TIMING SIDE CHANNEL ISSUES AND PHOTON BUDGET OPTIMIZATION IN QKD

A Dissertation

by

Melis Pahalı

Submitted to the
Graduate School of Sciences and Engineering
In Partial Fulfillment of the Requirements for
the Degree of

Doctor of Philosophy

in the
Department of Electrical and Electronics Engineering

Özyeğin University

TIMING SIDE CHANNEL ISSUES AND PHOTON BUDGET OPTIMIZATION IN QKD

Approved by:

Asst. Prof. Kadir Durak, Advisor
Dept. of Electrical and Electronics Eng.
Özyeğin University

Asst. Prof. Ahmed Akgiray
Dept. of Electrical and Electronics Eng.
Özyeğin University

Prof. H. Fatih Uğurdağ
Dept. of Electrical and Electronics Eng.
Özyeğin University

Prof. Özgür M. Müstecaplıoğlu
Dept. of Physics
Koç University

Date Approved: Dec. 2022

Prof. Sadi Turgut
Dept. of Physics
Middle East Technical University

To my family, friends and advisors,

ABSTRACT

Prepare-and-measure and entanglement-based quantum-key-distribution (QKD) protocols are vulnerable against a side channel attack that exploits the time difference in detectors' responses used to obtain key bits. There is a correlation between the timing histograms of the detectors and the values of bits they generate, and information leakage to an eavesdropper is quantified by mutual information between them. The recommended solution against the timing side channel attack is to use a large time bin width instead of high-resolution timing information in the QKD system. A common notion is that using a large bin width reduces the resolution of detectors' responses, hence supposedly minimizes the information leakage to an eavesdropper. We challenge this conventional wisdom and demonstrate that increasing the bin width does not monotonically reduce the mutual information between the key bits and the detectors' responses. Second, we discover the parameter of start time of binning and show the characteristic behaviour of the mutual information with respect to it. Third, we examine the effect of full width half maximums of the detectors' responses on the mutual information. As a result, although QKD is theoretically secure in cryptographic point of view, it should be protected against side channel attacks, and our findings about these three points should be found in the body of the thesis and should be taken into account in order to estimate leakage information to a possible eavesdropper correctly.

Additionally, there is a huge effort to improve data transfer capacity in QKD technologies to make it deployable in various size establishments and on a global scale. We propose a method to increase raw key rate in discrete-variable entanglement-based QKD applications in which a Bell's inequality is employed for security check. We

focus on a standardized E91 QKD system. This method relies on the optimization of photon budget allocation among different types of bits generated purposely and occurred unavoidably in the QKD system. Additionally, we examine the optimized values of core variables depending on various photon budgets. Meanwhile, we remind the dependencies and limitations of photon counting process to the reader.

ÖZETÇE

Hazırla-ve-ölç ve dolanıklık-tabanlı kuantum anahtar dağıtımı (KAD) protokollerinin, anahtar bitleri elde etmek için kullanılan dedektörlerin yanıtlarındaki zaman farkından yararlanan bir zamanlama yan kanal saldırısına karşı savunmasız olduğu bilinmektedir. Bu yan kanal saldırısına karşı önerilen çözüm, yüksek çözünürlüklü zamanlama bilgisi yerine geniş bir zaman bölmesi kullanmaktır. Yaygın bir görüş, geniş bir zaman bölmesi kullanmanın, dedektörlerin yanıtlarının çözünürlüğünü azalttığı, dolayısıyla muhtemel bir saldırgana bilgi sızıntısını en aza indirdiği yönündedir. Bu çalışmada, zaman bölmesi genişliğini artırmanın, foton algılama zamanları ile anahtar bitleri arasında olan ortak bilgiyi ve dolayısıyla bir saldırgana sızabilecek bilgiyi monoton bir şekilde azaltmadığını gösteriyoruz. İkinci olarak, başka bir parametre keşfediyoruz ve ortak bilginin ona göre karakteristik davranışını gösteriyoruz. Üçüncü olarak, dedektörlerin yanıtlarının ortak bilgi üzerindeki etkisini inceliyoruz. Bu üç nokta ile ilgili tespitlerimiz tezin ana metninde bulunmalı ve olası bir saldırgana sızacak bilgiyi doğru tahmin edebilmek için dikkate alınmalıdır.

Ek olarak, KAD teknolojilerinin çeşitli büyüklükteki kuruluşlar için kullanılabilir ve küresel ölçekte konuşlandırılabilir hale getirilmesi için veri aktarım kapasitelerinin geliştirilmesi üzerine büyük çabalar sarf edilmektedir. Ayrık-değişkenli, dolanıklık-tabanlı, Bell eşitsizliği üzerinden güvenlik kontrolü yapan KAD uygulamalarında ham anahtar oranını artırmak için bir yöntem öneriyoruz. Standartlaşmış bir E91 KAD sistemini ele alıyoruz. Yöntemimiz, kasıtlı olarak üretilen veya kaçınılmaz olarak meydana gelen farklı bit türleri arasında foton bütçe tahsisinin optimizasyonuna dayanıyor. Ayrıca, çeşitli foton bütçelerine bağlı olarak optimize edilmiş en önemli değişkenlerin değerlerini inceliyoruz. Bu arada, okuyucuya foton sayma işleminin

bağımlı olduğu parametreleri ve limitlerini anımsatıyoruz.

ACKNOWLEDGEMENTS

Research topics discussed in this dissertation were supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK), Academic Research Funding Programs Directorate (ARDEB), Primary Subjects R&D Funding Program (Program No. 1003), Project No. 118E991. Additionally, experiment which is demonstrated in Sec. 2.5 was performed with my colleagues Hashir Kuniyil and Ramin Sattari. I would like to thank my advisor Asst. Prof. Kadir Durak for giving me the opportunity to study on the topics and for his supports. I would like to thank Dr. Utku Tefek for his supports in various ways. I would like to thank Abdulrahman Dandaşi, Ekin Aykut, Dr. Reza Bayat, Kaan Batu Süar and Hashir Kuniyil for various useful discussions we had during the study process on the topics. I would like to thank Prof. Dr. Ömer Faruk Dayı, Prof. Dr. Ferid Salehli, and Prof. Dr. Ali Yıldız for the discussions and their guidance.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Today, classical cryptography is used in all the applications where security (data privacy, and authentication of communicating sides and information transceived) is required. For data privacy, a transmitter uses a cipher (algorithm) to encode a plaintext with a key to convert it to a ciphertext, and receiver decodes it into original plaintext by using a cipher (decipher, inverse algorithm) with the same or a paired key. There are two types of cryptographic systems which are symmetric and asymmetric cryptography. The most recognizable feature of symmetric cryptography is that only a single-key value is used for both encryption and decryption. Early examples of symmetric key encryption are block ciphers and stream ciphers which differ in the speed of encryption/decryption (caused by the waiting time of data being collected) and the memory usage of hardware being used (because while block ciphers encrypt data as the groups of 64, 128, 192 or 256 bits, stream ciphers can encrypt each bit or 8 bits separately). There are rounds of computations in which different subkeys derived from an encryption key and an encryption function are used to generate a ciphertext. If we think in terms of a matrix configuration, each round is composed of the stages of substitution of bytes as a padding, row shifting, column mixing and XOR operation. Modern symmetric key cryptography algorithms like Data Encryption Standard (DES) [2], Advanced Encryption Standard (AES) algorithms [3], International Data Encryption Algorithm (IDEA) [4], Blowfish are commonly used today. On the other hand, in asymmetric cryptography there are two keys which are paired. While one key is used for encryption (it is sent by a receiver to a transmitter publicly) and is called public-key, the other one is used for decryption at the receiver and is called private-key.

Asymmetric cryptography can be used for both data privacy and authentication purposes. Asymmetric cryptography algorithms can be grouped into three types which are RSA, Elliptic Curve Variant (ElGamal) and Elliptic Curve Cryptography (ECC) algorithms. RSA is based on the factorization of prime numbers problem, ElGamal and ECC are based on discrete logarithm problems. While symmetric cryptography is based on the operations on the strings of bits, asymmetric cryptography is based on the (arithmetical) operations on numbers and a publicly shared key (public-key). The most common algorithms used are that of AES algorithms in symmetric cryptography algorithms and RSA ciphers in asymmeric cryptography algorithms. They are used to secure valuable information in governments, critical infrastructures, financial applications, synchronization banking etc. The security of public key cryptography relies on the computational complexity in the era of classical computers. However, since none of the computational complexities are unsurpassed against the computational capabilities of quantum computers, the algorithms based on computational complexity become vulnerable against quantum computers. More precisely, Shor's algorithm is the threat against factorization and discrete logarithm problems [5]. The superiority of quantum algorithms which are running on quantum computers come from parallel computational capability which results from the superposition property of quantum states and speeds up the computational process. On the other hand, symmetric cryptography offers a more layered and complex ecosystem, it is resilient to cryptoanalysis (transform ciphertext to plaintext without estimating key correctly), and there is no a publicly shared key usage. Quantum computers enable quadratic speed up with Grover's algorithm against symmetric cryptography and exponential speed up with Shor's algorithm against asymmetric cryptography [6]. The quadratic speed up may become slow against symmetric cryptography depending on the key length used. Thus, symmetric algorithms are stronger and they can continue to be used. In addition to the conventional symmetric algorithms, there is another algorithm called

one-time pad (OTP) which offers cryptographically ideal security [7, 8] if the following conditions are satisfied. Encryption/decryption key must be composed of random (equally likely) bits in order to have maximum uncertainty in estimating the values of bits [6]. It must be in the same size as plaintext and must not have repetitive sequences of bits, otherwise it may cause repeating patterns in ciphertext. It must be used only once per plaintext in order not to be predictable by non-authenticated sides, and then it should be destroyed by taking into account the possibility of a security gap related to memory device. The encryption (decryption) method is based on the XOR operation of key with plaintext (ciphertext). Until recently, the use of OTP algorithm was limited to a few areas like military and diplomacy because it requires long encryption keys (against the simple encryption algorithm) and it was not feasible in terms of encryption processing time in daily life, also the usage of the conventional cryptography algorithms was offering sufficient secrecy with 192-bit, 256-bit keys etc. (in a more complex cryptosystem) in the era of classical computers, and the distribution of key to legitimate communicating sides are not feasible in terms of the number of trusted couriers required in daily life. However, it is thought that the use of OTP algorithm will be encountered more frequently in various fields against attacks with quantum computers in the future, for that reason we want to elaborate it more. To begin with, ideal security (perfect secrecy) for a cryptographic system is defined by the following. Key space is the space of all the probable keys which can be used in a cryptographic system. The number of elements of key space depends on the length of key that will be used, and there is a probability distribution for all the elements on key space. Likewise, there is also a probability distribution for all the possible values of plaintext having a certain length. Perfect secrecy is defined as the equivalence of the conditional probability of obtaining a plaintext (among all the possible plaintexts) given a ciphertext and the marginal probability of obtaining

the plaintext as given in Eq. (1) [9].

$$\mu_{\mathbf{P}|\mathbf{C}}(p|c) = \mu_{\mathbf{P}}(p) \tag{1}$$

where $\mu_{\mathbf{P}}(p)$ is the marginal probability of obtaining plaintext $p \in \mathbf{P}$ and $\mu_{\mathbf{P}|\mathbf{C}}(p|c)$ is the conditional probability of obtaining p given ciphertext $c \in \mathbf{C}$ where $\mathbf{P}$ and $\mathbf{C}$ are plaintext and ciphertext space, respectively. Namely, the knowledge of a ciphertext does not reveal any information about the original plaintext (for an attacker) [10]. In information theory, the expected value of or the quantification of uncertainty is given by (Shannon) entropy whose unit is bits (or bits/symbol) and it is given as in Eq. (2) for key space $\mathbf{K}$.

$$H(K) = -\sum_{k} \mu_{\mathbf{K}}(k) \log_2 \mu_{\mathbf{K}}(k) \tag{2}$$

where $\mu_{\mathbf{K}}(k)$ is the probability of obtaining key $k \in \mathbf{K}$ and $H(K)$ is the entropy of random variable K. For uniform probability distribution ($\mu_{\mathbf{K}}(k) = \frac{1}{|\mathbf{K}|}$ where $|\mathbf{K}|$ is the number of elements (events) of $\mathbf{K}$), entropy has the maximum value among its all possible values. It means there is max uncertainty in estimating key (for an attacker). True random key generation can be realized with the use of quantum random number generators, encryption processing time can be decreased with the computational capacity of quantum computers, and the use of OTP can be encountered more frequently in daily life. The usage of one or more symmetric cryptography algorithms (so called a hybrid system and its one component is generally OTP as encountered in the literature) [11, 12, 13] would be sufficient for encryption, however, there will be the problem of key management or the secure distribution of encryption/decryption keys, and quantum cryptography (QC) plays a role here. QC is used for the secure distribution of the classical cryptographic encryption/decryption keys and the security is provided with the laws of physics.

In QC, logic bit 0 and 1 can be encoded into various degrees of freedom of photons like polarization (spin angular momentum [14]), orbital angular momentum, arrival

time to a detector, or they can be encoded into the amplitude [15] or phase [16] quadrature of electromagnetic field of light. Logic bits are in the form of quantum states in the (quantum) channel between sender and receiver, and until they are measured they do not have certain values. Here, quantum states refer to being in a superposition of all logic bit values and the values of logic bits are assigned with the operation of measurement. As a quantum channel, single particle quantum states in superposition or entangled particles can be used. In QC, non-orthogonal states or non-orthogonal basis sets each of which is composed of two basis is used for encryption/decryption. Quantum key distribution (QKD) protocols can be divided into various categories based on different perspectives, for example either prepare-and-measure (PAM) or entanglement-based (EB) QKD protocols, either discrete-variable (DV) or continuous-variable (CV) QKD protocols etc. In PAM QKD, there is a well-defined sender and receiver which are legitimate communicating parties. Sender encodes, receiver decodes. This is the original scheme on which QKD protocols are based. However, in EB QKD, all communicating parties can be receivers, even if an entanglement source is owned by a communicating party. Even, an entanglement distributing node may not be seen as a trusted node. In DV QKD, one works with single photons and avalanche photodiodes operated in Geiger mode for their detection and the degree of freedom in which information is encoded takes finite number of values. On the other hand, in CV QKD, one works with photodiodes operated in linear mode so works with photocurrent proportional to the power of incoming laser and in parallel to that the degree of freedom takes infinite number of values. While the advantage of using DV QKD over CV QKD is that achievable distances would be higher, the advantage of CV QKD over DV QKD is that more information can be communicated. The research topics presented in this thesis are based on DV QKD systems, the topic discussed in Chap. 2 concerns both PAM and EB systems, and the topic discussed in Chap. 3 is related to an EB QKD system. There are a lot of QKD

protocols like BB84 (PAM), E91 (EB), BBM92 (EB), B92 (PAM), six-states (PAM), differential-phase-shift (DPS) (PAM), decoy state, SARG04, coherent one-way, high dimensional QKD protocols, device-independent (DI) (a modified version of E91 can be a DI QKD [17] and different versions of other protocols may be regarded as DI QKD if some requirements are satisfied [18]) and measurement-device-independent (MDI) QKD protocols. Summary descriptions of some protocols can be found in the following paragraphs.

In BB84 [19] (PAM QKD) which is the first QKD protocol, two non-orthogonal basis sets, each of which comprised of two orthogonal basis, are used in encryption/decryption. The basis positioned along the direction of 0° and 90° represent bit 0 and bit 1, respectively, and this is called rectilinear basis set. The basis positioned along the direction of $+45^\circ$ and -45° represent bit 0 and bit 1, respectively, and this is called diagonal basis set. Information is encoded into polarization degree of freedom. Sender, Alice, encodes each bit taken from a random bit string, which is generated by a quantum random number generator source, into a polarization direction by using basis sets chosen randomly. Thus, for bit 0, there are two possibilities of polarization directions, either 0° or 45°. As the information is encoded into photons, they are sent to receiver, Bob. He randomly chooses a basis set for each incoming photon, measures them and obtains a logic bit. All the bits at a communicating side are called raw key bit string. Then, the encoding and decoding basis sets are compared for all the bits among Alice and Bob. While the results of the same basis sets are preserved for formation of key bit string, the results of different basis sets are discarded because of being in a random bit value. In this stage, the bit string is called sifted raw key bit string. From now on, all the bits are expected to be in the same value among Alice and Bob except a portion of them corresponds to an error rate which is caused by trusted error sources. In order to test the channel security between Alice and Bob and to compute the error rate, which is called quantum error rate (QBER), they

choose some bits randomly and compare the bit values. The ratio of the number of mismatched values to the total number of bits in the substring gives the QBER. An intercept-resend attack can be performed by an eavesdropper, Eve. Eve gets the quantum states send by Alice and prepares another ones to send to Bob. Eve has 25% probability of introducing an error in the values of bits which will be obtained by Bob. This is the value introduced by the attacker, but a value below this one and above the expected error rate caused by trusted error sources can also be chosen as a threshold. If the QBER is higher than the threshold, the protocol is aborted. If it is below the threshold, then remaining bit string is called secret key bit string and has enough secrecy to continue with privacy amplification and error correction stages.

