B92 BASED QUANTUM KEY DISTRIBUTION WITH FAINT PULSED LASER

A Thesis Submitted to
the Graduate School of Engineering and Sciences of
İzmir Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE

in Physics

by
Görkem MUTLU

December 2021
İZMİR

ACKNOWLEDGMENTS

Firstly, I would like to thank to my esteemed advisor Assoc. Prof. Dr. Serkan ATEŞ, who guided me at every stage of the thesis work, for his valuable efforts and contributions.

I wish to express thanks to my co-advisor Assoc. Prof. Dr. Özgür ÇAKIR, whose knowledge and advice I consulted in the thesis study and who made an important theoretical contribution to quantum communication.

I would like to say my gratitude to my dear wife, Ece MUTLU, who supported me under all circumstances during my undergraduate and graduate education, and who was with me at all times during this long process, for her help and patience.

I would like to thank Metin TAN, Çağlar SAMANER, Serkan PAÇAL, Ozan ARI, and NQO Group members, who shed light on my problems with their valuable comments in the thesis work and showed me new ways with their suggestions.

I really would like to thank Metin TAN and Ümit PURÇAK for their fun friendship and being always there for me.

I would like to thank my IZTECH Physics Department professors, whose opinions I frequently consulted and participated in during my master's education and thesis work.

Lastly, I would like to express my special thanks and gratitude to all the members of my family who have stood by me under all circumstances throughout my life and supported me through all the difficulties I faced.

This study was supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) with the project number of 117F495 and the project name is Quantum Cryptology with Single Photons Obtained from Hexagonal Boron Nitride Defect Centers.

ABSTRACT

B92 BASED QUANTUM KEY DISTRIBUTION WITH FAINT PULSED LASER

In quantum key distribution (QKD), photons are used to share the key between the transmitter and receiver, and in principle, single photon sources should be used to create a secure communication channel. Nowadays, attenuated laser sources are used in many studies. While it is practical to use attenuated laser pulses for QKD system, it poses many safety issues due to the possibility of multiple photons in the laser pulses. In addition, the key rate is waived to increase the level of security. However, the use of single photon sources is not as easy and practical as using attenuated laser sources. Today, studies of single photon sources to be used for QKD continue. In order for these single photon sources to be used actively, a photon source that operates at room temperature, operates in a wide band-gap range for different areas of use (underwater, optical fiber-based and free space) and can be excited at high speed is required. Since hBN defect centers are a material that can produce single photons at room temperature and have a wide band gap, it seems very ideal for these studies.

In this thesis, studies have been carried out on the realization of the protocol, which is a part of QKD, with solid-state materials that produce single photons. In the studies, a key was produced with a faint pulsed laser. Also, data is encrypted using the key of the transmitter. Then the data is successfully decrypted with the key measured by the receiver.

ÖZET

ZAYIFLATILMIŞ DARBELİ LAZER İLE B92 TABANLI KUANTUM ANAHTAR DAĞITIMI

Kuantum anahtar dağıtımınında (KAD) anahtarın alıcı ve verici arasında paylaşımı için fotonlar kullanılmaktadır ve güvenli bir iletişim kanalı oluşturmak için prensipte tek foton kaynakları kullanılması gerekmektedir. Günümüzde, yapılan pek çok çalışmada zayıflatılmış lazer kaynakları kullanılmaktadır. KAD için zayıflatılmış lazer darbeleri kullanılması pratik olsa da lazer darbelerinde birden fazla foton bulunma olasılığından dolayı pek çok güvenlik sorunu oluşturmaktadır. Ayrıca, güvenlik seviyesinin arttırılması için anahtar hızından feragat edilmektedir. Fakat, tek foton kaynaklarının kullanımı zayıflatılmış lazer kaynaklarını kullanmak kadar kolay ve pratik değildir. Günümüzde, KAD için kullanılacak tek foton kaynaklarının çalışmaları sürmektedir. Bu tek foton kaynaklarının aktif olarak kullanılabilmesi için oda sıcaklığında çalışan, farklı kullanım alanları için geniş bant aralığında çalışan (su-altı, optik fiber-tabanlı ve havadan) ve yüksek hızda uyarılabilen bir foton kaynağı gerekmektedir. hBN kusur merkezleri oda sıcaklığında tek foton üretebilen ve geniş bant aralığına sahip bir malzeme olduğundan dolayı bu çalışmalar için çok ideal görülmektedir.

Bu tez çalışmasında, tek foton üreten katı hal malzemeleri ile KAD'ın bir kısmı olan protokolün gerçekleştirilmesi üzerine çalışmalar yapılmıştır. Yapılan çalışmalarda, zayıflatılmış darbeli lazer ile bir anahtar üretilmiştir. Ayrıca, gönderici tarafındaki elenmiş anahtar kullanılarak bir veri şifrelenmiş, ardından alıcı ile ölçülen anahtar ile verinin şifresi çözülmüştür.

TABLE OF CONTENTS

LIST OF FIGURES vii

LIST OF ABBREVIATIONS xix

CHAPTER 1. INTRODUCTION 1

CHAPTER 2. THEORY 4

2.1. What is Cryptography 4

2.2. Types of Cryptography 5

2.2.1. Classical Cryptography 6

2.2.1.1. Basic Terminology: Encryption and Decryption 7

2.2.1.2. The One-time Pad 8

2.2.1.3. Modern Algorithm 8

2.2.2. Quantum Cryptography 10

2.3. Basic Principles of Quantum Cryptography 10

2.3.1. Heisenberg Uncertainty Principle 11

2.3.2. No-cloning Theorem 12

2.3.3. Qubit 14

2.4. Protocols of Quantum Cryptography 16

2.4.1. BB84 18

2.4.2. B92 21

2.4.3. Other Protocols 23

2.4.3.1. E91 (Ekert or EPR Protocol) 23

2.4.3.2. BBM92 protocol 27

2.5. Photon Statistics 28

CHAPTER 3. EXPERIMENTAL ANALYSIS 32

3.1. Optical Setup and Control Program of BB84 Protocol 33

3.1.1. Alice 33

3.1.2. Bob 36

3.1.3. Control Program 37
3.2. Photon Statistics and Laser Attenuation 38
3.3. Optical Properties and Theoretical Analysis of The Optical Setup . 42
3.4. Determining The Suitable Voltage Values of The EOM 48
3.4.1. Solution of The Problems 48
3.5. Optical Setup and Control Program of B92 Protocol 55
3.5.1. Alice 59
3.5.2. Bob 61
3.5.3. The Suitable EOM Voltage 62
3.6. Synchronization and Electronic Control 62
3.6.1. Understanding and Analysing The Obtained Data 68

CHAPTER 4. EXPERIMENTAL RESULTS 76
4.1. Key Rate and Quantum Bit Error Rate 76
4.2. Encryption and Decryption with The Key 78

CHAPTER 5. CONCLUSION 81

INDEX 83

REFERENCES 83

LIST OF FIGURES

Figure		Page
Figure 2.1.	Secure information sharing method. The information is encrypted with the help of a key, then the encrypted information is decrypted by the receiver. 3rd Party people trying to steal information are also called Eavesdroppers. …….	7
Figure 2.2.	Example of the one-time pad. Pre-prepared one-time keys are used in the one-time pad, and each character of the text is encrypted by modular addition with this key. Each character has a binary equivalent. ……..	8
Figure 2.3.	Example of Symmetric-Key and Public-Key cryptography. In the modern algorithm, information is encrypted and decrypted with the help of hard-to-solved mathematical algorithms. This section is divided into two as symmetric key and antisymmetric key cryptography in terms of the key usage. In symmetric keys, the transmitter and receiver use the same private key, while in antisymmetric, the key is different from each other and can be shared. ……	9
Figure 2.4.	Measurement on the quantum channel. In the no-cloning theorem, it is necessary to measure on a particle to detect its state, and it cannot be measured without affecting the system. For example, the measurement result can be determined when the measurement is made on the correct basis, while the measurements made on the wrong basis give an incorrect result and the true state cannot be determined. …….	13
Figure 2.5.	Representation of the qubit on the Bloch Sphere……	16

Figure		Page
Figure 2.6.	Representation of the qubit on the Poincare Sphere. Qubits are superposition of 1 and 0. …….....	17
Figure 2.7.	Basic representation of the BB84 protocol. Each bit of the secret key is encoded in the direction of the polarization of the photon. It is used a non-orthogonal two basis, four states. One basis must give the value 0.5 value of its conjugate to the other basis horizontal (H), vertical (V), 45 degrees (45) and 135 degrees (135) Alice and Bob select their basis randomly and 50% of measurements are rejected. The key must be sifted because of the chance of different basis selection. …….	19
Figure 2.8.	BB84 protocol raw key and sifted key generation. In Figure (a), Alice sends the photons she chooses in random basis and polarizations to Bob, and Bob measures the incoming photons again on random basis. In Figure (b), after Bob shares the empty measurements and the measurements he made on the wrong basis with Alice over the classical channel, these measurements are mutually eliminated, and the sifted key is created. Incorrect measurements are found and corrected by error detection and error correction methods. ……	20
Figure 2.9.	Corrected secure key. The measurements are converted to bit-matches and the key is obtained. ……	21
Figure 2.10.	Basic representation of the B92 protocol. The B92 protocol is a simplified version of the BB84 protocol. Two non-perpendicular basis and two states are used. Each bit is encoded in the polarization directions. The table shows the bit equivalent of the polarization and basis of Alice and Bob. ….....	22

Figure **Page**

Figure 2.11. Working principle of B92. In Figure (a), Alice sends the photons to Bob, randomly at the two selected non-orthogonal polarization direction. Bob makes measurements randomly at the other two polarization direction. Empty measurements are due to both non-ideal optical elements and detectors, and the B92 protocol. In Figure (b), the raw key generated after eliminating empty measurements. Yellow measurements on the Bob side indicate incorrect measurements due to experimental errors. Incorrect measurements are found and corrected by error detection and error correction methods. ……..... 24

Figure 2.12. Corrected secure key. The obtained measurements are converted to the corresponding bit state. Then, the key is obtained. ……... 25

Figure 2.13. Basic representation of the E91 protocol. One of the polarization-entangled photon pairs are sent to Alice and the other one is sent to Bob. Alice and Bob choose a random basis to detect photons by 50% chance. After that, photons are selected by polarization direction. If both Alice and Bob choose a true basis at the same time, measurement is considered correct. Otherwise, the measurement is discarded. For example, if Alice measures H, Bob must measure V or vice versa. If Alice measure 45, Bob must measure 135 or vice versa. ……..... 26

Figure **Page**

Figure 2.14. Basic representation of the BBM92 protocol. In this protocol, polarization-entangled photon pairs have different wavelengths. One of the photons is sent to Alice and the other one is sent to Bob. Alice and Bob choose a random basis to detect photons by 50% chance. After that, photons are selected by polarization direction. If both Alice and Bob choose a true basis at the same time, measurement is considered correct. Otherwise, the measurement is discarded. For example, if Alice measures H, Bob must measure V or vice versa. If Alice measure 45, Bob must measure 135 or vice versa. …….. 27

Figure 2.15. Detection of photon. In order to obtain the photon statistics of the photon source, a sensor that can measure a single photon (APD, PMT, etc.) and a time stamp that can record the time of this measurement in high resolution are required. ……. 29

Figure 3.1. First configuration of the BB84 protocol of QKD Optical Setup. In Alice, laser pulses are attenuated with the help of an ND filter and polarizer and then sent to a fiber, then the key is added in the direction of the polarization of the photons. Next, In Bob, incoming photons are split into 2 paths with a 50% chance with BS. Then, with the help of PBS, the selection is made according to the direction of their polarization and measured with single-photon detectors. Measured photons are recorded as measurement time and measured detector by TTM. With a synchronization signal, the key is detected. ……..... 34

Figure 3.2. List of used optical components in BB84 Protocol. …….. 35

Figure 3.3. The front panel of the Labview program created to control the optical installation via computer. …… 37

Figure **Page**

Figure 3.4. Optical setup configuration for photon statistics. The pulsed laser is driven by a signal generator and the same signal is sent to the TTM. Laser pulses are attenuated with the help of an ND filter and polarizer and passed through a BS. Photons reflected and transmitted from the BS are measured by APDs. Measurement results are recorded with TTM. Here, the reason for separating the photons into two separate paths is to determine the number of coincidences and to reduce the dead time of the APDs. …… 38

Figure 3.5. Variation of number of coincidence and μ depending on the power of the laser. In Figure (a), the μ calculation was found as the ratio of the total laser pulse to the number of photons measured, then normalized to the second and recalculated at each tune value. The total count divided by the quantum efficiency of the APD to find the number of photons actually sent. In Figure (b), it is obtained by summing the simultaneous measurements made by the APDs at each tune value. As the power of the laser increases, the number of coincidences increases logarithmically. …….. 40

Figure 3.6. Coincidence versus Mean Photon Number. Coincidence increases with increasing mean photon number, as expected. ……... 41

Figure 3.7. Theoretical representation of the EOM and QWP output polarizations of the vertically incident photon. ……... 46

Figure 3.8. The voltage-dependent irradiance measurement results expected to be seen in the detectors. The purple, blue, red, and yellow lines indicate the vertical, horizontal, 45, and 135 polarization directions, respectively. The maximum peaks show the voltage to be applied to the EOM for that polarization. …….. 47

Figure **Page**

Figure 3.9. First measurement result of output signals. This data was obtained by measuring the intensity at the output ports of the PBS by sweeping the voltage of the EOM between -200 and 200V. With the help of this graph, the appropriate voltage is found for the appropriate polarization directions. However, the maximum powers measured in PBSs are not balanced. …….. 49

Figure 3.10. Polarization analysis of after QWP. By varying the voltage applied to the EOM, a PBS was placed behind the component to be measured and the intensity at the PBS outputs was measured. Thus, it is desired to detect polarization disorders originating from the component. As you seen, there are no polarization disorders on Alice's part. However, there is some shifting the polarization direction, because its polarization in the vertical direction should not change at 0V. …… 50

Figure 3.11. Polarization analysis of after M6. As can be seen, since the reflectivity coefficient of the mirrors changes depending on the direction of the polarization, the peaks vary between polarizations. Therefore, it is beneficial to minimize the use of mirrors in QKD systems using a single laser. If different lasers were used for each polarization direction, the intensity between them could be equalized. ……..... 51

Figure **Page**

Figure 3.12. Correct HWP angle and EOM alignment. Although this figure seems complicated, it is actually the data obtained with the help of PBS by changing the angle of the HWP on a diagonal basis. A PBS was added after the HWP and the voltage of the EOM was varied between -200 and +200V at each HWP angle. The goal here is to find the right angle of the HWP. However, if the laser beam does not pass straight through the EOM, circular polarization is observed as in Figure (a). To avoid this circular polarization, either the laser beam is corrected or the angle of the QWP is adjusted to the appropriate position. The inaccuracy in the EOM alignment can be understood from the fact that the light passing over it changes the polarization when no voltage is applied to the EOM. Figure (b) is obtained after correcting the EOM. …… 52

Figure 3.13. Last configuration of BB84 protocol optical cetup. In order to align the EOM properly, all mirrors in the system, except the 2 mirrors in the Alice part, have been removed. ……..... 54

Figure 3.14. Figure (a) shows powermeter results. Figure (b) shows the APDs results. The results are shown after all adjustments and component eliminations. As can be seen, all polarization problems are resolved and equal power is received from each polarization direction and equal number of counts are received from the APDs. Thus, it will now be possible to take measurements in a highly efficient way with the optical system. …… 56

Figure **Page**

Figure 3.15. Figure (a) shows outputs with powermeter. Figure (b) shows outputs with APD. In this graph, the data obtained from the theoretical results and the measurement data are compared. The measurement results agree with the theoretical values obtained. Due to the extinction ratio of PBSs, their minimum cannot be measured as 0. ……..... 57

Figure 3.16. Optical setup of B92 protocol. Attenuated laser pulses with vertical polarization arrive at the EOM, where the key is encoded to the polarization direction of the photon. When no voltage is applied to the EOM, photons are sent in vertical polarization. When applied 90V, it is sent at a 45-degree angle and sent to Bob. The EOM is only turned on and off according to the value of the key. Photons coming to Bob are chosen in a random basis direction by BS. If a photon with a vertical direction chooses an orthogonal basis, it is discarded from the system. If it chooses the diagonal basis, it has a 50% chance to measure at 135 degrees. Besides, the photon with a 45-degree polarization direction will be measured horizontally with a 50% chance if it chooses the orthogonal basis. If it chooses a diagonal basis, it is kicked out of the system. …… 58

Figure 3.17. Optical Setup of Alice. The attenuated laser system is shown on the left side. On the right side, the EOM for the polarization control is shown. ……. 60

Figure 3.18. Optical Setup of Bob. On the left, a 50:50 BS are used for random photon selection and PBSs were used for polarization selection of photons. On the right, APDs are used to detect the incident photons in the channels. ……. 61

Figure **Page**

Figure 3.19. Outputs of B92 protocol. As can be seen, no measurement is taken on an orthogonal basis when no voltage is applied to the EOM. However, half of the intensity is measured on a diagonal basis. In addition, when 95V is applied to the EOM, half of the intensity is measured on an orthogonal basis, while intensity is very low (this is our error rate) on a diagonal basis. Thus, it is necessary to apply 0 and 90V to the EOM to encode the key. ……. 63

Figure 3.20. Installation of Control Part. ……..... 64

Figure 3.21. Schematic representation of the electronic control system prepared for the B92 protocol. 2 channels of the signal generator are used and 25% phase difference is added between them. The delayed channel is connected to the laser and the TTM. Thus, the signal is recorded both while driving the laser and by connecting to a channel of the TTM to ensure synchronization. The other channel is connected to the I/O channel of the MCU. On each incoming high signal, the MCU applies the elements in an array of pre-generated pseudo-random numbers, respectively, to its digital output as a logic level. Depending on the voltage at the output of the MCU, the high voltage amplifier changes the voltage to 0 or 90V. ……..... 65

Figure **Page**

Figure 3.22. Image is taken from the oscilloscope. The signal with the yellow line is used to drive the laser and is connected to the TTM for synchronization and is recorded. The signal with the red line is the output signal of the MCU and is used to drive the EOM. It is adjusted to change the polarization state on the pulse so that it can be seen easily on the oscilloscope. As can be seen from the picture, before the laser signal is generated, the state of the EOM has changed and is ready for proper polarization. After some time has passed after the laser pulse has finished, the system prepares to change state to encode the next key. 66

Figure 3.23. B92 protocol signals representation. First, the graph on the left is a representation of the signal generated for a periodic switch. The graph on the right is the signal representation of a randomly generated key. The signal driving the laser, the signal driving the MCU, and the signal driving the EOM are plotted over time. 67

Figure 3.24. The first raw key configuration. In this part, we wanted to make a visualizable key. Alice will send twenty-five vertical and then twenty-five 45 degree polarizations and then waited for 1 second. After that, alice will repeat this situation periodically. 68

Figure **Page**

Figure 3.25. Measurements of the first raw key configuration part 1. The graphs (a) show the measurement density over time histogram. In Figure, from top to bottom, measurements of 135 channels, measurements of the horizontal channel, and synchronization pulses are seen. As can be seen, the resulting intensities mean that the number of measurements increased. First, the measurement increased in channel 135, then the measurement increased in the horizontal channel. The Redline is the area to be zoomed in and (b) is zoomed part of (a). As can be seen in figure (b), the measurement density changes due to the change in polarization. ……. 69

Figure 3.26. Measurement of the first raw key configuration part 2. When these densities are zoomed by 2 times, it is seen that the measurement is made in each sent pulse. It can be seen that we have accurately measured the photons we send from here. In order to get a clearer vision, the laser power has been increased and the number of measurements has increased. ……..... 70

Figure 3.27. Comparing high laser count and low laser count. In this graph, it is seen why the laser intensity should be attenuated. In the graph (a), there are simultaneous photon measurements in both channels in each pulse. But at (b) low power, the number of measurements is greatly reduced. …….. 71

Figure **Page**

Figure 3.28. System delay at high frequency. This graph was obtained by subtracting each synchronization signal from each others. Thus, the region where the measurement is dense has emerged. If we zoom in on the except dense part, it will be seen that the measurements from the dark count disperse over the entire range. Thus, we can eliminate false measurements based on dark count and this situation reduces QBER. …… 72

Figure 3.29. Dense part of the Figure 3.28. Subtracting the measurement time of each synchronization signal, all photon measurements will be collected in a area. Measurements of laser photons create a denser area. This is the area where the key is located. Then, the key is obtained from this area with the analysis algorithm created in Matlab. ……... 75

Figure 4.1. Encryption and decryption method of the logo. In order to encrypt the information, the information is first converted into binary form. Then, the information in binary form is added by the obtained key, and the sum of the information is taken as a modulus of 2. The encrypted information is obtained and sent to Bob. Then Bob adds the encrypted information with the key he obtained and gets a modulus of 2 again. Bob decrypts the information. …….. 77

Figure 4.2. Encrypted and decrypted Iztech logo. Figure (a) shows the encrypted and decrypted logo with the uncorrected key. Figure (b) shows the encrypted and decrypted logo with a corrected key. With uncorrected key, there is some noise in the figure. …… 78

Figure 4.3. Key Rate Dependent Encrypted and Decrypted Iztech logo and the key rates are 15.981, 39.674, 63.947 Kbps from top to bottom, respectively. ……. 79

LIST OF ABBREVIATIONS

hBN . . . . . Hexagonal Boron Nitride
APD . . . . . Avalanche Photo-diode
PMT . . . . . Photomultiplier Tube
EOM . . . . . Electro Optic Modulator
BS . . . . . Beam-splitter
PBS . . . . . Polarizing Beam-splitter
HWP . . . . . Half Wave-plate
QWP . . . . . Quarter Wave-plate
TTM . . . . . Time Tagging Module
PMFB . . . . . Polarization Maintained Single Mode Fiber
MMFB . . . . . Multimode Fiber
RSA . . . . . Rivest, Shamir, Adleman
BBO . . . . . Beta-Barium Borate)
DES . . . . . Data Encryption Standard
OTP . . . . . One Time Pad
AES . . . . . Advanced Encryption Standard
QBER . . . . . Quantum Bit Error Rate
EPR . . . . . Einstein, Podolsky, Rosen
CHSH . . . . . Clauser, Horne, Shimony, Holt
SSP . . . . . Six-State Protocol
DPS . . . . . Differential Phase Shift
PNS . . . . . Photon Number Splitting
COW . . . . . Consistent One Way
CW . . . . . Continuous Laser
PMT . . . . . Photo-Multiplier Tube
STD . . . . . Standard Deviation
HBT . . . . . Hanbury Brown-Twiss

CHAPTER 1

INTRODUCTION

Nowadays, as much as the transmission of information, the security of information while being transmitted from one place to another has become a very important issue. The importance of information security is increasing day by day and it is foreseen that it will become very critical in the coming years. Although the discovery, development, and studies on the quantum computer since 1980 are not yet at sufficient processing power levels, it poses a great threat in terms of classical cryptology used to provide information security like public-key encryption based on RSA algorithm (Benioff, 1980; Feynman, 1982; Gibney, 2019a; Pan and Zhang, 2021; Gibney, 2019b). Precautions can be taken against classical computers with classical cryptology techniques. Therefore, quantum cryptology, which will provide superior protection against classical computers, will also provide security against quantum systems (Steane, 1998). In addition, qubits are indispensable for quantum cryptology, quantum computing, and quantum information theory (Monroe, 2002). In short, quantum cryptology, which is at the intersection of information theory and quantum mechanics, has been understood to offer incredible possibilities with the studies and developments in the last few decades. For this reason, the studies and developments carried out today are increasing significantly and integration into today's systems has begun. Moreover, it is foreseen that the use of these systems will increase in the future.

Quantum cryptology, also known as quantum key distribution (QKD), which is one of the most applicable areas of quantum mechanics today, was first proposed by Charles H. Bennett and G. Brassard in 1984 by using a quantum channel to send a key produced with true randomness with the help of four directions of polarizations of photons (Bennett and Brassard, 2014). Afterward, in 1991, A. Ekert, while still a doctoral student, showed that a key could be obtained using photons with polarization entanglement, and the protocol he found was named E91 (Ekert, 1991). Next, again in 1992, C. Bennett proposed a protocol using 2 quantum states, which is seen as a simplified version of the BB84 protocol, and this protocol was named B92 (Bennett, 1992).

In quantum cryptography, photon sources used for key generation are also a very important issue. The reason for this is that the key produced by single photons, which can naturally prevent methods such as photon number separation (PNS) attack, increases eavesdropping security, and increases system performance compared to systems using attenuated pulsed lasers (Kupko et al., 2020). Today, photon sources used in quantum key distribution systems vary according to the protocol used. Some protocols use sequential single photons with polarization (Monroe, 2002), while some protocols use entangled photon pairs (Silverstone et al., 2015). Attenuated lasers and single atoms and molecules, which emit a photon, are also widely used as single-photon sources, as well as 0, 1, and 2-dimensional and bulk materials. There are drawbacks in the use of laser as a single-photon source, due to the possibility of multiple photons coming in at the same time (Eisaman et al., 2011; Al-Kathiri et al., 2008). However, it can be considered as the most practical method in practice. On the other hand, discrete electronic levels are needed to produce sequential single photons. While single atoms (Rb87 atoms and sodium atoms), ions (Ca^+ ion), and single molecules (isolated terrylene molecules) already have discrete electronic levels, it is quite difficult to work with single atoms, ions, and single molecules (Chen et al., 2006; Kimble et al., 1977; Maurer et al., 2004; Steiner et al., 2007). Working with 0D, 1D, 2D and bulk materials having discrete energy levels is much easier than working with single atoms or molecules. Examples of the most popular materials that produce single photons are nitrogen-vacancy center (NV center) in diamond (Kurtsiefer et al., 2000), silicon carbide (Defects in SiC) (Lohrmann et al., 2016), hexagonal boron nitride (Defects in hBN) (Tran et al., 2016), tungsten diselenide (Monolayer WSe2) (He et al., 2015; Castellanos-Gomez et al., 2015), Molybdenum diselenide (MoSe2) (Tonndorf et al., 2013) (they are called Transition-metal dichalcogenide (TMD or TMDC) material) and quantum dots (QDs) (Grangier et al., 1986). In addition, carbon nano-tube is among the materials studied (Ma et al., 2015). These materials can be classified among them in terms of some properties. While some materials produce a single photon at room temperature, such as hBN, MoSe2, NV centers in diamond, SiC (Grosso et al., 2017; Chowdhury et al., 2021; Mizuochi et al., 2012; Castelletto et al., 2014), some need to work at cryogenic temperatures, such as QDot, WeSe2 (Michler et al., 2000; Aharonovich et al., 2016). In terms of operating temperature, materials that produce single photons at room temperature are more useful than those that operate at cryogenic temperatures.

The reason for this is that large and costly devices must be used to reach the operating cryogenic temperature of such materials. Furthermore, single-photon producing materials can be classified in terms of the spectral range in which they emit. This classification also determines the places where this photon source can be used. For example, when the material is desired to be used for an optical-fiber based system, working with a material in the NIR wavelength range is very important in terms of loss in the optical-fiber (Müller et al., 2018), or if it is desired to be integrated into a system operating underwater, a material that glows around the blue-green optical color should be selected for minimum loss (Feng et al., 2021). In addition, for free-space, the visible wavelength and some regions of the NIR are ideal (Graham, 1999). In the light of this information, mostly Qdots are very useful for free space and optical fiber-based systems (Birowosuto et al., 2012). In addition, materials emitting at different wavelengths can be used in fiber optic based networks by down-conversion method (Pelc et al., 2012). To talk about the sources that produce polarization-entangled photons, entangled photons can be produced with the spontaneous parametric down-conversion method, with the help of high-power laser and BBO (beta-barium borate) or lithium niobate non-linear crystal (Lamas-Linares et al., 2001; Takesue et al., 2005), or excited atomic radiative (calcium) cascade with a laser (krypton) (Aspect's experiment) (Aspect, 1975, 2004; Goetz and Bartschat, 2021) and ring-resonator photon-pair sources on a silicon chip (Silverstone et al., 2015).

Up to now, one of the longest distances with 1 Mbps key rate (around 147 kilometers) in free space has been reached in the demonstrated quantum key distribution systems with entangled photons and weak coherent laser pulses in 2007 with high key rate (Ursin et al., 2007; Schmitt-manderbach, 2007). In addition, up to 307 kilometers have been reached with optical fiber-based systems with entangled photons (Korzh et al., 2015). Moreover, fiber-based and free-space quantum key distribution has been made at a distance of 250 meters with entangled photons produced by QDots (Basset et al., 2021). Quantum key distribution is also done using different single-photon sources like NV centers (Leifgen et al., 2014; Liu et al., 2015). Furthermore, in 2017, it was shown the longest distance that entangled photon-based quantum key distribution between two satellites (with distances ranging from 1600 to 2400 kilometers) will work more efficiently at much longer distances on Earth (around 1200 km) than fiber and free space-based systems (Yin et al., 2017).

In this thesis, we implemented a B92-based QKD system using attenuated laser pulses for a proof-of-concept demonstration, which can be extended to BB84 protocol with true single photons generated from solid-state quantum emitters, such as defects in hBN.

CHAPTER 2

THEORY

Quantum technologies take advantage of the properties of controlled quantum mechanical systems for computation, communication, and understanding of complex natural phenomena, allowing us to advance our understanding of basic physics. One of these technologies that are closest to application in the near future in the field of quantum cryptology. This area, which was proposed in the 1970s, was not feasible with the technology at that time, and information security was not a very important issue. However, besides the security of information being a very important issue today, this technology has also created a new engineering field. Nowadays, studies are in the direction of carrying these systems to longer distances, creating faster and safer systems, and developing new protocols.

2.1. What is Cryptography

First of all, the origin of the word cryptography goes back to ancient Greek times. It consists of two main words. The first part of the word, crypto, comes from 'Kryptos' and means to hidden, the other part of the word graphy comes from 'Graphein' and it means writing (Pawlan, 2005). The definition of cryptography is the study of various mathematical methods to ensure the security of information, such as confidentiality of information, protection of data integrity, entity verification, and identification of data source. Although cryptography is not the only method to ensure the security of information, it is the application of a series of mathematical techniques (Bellare and Rogaway, 2005; Menezes, 1996).

