optical resonators and cavities or waveguide laser emitters may be utilized for that purpose.

For our experimental scheme, we have implemented HFE4093-332 vertical-cavity surface-emitting laser diodes (VCSELs) from Finisar as light sources. It is a free-space emitter and the beam profile of such sources should be taken care of. The structure of semiconductor emitters does not necessarily produce a symmetrical Gaussian beam profile that would be effectively propagated in single-mode optical fibers. The main features of implemented VCSELs are a rise time of 150 ps, which allows modulation up to 3,3 GHz, low drive current, narrow spectral line, and well defined homogeneous spatial mode of emission. The typical beam profile of one of the chosen VCSELs HFE4093-332 is captured in Fig. 2.2 in comparison with OPV302 from Optek. The figure demonstrates that there is a difference between sources utilizing the very same technology, but being offered by a different manufacturer. Several types of VCSELs were tested but HFE4093-332 offers the highest optical power that can be coupled into the single-mode optical fiber.

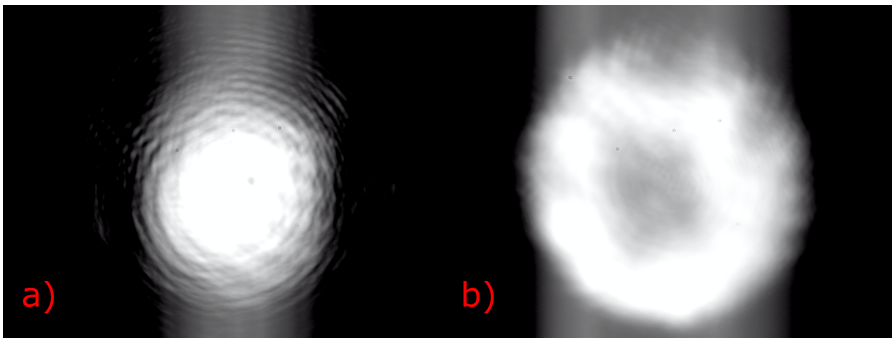

Figure 2.2: The beam profiles of a) HFE4093-332 from Finisar and b) OPV302 from Optec demonstrating the variety of spatial profiles of VCSEL sources offered by various manufacturers.

The spectra of four chosen VCSELs pieces are shown in Fig. 2.3. The particular pieces were chosen from a set of 12 pieces so that their spectra are as close to each other as possible at room temperature. Even though they are not spectrally indistinguishable, there are methods to adjust their CWL. The drive

current control is an example. Fig. 2.4 shows how the spectrum of a single VCSEL changes when different current is applied to it. It should be noted, that the shift of the CWL may not occurs only due to applied current but also due to the temperature change caused by the current. The temperature of VCSEL is not actively controlled as it is only cooled passively with the whole holding system.
Another, probably more robust, method we may use to adjust the CWLs of the VCSELs is active temperature control. According to the manufacturer, HFE4093-332 has a temperature variation of 0.06 nm/°C, which allows sufficient tuning. Last but not least, I would like to stress an importance of the pre-selection of suitable pieces with the same spectra form a larger set as it is easier to adjust the spectral indistinguishability.

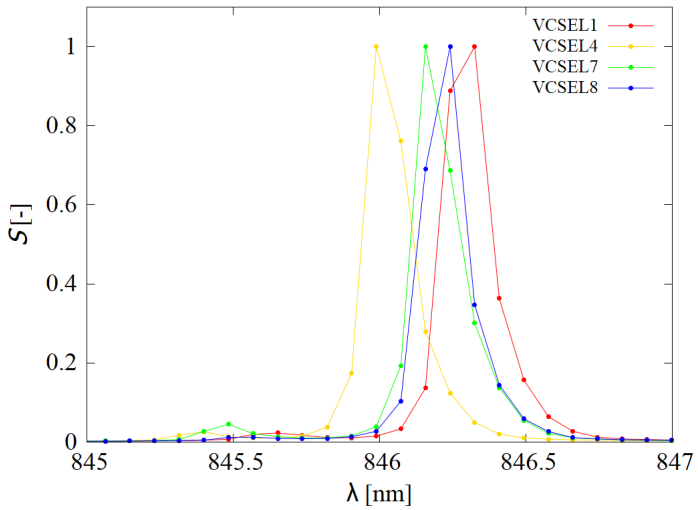

Figure 2.3: The spectra of VCSELs HFE4093-332 from Finisar incorporated into the experimental setup. The spectra are captured at room temperature and for the same drive current of 4 mA.

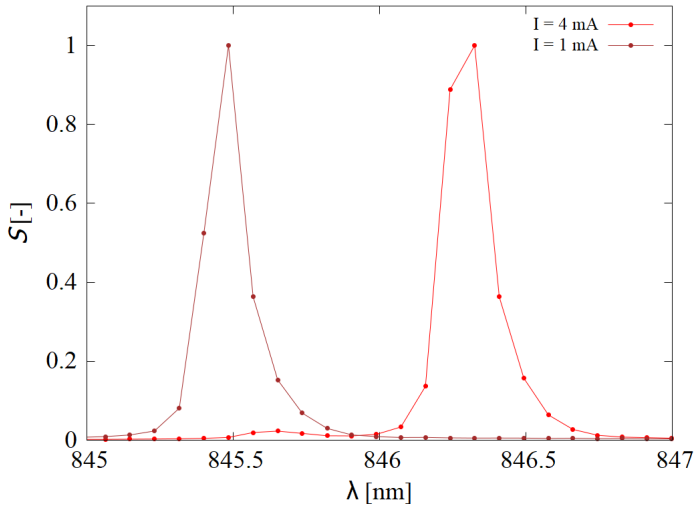

Figure 2.4: The frequency dependence of a single VCSEL1 (HFE4093-332 from Finisar) on applied driving current.

2.4 Experimental setup

In this section, I will describe the experimental setup designed to test the parameters of QKD with the decoy-state BB84. The setups of Alice and Bob are realized on the separate breadboards so that there is a possibility to move each device individually. Although they can be connected with different types of the quantum channel (i.e. free space or optical fiber), both encoding and decoding of the states are realized in free space.

We incorporate four pieces of VCSELs HFE4093-332 in our experimental system. Each of them generates one of four polarization states ($|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$) as shown in Fig. 2.5. The transmitter is divided into two arms, each consisting of two VCSELs generating $|H\rangle$ and $|V\rangle$ state. The polarization states in one arm are then rotated by 45 °C to produce $|D\rangle$ and $|A\rangle$ states.

The intensity modulation required for the decoy-state method is utilized by selecting the proper value of driving current, which will be covered in section 2.5 in detail. Some experimental implementation incorporates an external intensity modulator [25], which are quite expensive. Alternatively, one may implement eight laser sources and set their intensities individually. However, it is advantageous to use only four light sources as it is easier to match the spectra of only four of them, especially when it is realized by pre-selection. Additionally, with fewer lasers, it is easier to couple them to the single spatial mode and simplify the experimental setup.

Let us now go through the scheme of the transmitter (Alice) shown in Fig. 2.5 in detail. Alice incorporates four pieces of VCSELs HFE4093-332 generating linear optical polarization state roughly set to $|H\rangle$ state. The four VCSELs are mounted in a holder that includes a C220TME-B lens from Thorlabs with a

focal length of 11 mm. The holder system allows adjusting the distance between the lens and the VCSEL to collimate the beam thanks to the Z-axis translation mount SM1Z also from Thorlabs. Moreover, by doing so one can also adjust the width of the beam (by making the beam slightly convergent or divergent) at the surface of the other lens that couples the signal to single-mode fiber (SMF). That is a very important feature allowing efficient coupling to SMF. Two mirrors in kinematic mounts behind each VCSEL ensure complete control of the beam directing. Alice is divided into two arms representing the bases $\mathbb{Z}$ and $\mathbb{X}$. Each arm consists of two VCSELs, polarizers LPNIRE050-B from Thorlabs, and high power half-wave plates (HWP) from Altechna which generate the required states $|H\rangle$ and $|V\rangle$. In each arm, these two states are merged together to one spatial mode by a polarization beam splitter (PBS). PBS122 from Thorlabs. The polarization states at the output of one arm are rotated by 45° by another HWP to produce $|D\rangle$ and $|A\rangle$ states. Further, these two arms with four optical states are merged together to one spatial mode by a beam-splitter (BS) BS005 from Thorlabs. The light then goes through a set of neutral density filters (ND) before it is being coupled to the SMF with fiber collimator 60FC-4-M11-18 from Schäfter + Kirchhoff. SMF ensures the spatial indistinguishability of individual sources.