In E91 protocol [20] (EB QKD), Alice can be called a sender if she bears source or can be called a receiver like Bob because particles will also be distributed to her and measured at her side. In this protocol, electrons and their spin angular momentum is assumed to be the degree of freedom for encoding. A source emits pairs of spin-1/2 particles in singlet state and each particle of a pair is distributed to Alice and Bob. For each incoming particle, a (Stern-Gerlach) measurement is performed via analyzers in the orientation of one of the non-orthogonal states $0°$, $45°$, $90°$ at Alice's side and $45°$, $90°$, $135°$ at Bob's side by choosing randomly. The result of each measurement is either $+\hbar/2$ or $-\hbar/2$ representing spin-up or spin-down states, is taken as $+1$ or -1 corresponding to bit 0 or bit 1. Since each particle of a pair has correlation in-between, a correlation coefficient, S, is defined based on the measurement results, which tests whether they still bear the original correlation before measurement. S is computed over the measurement results. S is an inequality and there is a boundary for the value of S. According to which side of the inequality S takes a value, Alice and Bob understand whether the quantum correlation is preserved and communication system has enough secrecy to continue. The details of the correlation coefficient is explained in Chap. 3. Lastly, in the experiments of E91 protocol, photons are used as opposed

to electrons in this original version.

In BBM92 protocol [21] (EB QKD), singlet states composed of spin-1/2 particles are assumed to be used as a quantum channel because it is explained based on the original version of E91 protocol. Measurement states are 0° and 90° at both Alice's and Bob's sides. One of them is chosen randomly for each incoming particle and either $+1$ or -1 is obtained as the result of a measurement. They prove that since the particles are correlated, measurement results in the same measurement states among Alice and Bob will be correlated and no need to an additional inequality, as used in E91, in order to test the secrecy. (Also, to note that in the experiments of BBM92 protocol, photons are used instead of electrons like the implementations of E91 protocol.) Namely, it may be inferred that secure key distribution is also possible using less resources on the measurement side.

In an application of B92 protocol [22], Alice uses any two non-orthogonal states for the encryption, for example 0° and 45°, which correspond to bit 0 and bit 1, respectively. Bob uses two states, each of which is orthogonal to a state at Alice's side, for example 90° and 135°, which correspond to bit 1 and bit 0, respectively. Whenever a photon sent by Alice can be detected at Bob's side, its value will be the same for both Alice and Bob. Its application can be considered by using the polarization degree of freedom of photons and polarization analyzers for all possible combinations of sender and receiver. Here, there is no publicly announcement of states as in BB84, E91 and BBM92 and there is only the comparison of a subset of measurement results to compute QBER. Additionally, since this is a PAM QKD protocol and two states are used at each side, the error rate which will be introduced by an eavesdropper in an intercept resend attack will be 25%. This protocol presents flexibility in choosing of encoding states depending on the physical channel characteristics for experimental implementations.

DPS protocol [23] is a simplified version of a different application of B92 protocol

[22] in which two unbalanced Mach-Zehnder interferometers (MZIs) are used, one is at Alice's side, the other one is at Bob's side in a PAM QKD configuration. This application can also be referred to as conventional B92 in the literature. Unbalance is seen in the beam splitting ratios of beam splitters (BSs) and in the path lengths of two arms of interferometers. At Alice's side, the unbalance in the BS enables to generate single photons from bright pulses. In the short arm of the MZI (at Alice's side), a phase shifter randomly switches between two values, and generates phase encoded single photon states. A bright pulse follows a single photon in the quantum channel between Alice and Bob and is used for security purposes. At Bob's side, the function of the MZI is to generate two phase difference values in the interfered single photon states. Each phase difference corresponds to a bit value. On the other hand, in DPS protocol, at Alice's side, there is a phase modulator in front of a coherent light source followed by an optical attenuator and as a result phase encoded single photon states are generated. At Bob's side, there are two unbalanced couplers in the interferometric configuration presents different length arms without any phase shifter. With this design, two possible phase difference values are produced for the two photons that will interfere, only through the difference in path lengths. Thus, DPS is a simplified version of the B92 and is interpreted differently in security aspects.

QC presents information-theoretically unconditional security, however, experimental implementations cause imperfections and can generate security loopholes. There are several types of attacks exploiting different vulnerabilities of QKD systems in the literature. The types of attacks are as follows: individual attacks, collective attacks, coherent attacks and incoherent attacks. In an individual attack, an eavesdropper measures all the quantum states during their distribution between legitimate communicating sides. According to her attack strategy, she may not prepare a quantum state (like in photon-number-splitting attack which will be mentioned below), may

try to prepare the original state (like in intercept-resend attack which will be mentioned below) or may prepare a different state (like in faked-states attack which will be mentioned below) to send to Bob. In a collective attack, eavesdropper has ancilla states interacting with the quantum states distributing to legitimate communicating side(s), she does not measure her ancillas during the distribution, she stores them to her memory unit. She listens to the measurement basis sets shared in public channel by Bob and/or Alice and applies the optimal measurement or the same measurement basis sets with the legitimate communicating side(s) globally. This type of attack is not realized because the required timescales to maintain the original quantum states in memory devices have not been achieved yet [24]. In a coherent attack, eavesdropper has a single ancilla state represented by any dimensional Hilbert space [25] and interacting with all the quantum states distributed between Alice and Bob. It can be the interactions of mutually dependent modes of the single ancilla with the quantum states [26] and hereby there can be more correlations which will be utilized by Eve. It offers more powerful attacks than collective attacks to an eavesdropper. In an incoherent attack, eavesdropper attacks with an external light source and incoherent signals, which can be based on various strategies. Other than the generalized attack types as mentioned above, specific attacks can be listed as photon-number-splitting attack, intercept-resend attack, faked-state attack, man-in-the-middle attack, trojan horse attack, time-shift attack, detector blinding attack, large pulse attack etc. and some of them are mentioned in the following paragraphs.

Photon-number-splitting attack (PNS) [27] is caused by the absence of real single photon sources. As a representative, low-intensity coherent pulses are used. Actual number of photons in a pulse follows Poisson statistics and can change around an average number of photons. When the actual number of photons is higher than one, photon content can be divided into two outputs by an eavesdropper: one for a legitimate receiver side and one for the eavesdropper. In this way, she can have the

exact quantum states that are send by Alice to Bob in a PAM QKD configuration.

In intercept-resend attack [28], Eve gets all the single photons send by Alice to herself, she measures incoming signals by projecting onto randomly chosen states. Then, she encodes the measurement results to the same states that she used in the measurement and sends them to Bob. She tries to prepare the same states send by Alice. This is a system vulnerability based on Eve's interception ability.

In faked-state attack [29], intercept-resend is an intermediate stage. As a general scheme, Eve gets a photon sent by Alice by intercepting the quantum channel, notes measurement basis set in which the photon is measured, prepares a quantum state not necessarily in the original state send by Alice and sends it to Bob. Moreover, Eve determines the basis set in which the photon will be measured and the result of the measurement at Bob's side. In this way, QBER does not become as high as in intercept-resend attack. This scheme could be applied to various QKD systems. For example, in a DPS QKD system there are only two phase values representative of two non-orthogonal states and correspond to two bit values. Phase detectors are used. Eve prepares quantum states having certain phase values and sends to Bob. She determines the measurement result to be obtained at Bob's side by interfering the quantum states she prepared. This attack can lead a decrease in the detection probability of Bob but may be compensated by increasing the power of faked-states.

Time-shift attack [30] is based on detectors' profiles not overlapping in time completely. Detectors having the same response profile but a time shift or detectors having different response profiles without a time shift can cause a security gap because of having different quantum detection efficiencies at various times. There are various attacks based on different scenarios, for example, Eve can send faked-states to Bob by introducing a delay or she can shift original states send by Alice in time. In both cases and in a time-multiplexed detection scheme with the usage of a single detector, the bit value which will be obtained by Bob is determined according to the

arrival time of photon chosen by Eve. Or in a detection scheme in which two detectors are employed, Eve can introduce a delay into the original quantum signal that Alice sends or the gate signal that actives a gated mode detector at Bob's side if these types of detectors and synchronization signals are used. Eve aims the times that both detectors either do not response at the same time or do have different efficiencies in order to access the bit values related to quantum signals.

In detector blinding attack [31], in a DPS QKD system Eve gets the photons send by Alice, measures them and obtains a phase (bit) value. In this case, Eve encodes quantum states into bright pulses instead of single photons. The interference designed by Eve is observed at Bob's side with a higher detection probability compared to faked-states attack and with higher success probability of Eve because of the amplitude of the bright pulses compared to single photons. Detector cannot see single photons and reacts to bright pulses inevitably. The name blinding comes from the detector clicking corresponds to linear mode operation instead of Geiger mode.

All the communication networks require time synchronization to perform data processing and integration precisely. One way to synchronize communication nodes is to use clock signals [32] to be transmitted from one node to another. Approximately, $9 \cdot 10^9$ transitions of a caesium-133 atom between two hyperfine levels of its ground state per second is defined as absolute time. The implementation of it at a node is an oscillator, which is associated with a clock rate. Time synchronization can be affected by various reasons. For example, in the node implementation, real clock rate can differ from ideal clock rate with certain error bounds. The accumulation of errors occurred in the transitions, which is referred to as clock drift, can affect time synchronization. As well as the generation of clock signals, there can be imperfections in their transmissions like the reasons caused by the specifications of intermediary apparatus like electrical to fiber optical converters and vice versa, long-distance fiber

channels or wavelength division multiplexing systems etc. Also, the motion of communicating side(s) and Doppler effect in the frequency of signals being transmitted and received [33] can be another reason. All of them cause time jitter in clock signals, which are evaluated in three ways: period jitter, cycle-to-cycle jitter and phase jitter. Additionally, converters between analog and digital signals, function generators etc. contribute to the total jitter budget of a network. These parameters become important in quantifying system security, in determining data rate and maximum tolerable distance in case of a long-distance communication. In addition to the clock signals' jitter, detectors used in the key generation also have time jitter in their responses. All these can cause imperfect time synchronization in QKD systems where the time synchronization is of the greatest importance.

In addition to QKD protocols, there are also post quantum cryptography protocols [34, 35, 36, 37, 38, 39] in which there is a large volume of work studied. All in all, (post) QC can solve cybersecurity problems against quantum computer attacks. However, it is not correct to assume that a system is secure because of employing quantum cryptography without analyzing the system rigorously and optimizing parameters according to the physical system characteristics as seen in the previous paragraphs, otherwise major security loopholes may exist. Therefore, this thesis has been devoted to the improvement of QC ecosystem in terms of security and communication speed as discussed in the following paragraphs.

In order for the deployment of quantum communication technologies in a global scale, it is necessary to meet data exchange demand of various size establishments per certain time intervals. At the same time, it is important to make them cost effective and feasible. In order to meet these requirements, a lot of effort has been put into increasing key rate and having optimized systems. They can be achieved in different ways, for example, presenting a method based on consuming less resources for a constant throughput or by increasing the amount of information communicated

per unit time or by obtaining the highest rank key rate in the same conditions or by inventing a method that allows more users to communicate etc. The following three protocols are the examples of it.

In 2020, in a QKD system [40] which implements BBM92 protocol, 300bps key rate after error correction and privacy amplification was achieved at 143km atmospheric free-space link between two Canary islands La Palma and Tenerife characterized by a certain loss. It beated its preceded experiment (24bps in BBM92 protocol implementation in the same link [41]) done in 2009 with 92% improvement in the key rate by developing a higher brightness entanglement source.

In order to increase communication distance and improve key rate in conventional QKD systems, MDI QKD is created in 2012. Distance achieved in PAM QKD protocols is doubled by changing the protocol topology [42]. Shortly, Alice and Bob became transmitters and send quantum states to be measured to a third party. A transmitter unit consists of a weak coherent pulse source, a polarization modulator and an intensity modulator (IM). By means of an IM, a transmitter sends decoy states (randomly chosen intensity levels among certain values) having certain polarization values (one of the basis of either rectilinear basis set or diagonal basis set for each state) to Charlie which is not necessarily a trusted node. Charlie performs Bell state measurements in which two of four Bell states can be obtained (either $(|HV\rangle - |VH\rangle)/\sqrt{2}$ or $(|HV\rangle + |VH\rangle)/\sqrt{2}$) and can be used for key generation. According to Charlie's announcement of the measurement result, they eliminate bits encoded to quantum states and preserves the ones which resulted in successful measurements. Then, they announce intensity levels and basis sets correspond to the polarization states used in encoding for the successful measurements via a classical channel. They eliminate bits end up with unmatched basis sets. They use the same basis sets for key generation. The intensity values are used in the control of probability of obtaining each type of measurement result. They choose a subset of measurement results to compute QBER,

which has certain values for the pairs of intensity levels and polarization values used by Alice and Bob. Their reference for the QBERs are the expected QBER values which had been calculated during channel characterization. If QBERs are not higher than the expected values, either Alice or Bob flips the bit values in her or his ownership in order to obtain a raw key bit string. As a result, the usage of decoy states contributes to the increase of communication distance and makes the QKD system more robust to PNS attacks. Also, when MDI QKD protocol is implemented, system vulnerabilities caused by detector imperfections and side channel attacks based on this are eliminated. For this reason, MDI QKD protocol with its various variants like MDI QKD employing entangled state distribution from transmitters and performing entanglement swapping at the third node, MDI QKD based on phase-encoding [43], time-bin phase-encoding [44] or twin-field [45] protocols are in demand currently.

A study [46] published in 2021 optimizes four-intensity MDI QKD protocol [47] proposed in 2016 by defining new constraints and a new method called double-parameter scanning applied in data processing. Here, decoy states are employed and the protocol is applicable for polarization, phase or time-bin encoding schemes. They apply global optimization technique which includes all the parameters from transmitter side properties to secret key rate calculation obtained after error correction. Also, they examine symmetric and asymmetric quantum channels, in which the intensities and their probabilities to be chosen can be the same or different among Alice and Bob. Ultimately, they show that key rate can be improved between 35% and 280% with certain adjustments.

There are two research topics carried out in the thesis. While one of them is about a security loophole, the other one is within the scope of key rate improvement studies. In the topic presented in Chap. 2, we focus on a security gap that arises in case of an imperfect time synchronization, which is called timing side channel. The result of an imperfect time synchronization is the time shift between detectors' responses used

for key generation. Also, the research that we focus on can be referred to as detector efficiency mismatch. The leakage information is quantified by the mutual information between a legitimate communicating side and an eavesdropper about a key bit value. And a solution to this problem is to make binning on timing information revealed in a classical channel. In the literature [1], for a time difference between two detectors, the mutual information is examined for two time bin values. We believed that this is not sufficient and made a detailed analysis of this side channel by examining the mutual information for a wide range of time bin width values. Additionally, we present a characteristic of the mutual information and also showed the dependence of the mutual information to the uncertainty of a detector response. We challenge the recognized solution, binning, to this problem with our findings. This problem can exist in a wide range of applications because it is valid for both PAM and EB QKD systems. In the topic presented in Chap. 3, we make optimization in an EB QKD system and our objective is to obtain higher key rates than its standard configuration. There are three types of bits in the system which are key bits, Bell's inequality bits, which are used to quantify the security of the system, and discarded bits. In the quantification of security, we use Bell's inequality and base the security on the violation of it. In the standard configuration of the QKD system, a photon budget is allocated in the ratios of 25%, 50%, and 25% occur for three type of bits, respectively, for a given photon budget. These ratios are not optimum, they are required to be optimised and the system should be made operated with a higher performance. So that a proof-of-principle experiment would be more convenient for field implementations. And we study for its optimization by maximizing the ratio of key bits in order to maximize key rate. Lastly, in Chap. 4 we summarize the two topics studied in the thesis, rephrase what has been done in the literature and our findings comparatively, and our contributions to the literature.

CHAPTER II

TIMING SIDE CHANNEL ANALYSIS

2.1 Introduction

General scheme of QKD protocols [20, 19] are well known, their security proofs [48, 49, 50, 51, 52], side channels of QKD systems [53, 54, 55, 56, 57, 58, 59], and side channel attacks [60, 61, 62, 63, 64, 65, 66, 67, 68, 30, 69] are widely studied topics. In this chapter, we study timing side channel which can also be referred as detector efficiency mismatch [53, 30, 60].

Before starting a QKD protocol, detection modules need to be characterized. The characterization involves time synchronization between authorized communicating parties. Time synchronization involves determining the path differences between different receivers to the transmitter, and then compensating of these path differences physically or digitally (as a post-process). Path differences in a QKD experimental setup are represented in terms of time differences between detectors' responses. During QKD, two communicating parties share the basis set in which a photon detection is realized and the timestamp of this event via a classical channel to determine the coincidences, to generate raw key bits and to compute the quantum bit error rate and/or the amount of violation of Bell's inequality depending on the protocol followed. The timestamps of the events are important in order to determine the coincidences correctly. When the time synchronization is not perfect but realized up to a precision, the coincidences can still be determined correctly, however, a timing side channel attack can occur within that precision. An eavesdropper can estimate the raw key bits, which are required to be kept secret, by simply observing the timestamps and the relative delay between coincidence events in the same basis set. In

other words, non-overlapping coincidences in time domain make the values of raw key bits predictable for the eavesdropper. In summary, timing side channel can be understood as the exploitable correlation between the timestamps and the measurement results obtained from quantum channel. Measurement results carry the bit content and therefore the security is relied on them.

In the literature, a recognized solution to this problem is to minimize eavesdropper's information by increasing time bin width for the publicly shared detection times [1]. And only two values of time bin width are examined. However, in this study we examine a range of bin width values and show that arbitrarily increasing the bin width does not necessarily mitigate timing side channel attacks. Instead, the bin width should be carefully chosen depending on the delay between the coincidences.

In this chapter, we analyse the timing side channel of a QKD system with imperfect time synchronization.

