National Research University
Higher School of Economics

Moscow Institute of Electronics and Mathematics

Master Thesis

submitted for the degree of

Master of Science

Imperfect State Preparation in Quantum Key Distribution

by

Daniil Trefilov

Submission Date:	16th of May 2021
Supervisor:	Dr.Ing. Vadim Makarov
Co-supervisor:	Ph.D. Roman Ozhegov

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

Трефилов Даниил Олегович

НЕИДЕАЛЬНОЕ ПРИГОТОВЛЕНИЕ СОСТОЯНИЙ В КВАНТОВОМ РАСПРОСТРАНЕНИИ КЛЮЧА

Выпускная квалификационная работа – магистерская диссертация
по направлению 11.04.04 Электроника и наноэлектроника
шифр наименование направления подготовки

студента образовательной программы магистратуры
«Материалы. Приборы. Нанотехнологии»
наименование образовательной программы

Студент
_____

Научный руководитель
Dr.Ing., проф. НИТУ МИСиС
_____
В.В. Макаров

Рецензент
д.ф.-м.н., ВНС МИЭМ НИУ ВШЭ
_____
Г.М. Чулкова

Соруководитель
к.ф.-м.н., доцент ДЭИ МИЭМ НИУ ВШЭ
_____
Р.В. Ожегов

Москва 2021

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

ЗАДАНИЕ
на выполнение магистерской диссертации

студенту группы ММПН191 Трефилову Даниилу Олеговичу

1. Тема работы
Неидеальное приготовление состояний в квантовом распространении ключа.

2. Цель работы
Экспериментальный анализ межсимвольных интерференций в коммерческой системе квантового распространения ключа.

3. Формулировка задания
Провести аналитический обзор литературы по теме «Квантовая криптография и квантовое распространение ключа (КРК)». Изучить принципы работы современной коммерческой системы КРК. Экспериментально установить наличие межсимвольных интерференций и их влияние на работу системы.

Проект ВКР должен быть предоставлен студентом в срок до «15» декабря 2020 г.

Научный руководитель ВКР «15» ноября 2021 г. _____ В.В. Макаров

Первый вариант ВКР предоставлен студентом в срок до «31» марта 2021 г.

Научный руководитель ВКР «15» ноября 2021 г. _____ В.В. Макаров

Итоговый вариант ВКР предоставлен студентом в срок до «30» апреля 2021 г.

Научный руководитель ВКР «15» ноября 2021 г. _____ В.В. Макаров

Задание выдано студенту «15» ноября 2021 г. _____ В.В. Макаров

Задание принято к исполнению студентом «15» ноября 2021 г. _____ Д.О. Трефилов

Аннотация

Квантовое распределение ключа (КРК) - метод передачи секретной битовой последовательности между двумя пользователями, основанный на фундаментальных законах квантовой механики, обеспечивающих его бепрецедентную безопасность для использования. Однако, несмотря на доказанную теоретическую безопасность большинства используемых в КРК протоколов передачи данных, экспериментальные реализации систем КРК так или иначе являются приближениями к ним. Это свойство неизбежно ведет к появлению тех или иных уязвимостей в системах такого рода, что вполне может привести к их взлому и утечке секретных данных потенциальному злоумышленнику. В данной работе представлено экспериментальное исследование межсимвольных корреляций соседних электрических и оптических импульсов, возникающих на этапе подготовки состояний для секретной битовой последовательности. Наблюдаемые корреляционные эффекты могут быть серьезной уязвимостью в безопасности коммерческой системы КРК.

Abstract

Quantum key distribution (QKD) is a method of transmitting a secret bit sequence between two users, based on the fundamental laws of quantum mechanics, ensuring its unprecedented security for use. However, despite the proven theoretical safety of most of the data transfer protocols used in QKD, experimental implementations of QKD systems are, in one way or another, approximations to them. This property inevitably leads to the appearance of certain vulnerabilities in these systems, which may well lead to their hacking and leakage of secret data to a potential eavesdropper. This study provides experimental research of the intersymbol correlations of the adjacent electrical and optical pulses, which appear at the stage of preparing states for a secret bit sequence. The observed correlation effects could be a serious vulnerability in the security of a commercial QKD system.

Table of contents

1. Introduction

1.1 Historical review

Since the inception of writing, there was always a need to store, share, and use information privately. This is the moment where cryptography starts its history. The first monoalphabetic cryptography ciphers used the method of replacing one character of the alphabet in the sensitive written information with another character or with the number according to a certain secret rule. For example, in the Caesar cipher, which Julius Caesar invented, every letter of the secret message with the position A in the alphabet, was replaced by the letter with the position $A + \delta$, where δ is an arbitrary but fixed integer. How you can guess, these ciphers are relatively easy to hack with the help of statistical analysis (also known as frequency analysis) which was first performed by Al-Kindi in the middle of the IX century.

The next major point on a historical map of cryptography is the polyalphabetic ciphers, where each symbol of a secret message is substituted with the help of several monoalphabetic ciphers. The most widely used among them was introduced by Blaise de Vigenère in his work "Traicté des Chiffres" in 1585. This type of encryption turned out to be extremely reliable, that it was firstly hacked only in 1863 by the German infantry officer Friedrich Wilhelm Kasiski.

At the beginning of the XX century, an era of polyalphabetic electromechanical cryptographical systems has started. These systems found their application in secret communications, which was undoubtedly useful in the years of World War II.

Everyone knows about the famous German cryptography apparatus Enigma, which used a secret sequence of symbols (a secret key) that is a starting position of rotors in the device. Even though the German military government did not doubt the security of the information encoded by Enigma, its cipher was first cracked in 1932 by the Polish Cipher Bureau. A few weeks before the start of WWII, the Cipher Bureau revealed the cipher breaking methods and related equipment to the British military intelligence, which scientific group with the help of the bright mind of Alan Turing took up further work on breaking the cipher, which was constantly becoming more complicated. Nevertheless, Enigma was hacked, which undeniably played an important role in the history of WWII.

A more serious approach to describe cryptographic methods was taken by Claude Shannon in his pioneering work [1]. He showed strict mathematical apparatus characterizing the amount of the information, data transfer, encryption functions, and entropy. He also proved the cryptographic stability of the Vernam Cipher (also known as "One-time pad"). Despite the unconditional security of this cryptographic technique, there were several significant disadvantages. First of all, the length of a secret key must be equal to the length of a secret message, which is acceptable but not convenient. Secondly, to provide full secrecy in communication, for every single secret message there must be a new secret key. Finally, communication participants must somehow distribute a secret key between themselves (by a private talk or meeting, or with the help of a trusted courier). To sum up, there were always existed some undeniable weaknesses in these encryption methods.

Cryptography finally began to be described by mathematical instruments in the mid-70s. In 1976, the National Bureau of Standards (NBS) of the USA has registered the first crypto protocol as the national cryptography standard required for "non-critical" data encryption - DES (Data Encryption Standard). In the same year, a revolutionary paper on the new methods in cryptography [2] by W. Diffie and M. Hellman was published and marked the birth of public-key cryptography. This paper had a great impact on the whole crypto-society, and, around that time, the

RSA (Rivest-Shamir-Adleman)[3] has appeared which was de facto the first working prototype of the public-key cryptosystem. Modern cryptography is a combination of such cryptosystems, protocols, and cryptoanalysis.

1.2 Security vulnerabilities

As it was stated in the previous section, nowadays we are regarding cryptography as an area of science at the intersection of mathematics and informatics. The whole cryptographic history can be interpreted as an eternal confrontation between various encryption methods and their hackings. Each new emerging cryptosystem had in itself a set of security vulnerabilities that could be used by a potential malefactor. A permanent threat of a sensitive data compromise provoked the concerned part of society to concentrate on finding an absolutely safe approach to sensitive data protection.

The first great step in this direction was made by AT&T Bell Labs engineer Gilbert Vernam as he invented (1917) and patented (1919) his polyalphabetic cipher "One-time pad" [4]. The main idea of his method is to encrypt a secret message with a random bit sequence of the same length (a secret key). Every bit of the initial information adds up with the bit of a secret key by the operation XOR (exclusive or) in such a way, that the output encrypted line is the random bit sequence as well. This sequence cannot be decrypted without a secret key. Every possible combination of random bits in a secret key applicated to the encrypted data will output a set of all potential secret messages. The one-time pad is a classical example of an unbreakable cryptographic system.

Despite the obvious advantages of Vernam's invention, few mentioned inconveniences prevent its widespread use. In the modern globalized world, with all possibilities that the high-speed Internet has given to society and everything that is in need to be encrypted (bank transactions, private communications, medical data transfer, video/audio surveillance security systems, etc.) it is almost impossible to

imagine a scenario of many face-to-face meetings for a secret key distribution. That is why public-key cryptosystems began to develop actively in the 70s of the last century. The cornerstone of these technologies is using of one-way functions. It is relatively simple to calculate an outcome with this function for a given value, but at the same time, it is almost impossible to restore the initial value by the outcome.

The most widespread modern public-key cryptosystem is the RSA technology. The main algorithm of the RSA protocol is built around the computational complexity of factoring the product of two big prime numbers. To read the secret message encoded with the RSA method a potential eavesdropper will have to find the pair of these prime numbers which will take millions of years. There is no such algorithm that could be able to speed up these calculations.

The RSA protocol seemed to be a key to secure cryptography, but its unproven unconditional security has forced researchers in this field of science to continue their work on a completely safe and sufficient cryptosystem. In the year 1994, P. Shor has published an article [5] on a polynomial-time factoring quantum computer algorithm, which meant that with the creation of the first working quantum computer one could forget about the safety of the RSA method.

Of course, it is too early to talk about a full-fledged implementation of Shor's protocol on a quantum computer. However, there are already existed different experimental realizations of such an algorithm [6–8] which demonstrate factorization of small numbers. The further development of quantum computing technologies promises a potential risk of using the RSA cryptosystems.

A continuous increase in computational power and the RSA instability to possible quantum computer attacks have led to the search for a reliable method of encryption that will be independent of a potential eavesdropper technical and intellectual resources. The solution to this complicated problem can be viewed in terms of quantum mechanics. Researchers aim to formulate a complete cryptosystem whose security is guaranteed by fundamental laws of nature

1.3 Cryptography standards

A certification of the cryptography standard is a mandatory procedure for any state interested in the reliable protection of classified data. This term can be considered as a series of various regulated tests in order to ensure uncompromising reliability of the chosen cryptography standard. It should be noted, that the importance of this procedure cannot be overstated - state secrets and critical data will be encrypted employing this certified standard.

As it was mentioned before, the first of such a standard was DES. It was developed by an American technology company IBM and approved by the NBS as the national standard in 1976. DES is what is called a symmetric-key type algorithm for the encryption of digital data, which means that for both processes of encryption and decryption the same key is required. This cryptosystem is based on the use of a Feistel network with 16 rounds and a secret key of 56 bits of length (plus 8 additional parity bits). The Feistel network can be considered as the symmetric block structure where each block or cell transforms the given key and data by the chosen algebraic rule and transfer them to another cell in an iterative way. Although this cryptosystem has been chosen as the national encryption standard, it was cracked during the so-called "RSA challenges" - a series of full-scale tests organized by supporters of the RSA cryptosystem at the end of the XX century [9].

After the loss of confidence in the security of the DES algorithm, NIST (The National Institute of Standards and Technology, former NBS) has organized the national competition on a new encryption standard creation. This process was called AES - Advanced Encryption Standard and the announced winner was the Rijndael algorithm, which was developed by Belgium cryptographers J. Daemen and V. Rijmen. The Rijndael algorithm, which later was called by the name of the competition - AES, vaguely resembles the improved DES cryptosystem and is the most common symmetric encryption algorithm today. There are several known attacks on the AES, but none of them can be considered as a serious security vulnerability of the

protocol.

Despite the fact, that AES is a safe enough cryptosystem, in modern technologies, we are using various configurations of AES, RSA, and other protocols to speed up and maximally protect private communications. It is important to understand, that all the data that is transferred today and encrypted with mentioned methods is potentially vulnerable to future attacks with the application of quantum computer. These thoughts are worth considering especially when we are talking about the state secrets and classified data, that are in need to be encrypted for a long time (say tens and hundreds of years). There is a theorem by M. Mosca [10] which is governing these time frames. In this theorem, the author shows, that if the time needed to build a large quantum computer (Z) is much less than the sum of the time for deploying quantum-safe cryptosystems (Y) and the time that the classified data must stay secret (X), then we have problems today already (X+Y>Z). In these terms, we should seek answers to security questions in the field of quantum mechanics. The first starting point in this long run might be the key distribution problem, which is already being successfully implemented by quantum protocols.

1.4 Quantum cryptography

The first quantum revolution had its place at the end of the previous century. Among countless inventions that quantum technologies have brought to mankind at this stage, few dramatically changed the whole paradigm of human life. These days it is difficult to argue that lasers and semiconductor appliances are on the top of the leading technologies list. The "revolution" term in the main stands for the incredible ability to control the cooperative quantum properties of a large group of particles. Today, as the theory is generally accomplished, we are pleasured of using technologies of the first quantum revolution, which have evolved into mobile electronic portable devices, powerful computers, ultra-high-speed communications, etc.

Despite the unconditional importance of the mentioned breakthrough, this paper aims to focus on quantum cryptography that is one of the second quantum revolution applications, which are, on the whole, characterized by the manipulation of individual particles quantum effects. Apart from quantum cryptography, the theories of non-cloning [11–13], quantum teleportation [14–16], and quantum entanglement [17] were presented.

The birth of quantum cryptography can be linked to the idea by S. Wiesner of using the trapped photons with a certain polarization in money banknotes [18]. Even though the author could not publish his work as he finished it, the manuscript of the paper fell into the hands of scientist Charles Bennett, who later with his colleague Gilles Brassard submitted the first quantum cryptography protocol, which was named after them - BB84 [19]. The BB84 protocol is the most mature and investigated quantum cryptography technology.