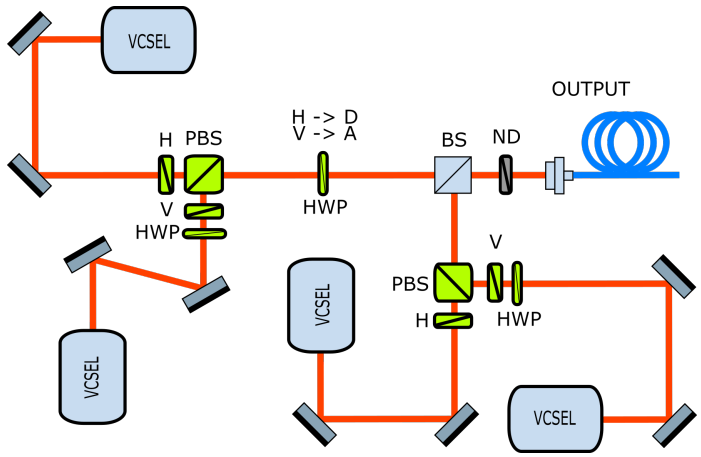

Figure 2.5: The detailed scheme of Alice, transmitter setup. VCSEL - vertical-cavity surface-emitting laser diode, H - linear polarizer set to horizontal polarization, V - linear polarizer set to vertical polarization, HWP - half-wave plates, PBS - polarizing beam splitter, BS - beam splitter, ND - neutral density filter.

On the other side of the quantum channel is Bob, the receiver. Bob's setup is organized in a similar way. First, the initial polarization state is recovered by the manual fiber polarization controller (PC) FPC030 from Thorlabs. The PC consists of three paddles. Each of them has a spool inside around which the optical fiber is wrapped. Those three paddles act as a series of $\frac{\lambda}{4}$, $\frac{\lambda}{2}$ and $\frac{\lambda}{4}$ waveplates. Rotation of the paddles provides a transformation of the polarization state of the light propagating through them. Then the light is coupled

into the free space with the fiber collimator. After that, it is split with a BS whose one output is rotated by 45°. Then the beams are analyzed by a pair of PBSs, it separated $|H\rangle$ and $|V\rangle$ polarization states (analogically $|D\rangle$ and $|A\rangle$ states). The second PBS is located in the reflected port of the first one and is rotated by 90° and serves as linear polarizer transmitting $|V\rangle$ polarization low loss and with high extinction ratio, which is typically from 20:1 to 100:1 and would inevitably induce errors.

The separated beams are then coupled into multi-mode optical fibers (MMF) using steering mirrors and fiber collimators and further detected by single-photon avalanche diodes (SPADs) from Excelitas.
The SPADs are not photon number resolving detectors and generate roughly the same avalanche current every detection. After the detection, the avalanche has to be quenched, which takes some time (a so-called dead time of the detector) during which no other detection can occur. The dead time of the incorporated detector is typically around 25 ns. However, not every photon causes the detector click. The quantum efficiency of the utilized SPADs is around 60 %. Furthermore, the detection may occur even if no photon has reached the SPAD. Such noise is called dark counts and originates from the thermal noise. The dark count rates of utilized SPADs are $DC_1 = (73 \pm 4)$ Hz, $DC_2 = (64 \pm 4)$ Hz, $DC_3 = (166 \pm 6)$ Hz, and $DC_4 = (242 \pm 7)$ Hz when the statistical set of 5 s long measurement was acquired.

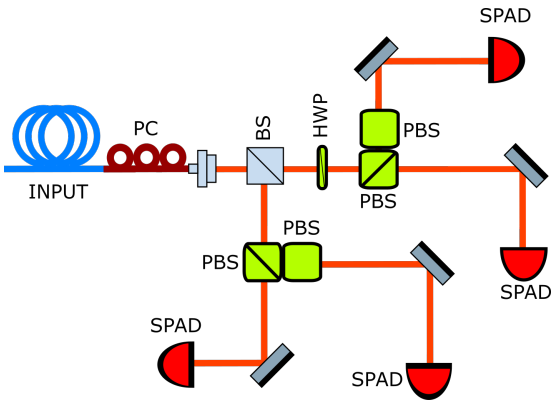

Figure 2.6: The detailed scheme of Bob, the receiver setup. PC - polarization controller, HWP - half-wave plates, PBS - polarizing beam splitter, BS - beam splitter, SPAD - single-photon avalanche diode detector.

2.5 Control electronics and synchronization

As already sketched in the previous section, we utilize four laser sources. One needs to be able to tune their output intensity required for generating signal and decoy states and to share an electronic clock signal with the receiver and thus synchronize the transmission. This is achieved with the custom-made pulse box controlled by the microcontroller.

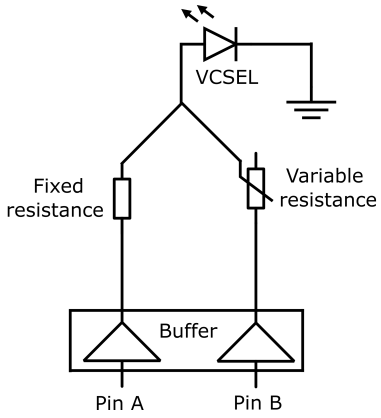

Figure 2.7: Scheme of the control electronics circuit of a VCSEL.

The function of a pulse box and even the intensity modulator are all secured by the Arduino DUE [26]. It is a microcontroller board based on the Atmel SAM3X8E ARM Cortex-M3 central processing unit (CPU) [27], which incorporates the true random number generator (TRNG). The TRNG generates 32-bit long random strings that pass the NIST and Diehard Random Tests Suites. The CPU operates with the inner clock frequency of 84 MHz making a single cycle of the processor almost 12 ns long. This allows generating pulses as short as 24 ns, thus having the maximal theoretical repetition frequency of 21 MHz [28]. Thanks to the parallel input/output controller (PIO) it is possible to control up to 32 Arduino pins at the same time, which enables simultaneously switch any of the VCSELs and the shared clock signal. One needs to only address the PIO directly and without the use of the Arduino built-in function. Our Arduino pulse box is capable of generating pulses with a repetition frequency of around 19 MHz, which is slightly lower than the theoretical value due to other processes the Arduino performs. However, during the actual QKD, the repetition frequency was set only around 2.8 MHz, as it is the maximal rate of Bob's detection device. This will be described more in the following section. Additionally, it is possible to incorporate the build-in TRNG at the repetition rate of 2.8 MHz. For a higher rate, an external TRNG has to be used.

The utilized HFE4093-332 VCSELs are designed to be operated by the driving current in the range from 1 mA to 4 mA, with the applied voltage around 2 or 2.1 V. Arduino due provides a fixed output voltage of 3.3 V on each pin, which is a deadly value for our particular VCSEL. In order to tune the voltage level, and thus control the driving current, an additional electronic circuit is required. The driving circuit is in a form of breakout board (BB), that transfers the electronic pulses from the Arduino pins to the VCSELs and other devices. The BB is plugged into the Arduino pin lines and it has a line of SMA connectors on the other side, which makes it easy to connect the BB to any device.

Two Arduino digital pins are required to control a single VCSEL. The control circuit on the BB, which is responsible for driving the VCSEL, is sketched

in figure 2.7. There are 74LVC245AD transceivers [29] working as buffers, which separate the Arduino digital pins and the VCSEL. The reason for incorporating the buffer is that the CPU of the Arduino cannot provide output current high enough to drive all the VCSELs and to generate auxiliary synchronization clock signals even though the provided voltage level is higher than the operating one. Especially during the testing, it was important to have the synchronization clock signals displayed on an oscilloscope, which could exceed the total DC output current of the CPU. The buffer is supplied from the Arduino board power supply, thus providing enough current.
The buffer output is connected to the VCSELs with a variable resistor in one arm of the circuit and the fixed resistor in the second one. The circuit operates in two modes as shown in table 2.3. In the first case when the signal state is generated, both pins A and B are set high, which makes the VCSEL to be driven with a current that is the sum of the currents that flow in the individual arms. In the second regime when the decoy state is generated, only pin A is set high while the pin B is set low meaning there is a voltage of 0V. This causes the current flowing through the VCSEL to be the difference of the currents in the individual arms.

Pin A	Pin B	Driving current	Generated state
High	High	$I_A + I_B$	signal
High	Low	$I_A - I_B$	decoy

Table 2.3: Operational modes of the driving circuit of the VCSEL.

Therefore by addressing the appropriate Arduino pins, I am able to generate either the signal state (the stronger one) or the decoy state (the weaker one). Moreover, by adjusting the variable resistance in arm B, I may modify the values of the driving currents, which allows me to change the intensity of the signal and decoy states. Although it should be noted, that it is not possible to set the intensities of the signal and decoy state independently. Since only the sum or difference of the individual currents is realized, I can rather set the ratio of the signal state intensity to the decoy state one.

Apart from the four circuit blocks designed to drive the VCSEL, there are also four other blocks consisting only of the buffer and a single fixed 50 Ω resistor. In this case, only one Arduino pin is utilized and those outputs are used to display the signals sent by Alice on the oscilloscope. Additionally, during the QKD one of the outputs is connected to the Bob's detection unit to synchronize the transmission (acts as the clock). The photograph of the BB is shown in figure 2.8.