The chapter is organized as follows; a detailed analysis of the mutual information is discussed in Sec. 2.2, two important parameters in the mutual information, start time of binning and the full width half maximum (FWHM) of detector response, are discussed in Secs. 2.3 and 2.4, respectively. In the continuation, an experimental method to put a time shift between detectors' responses is introduced in Sec. 2.5, the reason behind the time shift is explained in Sec. 2.6 and important findings are summarized in the last paragraph of the chapter.

2.2 Mutual Information

In an EB QKD system, two communicating parties Alice and Bob measure incoming photons in their detection modules to obtain raw key bits. A detection module involves a number of non commuting basis sets. A property represented by a discrete variable of the incoming photon is measured in one of non commuting basis sets. For example, the polarization of a photon is measured in one of the detector sets dedicated

to $(0°, 90°)$ and $(-45°, 45°)$ polarization measurements and a bit is obtained. To note that, $(0°, 90°)$ constitutes a basis set and each of the two orientations, $0°$ and $90°$, carries a bit content. If entangled photon pairs traveling to Alice's and Bob's detection modules are measured in the same basis set, the measurement outcomes are used as raw key bits. For each pair of bits, it is considered that whether they are raw key bits, violation of Bell's inequality bits or discarded bits according to coincided basis sets among communicating parties. Similarly, in a PaM QKD system the scenario is similar but the measurement outcomes obtained from all the basis sets are used as raw key bits as long as Alice's and Bob's basis sets are matching. Again, the measurement basis sets or bases and timestamps are publicly shared in these systems, which makes PaM protocols also vulnerable against timing side channel attacks. Because any time difference between coincidences obtained from the same basis sets makes those bit contents distinguishable. For the clarity of content, we will continue with the EB QKD protocol. However, the calculations are valid and can be repeated for PaM protocols also.

In QKD protocols single photon avalanche diodes (SPADs) are commonly used for detection of photons. For an incident photon, an SPAD outputs a Transistor-Transistor Logic (TTL) signal to create a register having the detection time. There is a time difference between the time that photons falls onto the active area of the SPAD and the generation of a TTL signal. This time difference is a distribution rather than a constant value. This timing histogram is called timing jitter or simply detector response. As the model of a detector response, we work with Eq. (3) [1], which is an exponentially modified Gaussian distribution

$$d(t) = \frac{1}{2\tau_e} e^{-\frac{\tau_G}{4\tau_e^2}} \cdot e^{\frac{t-t_0}{\tau_e}} erfc(\frac{t-t_0}{\tau_G}), \tag{3}$$

where '$\cdot$' is convolution product, τ_e and τ_G are model parameters and the peak density of $d(t)$ is observed at $t = t_0$. The values for a reference detector are $\tau_e = 400$ps, $\tau_G = 290$ps and $t_0 = 1000$ps. A second detector also has the same parameters except

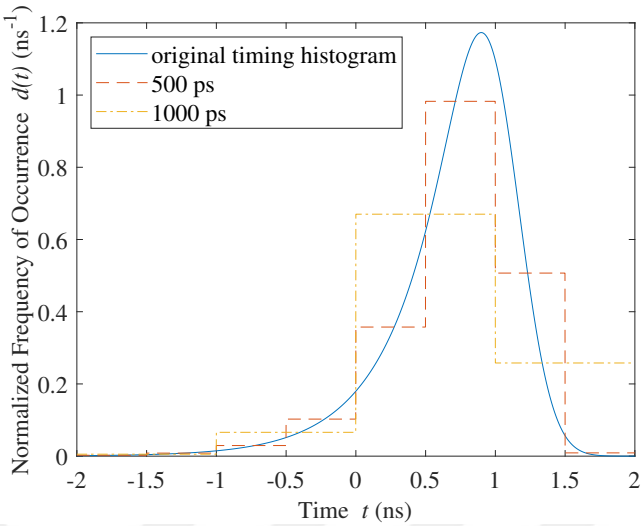


Figure 1: The graph of normalized frequency of occurrence dependence to time. Blue curve is the original timing histogram of the detector, red and yellow curves are the binned versions of the original histogram, and legend represents bin width values.

for t_0. By changing the value of t_0 for the second detector, a Δt_0 time difference between the two detectors is generated. The modeling of a detector response with an exponentially modified Gaussian function is common. In Eq. (3), we just use a certain function of this kind, and for the second detector, we shift its peak intensity position over time. The profile of the reference detector is the blue curve in Fig. 1. In Fig. 1, the y-axis represents the normalized frequency of occurrence, which is equivalent to the probability density for the original timing histogram.

Since there are two detectors dedicated to the measurement of raw key bits in one basis set, there are also two different paths a photon can traverse. Each path contains an optical path plus a distance from the start to the peak position of detector response. In the most general case, Δt_0 is the timing difference between two detectors due to optical path distances which may be caused by the motion of communicating side(s), electrical delays, thermal fluctuations in the system etc., and must be monitored and adjusted constantly. In Fig. 2(a), it is shown as only an extra optical path for the visualization. For example, if the raw key bit detection parts of the detection

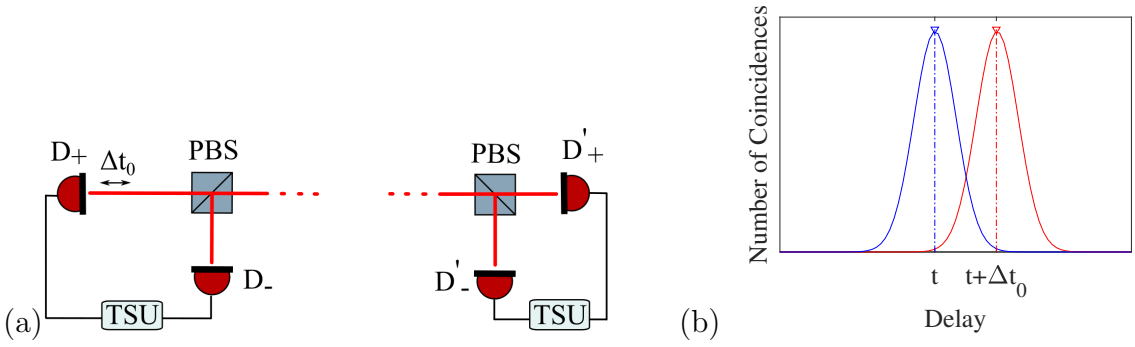


Figure 2: (a) Schematic representation of the detectors in the same basis sets at Alice's (left) and Bob's (right) sides. PBS is polarizing beam splitter. D_+ (D'_+) and D_- (D'_-) are detectors in the transmitted and reflected outputs, respectively. TSU is timestamp unit. Δt_0 is extra optical path. (b) The cross correlogram of coincidence events between Alice and Bob. t is the time difference between D_- and D'_-, $t + \Delta t_0$ is the time difference between D_+ and D'_+. Since there is an extra optical path, there are two separate peaks in the cross correlogram.

modules at Alice's and Bob's sides are represented schematically as in Fig. 2(a), the photon that goes to D_+ travels more than the one goes to D_-. If the entangled state in the quantum channel between Alice and Bob is $(|00\rangle + |11\rangle)/\sqrt{2}$, then the coincidence events coming from the detectors D_+ and D'_+, and D_- and D'_- are seen as separate peaks in a cross-correlogram as shown in the sketch in Fig. 2(b). The existence of this time difference will cause information leakage to an eavesdropper. This information leakage is quantified with mutual information which is a measure of the eavesdropper's information gain about key bit value [70, 71]. The source of the mutual information can be explained as follows. A detector generates an output signal for each photon it detects. In the QKD system, a basis set composed of two detectors. Depending on the position of a detector, every single pulse coming from this detector represents the same bit value. Likewise, a timing histogram is related to a bit value. When the timing histograms of two detectors do not overlap completely, they become distinguishable and bit values become predictable.

Time bin is the unit time interval used in a QKD system. In every time bin, a measurement may be performed in detection modules, and if there is a measurement,

one bit of information contributing to a bit string may be obtained. Time bin width determines the precision of timing histograms and the precision of timestamp information revealed via classical channel by communicating parties. However, there are processes which are binning for discrete time signals and quantization for continuous time signals. In binning process, the value of bin width is redetermined and representative values for normalized frequency of occurrences falling into each time bin are regenerated. In our study, we work with discrete time signals, namely quantized continuous time signals, and we apply the binning process on them. As an example to binning process, in Fig. 1 the red and yellow curves are the binned versions of the original timing histogram. The bin width is 500ps in the red curve and 1000ps in the yellow curve.

A timing histogram may be considered as having two regions, the region which corresponds to the observation of a photon and the region in which distribution is almost zero. During a binning process, required time interval may involve the region in which distribution is almost zero but must involve the region which corresponds to the observation of a photon. The required time interval, at most, must be the sum of these two regions. If it is needed to show these regions on a graph, although there is no a strict boundary between the regions, in Fig. 3 from -4ns to 4ns can be considered as the region where the photons are observed and from -13ns to -4ns can be considered as the region where the distributions are almost zero.

The formula used to find a required time interval is given in Eq. (5).

$$number\,of\,bins \geq \frac{time\,interval\,for\,a\,photon\,observation}{bin\,width} \tag{4}$$

$$required\,time\,interval = number\,of\,bins \cdot bin\,width \tag{5}$$

where *number of bins* is the minimum integer value that satisfies the inequality given in Eq. (4) and all the terms used in the formula were introduced in the previous

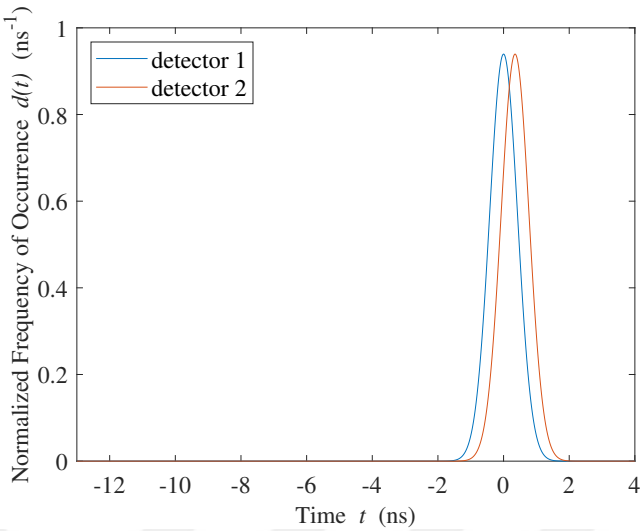


Figure 3: The timing histograms of two detectors having a time difference in-between. The regions of the timing histograms are as follows. From -4ns to 4ns is the region where the photons are observed and from -13ns to -4ns is the region where the timing histograms are almost zero.

Table 1: The pairs of bin width and required time interval which should exist in the timing histogram of a detector.

Bin Width (ps)	Required Time Interval (ps)
2	5000
248	5208
2120	6360
2500	5000
3500	7000
4998	9996
5000	5000

paragraph.

Required time interval for a bin width may vary since all the bins must have the same width in the binning process. Some of the pairs of bin width and required time interval can be seen in Table 1. In order to make binning on a timing histogram, the timing histogram should involve the required time interval related to the bin width which will be used in the binning process. Hence a timing histogram is generated for the required time interval before a binning process is applied on it.

In the literature, it is known that binning process with large bin width value

reduces the mutual information; however, in this study we show that not every increment of the value of bin width gives a reduction in the mutual information. Instead, there is a fluctuation behaviour which is explained in the rest of the chapter.

The mutual information $I(X;T)$ between the raw key bit values and detection times can be expressed as in Eq. (6).

$$\begin{aligned} I(X;T) &= \sum_x \int p(x,t) \log_2 \left[\frac{p(x,t)}{p(x)p(t)} \right] \mathrm{d}t \\ &= \sum_x \int p(x)p(t \mid x) \log_2 \left[\frac{p(t \mid x)}{p(t)} \right] \mathrm{d}t \\ &= \sum_x \int p^0(x) d_x(t) \log_2 \left[\frac{d_x(t)}{\bar{d}(t)} \right] \mathrm{d}t \\ = \sum_x p^0(x) \int d_x(t) \log_2 d_x(t) \mathrm{d}t &- \int \bar{d}(t) \log_2 \bar{d}(t) \, \mathrm{d}t \end{aligned} \tag{6}$$

where the first line follows from definition of mutual information and the third from substituting the relevant distributions. Namely, $p^0(x)$ is the probability mass function of the symmetric Bernoulli random variable x. $d_x(t)$ is the probability density of taking a click at time t given x. For example, $d_0(t)$ is the probability of taking a click for 0 at time t. Therefore, $d_0(t)$ and $d_1(t)$ are the detectors' responses of detectors dedicated to obtaining 0 and 1, respectively. $d_0(t)$ and $d_1(t)$ differ by Δt_0 as described above. Namely, while the peak density of $d_0(t)$ is positioned at t_0, the peak density of $d_1(t)$ is positioned at $t_0 + \Delta t_0$. $\bar{d}(t)$ is the probability density of taking a click at time t from an ensemble of detectors. The last step follows from algebraic manipulations and substituting Eq. (7).

$$\bar{d}(t) = \sum_x p^0(x) d_x(t) \tag{7}$$

Mutual information is computed for various Δt_0 values and it fluctuates as shown in Fig. 4 with varying bin width values. For each bin width value, binning is started at the same point of the original timing histogram so there is no phase difference between the binning processes. Bin width of 0.5ns and 1ns as the evaluation points

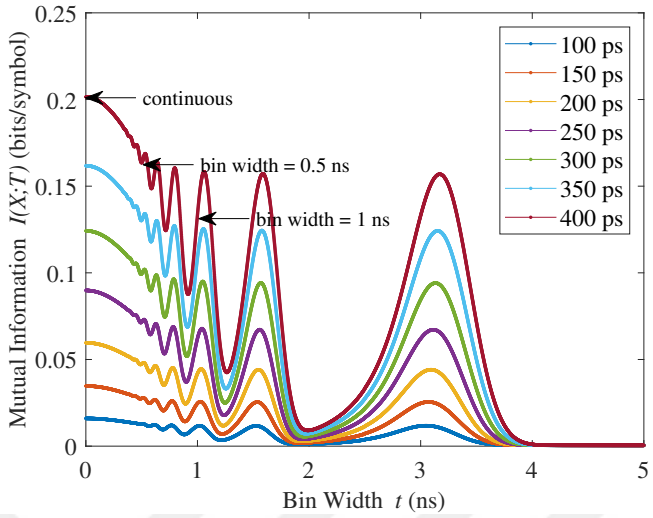


Figure 4: The graph of the mutual information dependence to the bin width and Δt_0. Legend represents Δt_0 values. Bin width of 0.5ns and 1ns shown on $\Delta t_0 = 400$ps curve are the evaluation points on the continuous time signal in [1].

on the continuous time signal in [1] are shown on the $\Delta t_0 = 400$ps (upper most) curve in Fig. 4 for comparison. The fluctuating behaviour of mutual information with increasing bin width indicates that a combination of bin width and Δt_0 should be chosen carefully to minimize the mutual information.

Since the mutual information is an entropic quantity, its unit is bits/symbol. Here, the term symbol is related to a symbol in constellation diagrams used in digital modulation schemes. For our protocol, each symbol physically represents a photon, carries one bit of information and is represented by a bit, 0 or 1. For bigger constellation sizes or higher dimensional QKD systems, a symbol carries more than one bit of information and represented accordingly. For example, for a constellation diagram having four symbols, each symbol is represented by two bits, 00, 01, 10 or 11.

2.3 Start Time of Binning

The index of the time bin at which a photon detection event is registered depends on the start time of binning as well as the bin width. Mutual information changes according to the start time of binning, it is periodic with respect to it for a constant

bin width value and the period is equal to the bin width itself. As a result, the start time of binning is also very critical for QKD security. In order to model this behaviour, we use Gaussian distribution which is a good approximation for timing histograms of two detectors from now on. For illustrating the effect of the start time of binning on the mutual information we considered the following values: Δt_0 is taken as 350ps (the mean (μ) of Gaussian distribution for a detector is 0ps, the mean of Gaussian distribution for a second detector is 350ps) and the FWHMs of detectors' responses are taken as 1ns. The timing histograms of the two detectors can be seen in Fig. 3. For these timing histograms, in Fig. 5, mutual information is computed for five values of bin width, which are 1ps, 1ns, 2ns, 3ns and 4ns. In the figure, the periodicity of mutual information can be seen explicitly. For example, if we look at 4ns (green) curve, the peak value seen around 12.3ns repeats itself at around 8.3ns. Time difference between the two peak values are exactly equal to the amount of time bin width value. In Fig. 3, the two detectors are plotted for the time interval of -13ns and 4ns. Since binning process must contain the observation of a photon, start time of binning starts from -13ns and ends at -5ns for Fig. 5 because significant values of the timing histogram related to a photon observation starts after around -4ns. Moreover, the periodicity of the binned version of the timing histogram of the detector having $\mu = 0$ps can also be seen in Fig. 6. In the figure, the binned versions are plotted for a constant bin width.