The goals of modern quantum cryptography are mostly focusing on the secure key distribution problem. As it was mentioned before, in the one-time pad cryptosystem, the key distribution is one of the weakest parts of the protocol. The quantum key distribution (QKD) proven excellence is that one can share the secret key to another user of quantum communications at a distance and no one else can extract the key which is guaranteed by quantum mechanics.

1.5 Quantum key distribution protocols

There are many ways to characterize the whole diversity of the QKD protocols. From my point of view, the most convenient one - is to split them into two categories: discrete variable (DV-QKD) and continuous variable (CV-QKD) protocols. Moreover, in this paragraph, I should note the classical designations of the protocol users. In quantum cryptography, historically the sides, between which the QKD is realized, are called Alice and Bob, and the potential eavesdropper has the name of Eve.

In the DV-QKD, the transmitted information is encoded by the properties of single particles of light - for example, in polarization or phase of photons. The detection parts of the DV-QKD systems are various single-photon detectors that can be built utilizing different technologies (superconducting nanowires, photomultipliers, avalanche photodiodes). Although, it is quite hard to develop a true one-photon source, in practical DV-QKD systems faint laser pulses are used. They are obtained as a result of strong attenuation of the semiconductor-lasers pulses. Pulses are attenuated in a way, that every one of them has a probability to contain much less than one photon. This is a necessary condition for these systems, because every pulse, that has two or more photons could be split by Eve and then may be used to extract the secret key. The amount of photons per pulse follows the Poisson distribution.

The situation with CV-QKD is quite different. Instead of operating the separate light portions properties, the information is encoded in the quadratures of the spreading electromagnetic field. The mechanism of detection is built around homodyning the incoming field [20]. The CV-QKD protocols are the new chapter in the history of quantum cryptography. Although its high-speed performance on short-range systems, the unconditional security proof of these systems currently absent.

The most common protocol in modern DV-QKD systems is the BB84. Secret information in BB84 can be encoded in either phase or polarization of transmitted photons. The security of the protocol is built around the concept of quantum indeterminism - the existence of several physical properties of a particle (a photon, in this case) that cannot be measured at one time. To illustrate the essence of the protocol, I will describe its polarization-based version.

To begin with, we should consider the linear polarization of the photon in a two-dimensional Hilbert space. We can introduce two bases of the photon polarization - rectilinear (Z) and diagonal (X). Alice can prepare her photons in each of these bases - to encode a bit with value "1" ("0") she uses either a vertical (horizontal)

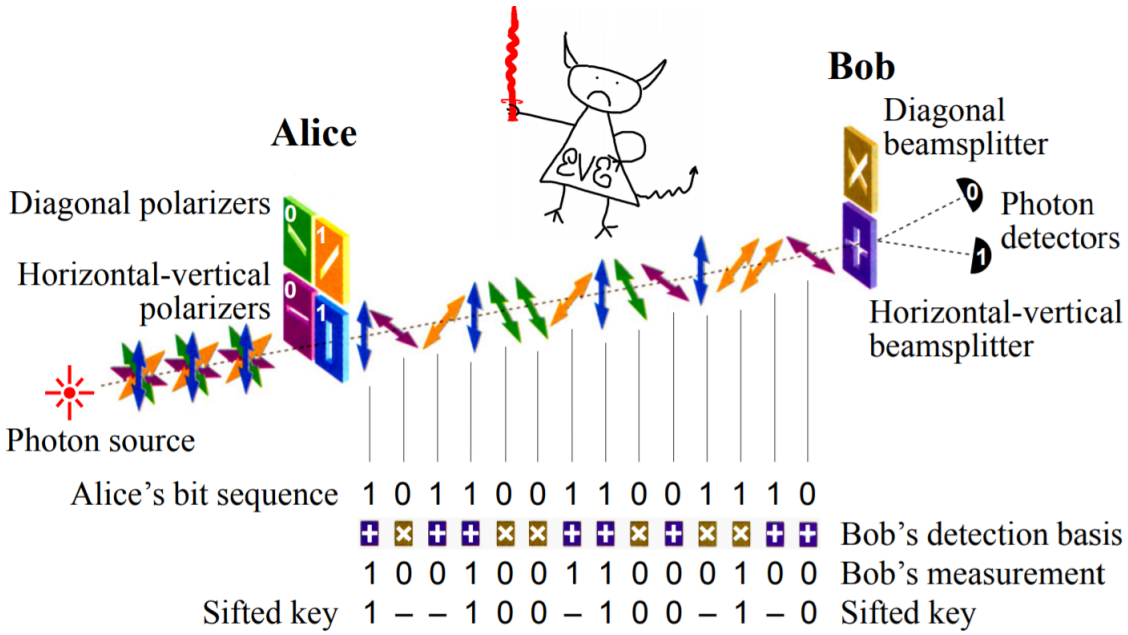

Figure 1.1: Polarization-based BB84 protocol explained (taken from [21], firstly printed in [22]).

polarization in the Z basis or +45°(-45°) polarization in the X basis. The bases are organized in such a way that, let us say, Alice has prepared one photon with the horizontal polarization (which means that she used Z basis and the encoded value is "0") and sent it to Bob, who later randomly has chosen the X basis for this photon measurement (which means, that he was wrong with the choice of the basis), he has 50% chance to detect one of the X basis states. In other words, if Alice and Bob pick the same basis, Bob with a 100% probability receives the secret bit that Alice encoded, and if their bases do not match, Bob gets one of two states of his basis each with the probability of 50%. In general, the BB84 protocol can be regarded as follows (Figure 1.1):

1. Alice generates a random sequence of bits by choosing a basis and the state of polarization in it with the help of a random number generator.

2. For every bit in this sequence Alice emits a photon with a corresponding to the basis chose polarization through a quantum channel.

3. Bob randomly chooses between bases as well and measures the polarization of

photons coming from Alice. If he is guessed right with the basis, he determines the polarization of the incoming photon, and therefore the state of the bit sent by Alice.

4. After the communication session, Alice and Bob through a public channel compare their chosen bases sequences (the polarization measurements performed by Bob are not disclosed). In about half of the cases, the bases turn out to be the same. The measurements corresponding to these cases are saved and will form the so-called sifted key, all other bits should be discarded. Under ideal conditions, the sifted key on the side of Alice and Bob is the same.

5. In real conditions, it is necessary to take into account the losses in the quantum channel, the mismatch of the bases on the side of Alice and Bob, as well as other possible errors. For this, the overall level of errors in the key is estimated, procedures for privacy amplification and hashing are applied.

6. If the steps of the algorithm are successful Alice and Bob have the same secret key. If the quantum bit error rate (QBER) exceeds the set threshold, the procedure is repeated until QBER is acceptable.

In 1992 the new quantum cryptography protocol that uses only two nonorthogonal states was introduced [23]. Despite the theoretical security of the given protocol, in a practical noisy environment, it is insecure. A good strategy was to apply a third nonorthogonal state into cryptosystem [24]. Later it was shown that these three-state protocols provide the same level of security and speed performance as the original BB84 [25].

As it was mentioned before, the true one-photon source does not exist and the amount of photons per pulse in DV-QKD systems is one of its main problems. Instead of one-photon sources, faint coherent pulses with a randomized phase are used. To prevent possible photon number splitting (PNS) attacks on the quantum cryptosystem, the new decoy-state method was introduced [26, 27]. The essence of

this approach is to apply an additional intensity modulator to the QKD system, which will randomly include informationless "decoy" pulses into the communication pulses sequence with aiming to detect a possible eavesdropper.

Along with the mentioned attacks on the quantum cryptography protocols, new ones began to appear. Imperfections in the practical realizations of QKD systems are often lead to their potential vulnerabilities. For example, there is a group of attacks, aimed at the work instability of single-photon detectors (SPDs) [28–33]. In addition to the SPD, many other devices inside the QKD system can serve as a vulnerability to a potential eavesdropper. These considerations are taken into account of the idea of measurement-device-independent QKD (MDI QKD) [34–39]. In the MDI QKD, there is the third (possibly dishonest) intermediate member of the protocol - Charlie. Alice and Bob in this protocol are sending Charlie their encoded states and he completes the measurement which is leading to the QKD range increase. At the same time, the speed performance of these systems is not very high - to extract a bit of the secret key, the states from Alice and Bob must be equal to each other and arrive at Charlie at the same moment.

The next step in this area is the twin-field QKD (TF QKD). The scheme of the protocol is much alike to the MDI QKD, but in this case, Alice and Bob are sharing pairs of optical fields with a randomized phase [40]. The TF QKD technology allows to overcome the known speed-limit threshold without using so-called quantum repeaters. Nonetheless, it is worth saying that the most studied quantum cryptography protocol with proven security is the BB84.

1.6 Intersymbol correlations

The preparation stage of the qubits (in quantum cryptography, it is possible to call encoded photons qubits) is a necessary step in DV QKD protocols. Usually, in the QKD systems, there are two special appliances, that directly perform the conversion of random bits in the secret sequence to their physical form of encoded qubits. This

is about an intensity modulator (IM) and phase modulator (PM). These instruments are usually located at Alice's side because that is where the process of encoding is happening (even in those cases, when a laser source is located at Bob's side, for example in Plug&Play QKD systems [41–43]). The necessity of two modulators is quite understandable for QKD systems that employ a BB84 protocol with decoy-state technology. The phase modulator provides a bit encoding, while the intensity modulator affords the implementation of different amplitude levels of the signal which is needed for the decoy-state technology application. Under ideal conditions, these devices are working independently perfect with each qubit. The PM provides perfect encoding of the qubit with any state on the Poincare sphere and the IM attenuates each pulse to a certain energy level whether it is a signal, a decoy, or a vacuum state. However, under the real conditions of modern high-frequency QKD implementations, there are different imperfections in modulators' performance at the stage of the state preparation. The main aim of this master's thesis is to analyze the working principles of these modulators in the real implementation of the QKD system and investigate the possible imperfections in their performance. Intersymbol correlations are one of these imperfections.

As already stated, a key feature of QKD technology is that it is ultimately impossible to steal the bits of a private key unnoticed. When measuring the carriers of the secret key, their states change and cannot be restored according to the laws of quantum mechanics. However, due to the discrepancy between practical implementations and theoretical descriptions, there are various vulnerabilities in QKD systems. In order to determine the fact of eavesdropping there exists a certain boundary of errors made in the distribution of the secret key called QBER (Quantum Bit Error Rate). If the QBER value does not exceed the threshold, then Alice and Bob believe that the secret key has not been eavesdropped on and can be used. Nevertheless, several attacks are using the various statistical imbalances which allow an eavesdropper with a certain probability to measure states in such a way that QBER does not increase [44]. In this way, the indistinguishability of the qubits is a

key condition for a safe QKD, while the different correlation effects between them can lead to secret key compromise.

The impact of the intersymbol correlations on the QKD system's security was described in [45] in detail. The security proof of the BB84 protocol assumes the presence of a single-photon source or a source of faint coherent pulses with a randomized phase. The randomness of the phases from these light sources was confirmed experimentally by various interferometric methods. This is correct for the low-repetition rate systems. Due to their low frequencies of the repetition rate, generated optical pulses in these systems have a true random initial phase. As the frequency of the clock generator gets higher the generated optical pulses may overlap each other what affects the degree of randomness of their phase, in other words, the phase of such impulses can be correlated and cannot be perceived as purely random, which indicates that these optical pulses are no longer indistinguishable. This is the potential loophole for an eavesdropper to find out the encoded secret key bits, and, to evaluate the QKD system security, we must take into account these correlation effects and assess the degree of their threat to the secrecy of the system.

Apart from intersymbol correlations in the qubit states, since the optical impulses are distinguishable there could be correlations in their intensity which is especially important for systems that use the decoy-state method. There is a paper [46] which declares an attack that utilizes these correlations in the USD (Unambiguous State Discrimination) measurement which allows Eve to distinguish the signal pulses from decoy pulses, which in a combination with PNS attack leads to secret key compromise.

Imperfections in state preparation are a serious problem on the way from the theoretical model of the QKD implementation to its real working prototype. A major attempt to characterize these effects was made in [47] with an introduction of real-world QKD implementation that is tolerant to channel losses and source flaws with an experimental application of a loss-tolerant protocol [48]. A step closer to the problem of this thesis is a consideration of various correlation effects that take place

at the high-repetition rate QKD system that was performed in [49]. The authors consider the impact of state preparation flaws (SPF) on the system's performance as well as the inter-pulse correlation effects that are taking place at modulators. A similar work [50] is focusing on intersymbol correlations in the intensity modulator. The authors proposed the idea of considering a correlation effect in a pattern-splitting way, which means that only those pairs of pulses that satisfy the pattern condition are taken into account in the calculation of the average pulse intensity.

The analysis of intersymbol correlations that could take place in a high-frequency QKD system is a major part of this master's thesis. In this work, I will describe the QKD system under study and the main principles of its operation in detail. I will show the performed experiments and their results as well. At the end of the thesis, I will finish with conclusions about the work done.

2. Consideration of the problem

In this master's thesis, I introduce the experimental work accomplished with the commercial QKD system manufactured by the Russian company QRate which is a spin-off of the Russian Quantum Center (RQC). The company presents to the market a set of high-tech products, including already mentioned QKD systems, single-photon avalanche detectors (SPADs), and quantum random number generators (QRNGs). We will focus primarily on QRate's QKD commercial system (QRate has QKD systems for educational purposes with slightly more modest performance characteristics. Hereinafter I shall consider a commercial version of the product which is the professional equipment to ensure the security of various companies at the highest level). Although the actual information about the device (blueprints, detailed schemes, various internal characteristics) is a trade secret, I will refer to the information available from the public domain [51].