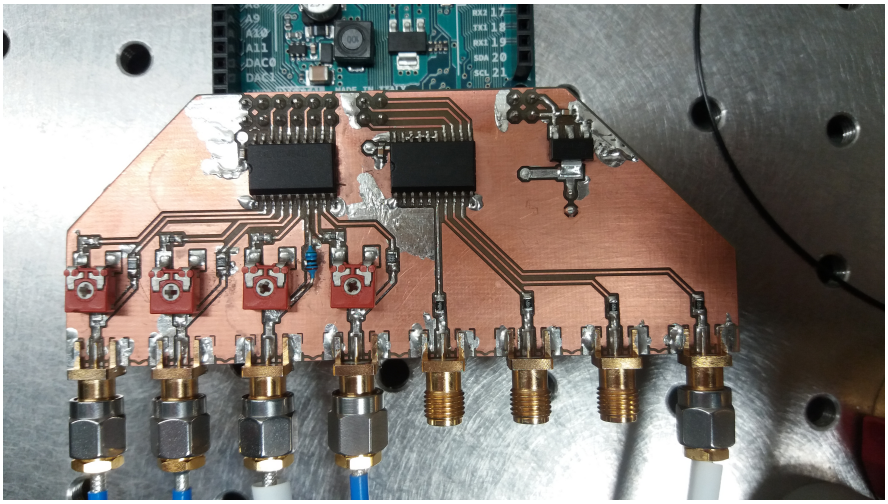

Figure 2.8: A photograph of the breakout board. Four SMA connectors on the left are connected to the VCSELs and the other four are the auxiliary outputs with 50 Ω resistors.

Chapter 3

Postprocessing of the raw key

The physical transmission of qubits over the quantum channel is only a part of the quantum cryptographic protocols. In this section, we will discuss classical post-processing, which consists of the sifting, information reconciliation (also known as error correction), and the privacy amplification.

The sifting is a natural part of every protocol and depends on its design. As the QKD often relies on measurements performed in non-orthogonal bases, the bit of information may be successfully transmitted only if both participants used the same bases. This part of the quantum cryptography was already dealt with during the description of our protocols. Therefore in this section, we will focus on the other two parts of classical post-processing of the raw key.

3.1 Information reconciliation

First, let us go through the error correction process and mention some algorithms designed for that purpose. After the raw data are shifted and the raw key is obtained, QBER has to be estimated. If its value is not too high and protocol is not aborted, information reconciliation follows to correct the errors between Alice's and Bob's data frames. The errors in their data may occur due to the practical implementation of the utilized protocol as the imperfect measurement settings or fluctuations of the parameters of the quantum channel. However, all the errors might also be caused because of Eve's intervention.
Correction algorithms are usually based on the parity check of blocks of the raw key. The parity values are exchanged via an authenticated public channel. As Alice and Bob reveal particular information about their data sets, the key is usually shrunk as a consequence. The most widely used error correction protocol is the Cascade protocol proposed in 1994 by G. Brassard and L. Salvail [30], which was the improvement of their previous BBBSS protocol [31].

The Cascade works in several passes. Alice and Bob divide their data frames into the blocks of a fixed length. The block length is usually a function of QBER and gets shorter for higher QBER. Then they compute the parity (i.e. the sum of the bits modulo 2) of each block and exchange the results. If the parity of a block differs in Alice's and Bob's data frames, they can correct the error. It should be noted that only an odd number of errors in a single block is detectable this way. The simplest way to correct one error in the block is to use the binary search (also referred as a dichotomic search), during which Alice and Bob divide the particular block, check the parity of one half to determine which of the two halves contains the error, then divide this sub-block again, and so on. Doing so, they isolate the erroneous bit and correct it. As its parity is already publicly announced, such a bit is not secure to use for encryption and it is discarded at the end of the protocol. Before it is proceeded to the second pass, the sifted key has to be randomly (but in the same way by both Alice and Bob) permuted in order to reveal new errors. Then they divide their dataset to larger blocks (most commonly doubled). Alice and Bob again exchange their parities, search for errors, and correct them. However, errors found in this pass may now be utilized to correct more errors that were not detected in the prior run. As every error in this pass was previously hidden in a block with an even number of errors, thus there has to be another error that can be now corrected. Before any other pass, the key is always shuffled and the block size doubled. Newly discovered errors are traced back from the first pass onwards starting a cascade of correction. According to the authors, four passes is enough to reconcile a data frame of 10^4 bits.

There is a large variety of modifications to the Cascade protocol, which optimizes the block lengths, random shuffling between the passes or they add new features to the protocol. I would point out BICONF algorithm [32] as an example, which is sometimes used in the reconciliation process. BICONF algorithm randomly chose a subset of the data frame and performs a binary search on it and also on the rest of the frame. The subset may be as large as half of the whole frame. An interesting analysis of the Cascade protocol in comparison with several of its modification was done in [33]. Apart from the Cascade, the Winnow [34] is a different example of error correction protocol. Winnow does not work with parity exchange but utilizes the Hamming code. An advantage is the reduced number of public interaction, which makes it faster than Cascade. Although Winnow is not as efficient as the Cascade for low QBER values.

As mentioned before, the reconciled key is always shorter than the initial sifted one. Eve may monitor the public channel used for error correction without disturbances. Processing the parities during the public communication between Alice and Bob leaks additional information about the sifted key. Such revealed bits have to be discarded making the length of the reconciled key shorter. The discarded part of the sifted key m_{rc} may be expressed as

$$m_{\mathrm{rc}} = \eta n_{\mathrm{sf}}, \tag{3.1}$$

where n_{sf} stands for the length of the sifted key and η is a probability, that a bit is lost during the error correction process. Obviously, with higher values of QBER, the lower the value of η will be. However, there is a Shannon lower bound for η for a given value of QBER e such that $\eta_{\mathrm{min}} = h_2(e)$, where

$$h_2(e) = -e\ \log_2 e - (1-e)\log_2(1-e) \tag{3.2}$$

is the binary Shannon entropy. We can now define the reconciliation efficiency as a fraction of disposed key to the minimal key required to reconcile the sifted key n_{sf} as

$$f_{\mathrm{EC}} = \frac{m_{\mathrm{rc}}}{n_{\mathrm{sf}}\ h_2(e)}. \tag{3.3}$$

For the perfect reconciliation following the Shannon limit is $f_{\mathrm{EC}} = 1$. However, practical algorithms work usually above this threshold so that $f_{\mathrm{EC}} \geq 1$, making the reconciliation efficiency an important criterion of the quality of the error correction protocol [33].

3.2 Privacy amplification

After the error correction process, Alice and Bob share identical keys with high probability. However, also Eve may have partial information about the key. Eve's information may be estimated based on the initial QBER. During the privacy amplification, the reconciled key is used to extract a new shorter secret key and thus reduce Eve's information about the final key to an arbitrarily low value.

There are more ways one can perform privacy amplification. The usual one is to compute the secret key using a universal hash function, which outputs a random bit string of a given length according to the initial QBER [35], [36]. Even though the process of privacy amplification is a quite difficult numerical problem, the secret key rate of QKD implementation may be estimated according to the transmission parameters achieved over the physical channel as will be shown in the following section.

3.3 Secure key rate estimation of decoy-state BB84

After the transmission of qubits between Alice and Bob, it is crucial to estimate the transmission parameters such as the QBER or quantum state transmittance as they are needed to correctly decide whether the protocol run has been successful or whether it has to be aborted. In my experimental scheme, I implement weak laser pulses that are vulnerable to the PNS attack. Therefore, it is essential to verify that the transmittance of single-photon pulses and those consisting of multiple photons have not been tampered. As only the single-photon states ensure secure bit transmission, one needs to be able to estimate the probability of detection of such states. This is luckily possible with the help of the decoy states. In the following description, I will follow the ideas published in [37], [38].

A QKD system with weak laser pulses is capable of generating the secure key rate R at least

$$R \geq q\{-Q_\mu f_{\mathrm{EC}} h_2(e_\mu) + Q_1[1 - h_2(e_1)]\}, \tag{3.4}$$

where q is a fraction of states Alice measures in the correct basis, i.e. for the standard BB84 $q = \frac{1}{2}$, because Alice and Bob choose the same basis only in half of the instances. Q_μ and e_μ are the gain and QBER of the signal states, respectively. Q_1 and e_1 are then the gain and QBER of single-photon states, respectively. The gain Q is defined as a fraction of detection events registered by Bob to the number of states emitted by Alice. One may express the gain of signal states as

$$Q_\mu = \sum_{i=0}^{\infty} Q_i, \tag{3.5}$$

where Q_i is a gain of i-photon state given as

$$Q_i = Y_i \frac{\lambda^i}{i!} e^{-\lambda}. \tag{3.6}$$

This equation consists of two terms. The first one is called the yield of the i-photon Y_i state and refers to the probability, that such a state will cause a detection at Bob's side, i.e. it includes channel transmission, losses in the setup, and detector efficiency. The second term in Eq. 3.6 expresses the probability that an i-photon state is generated by the laser source according to the Poisson distribution for a given mean photon number λ.