In Fig. 7, the mutual information is calculated for bin width values ranging from 0 to 4ns. In all the mutual information calculations related to different values of bin width, the phase at the start is 0 and after one bin width the phase becomes 2π. Instead of showing the start time of binning as an axis in Fig. 7, we chose the phase because of being a better indicator of periodicity, and in order to show the periodicity obviously, the phase is chosen from 0 to 4π. This graph shows that even carefully chosen bin width is not sufficient for QKD security as the start timing of binning also

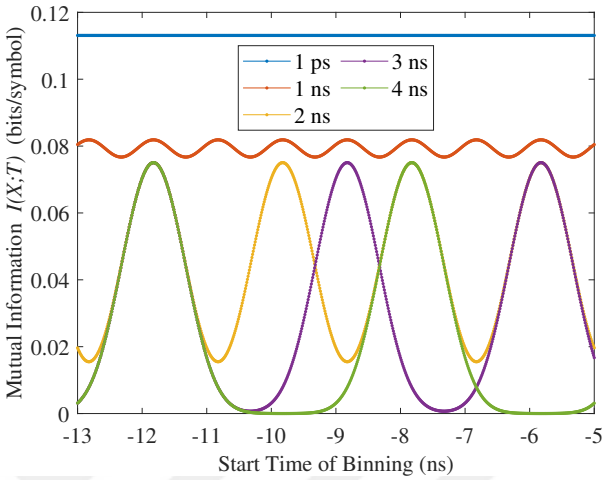


Figure 5: The graph of the mutual information dependence to the start time of binning. Legend represents bin width.

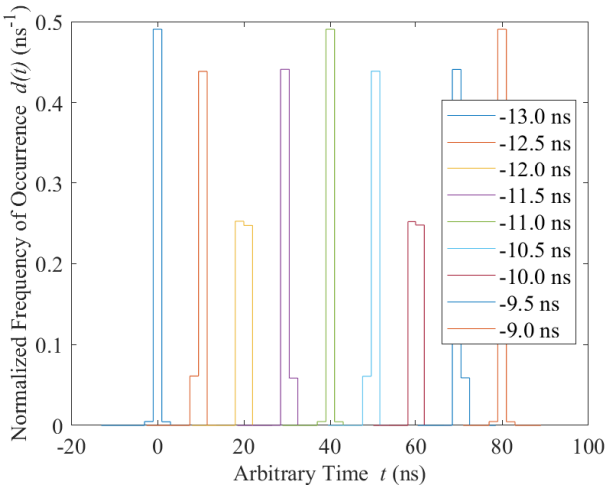


Figure 6: The binned version of the detector having $\mu = 0$ps which is seen in Fig. 3. Bin width = 2001ps. Legend represents start time of binning.

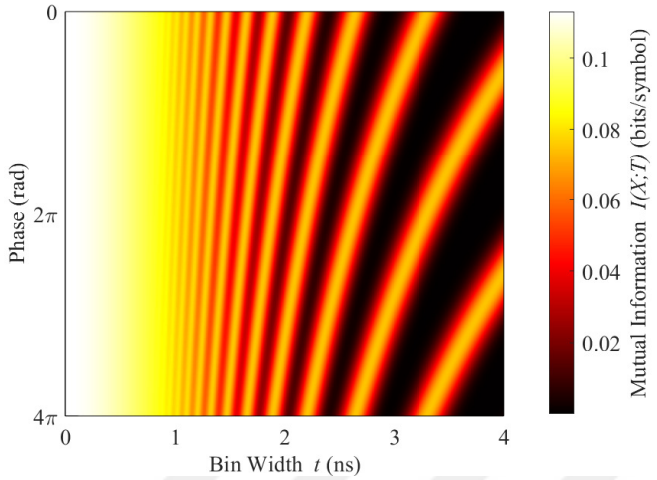


Figure 7: The graph of the mutual information dependence to the start time of binning. The start time of binning is represented in terms of phase. Color bar represents the mutual information.

Table 2: Some examples of FWHM of detector response in the QKD market.

Brand	Product	Time Jitter (FWHM)
Single Quantum	A typical SNSPD with a cryogenic amplifier	< 15ps [72]
IDQ	Superconducting Nanowire System (ID281)	$< 30 - 60$ps [73]
Hamamatsu	Silicon Photomultipliers	on the order of 100ps [74]
Qubitrium	SPADs	$1.5 - 2$ns, 3ns

plays a crucial role.

2.4 FWHM of Detector Response

In the QKD market, there is a variety of companies offering detectors having low time jitters, which are characterized by FWHMs, as products in order to allow high key rates in QKD implementations (as an example, some detectors and their time jitters can be seen in Tab. 2). On the other hand, for a constant Δt_0, when FWHMs of detectors' responses decrease, the overlap portion of their timing histograms decreases and their profiles become distinguishable as can be seen in Fig.8, and ultimately the mutual information increases. For this reason, detectors having low time jitters are more vulnerable to the timing side channel attack.

Fig. 9 shows the scan of FWHM of detector response and bin width values for

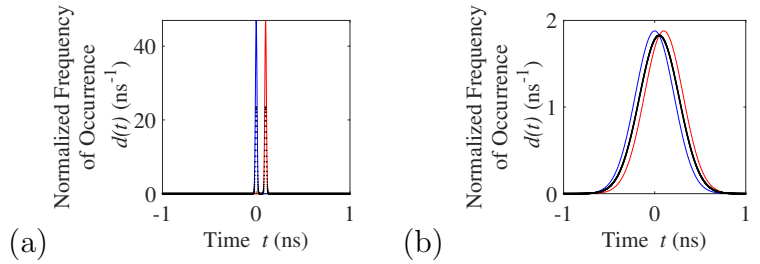


Figure 8: The effect of the FWHMs of detectors' responses having $\Delta t_0 = 100$ps on the distinguishability of the profiles and hence the values of coincidences. Blue and red curves are two detectors' responses. Black curve is the summation of them after multiplied by 0.5. The distinguishability of the two can be seen in the summation curve. (a) FWHMs = 20ps. (b) FWHMs = 500ps.

$\Delta t_0 = 350$ps. A constant start time of binning is used for varying bin width. It is very critical that when the FWHM of detector response is smaller than Δt_0, the mutual information is almost 1. This is a direct consequence of the fact that the coincidence peaks in the cross correlogram are almost completely distinguishable from the publicly shared timestamps and basis sets when the FWHM of detector response is smaller than Δt_0. The message that should be taken from this graph is that the FWHMs of detectors' responses should be negligible compared to Δt_0. More generally, the coincidence peaks in the cross correlogram should overlap as mush as possible. This can easily be arranged in a typical QKD setup by a careful physical adjustment of the distances from the PBS to the detectors, and using the detectors the same (or similar) FWHMs of the responses and/or electronic delays. However, an exhaustive search of ways to prevent a loophole in the security of the QKD system is required against an externally given delay to one of the coincidence curves as shown in Sec. 2.5.

The timing side channel mentioned in this work is due to the timestamp and basis set information sharing of Alice and Bob in the public channel. An alternative solution to this problem is that only Alice (Bob) shares the timestamp and basis set information in the public channel and Bob (Alice) checks for the distinguishability in the cross correlogram peaks of $+$ and $-$ coincidences. After the analysis, Bob

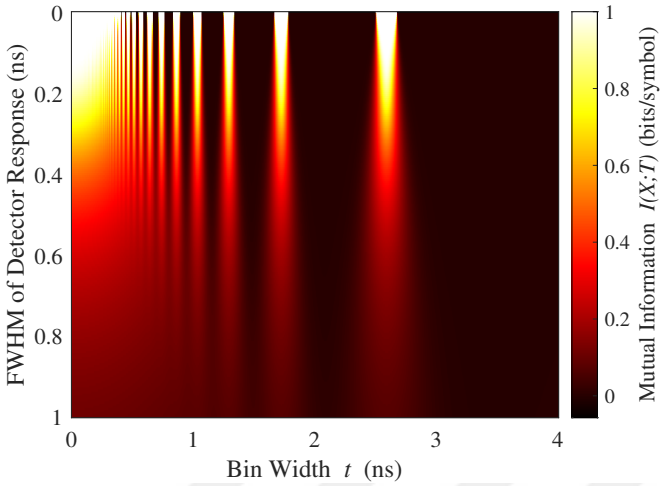


Figure 9: The graph of the mutual information dependence to the FWHMs of detectors' responses with varying bin width. Color bar represents the mutual information.

eliminates the offset delay in one of the detectors to make the cross correlogram peaks completely overlapping. After this compensation Bob can share his timestamp and basis set information with Alice in the public channel. In this way, the eavesdropper never learns about the relative delay in coincidences from different detector sets in a basis set. Also, measurement-device-independent schemes can be applied to eliminate this problem.

2.5 A Method to Introduce Time Shift Between Detectors' Responses

In this section, a method to introduce time shift between detectors' responses is explained. Experiment on which the method will be described and the study start with a beam profile having pump and down converted photons, however, for a complete description of the experimental setup, stage until the generation of the profile will be mentioned briefly.

For the purpose, a spontaneous parametric down conversion source (SPDC) is utilized which is shown in Fig. 10. A laser source emits vertically polarized collimated beam whose central wavelength is 405nm. The beam is passed through a band-pass

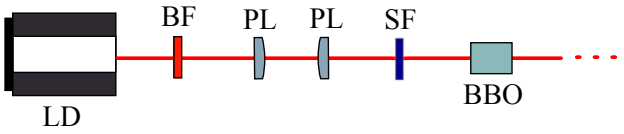


Figure 10: First part of the experimental setup shown in Fig. 12. LD is laser source. BF is band-pass filter. PLs are plano-convex lenses in a telescope configuration. SF is spatial filter. BBO is beta barium borate nonlinear crystal.

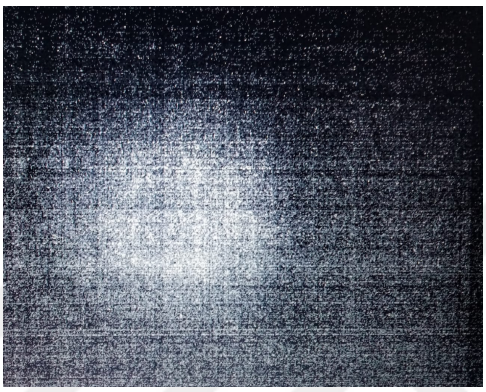


Figure 11: The beam profile having pump photons ($|V\rangle$) and down converted photons ($|HH\rangle$), which is obtained after the BBO crystal.

filter having 405±2nm central wavelength and 10±2nm FWHM of bandwidth in order to eliminate the unwanted wavelengths around the central wavelength. A telescope configuration composed of two plano-convex lenses is used to expand non-Gaussian beam profile and a spatial filter is used to take a relatively more uniform portion from the non-Gaussian profile. Then, the beam is passed through a nonlinear crystal whose cut angle is for type-I SPDC, and horizontally polarized down converted photons are generated.

The experiment continues with a beam profile having pump and down converted photons which is shown in Fig. 11 captured by a camera (Thorlabs Thorcam DCC1645C-HQ).

In Fig. 12, a long-pass filter having 750nm cut-on wavelength is used in order to block the pump beam. A dicroic mirror having 805nm cut-off wavelength separates the signal and idler beams whose wavelengths are 780nm and 842nm, respectively. At the reflected arm of the dicroic mirror, there is the signal beam and beam walk

is performed with the help of two mirrors for fine tuning while coupling them to a single mode fiber. Then, an aspheric lens focuses the collimated beam to single mode fiber launch. The fiber is connected to detector 1 (S-fifteen Instrument, SI-APD Visible Single Photon Detector) which outputs an electrical pulse in NIM logic family for a photon falls onto the active area of it. Timestamp unit (TSU) (qutools, quTAU time-to-digital converter) processes input signals in TTL logic family. Then, a NIM2TTL converter is required in-between to make the logic families compatible. At the transmitted arm of the dicroic mirror, the collimated idler beam is focused onto the active area of detector 2 (Excelitas Technologies, Single Photon Counting Module SPCM-AQRH-10) with the help of a plano-convex lens. TSU is connected to a software, which makes cross correlation of the two time series obtained from the detectors and generates the number of coincidences vs time graph, running on a personal computer (PC). From the graph, time difference between the detectors can be read. In the second stage of the experiment, white noise is injected to detector 2 at various amounts without saturating it with an external light source, and time shifts that occur between detectors' responses accordingly can be read from the same graph.

Initially, the time difference between the detectors is read from the cross correlogram and the number of photons observed by detector 2 per second is read from the (individual) count rates tab of the TSU software in the PC. The original cross correlogram obtained is shown in Fig. 13. Then, (white) noise is injected gradually, the cross correlogram depending on each noise injection is obtained and the total number of photons observed by detector 2 per second is obtained in each noise injection from the count rates tab. In the legend of the figure, the values seen are the total number of photons, namely the number of photons without noise injection, which is 120 K/s.

Figure 14 is generated from Fig. 13 and shows the amount of accumulative time difference occurred between detectors' responses depending on the amount of the

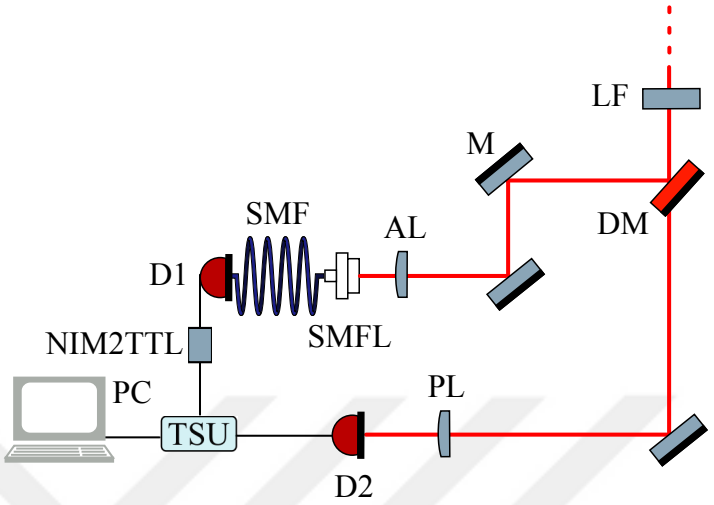


Figure 12: The experimental setup built in order to introduce time shift between detectors' responses. LP is long-pass filter. DM is dicroic mirror. M is mirror. AL is aspheric lens. SMF is single mode fiber. SMFL is SMF launch. D1 and D2 are detectors. PL is plano-convex lens. NIM2TTL is a converter between logic families. TSU is timestamp unit. PC is personal computer.

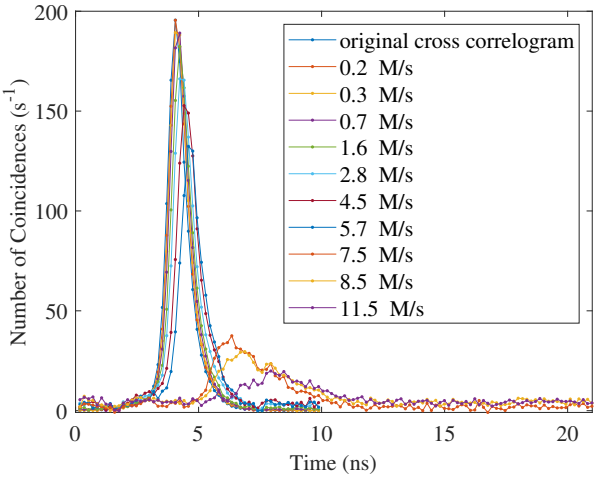


Figure 13: The legend represents the values of total number of photons. The unit of the noise (M/s) is million per second. The number of photons was 120 K/s when original cross correlogram is obtained.

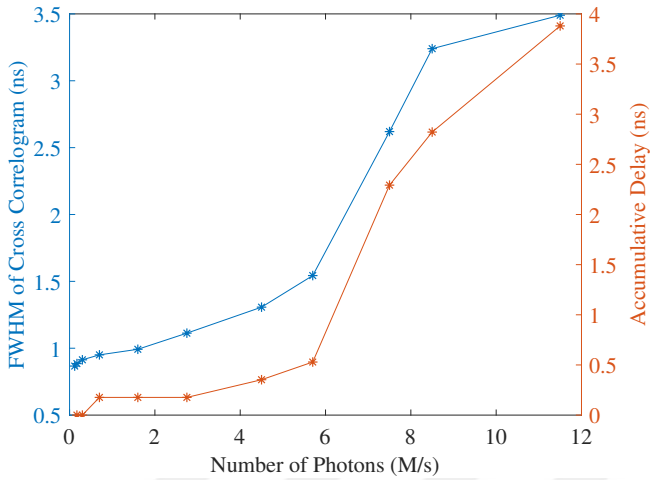


Figure 14: The time shift dependence to the amount of total number of photons.

noise. The time difference is initially 4.056ns, finally 7.937ns, hence the total amount of time shift produced in this setup is 3.881ns. Initial time difference is caused by optical path differences and electrical delays between detectors as mentioned in Sec. 2.2, and final time difference is caused by the reasons explained in Sec. 2.6.

2.6 FWHM Increase and Peak Shift of the Cross Correlogram

Dead time is a crucial parameter in determining the counting performance of an SPAD, which is also the type of the detector to which we inject noise. It is referred to as the decrease of sensitivity of the SPAD against incoming photons. In order to detect a single photon, SPADs can be operated with various reverse bias voltages above the breakdown voltage. Operation with how much above the breakdown voltage is determined by excess bias voltage. When a photon is detected, SPAD's dead time launches with a decrease of excess bias voltage below breakdown voltage, and followed by an increase of it up to the designed operating value. These two stages are called quenching and twilight zones [75]. The aims of the stages are to protect the SPAD from overheating by increased energy inside caused by the absorption of the photon, and to recover the SPAD after the required cooling is completed,

respectively. SPAD can detect photons as long as the excess bias voltage is above the breakdown voltage. So depending on the incoming photon rate and SPAD recovery time, incoming photons can also be detected in the twilight zone. As the excess bias voltage increases, the detection efficiency of the SPAD increases and time jitter decreases [76]. SPAD response may vary with operating conditions, also by third parties as shown in Sec. 2.5. As a result, the more number of photons, the earlier detection of the subsequent photons in twilight zone, and the less excess voltage across SPAD, the more time jitter. As the number of photons injected to a detector increases, the cross correlogram appears to be time shifted and widened.