2.1 QKD system under examination

The QKD system under consideration implements the execution of the BB84 protocol with the decoy-states technology application. In this system, a polarization version of the protocol is realized. Depending on the sending state ("0" or "1") Alice sets the polarization vector of each qubit in a random sequence. In this way, the values of the polarization vector angle of 90° and 135° correspond to the bit value of "1", and for the angles of 0° and 45° this value is "0" respectively. The pair of angles 0° and 90° form the rectilinear basis, while the pair of angles 45° and 135°

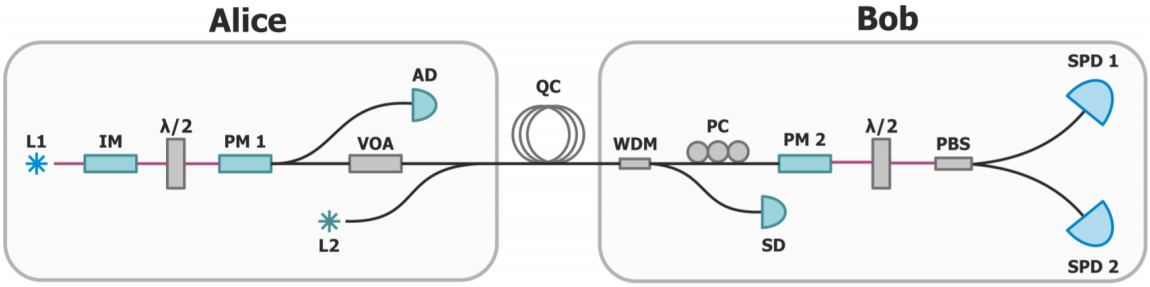

Figure 2.1: Scheme of the QRate's commercial QKD system (taken from [51], see text for details).

correspond to the diagonal basis. As it can be seen, the internal states of each basis are orthogonal to each other, while the states from different bases are not orthogonal what is done on purpose. Non-orthogonality is a useful property that allows one to track attempts of eavesdropping. According to the protocol, values of basis and bit are choosing randomly.

Let's discuss the schematic diagram of the device (Figure 2.1). The whole QKD system consists of two main blocks that are Alice and Bob stations. They are connected via two channels, one of them is a quantum channel which is the optical fiber, and another one is a classical channel - a simple Ethernet cable. The quantum channel is required for the qubits transmission and the main purpose of the Ethernet cable is a non-secret communication of Alice and Bob. Abbreviations in the figure are stated for:

1. L1 - main laser. This is a temperature-stabilized solid-state laser diode with a well-determined wavelength that is needed to emit short (100 ps or $1 \cdot 10^{-10}$ s) optical pulses for their further transformation into qubits with a high-repetition rate which is achievable with an external reference precise generator.

2. IM - intensity modulator. This device is changing the amplitudes of incoming indistinguishable pulses according to decoy-state protocol. In general, phase and intensity electro-optical modulators have the same principles of work, which will be discussed later in the next section.

3. $\lambda/2$ - polarization rotation system. Using a phase modulator (PM 1) in Alice's setup imposes restrictions on the polarization of incoming laser pulses. The polarization components along the ordinary and extraordinary axis of the birefringent crystal inside PM should be equal to each other. That is why preliminary processing of polarization is needed. The rotation system is a special polarization-maintaining optical fiber (PANDA) that is welded to at the input of the PM at a specific angle.

4. PM 1 - Alice's phase modulator. This is a device, that allows Alice to transform her secret bit sequence into states of qubits.

5. AD - amplitude detector. Thermo-stabilized precise detector, which controls the amplitude level of transmitting pulses in order to determine the appropriate attenuation on the VOA, taking into account the losses in the quantum channel.

6. VOA - variable optical attenuator. The instrument that is needed to attenuate pulses to the one-photon level of energy.

7. L2 - synchronization auxiliary laser. The repetition rate of the QKD system is 312.5 MHz thereby the internal clocks inside Alice's and Bob's stations must be synchronized with high accuracy. This laser generates pulses with a frequency that correlates with Alice's internal clock generator. These pulses are non-informative and will be processed by Bob's synchronization detector (SD).

8. QC - quantum channel. A quantum channel is an optical fiber with the lowest possible attenuation level (typically 0.2 dB/km) that is needed to transfer qubits from Alice to Bob.

9. WDM - wavelength division multiplexor. A special apparatus that separates incoming informative and synchronization pulses due to their difference in

wavelength.

10. PC - polarization controller. As was mentioned above, a polarization of pulses in front of the phase modulator should be oriented in a determined way. That is why a polarisation controller or a similar device is needed.

11. SD - synchronization detector. This detector transforms registered pulses from Alice's synchronization laser into an electrical signal, according to which the frequency of Bob's internal reference generator is adjusted.

12. PM 2 - Bob's phase modulator. Bob uses this modulator to actively choose the basis of his measurement by applying a different voltage to the device.

13. PBS - polarizing beamsplitter. A polarized beamsplitter is needed to effectively split the logical states of the same basis (determination of the value "0" or "1").

14. SPD 1,2 - single-photon detectors. High-precision SPADs that allow registering single photons.

At first, the signal laser L1 which is a solid-state laser diode generates a sequence of identical pulses with a length of approximately 100 ps each with a repetition rate of 312.5 MHz (which corresponds to the period of 3.2 ns). The signal laser works on a wavelength of around 1550 nm, which matches a so-called third transmission window (or a telecom window, C-band). Electromagnetic radiation in this range is invisible to the human eye, but it is affected by the minimum attenuation in the optical fiber.

After the generation laser pulses are going into the intensity modulator through a polarization-maintaining fiber (colored red on the Figure 2.1). In conventional optical fibers without polarization-maintaining effect despite the cylindrical symmetry, due to temperature fluctuations, mechanical stresses, and heterogeneity, the initial state of polarization necessarily changes at the end of a fiber. Hopefully,

there is a set of various polarization-maintaining technologies, which save the linear polarization of light if it was oriented along special axes of the fiber. This technology turns out to be even more useful in a combination of electro-optical modulators, that are particularly sensitive to the orientation of the polarization of the incoming electromagnetic radiation. The main principle of work of these fibers is creating a constant birefringence effect along their entire length by adding special inclusions with specific geometry in a fiber structure. These inclusions create permanent mechanical stress in fiber and cause a birefringence. In this way, two orthogonal axes with different refractive indices appear in the fiber, which affects the phase velocity of light propagation along them (that is why they are called "fast" and "slow"). There are several polarization-maintaining technologies, the most common among them are PANDA(Polarization-maintaining AND Absorption-reducing), bow-tie, and elliptical-clad.

At the intensity modulator, the decoy-state method is being implemented. The essence of this technique is to apply one of three different amplitude levels to each pulse randomly. This is a safe approach, that allows one to recognize the PNS attack by comparing the channel capacity of each chosen amplitude level. The IM is an electro-optical modulator that functions as the Mach-Zehnder interferometer which is made with a lithium niobate (LiNbO3) birefringence crystal. In such a crystal, the intensity of modulated pulses is being changed depending on the voltage applied due to the phase shift between pulse components along crystal axes caused by the Pockels effect.

After the IM pulses are transmitted into Alice's phase modulator (PM) through a polarization rotation mechanism which in this QKD system is the polarization-maintaining fiber the end of which is connected to the modulator in a way, that an angle between axes of the fiber and birefringent crystal inside the PM equals exactly 45° (detailed description in the next section). This method of rotation of the fiber not the only possible, but a very elegant solution to a complex problem.

PM 1 is another electro-optical modulator on the lithium niobate crystal, that

is needed to effectively set logical values in polarization states of photons. Pulses are being injected in PM in a way, that the amplitudes of the electric field along the ordinary and extraordinary axes are equal, which is necessary. Logical states are formed by applying one of four levels of voltage to the modulator. The electric field is acting on the nonlinear crystal inside the modulator which is causing a birefringence due to the Pockels effect.

After the PM modulation, pulses are split into two equal parts by intensity on the 50/50 beamsplitter. One part is going to the amplitude detector (AD), which is needed to calibrate the possible drift of the IM operating point and determine the attenuation on the VOA. Another part is propagating into the quantum channel (QC), getting attenuation before this to a single-photon level at the VOA. At this step, a series of powerful pulses are being generated by the synchronization laser (L2) with a different wavelength than a signal laser (L1) and transmitted along with the modulated informational pulses.

At Bob's side pulses are firstly meeting the WDM filter - a special device that is needed for effective separation of pulses with a different wavelength. In this way, synchronization pulses are going to the synchronization detector (SD), which then corrects the frequency characteristics of Bob's electronics in order to synchronize high-repetition rate processes. Due to different wavelength qubits propagate through another output of the WDM and enter the polarization controller (PM) in front of Bob's PM, where he chooses the basis for each incoming photon. After PM 2, pulses can be detected at the pair of avalanche-type SPDs, which are based on the InGaAs structures.

2.2 Electro-optical modulators

The main idea of the BB84 protocol is to distribute a secret key between parties with minimal possible leakage to an eavesdropper. In these terms, secret information is being encoded in the different physical properties of photons in a way, preventing

unnoticed theft of the key or its parts. The cornerstone of this technology is a process of encoding the qubits according to the logical values of a random secret sequence (a state preparation stage) and their decoding after transmission through a quantum channel. In the considered QKD system this encoding occurs by controlling the rotation of the linear polarization for each qubit. In this way, precise and reliable instruments to operate with polarization are needed. This section provides an overview of the most popular of them as well as defines the principles of modulators operation that are in use in the considered QRate's QKD system.

Different technologies implement the transformation of any initial polarization state into any output state. The most common of them is known as polarization controllers. There are different technical realizations of this technique but any of them operates by the birefringence effect. Birefringence is an optical property of various anisotropic materials that have a different refractive index depending on the direction of light propagation. In such materials, the initial ray of light could be split into two components with different polarizations. Each of these components is affected by its own refractive index. There are two types of birefringent materials - uniaxial and biaxial. Most of the uniaxial materials are crystals with an asymmetric crystal structure that is stretched or compressed in a certain direction which determines the optical axis of the crystal. The propagation of light in uniaxial materials depends on its initial direction and polarization. The polarization of a lightwave defines whether it is an ordinary or extraordinary wave. The polarization of the ordinary wave is perpendicular to the optical axis, and the polarization of the extraordinary wave is orthogonal to the polarization of the ordinary wave. There are three main cases of the initial direction of a lightwave. A lightwave can be propagating along with the optical axis of the crystal. In this situation, a refractive index is the same for any polarization state. Another case happens, while a lightwave travels perpendicular to the optical axis that leads to polarization splitting into two components affected by different refractive indices. Due to the difference in refractive indices, there could be a phase shift between these polarization components, which also depends on the

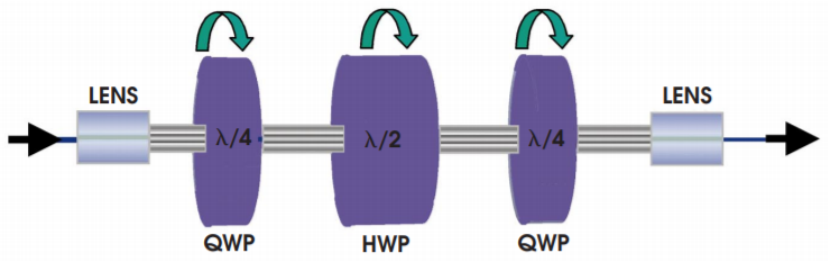

Figure 2.2: $\lambda/4$-$\lambda/2$-$\lambda/4$ mechanical polarization controller (taken from [52]).

material thickness and wavelength. A lightwave can be also directed at an arbitrary angle to the optical axis. In this case, a lightwave splits into two beams which are propagating inside the material. Biaxial materials, in turn, are characterized by two optical axes and have three refraction indices that represent three principal axes of the birefringence material.

As it was already mentioned, polarization controllers are the devices, that operate with input and output states of polarization. There are several types of these controllers that are used in different applications. The first of these types is the polarization controllers that are implemented by the instruments of volume optics. These devices consist of few optical waveplates, the most common realization is the composition of two quarter-wave plates and one half-wave plate in a determined configuration: $\lambda/4$-$\lambda/2$-$\lambda/4$ (Figure 2.2).

The changing of the polarization state is performing by the precision adjustment of angles for every waveplate which could be done manually or with external electronics. These systems are good for laboratory demonstrations but not for the industrial implementations of the QKD, due to relatively large sizes and slow rates of operation. A similar principle is used in manual fiber polarization controllers (Figure 2.3). In these systems, single-mode optical fiber is twisted in three consecutive rings. An application of mechanical stress to the fiber causes the birefringence effect and the output polarization state is depending on the radius of circles and their rotation angles.

At this step, we should move on to the electronic polarization controllers. The

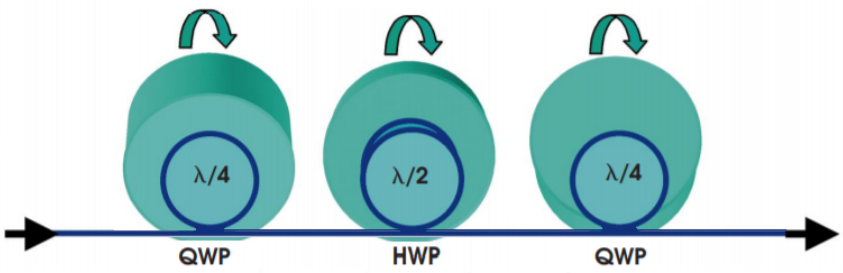

Figure 2.3: $\lambda/4$-$\lambda/2$-$\lambda/4$ fiber polarization controller (taken from [52]).

first of them is fiber polarization controllers with piezoelectric actuators [53]. In these devices, a birefringence effect is caused by the application of mechanical stress on the fiber that appears through the use of piezoelectric actuators which are connected to the voltage supply. The repetition rate of these devices is around tens of kHz, which is much better than for previous polarization controllers but still poorly applicable to the realistic high-speed QKD system. Besides, there are some disadvantages in the operation of these polarisation controllers, like hysteresis in set polarization and unwanted effects such as linearity and creep behavior that limit the whole system performance. Another principle of work is implemented in electro-optical polarization controllers. The birefringence effect in these mechanisms is caused by the Pockels effect, which will be discussed in detail later. The maximum operating frequency of such polarization controllers is around 100 MHz, which still does not match the needs of the professional QKD system.