Modern cryptography is an interdisciplinary science and is the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Cryptography is the keystone of computer and communication security. Nowadays, cryptography is frequently used in electronic commerce, credit cards, digital currencies, computer passwords, mobile phone messaging applications, and mili-

tary communication.

It is the application and examination of techniques for secure communication in the presence of third parties called eavesdropper (van Leeuwen, 1990). To prevent eavesdroppers access, the creator of an encrypted message only shares the decoding technique with the targeted recipients.

Cryptography uses the names Alice as the transmitter, Bob as the receiver, and Eve as the eavesdropper in the literature (Biggs, 2009).

Cryptography or 'encryption' is all of the methods used to transform the information contained in readable data into a form that cannot be understood by undesirable parties. For over 6000 years, cryptography has been the art of encryption so that only legitimate people can read the content of messages. Examples of the use of cryptography in the military field date back to the ancient Egyptians, Spartans, and Romans. In the recent past, the use of cryptographic systems affected international conflicts and played an important role, especially in World War II. In the 1940s British militaries were able to decode messages encoded by the German ENIGMA and learned about the coordinates of German military units with the first working computers for cryptanalytic. After the use of computers in World War II, the methods used to perform cryptography became increasingly complex and its applications more common.

Today, cryptography has become a part of life, not just military forces. Confidential data such as personal identification numbers (PIN) and credit cards that we use frequently throughout the day are usually encrypted (van Leeuwen, 1990; Goldreich, 2004; Merriam-Webster.com Dictionary, 2021).

2.2. Types of Cryptography

All encryption methods that we mostly use today are classical encryption methods. The password created in classical encryption is obtained with a strong mathematical equation and very high processing power is required to decrypt the generated password. In addition, the generated password changes periodically, making it difficult to decipher.

Quantum encryption methods, which are a newer technology compared to classical encryption, are not widely used today due to their much larger size, limited working distance, and sensitivity to environmental factors. However, as the technology develops,

it is thought that quantum cryptography will replace classical encryption. Because the generated code is based on quantum mechanics, there is real randomness and the measurement made on the system affects the result. This does not make it possible to decrypt the password with classical computers as it is created with no-cloning and true randomness. Thus, where the security of information is concerned, quantum cryptology comes to the fore.

2.2.1. Classical Cryptography

Cryptology, which has a long and impressive history, has not lost its importance from the past to the present and even gained importance. During this time, many impressive and clever cryptology methods were developed and played a critical role from the ancient Egyptians to the present day. Although cryptology has been used predominantly by the military, diplomatic services, and government in the past as a tool to preserve their national strategies and their secrets, information security has become a very important issue for everyone today. The reason for this importance is the importance of protecting our information from 3rd parties, together with the convenience brought by technology today because the information obtained can be used maliciously and bank accounts can be easily accessed (Damico and Davies, 2009).

As mentioned before, with the increase in the use of computers in communication systems in the 1960s, the importance of storing and securing information in a digital way has increased. In 1977, they got the result of IBM's work that started with Feistel in the 1970s, and the Data Encryption Standard (DES), which was adopted as the US Federal Information Processing Standard, was developed to encrypt information (Feistel, 1973). DES is known as the most well-known encryption mechanism in the history of classical cryptography. It is still used in many financial institutions around the world (Menezes, 1996).

The most important development in classical cryptography came in 1976 with the article New Directions in Cryptography by Diffie and Hellman (Diffie and Hellman, 2019), which introduces the concept of public-key cryptography. For the security of information, it is suggested to use the hard-to-solve discrete logarithm problem. Two years later, Rivest, Shamir, and Adleman came up with the first easy public-key encryption and

signature scheme known as RSA (Rivest et al., 2019). RSA uses a method of factoring large hard-to-solve integers, unlike what Diffie and Hellman suggested. It took until the 1980s to apply this difficult mathematical problem to cryptography. In 1985 ElGamal found a different class of hard-to-solve and practical public-key scheme, again based on discrete logarithm problems (ElGamal, 1985).

2.2.1.1. Basic Terminology: Encryption and Decryption

Encryption is the hiding of information in such a way that it cannot be understood when it is obtained by 3rd parties. The recovery of hidden information is called decryption and it can also be called a decipher. Third-party people trying to obtain information are called eavesdroppers.

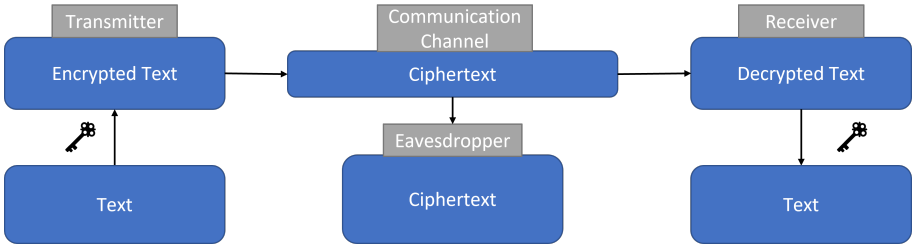


Figure 2.1. Secure information sharing method. The information is encrypted with the help of a key, then the encrypted information is decrypted by the receiver. 3rd Party people trying to steal information are also called Eavesdroppers.

Figure 2.1 shows that the sender encrypts the information to be sent and then sends it over the communication channel. The receiver, on the other hand, decrypts and obtains the received encrypted information. The eavesdropper in the communication channel can only obtain the encrypted information and should not be able to obtain the original text.

Algorithm Methods and Key:

Generally, the algorithm procedure is set up as the sender encrypts the information

and the receiver decrypts the encrypted information. The strength and security of the algorithm are based on ensuring the security of the information. Auguste Kerckhoffs van Nieuwenhof proposed in 1883 in his book La Cryptographie Militaire that it is sufficient to use the key in the algorithm and only keep the key secret.

Algorithms with key are also divided into two categories. These are symmetric-key algorithms, that is, algorithms where the transmitter and receiver use the same key, and asymmetric-key algorithms, that is, algorithms where the transmitter and the receiver use different keys.

2.2.1.2. The One-time Pad

Known as a one-time pad (OTP), it is a method of cryptography that Claude Shannon also proved mathematically unbreakable. It is an encryption technique that uses a single-use and pre-shared key that is at least as large as the message sent. In this technique, plain text is encrypted with the help of randomly generated keys, combining each digit or character with the bits or characters from the key using modular addition. Figure 2.2 shows the schematic of the one-time pad.

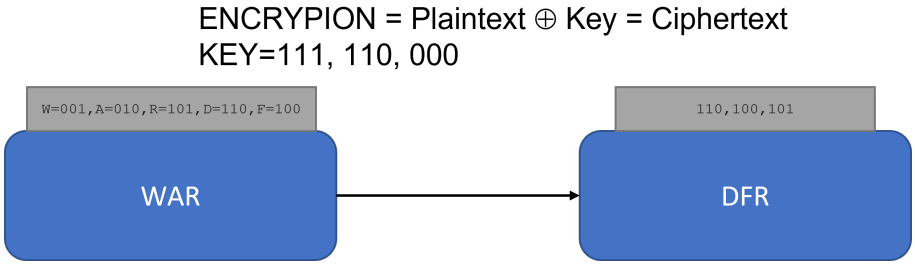


Figure 2.2. Example of the one time pad. Pre-prepared one-time keys are used in the one-time pad, and each character of the text is encrypted by modular addition with this key. Each character has a binary equivalent.

2.2.1.3. Modern Algorithm

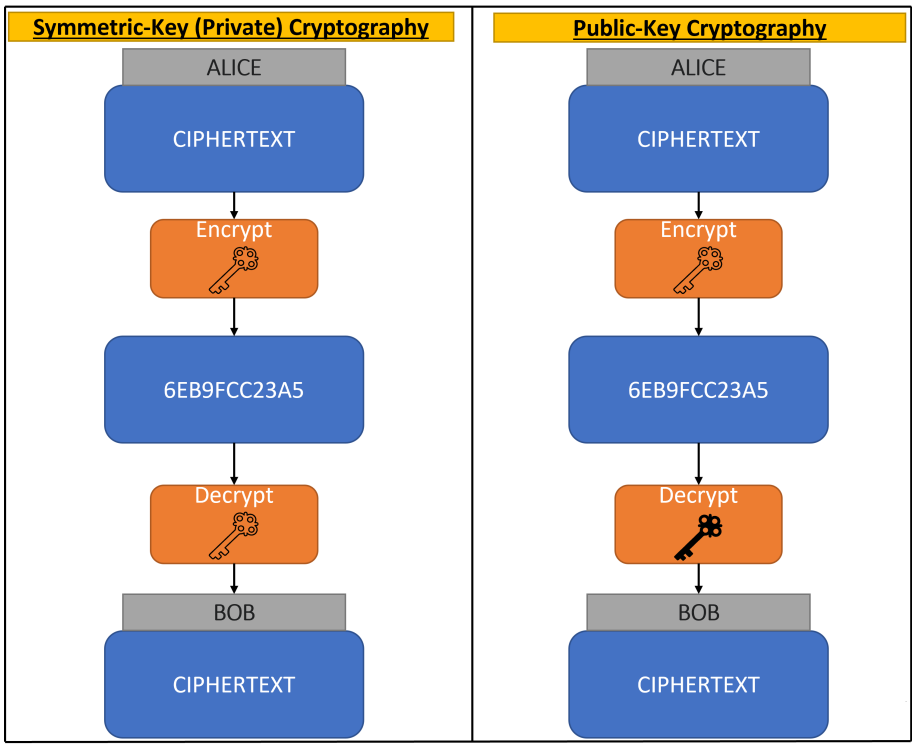


Figure 2.3. Example of Symmetric-Key and Public-Key cryptography. In the modern algorithm, information is encrypted and decrypted with the help of hard-to-solved mathematical algorithms. This section is divided into two as symmetric key and antisymmetric key cryptography in terms of the key usage. In symmetric keys, the transmitter and receiver use the same private key, while in antisymmetric, the key is different from each other and can be shared.

Modern cryptography has a very important place for computer and communication security nowadays. In this cryptography method, mathematical concepts such as number theory, computational complexity theory, and probability theory are used. Since it is used in the computer environment, binary bit sequences are used and well-known mathematical algorithms are used to encrypt the information. Privacy is encrypted with the help of a secret key and the computational difficulty and time of the algorithm are exploited. Even if the attacker knows the algorithm used, it is impossible to reach the original information

without the key. In modern cryptography, communication can be achieved by having a private key between the parties.

Symmetric-Key (Private Key) Cryptography:

In symmetric-key cryptography, the same key is used both when encrypting and decrypting the information. It is clear from this that the key cannot be sent over the public channel. Until 1976, this method was widely used.

Symmetric keys are generated as block ciphers using plain text blocks or stream ciphers using individual characters. The Data Processing Standard (DES) and Advanced Encryption Standard (AES) standards determined by the USA as the cryptography standard are block cipher designs. Although the DES standard remained in the background after AES was developed, it still continues to be used in many areas. Figure 2.3 shows the symmetric-key cryptography schematically.

Public-Key (Antisymmetric-Key) Cryptography:

In public-key cryptography, the public key can be freely distributed, but the paired private key must remain private. In this system, the public key is used to encrypt the information, while the private key is used only to decrypt it. Thus, the keys of the receiver and transmitter are different from each other. In 1978, with the suggestion of Ronald Rivest and Adi Shamir, the Rivest, Shamir, Adleman (RSA) algorithm with a high-quality public key algorithm was developed by Len Adleman and is widely used today. Figure 2.3 shows the public-key cryptography schematically.

2.2.2. Quantum Cryptography

Quantum cryptography (QC) is a system in which true randomness is used and special features such as the basic principles of quantum mechanics (qubit, no-cloning theorem, Heisenberg Uncertainty Principle) are used. In addition, indivisible quanta and entangled systems, which come from the basic principles of quantum mechanics, are used. One of the most usable and commercialized areas of quantum today is quantum

cryptology. In addition, in the 20th century, developments in information theory and relativity helped formalize the concept of information measured in bits and probabilities. Quantum cryptography actually sits where quantum mechanics and information theory meet. In this section, many topics will be covered, from the foundations of quantum cryptography and attenuated lasers to entangled photon pairs (Gisin et al., 2002).

2.3. Basic Principles of Quantum Cryptography

In this section, the basic principles of quantum mechanics and their mathematical proofs, which ensure the security of quantum cryptology, will be briefly mentioned. The basic principle of quantum mechanical properties on which quantum cryptography is based is the Heisenberg Uncertainty Principle, the No-cloning Theorem, and qubit.

2.3.1. Heisenberg Uncertainty Principle

The security of quantum cryptography is based on quantum mechanics foundations. One of them, the Heisenberg Uncertainty principle, firstly introduced in 1927 by the German physicist Werner Heisenberg, can know exactly one of a pair of conjugate properties at the same time. Heisenberg proved that the double conjugate position and momentum of a particle cannot be measured simultaneously (Heisenberg, 1927, 1989). It also uses this principle in quantum cryptography and uses the polarization of photons on a different basis as a conjugate feature.

Before explaining the theorem, it is necessary to give a few basic mathematical information. The feature that makes it impossible to measure the previously mentioned quantities simultaneously is called a commutator in mathematics. If we define two quantum mechanical operators as operators $\hat{X_1}$ and $\hat{X_2}$, the commutator of $\hat{X_1}$ and $\hat{X_2}$ is written as follows.

$$\left[\hat{X_1}, \hat{X_2}\right] = \hat{X_1}\hat{X_2} - \hat{X_2}\hat{X_1} \tag{2.1}$$

If the result is equal to 0 when we swap the places of the two operators, it means

that we can measure the two properties simultaneously with full accuracy. However, if its commutator is not equal to 0, that is, it cannot be displaced, it means that we cannot measure two quantities at the same time, and it means that the measurement of one quantity affects the measurement of the other quantity. This situation reveals the uncertainty relation described by the Heisenberg uncertainty principle.

Now, going to the theorem, the theorem clearly states that it is not possible to measure the quantum state of any system without disturbing that system. The conclusion to be drawn from this is that the polarization of a photon can only be known at the location in which it is measured. Moreover, this principle plays an important role in exposing eavesdroppers, which ensures the reliability of quantum cryptography. For any two interconnected observable properties, such as the non-orthogonal two polarization of the photon, the following equation can be written.

$$\left\langle \left\langle \Delta\hat{X}_1 \right\rangle^2 \right\rangle \left\langle \left\langle \Delta\hat{X}_2 \right\rangle^2 \right\rangle \geq \frac{1}{4} \left| \left\langle \left[\hat{X}_1, \hat{X}_2\right] \right\rangle \right|^2 \tag{2.2}$$

Where

$$\Delta\hat{X}_1 = \hat{X}_1 - \left\langle \hat{X}_1 \right\rangle, \; \Delta\hat{X}_2 = \hat{X}_2 - \left\langle \hat{X}_2 \right\rangle \tag{2.3}$$

for

$$\left[\hat{X}_1, \hat{X}_2\right] = \hat{X}_1\hat{X}_2 - \hat{X}_2\hat{X}_1 \neq 0 \tag{2.4}$$

According to the theorem, two conjugate quantities cannot be measured individually without affecting the system such as momentum and position of particle. Since the photon is also an indivisible particle, measuring the polarization of photon will affect the values of photon. For this reason, if a measurement is made between the receiver and the transmitter, it means that the wrong information will be sent to the transmitter.

2.3.2. No-cloning Theorem

The no-cloning theorem was proposed by Wooters, Zurek, and Dieks in 1982, and they mentioned that it is impossible to produce exact copies of a randomly occurring

quantum state (Wootters and Zurek, 1982).

In classical cryptography, no precaution can be taken about whether listening is made on the data transmission channel. Because, even if classical cryptography is done with photons, communication is made with very high numbers of photons. The data transmitted from the channel to the home can be obtained very easily with the help of a beam-splitter, and the other party cannot understand it at all. Even if the photons are transmitted with a fiber optic cable, some of the data can be received with the help of fiber near it. This is because in classical cryptography there is no physical phenomenon to prevent this.

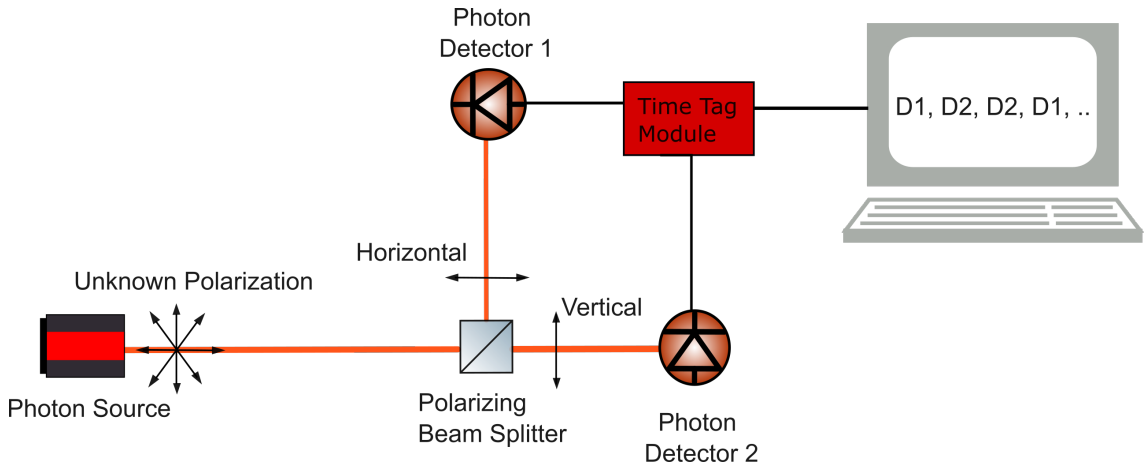


Figure 2.4. Measurement on the quantum channel. In the no-cloning theorem, it is necessary to measure on a particle to detect its state, and it cannot be measured without affecting the system. For example, the measurement result can be determined when the measurement is made on the correct basis, while the measurements made on the wrong basis give an incorrect result and the true state cannot be determined.

On the other hand, when we examine quantum mechanics, it says that in order to learn the state of single particles, it is necessary to measure on particles and that measurement cannot be made without affecting the state of the particle. That is, we cannot learn the state of a particle without affecting it and producing a particle with this state. This situation is called the quantum no-cloning theorem. From here, if we send the code using

quantum mechanical methods, the existence of the eavesdropper will be revealed.

Let's assume that an experimental setup is created as in the Figure 2.4. The aim here is to detect a photon produced in random polarization. When the photon passes through the polarizing beam splitter, its polarization will be defined. Photons, which are vertically and horizontally polarized, are accurately measured, while the projection of photons with horizontal or vertical is measured. Here, the polarization state of the photon would actually be distorted. As the measurer does not know which basis he has, he will have incorrect information and will send incorrect data to the receiver. The photon must be reconstructed in the measured polarization, and false results will be sent to the other party as measurements made on a different basis will measure in false results. This will reveal the presence of someone in the system. The no-cloning theorem explains this situation. In addition, there is one more thing here. As it can be understood from the system, on the quantum channel, it is not possible to sequentially measure and then send the measurement result at the same time. There will be a time difference between these two actions. This will reveal the existence of one in the meantime.

To represent this situation mathematically, let's use the states respectively $\mid 0 \rangle$ and $\mid 1 \rangle$ to describe the horizontal and vertical quantum states. The quantum state of a photon with an arbitrary polarization angle can be written as the superposition of $\mid 0 \rangle$ and $\mid 1 \rangle$.

$$\mid \psi \rangle = \cos(\theta) \mid 0 \rangle + \sin(\theta) \mid 1 \rangle \tag{2.5}$$

The probabilities of measuring the photon with random polarization angle of the 1st and 2nd photon detectors are as follows.

$$P_V = \mid \langle 1 \mid \psi \rangle \mid^2 = (\cos(\theta) \langle 1 \mid 0 \rangle + \sin(\theta) \langle 1 \mid 1 \rangle)^2 = \sin^2(\theta) \tag{2.6}$$

$$P_H = \mid \langle 0 \mid \psi \rangle \mid^2 = (\cos(\theta) \langle 0 \mid 0 \rangle + \sin(\theta) \langle 0 \mid 1 \rangle)^2 = \cos^2(\theta) \tag{2.7}$$

As can be clearly seen from the equation, Eve will be able to measure on a single basis on a photon with a random polarization angle. If the incoming photon makes angle

of $\theta = 0^o$ or $\theta = 90^o$, it will measure correctly, but for other values of θ, it will not be able to measure correctly and will obtain incorrect information and send to Bob. The probability of measuring the photon correctly is $\cos^2(\theta)$ and $\sin^2(\theta)$. As a result, it has been seen that Eve cannot receive information in quantum systems without changing the state of the system.

2.3.3. Qubit

The smallest unit for the transmission of information with the classical method is defined as a bit (binary digit). The bit can only take the values 1 and 0. Similarly, in an electrical switch, 0 is the position representing the off position, and 1 is the on position. However, in quantum information theory the smallest unit for the transmission of information is called as a qubit (quantum bit). The qubit is expressed as a state $\mid \psi \rangle$ in a two-dimensional Hilbert space and it consists of two orthogonal basis vectors which are $\mid 0 \rangle$ and $\mid 1 \rangle$. The main difference between them is that in the classical system a bit has a definite value of 0 or 1, whereas the state of a qubit is uncertain. There is a quantum superposition of 0 and 1 in a qubit. In this sense, the qubit is:

$$\mid \psi \rangle = \alpha \mid 0 \rangle + \beta \mid 1 \rangle \tag{2.8}$$

Here α and β are probability amplitudes and in general both can be in complex numbers. If this qubit is measured in standard basis, the probabilities of them are $\mid \alpha \mid^2 \mid 0 \rangle$ or $\mid \beta \mid^2 \mid 1 \rangle$. Since the absolute squares of their amplitudes are equal to their probabilities of measurements and the sum of all the probabilities have to equal one, the following should be constrained by the equation α and β:

$$\mid \alpha \mid^2 + \mid \beta \mid^2 = 1 \;\; and \;\; \langle \psi \mid \psi \rangle = 1 \tag{2.9}$$

The probability of a single qubit state can also be expressed with a Bloch sphere, which is shown in Figure 2.5 shows the qubit representation on a block sphere.

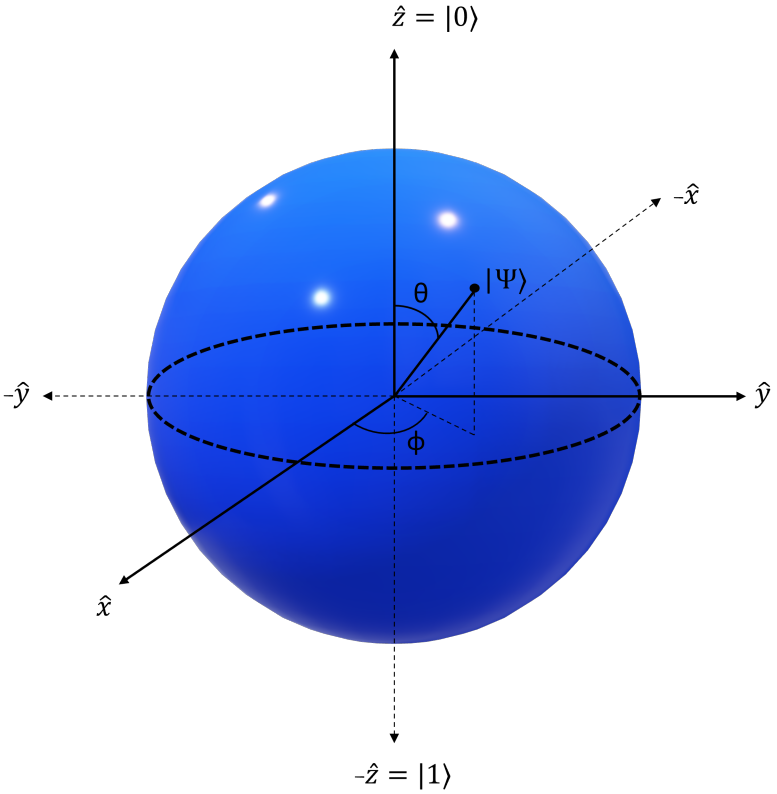


Figure 2.5. Representation of the qubit on the Bloch Sphere

The probability state density on the Bloch sphere can be given as,

$$| \psi \rangle = \cos\left(\frac{\theta}{2}\right) | 0 \rangle + e^{-i\phi} \sin\left(\frac{\theta}{2}\right) | 1 \rangle \ \ and \ \ | \alpha |^2 + | \beta |^2 = 1 \tag{2.10}$$

Here, a Qubit can be represented by any 2-level system. The polarization of a photon behaves like a particle with spin $\frac{1}{2}$, and this can be represented in terms of its eigenfunctions. For instance, $| 0 \rangle = |\downarrow \rangle$ and $| 1 \rangle = |\uparrow \rangle$ are eigenfunctions of a particle with spin $\frac{1}{2}$. In 2 dimensional Hilbert space, the particle with spin $\frac{1}{2}$ has 3 conjugate bases, denoted as eigenfunctions of the operators σ_z, σ_y and σ_x. Further, the eigenfunctions are $\sigma_z = | 0 \rangle + | 1 \rangle$,$\sigma_y = \frac{1}{\sqrt{2}}(| 0 \rangle \pm i | 1 \rangle)$, $\sigma_x = \frac{1}{\sqrt{2}}(| 0 \rangle \pm | 1 \rangle)$. When we apply this notation for the experimental setup, the following Figure will emerge. The basis

functions for the orthogonal basis are $\mid H \rangle$ and $\mid V \rangle$, while the basis functions for the non-orthogonal basis are $\mid 45 \rangle$ and $\mid 135 \rangle$. Also, $\mid L \rangle$ (left) and $\mid R \rangle$ (right) corresponding to the eigenvectors σ_y and σ_x are circular. This special case is called the Poincare sphere.

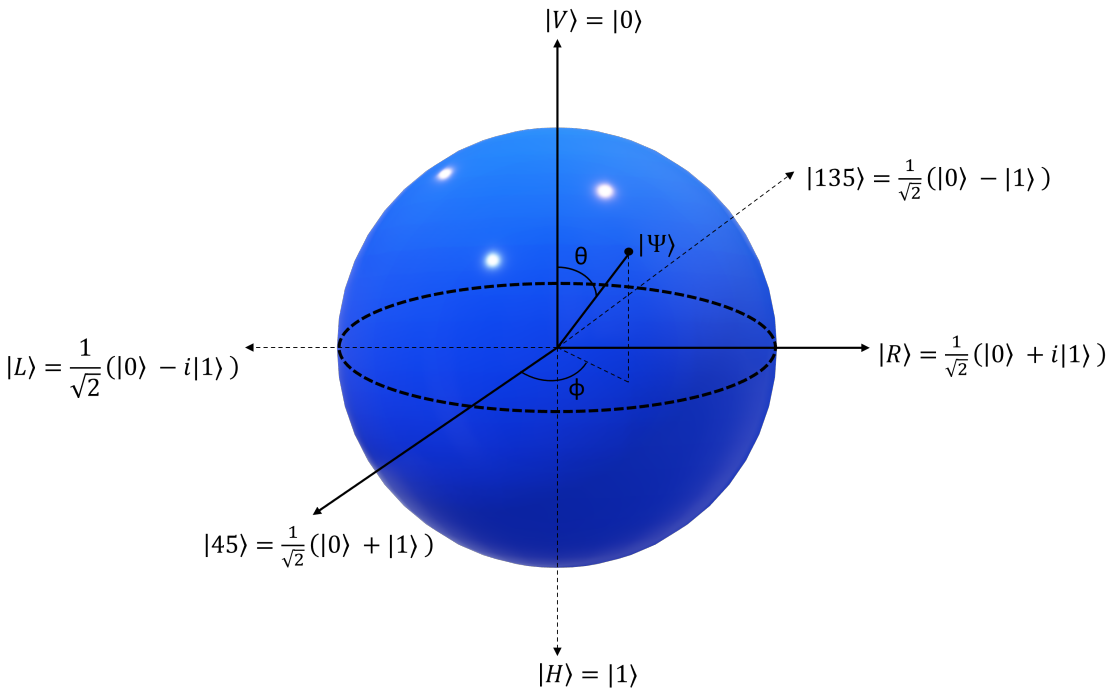


Figure 2.6. Representation of the qubit on the Poincare Sphere. Qubits are superposition of 1 and 0.

2.4. Protocols of Quantum Cryptography

Quantum key distribution is the system that enables the generation of the unbreakable and unobtainable key necessary for secure communication. With the generated key, the information can be encrypted and this encrypted information can be shared through the open channel safely. The receiver can decrypt the information by the key. In this

section, the protocols used for key sharing will be discussed.

There are many quantum key distribution protocols. The most common ones are the BB84 protocol, B92 protocol, E91 protocol and BBM92 protocol. Each protocol has its own, advantages and disadvantages. Additionally, some protocols use single photons as photon sources, while some protocols use polarization-entangled photon pairs. In addition, some protocols transmit a pre-prepared key, and the receiver measures this key, while in some protocols they determine the key between them according to the measurement they made. QKD protocols are divided into two according to the source used. These are protocols using entangled photon pairs and preparing and measuring protocols. Examples of protocols using photon pairs are E91 and BBM92. On the other hand, BB84 and B92 protocols can be given as examples of protocols with sequential polarization.