For our particular implementation and due to the better understanding of the equation 3.4, let us rewrite it as follows

$$R \geq Q_\mu\{-f_{\mathrm{EC}} h_2(e_\mu) + \frac{Q_1}{Q_\mu}[1 - h_2(e_1)]\}. \tag{3.7}$$

Here, we set $q = 1$, because in our setup the choice of the basis is done passively. Actually, the fact that Bob measures in the right basis only 50 % of the time is already incorporated in the gain Q_μ in our case.
Apart from that, the gain of signal states Q_μ may be associated with the raw key rate. Then the expression in the bracket of equation 3.6 refers to the fraction of the raw key that is transformed into the secret key, where the first term describes key shortening during the information reconciliation. Fraction $\frac{Q_1}{Q_\mu}$ is the ratio of single-photon pulses, and thus secure ones, while the rest of the product expression represents bit losses due to the privacy amplification.

From the experimental results, it is possible to obtain the values of Q_μ and e_μ. However, one cannot directly measure Q_1 and e_1, which are those parameters ensuring secure key transmission. Therefore, they have to be estimated. That gets easier with the use of the decoy states. It is shown in [38], that the gain of single-photon states Q_1 can be lower bounded such as

$$Q_1 \geq \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0), \tag{3.8}$$

where μ and ν are the expected mean photon number of the signal state and the decoy state, respectively and Q_ν stands for the gain of the decoy states. Y_0 is the yield of the vacuum state, i.e. the background detection rate. Also, the QBER of the single-photon state can be upper bounded as

$$e_1 \leq \frac{e_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1 \nu}, \tag{3.9}$$

where e_ν is the QBER of the decoy states and the e_0 is the error rate of the dark counts. Because dark counts occur randomly on any detector, the value of e_0 equals to $\frac{1}{2}$. The yield of the single-photon states Y_1 may be expressed as $Y_1 = \frac{Q_1}{\mu e^{-\mu}}$.

Chapter 4

Results

The actual state transmission over the physical quantum channel is always accompanied by other tasks as the proper setting of the whole system and the analysis after the transmission. In this chapter, I would like to mention these tasks, and at the end of the chapter, I will also present the results of the analysis performed with the designed QKD system.

4.1 Experiment setting

In order to set the desired mean photon number per pulse, I need to estimate the overall transmittance of the receiver. It is done by measuring the optical power of the unattenuated continuous signal from the VCSELs. I used the photodiode power sensor S120VC from Thorlabs, which provides the value of optical power with an uncertainty of 3 %. Apart from the transmittance of the necessary optical fibers involving the fiber-based PCs and the transmittance of Bob's setup, the quantum efficiency of the SPADs has to be taken into account, which is around 60 %. In my case, the transmittance of the necessary optical fibers with the PC is around 0.95, which is mainly caused by the backward reflection of light on the two fiber optic connectors. The optical power was measured right after the light is coupled into the SMF after Alice's setup and at the beginning of Bob's setup. The transmittance of Bob's setup is around 0.79, which is a fraction of the sum of optical powers behind the MMFs coupled to the detectors to the optical power in front of the first BS in Bob's setup. Here, the attenuation is due to the non-unity coupling efficiency into the MMF, backward reflection of light from the optical surfaces, and possibly also due to the absorption on the optical components. The transmitted state will also feel an additional 0.5 transmittance caused by the first BS in the receiver, which performs the passive choice of the basis. Thus, I have estimated the overall transmittance of the setup to be around 0.225 ± 0.007.

Before attenuating the VCSEL's outputs to the single-photon level, the PC has to be set appropriately to compensate for the polarization transformation in the channel. To do so, a polarizer is placed behind the PC and set orthogonally to the polarization state that is being sent by Alice. Then I rotate the paddles

of PC so that the optical power behind the polarizer is as low as possible. After that, I rotate the polarizer by 45° and change the state sent by Alice accordingly. Now I try to minimalize the optical power behind the polarizer again. In this manner, I am switching the described settings several times until the polarization transformation made by the channel is sufficiently compensated. For example, if I set the polarizer to the H polarization, I switch on only the VCSEL providing the V polarized light. After I minimalize the optical power behind the polarizer, I set the polarizer to D polarization and make Alice send A polarization light. When the compensation is successful in this basis, I repeat the process again several times.

Once everything is set, the continuous optical signal sent by Alice is changed to the pulses and ND filters are added to attenuate them to a single-photon level. One of the ND filters (NDC-100C-4M from Thorlabs) provides a continuously variable level of attenuation allowing fine tuning. The possibly different initial intensity of the individual VCSELs may be adjusted by modifying the coupling efficiency of the particular VCSELs into the channel.

4.2 Detection electronics and data analysis

The output signals from SPADs and the synchronization clock signal are captured with a time-to-digital converter (TDC) from UQDevices, which turns the signal arrival time to digital tag with a resolution of 156.25 ps. Each time tag is saved in the memory as a ten-byte long number, where the first 8 bytes represent the arrival time in the resolution units, and the last 2 bytes inform about the channel where the signal was registered. The data from the TDC are transmitted to the computer via USB interface and saved. However, the data transmission speed of the TDC is limited. If the total count rate exceeds 3 MHz, the data transfer becomes unreliable meaning that the TDC may become overflowed with the data and stop uploading them to the PC for quite a long duration of hundreds of milliseconds typically. The repetition rate of 2.8 MHz is the possible maximal limit that allows transmission without the dropouts.

It is crucial to have synchronization of the transmission under control, thus every optical pulse is accompanied by an electronics synchronization pulse. While having the mean photon number in a pulse bellow 1, most of the detections captured by the TDC are from the synchronization signal. It should be also noted, that with such a repetition rate, the data files saved in the computer are very large, typically more than 25 Mb after 1 second of operation. Obviously, this is not the most efficient way of synchronization and the system needs further improvements. There might be only one electronics pulse for every N optical pulses, which would allow even a higher repetition rate of the transmission. Alternatively, both the Arduino-based pulse box and the TDC may be synchronized with outer synchronization inputs.

The data analysis described in this section is based on searching for coincidences between the clock signals and the signals from the SPADs. Hence the whole data files have to be loaded into the memory of a computer to be ana-

lyzed, the limit of computer's RAM would be reached for larger datasets. Thus with this detection logics and the offline processing of the data, only short QKD runs of tens of seconds are reasonable. Which is still sufficient for testing the parameters of the whole system, but needs to be enhanced in order to perform real-time QKD.

Now let us take a look at how the raw data from TDC are analyzed. Each SPAD and the synchronization signal are registered on a different channel, which allows me to determine what polarization state was detected or in case of synchronization signal when the clock period begins. Since the repetition rate is around 2.8 MHz, it gives us a clock period of about 360 ns between two pulse arrivals. Even though the driving pulse and the electronic synchronization pulse are sent at the same moment, they obviously do not arrive simultaneously. Thus, one of the pulses has to be delayed (either physically or using the software) to be detected at the same time. Bob detects a valid state only if it occurs in a detection window of 24 ns after the synchronization pulse. Let us call such a tag simply as a detection. The rest of the tags are ignored as they are caused by dark counts or stray light or afterpulses.

First of all, the detections registered by Bob have to be synchronized with the data sent by Alice. It is done by performing the analysis of a small calibration frame of the 10^4 tags. After the file with time tags is loaded into the computer memory, the positions of the detection are noted. Since Alice transmits only pre-determined patterns and no randomness was involved, the copy of Alice's bits of the same length as the number of clock periods is simply loaded into the computer. A subsection of Alice's pattern is selected according to the positions of Bob's detections (forming a raw key sent by Alice). By comparing it to Bob's detection, the QBER is computed. If it is too high, obviously the pattern that was generated does not match with what Bob detected. In that case, Alice's pattern is shifted to match Bob's detections.

Now, when Alice's data pattern is synchronized, the whole data frame is loaded in the computer memory and the analysis is performed. If the click of any SPAD occurred in the detection window, it is evaluated as the detection and it is also noted what Alice sent at that time. When all the data frame is analyzed, the QBER is evaluated by comparing Bob's detection with what Alice sent. The fraction of the detections to the length of the record is evaluated as a gain of the transmitted state. According to it and to the total channel attenuation the mean photon number in a pulse is computed.

It should be noted, that it takes most of the time to find the detections as the software has to go through almost every tag with a for-cycle. Additionally, it appears faster to cut the data frame into smaller frames and analyze them one by one. For real-time QKD, it would be advantageous to evaluate the coincidences between the synchronization signal and the signals from SPADs with a dedicated electronic coincidence unit.

4.3 QKD system analysis

In this section, I will introduce the results of the QKD system analysis. Once the experiment was set according to section 4.1, I performed the transmission of the quantum states for a duration of 20 s (10 s for each basis) and then I changed the intensity of the transmitted states and performed another 20 s long measurement to acquire data for the decoy states.

For the decoy and signal states, I have set the detector count rate to around 15 kc/s and 62 kc/s, respectively. Which in result corresponds with the mean photon number in a pulse of $\nu = 0.05$ and $\mu = 0.22$, respectively. After data analysis, the gain of the decoy states was estimated to be around $Q_\nu = 0.011$ and $Q_\mu = 0.044$ for the signal states. The QBER of the decoy states was around $e_\nu = 0.3$ % and the QBER of the signal states was around $e_\mu = 0.2$ %. The error rate obtained during the transmission is caused mainly due to the imperfect setting of the PC. Even though there is no added fiber-based channel (apart from the necessary optical fibers), it is not easy to compensate for the transformation of the polarization state performed by the optical fiber. Still, the measured values of QBER are sufficient initial parameters.