In conclusion, in order to reduce or minimize the information leakage to an eavesdropper, choosing the bin width and start time of binning values are very important in QKD protocols. Because the mutual information fluctuates with respect to the bin width and the mutual information periodically fluctuates with respect to the start time of binning. Therefore it can be concluded that arbitrarily increasing the bin width is not a precaution to a timing side channel attack. For the security of a QKD system, the bin width, the start time of binning and the ratio of the FWHMs of detectors' responses to the time difference between the timing histograms or the coincidence peaks in the cross correlogram should be carefully adjusted with the characterization of physical system parameters. It is also possible to avoid the timing side channels by allowing one side to compensate for the time delays between cross correlogram peaks.

CHAPTER III

PHOTON BUDGET OPTIMIZATION

3.1 Introduction

In QKD literature, various methods were studied to increase key rate. For example, encryption and decryption in various degrees of freedoms [77] were put into use, brightness of entanglement source was increased [40] via fidelity and repetition rate increase, error correction with high speed [78] and varied schemes [79] were performed, high dimensional QKD protocols [80, 81] were generated, alternative QKD schemes like twin-field QKD [82, 83, 84, 85] were created and achievable distances were improved [86, 87, 88].

In DV-QKD, there are two EB protocols E91 [89] and BBM92 [21], and there are different protocols which use entangled photons [90, 91]. The studies performed related to E91 are security analysis [92, 93], examination of protocol under a certain noise model [93], employing optoelectronic polarization rotators (OPRs) in the implementation of violation of Bell's inequality [94] or throughout the QKD system [95] as dynamic components instead of employing beam splitters and wave plates [96] as the conventional static components, usage of entanglement between different degrees of freedoms (hybrid entanglement) [97], efficiency analysis and improvement [98], feasibility study on satellite-based communication [99], side channel analysis [100], and eavesdropping attack [101].

Here, we studied E91 protocol. We focused on the key rate after the steps of sifting and parameter estimation, before the steps of error correction and privacy amplification, which can also be called raw key rate, and aimed at increasing it.

In the EB QKD modified protocol of Ekert which is studied in Ref. [96], there

are three types of bits whose ratios are determined according to the beam splitting ratios of beam splitters at Alice's and Bob's sides. The three types of bits are key bits, Bell's inequality bits and discarded bits whose ratios are 25%, 50% and 25%, respectively. These ratios are not optimum. Our method of increasing the raw key rate will be the optimization of these ratios.

Photon budget defines the number of photons entering the detection module of a communicating side in a certain time interval. While the photon budget can take various values, a typical value is 10^6/s, as also assumed and used in our study.

For this study, our motivation is to increase the ratio of key bits in order to maximize raw key rate given photon budget without compromising the security of key. This can be achieved by decreasing the ratios of discarded bits and Bell's inequality bits. We examined various beam splitting ratios of beam splitters at Alice's and Bob's sides, and determined the optimum ratio of key bits yielding the maximum key rate. However, this optimization study can also be implemented to the QKD systems employing OPRs which are used for the same function as beam splitters and wave plates. This would be done by determining OPRs' optic axes' directions and the speed of change of the optic axes. Furthermore, this optimization study can also be implemented to the QKD systems which would use metamaterials having quantum phase transition materials for polarization change to be used in faster cryptography. The security of raw key relies on quantum bit error rate and Bell's inequality parameter. Quantum bit error rate will be a threshold determining the continuation or termination of the communication system. Bell's inequality parameter which depends on the amount of Bell's inequality bits will quantify how secure the system would be.

Organization of the chapter is the following. In Sec. 3.2, we investigated the uncertainty of the violation of Bell's inequality dependence to the number of photons used in the calculation of it and to the beam splitting ratios. In Sec. 3.3, we examined the effect of dead time of a detector in photon counting and examined the concept

on which photon budget allocation in the E91 protocol [96] is based. In Sec. 3.4, we introduced key rate expression that we use in our study and introduced the optimized photon budget. In Sec. 3.5, we presented the effects of photon detection efficiency and dark count of a detector on photon counting, explicitly. Lastly, in Sec. 3.6, we represent another approach to photon budget optimization at an idea level, and then finalize the chapter by summarizing the topic, giving our results and mentioning the importance of the study.

3.2 Dependencies of Uncertainty of the Violation of Bell's Inequality

In the process of obtaining a final raw key to be used in the encryption and decryption, key bits and Bell's inequality bits are collected for a period of time. At the end of each period, the security of key bits is quantified with a parameter, which is generated by using Bell's inequality bits. If this parameter, so called Bell's inequality parameter, is below a threshold, that block of key bits cannot contribute to final raw key and is discarded. Bell's inequality parameter is calculated frequently within the process of key distribution until final raw key could be obtained. Whenever the parameter is above the threshold, the related block of key bits can be used to contribute final raw key. In this way, the blocks of key bits are collected and final raw key is obtained.

The Bell's inequality parameter we used throughout the chapter is given in Eq. (8).

$$S = E(a_0, b_0) + E(a_0, b_1) - E(a_1, b_0) + E(a_1, b_1) \tag{8}$$

where $a_0(b_0)$ and $a_1(b_1)$ are two sets of detectors located at Alice's (Bob's) detection module. Each set of detectors consists of two detectors. In other words, each of $a_0(b_0)$ and $a_1(b_1)$ can be called a basis set and consists of two orthogonal basis. Thus each detector is related to a basis and is dedicated to measure a polarization direction which is shown in Fig. 15 [96]. $E(a_i, b_i)$ is a correlation coefficient related to measurement results obtained from basis sets a_i and b_i. The mathematical expression

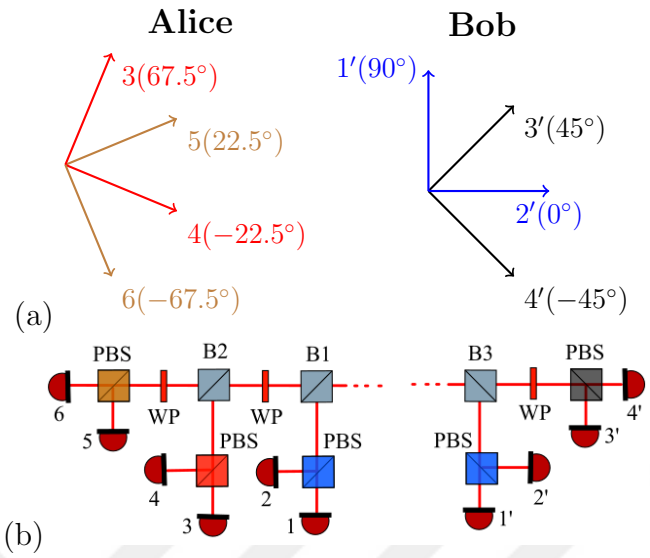


Figure 15: (a) Measurement basis sets used in the calculation of the amount of violation of Bell's inequality at Alice's and Bob's sides. The four basis sets and their components are as follows: $a_0 \equiv \{3, 4\}$, $a_1 \equiv \{5, 6\}$, $b_0 \equiv \{1', 2'\}$, $b_1 \equiv \{3', 4'\}$. (b) B1, B2, B3: Beam splitters. PBS: Polarizing beam splitter. WP: Wave plate. The numbers indicate detectors, in other words, the basis sets' components. Figure on the left and right represent the detection modules at Alice's and Bob's sides, respectively. Reflected outputs of B1 and B3 constitute key bit detection parts of the detection modules.

of this correlation coefficient for various values of a_i and b_i can be found in Eq. (9). Lastly, S is the combined correlation coefficient used to quantify the quantumness a QKD system has. While the Bell's inequality satisfies $|S| \leq 2$, which we call classical region, its violation is realized when $2 < |S| \leq 2\sqrt{2}$.

In a pair of measurement among Alice and Bob, the coincidence of two of the basis in Fig. 15 (a) results in a Bell's inequality bit being obtained in the QKD system. The reflected outputs of B1 and B3 in Fig. 15 (b) represent the same basis set, thus the coincidence of these basis sets results in a key bit being obtained in the system. Lastly, the coincidence of a measurement at the reflected output of B1 and a measurement at the basis set labeled with $\{3', 4'\}$ results in a discarded bit being obtained in the system. Namely, the type of a bit is determined by which basis sets coincide.

The components of S are given in Eq. (9).

$$\begin{aligned} S &= E(a_0,b_0)+E(a_0,b_1)-E(a_1,b_0)+E(a_1,b_1) \\ &= \frac{n_{31'}+n_{42'}-n_{32'}-n_{41'}}{n_{31'}+n_{42'}+n_{32'}+n_{41'}}+\frac{n_{33'}+n_{44'}-n_{34'}-n_{43'}}{n_{33'}+n_{44'}+n_{34'}+n_{43'}} \\ &\quad -\frac{n_{51'}+n_{62'}-n_{52'}-n_{61'}}{n_{51'}+n_{62'}+n_{52'}+n_{61'}}+\frac{n_{53'}+n_{64'}-n_{54'}-n_{63'}}{n_{53'}+n_{64'}+n_{54'}+n_{63'}} \end{aligned} \tag{9}$$

where $n_{k,l}$ with $k \equiv \{3,4,5,6\}$ and $l \equiv \{1',2',3',4'\}$ which are shown in Fig. 15 (a) is the number of coincidences in polarization directions k and l at Alice's and Bob's sides. n_{kl} can be written in terms of four parameters as given in Eq. (10) by using statistical approach.

$$n_{kl} = \eta \cdot B2_k \cdot B3_l \cdot p_{kl} \tag{10}$$

where η is the total number of photons which will be used for the calculation of S or total number of coincidence counts, $B2_k$ is the beam splitting ratio of the beam splitter B2 shown in Fig. 15 (b) at the direction of the basis set of which the basis k is a component, $B3_l$ is the beam splitting ratio of the beam splitter B3 shown in Fig. 15 (b) at the direction of the basis set of which the basis l is a component and p_{kl} is the probability of coincidences in k and l whose expression is given in Eq. (11).

$$p_{kl} = Tr[(\hat{M}_k \otimes \hat{M}_l)\hat{\rho}] \tag{11}$$

where Tr is trace operator, $\hat{M}_k(\hat{M}_l)$ is the operator represents measurement along the direction of $k(l)$, $\hat{\rho}$ is the density matrix of the quantum state used in the quantum channel and $\otimes$ is tensor product enabling a joint measurement along the directions of k and l on the quantum state. Measurement operator $\hat{M}_k(\hat{M}_l)$ is obtained by the outer product of ket (column vector) $|k\rangle(|l\rangle)$ and bra (row vector) $\langle k|(\langle l|)$, which is the complex conjugate of $|k\rangle$, as given in Eq. (12).

$$\hat{M}_k = |k\rangle \langle k| \tag{12}$$

$|k\rangle$ represents a polarization direction (θ) as shown in Fig. 15 (a). Matrix representations of computational basis $|0\rangle$ and $|1\rangle$ are given in Eq. (13). $|0\rangle$ and $|1\rangle$ represent

horizontal and vertical polarization directions, respectively. Thus each of the polarization directions can be expressed in terms of computational basis as given in Eq. (14). An example of it can be seen in Eq. (15).

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{13}$$

$$|k\rangle \equiv |\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \tag{14}$$

$$|k=3\rangle \equiv |67.5^\circ\rangle = \cos 67.5^\circ\,|0\rangle + \sin 67.5^\circ\,|1\rangle \tag{15}$$

Ultimately with Eq. (10), the total number of photons, which is allocated from photon budget to Bell's inequality bits and is used in the calculation of S, is allocated to the components of S, namely, n_{kl} for all the values of k and l. The mathematical expression of it is given in Eq. (16).

$$\eta = \sum_k \sum_l n_{kl} \tag{16}$$

A mixed state consisting of the singlet state $|\psi^-\rangle$ given in Eq. (17) and white noise, which is also called Werner state, was used in the quantum channel. The visibility (V) of singlet state is taken as 0.95. Expression of the mixed state can be seen in Eq. (18) explicitly.

$$\begin{aligned} |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \\ &\equiv \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{17}$$

$$\hat{\rho} = V\,|\psi^-\rangle\langle\psi^-| + \frac{(1-V)}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|) \tag{18}$$

Values of the probability of coincidences are given in Table 3.

Beam splitter B2 in Fig. 15 (b) has a constant beam splitting ratio among transmitted and reflected beams, and it is 0.5. Thus the value of $B2_k$ is equal to 0.5 for all the values of k. The change of the beam splitting ratio of beam splitter B3 in Fig.

$p_{31'} = 0.0821$	$p_{33'} = 0.0821$	$p_{51'} = 0.4179$	$p_{53'} = 0.0821$
$p_{42'} = 0.0821$	$p_{44'} = 0.0821$	$p_{62'} = 0.4179$	$p_{64'} = 0.0821$
$p_{32'} = 0.4179$	$p_{34'} = 0.4179$	$p_{52'} = 0.0821$	$p_{54'} = 0.4179$
$p_{41'} = 0.4179$	$p_{43'} = 0.4179$	$p_{61'} = 0.0821$	$p_{63'} = 0.4179$

Table 3: Values of the probability of coincidences.

15 (b) enables various ratios among three types of bits. Thus we examined a range of beam splitting ratio of B3. For a chosen reflectance (R) of B3, the relations given in Eq. (19) are obtained.

$$B3_{1'} = B3_{2'} = R \tag{19a}$$

$$B3_{3'} = B3_{4'} = (1 - R) \tag{19b}$$

As a result, n_{kl} can be written in terms of two independent parameters η and $B3_l$. Thus it can be interpreted as S is a function of independent and random variables. Propagation of uncertainty can be applied to S and the uncertainty of S can be expressed as given in Eq. (20) [102, 103].

$$\delta S = \sqrt{\sum_k \sum_l \Big(\frac{\partial S}{\partial n_{k,l}} \delta n_{k,l}\Big)^2} \tag{20}$$

where δ stands for uncertainty. The definition of uncertainty of coincidence counts is given in Eq. (21) because in Poisson statistics, standard deviation is equal to the square root of mean. Uncertainty of S, δS, can give an idea about how reliable an S obtained would be relatively. Lastly, ∂ stands for partial derivative.

$$\delta n_{k,l} = \sqrt{n_{k,l}} \tag{21}$$

For the mixed state ρ, the uncertainty of S depending on the various numbers of photons and various values of the reflectance of beam splitter B3 was computed and shown in Fig. 16.

Expected value of S is obtained by using Eq. (22).

$$\langle \hat{S} \rangle = Tr[\hat{S}\hat{\rho}] \tag{22}$$

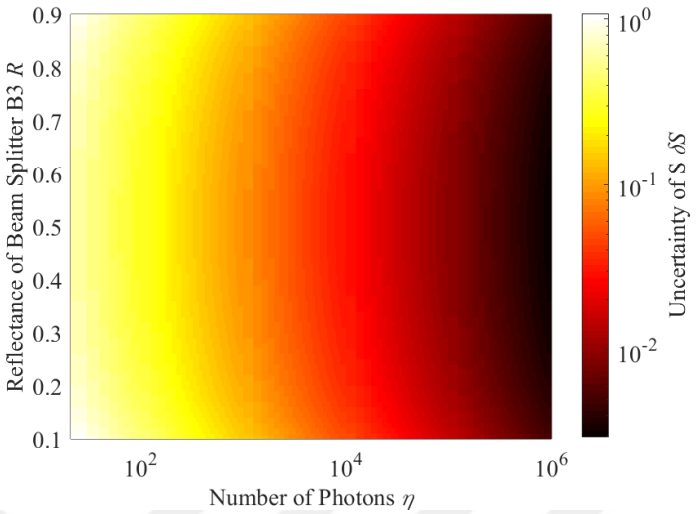


Figure 16: The graph of the uncertainty of S dependence to the number of photons and the reflectance of beam splitter B3. Color bar represents the uncertainty of S.

where $\langle \hat{S} \rangle$ is the expected value of $\hat{S}$, $\hat{S}$ is the operator acting on the density matrix $\hat{\rho}$. $\hat{S}$ is obtained by substituting the joint measurement operators of k and l which are related to n_{kl} into Eq. (9). Also, ideally expected value of $\hat{S}$ can be obtained by using Eq. (23).

$$S = 2\sqrt{2}V \tag{23}$$

where V is the visibility of the quantum state. In addition to Fig. 16, the uncertainties in terms of error bars around the ideally expected value of $\hat{S}$ can be seen in Fig. 17. In the figure, the dependence of the uncertainty to the number of photons is shown for the case of $50:50$ beam splitters are employed at both communicating sides.