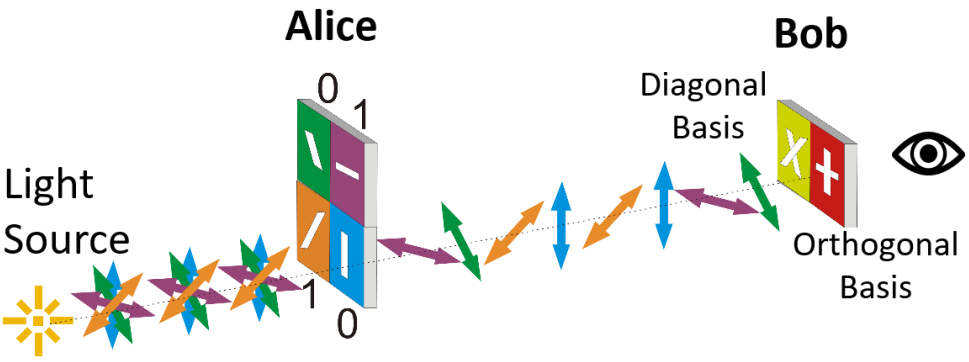
2.4.1. BB84

Quantum key distribution was developed in the USA in 1984 in order to solve the problem of secure key distribution by physicist Charles Henry Bennett and Canadian cryptographer Gilles Brassard. The protocol was named BB84 by combining the first letters of their surnames and the year information of the study (Bennett and Brassard, 2014). In Figure 2.7, simple representation of the BB84 protocol is shown.

They tried the BB84 protocol in the open-air laboratory in 1989 and succeeded in transferring information at a rate of 10 bits/second with a distance of 30 cm between two ends. Today, these values are increased by fiber optic cable up to 307 km (Korzh et al., 2015) in communications, and 144 km for air (Ursin et al., 2007) and speeds of 1Mbps have also been reached (Dixon et al., 2008).

The photon and its polarization nature are used as a quantum particle to transport each bit of the secret key to be used for secure communication in the BB84 protocol. (Wolf, 2021; Roe, 1998; Nielsen et al., 2002). Figure 2.8 shows the basic flow of the steps of the BB84 Protocol.

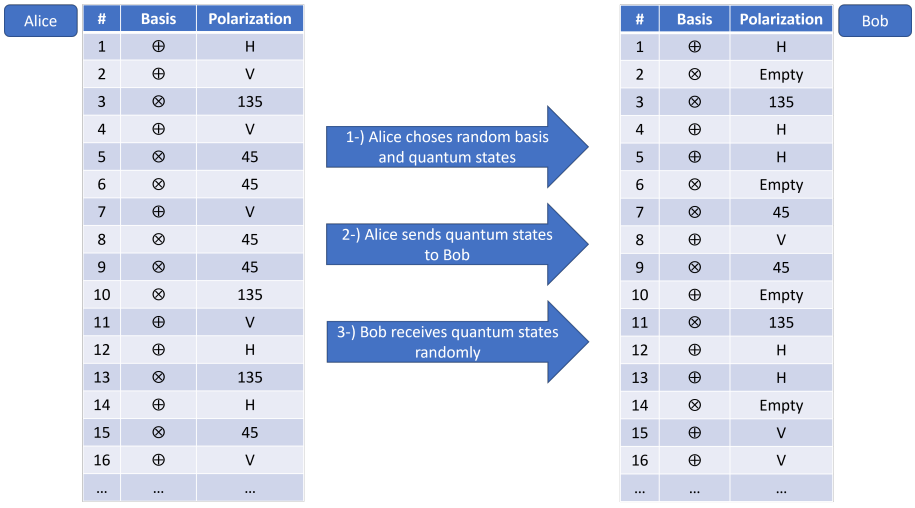
In this section, to describe how to solve the Quantum key distribution problem using quantum mechanics by the BB84 protocol. Figure 2.8 shows the basic flow used by quantum key distributions with BB84 Protocol.



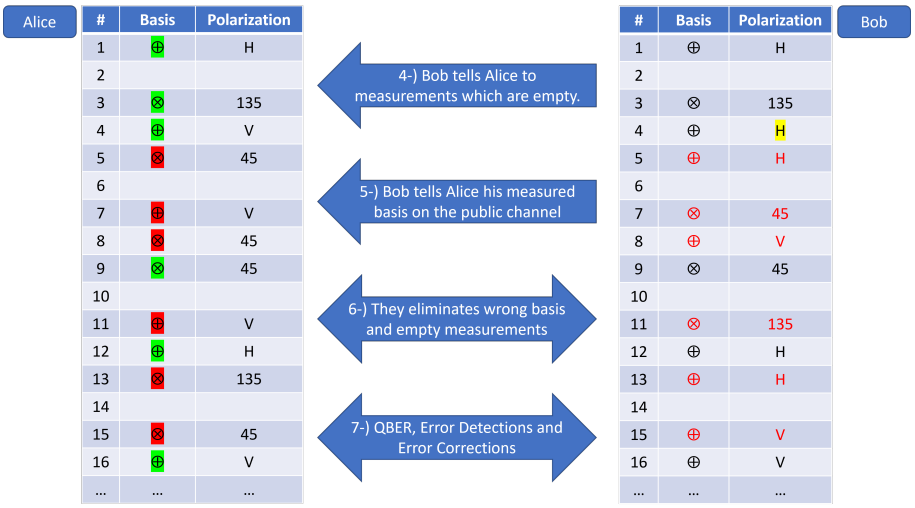
Bit	0	1	0	1
Basis	⊕	⊕	⊗	⊗
Polarization	↕	↔	↘	↗

Figure 2.7. Basic representation of the BB84 protocol. Each bit of the secret key is encoded in the direction of the polarization of the photon. It is used a non-orthogonal two basis, four states. One basis must give the value 0.5 value of its conjugate to the other basis horizontal ($|\ H\ \rangle$), vertical ($|\ V\ \rangle$), 45 degrees ($|\ 45\ \rangle$), and 135 degrees ($|\ 135\ \rangle$), Alice and Bob select their basis randomly and 50% of measurements are rejected. The key must be sifted because of the chance of different basis selection.

In the BB84 protocol, two non-orthogonal basis and 4 quantum states are used. One basis must give the value $\frac{1}{2}$ of its conjugate to the other base. These quantum states are horizontal ($|\ H\ \rangle$), vertical ($|\ V\ \rangle$), 45 degrees (45), and 135 degrees (135), and each correspond to the directions of polarizations of the photons.



(a)



(b)

Figure 2.8. BB84 protocol raw key and sifted key generation. In Figure (a), Alice sends the photons she chooses in random basis and polarizations to Bob, and Bob measures the incoming photons again on random basis. In Figure (b), after Bob shares the empty measurements and the measurements he made on the wrong basis with Alice over the classical channel, these measurements are mutually eliminated and the sifted key is created. Incorrect measurements are found and corrected by error detection and error correction methods.

If we talk about the operation of the system, the Alice part sends the randomly selected states among these 4 quantum states to Bob. The synchronization of Alice and Bob is an important point here. Bob, on the other hand, measures the random quantum states Alice sends by random selection of basis. Here, if Alice and Bob choose the same basis, Bob measures (correlated) with perfect accuracy. However, if Alice and Bob choose different bases, Bob gets an uncorrelated result. Next, Bob has recorded a series of measurements. This is called a raw key. Later, Alice and Bob share the base information of the quantum states they sent without sharing the key, and sharing the base information does not compromise the security of the key because the key has already been shared. Matching bases are considered the correct measurement and ignore the others. In this section, 50% of the key is discarded because of different basis measurements, and the remainder of the key is called the sifted key.

An important point emerges here. Alice and Bob can't interfere with the creation of the key in any way. They both get the key by making random choices. The key comes into existence by their random selections.

Alice

#	Basis	Polarization	Key
1	⊕	H	0
2	⊗	135	1
3	⊕	V	1
4	⊗	45	0
5	⊕	H	0
6	⊕	V	1
...	...	...	...

H=0, V=1, 45=0, 135=1

Bob

#	Basis	Polarization	Key
1	⊕	H	0
2	⊗	135	1
3	⊕	V	1
4	⊗	45	0
5	⊕	H	0
6	⊕	V	1
...	...	...	...

H=0, V=1, 45=0, 135=1

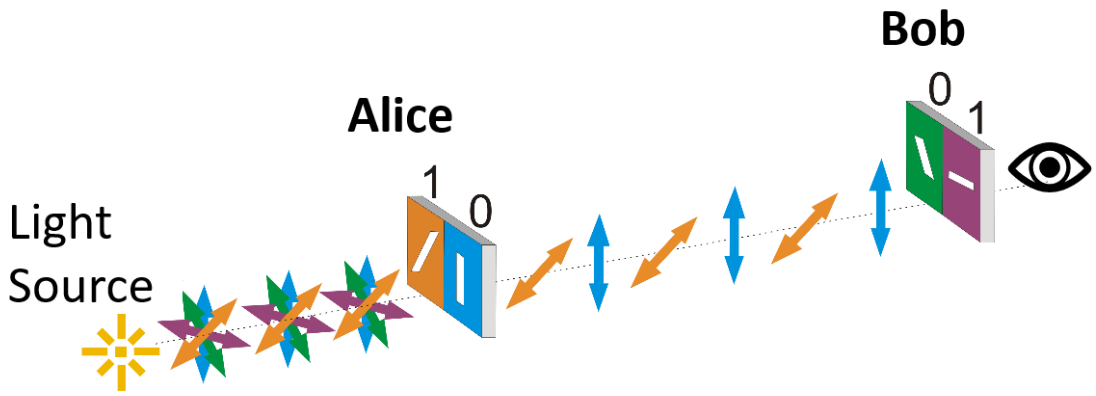
Figure 2.9. Corrected secure key. The measurements are converted to bit-matches and the key is obtained.

Therefore, the bitstream they will use as the secret key will be less than the bitstream generated first. In the last step, the transmitter and receiver pass the stage of detecting and correcting errors in the bit sequence to transmit over the noisy quantum

channel. This error detection and correction step are made from a classic/noiseless channel. This process includes Error Detection and Correction techniques, e.g. CASCADE protocol.

As a result of a successful Error Detection and Correction, the transmitter and receiver obtain a bit sequence (secret key) with exactly the same values.

2.4.2. B92



Bit	Alice 0	Alice 1	Bob 0	Bob 1
Basis	⊕	⊗	⊗	⊕
Polarization	↕	↘	↗	↔

Figure 2.10. Basic representation of the B92 protocol. The B92 protocol is a simplified version of the BB84 protocol. Two non-perpendicular basis and two states are used. Each bit is encoded in the polarization directions. The table shows the bit equivalent of the polarization and basis of Alice and Bob.

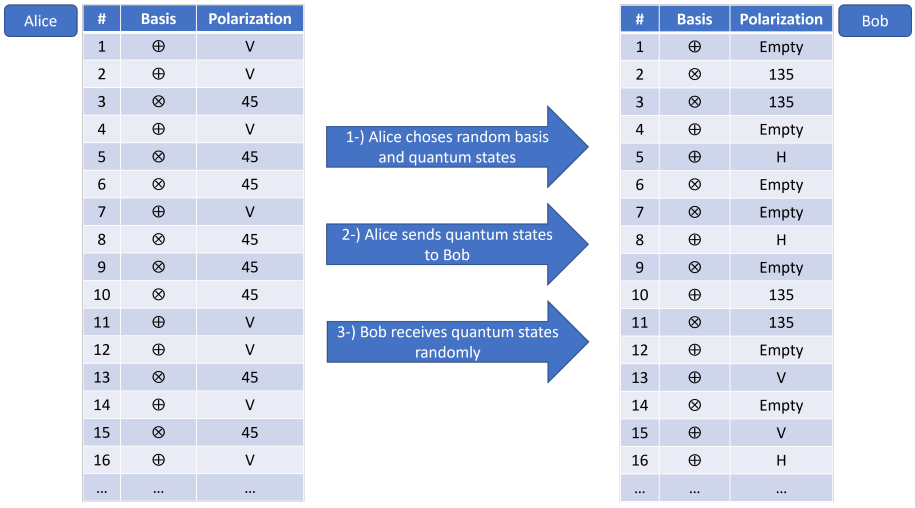
The B92 protocol is a prepare and measure based QKD protocol proposed by Bennet in 1992 (Bennett, 1992). In fact, it is basically a simplified version of the BB84 protocol. Instead of the 4 photon polarization used in the BB84 protocol, 2 photon polar-

ization directions are used, provided that they are on a different basis. In the B92 protocol, it is encoded as 0 bits in the vertical direction or 0 bits in the horizontal direction, 45 degrees or 135 degrees 1 bit.On the other hand, Alice will measure 0 bit in 135 or 45 degrees respectively according to the selected direction, and 1 bit in the horizontal or vertical direction, respectively, according to the selected direction. Here, in fact, half of the photons are automatically ejected from the system. If Bob chooses the wrong basis, all photons will be thrown out of the system and Bob will measure nothing. This situation is called deletion in quantum mechanics (Bruss et al., 2007). Moreover, in the B92 protocol, the measured raw data directly constitutes the key and the key itself is the result of the measurement. As in the BB84 protocol, Alice and Bob do not need to compare their basis in the B92. In Figure 2.10, simple representation of the B92 protocol is shown.

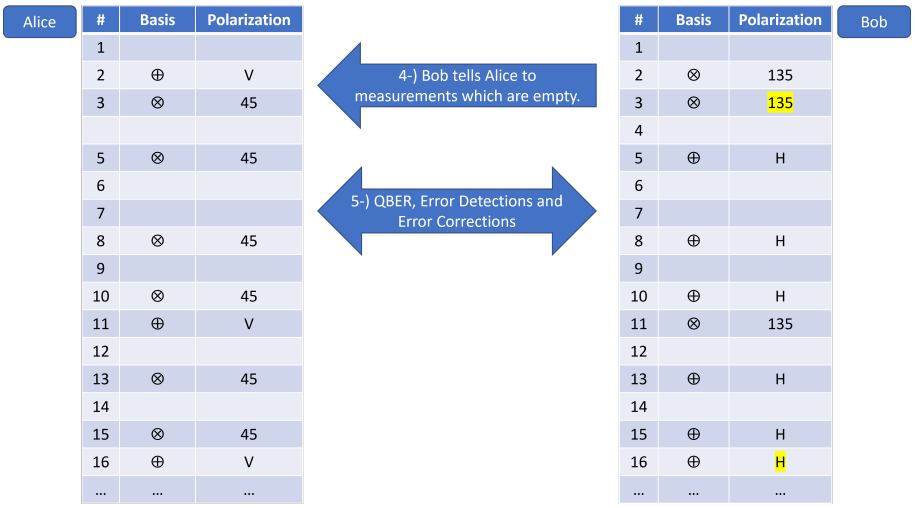
B92 protocol uses two non-orthogonal basis and 2 quantum states. A basis must give the $\frac{1}{2}$ value of its conjugate to the other basis. These quantum states are horizontal ($\mid H \rangle$) and 45 degrees (45) or vertical ($\mid V \rangle$) and 135 degrees (135), and each corresponds to the polarization directions of the photons.

If we talk about the functioning of the system, Alice sends randomly selected states among these 2 quantum states to Bob. The synchronization of Alice and Bob is also very important here. Bob measures the random quantum states that Alice sends with a random selection of basis. Here, if Alice and Bob choose different bases at the same time, Bob has a $\%50$ chance to measure correctly or the photon will be ejected from the system. However, if Alice and Bob choose the same base at the same time, Bob gets no results and the photon is thrown directly from the system. Next, Bob records a series of measurements, and this is called a key. Here, unlike the BB84 protocol, they do not share any bases. Because on whatever basis Alice sent, if Bob made a measurement, it means that he measured on the opposite basis. The measurement taken by Bob is considered the correct measurement. Bob can measure only $\%25$ of the photons sent by Alice in this part.

Afterwards, QBER, error detection, and correction are performed and the correct key is obtained.



(a)



(b)

Figure 2.11. Working principle of B92. In Figure (a), Alice sends the photons to Bob, randomly at the two selected non-orthogonal polarization direction. Bob makes measurements randomly at the other two polarization direction. Empty measurements are due to both non-ideal optical elements and detectors, and the B92 protocol. In Figure (b), the raw key generated after eliminating empty measurements. Yellow measurements on the Bob side indicate incorrect measurements due to experimental errors. Incorrect measurements are found and corrected by error detection and error correction methods.

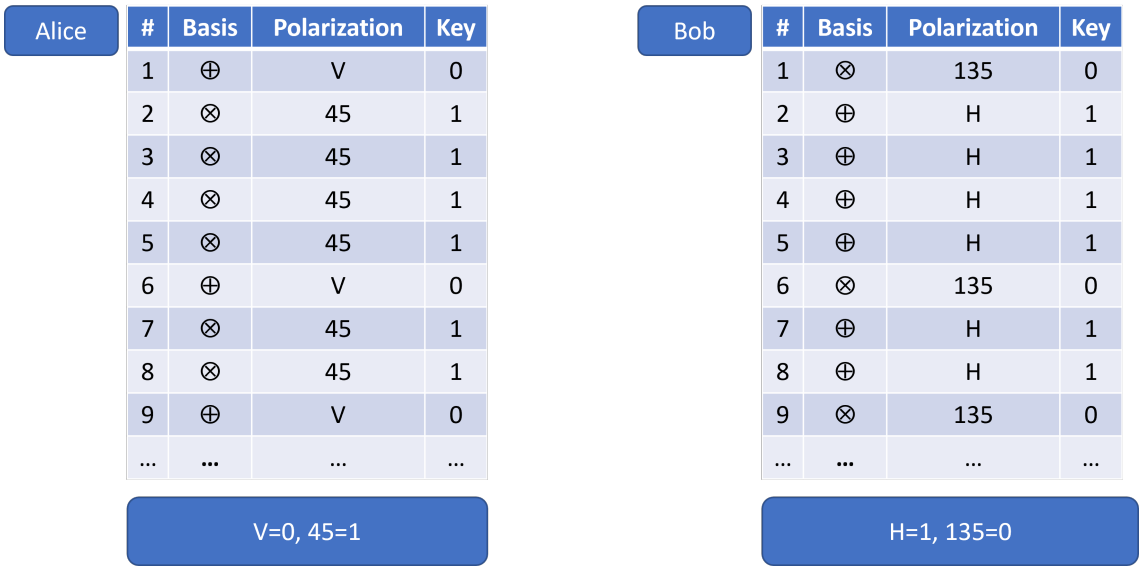


Figure 2.12. Corrected secure key. The obtained measurements are converted to the corresponding bit state. Then, the key is obtained.

2.4.3. Other Protocols

Over the years, many quantum key distribution protocols have been developed. Although some protocols show similarities with each other in terms of working principle, there are many differences between them, such as the type of photon source and the way the key is prepared. In this section, brief information about other protocols will be given. There are many protocols other than the ones mentioned.

2.4.3.1. E91 (Ekert or EPR Protocol)

In 1935, A. Einstein, B. Podolsky, and N. Rosen first mentioned the EPR paradox in their article (Einstein et al., 1935). In the paper, entangled particle pairs had an interesting property between them. If a measurement is made on one of these entangled pairs of particles, the state of the other is also determined. In addition, this happens instantaneously. The discovery of this surprising effect later paved the way for new studies. These studies are quantum cloning, quantum teleportation, quantum key distribution, and

quantum dense coding.

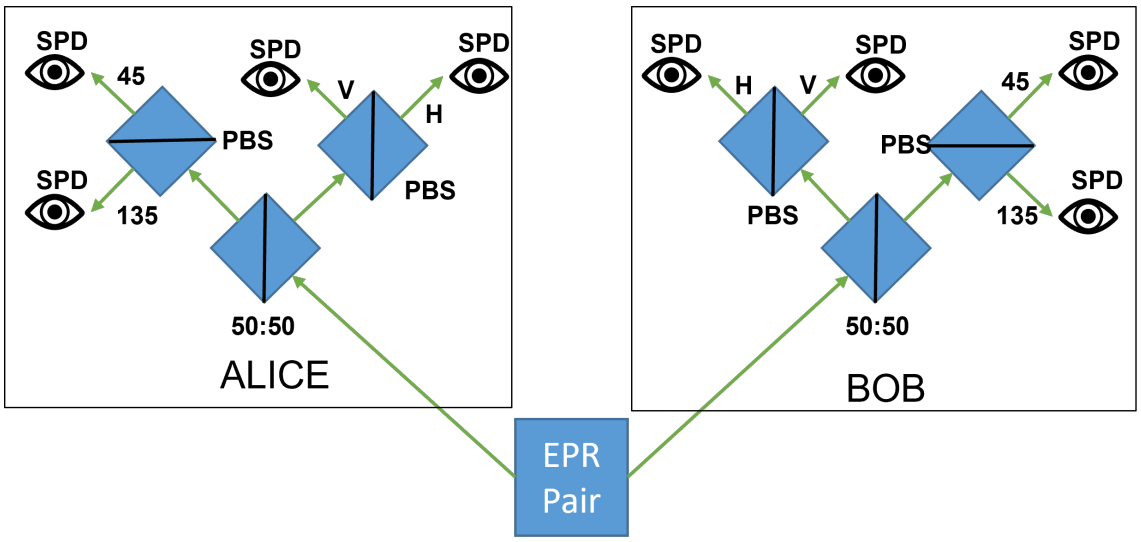


Figure 2.13. Basic representation of the E91 protocol. One of the polarization-entangled photon pairs are sent to Alice and the other one is sent to Bob. Alice and Bob choose a random basis to detect photons by 50% chance. After that, photons are selected by polarization direction. If both Alice and Bob choose a true basis at the same time, measurement is considered correct. Otherwise, the measurement is discarded. For example, if Alice measures H, Bob must measure V or vice versa. If Alice measure 45, Bob must measure 135 or vice versa.

Later in 1991, Artur Ekert suggested in his article that quantum key distribution can be made with entangled photon pairs, and it was called the E91 protocol (Ekert, 1991). Alice and Bob generate the key using a source of entangled photon pairs placed between them. Alice and Bob make random and independent measurements on the incoming photons (H-V basis or 45-135) and then compare the basis of the measurements between them. They separate measurements that coincide on the same basis and eliminate the others. Thus, they get opposite measurements between them. That is, if Alice measures in the vertical direction, it means that Bob has measured in the horizontal direction. Using this method, they can distribute keys among themselves.

However, they failed to determine that the key was secret. In order to determine the security of the key, they will use the measurements they have made on a different basis. Since they will not use this part of the key, they can compare this part between them on an open channel and understand whether there is listening or not. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt (CHSH) inequality is used for this control (Clauser et al., 1969). This inequality is actually a derivative of Bell's inequality (BELL, 1995). In those circumstances of the Ekert protocol where Alice and Bob measure on a distinct basis, the CHSH inequality establishes a constraint for classically coupled particles that is maximally violated by quantum correlations. Since the discarded part of the key will also supply the obtained key itself, these inequality results are valid for the entire key. In Figure 2.13, a schematic representation of the E92 protocol is shown.

The most important feature of this protocol is that there is no need to rely on the photon source. Thus, with this protocol, it is safer to distribute keys between satellites or to distribute keys over very long distances.

2.4.3.2. BBM92 protocol

The BBM92 protocol is a protocol that uses polarization-entangled photon pairs. Basically, both the key exchange mechanism and the key elimination mechanism are very similar to the BB84 protocol. This protocol was found by Bennett, Brassard, and Mermin in 1992 after Ekert suggested in 1991 that entangled photons could be used in QKD systems. The photon pairs with polarization-entangled produced have different wavelengths from each other. With a dichroic mirror, these photons are split into two separate paths and are measured by the two receivers. In this protocol, Alice also has a receiver part. Alice and Bob compare the photons they have measured. If Alice measured vertically, Bob should measure in horizontal polarization. If Alice measured 45 degrees, Bob should measure at 135 degrees of polarization (Bennett et al., 1992; Schimpf et al., 2021). In Figure 2.13, a schematic representation of the BBM92 protocol is shown.

This protocol is very similar to the E91 protocol. The only difference is that for security control, the E91 protocol uses CHSH inequality, while the BBM92 protocol uses raw key and QBER like B92 protocol.

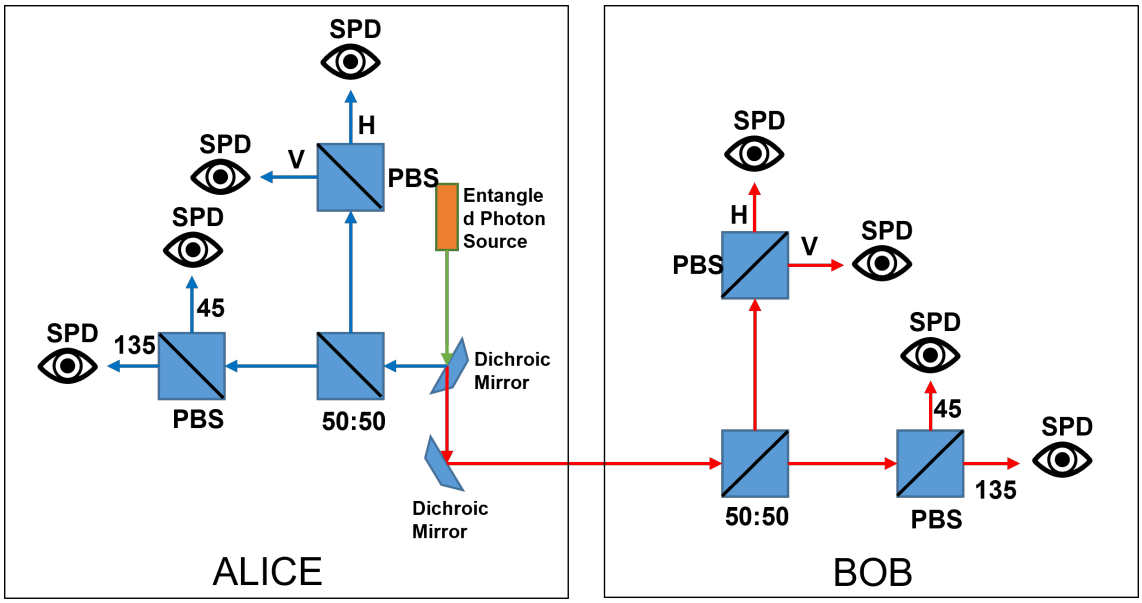


Figure 2.14. Basic representation of the BBM92 protocol. In this protocol, polarization-entangled photon pairs have different wavelengths. One of the photons is sent to Alice and the other one is sent to Bob. Alice and Bob choose a random basis to detect photons by 50% chance. After that, photons are selected by polarization direction. If both Alice and Bob choose a true basis at the same time, measurement is considered correct. Otherwise, the measurement is discarded. For example, if Alice measures H, Bob must measure V or vice versa. If Alice measure 45, Bob must measure 135 or vice versa.

2.5. Photon Statistics

The main idea of quantum optics is to study the beam of light as a distribution of photon or wave packets rather than as a classical wave. Thus, when various light sources such as single-photon sources, lasers, thermal lights, etc. are studied, they show different distributions and characteristics. These properties can easily be explained by quantum theory and statistics rather than classical theory. In this section, the statistical properties of a photon stream are going to be examined.

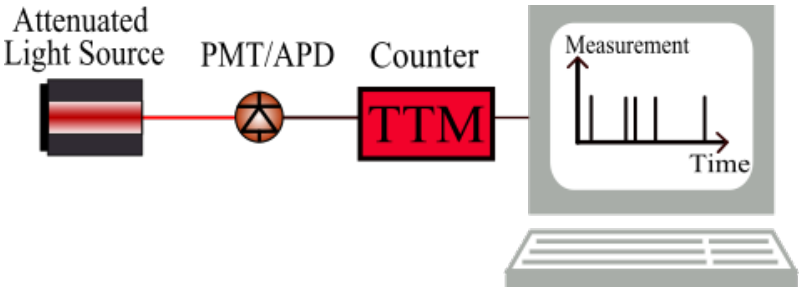


Figure 2.15. Detection of photon. In order to obtain the photon statistics of the photon source, a sensor that can measure a single photon (APD, PMT, etc.) and a time stamp that can record the time of this measurement in high resolution are required.

There are three different types of photon statistics which are Poissonian statistics, sub-Poissonian statistics, and super-Poissonian statistics. Except for sub-Poissonian statistics, observations of other statistics types with photo-detectors are compatible with the classical light theory. Therefore, the observation of the sub-Poissonian photon statistics is due to the photon nature of light. An illustration of a photon statistics measurement by a photon counter is shown in Figure 2.15. While photon is being counted, very sensitive light detectors are used such as avalanche photodiode (APD) or photomultiplier tube (PMT) and they are connected to an electronic circuit that works as a counter. The counter detects every single signal from the photon detector and each measurement is registered by the counter within a certain time interval (Fox, 2006).

Equation of Poisson distribution is shown in Eqn. 2.11.

$$\mathcal{P}(n) = \frac{\langle n \rangle^n}{n!} e^{-\langle n \rangle} \text{ and } n = 0, 1, 2, ... \tag{2.11}$$

$$n = \frac{\Phi L}{c} \, , \Phi = \frac{P}{\hbar \omega} \tag{2.12}$$

Here, Φ is photon flux and it can be defined as the ratio of energy flux to individual photon energy. Moreover, n is an average number of the photon in a beam segment and it can be defined as the length of beam segment (L) is multiplied by photon flux and they

divided by the speed of light (c).

The standard deviation for fluctuations in the number of photons above and below the mean value can be expressed as;

$$\Delta n = \sqrt{\langle n \rangle} \tag{2.13}$$

However, this situation can be defined for a perfectly coherent light beam with constant optical power, and from a classical viewpoint, a beam of constant intensity and perfect harmony is the most stable type of light imaginable. Thus, this situation allows us to classify light types according to photon statistics according to the standard deviation (STD) of their photon number distribution. Generally, there are 3 cases for a light with photon statistics. These are

1-) If STD of photon distribution of light is $\Delta n = \sqrt{\langle n \rangle}$, it is called Poisson statistics.

2-) If STD of photon distribution of light is $\Delta n < \sqrt{\langle n \rangle}$, it is called sub-Poisson statistics.

3-) If STD of photon distribution of light is $\Delta n > \sqrt{\langle n \rangle}$, it is called super-Poisson statistics.

Poissonian Statistics:

Poissonian statistics exhibit a statistical distribution with $\Delta n = \sqrt{\overline{n}}$ variance. An ideal light source of constant intensity can be modeled as a spatially and temporally coherent electromagnetic wave of a single frequency in classical electromagnetic theory. These light sources can be identified by the following formula.

$$E\left(x,t\right) = E_0\left(kx - \omega t + \phi\right) \tag{2.14}$$

In equation 2.14, E_0 is the amplitude of the electromagnetic field, ω is the frequency of the field, ϕ is a time-independent phase difference and lastly, k is wave vector.