In this way, the application of polarization controllers for fast qubits encoding is unacceptable with modern technologies. However, due to the BB84 protocol only four output polarization states are needed, which is much more modest than the functionality of the polarization controller. An application of a single Pockels cell is enough for these purposes which exactly was performed in the first demonstration of the working QKD system with BB84 implementation [54]. The Pockels effect is an appearance of birefringence in an optical medium which is induced by the external constant or alternating electric field. The relationship between applied voltage and birefringence is linear. This effect is almost inertia-free (the characteristic time is

about 10^{-10} s) which allows its use in high-frequency systems. The Pockels cell is a waveplate, based on a Pockels effect crystal (KD_2PO_4, $KTiOPO_4$, BaB_2O_4, $LiNbO_3$, etc.). One of the main parameters of the Pockels cell is a half-wave voltage V_π which defines the value of voltage that needed to be applied at the cell to change the phase of transmitted light by π. Usually, this voltage is relatively high, say hundreds and even thousands of volts. Nevertheless, a Pockels cell can be utilized as a polarization modulator in the QKD system by injecting light pulses with a linear polarization of 45° to the optical axis of the cell and applying different levels of voltage which corresponds to the phase shift of 0, $\frac{\pi}{2}$, π, and $\frac{3\pi}{2}$. Unfortunately, the realistic QKD implementation on Pockels cells is not achievable due to their high voltages of operation, bulkiness, and possible vulnerabilities in side channels.

Another excellent option is to use fiber electro-optical modulators on a lithium niobate crystal. These modulators are also based on a Pockels effect but have a much smaller half-wave voltage (on the order of few volts) and compact form factor. There are several implementations of such modulators depending on the construction technology being used. The intensity modulator (IM) (EOSPACE, USA) which is in use in the QRate's QKD implementation is made on a $LiNbO_3$ crystal and based on a Mach-Zehnder interferometer with arms of equal length.

In such modulators, the initial ray of light is separated by a 50/50 Y-beamsplitter at the input and then recombined by the similar Y-beamsplitter at the output. The modulator is built in a way, that these two paths for separated light components are equal and represent arms of the Mach-Zehnder interferometer. The configuration of these modulators implies the presence of planar electrical electrodes that are used for inducing an electric field for modulation (RF electrodes) and setting the operating point (DC electrodes). The electric field by RF electrodes with the help of the Pockels effect causes the opposite changes in the refractive index of both waveguides (due to birefringence) which determines the phase shift between light components in the interferometer. As a result, at the output of this modulator, the intensity of light is depending on the interference of these light components that is controled by

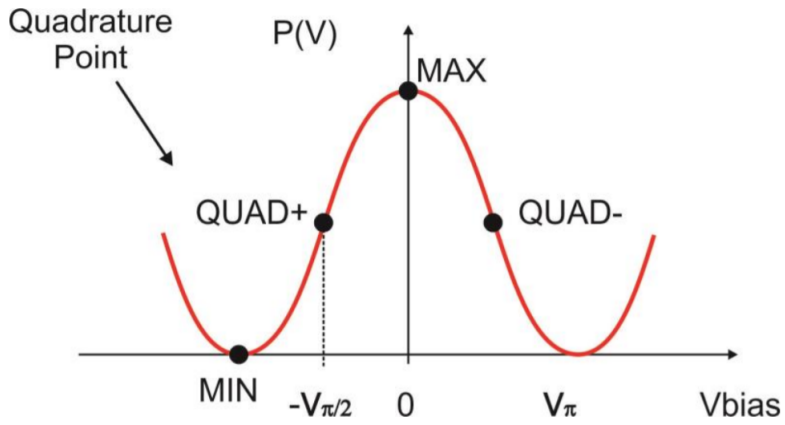

Figure 2.4: Transfer function of the IM (taken from [55]).

the applied voltage which is necessary due to the decoy-state technique.

The interaction between the applied voltage on the RF electrodes and the output intensity is defined by the so-called transfer function (Figure 2.4). This function can be written as:

$$I(t) = T_{mod}\frac{I_0}{2}\left(1 + \cos(\frac{\pi}{V_\pi}V(t) - \phi)\right) \tag{2.1}$$

with:

- $I(t)$ - output intensity
- I_0 - input intensity
- T_{mod} - optical transmission of the modulator
- V_π - half-wave voltage
- ϕ - phase shift between components

The presence of the ϕ term in the equation 2.1 is explained by the non-equality of the Mach-Zehnder interferometer arms. In the perfect theoretical description, these arms have the same length and $\phi = 0$ but it is impossible to perform that in real modulators, so the ϕ term is always nonzero. By the transfer function, it is possible to define the most suitable operating point around which the modulation

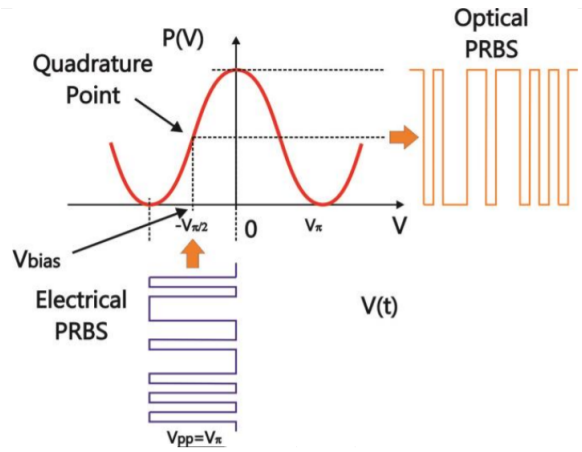

Figure 2.5: Defining the operating point on the transfer function of the IM (taken from [55]).

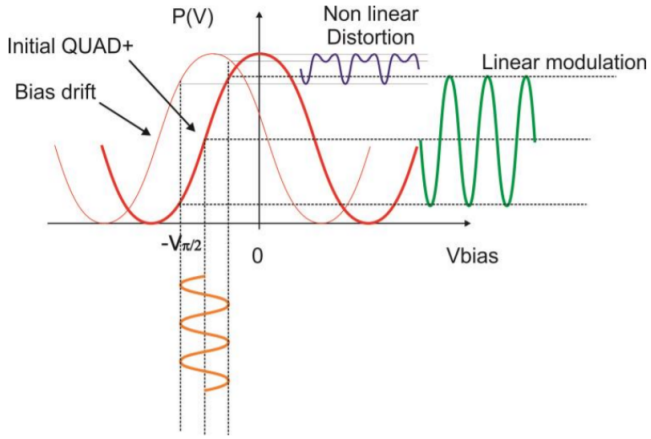

Figure 2.6: Demonstration of the transfer function drift (taken from [55]).

signal from RF electrodes will be applied. One can set this point by applying a bias voltage to the pair of DC electrodes (Figure 2.5).

During the long-time operation, temperature instability, and charge drift, the transfer function can fluctuate along X-axis (Figure 2.6). This leads to an incorrect definition of the operating point which then strongly affected the quality of intensity modulation. In this way, an external source should provide a stable and well-suited bias voltage to the DC electrodes. In the described QKD system, to prevent the possible drift of the operating point, the active feedback loop is employed, using the amplitude detector (AD) at the output of the intensity modulator.

At the sides of Alice and Bob, there are identical phase modulators (PM, EOSPA-

CE, USA) implemented. The main principle of work of these modulators is almost the same as in the IM, but these modulators do not have the Mach-Zehnder interferometer in their design. Instead of the Mach-Zehnder interferometer technology, in the PM there is only one waveguide that is affected by the electric field from the RF electrodes which is causing the Pockels effect and changes the phase of a transmitted light pulse.

In order to figure out how these modulators affect the polarization states of the incoming pulses, let us take a closer look at the theoretical aspects behind the operation, which are demonstrated in [51] in detail. To begin with, it is worth saying, that it is very convenient to describe the polarization states in terms of the Jones calculus, which is the method that was invented in 1941 by R. C. Jones. In this technique, polarized light can be expressed as a Jones vector, while different optical instruments (as the described PM) are represented as Jones matrices. The initial polarization state of an incoming to the modulator wave can be represented as:

$$\begin{pmatrix} E_{0o}e^{i\phi_o} \\ E_{0e}e^{i\phi_e} \end{pmatrix}, \tag{2.2}$$

with E_{0o} and E_{0e} which are the polarization amplitudes along ordinary and extraordinary axes of the $LiNbO_3$ crystal respectively. We can rewrite them as $E_{0o} = A$ and $E_{0e} = B$ for convenience and simplify the expression, leaving only the phase difference term $\phi_{dif} = |\phi_e - \phi_o|$:

$$\begin{pmatrix} A \\ Be^{i\phi_{dif}} \end{pmatrix}. \tag{2.3}$$

The phase modulator is expressed as the Jones matrix with zero off-diagonal terms:

$$\begin{pmatrix} e^{i\phi_o} & 0 \\ 0 & e^{i(\phi_e+\Delta\phi)} \end{pmatrix}. \tag{2.4}$$

In this matrix, the terms $\phi_{o,e}$ represent the assuming phase shift of propagating wave along the corresponding axis of the birefringent crystal, while $\Delta\phi$ is the phase shift

under applied voltage conditions. Let us consider the interaction between modulator (2.4) and lightwave (2.3) with different phase shifts, that are denoted as $\Delta\phi_{1,2}$:

$$\begin{pmatrix} e^{i\phi_o} & 0 \\ 0 & e^{i(\phi_e+\Delta\phi_1)} \end{pmatrix} \begin{pmatrix} A \\ Be^{i\phi_{dif}} \end{pmatrix} = \begin{pmatrix} Ae^{i\phi_o} \\ Be^{i(\phi_{dif}+\phi_e+\Delta\phi_1)} \end{pmatrix}, \tag{2.5}$$

$$\begin{pmatrix} e^{i\phi_o} & 0 \\ 0 & e^{i(\phi_e+\Delta\phi_2)} \end{pmatrix} \begin{pmatrix} A \\ Be^{i\phi_{dif}} \end{pmatrix} = \begin{pmatrix} Ae^{i\phi_o} \\ Be^{i(\phi_{dif}+\phi_e+\Delta\phi_2)} \end{pmatrix}. \tag{2.6}$$

To achieve orthogonality of each basis we should equate (2.5) and (2.6) to zero and find their scalar product, which then can be represented as:

$$A^2 + B^2 e^{i(\Delta\phi_1-\Delta\phi_2)} = 0, \tag{2.7}$$

which defines the main condition of the states orthogonality in basis:

$$A = B, \tag{2.8}$$

$$\Delta\phi_1 - \Delta\phi_2 = \pi + 2\pi n, n \in \mathbb{Z}. \tag{2.9}$$

In this way, to encode the qubit with one of the basis states, as was already mentioned, we need to ensure the equality of the polarization amplitudes along the crystal axes. For this, the mentioned polarization rotation system is used. The phase shift of π, which is obtained by the different voltage levels, is needed for creation a pair of the orthogonal states in the same basis. In this way, by varying the voltage at the RF electrodes of the PM, we can encode the qubits with phases 0 and π which correspond to the states:

$$\begin{aligned} |\psi_1\rangle &= \tfrac{1}{\sqrt{2}}(|\leftrightarrow\rangle + e^{i\phi_1} |\updownarrow\rangle), \\ |\psi_2\rangle &= \tfrac{1}{\sqrt{2}}(|\leftrightarrow\rangle + e^{i(\phi_1+\pi)} |\updownarrow\rangle). \end{aligned} \tag{2.10}$$

These are the orthogonal polarization states of the same basis. To achieve the BB84 requirements, we can introduce the second basis which states are shifted relative to

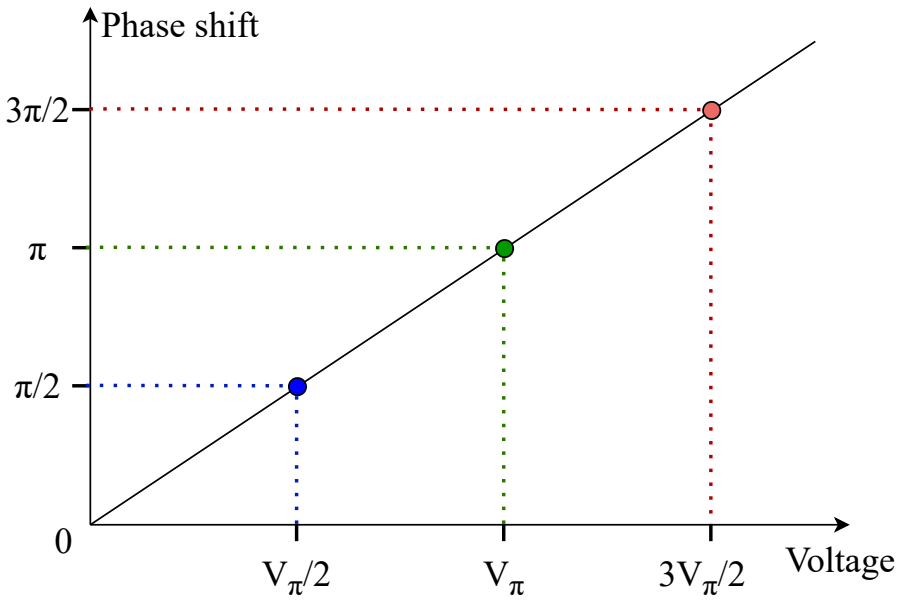

Figure 2.7: An application of the phase shift from the PM to a lightwave versus the voltage on its RF electrodes.

the first basis states by the $\frac{\pi}{2}$. The states of the second basis are:

$$\begin{aligned} |\chi_1\rangle &= \tfrac{1}{\sqrt{2}}(|\leftrightarrow\rangle + e^{i(\phi_1+\frac{\pi}{2})}\,|\updownarrow\rangle), \\ |\chi_2\rangle &= \tfrac{1}{\sqrt{2}}(|\leftrightarrow\rangle + e^{i(\phi_1+\frac{3\pi}{2})}\,|\updownarrow\rangle). \end{aligned} \tag{2.11}$$

Taking (2.10) and (2.11) into account, we can introduce a relationship between phase shift, that the PM applying to lightwave, and the voltage on its RF electrodes (Figure 2.7). In contrast to the IM, the intensity of the output light is not changing during the operation of the PM (if we are not taking into account the permanent attenuation of light from the birefringence crystal). The phase of a lightwave is changing linearly according to the voltage supplied to the PM. In this way, to achieve 4 different states of the polarization of the output lightwave, we need to apply 4 various phase shifts which are corresponding to the 4 levels of voltage that are mentioned above (Figure 2.7).