According to the equation 3.7, I have estimated the initial secure key rate of $R = 0.037$ secure bits per pulse, which is a relatively high value signaling that around 84 % pulses are secure in the sense that they would "survive" information reconciliation and privacy amplification. All those estimated parameters represent the performance of the QKD system with zero attenuation in the channel, so I used them to numerically calculate the dependence of the secure key rate on the transmittance when an additional channel is placed between Alice and Bob. The result of the simulation is shown in Fig. 4.1 as a blue dashed line. According to it, the achievable secure key rate reaches zero for the attenuation of around 27 dB. There is a second x-axis in Fig. 4.1, which represents the channel attenuation as the distance of the signal transmission in standard telecommunication optical fiber with the attenuation of 2.4 dB/km at 850 nm. Therefore, at this wavelength, the secure communication could be performed over the maximal distance of around 11.3 km. However, if the long-distance QKD over optical fibers was required, the VCSELs could be exchanged for different sources at the wavelength of 1550 nm, and the achievable distance of secure communication would be almost 130 km. During the computation, I assumed that the polarization transformation induced by the channel does not change. That would not be true in practice, as the effect of a long attenuating optical fiber on the polarization states could vary in time dramatically and could not be perfectly compensated with the PC. However, with an active polarization control system that may be the case.

Then I performed another transmission of the quantum states for the same duration, but with an additional ND filter with the attenuation of 19.3 dB (uncertainty of this value is ±3 % due to the used sensor S120VC). The added ND filter simulates the attenuating channel, which does not change the polarization transformation of the channel as assumed by the calculations. The achieved secure key rate from this measurement is $(3.5 \pm 0.1) \cdot 10^{-4}$ secure bits per pulse, which is also plotted in figure 4.1 (red dots). Even though the obtained secure

key rate at this attenuation matches the calculation well, it should be noted that it is also due to two effects that partially compensate for each other. First, the gain of signal and decoy states are $5.5 \cdot 10^{-4}$ and $1.4 \cdot 10^{-4}$, respectively, which is higher (around 7 % for the signal states and around 14 % for the decoy ones) than it should be according to the calculation. However, it is not such a surprise as the contribution of the dark counts in the secret key is higher in this case. Unsurprisingly, the measured QBER is considerably higher at this attenuation. QBER of the signal state e_μ is around 1.7 % and QBER of the decoy ones e_ν is 6.2 %.

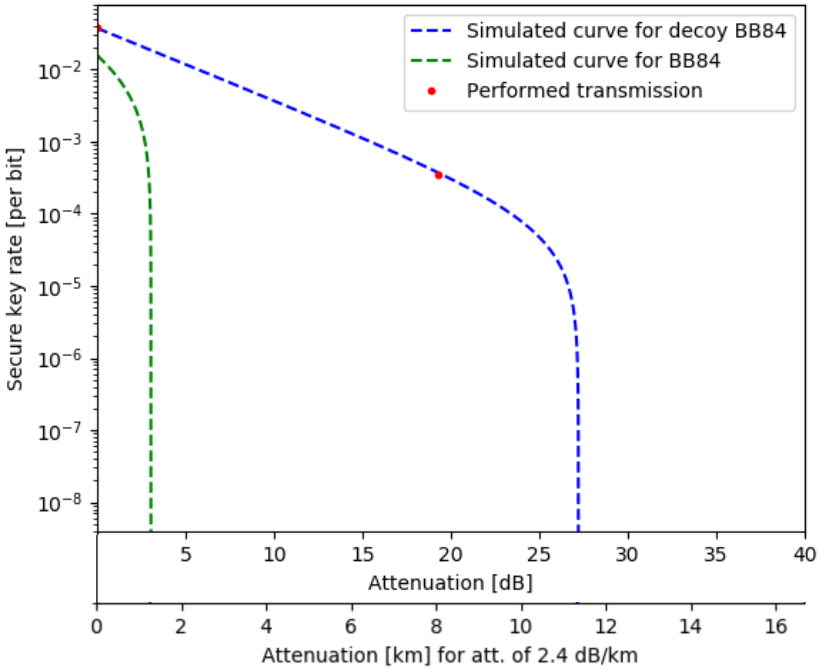

Figure 4.1: Dependence of the secure key rate R on the channel attenuation (and distance in telecommunication optical fiber for 850 nm optical signal.) for the original BB84 (green curve), and the decoy-state assisted BB84 (blue curve). The measured values of R for two attenuation values are shown (red markers). The uncertainty of the R values are comparable with the size of the markers.

The green dashed line plotted in figure 4.1 is a secure key rate achievable with the standard BB84 protocol when only signal states are used to distribute the key without decoy states. The theoretical model for estimating the secure key rate was taken from [39]. The secure key rate of the standard BB84 reaches zero already for the attenuation of 3 dB demonstrating a tremendous increase in possible QKD reach by adding decoy states to the standard BB84 protocol.

Chapter 5

Entanglement based QKD

5.1 Introduction to quantum entanglement

First of all, let me give a brief introduction to quantum entanglement before going through its application in quantum cryptography. A joint state of multiple subsystems (photons in our case) is said to be entangled if it cannot be factorized. The correlations between the entangled subsystems are stronger than any other classical statistical correlations between them. The opposite of the entangled state is a separable state which may be written as a product state of the individual wave functions for instance.

The well-known examples of 2-qubit maximally entangled states in quantum optics are Bell states defined as follows

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|H_1, H_2\rangle \pm |V_1, V_2\rangle) \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|H_1, V_2\rangle \pm |V_1, H_2\rangle). \end{aligned} \tag{5.1}$$

Here, the photons are entangled in the polarization degree of freedom. However, the pair of photons may be also correlated in frequency, time of arrivals, or in direction of propagation. The projective measurement taken on one half of the pair determines the state of the second remote photon. This feature demonstrates the non-locality of quantum mechanics.

A common way to generate entangled photon pairs is parametric frequency down-conversion. It is a three-wave mixing process in nonlinear optical media where a pump photon with a frequency ω_0 is converted to the two photons with frequencies ω_1 and ω_2. This process requires conservation of the energy and the momentum, which is covered in the phase-matching conditions

$$\begin{aligned} \omega_0 &= \omega_1 + \omega_2 \\ \overrightarrow{k_0} &= \overrightarrow{k_1} + \overrightarrow{k_2}, \end{aligned} \tag{5.2}$$

where $\overrightarrow{k_i}$ are the wave vectors. The dispersion in nonlinear media causes the refractive index frequency dependent which under ordinary circumstances

makes the second equation in 5.2 impossible to meet. Luckily enough, the non-linear crystals are often birefringent, i.e. the refractive index depends on the direction of light polarization. One then only needs to tune the angle of the polarization vector with respect to the optical axes of the crystal. Apart from that, the level of birefringence may be also temperature-dependent. Another approach to phase-matching the generation of entangled photon pairs is the so-called quasi-phase-matching. The material is periodically poled so that the crystalline axis is periodically inverted to achieve the effect of phase-matching [40].

The entanglement plays an important role in quantum information, though its application we are most interested in is of course QKD. The application of the entanglement in QKD was suggested for the first time by A.K. Ekert in 1991 [41]. His scheme (E91) consists of a source of entangled photon pairs connected to Alice and Bob with an untrusted quantum channel. Each of them receives half of the photon pair. Alice measures her half of the pair in one of the three non-orthogonal bases, e.g. $\mathbb{Z}$, $\frac{\mathbb{Z}+\mathbb{X}}{2}$ and $\mathbb{X}$. Bob may use the following measurement bases $\frac{\mathbb{Z}+\mathbb{X}}{2}$, $\mathbb{X}$ and $\frac{\mathbb{Z}-\mathbb{X}}{2}$. They use the instances, in which they have chosen the same bases, to extract the secret key. The CHSH test is carried out for all the other cases to check whether the correlation between Alice's and Bob's data remains non-local. Without the presence of Eve, the maximal violation of CHSH quantity equals $2\sqrt{2}$ (for maximally entangled state), while for the classically correlated data the maximal value is 2. As far as Alice and Bob share the entangled state, they can produce the secret key.

One year later the BBM92 protocol was proposed by C. H. Bennett, G. Brassard, and N. D. Mermin [42]. They aimed to simplify the Ekert's protocol omitting the Bell's measurement and modified the original BB84 protocol with the source of entangled photons. In the analogy to E91, the source of the photon pairs provide both parties with half of the pair. Alice and Bob then measure their photon randomly and independently in one of the two bases. They proceed with public discussion of bases used and after that Eve's information is evaluated form the data sample. It should be noted that Alice's measurement on her half of the pair corresponds to the preparation of the state in the original BB84. Once Alice performs the measurement the BBM92 "collapses" to BB84 protocol.