In poissonian statistics, photon distribution of probability is as mentioned before like following equation.

$$\mathcal{P}(n) = \frac{\langle n \rangle^n}{n!} e^{-\langle n \rangle} \text{ and } n = 0, 1, 2, ... \tag{2.15}$$

Laser sources can be given as an example of light sources with this characteristic.

Super-Poissonian statistics

The situation where the variance of the statistical distribution is $\Delta n > \sqrt{\langle n \rangle}$ is called Super-Poissonian light sources. Examples of such light sources are thermal light sources. In these light sources, the light intensity is constantly fluctuating randomly. Thanks to this feature, the photon statistical distribution differs from other light sources. Photons in Super Poissonian light sources are formalized by the Bose-Einstein distribution. The following probability distribution formula formalizes the Super Poissonian statistics.

$$\mathcal{P}(n) = \frac{1}{(\langle n \rangle + 1)} \left(\frac{\langle n \rangle}{\langle n \rangle + 1} \right)^n \tag{2.16}$$

Sub-Poissonian statistics

The situation where the variance of the statistical distribution is $\Delta n < \sqrt{\langle n \rangle}$ is called. Such light sources cannot be modeled with classical electromagnetic theory. Therefore, in order to model such light sources, it is necessary to quantize the electromagnetic wave. In addition, ultra-fast photon detectors must be used to obtain the statistics of the light source with Sub-Poissonian statistics. Squeezed light sources are examples of light sources with Sub-Poissonian statistics (Fox, 2006).

CHAPTER 3

EXPERIMENTAL ANALYSIS

In 1884, Bennett and his teammates proposed the BB84 protocol and then performed the experiment at a distance of about half a meter. The experiment was carried out using a pulsed green color LED, a polarizer, and a pinhole. Thus, weak pulse signals were generated. With the help of two Pockels cells, a key was added to the weak beam pulses produced and transmitted to the receiver part, which is about half a meter away. Again, a pockels cell was used to randomly select bases in the receiver part, and then they split the rays into different paths using a crystal that separates them according to their polarization direction and measured the photons with the help of a photomultiplier tube. Although they achieved a very low rate, these results proved that the protocol was feasible (Bennett and Brassard, 2014).

After the experiment, optical fiber-based (Lo et al., 2005) and free space-based (Ursin et al., 2007) and underwater systems (Feng et al., 2021) was developed with the developing technology. In addition, different protocols have been developed with their advantages and disadvantages. In addition, attenuated lasers are often used instead of a pulsed LED source. However, due to the security problem created by the attenuated laser source and the waiver of the key rate in order to reduce the security risk, studies have started with single photon sources that can be obtained with a safer and higher key rate. As some photon sources operate at very low temperatures, it has brought different problems with them. Photon sources operating at room temperature were both an inexpensive solution and more practical for quantum key distribution.

In this section, firstly the BB84 protocol will be tried to be performed with the attenuated laser source, then for some reason, it will be turned the optical setup to the B92 protocol and a key will be generated with the attenuated laser successfully. A logo will then be encrypted and decrypted with the generated key. The aim of this thesis is to perform optical setup, electronic control, and software developments in order to realize a quantum key distribution with the help of single photons obtained from hBN defect centers at room temperature. However, QKD could not be performed with a single

photon, since sufficient time could not be found within the scope of this thesis.

In the following sections, first of all, studies related to optical setup will be discussed in order to realize quantum key distribution. Then, the photon source, which is one of the most important features that ensure the security of quantum key distribution, will be examined and the laser pulses will be reduced to a safe level. After that appropriate polarization positions and polarization selections will be made. After this section, synchronization and electronic controllers will be mentioned so that the right photon can be detected at the right time and the key can be added to the photons correctly.

3.1. Optical Setup and Control Program of BB84 Protocol

In the BB84 protocol, there are two parts which are Alice and Bob. Alice is described as a transmitter. She sends photons that have different photon polarization orientations at different time intervals and these are recorded according to the polarization direction of photons and their sent time. Bob is described as a receiver. He receives photons and separates these photons as their direction of polarization and these separated photons are measured by single-photon detectors and these measurements are recorded according to their measured time and which polarization direction of the photon is. Then, recorded Alice's data and Bob's data are compared in terms of their basis. Next, the sifted key is obtained by eliminating false basis match.

This section is going to be focused on the established optical setup of BB84, the optical components used in the optical setup, and their behavior, and the control and analysis programs created to perform sequential controlled experiments will be discussed. In Figure 3.1, the first configuration of the QKD setup with the BB84 protocol is shown. Optical setup will be examined under two titles as Alice and Bob.

3.1.1. Alice

Thanks to this part of the optical setup, the key is created and sent to Bob with basically attenuated pulsed laser source and electro-optic modulator (EOM) for encoding the key to the directions of the polarization of the photons.

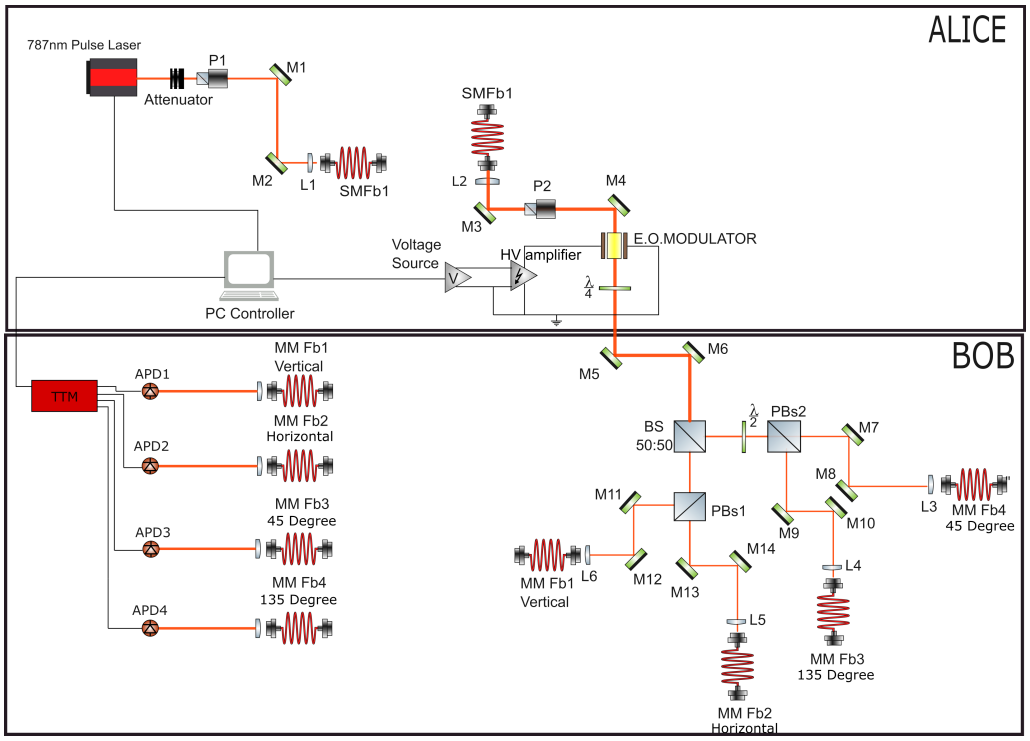


Figure 3.1. First configuration of the BB84 protocol of QKD Optical Setup. In Alice, laser pulses are attenuated with the help of an ND filter and polarizer and then sent to a fiber, then the key is added in the direction of the polarization of the photons. Next, In Bob, incoming photons are split into 2 paths with a 50% chance with BS. Then, with the help of PBS, the selection is made according to the direction of their polarization and measured with single-photon detectors. Measured photons are recorded as measurement time and measured detector by TTM. With a synchronization signal, the key is detected.

In the optical setup of Alice, there is a 787nm Coherent Cube Pulse Laser and it can be pulsed up to 350 MHz. After the laser, there is a polariser. This device not only allows us to determine the direction of the polarization of incoming light but also to attenuate the laser. Attenuation of laser occurs with the help of the polariser by the direction of incoming polarization of light and it reduces laser intensity with a cos^2 function (Malus's Law formula is $I(\Theta) = I_0 cos^2(\Theta)$), so the intensity of the light can be tuned with the angle of the polariser. Thus, the intensity of the laser incoming to the receiver

part of the optical device (BOB) is adjusted. Polarization maintained single-mode fiber (PMFB) is used after the polariser to protect the direction of linear polarization of light thanks to their stress rods, so the polarization of the laser is transferred to the system in a preserved manner, and when it is desired to connect another light source to the system, it can be easily added without disturbing the system. Further, there is an electro-optic modulator (EOM) for changing the direction of polarization of light depending on the applied voltage. Additionally, in the Alice part, there is a polariser (P), that is used to set and precise the direction of the polarization of the incoming laser, and a quarter wave-plate ($\frac{\lambda}{4}$) (QWP), that converts the circular polarization to linear polarization. Furthermore, after the laser, there is an ND filter. This filter sharply reduces the laser intensity to levels that behave like a single photon. This part will be discussed in the next section.

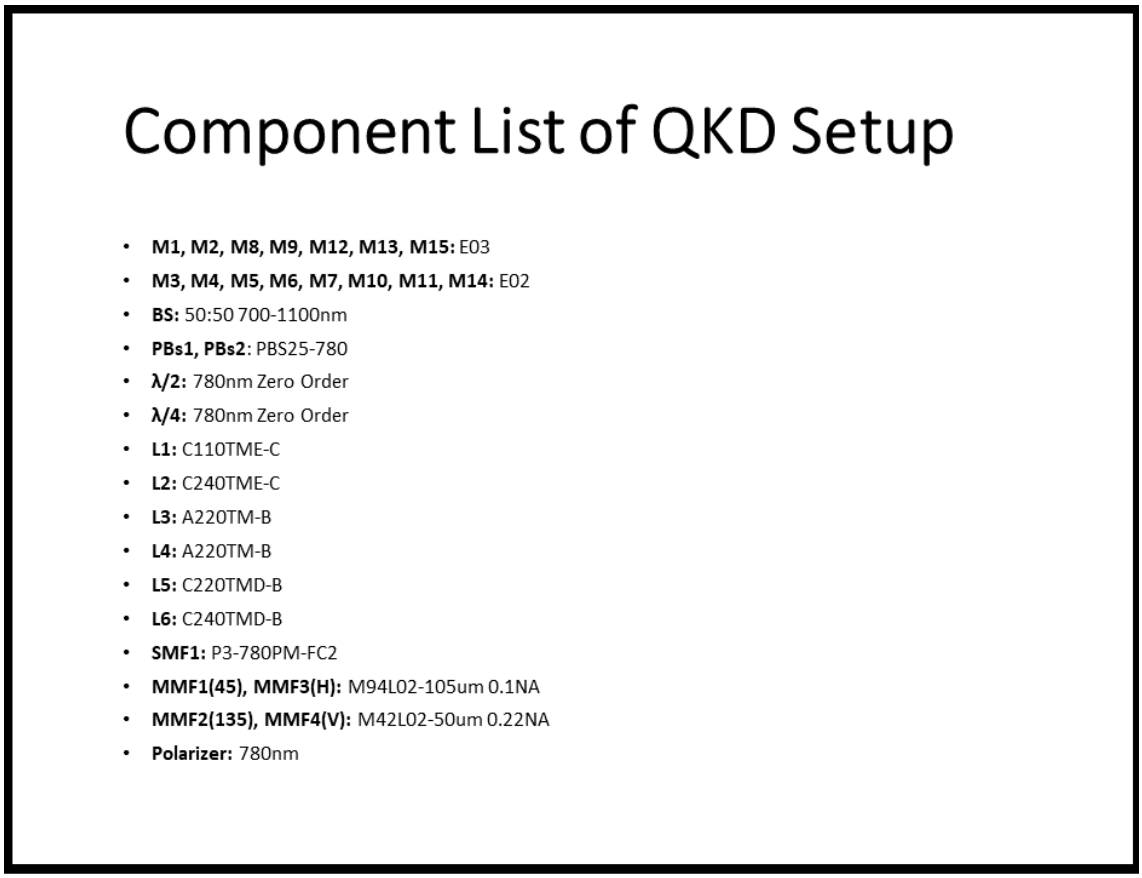


Figure 3.2. List of used optical components in BB84 Protocol

Collimated laser comes out with the lens from PM fiber. Then, thanks to mirrors, it

passes smoothly and uprightly through the polariser and the hole of the modulator. Here, the polarizer is used to determine the polarization of the coming light and it changes the direction of the polarization of the initial light before EOM. The modulator changes the direction of the polarization of the corresponding laser according to the applied voltage between -200V and 200V. The direction of polarization corresponding to the voltage is as follows. 0V equals vertical polarization, -90V and 90V equal 135° and 45° respectively, lastly 180V equals horizontal polarization. After the modulator, there is a quarter wave-plate. This component converts the circular polarization from the modulator to linear polarization. Figure 3.2 shows a list of components that have been used.

3.1.2. Bob

Bob is the name of the receiver design. Thanks to this part of the setup, created keys are received by APDs at four different polarization paths.

When it comes to Bob part of the optical setup, there are beam-splitter (BS), polarization beam-splitters (PBS), half wave-plate ($\frac{\lambda}{2}$)(HWP), multimode fibers (MMFB) and APDs. Figure 3.2 shows a list of components that have been used.

When laser pulses come to 50:50 beam-splitter, it is divided equally into two paths. At one of the paths, there is a half-wave plate. This component changes the direction of polarization to be set two times of its value. It is set at 22.5°. Thus, It rotates at an angle of 45 degrees. The reason for using this setting degree is that when the direction of polarization of coming light is 45° or 135°, it changes the polarization of the light to be perpendicular or parallel to the optical setup. Thus, thanks to the polarization beam-splitter, we can select the photons by the direction of polarization and they are divided into two different paths. The other path selects photons that have horizontally and vertically directions of polarization to separate two different paths. Thus, photons that have four different polarizations are obtained on 4 different ports of PBS's. The photons are coupled into an optical fiber with the help of a lens and two mirrors. However, as can be seen, there is a problem here. The problem is that if photon which has vertical or horizontal polarization choose their non-orthogonal basis port which is PBS2 path after beam splitter or if photon which has 45° or 135° polarization choose their non-orthogonal basis port which is vertical or horizontal after beam splitter, they will transmit or reflect by fifty

percent. This situation will cause incorrect polarization information to be measured but these incorrect measurements will be removed from the key since the basis comparison will be made after the key is sent. Thus, the problem will be solved with this method. This is called key sifting.

3.1.3. Control Program

Controlling the devices used in optical installation from the computer environment is a very important factor. A Labview program was designed to increase the reproducibility of the experiments. Thus, it was provided to make reproducible experiments under similar conditions. The front panel of the designed program is shown in Figure 3.3.

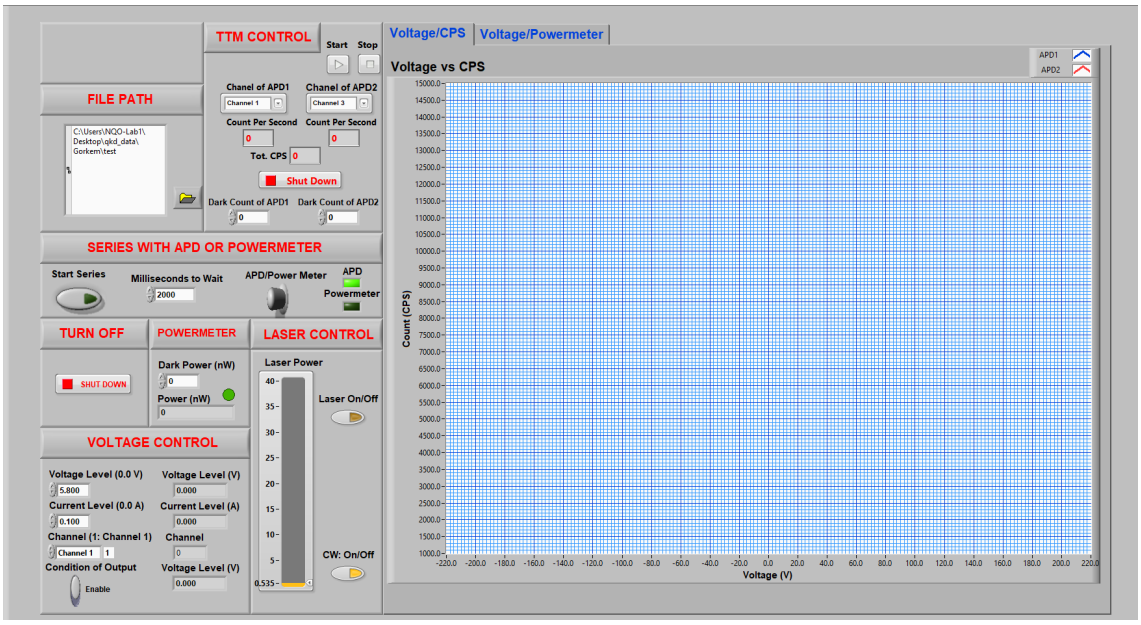


Figure 3.3. The front panel of the Labview program created to control the optical installation via computer

With the help of this program, the power of the laser can be tuned and one can change the mode between continuous and pulsed mode. Moreover, power meter value can be read and also voltage and current of the power source can be controlled and counts

per second which are measured by APDs, can be seen on the screen and lastly program can automatically do voltage-dependent intensity measurement by power-meter or show count per second by APD and it draws instantly the measurement data which comes from APDs or power meter. Furthermore, it writes these measurement data to a text file for the generated Matlab code to analyse the results.

3.2. Photon Statistics and Laser Attenuation

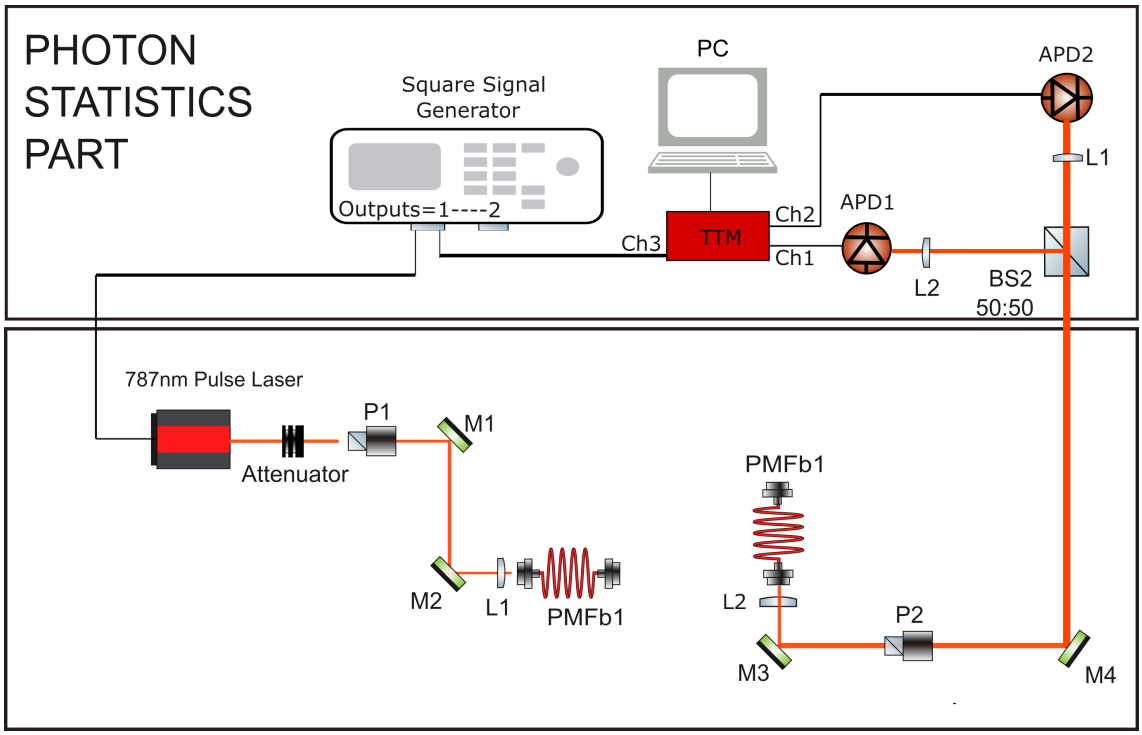


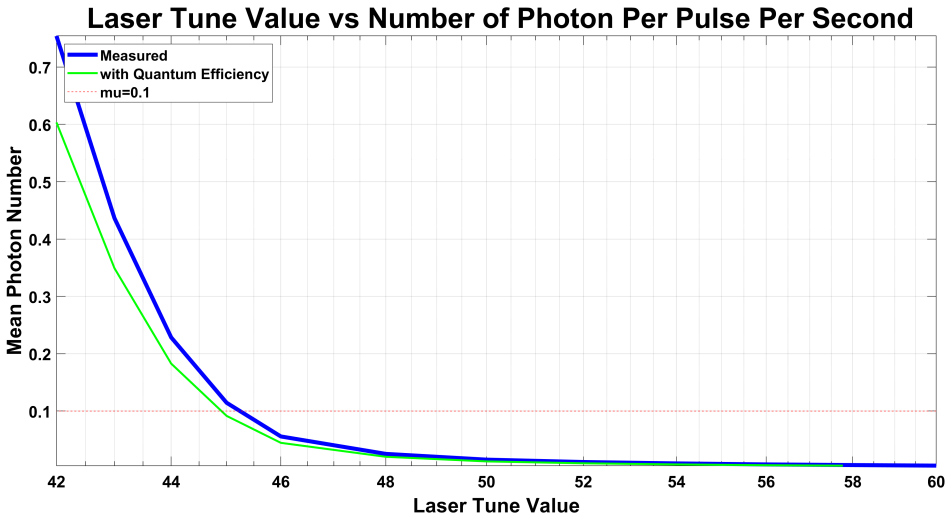
Figure 3.4. Optical setup configuration for photon statistics. The pulsed laser is driven by a signal generator and the same signal is sent to the TTM. Laser pulses are attenuated with the help of an ND filter and polarizer and passed through a BS. Photons reflected and transmitted from the BS are measured by APDs. Measurement results are recorded with TTM. Here, the reason for separating the photons into two separate paths is to determine the number of coincidences and to reduce the dead time of the APDs.

Photon statistics part is one of the most important parts for the security because

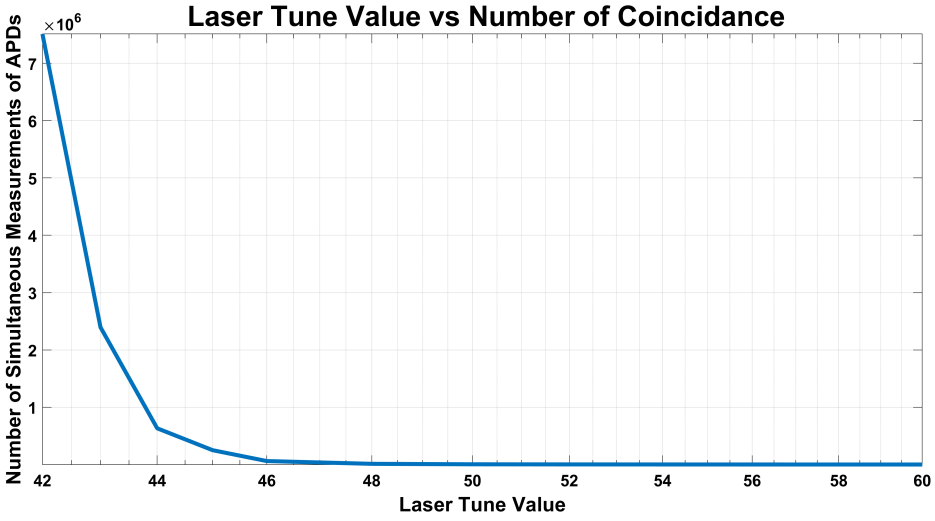
sent photons must behave like a single-photon source. For the security part of the optical setup, sent photons should be measured one by one. The reason for using single-photon is that Eve can attack the quantum channel and Eve can winkle key information out of Bob. If the sent photons are not sent one by one, Eve may obtain all or part of the sent key without Alice realizing that she is eavesdropping. Eve can easily do this with the help of a non-polarizing beam-splitter. If there is more than one photon for each laser pulse, Eve could split the photons into different paths and she can measure the key randomly and can get the key without disturbing the Alice channel. This method is called a photon number splitting attack (PNS). However, there is a problem in using the laser as a single-photon source. Photon statistics of the laser source are Poisson statistics. This means that each number of photons per pulse has a different value and the number of photons for the laser is obtained as an average number in a certain period as mentioned before but, the faint laser can be used for this purpose as a pseudo-single photon source.

Figure 3.4 shows optical setup configuration of photon statistic. Thanks to this optical setup, we can measure the number of photons per pulse per second, so the laser can be attenuated to levels that produce a single photon. In the setup, faint laser photons come to BS and then they are separated into two paths. After that these photons are detected in APDs. The reason for using BS here is to understand if there is more than one photon in each pulse. Since the dead time of the APDs used is very high, after one APD has been measured, the other APD has a chance to measure. In fact, data from two APDs will be collected and will be assumed to be measured with a single APD. Thus, the dead time of the APDs will be halved and it will be determined whether there is a coincidence or not. The laser will be dropped so that one measurement is taken for every ten pulses and minimum coincidence. This corresponds to the level where μ (mean photon number) is 0.1. According to the literature, this level is the level at which the laser can be used as a single-photon source.

In order to find the number of photons per pulse per second, it is sufficient to know the pulse generated by the laser and the number of photons measured. It is also necessary to know the quantum efficiency of the detector. Moreover, all measurements should be normalized to one second. Thus, if detections of channel-5 are counted and the total number of detection of channel-1 and channel-3 are counted and summed, the number of pulses and the number of photons are found.



(a)



(b)

Figure 3.5. Variation of number of coincidence and μ depending on the power of the laser. In Figure (a), the μ calculation was found as the ratio of the total laser pulse to the number of photons measured, then normalized to the second and recalculated at each tune value. The total count divided by the quantum efficiency of the APD to find the number of photons actually sent. In Figure (b), it is obtained by summing the simultaneous measurements made by the APDs at each tune value. As the power of the laser increases, the number of coincidence increases logarithmically.

Then, when this rate is divided by the time passed in the total experiment, the rate for 1 second is obtained. Next, if this rate is divided by the quantum efficiency of the detectors (around 0.80 for 787nm), the number of photons per pulse per second of the optical system is found. Quantum efficiency means the ratio of detection of each photon. Thus, the APD can detect approximately 80 out of 100 incoming photons. In addition, the reduction of the coincidence measurements means that a single photon is produced in the system.

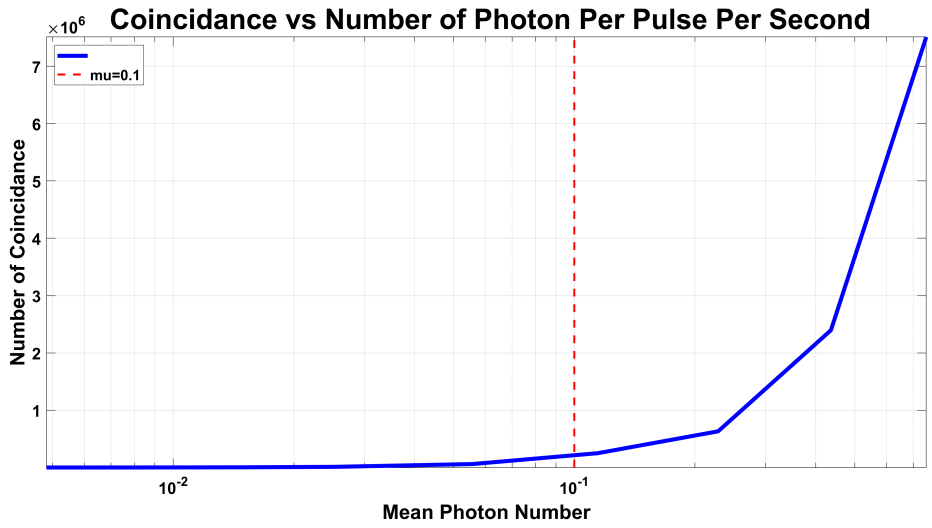


Figure 3.6. Coincidence versus Mean Photon Number. Coincidence increases with increasing mean photon number, as expected.

For 1MHz laser pulse, if we took 1 photon from all pulses, we would measure 1 million photons per second. If we measured 1 photon out of 10 pulses on average, we would measure 100 thousand photons per second, but this is a very ideal situation. The APDs could not measure all photons, so theoretically 80000 photon count per second means that the laser produces approximately 1 photon per every 10 pulses.

Figure 3.5 shows the variation of the number of photons per pulse per second in laser pulses and a number of APD measurements that is at the same time, depending on the power of the laser. When the mean photon number is higher than 0.1, photon counts sharply increase and also the number of coincidences also shows a sudden increase. This

increment means that this is due to the logarithmic increase in the number of photons in each pulse.

Figure 3.6 shows that the number of a coincidence depends on the number of photons per pulse per second. When μ is 0.1, there are still many coincidences. However, single APD measurements are much more than the number of coincidences. The power of the laser can be increased to a value that has minimum coincidence, but the efficiency and count rate of the system also drops because photon measurements per pulse are extremely reduced like 1000:1 or 10000:1, so the most acceptable value is the value where μ is 0.1.

If a single photon source is used as the photon source in the system, the number of photons produced per pulse will increase. Thus, higher measurements per second will be possible. This means an increase in the number of measurements taken per second (rate). As a result, a longer key can be obtained. It also means that besides the more secure transmission of the key, a more secure key can be obtained by sending and receiving a longer key. Here, the laser source limits us and the system operates at lower performance.