3. Experimental work

3.1 Experiment description

As it was demonstrated in [49, 50], the stage of states preparation is a bottleneck of QKD systems security. The states, that are generated by the intensity modulator, should only differ by their intensity, whether they are signal, decoy, or vacuum. Moreover, the states of equal intensity should be absolutely indistinguishable. The same goes for the operation of the phase modulator, pulses of which (at the same amplitude level) should differ only in the polarization if they are not of the same basis and state. As practice shows, in the high-repetition rate modern QKD systems implementations, there exist various correlation or intersymbol effects between adjacent pulses, which is a serious vulnerability. Due to these effects, a potential eavesdropper can, in theory, predict the state of the pulse based on the measurements of the adjacent predecessor pulse and the statistical analysis of intersymbol artifacts. In this way, the main goal of the experimental work performed is to describe the presence of these correlation effects in the commercial QKD implementation.

As was already mentioned before, in this experimental work I will focus primarily on investigating these correlation effects in the electrical pulses, that are applied to both modulators. I will introduce the experimental setups, describe the methods, and provide the results.

At first, let us describe the main parts of Alice's setup that are being tested (Figure 3.1). The control signals are firstly generated by the inbuilt FPGA (Field-

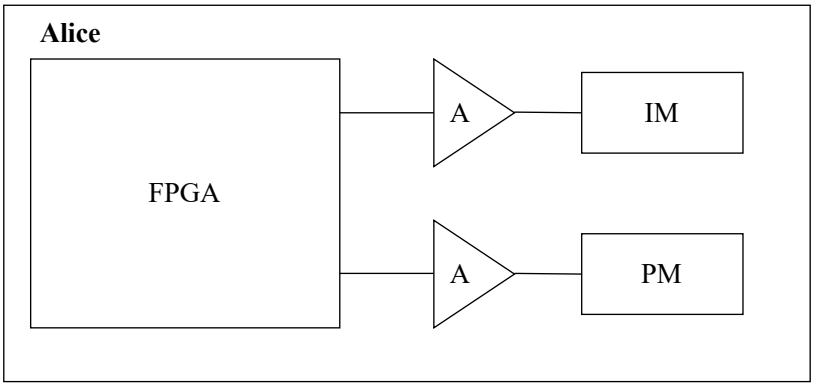

Figure 3.1: Schematic view of Alice's setup.

Programmable Gate Array, let us name it as "the main FPGA"), which combines functions of the motherboard and supports communications with peripheral devices. This FPGA is driven by a 2.5 GHz Intel® Quad-Core Pentium® Processor, which allows forming different service pulses with a high frequency and variable length. After the signals are generated, they are proceeding through a RF cable to the amplifiers' sub-FPGAs. The initial controlling signals from the main FPGA have an explainable low amplitude (much below 1V), therefore they need amplification (the V_π value for both modulators is about a few volts). After the amplification, signals are propagating to the RF electrodes of the modulator (which is true for both of them), where they are needed as a required modulation attribute. It should be said that initially two series of measurements were planned, which would more fully describe the observed correlation effects. In one of these series, the signal would be measured from the outputs of the main FPGA, which is implemented in this work, and in another series, the same signal would be measured after amplification on Alice's amplifying boards (marked with the "A" letter in the Figure 3.1). Both series of measurements were carried out, however, when processing the experimental data of the signals measured with the amplifier, a strong non-uniformity in the distribution of states was found, which indicates a non-linear nature of the amplification, especially at high voltages (from 5 volts). The author decided not to include this series of measurements in the work, since it requires more careful further consideration. It should be said right away that the correlation effects will be determined in

mathematically modulated optical pulses based on the measured electrical pulses. There are several reasons to initially carry out the experimental work in this way. In order to measure the electrical signal taken from the main FPGA, it only needs to disconnect the amplifier boards and connect the oscilloscope, while the measurements of the optical signals require the creation and calibration of an experimental optical setup, in which the necessary parameters will be effectively measured, and the schemes of the experimental setups for the two modulators are different. Under conditions when it is possible to comparatively accelerate this process by first carrying out measurements of the electrical signal, it was decided to do so, since qualitatively performed measurements with subsequent modulation could show the results of a complete absence of correlations, in which there would be no need for optical experiments. On the other hand, the comparison of the results obtained by the measurements of the electrical and optical pulses will give a more complete picture of the describing correlation effects than measuring only optical pulses. From the same point of view, it is wrong to refuse to carry out measurements with optical pulses in the presence of the correlation effects in the results of the electric pulses measurements. The formation of a vulnerability in the security of a system cannot be interpreted without the final attendance of an effect in optical measurements, because the electrical signals inside Alice's block are considered to be safe and cannot be used by Eve to reveal the secret key, while the optical pulses are leaving the safe area of Alice's side.

The experimental work was carried out as follows. At the first stage, the RF cables were unplugged from the RF inputs of the amplifiers and connected to the channels of the high-speed Teledyne LeCroy (816Zi, 40 GHz discretization frequency, 16 GHz bandwidth) oscilloscope. The examinated output ports of the main FPGA have the RF SMA 3.5 mm connectors (the same connectors are placed on the amplifiers' circuit boards). They were connected to the high-frequency channel of the oscilloscope through the so-called "K-type" adapter, which provides the connection of the RF cable's SMA 3.5 mm port to the 2.92 mm K port of the oscilloscope

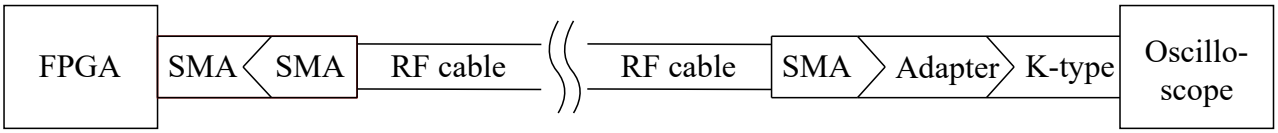

Figure 3.2: A connection between the main FPGA and the oscilloscope.

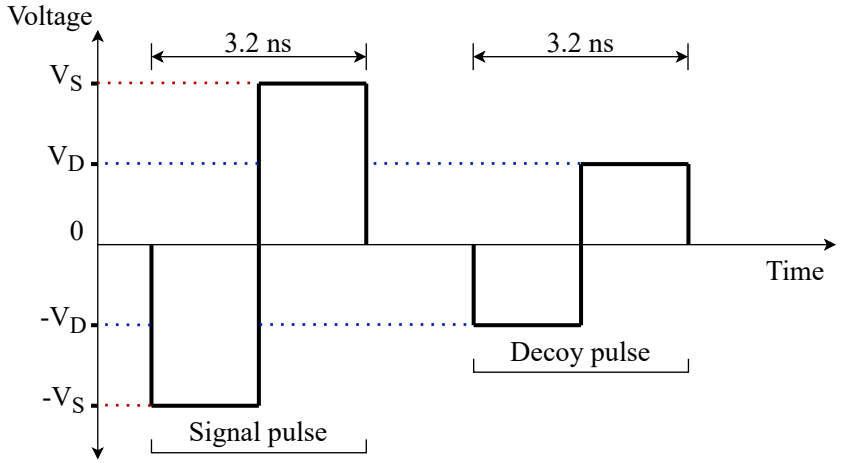

Figure 3.3: Demonstration of the signal and decoy pulses.

and implements the functions of the LeCroy's ProLink interface (Figure 3.2). Voltage measurements were performed in cycles (due to the presence of only one 2.92 K-type adapter; moreover, the crosstalk between oscilloscope channels with simultaneous measurements could increase the noise on the oscillograms): the first part of the measurements was made with the connected IM, the second part with the connected PM. The investigated pulsed signal, as mentioned, was produced by the main FPGA, and its characteristics were determined by QRate software provided. In this way, to analyze the correlation effects in the electrical pulses propagating to the IM, the form of the pulses for each state (signal, decoy, vacuum) was determined as the bipolar rectangular meander (Figure 3.3). Impulses have a well-defined length of 3.2 ns which corresponds to the repetition rate of the QKD system - 312.5 MHz. The clock generator inside the main FPGA highly depends on the frequency rate of the Intel® processor and has the same working frequency of the 2.5 GHz, which is 8 times higher than the requested frequency. With keeping that in mind, it is possible to discretize each pulse on 8 equal parts and manage the amplitude of each

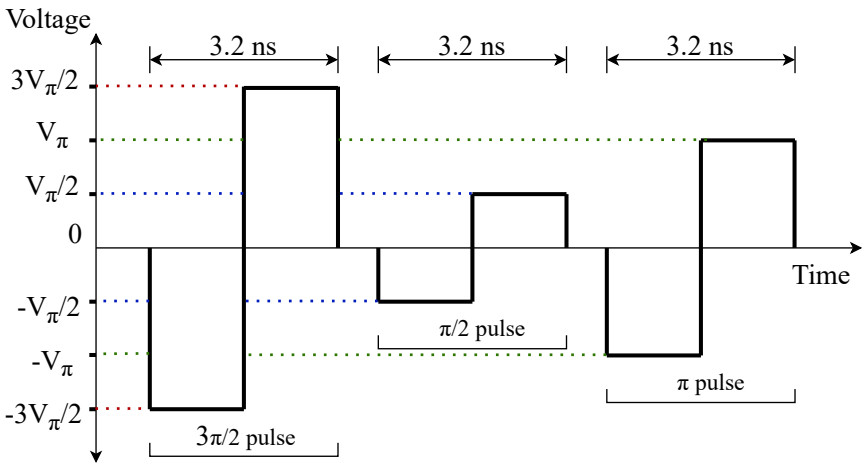

Figure 3.4: Demonstration of the all possible amplitude levels for the PM pulses.

part with the help of QRate software. Nevertheless, this ability is redundant for our experimental session. In this way, the four first parts of the signal have the same amplitude of $-V_{S,D}$, and the four parts of the pulse second half have the amplitude of $V_{S,D}$. It is worth not forgetting that the operating point of the IM is setting by the DC voltage, which in our experiment will be presented by mathematical modeling. On the oscilloscope, the operating mode with the highest possible resolution was chosen. In this mode, the oscilloscope captures the signal for about 5 ms with a resolution of 25 ps which corresponds to the measurement file with 200 million points each of which is represented as a row with amplitude and time values. After the setting of voltage levels was performed and the oscilloscope was prepared, the QKD system was turned on into the regime of key distribution. During this process, the signals are proceeding to the channel of the oscilloscope as if it would be the intensity modulator. There were three series of distribution with different regimes: in the first series the states (signal, vacuum, and decoy) were mixed, in the second session there were only signal and vacuum states, and in the third session there were only decoy and vacuum states. This was done in such a way that at the outcome of the measurement three files were received: one consisted of the mixed states is needed to determine the correlation effects between the states, as they mixed as in the real QKD process, other two are necessary to calculate the intensities of the

decoy and signal solitary impulses in order to compare these "pure" intensities with ones from the mixed-states file.

In this way, three files with the IM data pulses were produced in the series of direct measurements of the signals from the main FPGA. The same methods were obtained at the cycle of the PM measurements: four files were received after direct measurements of the pulsed signal.

The process of the PM pulses measuring was much alike to the IM data pulses collection but in this case, 4 files were received: a file with a mix of states (Figure 3.4), and one file for each amplitude level.

3.2 Phase modulator

At first, let us describe the part of the PM measurements that was accomplished by direct connection between the oscilloscope and the main FPGA. The shape of real pulses (Figure 3.5) due to various distortions in the electrical path is slightly different from their theoretical description (Figure 3.4). However, as it can be seen in the Figure 3.5, the characteristic bipolar meander form is presented and we can clearly identify three different types of pulses, which are corresponding to the phase shifts of $\frac{\pi}{2}$, π, and $\frac{3\pi}{2}$. According to the phase shift-voltage relationship of the PM (Figure 2.7), there is no need to apply an additional type of pulses for the zero phase shift. It should be borne in mind that these amplitude levels which are generated by the main FPGA in conditions of the amplifier absence are too low for the real phase modulation (the half-wave voltage of the PM is V_π=4.9 V), but they can be normalized by the further mathematical modeling. It is important to note that on the oscillogram of the PM electrical signal, with the naked eye, manifestations of correlation effects are noticeable, which consist in different levels of the signal amplitude of the same state, depending on the type of the predecessor signal (Figure 3.6). These correlations are cannot be the manifestation of the measuring error of an oscilloscope or a systematic error, otherwise, such errors would have the same effect

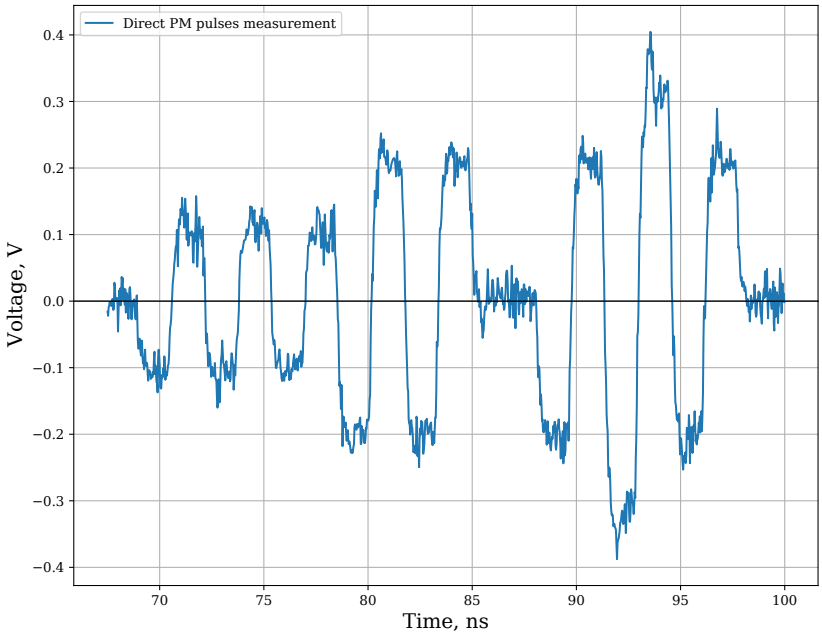

Figure 3.5: The oscillogram of the PM pulses measured directly.

on all impulses, regardless of the state. The same applies to the applied filtering algorithm, which effectively smooths out high-frequency noise, but leaves the pulse shape unchanged.