Since the number of photons used in the calculation of S follows Poisson distribution, S also follows the same statistics. A Poisson distribution can be approximated with a Gaussian distribution when its mean > 20 [104]. We considered different pairs of numbers of photons η and reflectance R as independent experiments and modeled the probability distribution of S in each case with a Gaussian distribution approximation whose standard deviation is the corresponding uncertainty in Fig. 16. We called the region $|S| \leq 2$ as classical region, computed the areas under the probability

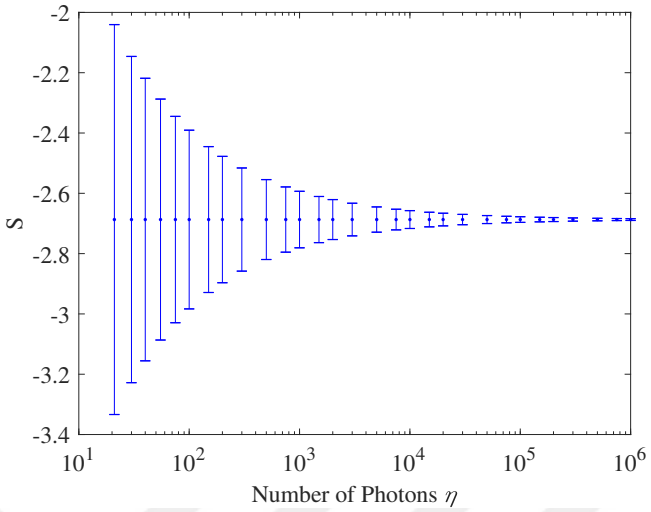


Figure 17: The graph of the uncertainty of S dependence to the total number of photons used in the calculation of S in case of $50:50$ beam splitters are employed.

distributions of S which fall into the classical region and showed the dependence of the probability to η and R in Fig. 18.

The probability shows the percentage of all the blocks of key bits collected in a key distribution process which cannot contribute to the final raw key. In other words, it represents the ratio of key rate which will be discarded in unit time interval. Even if the quantum channel is secure, communicating sides can obtain an S value from the classical region at that probability. We will call the raw key rate remains after the decrease at that probability as average raw key rate in the rest of the chapter.

3.3 Effect of Dead Time of Detector in Photon Counting

Dead time is the bottleneck which limits photon counting in a detector. The number of photons observed at a detector may differ from the number of photons reaching the detector. The relation between them is given in Eq. (24).

$$N = \frac{n}{n \cdot t \cdot 10^{-12} + 1} \tag{24}$$

where n is the number of photons reaching detector per second, t is the dead time of detector in terms of ps and takes value within the range of $1\text{ps} \leq t \leq 10^{12}\text{ps}$, and N

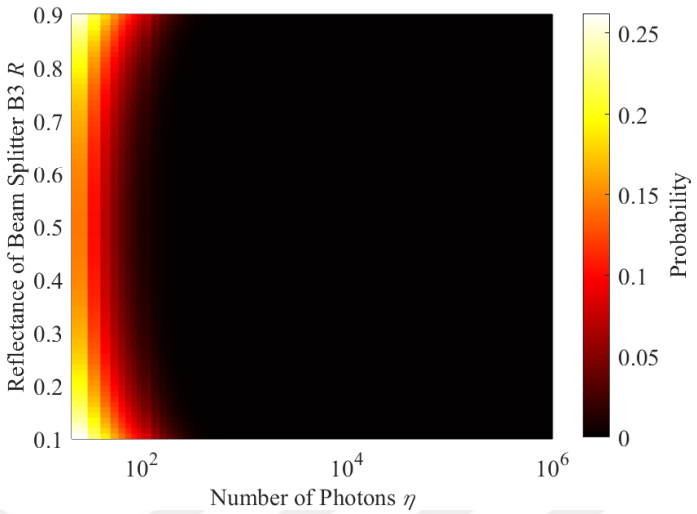


Figure 18: The graph of the dependence of the probability to the number of photons and the reflectance of beam splitter B3. Color bar represents the probability of obtaining a value from the classical region for S.

is the number of photons observed at detector per second. Dependence of N to t is shown in Fig. 19.

There are three types of n with which we are dealing. Photon budget is allocated among three types of n as given in Eq.(25). They are the numbers of photons reaching detectors or detectors' groups which are dedicated to obtain three types of bits.

$$n = n_{key} + n_S + n_{discarded} \tag{25}$$

The numbers of photons reaching these detectors are determined by the ratios of three types of bits as given in Eq. (26).

$$n_{key} = n \cdot ratio\, of\, key\, bits \tag{26a}$$

$$n_S = n \cdot ratio\, of\, Bell's\, inequality\, bits \tag{26b}$$

$$n_{discarded} = n \cdot ratio\, of\, discarded\, bits \tag{26c}$$

The ratios of three types of bits change according to the beam splitting ratios at communicating sides as given in Eq. (27).

$$ratio\, of\, key\, bits = B1_R \cdot R \tag{27a}$$

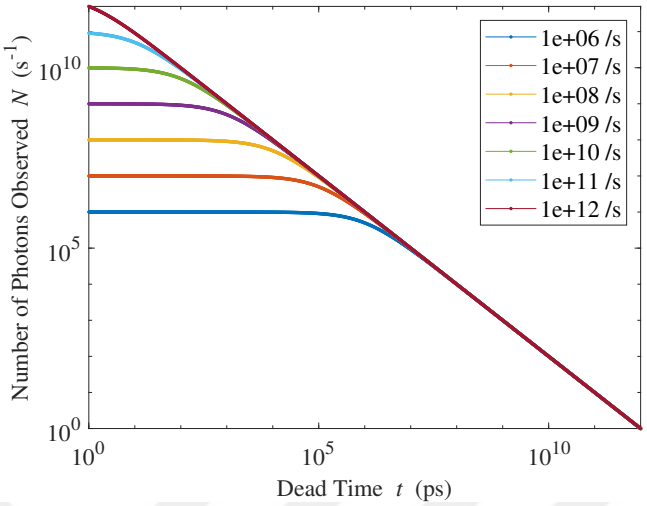


Figure 19: The graph of the number of photons observed at a detector per second dependence to the dead time of detector. Legend represents n, namely, the number of photons reaching detector per second.

$$ratio\,of\,Bell's\,inequality\,bits = (1 - B1_R) \cdot 1 \tag{27b}$$

$$ratio\,of\,discarded\,bits = B1_R \cdot (1 - R) \tag{27c}$$

where $B1_R$ and R are the reflectances of the beam splitters B1 and B3 in Fig. 15 (b). Ratios of three types of bits dependence to the beam splitting ratios are shown in Fig. 20. In the figure, the beam splitting ratios are taken symmetric for both sides, namely, it is taken as $B1_R = R$ so the x-axis shows the values of R. The ratios of key bits, Bell's inequality bits and discarded bits are %25, %50 and %25, respectively, where the beam splitting ratio for key at both sides = 0.5.

In the rest of the chapter, dead time was be taken as 1ps. In the calculation of the numbers of photons in three types of bits, coincidence window, which is the time interval to determine coincidences (pairs of bits) among communicating sides, is also chosen equal to dead time. Given the dead time and coincidence window, we continued our study with the numbers of photons observed in three types of bits which are given against the ratio of key bits in Fig. 21.

While η in Eq. (10) is the number of photons which will be used in the calculation

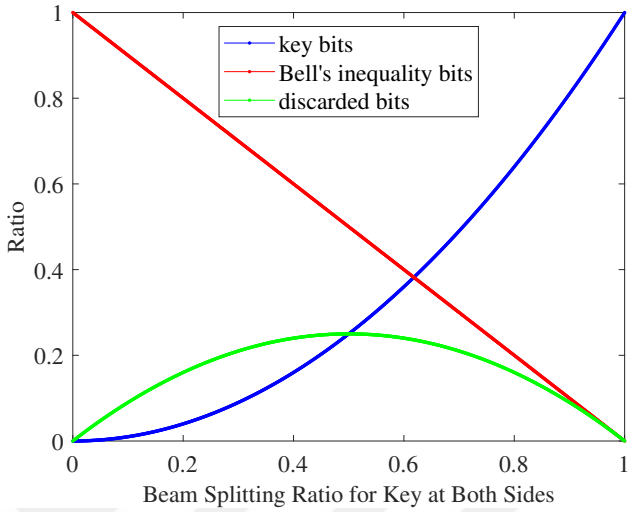


Figure 20: The graph of the ratio of three types of bits dependence to the beam splitting ratio for key at both sides, namely, dependence to the ratios in the reflected outputs of B1 and B3 in Fig. 15 (b).

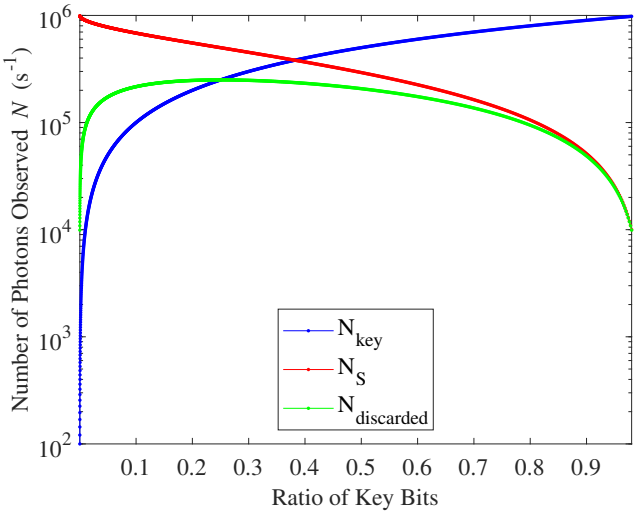


Figure 21: The graph of the numbers of photons observed in three types of bits' change against the ratio of key bits. N_{key}, N_S and $N_{discarded}$ are the numbers of photons which will be used in the calculations of raw key rate, Bell's inequality parameter and the number of photons discarded, respectively.

of S, N_S in Fig. 21 is the number of photons which will be used in the calculation of S per second.

3.4 Average Raw Key Rate

The key rate formula we used is that of device-independent QKD which is based on collective attacks scenario [17]. In collective attacks scenario, an eavesdropper collects her ancilla qubits which interact with Alice's and Bob's qubits, and stores them in a memory unit without performing any measurement. After she learns the measurement basis sets performed at Alice's or Bob's side via classical channel, she makes the optimal measurement (or maybe the same measurements as Alice or Bob) on them. The key rate formula is the first multiplier in Eq. (28) whose unit is bits/symbol.

$$\left(1 - h(Q) - h\Big(\frac{1+\sqrt{((S+\delta S)/2)^2 - 1}}{2}\Big)\right) \cdot N_{key} \cdot (1-P) \tag{28}$$

where 1 is the entropy of Alice or Bob, it is equal to the initial mutual information between them in accordance with the entropic relation given in Eq. (29).

$$I(A;B) = H(A) - H(A|B) \tag{29}$$

This initial entropy is at its max value because of the assumption that they have the same key bit string and it is secure ($H(A|B) = 0$). $h(Q)$ is the binary entropy of quantum bit error rate Q, which is calculated as given in Eq. (30).

$$Q = Tr[(\hat{M}_1 \otimes \hat{M}_{1'})\hat{\rho}] + Tr[(\hat{M}_2 \otimes \hat{M}_{2'})\hat{\rho}] \tag{30}$$

where $\hat{M}_{1'}$ and $\hat{M}_{2'}$ are measurement operators along the directions of 90° and 0°, respectively, as shown in Fig. 15 (a). $\hat{M}_1$ and $\hat{M}_2$ are measurement operators, which are applied at Alice's side, along the same direction as $\hat{M}_{1'}$ and $\hat{M}_{2'}$, respectively. The expected value of $\hat{Q}$ is 0.025 caused by the visibility V of the quantum state $|\psi^-\rangle$ within the mixed state $\hat{\rho}$. The threshold of Q which is determined by the attack type

assumed is 0.071 [17]. Thus, in an implementation of this experiment, a value between these two values can be chosen as the threshold for Q, depending on the physical conditions. We continue with the value of 0.025. The first two terms constitute the new mutual information between Alice and Bob. It can also be referred to as classical mutual information because of basing on classical bits. $h\left(\frac{1+\sqrt{((S+\delta S)/2)^2-1}}{2}\right)$ is the accessible information about the quantum state (Holevo bound) by an eavesdropper. It is the maximum quantum mutual information between one of the legitimate parties and Eve in a one-way communication of classical information between Alice and Bob in the parameter estimation stage. Here, S is the mean and δS is the uncertainty of Bell's inequality parameter. In the comparison of different distributions of S in the experiments using different total number of photons, the range of $\mu \pm \sigma$, where μ is the mean and σ is the standard deviation of the distribution, can be used. Thus from the range of $S \pm \delta S$, we chose $S + \delta S$ because of being closer to the classical region to distinguish the effect of different distributions of S as the worst case scenario that can be encountered in an experiment. With the subtraction of this term, key rate, which is secure, between Alice and Bob is obtained. N_{key} is as defined in Sec. 3.3 and is the conversion parameter from bits/symbol to bps which would be the unit of the key rate used in the rest of the chapter since each symbol or photon carries one bit of information. P is the probability of obtaining an S from the classical region and with the use of it the key rate formula turns into average key rate.

The average key rates that can be obtained depending on the beam splitting ratios, and the maximized key rate can be seen in Fig. 22. While average key rate is 0.1331Mbps in the standard configuration which is the employment of 50 : 50 beam splitters [96] and is shown as a red circle in the figure, it becomes 0.4342Mbps in the employment of 90 : 10 beam splitter at Alice's side and 97 : 3 beam splitter at Bob's side and shown as a blue circle in the figure. Hence our method presents an increase in the average key rate up to 226.22%. Also, while the ratios of key

bits, Bell's inequality bits and discarded bits are 25%, 50% and 25% in the standard configuration, their ratios in the maximized key rate configuration is 87%, 10% and 3% which can be seen in Fig. 23, 24 and 25, respectively. In the figures, the labels of x-axes and legends were kept the same in order to enable reading the values of all the parameters which depends on the beam splitting ratios. Additionally, the number of photons used in the calculation of S becomes 10^5/s with the 10% allocation. This value can be read from the graph of N_S dependence to the beam splitting ratios at Alice's and Bob's sides which is Fig. 26. S with its uncertainty corresponding to that much of photons is -2.6870 ± 0.0255. The uncertainty can be seen in Fig. 27. The quantification of violation of Bell's inequality can be given in terms of the number of standard deviations (SDs). It is computed as given in Eq. (31).

$$number\,of\,SDs = \frac{2\sqrt{2}V - 2}{\sigma} \tag{31}$$

where σ is 1SD, which can be seen in Bell's inequality parameter given in the form of $-2.6870 \pm \sigma$. Thus in the optimized allocation, Bell's inequality is violated with 26.95SD and it can be seen in Fig. 28. In the literature, there are various numbers of standard deviations in the violations of Bell's inequality, such as 6SD, 12SD [105], 8.5SD, 9.3SD [106], 10SD [107, 108], 24SD [109, 108], 203SD [110], and there is no threshold other than the trivial conclusion that the number of standard deviations > 0 must be satisfied. Thus 26.95SD is within the acceptable range of the numbers of standard deviations of the violation, and 10% allocation instead of 50% to the Bell's inequality bits does not expose a compromise in the security of the QKD system which is based on S.

Incremental steps of the beam splitting ratio at Alice's side is 0.1 and at Bob's side is 0.001. More precise optimum values can be obtained by reducing the incremental steps of the beam splitting ratios in the simulations for the QKD systems which enable more sensitive implementations. However, the change in the beam splitting ratios from 50 : 50 to roughly 90 : 10 would give a considerable increase in the key

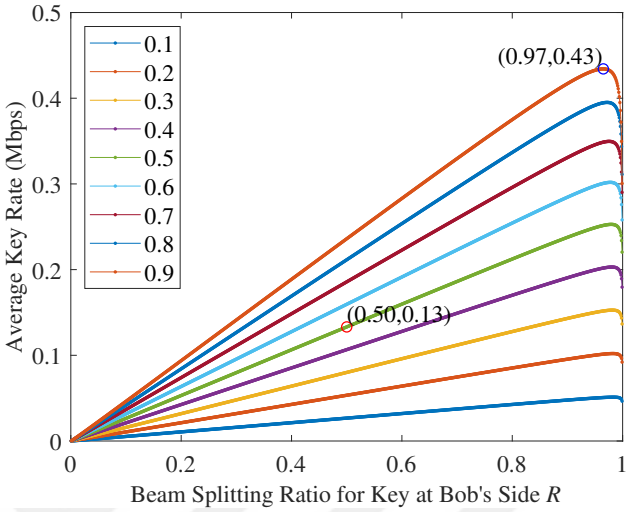


Figure 22: The graph of the average key rate dependence to the beam splitting ratio for key at Bob's side, namely, dependence to the beam splitting ratio at the reflected output of B3 in Fig. 15 (b). Legend represents the beam splitting ratio for key at Alice's side, namely, the beam splitting ratio at the reflected output of B1 in Fig. 15 (b).

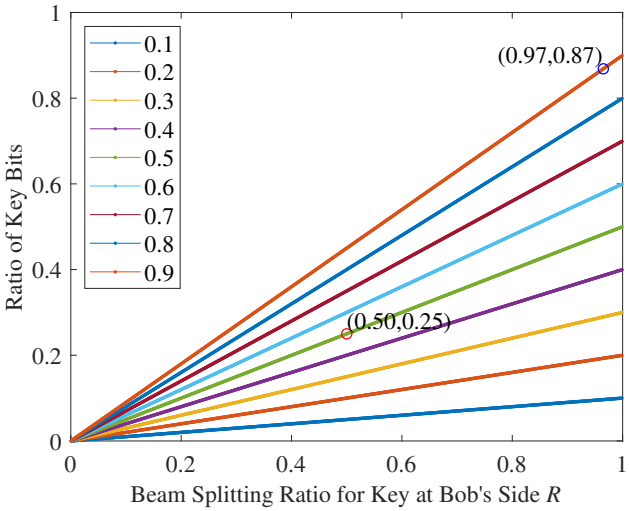


Figure 23: The graph of the ratio of key bits dependence to the beam splitting ratios for key. Legend represents the beam splitting ratio for key at Alice's side.