3.3. Optical Properties and Theoretical Analysis of The Optical Setup

In this section, the polarization of the photons to be used in the quantum key distribution setup and the various optical tools (Electro-optical modulator (EOM), half-wave plates, quarter waveplates, etc.) used in the optical setup will be mathematically formulated, and the expected behavior of the polarization will be emphasized depending on the configuration in the current system. The base vector of a horizontally or vertically polarized photon is expressed in terms of Jones vectors, respectively, as follows:

$$| H \rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad | V \rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.1}$$

The photon incident at a random angle to the horizontal polarization axis can be expressed by a suitable superposition of the state kets given above. Photons that will be used in addition to horizontal and vertical polarization in the QKD system, making an

angle of 45° (diagonal) and 135° (anti-diagonal) with the horizontal axis, are expressed as follows:

$$| 45 \rangle = \tfrac{1}{\sqrt{2}}\big(| H \rangle + | V \rangle \big) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{3.2}$$

$$| 135 \rangle = \tfrac{1}{\sqrt{2}}\big(| H \rangle - | V \rangle \big) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{3.3}$$

In addition, we can write these diagonal base vectors in terms of anti-diagonal base vectors as follows.

$$| H \rangle = \tfrac{1}{\sqrt{2}}\big(| 45 \rangle + | 135 \rangle \big) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{3.4}$$

$$| V \rangle = \tfrac{1}{\sqrt{2}}\big(| 45 \rangle - | 135 \rangle \big) = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.5}$$

The 4 different polarization directions shown above will be used to generate the key. Let's assume that the photons are sent to the EOM using the necessary optical components, only in the vertical direction. EOM will generate the key by rotating the directions of polarization of these incoming photons in 4 different desired directions. Depending on the voltage applied on the EOM, it changes the polarization directions of the photons passing through it. Optical components that make such effects on the photon are mathematically expressed as operators that act on state kets. For example, a wave plate consists of a birefringent material with different refractive indices (fast and slow axes) in two perpendicular axes. As a photon with a random polarization direction passes through birefringent materials, a phase delay occurs between perpendicular polarization components due to the refractive index difference. This causes the polarization of the photons to change direction. If we want to express this optical component in terms of the Jones matrix, it can be expressed as follows.

$$\hat{O}(\theta,\eta) = \begin{pmatrix} e^{i\frac{\eta}{2}}Cos^2(\theta) + e^{-i\frac{\eta}{2}}Sin^2(\theta) & 2iSin(\frac{\eta}{2})Cos(\theta)Sin(\theta) \\ 2iSin(\frac{\eta}{2})Cos(\theta)Sin(\theta) & e^{-i\frac{\eta}{2}}Cos^2(\theta) + e^{i\frac{\eta}{2}}Sin^2(\theta) \end{pmatrix} \tag{3.6}$$

Here θ and η are respectively the angles of the fast axis of the birefringent material with the horizontal and the relative phase delay between the perpendicular components of the light-induced by the material. For example, the retardation values for half-wave plate (HWP) and quarter-waveplate (QWP) take fixed values such as $\eta = \pi$ and $\eta = \frac{\pi}{2}$, respectively. However, EOM provides a phase delay that varies depending on the voltage applied to it, such as $\eta(V)$. When a vertically polarized photon passes through a modulator positioned in such a way that the fast axis of the crystal is at an angle of 45 $^\circ$ with the horizontal, the changing state ket of its photon is expressed as follows.

$$\begin{aligned} \hat{O}_{EOM}\Big(\frac{\pi}{4},\eta(V)\Big) \mid V \rangle &= \begin{pmatrix} Cos(\frac{\eta(V)}{2}) & i\,Sin(\frac{\eta(V)}{2}) \\ i\,Sin(\frac{\eta(V)}{2}) & Cos(\frac{\eta(V)}{2}) \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} i\,Sin(\frac{\eta(V)}{2}) \\ Cos(\frac{\eta(V)}{2}) \end{pmatrix} \end{aligned} \tag{3.7}$$

As can be seen from the equations, when the phase delay induced by the modulator is not equal to $\eta = 0, \pm\pi, \pm 2\pi \cdots$, it is seen that a photon with linear polarization turns into circular polarization. This is due to the formation of a relative phase difference between the polarization components. In other words, photons with the polarization of 45 and 135 degrees that we want to achieve create undesirable effects. The experimental results of these undesirable effects will be shown later.

To correct this undesirable effect, a QWP should be used at the output of the modulator with the fast axis parallel to the horizontal ($\theta = 0^\circ$). After placing the QWP in the system in the appropriate position, the state of the photon can be expressed as follows.

$$\begin{aligned}
\hat{O}_{QWP}\Big(0,\frac{\pi}{4}\Big)\,\hat{O}_{EOM}\Big(\frac{\pi}{4},\eta(V)\Big)\mid V\rangle &= \begin{pmatrix} e^{i\frac{\pi}{4}} & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix}\begin{pmatrix} i\,Sin(\frac{\eta(V)}{2}) \\ Cos(\frac{\eta(V)}{2}) \end{pmatrix} \\
&= \begin{pmatrix} e^{i\frac{\pi}{4}}\,e^{i\frac{\pi}{2}}\,Sin(\frac{\eta(V)}{2}) \\ e^{-i\frac{\pi}{4}}\,Cos(\frac{\eta(V)}{2}) \end{pmatrix} \\
&= e^{-i\frac{\pi}{4}}\begin{pmatrix} Sin(\frac{\eta(V)}{2}) \\ Cos(\frac{\eta(V)}{2}) \end{pmatrix} \qquad (3.8)
\end{aligned}$$

As can be seen in Equation (3.8), a right-angled QWP converts circularly polarized photons originating from the modulator into linear polarization. Also, as can be seen from the equation, the QWP angle has no dependence on the voltage applied to the EOM.

In order to obtain a better interpretation, if we write the above equation as the superposition of the horizontal and vertical polarizations, we get an equation like the one below.

$$\hat{O}_{QWP}\Big(0,\frac{\pi}{4}\Big)\,\hat{O}_{EOM}\Big(\frac{\pi}{4},\eta(V)\Big)\mid V\rangle = e^{-i\frac{\pi}{4}}\begin{pmatrix} Sin(\frac{\eta(V)}{2}) \\ Cos(\frac{\eta(V)}{2}) \end{pmatrix} \qquad (3.9)$$

$$\begin{aligned}
\hat{O}_{QWP}\Big(0,\frac{\pi}{4}\Big)\,\hat{O}_{EOM}\Big(\frac{\pi}{4},\eta(V)\Big)\mid V\rangle &= e^{-i\frac{\pi}{4}}\Big(Sin(\frac{\eta(V)}{2})\mid H\rangle \\
&\quad + Cos(\frac{\eta(V)}{2})\mid V\rangle\Big) \qquad (3.10)
\end{aligned}$$

The common phase factor $e^{\frac{-i\pi}{4}}$ in the equation appears to have no effect on the direction of polarization because of constant value. Since the common phase factor is a scalar factor, it gives the state of a photon with the same physical state ket at a different instant. Another important effect is that the effect of the voltage value applied to the EOM only changes the direction of the photon's polarization without deteriorating the linearity of polarization. Special voltage values should also be mentioned here. The voltage required to change the polarization direction of a photon whose polarization is perpendicular to the axis by 90 degrees (π) is called V_π. Thus, vertically polarized photons coming to the EOM, where this voltage is applied, come out of the modulator horizontally. In

the table below, the variation of the photon with a vertical polarization depending on the applied voltage values is obtained by using the above equations.

Polarization of Incoming Photon	↕	↕	↕	↕	↕	↕	↕	↕	↕
Voltage Applied to EOM (V)	$-V_\pi$	$-\frac{3V_\pi}{4}$	$-\frac{V_\pi}{2}$	$-\frac{V_\pi}{4}$	0	$\frac{V_\pi}{4}$	$\frac{V_\pi}{2}$	$\frac{3V_\pi}{4}$	V_π
Phase Delay η(V)	$-\pi$	$-\frac{3\pi}{4}$	$-\frac{\pi}{2}$	$-\frac{\pi}{4}$	0	$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{3\pi}{4}$	π
EOM Output (θ=45°, η(V))	↔	⬭	○	⬭	↕	⬭	○	⬭	↔
QWP Output (θ=0°, η(V)=$\frac{\pi}{2}$)	↔	↗	↗	↗	↕	↘	↘	↘	↔

Figure 3.7. Theoretical representation of the EOM and QWP output polarizations of the vertically incident photon.

In the last two lines of the table in Figure 3.7, the polarization behavior of the photon at its output depends on the voltage applied to the modulator, and the polarization behavior of the photon when QWP is added to the output of the EOM is shown with theoretical calculations. However, when a quarter-wave plate is used at the output of the modulator, the direction of polarization has been successfully changed at all applied voltages and a linear polarization has been obtained. Thus, the 4 polarization values to be coded for the switch that will go from Alice to Bob are labeled with the voltage values of the modulator. Also, the effect of the quarter-wave plate added to the output of the modulator on non-linear polarization is clearly seen.

Figure 3.7 shows the values that are expected to be measured after the polarization beam splitter, depending on the voltage applied to the modulator as a result of theoretical calculations. These output results should be obtained from the vertical and horizontal ports of the polarizing beam-splitter. Also, 45 and 135 are the results obtained from the vertical and horizontal ports of the other polarizing beam splitter.

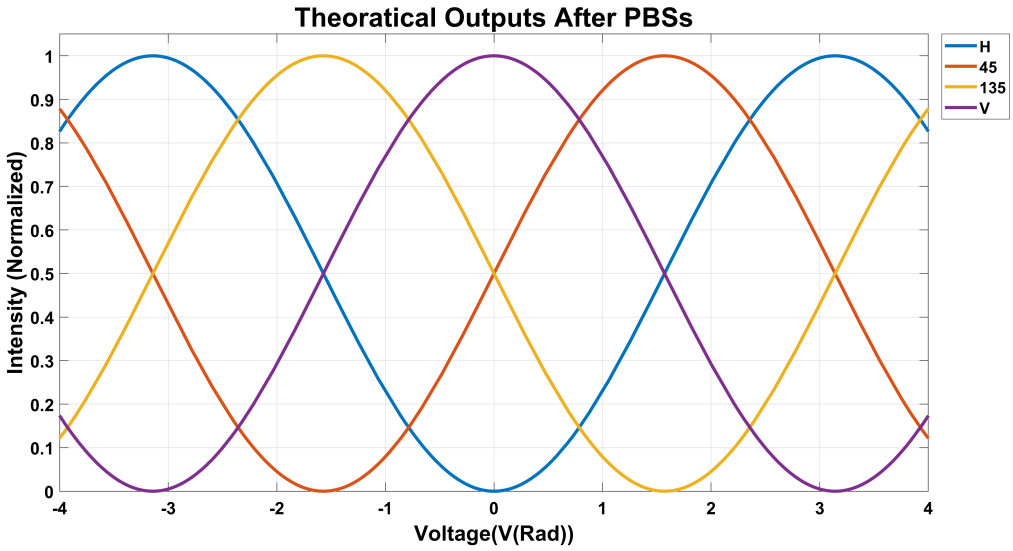


Figure 3.8. The voltage-dependent irradiance measurement results expected to be seen in the detectors. The purple, blue, red, and yellow lines indicate the vertical, horizontal, 45, and 135 polarization directions, respectively. The maximum peaks show the voltage to be applied to the EOM for that polarization.

The optical setup that achieves these results will be further shown in the next sections. This setup is sufficient for the random polarization of the resulting single photons to be tuned and measured by Bob. Figure 3.8 shows the simulation results of the variation of the light intensities going to each single-photon detector according to the voltage values applied to the modulator. Here, in the measurements of $\mid 45 \rangle$ and $\mid 135 \rangle$ polarizations, a half-wave-plate at $\theta = 22.5^{\circ}$ is added to rotate the polarization by 45 degrees. The polarization directions of the photons incoming vertically to the modulator will not change unless voltage is applied to the modulator. When these photons come to the beam splitter in the BOB part, they will either pass directly to one of the polarizing beam splitter (PBS) ports or be reflected to the other port (50/50). If it switches to the first PBS, they will definitely be reflected and measured with the vertical port since they are in vertical polarization. For this reason, at the horizontal port there will not be any measurement while at the vertical port, there will be measurements. If they are reflected from the reflecting port of the 50:50 beam-splitter, their polarization will return to the 135 state due to the

half-wave plate and will be reflected or passed after the PBS with a 50% probability. For this reason, ports of $\mid 45 \rangle$ and $\mid 135 \rangle$ will have measured at the same intensity (0.5). If these measurements are made with one photon at a time, only the measurement with $\mid 45 \rangle$ or $\mid 135 \rangle$ ($\%50$ probability) will be recorded. A similar analysis can be done for light output from the modulator in the $\mid 45 \rangle$ polarization state. In this case, photons coming through the BS to first PBS will be measured in $\mid H \rangle$ or $\mid V \rangle$ with a probability of $\%50$. However, since their polarization state will be $\mid V \rangle$ when they reflect from BS and pass through HWP, they will definitely be reflected after the second PBS and measured at $\mid 45 \rangle$ port. In this case, $\mid 135 \rangle$ will not be able to take measurements.

3.4. Determining The Suitable Voltage Values of The EOM

In this section, the work done to add the key, which is the most important part for Alice, to the direction of the polarization of the photons will be discussed. The required voltage levels of the EOM, which is used to rotate the photons in the appropriate polarization directions, will be determined for these directions.

Suitable output voltage levels of the first configuration of the QKD setup are shown in Figure 3.9. The Figure shows the intensity of the voltage-dependent output. While the voltage which is applied on the EOM is changed, laser polarization changes, so depending on the change of polarization of light, the change of intensity in 4 separated outputs is seen. Four different color shows four different outputs. As can be seen from the figure, the maximum intensity of the outputs is different from each other. When you are looking at the total intensity of the same basis outputs, the total intensity coming to the ports differs between each other. The color of the sum of the same basis intensity is shown with light blue and green and they show a periodic change. Moreover, as can be seen from the figure, when no voltage is applied to the EOM, the polarization of the incident laser should have been vertical. Namely, the maximum intensity of the vertical port (colored purple) should have been at zero voltage. However, there is some shift.

Thus, there are some problems with results. Therefore, analysis and improvements related to the system were required. In the next section, information about these developments and their results will be given.

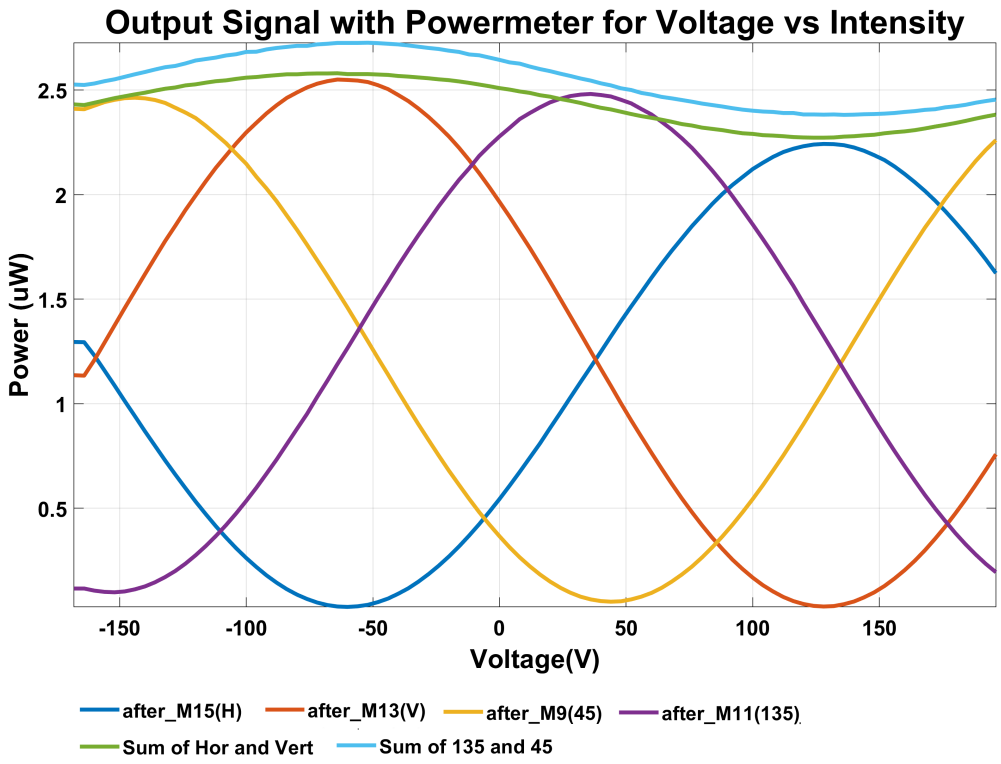


Figure 3.9. First measurement result of output signals. This data was obtained by measuring the intensity at the output ports of the PBS by sweeping the voltage of the EOM between -200 and 200V. With the help of this graph, the appropriate voltage is found for the appropriate polarization directions. However, the maximum powers measured in PBSs are not balanced.

3.4.1. Solution of The Problems

Some improvements have been considered regarding the optical setup, which will be mentioned in the following sections through experimental analysis, and it has been observed as a result of the experimental analysis that the efficiency obtained with these improvements increased.

First of all, two mirrors were used to couple the laser to the fibers after PBSs and the part after the EOM in the previous setup was removed. Based on the analysis made and the information provided by the manufacturer of the mirrors, it was realized that the reflectivity or transmittance of the mirrors against the rays in different polarizations was

changed. As will be mentioned with graphics in the experimental analysis part, data loss due to mirrors was observed. In order to eliminate this undesirable situation, the mirrors after PBSs were removed. Instead, the lenses at the output ports of the PBS were fixed to adapters that can move in one XY-axis, and the fibers were fixed to adapters capable of moving in the Z-axis. Thus, the rays coming from the output ports of the PBS are sent to the fibers with much less loss.

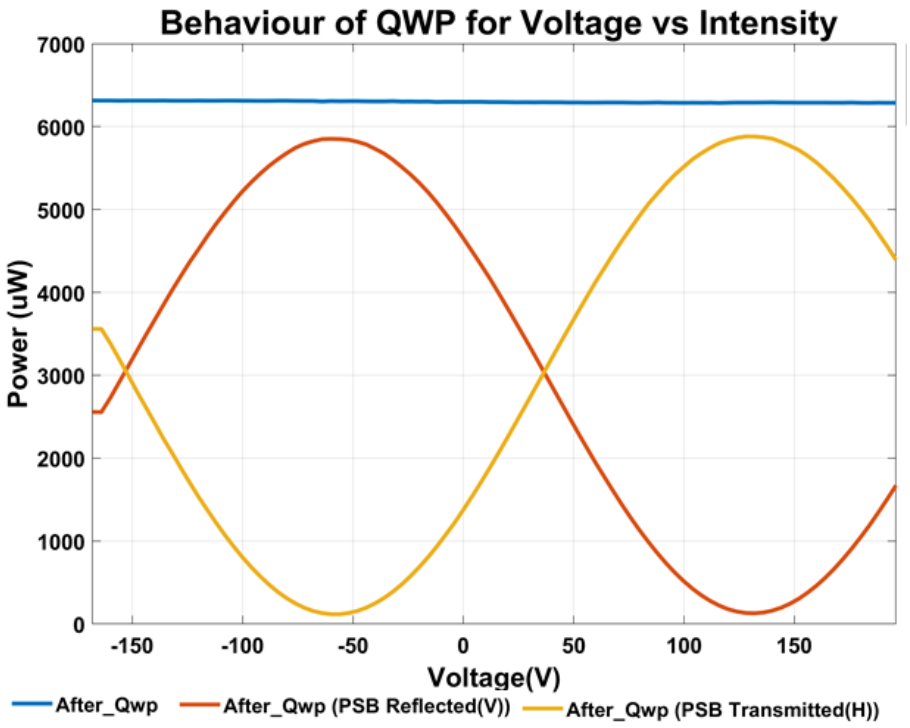


Figure 3.10. Polarization analysis of after QWP. By varying the voltage applied to the EOM, a PBS was placed behind the component to be measured and the intensity at the PBS outputs was measured. Thus, it is desired to detect polarization disorders originating from the component. As you seen, there are no polarization disorders on Alice's part. However, there is some shifting the polarization direction, because its polarization in the vertical direction should not change at 0V.

Another improvement was the determination of the most suitable positions of EOM and QWP with the help of theoretical calculations and experimental observations in

order to obtain the appropriate and desired polarizations with each other. With the help of a quarter-wave plate, the circular polarizations formed in the system were converted into linear polarizations. Besides, by placing the EOM perpendicular to the laser propagation direction, it has been ensured that the polarization of the incident beam does not change its direction at zero incidences.

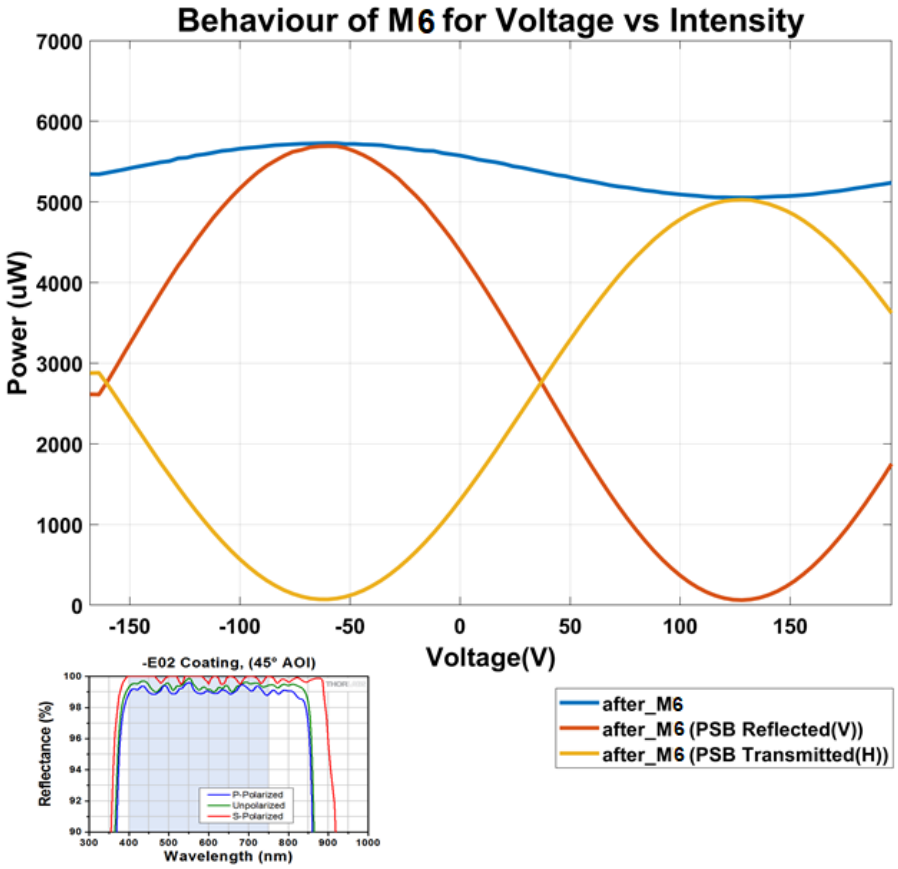
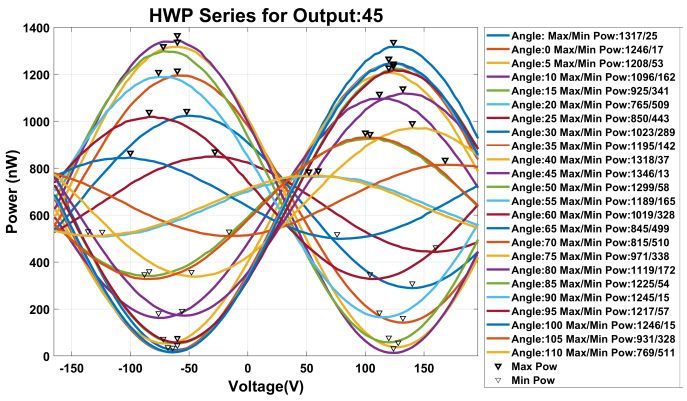
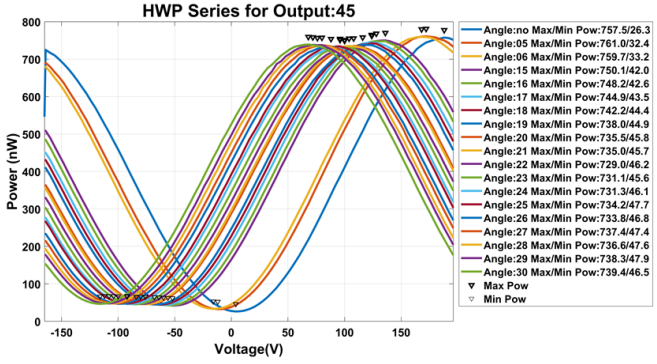


Figure 3.11. Polarization analysis of after M6. As can be seen, since the reflectivity coefficient of the mirrors changes depending on the direction of the polarization, the peaks vary between polarizations. Therefore, it is beneficial to minimize the use of mirrors in QKD systems using a single laser. If different lasers were used for each polarization direction, the intensity between them could be equalized.



(a)



(b)

Figure 3.12. Correct HWP angle and EOM alignment. Although this figure seems complicated, it is actually the data obtained with the help of PBS by changing the angle of the HWP on a diagonal basis. A PBS was added after the HWP and the voltage of the EOM was varied between -200 and +200V at each HWP angle. The goal here is to find the right angle of the HWP. However, if the laser beam does not pass straight through the EOM, circular polarization is observed as in Figure (a). To avoid this circular polarization, either the laser beam is corrected or the angle of the QWP is adjusted to the appropriate position. The inaccuracy in the EOM alignment can be understood from the fact that the light passing over it changes the polarization when no voltage is applied to the EOM. Figure (b) is obtained after correcting the EOM.

Now, experimental analyses of the previously mentioned developments will be shown. Firstly, the behavior of mirrors against the change of polarization will be described. In Figure 3.10, it is shown the polarization analysis of the incident light after QWP. This data was taken in three parts. The polarization of the incoming light by putting the power meter right after the QWP in the first part is shown with orange and yellow lines for vertical and horizontal polarizations, respectively, and data before PBS is described with a blue line. The voltage applied to the EOM is changed depending on the time. In this part, a change in the intensity of the incident light is not expected. Likewise in the graph, there is no change in intensity.

The second and third part of the measurement is the polarization analysis of the light after QWP. The analysis step is similar to the first part. However, this measurement was made with PBS. The PBS was put after the QWP and measurements were made at the reflected and transmitted port of the PBS. These measurement data in Figure 3.10 is shown with red and yellow lines. As can be seen from the data, the polarization of the light changes by an applied voltage on EOM without loss, and the polarization of the light changes symmetrically.

The purpose of making these measurements is to understand the changes in the polarization and intensity of the light entering and passing through the optical components. Thus, the aim is to reduce the losses in the system to the lowest levels.

In figure 3.11, it is shown that the behavior of the light changes after passing through the mirrors. The problem here is a reduction in the total intensity of the light and corruption in the polarization symmetry. When you look at figure 3.9, this situation affects the outputs and the change cannot be ignored. Thus, all mirrors after the QWP must be removed.

Moreover, there is one more problem in the graph. The polarization of the laser source has vertical polarization. At zero voltage, the polarization of the light should not have been changed. When you look at the graph, the vertical polarization port should have had maximum intensity at zero voltage. This means that incoming light does not pass exactly perpendicular to the EOM. Thus, there is a shift in the incoming light polarization. The problem is solved and appears to be caused by incoming polarization. The reason for this situation is that there is circular polarization on a non-orthogonal basis. It was mentioned in the section of the theory of EOM. As mentioned before with simulations and

in the manufacturer's manual, if the beam is not perpendicular to the EOM or if the QWP is not placed at an appropriate angle, or even if the beam is perpendicular to the EOM, circular polarization appears in the system except vertical and horizontal polarization. The effect of this circular polarization is that it causes the formation of a moving polarization in the system, and therefore a decrease and increase in the minimum or maximum appear.

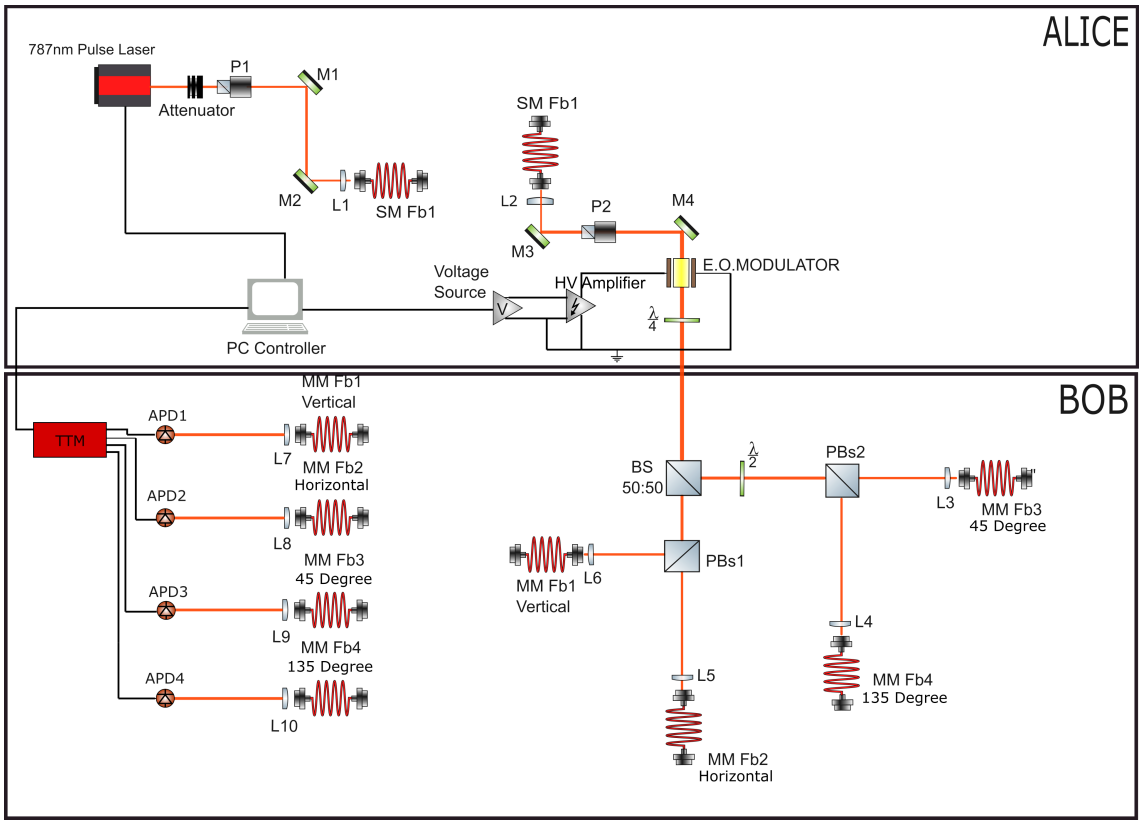


Figure 3.13. Last configuration of BB84 protocol optical cetup. In order to align the EOM properly, all mirrors in the system, except the 2 mirrors in the Alice part, have been removed.