As it can be seen from the Figure 3.5, the pulses form is noisy, which requires additional filtering. The raw unfiltered data, obtained from the oscillograms can also be used for further work. Nevertheless, it was decided to filter out the experimental data, since each measured file contained two hundred million measured points and the probable noise would accumulate, which on such a data range would lead to an incorrect description of the observed effects. For the digital filtering process, the Savitzky-Golay filter was chosen. This filter is one of the most popular and reliable anti-aliasing filters. At the same time, its structure is quite simple and allows one to save computing resources of the PC during the processing of a large array of measured experimental data. The mechanism of the filter is based on a way, that each filtered value can be calculated as a combination of values on the smoothed interval, in other words, a complex operation of polynomial approximation, which

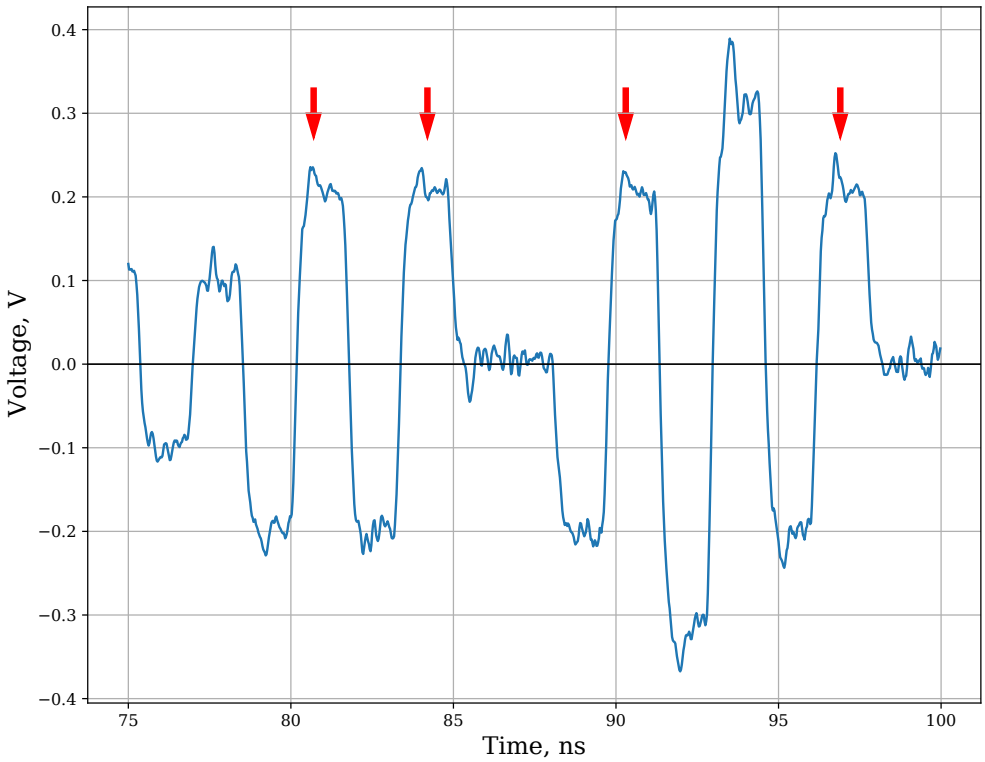

Figure 3.6: A fragment of the PM electrical signals measured oscillogram. Red arrows denote the possible correlation effects of the same signal state (in this case, a decoy state).

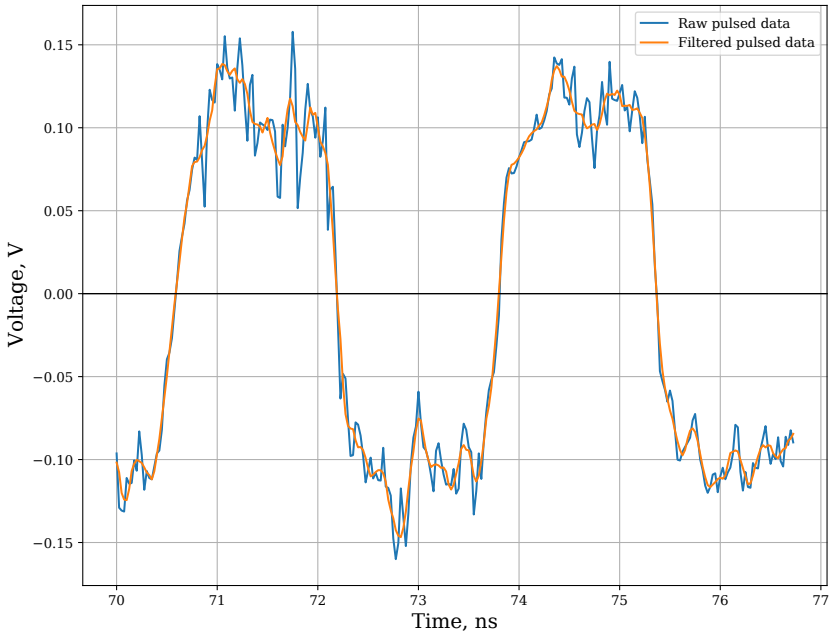

Figure 3.7: The application of digital filtering.

is the basis of the filter, can be replaced with discrete convolution, reducing the computational complexity [56]. The length of the filter window was chosen as 11 points, and the order of the polynomial used to fit the samples was chosen to 2. These parameters were chosen in such a way as not to greatly distort the original signal by smoothing, but at the same time to get rid of high-frequency noise. The comparison between noisy raw data and filtered pulses can be seen in Figure 3.7. As the pulses have much smaller amplitudes than needed for the phase modulation, the characteristic linear phase-voltage relationship (Figure 2.7) should be normalized according to these values. At the stage of setting the amplitude level for each type of pulse (for the phase shifts of $\frac{V_\pi}{2}$, V_π, and $\frac{3V_\pi}{2}$), which was performed with the QRate software, there were different values of voltages set, than ones that were measured because of the absence of the amplifier in the experimental setup (measurements with the amplifier will be presented further). However, these not-amplified pulses anyway still have corresponding amplitude levels only on a different scale. We can extrapolate these amplitude levels to the corresponding phase shifts and thus

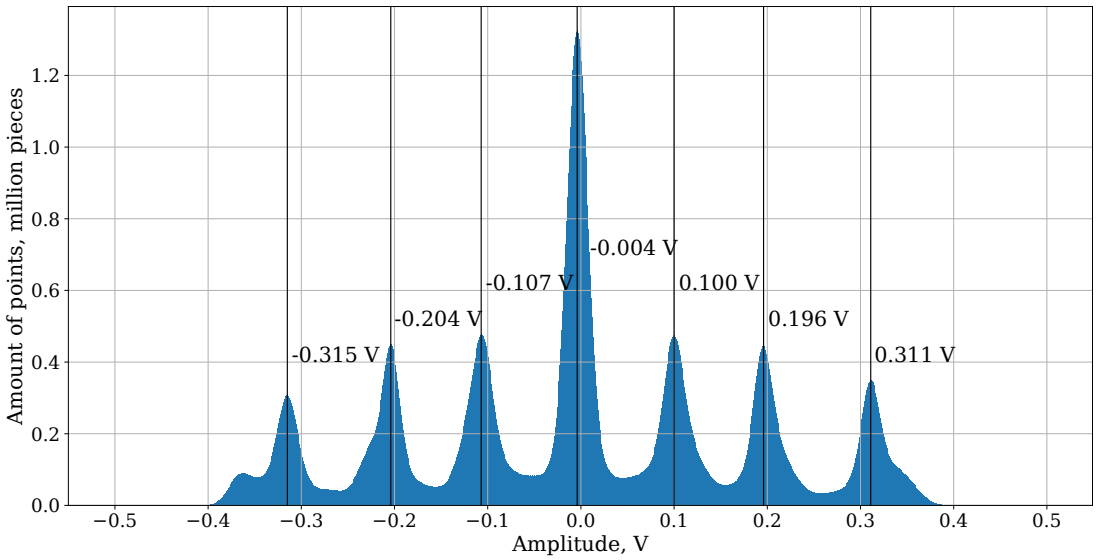

Figure 3.8: A histogram of the points' amount distribution from their amplitude in volts.

estimate the intersymbol correlations but at first, we need to determine them. It is relatively easy to do with the distribution of the points amount from the amplitude (Figure 3.8) This figure shows the number of points for each voltage value in the range from -0.5 volts to 0.5 volts. As each pulse is represented as the bipolar meander with one of three levels of amplitude, there are six peaks in the Figure 3.8. The seventh peak which is near the zero voltage value represents the states of zero phase shift and transient processes between pulses of different amplitudes. With this distribution, we can define the values of each phase shift voltage (Table 3.1). To effectively use these values in the mathematical model of the phase modulation they should be approximated by the least square method. The approximated values of voltages are represented in the Table 3.1 and the achieved approximation function, that is needed for further modeling is:

$$V = 0.065595\phi - 0.003286, \tag{3.1}$$

with V - voltage on the RF electrodes of the PM and ϕ - applied phase shift. The approximation result can be viewed in the Figure 3.9.

Table 3.1: Values of voltages with corresponding phase shifts.

Phase shift, rad	$-\frac{3\pi}{2}$	$-\pi$	$-\frac{\pi}{2}$	0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$
Meas. voltage, V	-0.315	-0.204	-0.107	-0.004	0.100	0.196	0.311
Approx. voltage, V	-0.312	-0.209	-0.106	-0.003	0.100	0.203	0.306

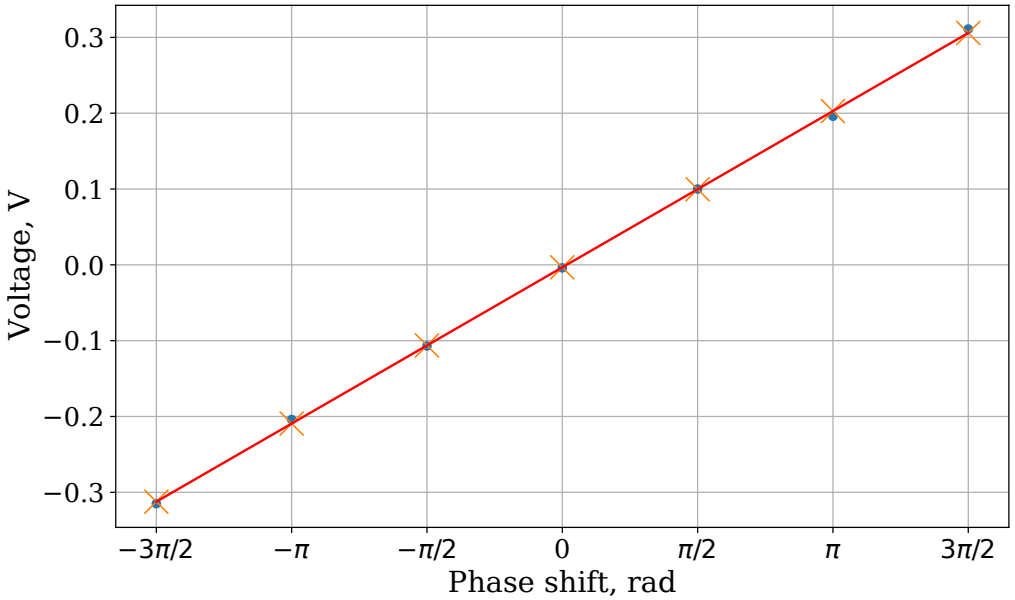

Figure 3.9: Approximation function (red) of the voltage by least squares method (measured voltage values - blue dots, approximated values - orange crosses).

As we now clearly understand how applied voltage would change the phase at the output of the PM, we should determine the presence of the intersymbol correlations in the phase deviations. As was already mentioned, the length of the light pulse emitted from the main laser L1 (Figure 2.1) is 100 ps, which means that only a small portion (let us call it "an optical window") of the applied 3.2 ns electrical pulse to the PM will take a part in the phase modulation (we consider the ideal conditions, where the PM and laser source are perfectly synchronized). In this way, we should virtually choose the window in the PM pulse, where the modulation would be performed. Unfortunately, there are no strict rules about this window

"placement", except for one: window should be placed at the most smooth positive area of the pulse with the stable voltage. That means, that in our modeling we will place the optical window after the transition from negative to a positive area of the IM pulse. The optical pulse was placed in the range of 2.2 ns to 2.3 ns from the start of the electrical pulse. These times are fully correspond to the given requirements and are located on the smooth part of the electrical pulse, not distorted by the transient process. To simplify the simulation, the pulse shape was chosen as rectangular, although to increase the simulation accuracy in further studies it is worth applying its more realistic model.

The mathematical modeling was accomplished as follows. At first, the whole sequence of measured points proceeded with the pulses detection algorithm. With precisely matched parameters for every electrical PM pulse, the following parameters for each pulse were determined: length, start and stop times, type of the pulse ($\frac{\pi}{2}$,π,$\frac{3\pi}{2}$). Then, with knowing the start and stop times of each pulse, it was relatively easy to place the 100 ps optical window at its positive plain part and calculate the corresponding phase with the approximation function (3.1). The next step was to determine 12 pair patterns and calculate the average phase of the second pulse in pair. The result of the calculation is presented in the Figure 3.10.