As we mentioned in the introduction, entangled pairs of photons find the application in DI QKD which provides better security due to the relaxation of some assumptions made on detection devices of Alice and Bob which may in principle be exposed to various side-channel attacks. Instead, the security is based on the non-local correlation in Alice's and Bob's data that violate Bell inequalities.

In the rest of this chapter, I will introduce a modification of Ekert's E91 protocol as an example of a DI QKD protocol, which is based on the CHSH test. According to the protocol, I analyzed two entangled Bell's states described by density matrices and estimates the secure key rate from the CHSH test.

5.2 Entanglement-based QKD

The protocol followed in this thesis was first proposed in [43] and further analyzed in [6]. Its security relies on the non-local correlation of the measurement results, which are verified by carrying out the CHSH test. According to the level of its violation Eve's information about the key is estimated and for the quantum violations large enough, the secure key can be distilled from the data.

Alice and Bob share the entangled photon pair $|\Phi^+\rangle$, which originates from a source that may not be necessarily trusted. In each instance, Alice performs one of three measurements denoted as A_0, A_1 and A_2 analogically to the Ekert's E91 protocol. However, contrary to E91, Bob performs only one of two measurements B_1 or B_2. There are no assumptions made on the measurement devices, only that each measurement yields a binary output, i.e. 0 or 1. The raw key may be extracted if both Alice and Bob take the same measurement. The measurements $\{A_1, A_2, B_1, B_2\}$ are used to evaluate the CHSH polynomial defined as

$$S = \langle a_1, b_1\rangle + \langle a_1, b_2\rangle + \langle a_2, b_1\rangle - \langle a_2, b_2\rangle, \tag{5.3}$$

where $\langle a_i, b_j\rangle$ is a correlator defined as $\langle a_i, b_j\rangle = P(a = b|ij) - P(a \neq b|ij)$, which is the difference between the probability of getting same results $a = b$ for a given pair of measurements and the probability of getting different results $a \neq b$. While the CHSH polynomial S is above the value of 2, the secret key may be extracted. Let us denote $A_0 = B_1 = \mathbb{Z}$, $B_2 = \mathbb{X}$, $A_1 = \dfrac{\mathbb{Z} + \mathbb{X}}{2}$ and $A_2 = \dfrac{\mathbb{Z} - \mathbb{X}}{2}$. The pair $\{A_0, B_2\}$ is discarded and not used in the procces. The measurement choice is typically asymmetrical meaning that the probability of Alice measuring in A_0 and Bob measuring in B_1 is high, which results in a higher secret rate.

As shown in the [6] the secret key rate may be estimated from the value of CHSH polynomial S and the value of QBER e as

$$R = 1 - h_2(e) - h_2(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}). \tag{5.4}$$

he QBER here is the probability $e = P(a \neq b|01)$ that Alice and Bob will obtain different results when taking the same measurement in basis $\mathbb{Z}$ $\{A_0, B_1\}$. However, in this thesis, I do not perform actual QKD with entangled photon pairs. I have instead analyzed two density matrices ρ provided by Radim Hošák, which were measured during the preparation of his master's thesis [44]. Those density matrices are the reconstruction of the $|\Phi^+\rangle$ Bell's state generated with a source of entangled photon pairs based on the spontaneous parametric down-conversion (SPDC) in a pair of birefringent nonlinear optical crystals BiBO with type-I phase-matching. Therefore, I cannot compute the values of S and e form the equations (5.3), (5.4), respectively. Luckily it is possible to derive the value of S directly from the density matrix as described in [45]

$$S_{\max} = 2\sqrt{t_{11}^2 + t_{22}^2}, \tag{5.5}$$

where t_{11}^2 and t_{22}^2 are the two largest eigenvalues of $T_p^T T_p$ quantity. T_p is so-called correlation tensor, which is in case of two-qubit system in the form of $t_{kl} = \mathrm{Tr}[\rho(\sigma_k \otimes \sigma_l)]$ for $k, l = 1, 2, 3$ with σ_k being the Pauli matrices. Moreover, such a value of S is already the highest one with respect to the choice of observables for a given state. Obtaining the value of e from the density matrix follows equation

$$e = \langle 01|\rho|01\rangle + \langle 10|\rho|10\rangle, \tag{5.6}$$

which is the sum of the ρ_{22} and ρ_{33} elements of the density matrix. Once the raw key is extracted, the information reconciliation and privacy amplification are performed as it is done in the classical prepare-and-measure QKD.

5.3 Results

The first density matrix visualized in the Fig. 5.1 represents a high quality $|\Phi^+\rangle$ state achieved with the coincidence window of 1 ns.

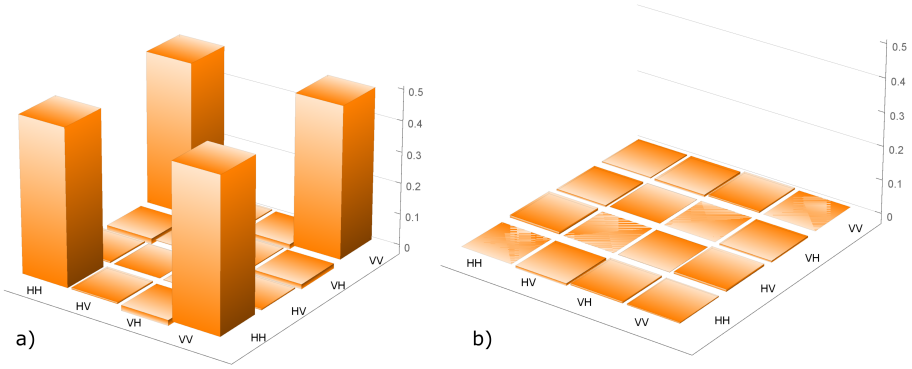

Figure 5.1: Visualization of the first density matrix representing high quality $|\Phi^+\rangle$ state with a) and b) being the real and imaginary part of the density matrix, respectively. This state was achieved with the coincidence window of 1 ns.

One can tell about the high quality of the density matrix as the values of elements $\langle HH|\rho_{AB}|HH\rangle$ and $\langle VV|\rho_{AB}|VV\rangle$ are close to 0.5 while the other two elements on the main diagonal are almost zero and the correlation elements $\langle HH|\rho_{AB}|VV\rangle$ and $\langle VV|\rho_{AB}|HH\rangle$ are close to 0.5. If we used such a source for QKD, we could obtain the initial QBER of 0.4 %. At the same time, the CHSH polynomial computed with (5.5) is around 2.816, which is close to the theoretical limit of 2.828 ($2 * sqrt2$). The achievable secure key rate would be around 0.92 bits/pair.

The second density matrix describes the same state generated from the same source but in this case, the coincidence window was increased to 500 ns. By extending the coincidence window, more noise can be detected as valid data

from which the density matrix is reconstructed. Therefore, by doing so the overall quality of the density matrix is lowered as it is shown in Fig. 5.2. Clearly, the entanglement quality of this state is poor as the correlation elements $\langle HH|\rho_{AB}|VV\rangle$ and $\langle VV|\rho_{AB}|HH\rangle$ are only around 0.4. Additionally, the QBER is also higher as the matrix elements $\langle HV|\rho_{AB}|HV\rangle$ and $\langle VH|\rho_{AB}|VH\rangle$ are significantly higher (around 0.06) in comparison with the first matrix shown in Fig. 5.1. The estimated QBER here is around 12.3 %. The value of CHSH polynomial is around 2.16 and even though it is still above the classical limit, the achievable secure key rate here is around -0.41 secure bits/pair, thus actually not suitable for the QKD.

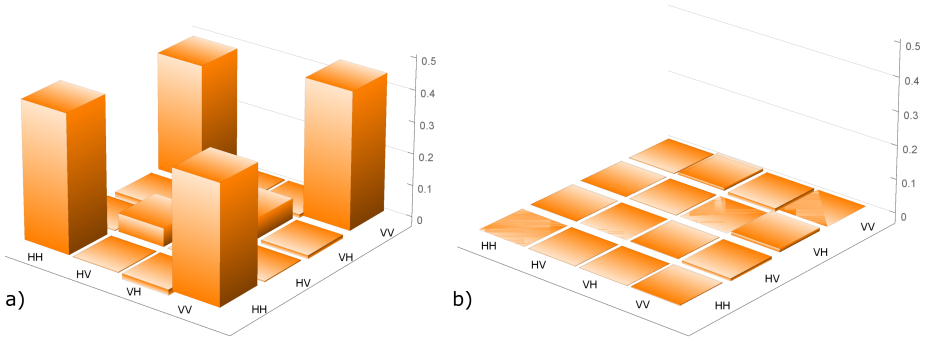

Figure 5.2: Visualization of the second density matrix with a) and b) being the real and imaginary part of the density matrix, respectively. This state was achieved with the coincidence window of 500 ns.

According to the Eq. (5.5), I have plotted the achievable secure key rate for various values of QBER and CHSH polynomial as shown in Fig. 5.3. The points referring to the two analyzed density matrices are plotted as yellow dots. The secure key rate in red areas is above zero while it is negative in the blue areas.