Figure 3.12 shows a more systematic analysis of the HWP behavior in the system. In Figure 3.12a, the measurement was done before EOM and QWP alignment and in Figure 3.12b, the same measurement was done after EOM and QWP alignment. While the experiment was being done, the HWP angle has been changed for each polarization series step by step. The purpose of this experiment is to find the correct angle of the HWP and to determine the basis of the circular polarization in the system. As can be seen from the

graphs, there is no problem at horizontal (blue line at angle:0)) and vertical (purple line at angle:25) polarizations but other non-orthogonal polarizations have circular polarization. When EOM alignment was done and the angle of QWP was set to zero degrees, each time the HWP angle is changed, a linear shift is seen on the Figure 3.12b. Therefore, the correct angle of the HWP is between 22 and 23.

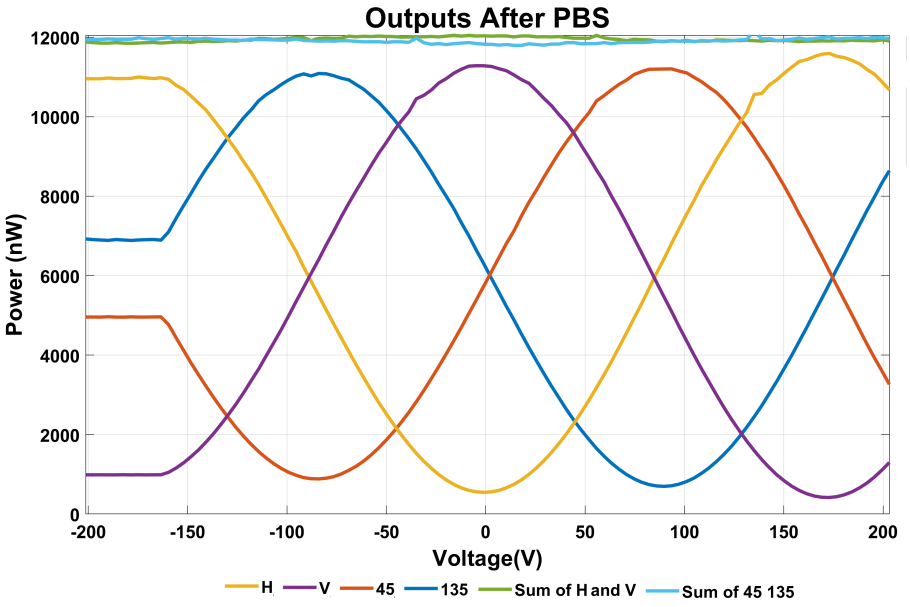
After all alignment and improvement were done, schematic representation of the optical setup is shown Figure 3.13.

Moreover, output signals of the system are shown in Figure 3.14. In Figure 3.14a, measurement is taken in front of the optical fibers, and measurement in the other Figure is taken from the exit of the fibers with APDs. Therefore, alignment and improvement of the optical setup made a noticeable difference. As can be seen from these graphs, four different polarizations at four different voltages are now available. These voltages are 0V for vertical, 180V for horizontal, 90V for 45, and -90V for 135. If we apply one hundred 180 volts to the EOM, it can be said that we are measuring photons with horizontal axis polarization at that port in the ratio of about eleven thousand to thousand. Furthermore, b part of the Figure was taken with APDs.

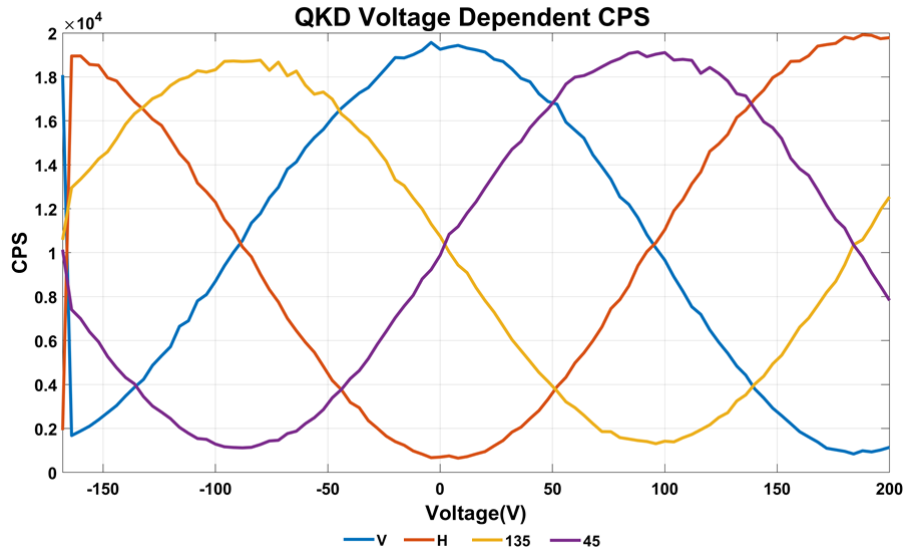
When these output signals are compared to theoretical data, matching corresponds to theoretical data. Figure 3.15 shows the compliance of the output signal obtained with APD and power meter and its fit data obtained by theoretical calculations.

After these improvements, the optical setup is ready to produce the key and synchronization part. For the measurement, there should be four different APDs. Also, we have four APDs but two of the APDs are fast (IDQ100) while others are slow (IDQ120) and quantum efficiencies of different types of APDs differ greatly from each other. Thus, as a result of this difference, there will be problems in the synchronization part and some efficiency problems. In order to avoid this problem, either two more APDs with the same features will be required or a system running with 2 APDs will need to be switched.

According to our researches, it has been decided that the most appropriate solution at this stage is to switch to the B92 protocol. It will be possible to switch quickly without making too many changes and new additions to the optical system, and if it is requested to switch to the BB84 protocol, it will be easy to reverse.

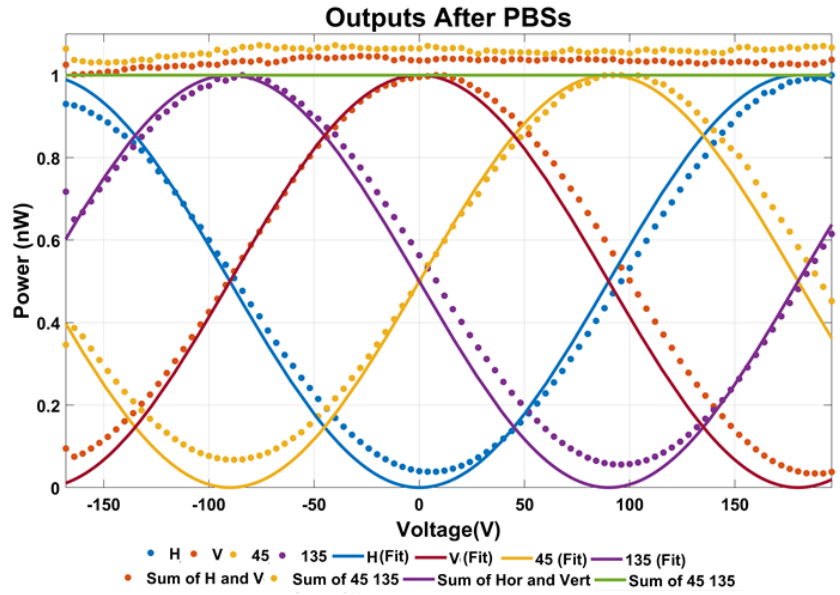


(a)

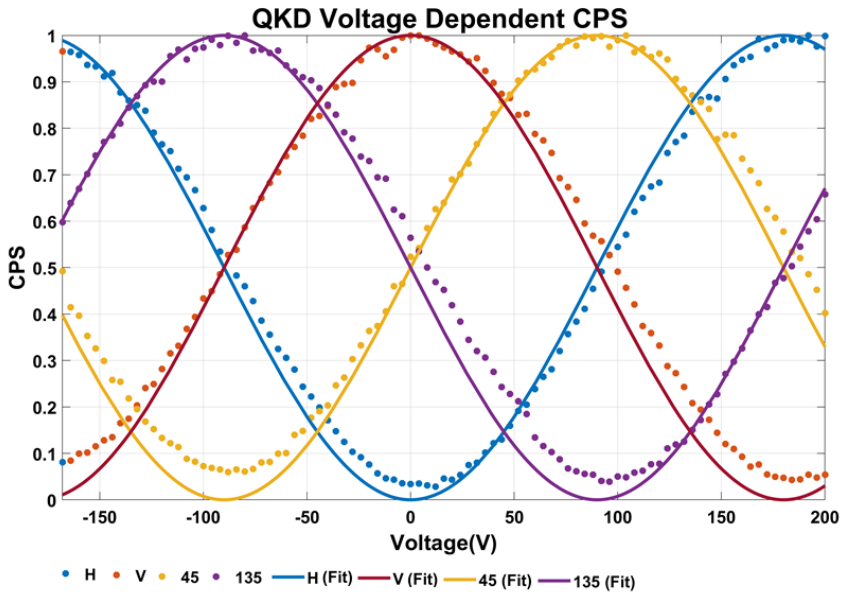


(b)

Figure 3.14. Figure (a) shows powermeter results. Figure (b) shows the APDs results. The results are shown after all adjustments and component eliminations. As can be seen, all polarization problems are resolved and equal power is received from each polarization direction and equal number of counts are received from the APDs. Thus, it will now be possible to take measurements in a highly efficient way with the optical system.



(a)



(b)

Figure 3.15. Figure (a) shows outputs with powermeter. Figure (b) shows outputs with APD. In this graph, the data obtained from the theoretical results and the measurement data are compared. The measurement results agree with the theoretical values obtained. Due to the extinction ratio of PBSs, their minimum cannot be measured as 0.

3.5. Optical Setup and Control Program of B92 Protocol

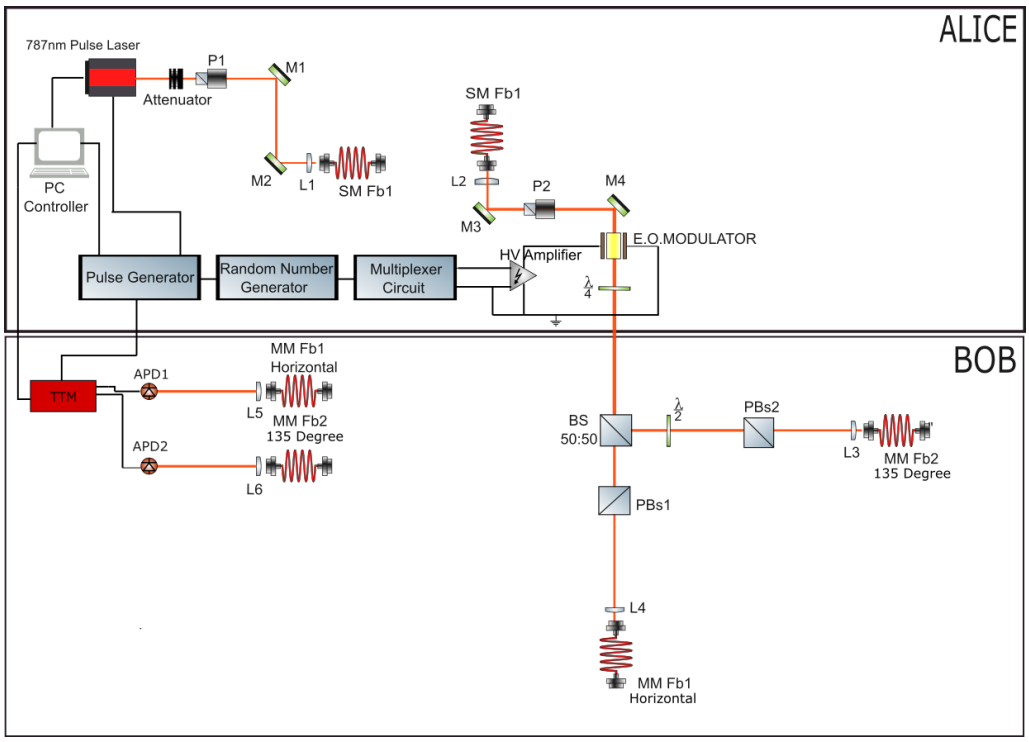


Figure 3.16. Optical setup of B92 protocol. Attenuated laser pulses with vertical polarization arrive at the EOM, where the key is encoded to the polarization direction of the photon. When no voltage is applied to the EOM, photons are sent in vertical polarization. When applied 90V, it is sent at a 45-degree angle and sent to Bob. The EOM is only turned on and off according to the value of the key. Photons coming to Bob are chosen in a random basis direction by BS. If a photon with a vertical direction chooses an orthogonal basis, it is discarded from the system. If it chooses the diagonal basis, it has a 50% chance to measure at 135 degrees. Besides, the photon with a 45-degree polarization direction will be measured horizontally with a 50% chance if it chooses the orthogonal basis. If it chooses a diagonal basis, it is kicked out of the system.

The B92 protocol is a protocol invented by Charles Bennett, one of the creators of the BB84 protocol. In this protocol, a qubit comes from two non-orthogonal bases. For

example, vertical polarization is qubit zero, 45-degree polarization is qubit one. However, the receiver does not read the polarization of the transmitted photons vertically or 45 as used in the same BB84 protocol. Instead, it reads the projections of polarization corresponding to another basis.

If the similarities and differences between BB84 and B92 protocols are compared, it is necessary to start with the sending of data or key generation. Suppose we send a key for the BB84 protocol without any loss. Data loss for this protocol is only 50% of data due to the 50:50 beam splitter. However, considering the B92 protocol, this loss is a valid data of 25% when we add the 50% loss in polarization beam splitters. However, if considered within the scope of the project, it is sufficient to prove that the key can be generated. Also, with the loss of 75%, it is necessary to increase the data transmission to generate keys, so it takes a long time to produce and send. This also reduces security. However, the B92 protocol provides much more advantageous listening security against interception compared to the BB84 protocol.

The optical setup considered for the B92 protocol is shown in Figure 3.16. The only difference from the previous optical setup for BB84 is that photons are only measured from the transmission ports of PBS's. Two different polarizations to be used for communication mentioned in the previous section will be provided by EOM. They will be vertical and 45-degree polarization will be used. The reason for choosing diagonal polarization is that voltage will not be supplied to the EOM for vertical polarization, but the voltage will be supplied to the EOM only for 45 degrees. The advantage of this choice is that it will only need to give a voltage to trigger the EOM. This is considered to be the most favorable condition for the efficiency and speed of the system.

3.5.1. Alice

The Alice part of the optical setup is almost the same as the previous setup and optical installation is shown in Figure 3.17. The only difference is that the voltage from 0V to 90V is now applied. In other words, the high-voltage amplifier will run or stop, i.e. work as a switch. Thus, we will only use vertical and 45-degree polarizations for communication. Alice part of Figure 3.16 shows that for the electronic part, a square wave pulse generator and an electronic card with a microprocessor are used to generate a random

number. The pulse generator produces square waves of the desired frequency, amplitude, and width, and these generated pulses are given to the time counter and drive the laser. In addition, the inverted square pulse, which is produced to drive the laser, is taken from the second channel and given to the digital signal reader pin of the microprocessor.

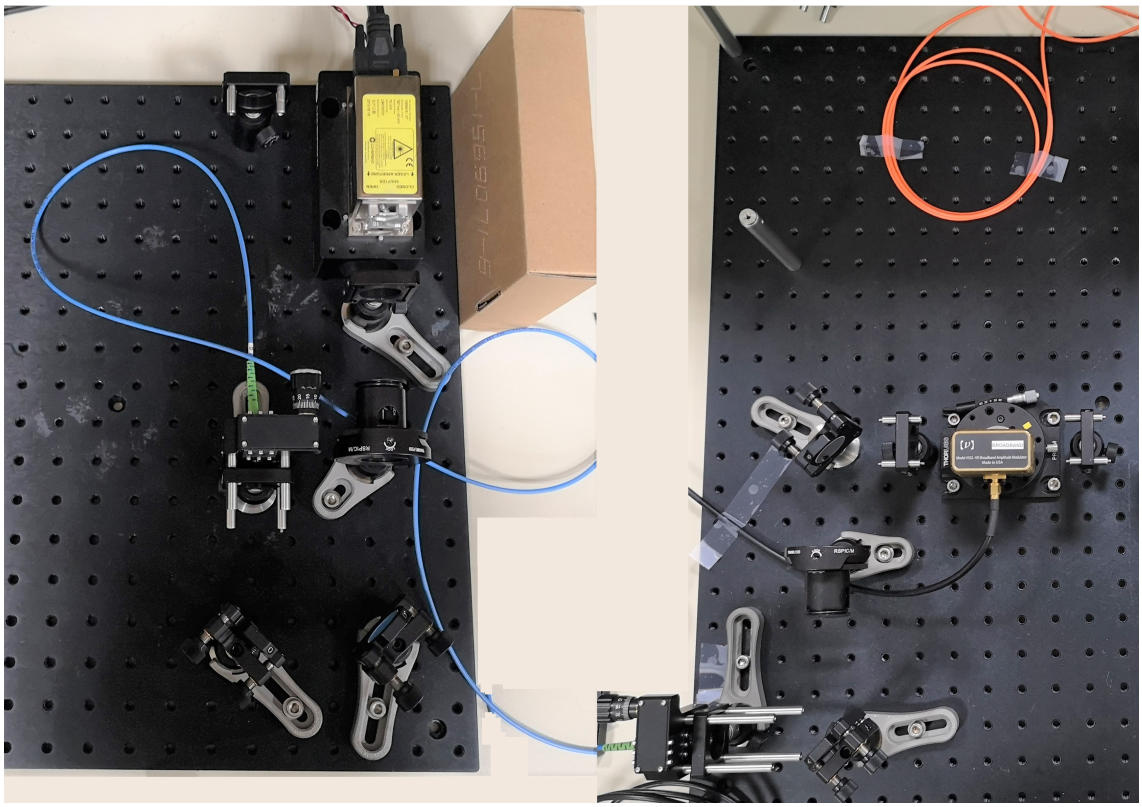


Figure 3.17. Optical Setup of Alice. The attenuated laser system is shown on the left side. On the right side, the EOM for the polarization control is shown.

The optical setup for the B92 protocol is shown in Figure 3.16. The only difference from the previous BB84 optical setup is that the measurement is taken only from the transmission ports of PBSs. Two different polarizations to be used for the communication mentioned in the previous section will be provided by the EOM control. The two polarizations that are used for communication are vertical and 45-degree polarizations. The reason for choosing these polarizations is that the voltage will not be supplied to the EOM for vertical polarization, but the voltage will be supplied to the EOM for only 45 degrees. The advantage of this choice is that it will only need to give a voltage to trigger

the EOM. This is considered to be the most suitable condition for the efficiency and speed of the system.

3.5.2. Bob

The Bob part of the optical setup is nearly the same as the BB84 protocol and optical installation is shown in Figure 3.18. The only difference from the previous part is that the measurements are done only at the transmission port of the PBS.

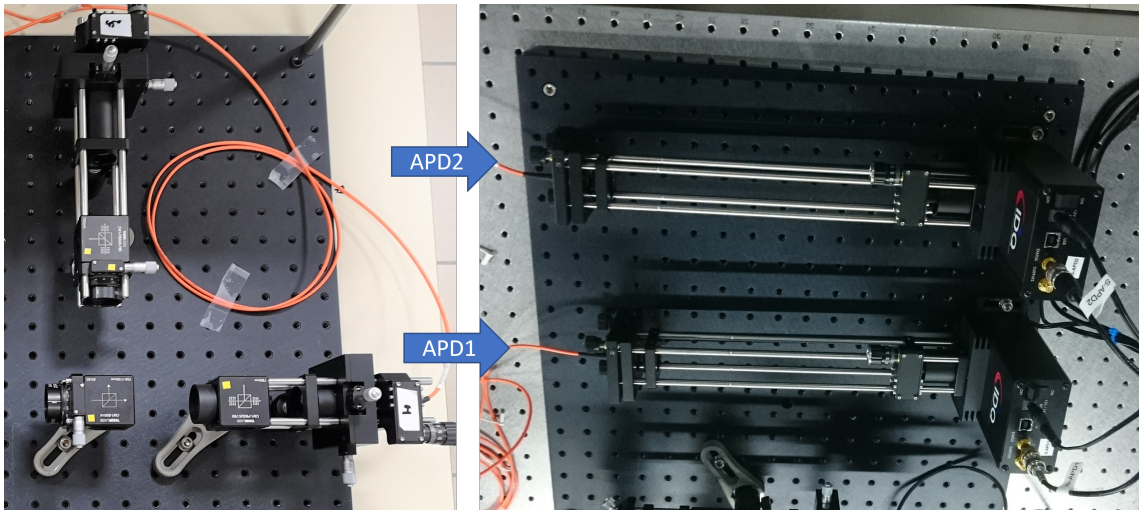


Figure 3.18. Optical Setup of Bob. On the left, a 50:50 BS are used for random photon selection and PBSs were used for polarization selection of photons. On the right, APDs are used to detect the incident photons in the channels.

The photon with one of the two different polarizations that will come to the system can go two different paths by the 50:50 BS. For example, considering that the vertically polarized photon chooses the port where PBS1 is, the photon coming to this path is taken off from the reflecting port of the PBS1. APD does no measurements. Suppose the vertically polarized photon chooses the path with PBS2. Here, the polarization direction of the photon passing through the HWP at -22.5 degrees will change to -45-degrees. There are two cases with a 50% probability for the photon that then passes through PBS2. In the

first case, the photon passes through the port through which only horizontal polarization can pass and is measured. In the second case, it can exit from the port where only the vertical polarization is reflected. In this case, the photon is expelled from the system. APD cannot measure anything.

Now supposes that the photon with the other polarization direction comes to Bob. The photon will either pass through or be reflected again by 50% of the beam splitting possibilities. The photon with a 45-degree polarization angle will come to PBS1 for the state it passes. In this case, the photon coming to PBS1 will encounter two situations with a 50% probability again. The photon will either reflect and exit the vertical port and eject or pass through the system and exit the vertical port and be measured by the APD. Considering the other case, that is, the beam splitter passes from the reflector side, the -22.5 degree half-wave photon passing through the plate will change to have vertical polarization. Thus, the photon that chooses this path will be removed from the system.

When we briefly examine the system, a vertically polarized photon can only be measured from the 135-degree port. A 45-degree photon can only be measured from the horizontal port. However, in this protocol, as can be understood from above, only 25% of the key can be sent exactly.

3.5.3. The Suitable EOM Voltage

Output port of horizontal and 135-degrees are measured with a power meter and shown in Figure 3.19. Using polarization of the incoming light as it is mentioned is vertical and 45-degree. However, these photons are measured at respectively 135-degrees and horizontal ports. When there is no applied voltage to EOM, photons that have vertical polarization come to Bob part and a quarter of incoming photons are measured at 135-degree port and there is no measurement at the horizontal port as can be seen from the blue line in Figure 3.19. When 95V is applied to EOM, photons that have 45-degree polarization come to Bob part and barely a half of the incoming photons are measured at the horizontal port like the red line in Figure 3.19 and at 135 port, photons are not observed like the blue line in Figure 3.19. Thus, thanks to this measurement, photons can be directed to the desired ports depending on their polarization.

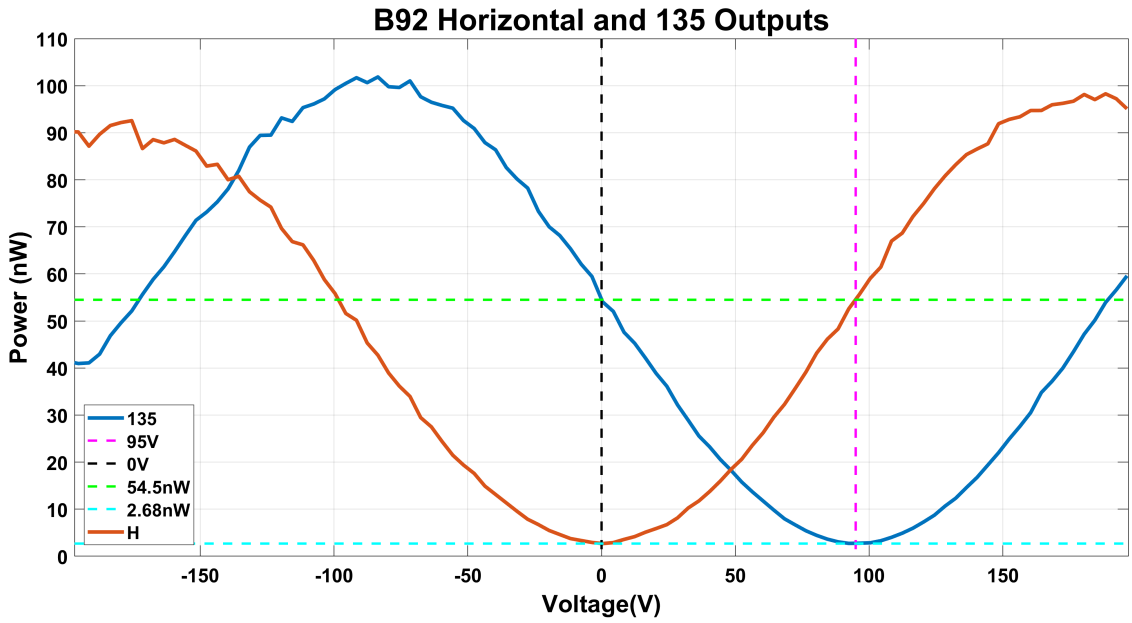


Figure 3.19. Outputs of B92 protocol. As can be seen, no measurement is taken on an orthogonal basis when no voltage is applied to the EOM. However, half of the intensity is measured on a diagonal basis. In addition, when 95V is applied to the EOM, half of the intensity is measured on an orthogonal basis, while intensity is very low (this is our error rate) on a diagonal basis. Thus, it is necessary to apply 0 and 90V to the EOM to encode the key.

3.6. Synchronization and Electronic Control

Synchronisation part of the system is also almost the most important part of the QKD system because if the production and measurement times of the photon are known, both Alice and Bob can correctly identify the key, and also the Bob part of the system can eliminate most of the inaccurate measurements caused by the environment or APDs. For instance, when there is no laser pulse in the system, APDs can measure background photons or the dark count. Due to the same trigger signal reaching both the TTM and pulse laser, wrong measurements are eliminated easily.

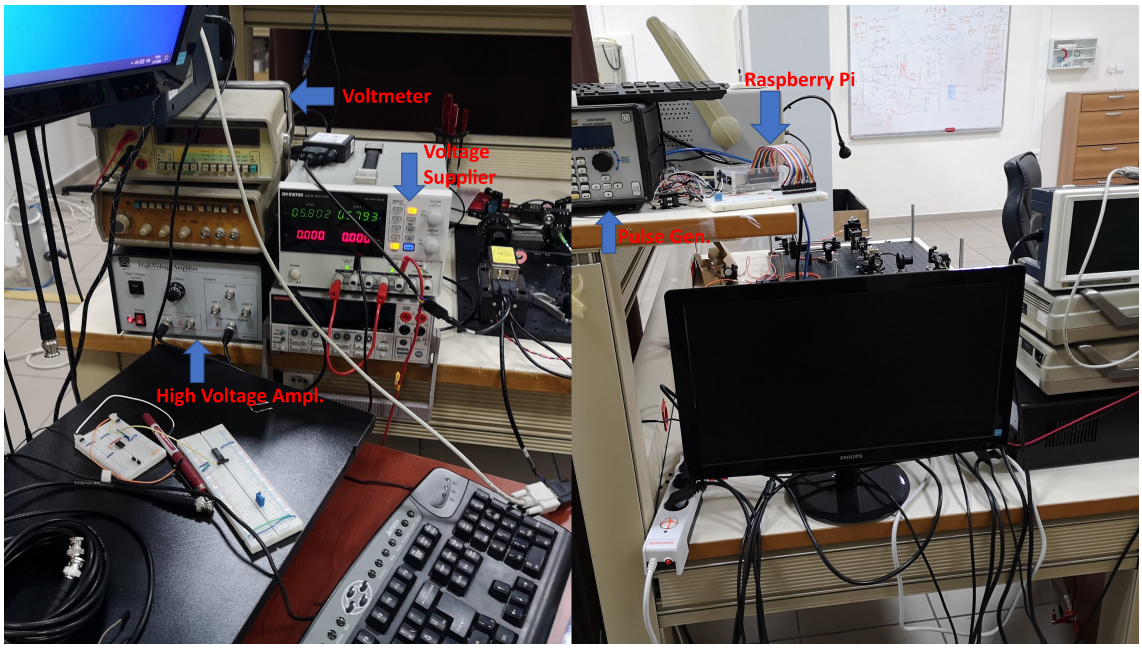


Figure 3.20. Installation of Control Part

When it comes to the synchronization part of the optical setup, a square wave signal is generated for pulsed laser, EOM, and TTM. Each square wave signal causes the pulsed laser to generate one pulse. At the same time, if the square wave is zero, as mentioned in the optical setup in Figure 3.21, the appropriate voltage is supplied to the EOM, thanks to the microprocessor used to generate two random digits which are one or zero. In this way, the EOM is hibernated to convert it to the appropriate polarization before the pulse is generated. In addition, the trigger signal is given to TTM, and it is aimed to use this signal as the synchronization signal. Measuring the laser pulses at the rising and falling edges of the square wave signal coming to the counter is guaranteed. Thus, we can ignore the measurements in the region outside this range. This helps us safely eliminate the majority of measurements due to surrounding noise because there are no photos from the laser in the system at that moment.