3.3 Intensity modulator

The pulses from the main FPGA in the series of the IM measurements had the same distorted bipolar meander form, as they had in the measurements of the PM signals. It is important to note, that, unlike the PM measurement session, the output optical signal of the IM has a non-linear relationship with the voltage applied (Figure 2.5). It is a cosinusoidal dependence, which, nevertheless, has linear sections, that are around the so-called quadrature points (Figure 2.5). By applying the voltage to the pair of DC electrodes, we can move the operating point of the IM exactly on this point, which corresponds to half of V_π (V_π of the IM described is 3.9 V). The IM

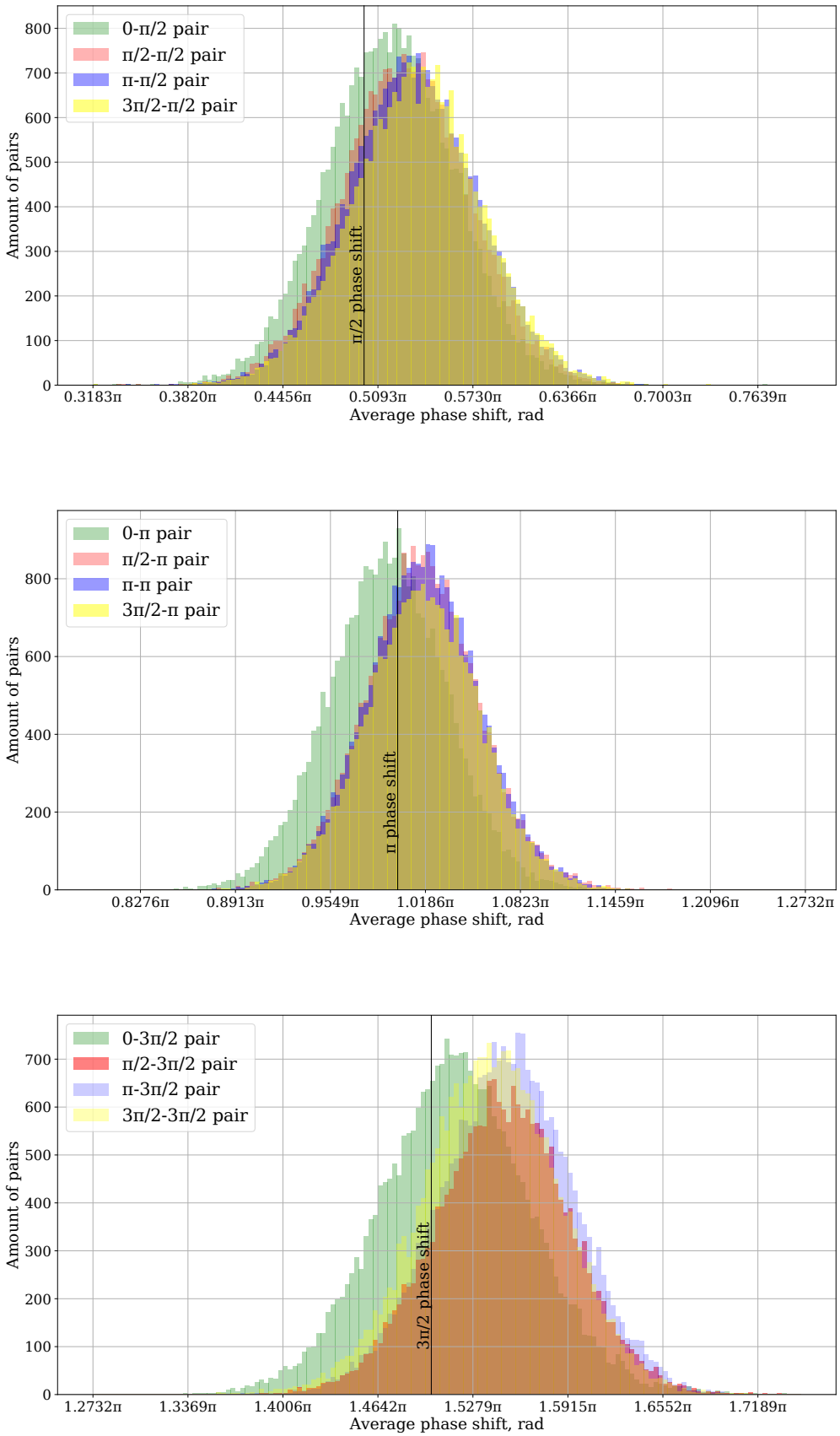

Figure 3.10: The comparison of the measured average pulse phase shift.

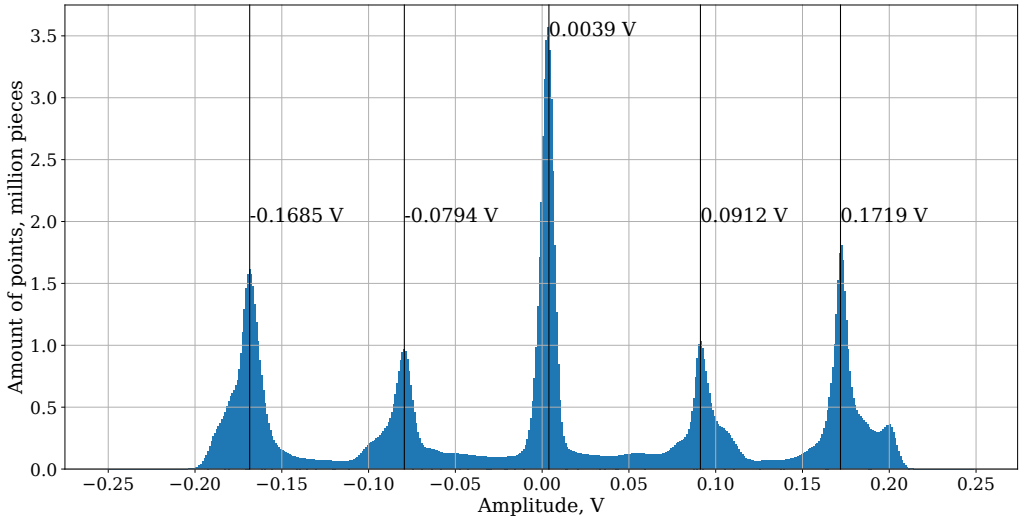

Figure 3.11: A histogram of the points' amount distribution from their amplitude in volts.

of the QRate QKD system is made with this technology application, which means that there is a separate low-frequency output on the auxiliary control board which energizes the pair of DC electrodes. In these terms, it is possible to extrapolate the normalized values of the measurements without an amplifier, which has the following amplitudes distribution (Figure 3.11) As it can be seen from Figure 3.11, the distribution of the amplitudes of the pulses is quite similar to the one of the PM, but in this case, there are only 5 peaks which are easy can be explained by the presence of only two states of amplitudes for the pulses - decoy and signal. The peak around 0 value of the voltage, as it was in the PM measurements, due to the vacuum states (which have zero amplitudes) and transition processes. From this distribution, we achieve the value of V_π. It is important to note, that in our modeling we can set any value of the DC voltage thereby we can work as if we set the DC voltage corresponding to the quadrature point. In these terms, the normalized averaged measured values of the signal states would represent half of the V_π, which in our case equals 0.1719 V. In this way, by modeling the electrical pulses with the cosine transition function of the PM and comparing the 6 patterns of pairs we have

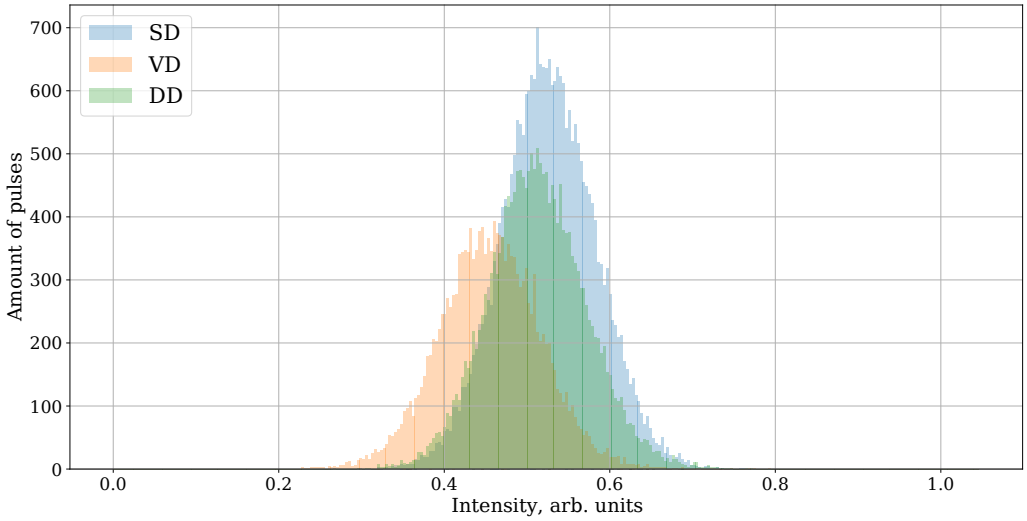

Figure 3.12: A distribution by the areas of the different patterns of pairs with the second decoy pulse.

obtained distributions of the second pulse in pair mean intensities. It should be said that the Figure 3.12 with the distributions of the decoy pulses deserves special attention here which clearly shows the heterogeneity in the mean intensities. Also, in these measurements the intensity level of the vacuum states was chosen as 0, which explains the lack of a third figure with SV, DV, and VV pairs. There were no pulses with a vacuum state - they are represented in the VS and VD pairs as the absence of a signal. Usually, in QKD systems, vacuum pulses still have an intensity, albeit very small (about 0.01-0.05, at a signal state pulse intensity of 1.00), in this study, the level was chosen as 0 following [50], where similar measurements took place at zero intensity of the vacuum state. Nevertheless, an investigation of the correlations for vacuum pulses with non-zero intensity might be one of the stages of further work.

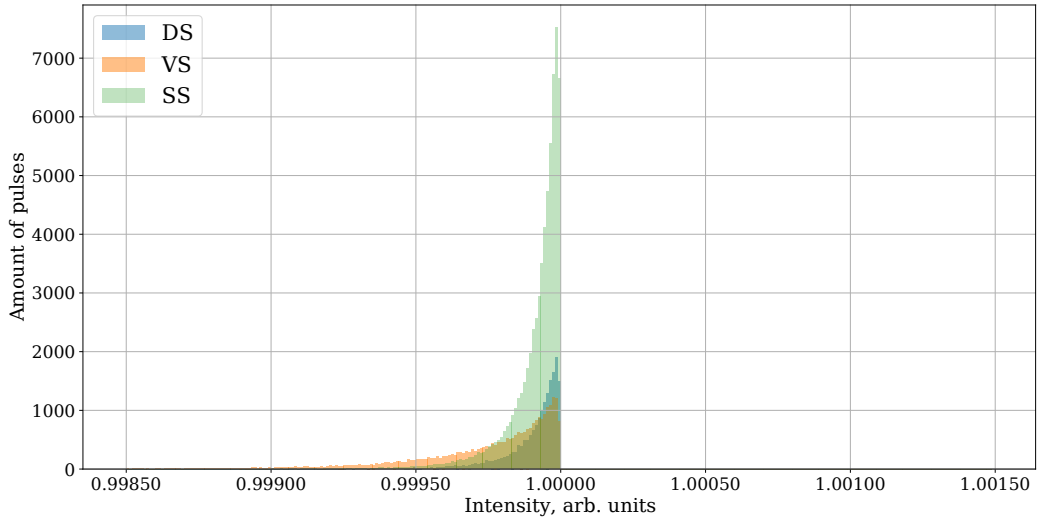

Figure 3.13: A distribution by the areas of the different patterns of pairs with the second signal pulse.

3.4 Results

The provided distributions (Figures 3.10, 3.12, and 3.13) of the average phase and intensity values should be considered as the main results of the work done. In this way, Figure 3.10 depicts three cases of the second modulated optical pulse in pair (the top subplot shows the distributions for a $\frac{\pi}{2}$ state, middle subplot - for a π state, and lower subplot for a $\frac{3\pi}{2}$ state), which are propagating through the phase modulator. Each of these cases is represented by a subplot, each of which presents four distributions depending on the state (0, $\frac{\pi}{2}$, π, and $\frac{3\pi}{2}$) of the first pulse. All three subplots show the corresponding black line of the pure state, which shows the degree of deviation of the experimental data. As it can be seen, there is a strong deviation of the distribution of the state with the phase shift of 0 as the first modulated optical pulse in pair, which can be interpreted as a manifestation of intersymbol interference between optical pulses in this mathematical model.

The Figures 3.12, 3.13 show the distribution of the normalized pulse intensity depending on the number of modulated optical pulses, which are propagating in the

intensity modulator. In this way, in the Figure 3.12 there are three distributions according to three different preceding intensity states (signal, vacuum, decoy), while the second pulse has the decoy intensity. As it can be seen, the increase in the intensity level of the first in pair optical pulse state leads to increased intensity of the second in pair decoy optical pulse. In Figure 3.13 represented the mentioned distributions for the case of the signal intensity of the second pulse. Unlike the decoy state distributions (Figure 3.12), all signal states, regardless of the first pulse, have approximately the same intensity.

4. Plans for an optical experiment

4.1 Necessity

The observed in this work correlation effects in the properties of the mathematical-modeled optical pulses are the worthy foundation of the future experiments with the real optical pulses and the experimental observation of the introduced correlations. Due to lack of thesis preparation time, the following experiments on the mentioned effects were not accomplished. However, the author is aware of the importance and correctness of experimentally substantiated correlation effects and will undoubtedly continue to work in this direction.

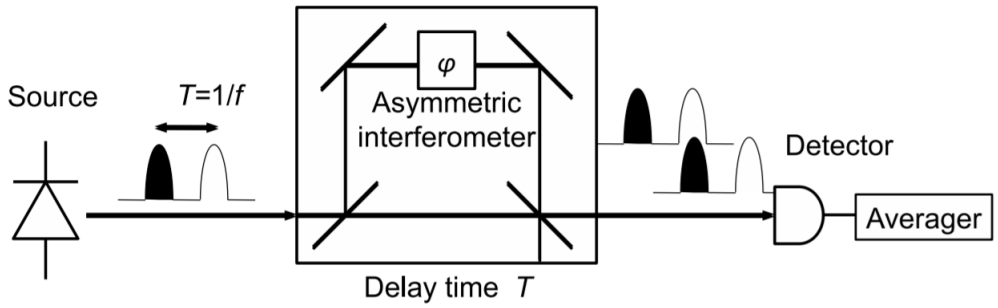

Figure 4.1: A schematic diagram of the measurement device for the correlations in the phase of the adjacent optical pulses (taken from [45]).