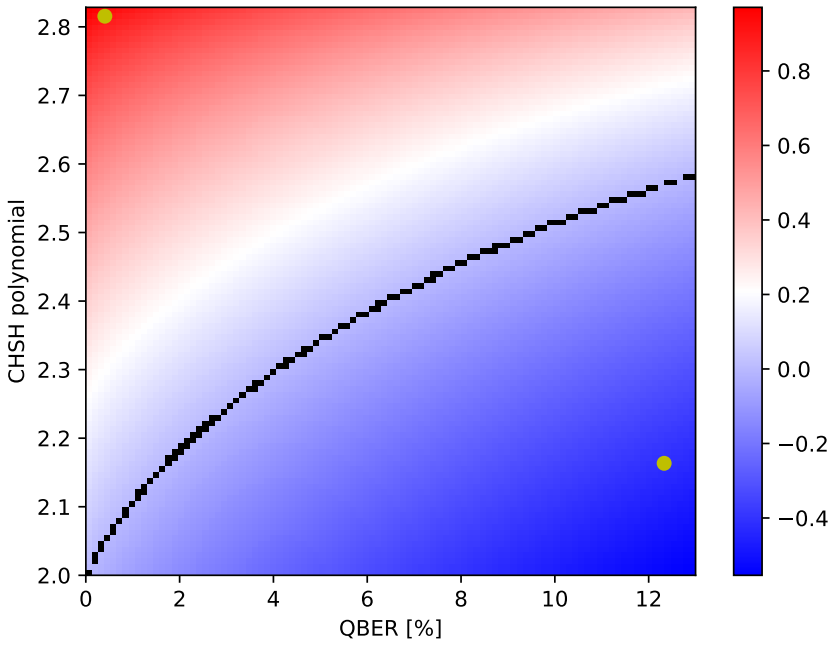

Figure 5.3: The achievable secure key rate R for different values of QBER and CHSH polynomial according to the modification of E91 protocol. The yellow markers show the estimated minimal R of two measured entangled states produced by a SPDC source, and the black markers show the line of zero R.

Chapter 6

Conclusion and outlook

6.1 Conclusion

Quantum key distribution offers absolutely secure communication by effective utilization of the Vernam cipher. There are different approaches one can follow to ensure secure communication, each facing different challenges. In this thesis, I have demonstrated a system capable of QKD with weak coherent states and the decoy states. To achieve it, I have incorporated the polarization encoded BB84 protocol.

To generate both signal and decoy states, I have developed a pulse box controlled by the Arduino Due which provides the maximal pulse repetition rate of around 19 MHz. Arduino due is also capable of generating true random numbers according to the standard NIST and Diehard Random Tests Suites at the maximal speed around 2.8 MHz. I have dealt with the state detection and synchronization of the detections with the clock signal. I have also developed a software toolbox to analyze the signals from the detectors, which analyzes the coincidences between the detection events and the synchronization clock signal.

The performance of the proposed QKD system was tested in the series of state transmissions without added attenuation in the quantum channel and with the attenuation. The trial state transmission was performed with the signal state intensity of 0.22 and decoy-state intensity of 0.05 per pulse. According to the analysis made afterward, the maximal channel attenuation which allows secure communication was estimated to be over 27 dB, which equals the distance in the optical fiber of around 11.3 km at the wavelength of 850 nm and almost 130 km at the wavelength of 1550 nm. To verify the model, another state transmission was performed over the quantum channel with attenuation of around 19.3 dB. At this attenuation, the secure key rate was almost 1 kb/s, which roughly follows the model.

Finally, the device-independent version of the entangled E91 QKD protocol was studied. I have analyzed two $|\Phi^+\rangle$ states described by given density matrixes, which were generated with a source of entangled photon pairs based on the spontaneous parametric down-conversion in a pair of birefringent nonlinear

optical crystals BiBO with type-I phase-matching. I have studied the performance of such states in the mentioned protocol. The first high quality $|\Phi^+\rangle$ state with QBER only 0.4 % and CHSH polynomial of 2.816. The achievable secure key rate with this source is around 0.92 bits/pair. Even though the CHSH polynomial of the second state is above the classical limit with a value of 2.16, this source is not suitable to generate the secret key.

6.2 Outlook

The results covered in this thesis deal with a wide range of experimental challenges that accompany the construction of the QKD system. However, there is much to improve before the presented system could be utilized for real-world QKD.

Firstly, the spectral indistinguishability of the VCSELs has to be ensured. Probably the most robust solution would be to equip the mount of the VCSELs with Peltier coolers and tune the temperature of the VCSELs. Alternatively, four VCSELs with the same spectra could be pre-selected from a larger set of components.

Another issue is the manual polarization controller, which provides the compensation of the channel transformation only in for a limited time. The variation of the channel parameters in time will get even more severe when long optical fiber will be set as the channel. In such a case, the QBER would probably fluctuate dramatically and we need an active polarization control system at Bob's side, which would adjust the polarization transformation in real-time. The additional strong optical signal at different wavelength would be probably needed in parallel with the quantum signal.

In the presented thesis, the intensities of signal and decoy states were predetermined and were not optimized in any manner. Generally, the higher intensity of the signal states means also the higher gain of the states, which is proportional to the secure key rate up to a certain point. However, the higher the intensity higher the ration of multiphoton pulses, which are insecure due to the photon-number splitting attack. attack. Therefore, there is a trade-off between the security and the gain, which results in the optimal setting of the intensity of the signal and the decoy states.

As quantum states suffer from large attenuation during the QKD over long distances, the repetition rate could be also increased to improve the secure key rate. For that purpose, a new pulse box would be beneficial. Such a pulse box based on a field-programmable gate array (FPGA) is already in development. Such a pulse box may provide the pulse repetition rate of hundreds of MHz typically. Also, the FPGA can be utilized to design a coincidence detection logics, which would evaluate the coincidences between the signals from the detectors and the synchronization clock signal in real-time. That would be a step towards the real-time QKD.

It should be also remarked that the synchronization of the transmission

should be improved for long-distance QKD. Alice and Bob would use their own clocks and they would be synchronized via a global positioning system (GPS).

Last but not least, it would be interesting to study the entanglement-based QKD even further. A whole new QKD system based on the entangled photon pairs could be developed to test the performance of the source in realistic conditions, which would verify whether the experimental system matches the theoretical model, and to identify how the quantum channel would affect the entangled photon pairs.

Bibliography

[1] Miloslav Dušek, Norbert Lütkenhaus, and Martin Hendrych. *Quantum cryptography*. Elsevier, 2006.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems & Signal Processing*, 1984.

[3] 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), 2008.

[4] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, 2010.

[5] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23), 2007.

[6] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[7] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden. Finite-key analysis for the 1-decoy state QKD protocol. *Applied Physics Letters*, 112(17):171104, 2018.

[8] Feihu Xu, Kejin Wei, Shihan Sajeed, Sarah Kaiser, Shihai Sun, Zhiyuan Tang, Li Qian, Vadim Makarov, and Hoi-Kwong Lo. Experimental quantum key distribution with source flaws. *Physical Review A*, 92(3), 2015.

[9] Bernd Fröhlich, Marco Lucamarini, James F. Dynes, Lucian C. Comandar, Winci W.-S. Tam, Alan Plews, Andrew W. Sharpe, Zhiliang Yuan, and Andrew J. Shields. Long-distance quantum key distribution secure against coherent attacks. *Optica*, 4(1):163, 2017.

[10] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure

quantum key distribution over 421 km of optical fiber. *Physical Review Letters*, 121(19), 2018.

[11] 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, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, 117(19), 2016.

[12] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7):481–486, 2007.

[13] Giuseppe Vallone, Davide G. Marangon, Matteo Canale, Ilaria Savorgnan, Davide Bacco, Mauro Barbieri, Simon Calimani, Cesare Barbieri, Nicola Laurenti, and Paolo Villoresi. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. *Physical Review A*, 91(4), 2015.

[14] P Villoresi, T Jennewein, F Tamburini, M Aspelmeyer, C Bonato, R Ursin, C Pernechele, V Luceri, G Bianco, A Zeilinger, and C Barbieri. Experimental verification of the feasibility of a quantum channel between space and earth. *New Journal of Physics*, 10(3):033038, 2008.

[15] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan. Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120(3), 2018.

[16] Kevin Günthner, Imran Khan, Dominique Elser, Birgit Stiller, Ömer Bayraktar, Christian R. Müller, Karen Saucke, Daniel Tröndle, Frank Heine, Stefan Seel, Peter Greulich, Herwig Zech, Björn Gütlich, Sabine Philipp-May, Christoph Marquardt, and Gerd Leuchs. Quantum-limited measurements of optical signals from a geostationary satellite. *Optica*, 4(6):611, June 2017.

[17] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[18] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, 1992.

[19] Kiyoshi Tamaki and Norbert Lütkenhaus. Unconditional security of the bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Physical Review A*, 69(3), 2004.

[20] Kiyoshi Tamaki, Norbert Lütkenhaus, Masato Koashi, and Jamie Batuwantudawe. Unconditional security of the bennett 1992 quantum-key-distribution scheme with a strong reference pulse. *Physical Review A*, 80(3), 2009.