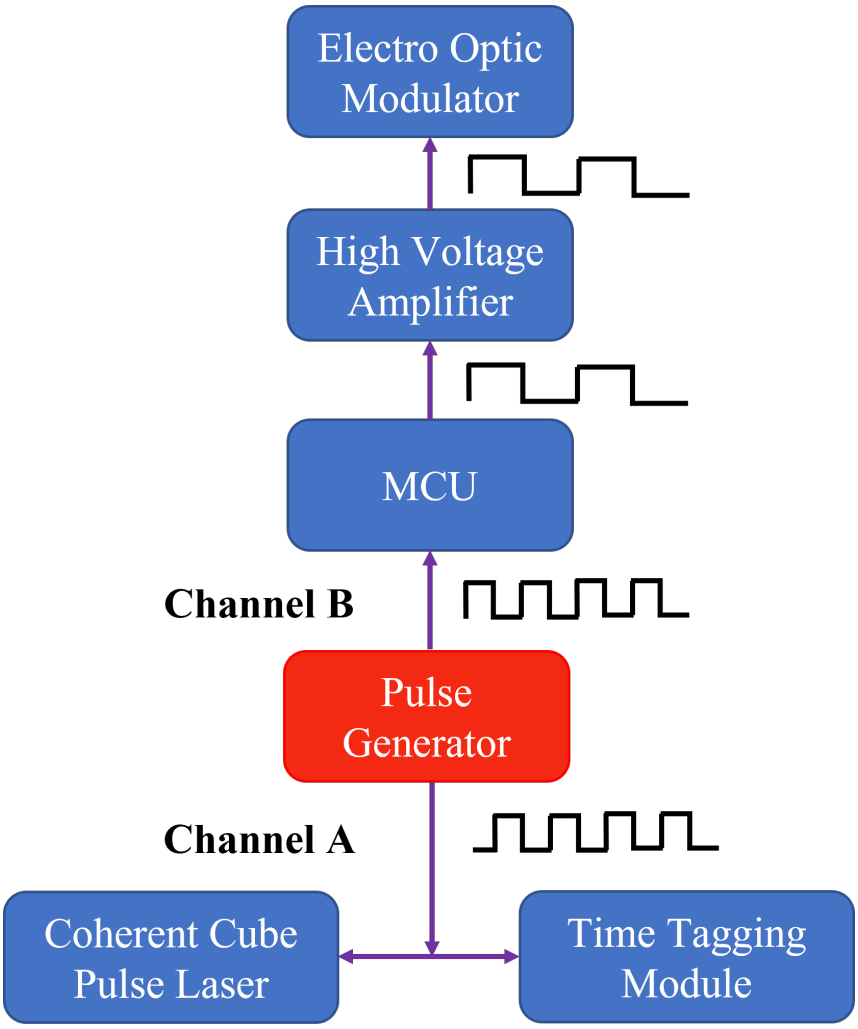


Figure 3.21. Schematic representation of the electronic control system prepared for the B92 protocol. 2 channels of the signal generator are used and 25% phase difference is added between them. The delayed channel is connected to the laser and the TTM. Thus, the signal is recorded both while driving the laser and by connecting to a channel of the TTM to ensure synchronization. The other channel is connected to the I/O channel of the MCU. On each incoming high signal, the MCU applies the elements in an array of pre-generated pseudo-random numbers, respectively, to its digital output as a logic level. Depending on the voltage at the output of the MCU, the high voltage amplifier changes the voltage to 0 or 90V.

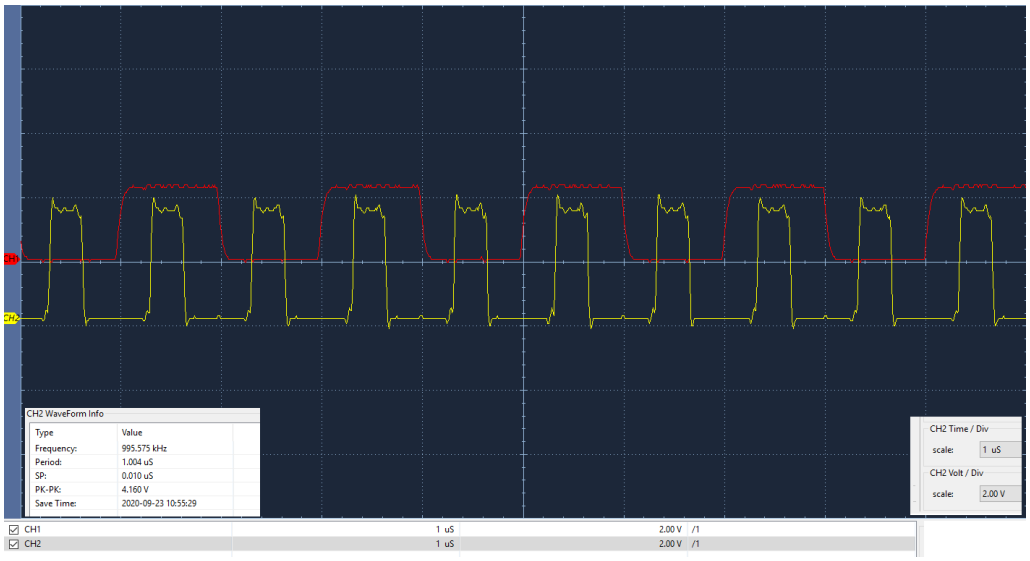


Figure 3.22. Image is taken from the oscilloscope. The signal with the yellow line is used to drive the laser and is connected to the TTM for synchronization and is recorded. The signal with the red line is the output signal of the MCU and is used to drive the EOM. It is adjusted to change the polarization state on the pulse so that it can be seen easily on the oscilloscope. As can be seen from the picture, before the laser signal is generated, the state of the EOM has changed and is ready for proper polarization. After some time has passed after the laser pulse has finished, the system prepares to change state to encode the next key.

The image of the generated signals from the oscilloscope is as in Figure 3.22. The signal with the yellow line in the figure is from the signal generator. The frequency of the signal is 1 MHz and is 25% duty cycle. This signal is wired to the laser and a channel of the TTM. While the signal drives the laser, the time of each simultaneously generated pulse is recorded in the TTM. This signal is used as the synchronization signal between Alice and Bob. A signal with a phase difference of 25% of the signal driving the laser is connected to the input channel of the MCU. The red line is the signal obtained from the output channel of the Raspberry Pi and drives the EOM. The MCU processes each high signal coming to the input signal. The MCU's algorithm is built in such a way that the EOM's state changes with each pulse produced by the laser to get this image. As can be

seen from the picture, the state of the EOM has been changed before the laser signal is generated and the EOM is ready for proper polarization. After some time has passed after the laser pulse has ended, the system changes state to encode the next key.

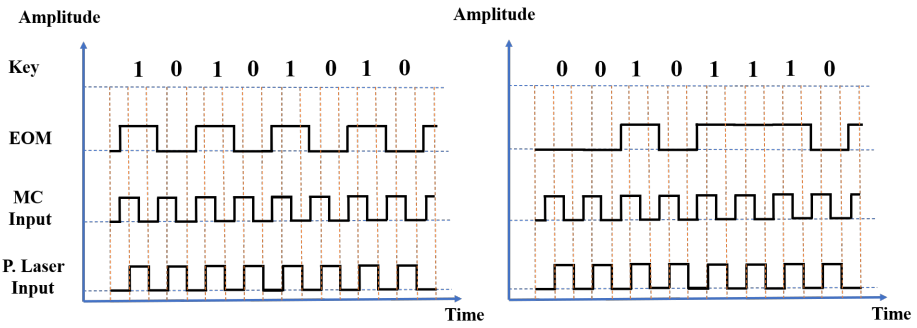


Figure 3.23. B92 protocol signals representation. First, the graph on the left is a representation of the signal generated for a periodic switch. The graph on the right is the signal representation of a randomly generated key. The signal driving the laser, the signal driving the MCU, and the signal driving the EOM are plotted over time.

Pulse generation of generator and micro-controller is shown in Figure 3.23. The left Figure is shown for the periodically changing key, while the right Figure is a digital operation for a randomly generated key. Pulse laser input (Channel A) periodically changes every step. When it becomes high or one, the laser produce pulse. The pulse width of the square wave determines how long the photons of the laser are produced or have been in the system. In the B channel of the signal generator, the reverse signal of the other channel is shifted by a quarter period and it is wired to MCU input. The MCU monitors the changes in this incoming signal from its input port and using the random numbers, which it generates and saves in an array before the experiment starts, gives the switch formed between each rising edge at its digitally determined output port, respectively. Thus, each key has entered the polarization of photons. When you look at Figure 3.23, it is clearly seen that each photon is produced after the position of EOM changes. It is also seen that there is no photon produced in the system during the next change. Thus, it is certain that the switch is entered in the polarization of the photons in each laser signal

generated. However, there is a problem at channels of TTM due to the time difference of measured photons by APDs and measured signal, which is produced by a signal generator, by TTM. Since this delay is periodic, this part of the data is easily extracted from the data recorded in TTM.

3.6.1. Understanding and Analysing The Obtained Data

In this section, it will be tested that the polarization of the photons produced from the attenuated laser can be managed in a controlled manner at each pulse. Also included will be the consequences of attenuating the laser to levels sufficient to generate a key.

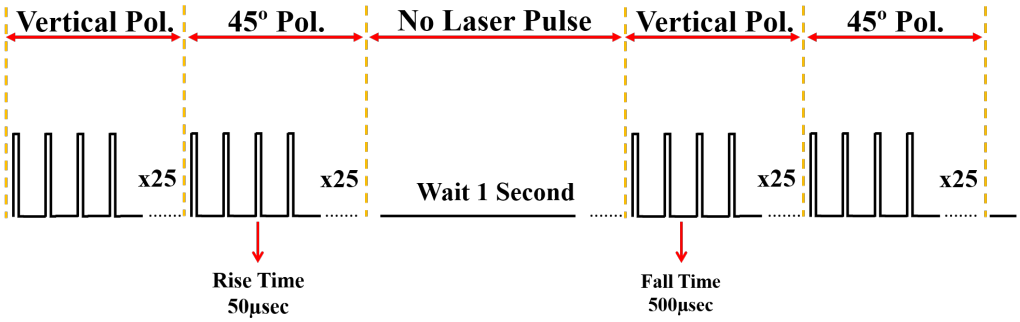


Figure 3.24. The first raw key configuration. In this part, we wanted to make a visualizable key. Alice will send twenty five vertical and then twenty five 45 degree polarizations and then waited for 1 second. After that, alice will repeat this situation periodically.

First raw key configuration is shown in Figure 3.24. The raw key is formed in such a way that one hundred vertical and then one hundred 45 degree polarizations are sent respectively, and the software of the micro-controller is added to control the electro-optic modulator in this way. After that, no data will be sent for one second. Each pulse is formed that their rise times are fifty microseconds and their fall times are five hundred microseconds. In other words, a pulse of fifty microseconds will be generated in five hundred fifty microseconds.

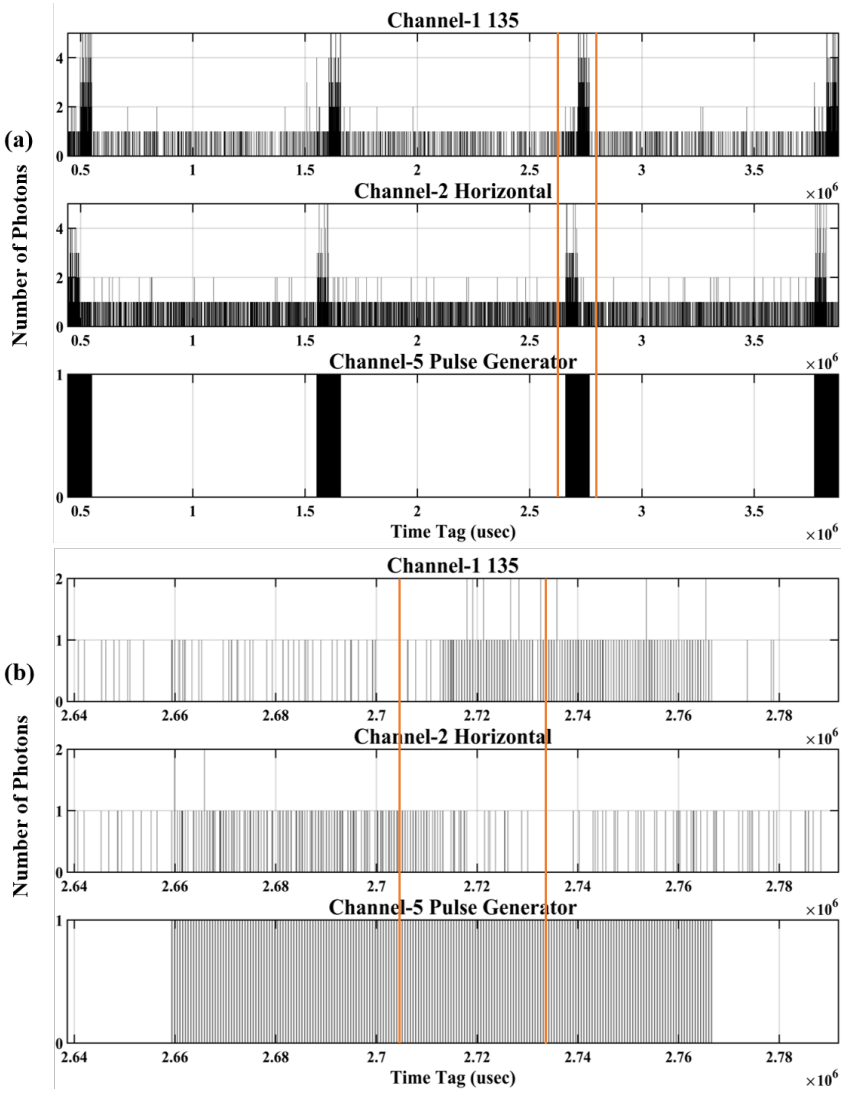


Figure 3.25. Measurements of the first raw key configuration part 1. The graphs (a) show the measurement density over time histogram. In Figure, from top to bottom, measurements of 135 channels, measurements of the horizontal channel, and synchronization pulses are seen. As can be seen, the resulting intensities mean that the number of measurements increased. First, the measurement increased in channel 135, then the measurement increased in the horizontal channel. The Redline is the area to be zoomed in and (b) is zoomed part of (a). As can be seen in figure (b), the measurement density changes due to the change in polarization.

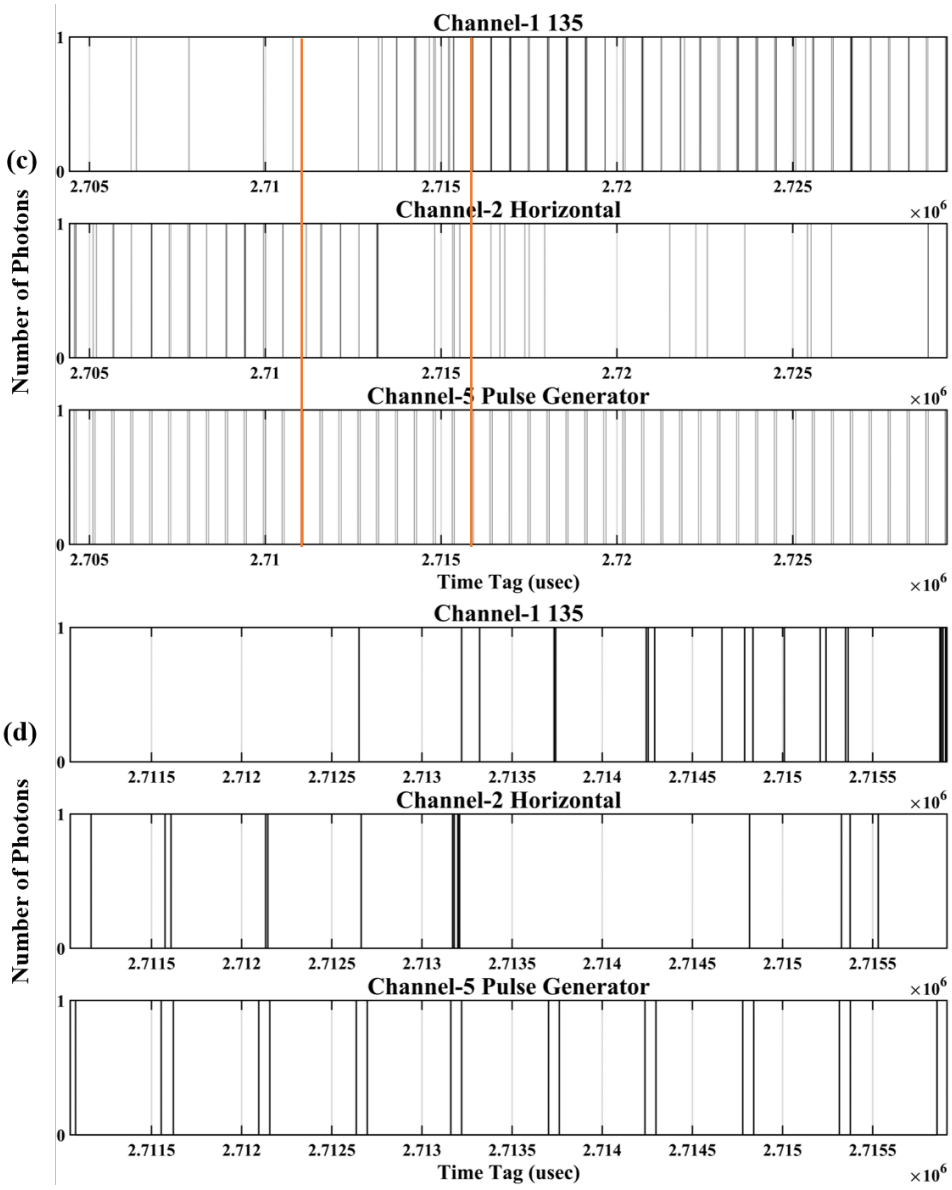


Figure 3.26. Measurement of the first raw key configuration part 2. When these densities are zoomed by 2 times, it is seen that the measurement is made in each sent pulse. It can be seen that we have accurately measured the photons we send from here. In order to get a clearer vision, the laser power has been increased and the number of measurements has increased.

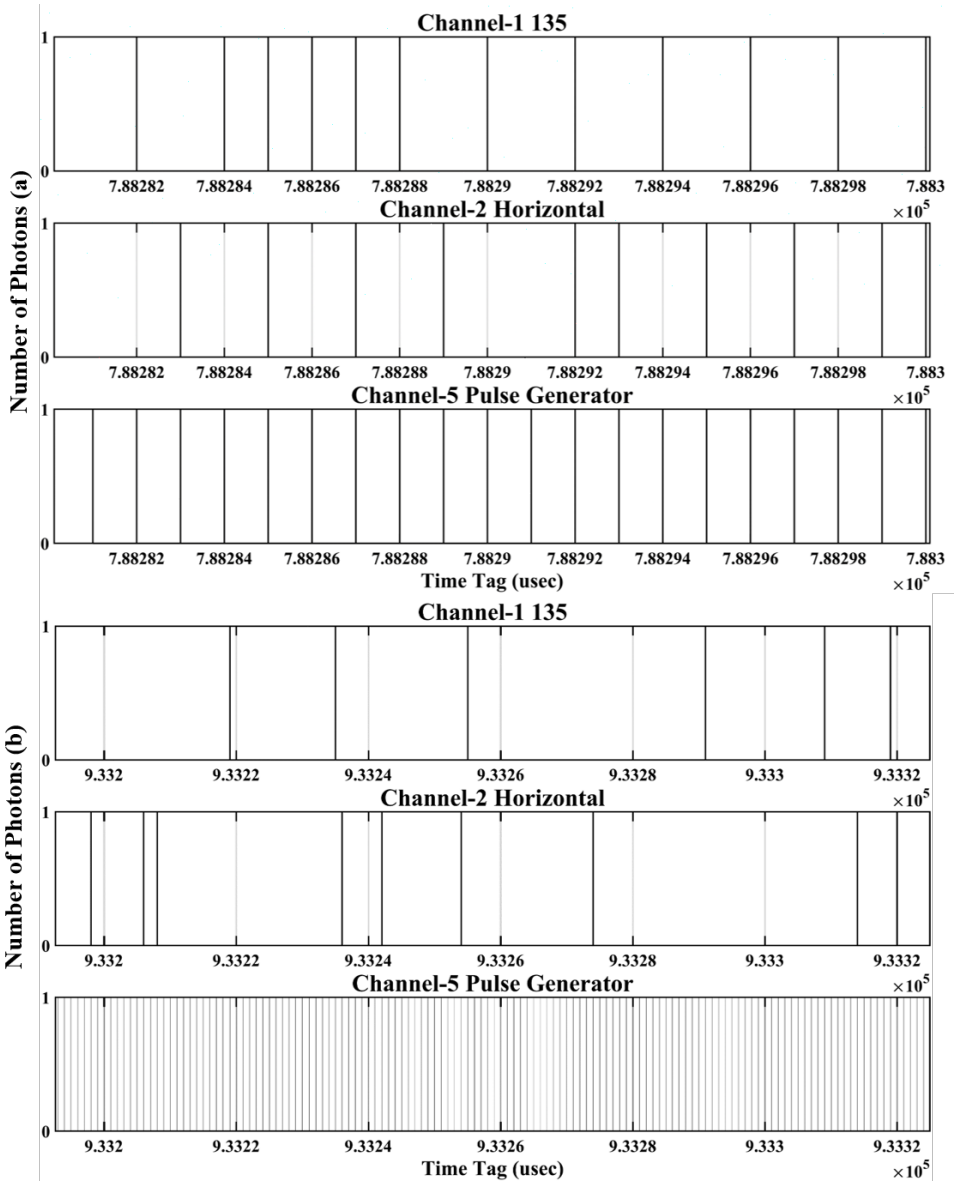


Figure 3.27. Comparing high laser count and low laser count. In this graph, it is seen why the laser intensity should be attenuated. In the graph (a), there are simultaneous photon measurements in both channels in each pulse. But at (b) low power, the number of measurements is greatly reduced.

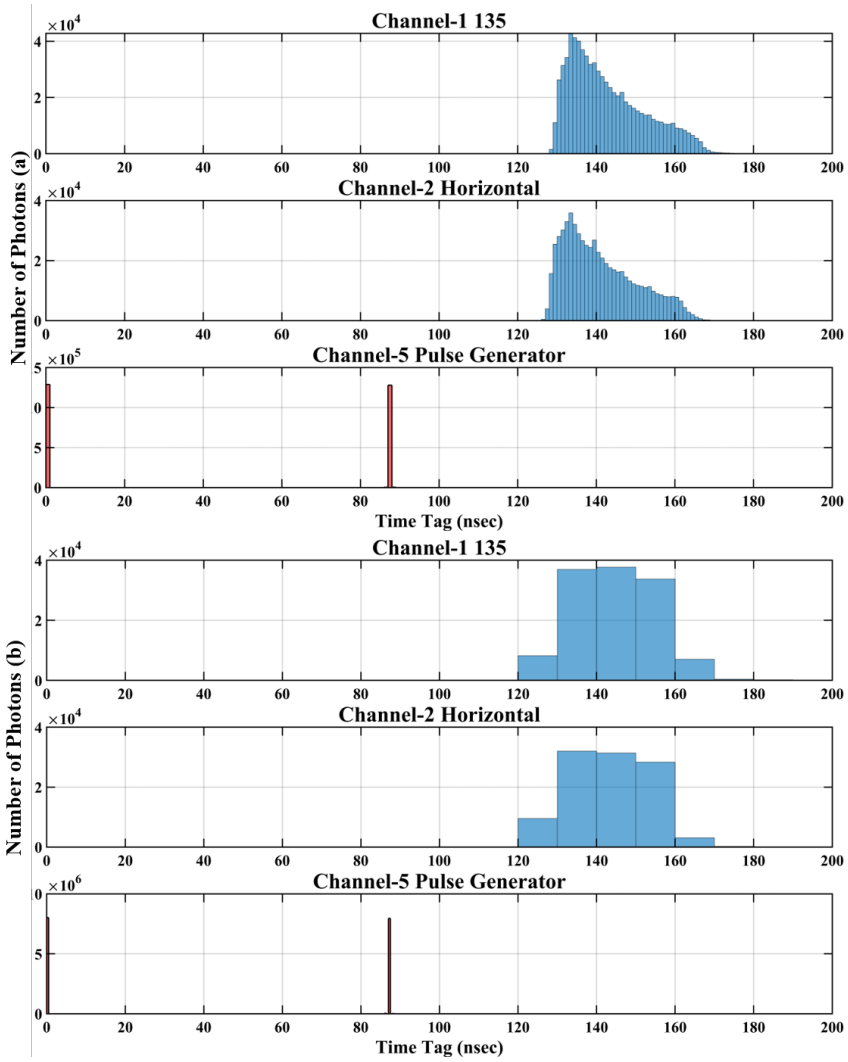


Figure 3.28. System delay at high frequency. This graph was obtained by subtracting each synchronization signal from each others. Thus, the region where the measurement is dense has emerged. If we zoom in on the except dense part, it will be seen that the measurements from the dark count disperse over the entire range. With the help of this region, we can reference the measurements in the selected range and discard other measurements. Thus, we can eliminate false measurements based on dark count and this situation reduces QBER.

In Figure 3.25 and Figure 3.26, the measurement of a key, which is sent periodically and at a certain interval, are shown with time tagging module and APDs. The Y-axis

of the graph is the number of photons measured and the X-axis of the graph is the time which was done measurement with APDs or signals. The interval between the red lines in the Figure determines the start and end time of the Figure just below it. In the Figure 3.25, the mentioned interval is zoomed in order to increase the resolution. As mentioned before, the photons, which have vertical polarization, are measured on a non-orthogonal basis, so measurement happens at the output port of 135. Also, photons with 45-degree polarization are measured at horizontal output. Only 25 percent of the produced photons can be measured. Therefore, such a key was considered to be sent to confirm that the system is working properly and to visualize this measurement. In addition, the pulse width and intervals are kept wide and the intensity of the laser is kept high in order to ensure that the possibility of measurement is increased with each pulse. Of course, high light intensity causes inaccurate measurements due to the behavior of optical components and security. However, this was necessary in order to visualize the sent key, because when measurements were made at a low light intensity and without increasing the probability of measurement, it was not possible to distinguish correct measurements from inaccurate measurements caused by optical devices and from the environmental background light in order to visualize the measurements. In subsequent measurements, the light intensity will be reduced considerably. The graphs, which have their title written channel-5, show the pulses used to drive the laser. These pulses are used to synchronize the photons. They show the rising and falling times of each pulse and in the following sections, measurements, which are made outside of these intervals, are discarded because there will be no laser photons in the system except for these parts.

It is seen that the measurement intensity increases with an interval of approximately 1 second in Figure 3.25 (a). The measurement time of the experiment is approximately 4 seconds. When there is no photon in the system, incorrect measurements are made due to the environment as can be seen. First, the measurement density has increased in channel-1. Immediately afterward, the measurements in channel-1 decreased and channel-2 increased. This shows us that the orientation of the key has been measured correctly. When the area between two red lines is zoomed-in Figure 3.25 (b), it is seen that the region, where the measurement density is high, is less than between approximately 2659 milliseconds and 2767 milliseconds. If we calculate the time that each raw key is sent, we need to multiply 500 microseconds by 100, then multiply the result by

2 because of the 500 microseconds pulse period. The result is 100 milliseconds. This corresponds to the time it takes us to send a key. If we subtract 2766 milliseconds from 2655 milliseconds, the result will be 101 milliseconds and the key measurement is fairly close to the range made. This calculation is not very detailed, so this problem may be from rounding off the high digit numbers. These results will be calculated in more detail in the following sections. As for Figure 3.26 (c), the measurements in channel-1 does not start periodic at all, but the measurements in channel-2 are quite periodic. However, when the EOM position change at 2.713 seconds, periodicity changes between them. When a certain region is selected and zoomed as in 3.26 (d), it is understood that the laser pulses are approximately 50 microseconds and the interval between two laser pulses is 500 microseconds. It is easily seen that each synchronization pulse corresponds to a measurement. Thus, in the next step, a random key can be sent.

Even if we guarantee to measure in each pulse at high laser counts, the possibility of making two measurements at the same time increases due to the fact that there is more than one photon in the system at the same time and this disrupts the security of the system. When we reduce the counts of the laser, a serious decrease in the number of measurements is observed. This is due to the Poisson distribution of photons generated from the laser. In Figure 3.27, this situation can be seen. Figure 3.27 (a) shows measurements with high laser counts while Figure 3.27 shows measurements with low laser counts. In Figure 3.27 (a), the polarization direction is changed in each pulse, so the key is like 101010... . As it is observable, the measurement starts with channel-1 then another measurement is made at channel-2. The measurements of the channels change each pulse. However, except for one thing, the generated key is successfully sent to Bob. There are measurements that are at the same time. Moreover, there are some empty parts. Empty parts are not the problem but measurements, which are at the same time, are a security problem. Thus, It is necessary to reduce the count of the laser so that it is one photon per pulse. When you look at Figure 3.27 (b), there are one channel measurements at each pulse but measurements are really rare.

If each measurement from the signal generator is subtracted from the previous measurement or each measurement is started from zero-second, the measured laser photons are collected in a certain area. Thus, this range can be called the area in the system where the laser photons are located. Measurements which were made in the part outside

this area are the wrong detection and the source of them are surrounding environment. Thus, these detections can be filtered out. Also, each measurement can be enumerated with this method. In Figure 3.28, data is plotted with this algorithm. Laser photons and dark count measurements are easily recognized from Figure 3.28. Moreover, in this figure, measurements of the different laser power are shown. The density of the bin number changes depending on the laser power, this difference is easily noticed from the figure.