4.2 Possible configurations

As it was mentioned in the previous sections, there are papers, which methods and ideas helped the author to better understand the idea of intersymbol interference and correlation effects. Most of them provide experimental confirmation of the observed effects. In this way, for example, in [45] an experimental method for determining the correlations of adjacent optical pulses is presented (Figure 4.1). In this way, to experimentally characterize correlation effects in the phase of the optical pulses, the authors introduce an experiment with the employing of the interferometric setup (Figure 4.1), the main purpose of which is to carry out the interference of two adjacent optical pulses. In this way, the light source is generating a pair of pulses with a certain time delay. Pulses are propagating into the arms of the asymmetric interferometer, where the length of the longer arm is adjusted in a way to achieve the simultaneous arrival of spaced optical pulses at the output of the interferometer. In the same arm, the phase modulator is placed which is creating a stable phase shift between the paths. Then, after the interference at the output of the interferometer, signals are detected at the photodetector and proceeded with the averager. The amplitude of the measured signal on the photodetector depends on the phase shift that was applied by the phase modulator. By varying the phase parameter of the first impulse in pair, it is possible to observe a clear interference fringe at the output. After the averaging, provided that the pulses have a random phase shift, the interference fringe term should disappear from the measured values due to the accumulation of the random component. In this way, if there exists an implicit correlation between the phases of pulses in pair, then it will be seen in the amplitude of the measured averaged signal. The value of the phase correlation can be measured in terms of visibility of interference Θ, which gets closer to one as the correlation becomes stronger (4.1).

$$0 \leq \Theta := \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \leq 1, \tag{4.1}$$

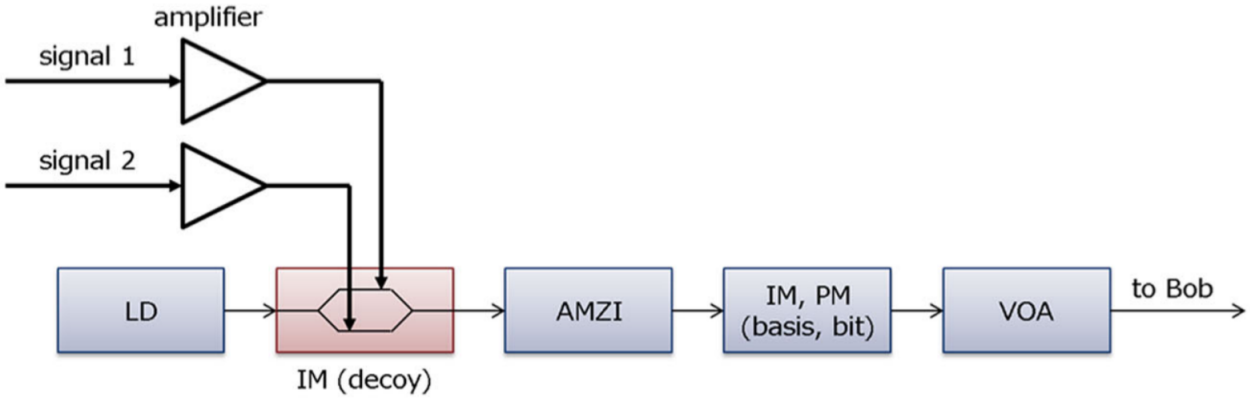

Figure 4.2: A schematic diagram of the measurement device for the correlations in the intensity of the adjacent optical pulses (taken from [50]). LD - laser diode, AMZI - asymmetric Mach-Zehnder interferometer, IM - intensity modulator, PM - phase modulator, VOA - variable optical attenuator.

where the variables $I_{max,min}$ are stated for the maximum and minimum values of the interference fringe respectively.

The upcoming experiments with the evaluation of the intersymbol interference in the intensity of the adjacent pulses will be carried out taking into account the experimental implementation of a similar investigation [50]. In this work, the authors provide the experimental observation of the intersymbol intensity correlations in a practical high-repetition rate QKD implementation. To examine these effects the authors proposed an experimental method, which can be partly used in the following experiments with QRate's system. They also propose to measure correlation effects using an experimental setup based on the QKD system implementation (Figure 4.2). To measure the intensities of the optical adjacent pulses, the authors connected the high-speed photoreceiver to the output of the intensity modulator (IM in the Figure [50]). The pulses were recorded by the oscilloscope with the 8 GHz bandwidth. The authors defined the pulse intensity as the area of the measured signal, and evaluate the correlations in intensities by the deviations in average pulses areas.

5. Conclusions

5.1 Summary

This master's thesis represents a result of experimental and theoretical work, that was performed during the last year of the master's studies. The work indicates the physical principles of operation of electro-optical modulators. Experiments were carried out to detect and describe intersymbol interference in adjacent pulses of the modulators control. Mathematical modeling of the corresponding experimental data was carried out showing the correlation effects in optical pulses, that are modulated following the physical principles of the modulators' work.

5.2 Recommendations

The one possible recommendation that the author will allow himself to give is connected to the observed in this thesis correlation effects. The correlations between states have been revealed only in the computer modeling so far, although there are experiments planned with real light pulses, which will put the final point on this issue. Nevertheless, the investigations carried out in this work revealed the presence of correlation effects in the operation of both electro-optical modulators. Ultimately, these correlations can lead to a decrease in the security level of the entire system as a whole. As a recommendation to QRate QKD system developers, it is possible to indicate the need to revise the position of the optical pulse window (100 ps) on

an electric pulse (3.2 ns). In this study, the optical pulse was placed in the middle of the positive part of the bipolar meander signal, but its possible placement in another place, as well as changing the shape of the electrical pulse, can reduce these correlation effects.

5.3 Conclusion

Quantum cryptography positions itself as uncompromisingly secure, but there is a whole section of science dedicated to numerous possible vulnerabilities in the QKD implementations and protocols. Nevertheless, it is worth understanding that quantum cryptography has every chance to soon become the global standard for secure data transmission. Work in this area allowed the author to fully understand the influence of various factors that can lead to the compromise of classified information. This thesis is devoted to one of these factors - the problems in the preparation of states stage, what could be a serious vulnerability in quantum cryptography protocols and systems. In particular, in the next stage of this large-scaled work, experimental measurements of correlation effects with real optical pulses will be implemented, and their influence on the overall safety of the QKD system will be evaluated. The logical and desirable conclusion of all the work done on this topic will be a publication in one of the international peer-reviewed journals.

Bibliography

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28:656–715, 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x.

[2] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22:644–654, 1976. doi: 10.1109/tit.1976.1055638.

[3] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21:120–126, 1978. doi: 10.1145/359340.359342.

[4] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.*, 45:109–115, 1926. doi: 10.1109/JAIEE.1926.6534724.

[5] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997. doi: 10.1137/S0097539795293172.

[6] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883–887, 2001. doi: 10.1038/414883a.

[7] Erik Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, and et al. Computing prime

factors with a josephson phase qubit quantum processor. *Nature Physics*, 8 (10):719–723, 2012. doi: 10.1038/nphys2385.

[8] Enrique Martín-López, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L. O'Brien. Experimental realization of shor's quantum factoring algorithm using qubit recycling. *Nat. Photonics*, 6(11):773–776, 2012. doi: 10.1038/nphoton.2012.259.

[9] P. Van De Zande. The day DES died. *SANS Institute: Information Security Reading Room*, 2001.

[10] Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41, 2018. doi: 10.1109/msp.2018.3761723.

[11] J. L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1):23–33, 1970. doi: 10.1007/BF00708652.

[12] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. doi: 10.1038/299802a0.

[13] D. Dieks. Communication by EPR devices. *Phys. Rev. A*, 92(6):271–272, 1982. doi: 10.1016/0375-9601(82)90084-6.

[14] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, 1993. doi: 10.1103/PhysRevLett.70.1895.

[15] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 80(6):1121–1125, 1998. doi: 10.1103/physrevlett.80.1121.

[16] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390: 575–579, 1997. doi: 10.1038/37539.

[17] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935. doi: 10.1103/PhysRev.47.777.

[18] Stephen Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1):78–88, 1983. doi: 10.1145/1008908.1008920.

[19] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. International Conference on Computers, Systems, and Signal Processing (Bangalore, India)*, pages 175–179, New York, 1984. IEEE Press. doi: 10.1016/j.tcs.2014.05.025.

[20] M. B. Costa e Silva, Q. Xu, S. Agnolini, P. Gallion, and F. J. Mendieta. Homodyne detection for quantum key distribution: an alternative to photon counting in bb84 protocol. In Pierre Mathieu, editor, *Photonics North 2006*. SPIE, Sep 2006. doi: 10.1117/12.707785.

[21] D. R. Hjelme, L. Lydersen, and V. Makarov. *A Multidisiplinary Introduction to Information Security*. CRC Press, 2011.

[22] Wolfgang Tittel, Gregoire Ribordy, and Nicolas Gisin. Quantum cryptography. *Physics World*, 11(3):41, 1998.

[23] C. H. Bennett. Quantum cryptography using any 2 nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992. doi: 10.1103/PhysRevLett.68.3121.

[24] Simon J. D. Phoenix, Stephen M. Barnett, and Anthony Chefles. Three-state quantum cryptography. *Journal of Modern Optics*, 47(2–3):507–516, 2000. doi: 10.1080/09500340008244056.

[25] Chi-Hang Fred Fung and Hoi-Kwong Lo. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. *Physical Review A*, 74(4), 2006. doi: 10.1103/physreva.74.042342.

[26] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, 2003. doi: 10.1103/PhysRevLett.91.057901.

[27] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, 2005. doi: 10.1103/PhysRevLett.94.230504.

[28] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.*, 7(1-2):73–82, 2007.

[29] V. Makarov, A. Anisimov, and J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74(2):022313, 2006. doi: 10.1103/PhysRevA.74.022313. erratum ibid. **78**, 019905 (2008).

[30] V. Makarov, A. Anisimov, and S. Sauge. Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve. 2009.

[31] V. Makarov and J. Skaar. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Inf. Comput.*, 8:622–635, 2008.

[32] V. Makarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys.*, 11(6):065003, 2009. doi: 10.1088/1367-2630/11/6/065003.

[33] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. Controlling an actively-quenched single photon detector with bright light. *Opt. Express*, 19: 23590–23600, 2011. doi: 10.1364/OE.19.023590.

[34] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, 2012. doi: 10.1103/PhysRevLett.108.130503.

[35] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A*, 88:052303, 2013. doi: 10.1103/PhysRevA.88.052303.

[36] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 111:130502, 2013. doi: 10.1103/PhysRevLett.111.130502.

[37] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 112:190503, 2014. doi: 10.1103/PhysRevLett.112.190503.

[38] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, , and Jian-Wei Pan. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.*, 113:190501, 2014. doi: 10.1103/PhysRevLett.113.190501.

[39] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L Braunstein, Seth Lloyd, Tobias Gehring, Christian S Jacobsen, and Ulrik L Andersen. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics*, 9:397–402, 2015. doi: 10.1038/nphoton.2015.83.

[40] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018. doi: 10.1038/s41586-018-0066-6.

[41] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "Plug and play" systems for quantum cryptography. *Appl. Phys. Lett.*, 70(7):793–795, 1997. doi: 10.1063/1.118224.

[42] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Automated 'plug & play' quantum key distribution. *Electron. Lett.*, 34(22):2116–2117, 1998. doi: 10.1049/el:19981473.

[43] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.*, 4:41, 2002. doi: 10.1088/1367-2630/4/1/341.

[44] M. Dušek, M. Jahma, and N. Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A*, 62(2):022306, Jul 2000. doi: 10.1103/PhysRevA.62.022306.

[45] Toshiya Kobayashi, Akihisa Tomita, and Atsushi Okamoto. Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser. *Phys. Rev. A*, 90(3), 2014. doi: 10.1103/physreva.90.032320.

[46] Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-Hang Fred Fung, Yang Liu, Hai-Lin Yong, Teng-Yun Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A*, 88:022308, 2013. doi: 10.1103/PhysRevA.88.022308.

[47] 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. *Phys. Rev. A*, 92:032305, 2015. doi: 10.1103/PhysRevA.92.032305.

[48] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A*, 90: 052314, 2014. doi: 10.1103/physreva.90.052314.

[49] Fadri Grünenfelder, Alberto Boaron, Davide Rusca, Anthony Martin, and Hugo Zbinden. Performance and security of 5 GHz repetition rate polarization-based quantum key distribution. *Appl. Phys. Lett.*, 117(14):144003, 2020. doi: 10.1063/5.0021468.

[50] Ken-ichiro Yoshino, Mikio Fujiwara, Kensuke Nakata, Tatsuya Sumiya, Toshihiko Sasaki, Masahiro Takeoka, Masahide Sasaki, Akio Tajima, Masato Koashi, and Akihisa Tomita. Quantum key distribution with an efficient countermeashowure against correlated intensity fluctuations in optical pulses. *npj Quantum Information*, 4(1), 2018. doi: 10.1038/s41534-017-0057-8.

[51] Дуплинский Александр Валерьевич. *Квантовое распределение ключа с высокочастотным поляризационным кодированием.* PhD thesis, МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ, 2019.

[52] Steve Yao. Polarization in fiber systems: Squeezing out more bandwidth. *The Photonics Handbook*, 2003.

[53] Changhai Ru and Lining Sun. Study of polarization control model for piezoelectric actuator. *Ultrasonics*, 44:e731–e735, 2006. doi: 10.1016/j.ultras.2006.05.199.

[54] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5:3–28, 1992. doi: 10.1007/bf00191318.

[55] iXblue. Application note: Introduction to ixblue mach-zehnder modulators bias controllers.

[56] Abraham. Savitzky and M. J. E. Golay. Smoothing and differentiation of data

by simplified least squares procedures. *Analytical Chemistry*, 36(8):1627–1639, 1964. doi: 10.1021/ac60214a047.