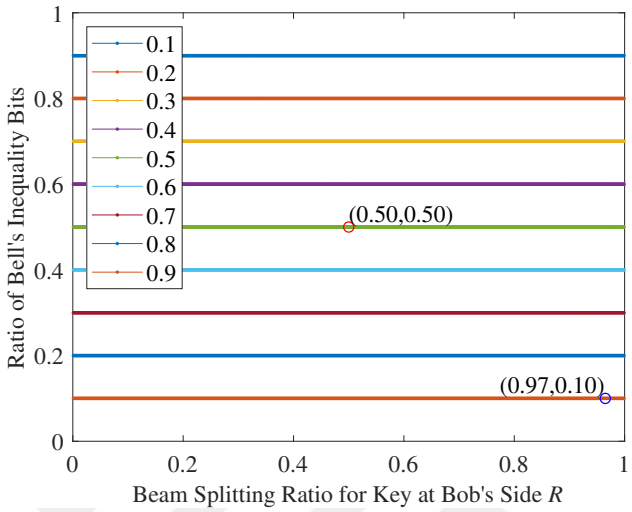


Figure 24: The graph of the ratio of Bell's inequality bits dependence to the beam splitting ratios for key. Legend represents the beam splitting ratio for key at Alice's side.

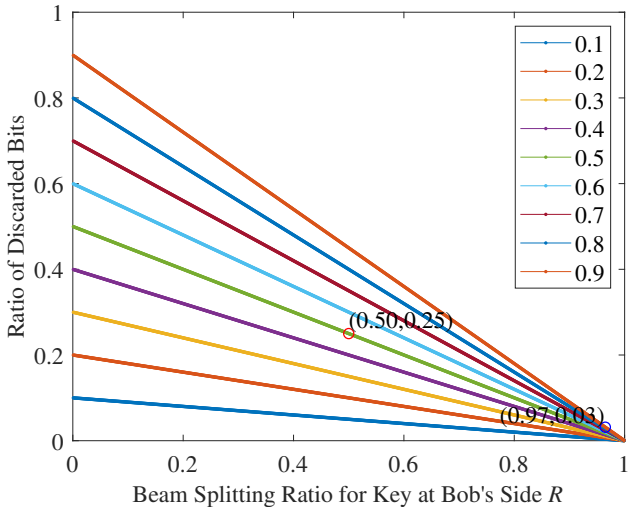


Figure 25: The graph of the ratio of discarded bits dependence to the beam splitting ratios for key. Legend represents the beam splitting ratio for key at Alice's side.

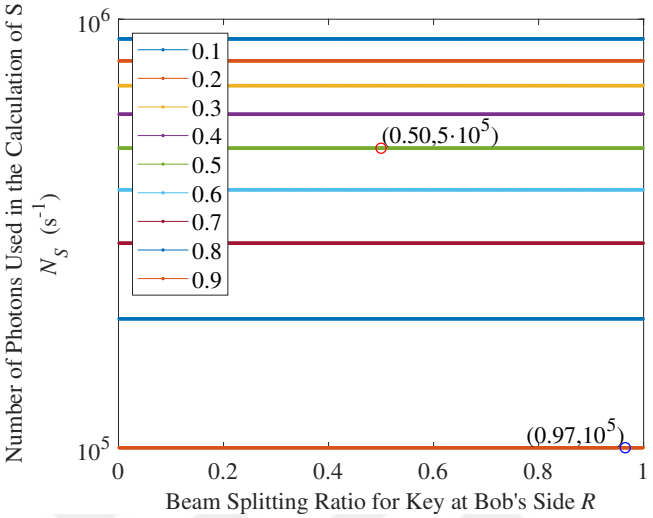


Figure 26: The graph of the number of photons used in the calculation of S dependence to the beam splitting ratios for key. Legend represents the beam splitting ratio for key at Alice's side.

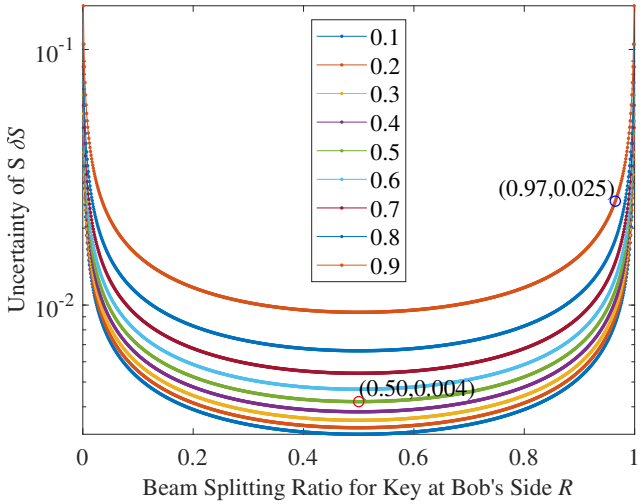


Figure 27: The graph of the uncertainty of S dependence to the beam splitting ratios for key. Legend represents the beam splitting ratio for key at Alice's side.

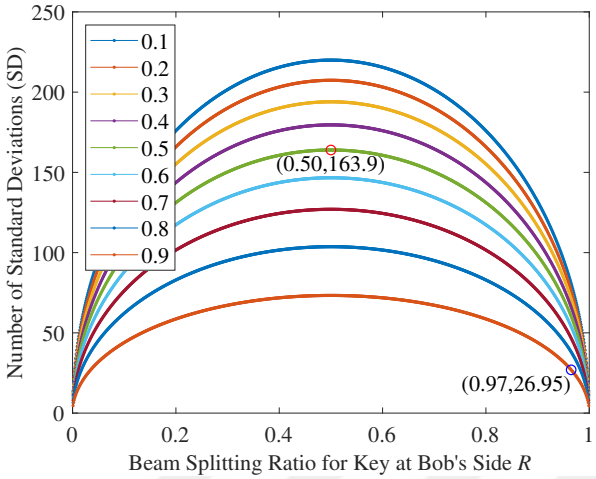


Figure 28: The graph of the number of standard deviations of the violation of Bell's inequality dependence to the beam splitting ratios for key. Legend represents the beam splitting ratio for key at Alice's side.

rate as shown in this study.

Fig. 29 is plotted to show at which beam splitting ratios a maximized average key rate can be achieved. In this figure, the beam splitting ratios at both sides are chosen as the same as indicated in the label of x-axis. Photon budget changes within the range of $[10^3, 10^9]$/s. Color bar shows normalized average key rate in which average key rates at various beam splitting ratios for a photon budget is normalized according to the maximized average key rate. After $n = 10^6$/s, maximized average key rate seems to happen when beam splitting ratios for key = 0.9. It is suggested to look at average key rate change in a graph of the type of Fig. 22. If the global maximum average key rate cannot be seen in such a graph, the conclusion that this experimental setup for higher photon budgets may not be effective can be inferred. For example, maximized average key rate values for $n = \{10^3, 10^4, 10^9\}$/s can be seen in Fig. 30, 31 and 32 along with corresponding numbers of standard deviations. And it can be concluded that when $n = 10^9$/s, it is not effective to work with the experimental setup configuration given in this study since the global maximum value of the average key rate cannot be seen in Fig. 32 (a).

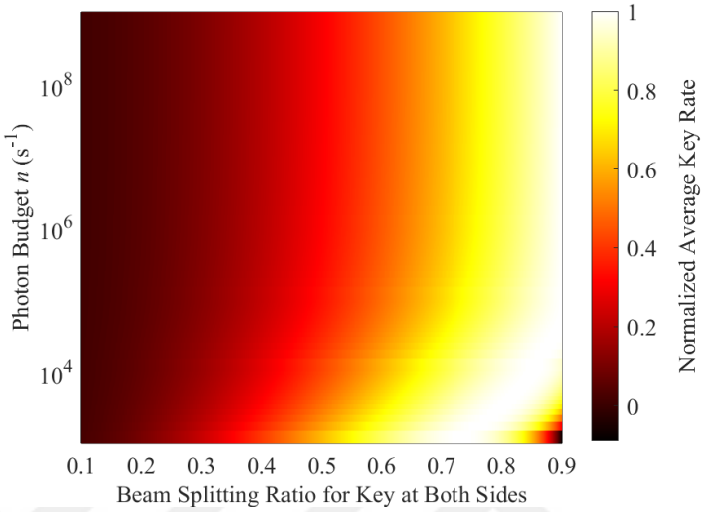
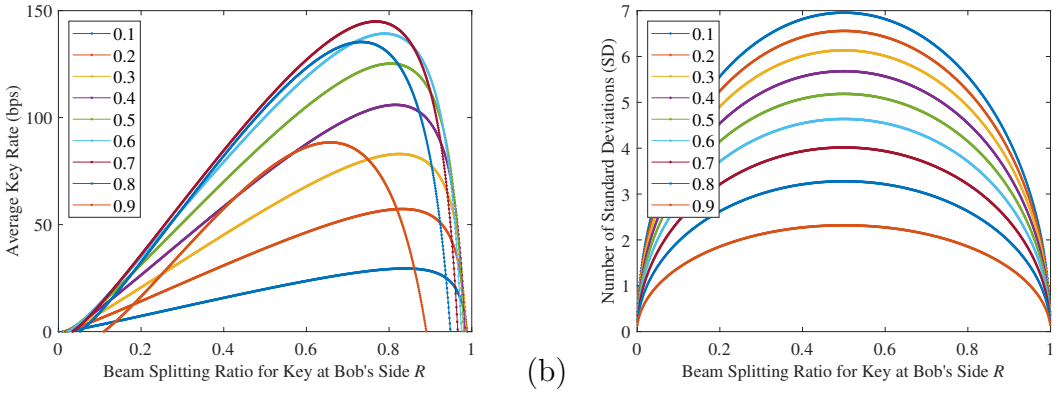


Figure 29: Normalized average key rate dependence to photon budget and beam splitting ratios for key at both sides.



(a) (b)

Figure 30: (a) Average key rate dependence to the beam splitting ratios for key at Alice's and Bob's sides when $n = 10^3/\text{s}$. (b) Number of standard deviations dependence to the beam splitting ratios for key at Alice's and Bob's sides when $n = 10^3/\text{s}$.

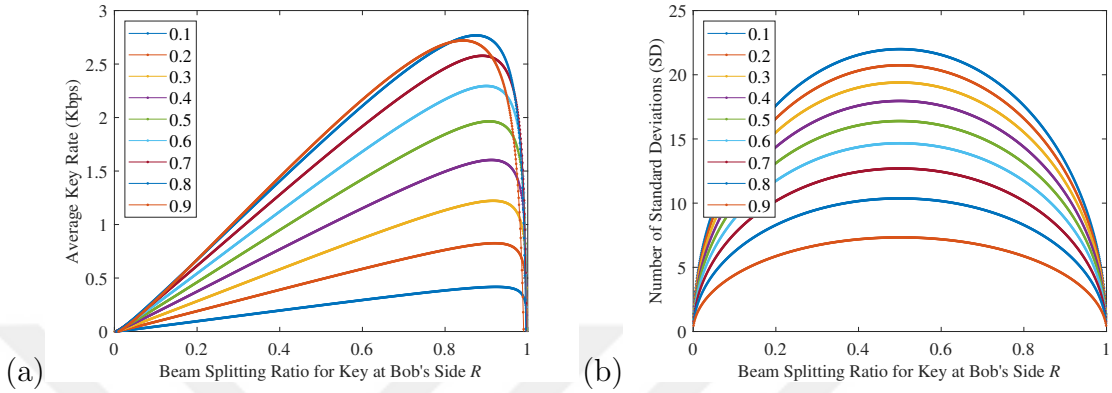


Figure 31: (a) Average key rate dependence to the beam splitting ratios for key at Alice's and Bob's sides when $n = 10^4$/s. (b) Number of standard deviations dependence to the beam splitting ratios for key at Alice's and Bob's sides when $n = 10^4$/s.

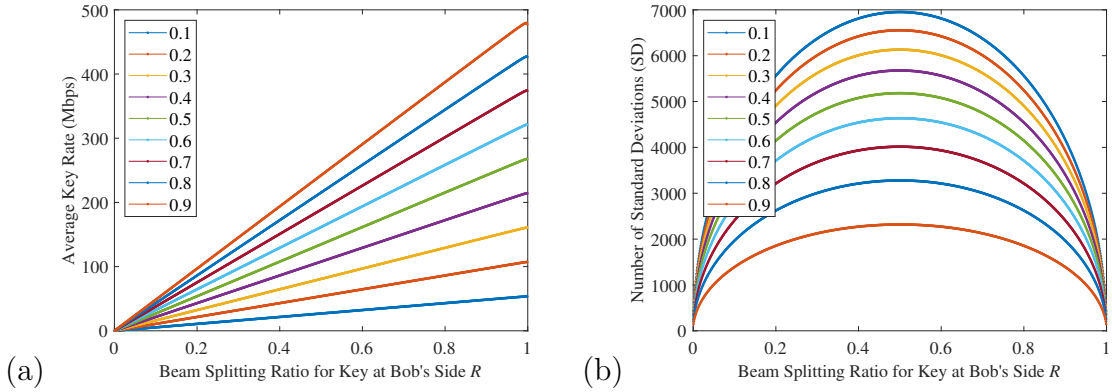


Figure 32: (a) Average key rate dependence to the beam splitting ratios for key at Alice's and Bob's sides when $n = 10^9$/s. (b) Number of standard deviations dependence to the beam splitting ratios for key at Alice's and Bob's sides when $n = 10^9$/s.

Average key rate values can change according to detector specifications. In order to see the effects of photon detection efficiency and dark count on photon counting, Sec. 3.5 should be consulted.

3.5 Effects of Photon Detection Efficiency and Dark Count of Detector in Photon Counting

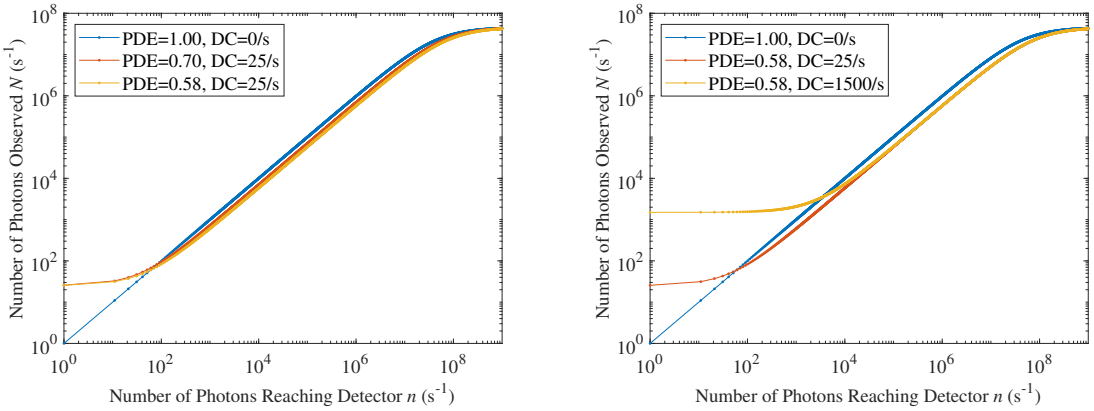
Besides dead time, photon detection efficiency (PDE) and dark count (DC) also take part in the relation between the numbers of photons reaching a detector and observed at the detector per second. They can be incorporated as given in Eq.(32).

$$N = \frac{n \cdot PDE + DC}{n \cdot PDE \cdot t \cdot 10^{-12} + 1} \tag{32}$$

where n, t and N are as defined in Eq. 24. In this study, PDE and CD are taken as 1 and 0/s, respectively, for the simplification. The effect of PDE can be seen in the left hand side of Fig. 33, which is a vertical shift in the linear region. And the effect of DC can be seen in the right hand side of Fig. 33, which shows itself as noise while working with relatively lower number of photons. And it shows the performance of a detector while working with relatively low number of photons. In this figure, dead time was taken as 22ns for all the curves and substituted into Eq.32 in terms of ps as compatible with Eq.24. Alternative to Eq.(32), a formula which characterizes a detector should be used in a specific implementation in order to obtain average key rates achievable.