[21] Marco Lucamarini, Giuseppe Vallone, Ilaria Gianani, Paolo Mataloni, and Giovanni Di Giuseppe. Device-independent entanglement-based bennett 1992 protocol. *Physical Review A*, 86(3), 2012.

[22] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5), 2004.

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

[24] Yang Liu, Teng-Yun Chen, Jian Wang, Wen-Qi Cai, Xu Wan, Luo-Kan Chen, Jin-Hong Wang, Shu-Bin Liu, Hao Liang, Lin Yang, Cheng-Zhi Peng, Kai Chen, Zeng-Bing Chen, and Jian-Wei Pan. Decoy-state quantum key distribution with polarized photons over 200 km. *Optics Express*, 18(8):8587, 2010.

[25] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields. Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security. *Optics Express*, 15(13):8465, 2007.

[26] Getting started with the Arduino Due. April 24, 2020, retrieved from. *https://www.arduino.cc/en/Guide/ArduinoDue*.

[27] Atmel SAM3X/SAM3A Series SMART ARM-based MCU datasheet. April 24, 2020, retrieved from. *https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel−11057−32−bit−Cortex−M3−Microcontroller−SAM3X−SAM3A_Datasheet.pdf*.

[28] Radim Hošák and Miroslav Ježek. Arbitrary digital pulse sequence generator with delay-loop timing. *Review of Scientific Instruments*, 89(4):045103, 2018.

[29] 74LVCH245A Product data sheet 74LVC245A. May 4, 2020, retrieved from. *https://assets.nexperia.com/documents/data-sheet/74LVC_LVCH245A.pdf*.

[30] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology — EUROCRYPT '93*, pages 410–423. Springer Berlin Heidelberg.

[31] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.

[32] Tomohiro Sugimoto and Kouichi Yamazaki. A study on secret key reconciliation protocol "cascade". *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E83-A(10):1987–1991(4):045103, 2000.

[33] Jesus Martinez-Mateo, Christoph Pacher, Momtchil Peev, Alex Ciurana, and Vicente Martin. Demystifying the information reconciliation protocol cascade. *Quantum Info. Comput.*, 15(5–6):453–477, 2015.

[34] 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. *Physical Review A*, 67(5), 2003.

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

[36] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[37] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23), 2005.

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

[39] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. *Quantum Info. Comput.*, 4(5):325–360, 2004.

[40] Robert W. Boyd. *Nonlinear Optics*. Academic Press, 2008.

[41] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[42] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557–559, 1992.

[43] Antonio Acín, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8(8):126–126, 2006.

[44] Radim Hošák. Optimization of a polarization-entangled photon source. *Palacky University*, Master thesis, 2018.

[45] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, 2009.

Appendices

A Photos of the experiment

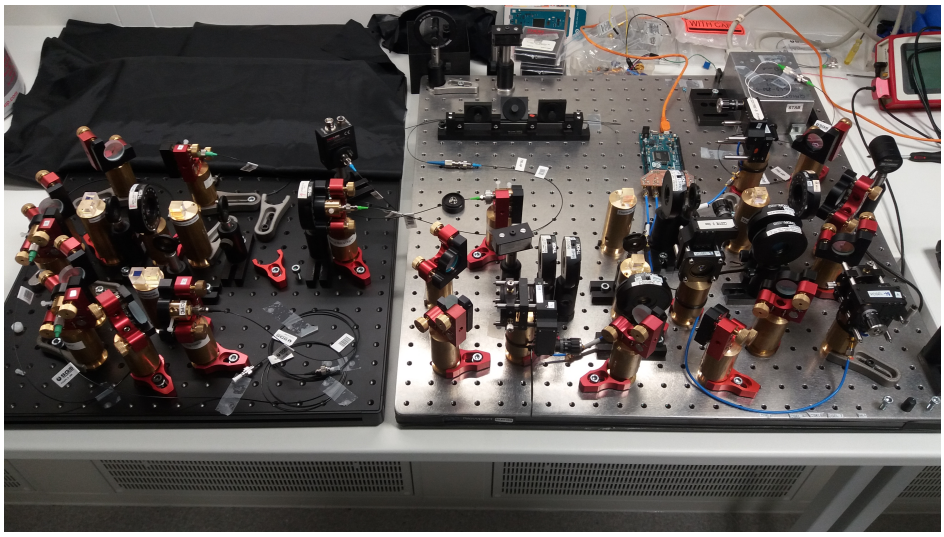

Figure A.1: A photograph of the experimental setup. Alice's setup is on the right and Bob's setup on the left. They are connected only with the short optical fiber without any added attenuation.

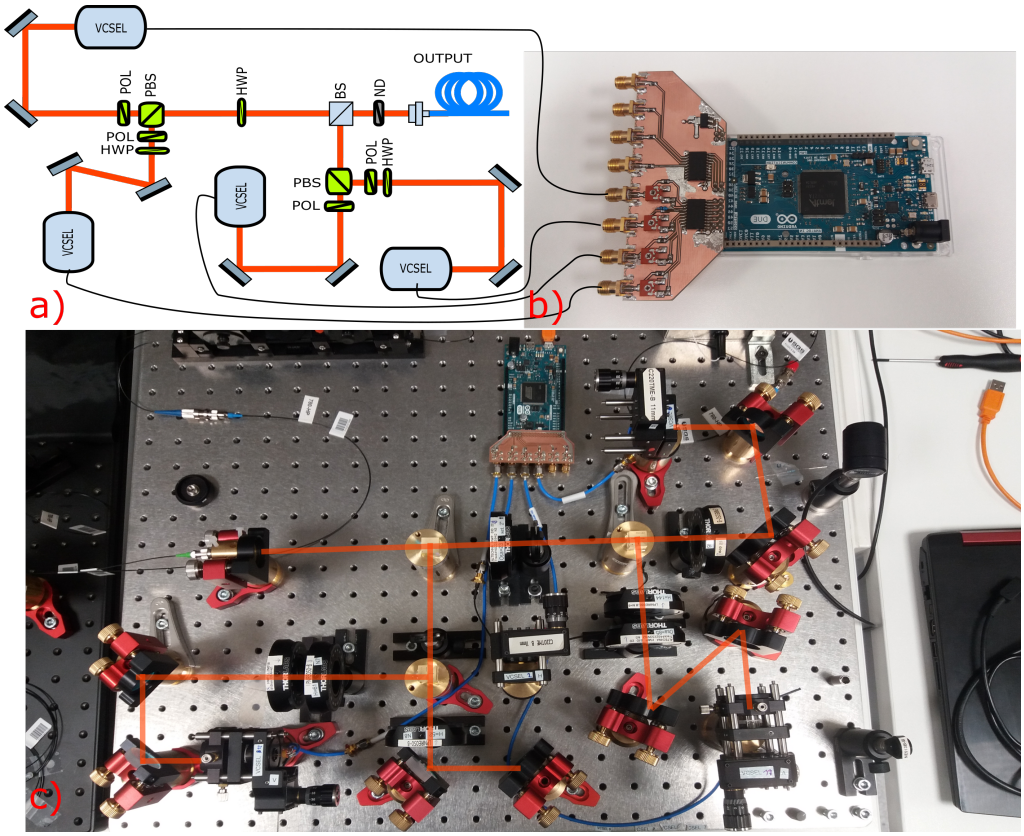

Figure A.2: A photograph of Alice, a) is the scheme of Alice controlled by Arduino-based pulse box, b) the Arduino-based pulse box consisting of the breakout board and the Arduino Board, and c) is a photograph of the Alice with beam paths.

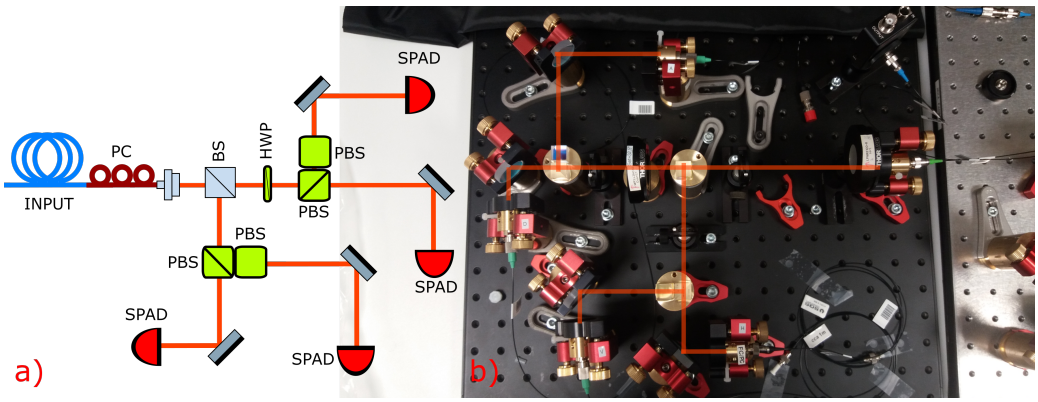

Figure A.3: A photograph of Alice, a) is the scheme of Bob, b) is photograph of the Bob with beam paths.