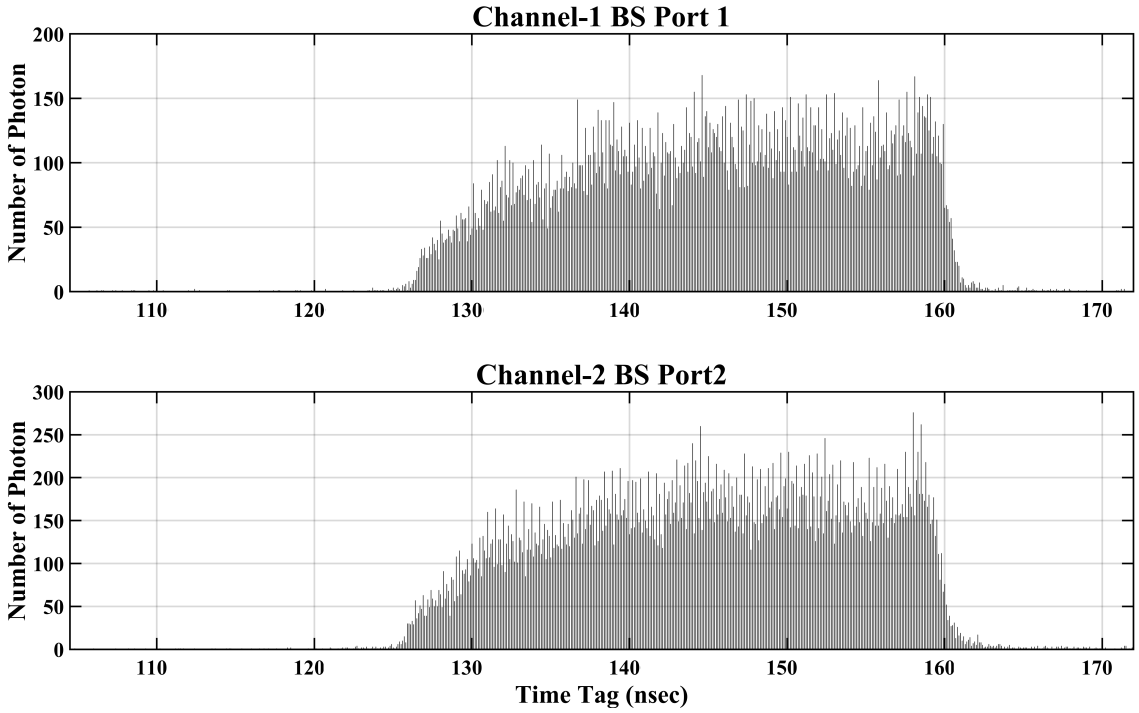


Figure 3.29. Dense part of the Figure 3.28. Subtracting the measurement time of each synchronization signal, all photon measurements will be collected in a area. Measurements of laser photons create a denser area. This is the area where the key is located. Then, the key is obtained from this area with the analysis algorithm created in Matlab.

If the dense part of the data is selected, Figure 3.29 is obtained. It is noticed that this interval is equal to nearly 350 ns. This value is equal to the pulse width of the laser.

CHAPTER 4

EXPERIMENTAL RESULTS

After all the preparations, studies, and analyses, it has come to the part of obtaining the key. Up to this section, the determination of the appropriate and safe laser power level, establishing the appropriate optical setup, measuring the polarization of the photons properly, controlling the polarization of the photons, ensuring that the photons sent by Alice are properly and accurately measured by Bob, between Alice and Bob. Studies such as sending information in a synchronized way have been carried out successfully. In this section, studies on determining the length of the generated and measured key (key rate), determining the accuracy of the key measured by Bob (QBER), and securely transmitting information with the generated key will be carried out.

4.1. Key Rate and Quantum Bit Error Rate

In this section, the average number of keys obtained and false measurements will be discussed. Before starting the test results, it is necessary to talk about the key rate and quantum bit error rate.

Key rate is divided into the raw key rate and sifted key rate. However, since there is no sifted key concept in the B92 protocol, it is possible to calculate the key rate directly. The key rate is the ratio of the generated key to time in bits. This gives us the length of the key we can generate in one second. The longer the key length obtained, the greater the security of the information to be encrypted. Because the key used for encryption requires processing power for people who do not know the key to obtain the key, and the longer the key length, the greater the processing power required to decrypt it.

Quantum bit error rate (QBER) is an equation that gives the ratio of incorrect measurements in the key. In addition, the reason for these incorrect measurements is due to environmental factors, as well as the information that third parties have infiltrated. For cases where the QBER rate is above 11%, the conclusion is that the key is not secure and is seen as evidence of the existence of an eavesdropper on the quantum channel. A QBER

rate below 11% ensures that the key is secure. The following equation gives the QBER.

$$QBER = \frac{N_{wrong}}{N_{true} + N_{wrong}} \tag{4.1}$$

An attack by making a measurement for all qubits and resending the measurement result will result in an error rate of 25%. This is because if Eve is measuring on the system, she only has a chance to detect half of the key correctly and 50% will resend the wrong key and this will cause an error rate of 25% on Bob. The QBER rate is used to detect the presence of the listener in the system. In addition, the QBER ratio increases due to environmental changes, the noise produced by ambient light, the extinction ratio of PBSs, the dark current of the single-photon detectors, deterioration of polarization, presence of circular polarization in the system. For reducing the actual QBER rate, it is necessary to minimize all error causes.

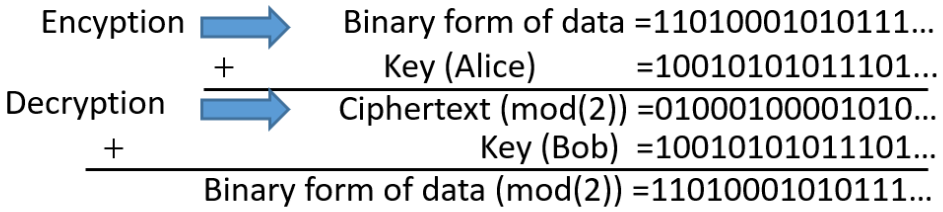


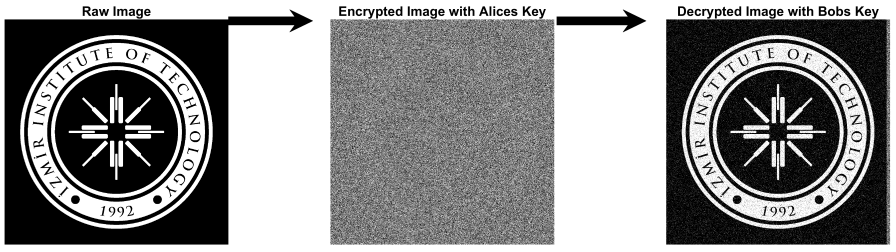
Figure 4.1. Encryption and decryption method of the logo. In order to encrypt the information, the information is first converted into binary form. Then, the information in binary form is added by the obtained key, and the sum of the information is taken as a modulus of 2. The encrypted information is obtained and sent to Bob. Then Bob adds the encrypted information with the key he obtained and gets a modulus of 2 again. Bob decrypts the information.

In the measurements made in the system, the average QBER took with a 1 MHz faint pulsed laser is 5.13%. Average key rate is 63.86 Kbit/sec at nearly $\mu = 0.25$. Min-

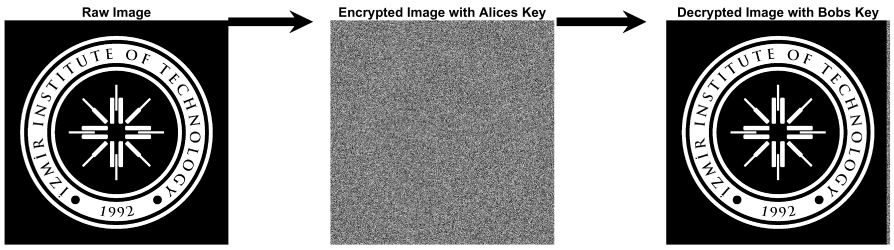
imum measured QBER is $\%2.43$ by software filter and the key rate is that level 15,981 Kbps at nearly $\mu = 0.1$. In case the mean photon number is the most ideal, the maximum key rate we can detect is 20Kbps with Qeff ($\%80$). In the case where we measure all photons, we can get a speed of 25Kbps from the system at 1 MHz (1000000 photons x 0.1 (μ) x 0.5 (from BS) x 0.5 (from PBS) =25000 photons).

4.2. Encryption and Decryption with The Key

In this section, an Iztech logo will be encrypted and then decrypted using the key generated between Alice and Bob. In Figure 4.2, a pre-generated random key is shared between Alice and Bob in the quantum channel. Then the measured key is compared with the help of Matlab.



(a)



(b)

Figure 4.2. Encrypted and decrypted Iztech logo. Figure (a) shows the encrypted and decrypted logo with the uncorrected key. Figure (b) shows the encrypted and decrypted logo with a corrected key. With uncorrected key, there is some noise in the figure.

First of all, to talk about how the logo was encrypted, Alice and Bob shared a key between them. Alice converted the logo into binary form and added the information in binary form and the key she sent with each other. Furthermore, she took the modulus of the obtained number sequence with respect to two. After that, she sent the encrypted information to Bob. Bob added the binary information he received with the key he obtained. Next, he took the modulus of the sum by two, and the information was decrypted. Then it converted the information in binary form into the logo. In the Figure 4.1, the method is shown.

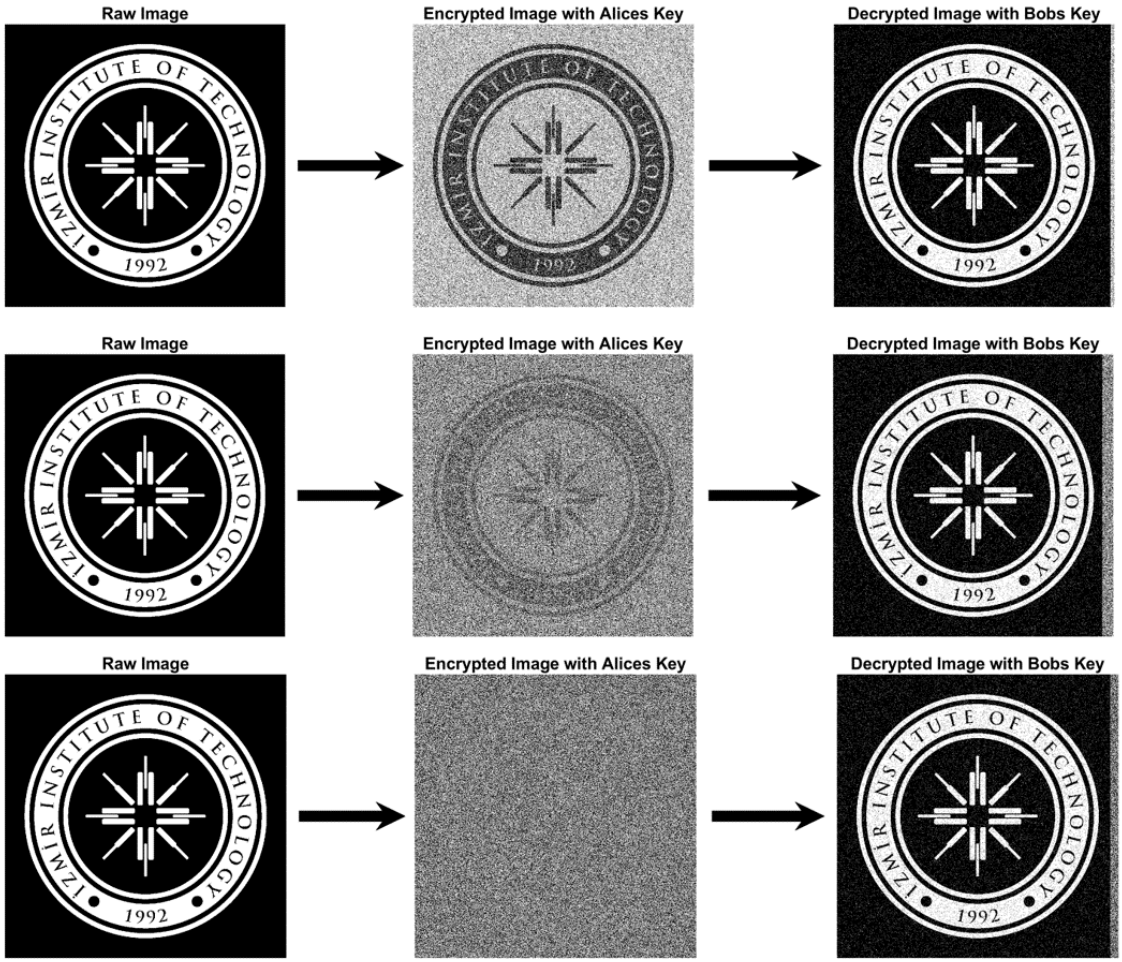


Figure 4.3. Key Rate Dependent Encrypted and Decrypted Iztech logo and the key rates are 15.981, 39.674, 63.947 Kbps from top to bottom, respectively.

As seen in the Figure 4.2a, a logo is encrypted and the logo is too noisily to be

understood (encrypted). Then it was decrypted with the key that Bob measured. When looking at the decrypted logo, there are noisy pixels in some places. The reason for these losses is due to QBER. If the key between Alice and Bob is exactly the same, there is no loss of the decrypted logo. In Figure 4.2b shows encrypted and decrypted Iztech logo with corrected key.

The encrypted and decrypted Iztech logo is shown in the Figure 4.3, depending on the length of the key. As can be seen from the figure, the length of the key distorts the image of the encrypted logo. As it can be understood from here, the rate of the generated key is an important factor in terms of security in the inability to understand the encrypted information. The rate of the keys used in the logos shown in the Figure is 15.981, 39.674, 63.947 Kbps from bottom to top, respectively.

CHAPTER 5

CONCLUSION

As a result, a proof of concept BB84 and B92 protocol was created with the help of an attenuated pulsed laser. Except for the high voltage amplifier, all of our equipment can operate at speeds higher than 1 MHz. However, the high voltage amplifier has limited us to 1 MHz. In this project, the goal is to set up a quantum key distribution and generate a key. Then, using this setup, it is possible to perform quantum key distribution with a solid-state material (hBN defects) that emits single photons. However, in the studies, it was not possible to show with single photons emission from hBN defects, because no suitable defect that could be excited at 1 MHz excitation rate was found during the studies. The reason for this was that the APDs used had a dark count (750 cps) and it was not looked possible to distinguish between photons coming from the surroundings and dark count and the photons coming from the hBN with optical losses. If the HBN defect that can radiate more efficiently such as increase its efficiency, or a more bright defect is found, the experiment can be carried out successfully. During this thesis, an optical setup is performed with an attenuated pulsed laser, and the obtained QBER and key rate are shown. While the best QBER result is $\%2.43$, an average of $\%5.2$ is obtained. Also, while the average key rate was 63.86 Kbit/s at $\mu = 0.25$, the minimum measured QBER is $\%2.43$ by software filter (time gating filter) and the key rate is that level 15.981 Kbps at $\mu = 0.13$.

What can be done after this study?

The QKD system is ready to apply for any single-photon source. In addition, easily change the optical setup to the BB84 protocol for increasing key rate by adding 4 identical APDs. Moreover, rate efficiency can be increased by reducing the lifetime of hBN defects emission with a cavity for getting more photons and higher speeds can be achieved by adding a faster high-voltage amplifier to the system. Thus, hBN defects can be excited at a higher frequency or the system can be used with a different material that emits a single photon.

Further, experiments can be made by increasing the distance between Alice and Bob. If there is a single-photon emitter that emits in the blue-green region, it can be tested underwater. Additionally, optical fiber-based single-photon experiments can be performed. Furthermore, in order to improve the system, error detection and correction algorithms can be developed and a true random number generator can be developed and added to the system.

REFERENCES

Aharonovich, I., D. Englund, and M. Toth (2016, sep). Solid-state single-photon emitters. *Nature Photonics 2016 10:10 10*(10), 631–641.

Al-Kathiri, S., W. Al-Khateeb, M. Hafizulfika, M. R. Wahiddin, and S. Saharudin (2008). Characterization of mean photon number for key distribution system using faint laser. *Proceedings of the International Conference on Computer and Communication Engineering 2008, ICCCE08: Global Links for Human Development*, 1237–1242.

Aspect, A. (1975). Proposed experiment to test separable hidden-variable theories. *Physics Letters A 54*(2), 117–118.

Aspect, A. (2004). *Bell's Theorem: The Naive View of an Experimentalist*.

Basset, F. B., M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, and R. Trotta (2021, mar). Quantum key distribution with entangled photons generated on demand by a quantum dot. *Science Advances 7*(12).

BELL, J. S. (1995). On the Einstein Podolsky Rosen paradox. pp. 701–706.

Bellare, M. and P. Rogaway (2005). Introduction to Modern Cryptography Bellare.pdf. pp. 1–283.

Benioff, P. (1980, may). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics 22*(5), 563–591.

Bennett, C. H. (1992, may). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters 68*(21), 3121–3124.

Bennett, C. H. and G. Brassard (2014, mar). Quantum cryptography: Public key distribu-

tion and coin tossing. *Theoretical Computer Science 560*(P1), 7–11.

Bennett, C. H., G. Brassard, and N. D. Mermin (1992, feb). Quantum cryptography without Bell's theorem. *Physical Review Letters 68*(5), 557–559.

Biggs, N. (2009). Codes: an introduction to information communication and cryptography. *Choice Reviews Online 46*(08), 46–4496–46–4496.

Birowosuto, M. D., H. Sumikura, S. Matsuo, H. Taniyama, P. J. Van Veldhoven, R. Nötzel, and M. Notomi (2012, mar). Fast Purcell-enhanced single photon source in 1,550-nm telecom band from a resonant quantum dot-cavity coupling. *Scientific Reports 2*(1), 1–5.

Bruss, D., G. Erdélyi, T. Meyer, T. Riege, and J. Rothe (2007, jul). Quantum cryptography: A survey. *ACM Computing Surveys 39*(2), 27.

Castellanos-Gomez, A., G. A. Steele, H. S. J. van der Zant, J. Kern, M. Buscema, P. Tondorf, R. Schmidt, R. Schneider, R. Bratschitsch, and S. M. de Vasconcellos (2015, apr). Single-photon emission from localized excitons in an atomically thin semiconductor. *Optica, Vol. 2, Issue 4, pp. 347-352 2*(4), 347–352.

Castelletto, S., B. C. Johnson, V. Ivády, N. Stavrias, T. Umeda, A. Gali, and T. Ohshima (2014). A silicon carbide room-temperature single-photon source. *Nature Materials 13*(2), 151–156.

Chen, S., Y. A. Chen, T. Strassel, Z. S. Yuan, B. Zhao, J. Schmiedmayer, and J. W. Pan (2006, oct). Deterministic and storable single-photon source based on a quantum memory. *Physical Review Letters 97*(17), 173004.

Chowdhury, T., K. Jo, S. B. Anantharaman, T. H. Brintlinger, D. Jariwala, and T. J. Kempa (2021, aug). Anomalous Room-Temperature Photoluminescence from Nanostrained MoSe2Monolayers. *ACS Photonics 8*(8), 2220–2226.

Clauser, J. F., M. A. Horne, A. Shimony, and R. A. Holt (1969, oct). Proposed experiment

to test local hidden-variable theories. *Physical Review Letters 23*(15), 880–884.

Damico, T. and D. Davies (2009). A Brief History of Cryptography - Inquiries Journal. *Information Security Technical Report*.

Diffie, W. and M. E. Hellman (2019). New directions in cryptography. In *Secure Communications and Asymmetric Cryptosystems*, pp. 143–180.

Dixon, A. R., Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields (2008, nov). Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Optics Express 16*(23), 18790.

Einstein, A., B. Podolsky, and N. Rosen (1935, may). Can quantum-mechanical description of physical reality be considered complete? *Physical Review 47*(10), 777–780.

Eisaman, M. D., J. Fan, A. Migdall, S. V. Polyakov, M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov (2011, jul). Invited Review Article: Single-photon sources and detectors. *RScI 82*(7), 071101–071101–25.

Ekert, A. K. (1991). Quantum cryptography based on Bellâs theorem. *Physical Review Letters 67*(6), 661–663.

ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Volume 196 LNCS, pp. 10–18.

Feistel, H. (1973, may). Cryptography and Computer Privacy. *Scientific American 228*(5), 15–23.

Feng, Z., S. Li, and Z. Xu (2021, mar). Experimental underwater quantum key distribution. *Optics Express 29*(6), 8725.

Feynman, R. P. (1982, jun). Simulating physics with computers. *International Journal of*

Theoretical Physics 1982 21:6 21(6), 467–488.

Fox, M. (2006). *Quantum Optics: An Introduction (Google eBook)*. Oxford University Press.

Gibney, E. (2019a, oct). Hello quantum world! Google publishes landmark quantum supremacy claim.

Gibney, E. (2019b, oct). Quantum gold rush: the private funding pouring into quantum start-ups. *Nature 574*(7776), 22–24.

Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden (2002, mar). Quantum cryptography. *Reviews of Modern Physics 74*(1), 145–195.

Goetz, R. E. and K. Bartschat (2021, apr). Quantum control of entangled photon-pair generation in electron-atom collisions driven by laser-synthesized free-electron wave packets. *Physical Review A 103*(4), 043112.

Goldreich, O. (2004). *Foundations of Cryptography*.

Graham, S. (1999, nov). Remote Sensing - Absorption Bands and Atmospheric Windows.

Grangier, P., G. Roger, and A. Aspect (1986, feb). Experimental evidence for a photon anticorrelation effect on a beam splitter: A new light on single-photon interferences. *EPL 1*(4), 173–179.

Grosso, G., H. Moon, B. Lienhard, S. Ali, D. K. Efetov, M. M. Furchi, P. Jarillo-Herrero, M. J. Ford, I. Aharonovich, and D. Englund (2017, sep). Tunable and high-purity room temperature single-photon emission from atomic defects in hexagonal boron nitride. *Nature Communications 8*(1), 1–8.

He, Y. M., G. Clark, J. R. Schaibley, Y. He, M. C. Chen, Y. J. Wei, X. Ding, Q. Zhang, W. Yao, X. Xu, C. Y. Lu, and J. W. Pan (2015, jun). Single quantum emitters in monolayer semiconductors. *NatNa 10*(6), 497–502.

Heisenberg, W. (1927, mar). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik 43*(3-4), 172–198.

Heisenberg, W. (1989). *Encounters with Einstein : and other essays on people, places, and particles*.

Kimble, H. J., M. Dagenais, and L. Mandel (1977, sep). Photon antibunching in resonance fluorescence. *Physical Review Letters 39*(11), 691–695.

Korzh, B., C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden (2015, jul). Provably secure and practical quantum key distribution over 307km of optical fibre. *Nature Photonics 9*(3), 163–168.

Kupko, T., M. von Helversen, L. Rickert, J. H. Schulze, A. Strittmatter, M. Gschrey, S. Rodt, S. Reitzenstein, and T. Heindel (2020, mar). Tools for the performance optimization of single-photon quantum key distribution. *npj Quantum Information 6*(1), 1–8.

Kurtsiefer, C., S. Mayer, P. Zarda, H. Weinfurter, C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter (2000, jul). Stable Solid-State Source of Single Photons. *PhRvL 85*(2), 290–293.

Lamas-Linares, A., J. C. Howell, and D. Bouwmeester (2001, aug). Stimulated emission of polarization-entangled photons. *Nature 412*(6850), 887–890.

Leifgen, M., T. Schröder, F. Gädeke, R. Riemann, V. Métillon, E. Neu, C. Hepp, C. Arend, C. Becher, K. Lauritsen, and O. Benson (2014, feb). Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution. *New Journal of Physics 16*(2), 023021.

Liu, Y., P. Siyushev, Y. Rong, B. Wu, L. P. McGuinness, F. Jelezko, S. Tamura, T. Tanii, T. Teraji, S. Onoda, T. Ohshima, J. Isoya, T. Shinada, H. Zeng, and E. Wu (2015, dec). Investigation of the silicon vacancy color center for quantum key distribution. *Optics Express 23*(26), 32961.

Lo, H. K., X. Ma, and K. Chen (2005, oct). Decoy state quantum key distribution. *Physical Review Letters 94*(23).

Lohrmann, A., S. Castelletto, J. R. Klein, T. Ohshima, M. Bosi, M. Negri, D. W. M. Lau, B. C. Gibson, S. Prawer, J. C. McCallum, B. C. Johnson, A. Lohrmann, S. Castelletto, J. R. Klein, T. Ohshima, M. Bosi, M. Negri, D. W. M. Lau, B. C. Gibson, S. Prawer, J. C. McCallum, and B. C. Johnson (2016, jan). Activation and control of visible single defects in 4H-, 6H-, and 3C-SiC by oxidation. *ApPhL 108*(2), 021107.

Ma, X., N. F. Hartmann, J. K. Baldwin, S. K. Doorn, and H. Htoon (2015, aug). Room-temperature single-photon generation from solitary dopants of carbon nanotubes. *Nature Nanotechnology 10*(8), 671–675.

Maurer, C., C. Becher, C. Russo, J. Eschner, and R. Blatt (2004, jul). A single-photon source based on a single Ca+ ion. *New Journal of Physics 6*(1), 94.

Menezes, A. J. (1996). *Applied Cryptography*, Volume 1.

Merriam-Webster.com Dictionary, s. (2021). Cryptology (definition).

Michler, P., A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. ImamoÇ§lu (2000, dec). A Quantum Dot Single-Photon Turnstile Device. *Science 290*(5500), 2282–2285.

Mizuochi, N., T. Makino, H. Kato, D. Takeuchi, M. Ogura, H. Okushi, M. Nothaft, P. Neumann, A. Gali, F. Jelezko, J. Wrachtrup, and S. Yamasaki (2012, may). Electrically driven single-photon source at room temperature in diamond. *Nature Photonics 6*(5), 299–303.

Monroe, C. (2002, mar). Quantum information processing with atoms and photons.

Müller, T., J. Skiba-Szymanska, A. B. Krysa, J. Huwer, M. Felle, M. Anderson, R. M. Stevenson, J. Heffernan, D. A. Ritchie, and A. J. Shields (2018, feb). A quantum light-emitting diode for the standard telecom window around 1,550 nm. *Nature Com-*

munications 9(1), 1–6.

Nielsen, M. A., I. Chuang, and L. K. Grover (2002, may). Quantum Computation and Quantum Information. *American Journal of Physics 70*(5), 558–559.

Pan, F. and P. Zhang (2021, mar). Simulating the Sycamore quantum supremacy circuits.

Pawlan, M. (2005). Cryptography: The Ancient Art of Secret Messages.

Pelc, J. S., L. Yu, K. De Greve, P. L. McMahon, C. M. Natarajan, V. Esfandyarpour, S. Maier, C. Schneider, M. Kamp, S. Höfling, R. H. Hadfield, A. Forchel, Y. Yamamoto, and M. M. Fejer (2012, sep). Downconversion quantum interface for a single quantum dot spin and 1550-nm single-photon channel. *Optics Express 20*(25), 27510.

Rivest, R. L., A. Shamir, and L. M. Adleman (2019). A method for obtaining digital signatures and public key cryptosystems. In *Secure Communications and Asymmetric Cryptosystems*, pp. 217–239.

Roe, P. (1998). Explorations in Quantum Computing. *AIAA Journal 36*(11), 2152–2152.

Schimpf, C., M. Reindl, D. Huber, B. Lehner, S. F. Covre Da Silva, S. Manna, M. Vyvlecka, P. Walther, and A. Rastelli (2021). Quantum cryptography with highly entangled photons from semiconductor quantum dots. *Science Advances 7*(16).

Schmitt-manderbach, T. (2007). Long distance free-space quantum key distribution. *Doctoral Dissertation*.

Silverstone, J. W., R. Santagati, D. Bonneau, M. J. Strain, M. Sorel, J. L. O'Brien, and M. G. Thompson (2015, aug). Qubit entanglement between ring-resonator photon-pair sources on a silicon chip. *Nature Communications 6*.

Steane, A. (1998, feb). Quantum computing. *Reports on Progress in Physics 61*(2), 117–173.

Steiner, M., A. Hartschuh, R. Korlacki, and A. J. Meixner (2007, may). Highly effi-

cient, tunable single photon source based on single molecules. *Applied Physics Letters 90*(18), 183122.

Takesue, H., K. Inoue, O. Tadanaga, Y. Nishida, and M. Asobe (2005, feb). Generation of pulsed polarization-entangled photon pairs in a 155-um band with a periodically poled lithium niobate waveguide and an orthogonal polarization delay circuit. *Optics Letters 30*(3), 293.

Tonndorf, P., R. Schmidt, P. Bottger, X. Zhang, J. Borner, A. Liebig, M. Albrecht, C. Kloc, O. Gordan, D. R. Zahn, S. M. De Vasconcellos, and R. Bratschitsch (2013, jun). Photoluminescence emission and Raman response of MoS2, MoSe 2, and WSe2 nanolayers. In *2013 Conference on Lasers and Electro-Optics, CLEO 2013*, pp. QTu1D.1. Optical Society of America.

Tran, T. T., K. Bray, M. J. Ford, M. Toth, I. Aharonovich, T. T. Tran, K. Bray, M. J. Ford, M. Toth, and I. Aharonovich (2016, jan). Quantum emission from hexagonal boron nitride monolayers. *NatNa 11*(1), 37–41.

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

van Leeuwen, J. (1990). *Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics*, Volume 4.

Wolf, R. (2021). Quantum Key Distribution Protocols. In *Lecture Notes in Physics*, Volume 988, pp. 91–116.

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

Yin, J., Y. Cao, Y. H. Li, S. K. Liao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, B. Li,

H. Dai, G. B. Li, Q. M. Lu, Y. H. Gong, Y. Xu, S. L. Li, F. Z. Li, Y. Y. Yin, Z. Q. Jiang, M. Li, J. J. Jia, G. Ren, D. He, Y. L. Zhou, X. X. Zhang, N. Wang, X. Chang, Z. C. Zhu, N. L. Liu, Y. A. Chen, C. Y. Lu, R. Shu, C. Z. Peng, J. Y. Wang, and J. W. Pan (2017, jun). Satellite-based entanglement distribution over 1200 kilometers. *Science 356*(6343), 1140–1144.