3.6 Another Approach for Photon Budget Optimization

In an E91 QKD system application having dynamic polarization rotators used instead of beam splitters and wave plates as shown in Fig. 34, different measurement basis sets are realized with the rotations of optical axes of OPRs. In Fig. 34, S is entanglement source, CAs are coincidence analyzers and QRNGs are quantum random number generators. QRNGs apply voltage to OPRs and change the direction of optical axes,



(a) (b)

Figure 33: The graphs of the number of photons observed vs the number of photons reaching detector. The effect of photon detection efficiency and dark count to the number of photons observed.

with uniform or non-uniform probabilities randomly. Uniform probability distribution among basis sets used in the generation of raw key bits, Bell's inequality bits and discarded bits yields 17%, 66% and 17%, respectively. Photon budget optimization can be applied to this systems in the similar way explained in the previous sections (and this study can also be found in [111]) and optimum ratios can be obtained by creating non-uniform probability distribution. In performing this optimization, a point needs to be taken into account differently from the previous method, which is explained as follows. Certain directions of optical axes will correspond to certain basis sets. When switching between basis sets, there exist time intervals in which photons will be discarded because of not measuring in the expected optical axes orientations or in the expected basis sets and will contribute to the discarded bits defined in Sec. 3.2. The time intervals and the number of photons which will be discarded depend on the speeds of changes of optical axes. Thus, this point also should be taken into account in the optimization. However, what we offer here is a different approach than this method. It is the idea of regaining of the discarded bits defined in Sec. 3.2 to the system and using them to apply voltage to OPRs. In this way, the number of

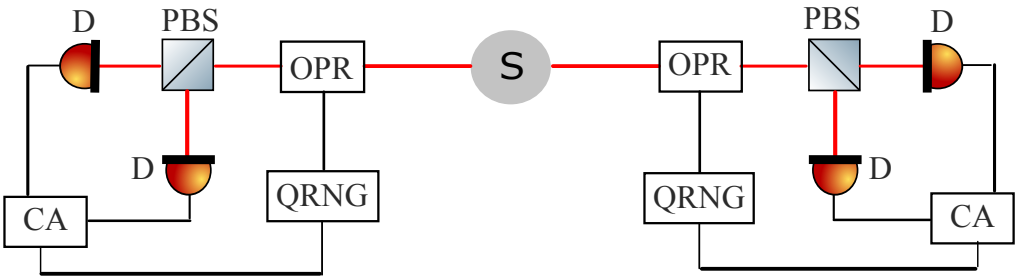


Figure 34: Reducing the number of discarded bits by regaining them to the system. S is entanglement source, OPRs are optoelectronic polarization rotators, PBSs are polarizing beam splitters, Ds are detectors, CAs are coincidence analyzers and QRNGs are quantum random number generators.

discarded bits will be reduced by 'recycling'.

As a result, in this chapter, we focused on a standardized E91 QKD protocol, in which 50 : 50 beam splitters are employed at both Alice's and Bob's sides. Depending on the positioning of measurement basis sets with respect to the beam splitters, there was the allocation of 25%, 50% and 25% of a photon budget among three types of bits, which are key bits, Bell's inequality bits and discarded bits. We calculated raw key rate for the 50 : 50 beam splitters and for the standard allocation as a reference point. Then, we examined the value of raw key rate for various beam splitting ratios and for various allocations of the photon budget. We searched the optimum beam splitting ratios and allocations yielding the global maximum raw key rate, and showed that 226.22% increase in raw key rate can be achievable with 90 : 10 and 97 : 3 beam splitting ratios, and with the allocation of 87%, 10% and 3%. Additionally, we showed that optimum beam splitting ratios can vary for different photon budgets in a constant configuration of experimental setup by defining a parameter called normalized average key rate and by using it. An E91 QKD protocol may have various configurations such as not including all the basis sets used in this study or establishing symmetrical detection modules in terms of basis sets at both communicating sides or the realization of basis sets by using OPRs instead of beam splitters and wave plates. The optimization of photon budget allocation should be applied to all the

experimental setups of the similar kind for the best use of resources and for the maximization of raw key rate.

CHAPTER IV

CONCLUSION

QKD protocols presents unconditional security in theory. Imperfections occur in experimental implementations unavoidably and they can cause security loopholes as opposed to its core promise. One of them is timing side channel or detector efficiency mismatch, which is valid for PAM and EB QKD systems. In the literature, there was a recognized solution to this problem, which is the increase of time bin width instead of revealing precise timing information via public channel. Mutual information between the values of key bits and the timestamp information of photon detection events is used in the quantification of leakage information to a possible eavesdropper. In the literature, it has been shown that as time bin width increases, the mutual information monotonically decreases. On the other hand, in the thesis, we performed a detailed analysis of timing side channel and showed that arbitrarily increasing the time bin width does not necessarily decrease the mutual information. It fluctuates as opposed to the monotonically decreasing behaviour shown in literature previously. Additionally, we revealed a characteristic of the mutual information, which is periodic fluctuation with respect to a parameter called start time of binning for a constant time bin width. Then, we continued with presenting the dependence of the mutual information to the uncertainty of a detector response and showed that decreasing the FWHM of a detector response increases the mutual information for a constant time difference between detectors' responses. Consequently, with this study, we demonstrate that three important parameters, time bin width, start time of binning and a comparison or the ratio between the FWHM and time difference between detectors' responses must be chosen carefully in order to prevent security loopholes caused

by experimental implementations. And before finalizing the chapter, we showed a method to introduce time shift between detectors' responses experimentally, which can be utilized by an illegitimate party for the purpose of creating a timing side channel.

For QKD systems to be deployable in real life, they need to be improved from an engineering point of view. This may include increasing the data exchange capacity of a system to meet the demands, identifying trade-off relations, making choices based on priorities and making tolerable compromises, or the simplification of system. Likewise, in the second part of the thesis, we focused on the improvement of raw key rate in a standardized E91 QKD system without compromising its security. Our method is to optimize photon budget allocation among three types of bits used in the system for different purposes or occurred unavoidably. These three types of bits were key bits, Bell's inequality bits and discarded bits and their ratios were 25%, 50% and 25%, respectively, in the proof-of-principle experiment. On the other hand, we presented 226.22% increase in raw key rate with 83%, 10% and 7% allocation of photon budget among three types of bits. These ratios were achieved by replacing 50 : 50 beam splitters with a 90 : 10 beam splitter at one communicating side and a 93 : 7 beam splitter at the other communicating side. In this way, we presented a study that will make the use of a standardized QKD system more effective. Before performing the optimization, as a required step, we showed that Bell's inequality parameter, S, used in the quantification of security can be written in terms of two independent random variables, and the propagation of uncertainty formula can be used in obtaining the probability distribution of S. Other than that, we reminded the effects of dead time, photon detection efficiency and dark count of a detector on photon counting process to the reader. We demonstrated that the optimum beam splitting ratios can vary depending on photon budget. Lastly, we presented another approach for photon budget optimization in a simplified system.

REFERENCES

[1] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Opt. Express*, vol. 15, pp. 9388–9393, Jul 2007.

[2] C. Paar and J. Pelzl, *The Data Encryption Standard (DES) and Alternatives*, pp. 55–86. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[3] W. Stallings, "The advanced encryption standard," *Cryptologia*, vol. 26, no. 3, pp. 165–188, 2002.

[4] H. Sahu, V. Jadhav, S. Sonavane, and R. Sharma, "Cryptanalytic attacks on idea block cipher," *Defence Science Journal*, vol. 66, pp. 582–589, Oct. 2016.

[5] V. Mavroeidis, K. Vishi, M. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, 03 2018.

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[7] F. Rubin, "One-time pad cryptography," *Cryptologia*, vol. 20, no. 4, pp. 359–364, 1996.

[8] R. Horstmeyer, B. Judkewitz, I. Vellekoop, S. Assawaworrarit, and C. Yang, "Physical key-protected one-time pad," *Scientific reports*, vol. 3, p. 3543, 12 2013.

[9] M. Barakat, C. Eder, and T. Hanke, "An introduction to cryptography." `https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf`, September 2018. Accessed: January 27, 2023.

[10] T. J. Shimeall and J. M. Spring, "Chapter 8 - resistance strategies: Symmetric encryption," in *Introduction to Information Security* (T. J. Shimeall and J. M. Spring, eds.), pp. 155–186, Boston: Syngress, 2014.

[11] D. Zhu, J. Zheng, H. Zhou, J. Wu, N. Li, and L. Song, "A hybrid encryption scheme for quantum secure video conferencing combined with blockchain," *Mathematics*, vol. 10, no. 17, 2022.

[12] I. R. Widiasari, "Combining advanced encryption standard (aes) and one time pad (otp) encryption for data security," *International Journal of Computer Applications*, vol. 57, pp. 1–8, 2012.

[13] A. Mink, X. Tang, L. Ma, T. Nakassis, B. Hershman, J. Bienfang, D. Su, R. Boisvert, C. Clark, and C. Williams, "High speed quantum key distribution system supports one-time pad encryption of real-time video - art. no.

62440m," *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 6244, 05 2006.

[14] Z. Chengxian, B. Guo, G. Cheng, J. Guo, and R. Fan, "Spin-orbit hybrid entanglement quantum key distribution scheme," *Science China Physics, Mechanics Astronomy*, vol. 57, pp. 2043–2048, 11 2014.

[15] L. Madsen, V. Usenko, M. Lassen, R. Filip, and U. Andersen, "Continuous variable quantum key distribution with modulated entangled states," *Nature communications*, vol. 3, p. 1083, 09 2012.

[16] C. Silberhorn, N. Korolkova, and G. Leuchs, "Quantum key distribution with bright entangled beams," *Phys. Rev. Lett.*, vol. 88, p. 167902, Apr 2002.

[17] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, 04 2009.

[18] W. Zhang, T. Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. Lim, and H. Weinfurter, "A device-independent quantum key distribution system for distant users," *Nature*, vol. 607, pp. 687–691, 07 2022.

[19] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[20] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[21] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.

[22] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992.

[23] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, p. 022317, Aug 2003.

[24] R. Kumar, F. Mazzoncini, H. Qin, and R. Alléaume, "Experimental vulnerability analysis of qkd based on attack ratings," *Scientific Reports*, vol. 11, 05 2021.

[25] E. Diamanti, "Security and implementation of differential phase shift quantum key distribution systems," 01 2006.

[26] F. Laudenbach, C. Pacher, C.-H. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation – the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, 03 2017.

[27] N. Lütkenhaus and M. O. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New Journal of Physics*, vol. 4, pp. 44 – 44, 2001.

[28] M. Curty and N. Lütkenhaus, "Intercept-resend attacks in the bennett-brassard 1984 quantum-key-distribution protocol with weak coherent pulses," *Phys. Rev. A*, vol. 71, p. 062301, Jun 2005.

[29] V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on sarg04, phase-time, dpsk, and ekert protocols," *Quantum Info. Comput.*, vol. 8, p. 622–635, jul 2008.

[30] B. Qi, C. Fung, H. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *Quantum Inf. Comput.*, vol. 7, pp. 73–82, 2007.

[31] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, pp. 686–689, 2010.

[32] B. Sprenger, J. Zhang, Z. H. Lu, and L. J. Wang, "Atmospheric transfer of optical and radio frequency clock signals," *Opt. Lett.*, vol. 34, pp. 965–967, Apr 2009.

[33] C.-Z. Wang, Y. Li, W.-Q. Cai, W.-Y. Liu, S.-K. Liao, and C.-Z. Peng, "Synchronization using quantum photons for satellite-to-ground quantum key distribution," *Opt. Express*, vol. 29, pp. 29595–29603, Sep 2021.

[34] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," 2016-04-28 2016.

[35] D. Micciancio and O. Regev, *Lattice-based Cryptography*, pp. 147–191. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[36] J. Ding and B.-Y. Yang, *Multivariate Public Key Cryptography*, pp. 193–241. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[37] D. Butin, "Hash-based signatures: State of play," *IEEE Security Privacy*, vol. 15, pp. 37–43, 01 2017.

[38] N. Sendrier and J.-P. Tillich, "Code-Based Cryptography: New Security Solutions Against a Quantum Adversary," *ERCIM News*, vol. Special Theme Cybersecurity, July 2016.

[39] R. A. Perlner and D. A. Cooper, "Quantum resistant public key cryptography: A survey," in *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, IDtrust '09, (New York, NY, USA), p. 85–93, Association for Computing Machinery, 2009.

[40] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin, "Strategies for achieving high key rates in satellite-based qkd," *npj Quantum Information*, vol. 7, pp. 1–7, 2020.

[41] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger, "Feasibility of 300km quantum key distribution with entangled states," *New Journal of Physics*, vol. 11, p. 085002, aug 2009.

[42] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012.

[43] Z. Zhuo-Dan, Z. Shang-Hong, D. Chen, and S. Ying, "Phase-encoded measurement device independent quantum key distribution without a shared reference frame," *Journal of Modern Optics*, vol. 65, no. 13, pp. 1529–1534, 2018.

[44] G.-Z. Tang, S.-H. Sun, H. Chen, C.-Y. Li, and L.-M. Liang, "Time-bin phase-encoding measurement-device-independent quantum key distribution with four single-photon detectors*," *Chinese Physics Letters*, vol. 33, p. 120301, dec 2016.

[45] Y. hua Lei and Y. Fu, "Measurement-device-independent twin-field quantum key distribution," *Scientific Reports*, vol. 9, p. 3045, 02 2019.

[46] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, "Higher key rate of measurement-device-independent quantum key distribution through joint data processing," *Phys. Rev. A*, vol. 103, p. 012402, Jan 2021.

[47] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Phys. Rev. A*, vol. 93, p. 042324, Apr 2016.

[48] R. RENNER, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 06, no. 01, pp. 1–127, 2008.

[49] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, "Security proof of quantum key distribution with detection efficiency mismatch," *Quantum Inf. Comput.*, vol. 9, pp. 131–165, 2009.

[50] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, "Security proof of practical quantum key distribution with detection-efficiency mismatch," *Phys. Rev. Research*, vol. 3, p. 013076, Jan 2021.

[51] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Information*, vol. 5, 12 2019.

[52] E. Biham, M. Boyer, P. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," *Journal of Cryptology*, vol. 19, pp. 381–439, 10 2006.

[53] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A*, vol. 74, 12 2005.

[54] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 75, p. 032314, Mar 2007.

[55] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," *Opt. Express*, vol. 18, pp. 27938–27954, Dec 2010.

[56] B. Mao, W. Hu, A. Althoff, J. Matai, J. Oberg, D. Mu, T. Sherwood, and R. Kastner, "Quantifying timing-based information flow in cryptographic hardware," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, ICCAD '15, p. 552–559, IEEE Press, 2015.

[57] B. Mao, W. Hu, A. Althoff, J. Matai, Y. Tai, D. Mu, T. Sherwood, and R. Kastner, "Quantitative analysis of timing channel security in cryptographic hardware design," *Trans. Comp.-Aided Des. Integ. Cir. Sys.*, vol. 37, p. 1719–1732, sep 2018.

[58] A. K. Biswas, A. Banerji, P. Chandravanshi, R. Kumar, and R. P. Singh, "Experimental side channel analysis of bb84 qkd source," *IEEE Journal of Quantum Electronics*, vol. 57, pp. 1–7, 2021.

[59] A. Duplinskiy and D. Sych, "Bounding passive light-source side channels in quantum key distribution via hong-ou-mandel interference," *Phys. Rev. A*, vol. 104, p. 012601, Jul 2021.

[60] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, p. 042333, Oct 2008.

[61] F. Xu, B. Qi, and H. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," *New Journal of Physics*, vol. 12, p. 113026, 2010.

[62] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, pp. 686–689, 2010.

[63] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system.," *Nature communications*, vol. 2, p. 349, 2011.

[64] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," *New Journal of Physics*, vol. 13, p. 113042, 2011.

[65] V. Makarov and D. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, pp. 691 – 705, 2005.

[66] A. Vakhitov, V. Makarov, and D. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of Modern Optics*, vol. 48, pp. 2023 – 2038, 2001.

[67] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, p. 022308, Aug 2013.

[68] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, p. 073024, 2011.

[69] J. Yin *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, pp. 501–505, 2020.

[70] D. Bruss, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, 05 1998.

[71] A. Rastegin, "On conclusive eavesdropping and measures of mutual information in quantum key distribution," *Quantum Information Processing*, vol. 15, 03 2016.

[72] SingleQuantum, "Photon detection with high time resolution." `https://singlequantum.com/technology/snspd/`. Accessed: January 27, 2023.

[73] IDQuantique, "Id281 superconducting nanowire series." `https://marketing.idquantique.com/acton/attachment/11868/f-023b/1/-/-/-/-/ID281_Brochure.pdf`. Accessed: January 27, 2023.

[74] Hamamatsu, "Silicon photomultiplier operation, performance & possible applications." `https://www.hamamatsu.com/content/dam/hamamatsu-photonics/sites/static/hc/resources/W0003/sipm_webinar_1.10.pdf`. Accessed: January 27, 2023.

[75] M. Stipčević, B. G. Christensen, P. G. Kwiat, and D. J. Gauthier, "Advanced active quenching circuit for ultra-fast quantum cryptography," *Opt. Express*, vol. 25, pp. 21861–21876, Sep 2017.

[76] J. Ma, M. Zhou, Z. Yu, X. Jiang, Y. Huo, K. Zang, J. Zhang, J. Harris, G. Jin, Q. Zhang, and J.-W. Pan, "High-efficiency and low-jitter silicon single-photon avalanche diodes based on nanophotonic absorption enhancement," 05 2015.

[77] E. Karimi, E. Soljanin, and P. A. Whiting, "Increasing the raw key rate in energy-time entanglement based quantum key distribution," *2020 54th Asilomar Conference on Signals, Systems, and Computers*, pp. 433–438, 2020.

[78] A. Dixon and H. Sato, "High speed and adaptable error correction for megabit/s rate quantum key distribution," *Scientific reports*, vol. 4, p. 7275, 12 2014.

[79] Z. Hua, Q. Dong xiao, F. Zhang, and C.-X. Pei, "Improving key rate of optical fiber quantum key distribution system based on channel tomography," *International Journal of Theoretical Physics*, vol. 52, 02 2013.

[80] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," *npj Quantum Information*, vol. 3, pp. 1–7, 2016.

[81] D. Bacco, J. Christensen, M. Usuga Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. Oxenlowe, "Two-dimensional distributed-phase-reference protocol for quantum key distribution," *Scientific Reports*, vol. 6, 06 2016.

[82] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, 05 2018.

[83] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, p. 031043, Aug 2018.

[84] J.-P. Chen *et al.*, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, 08 2021.

[85] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. Yuan, and A. J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nature Photonics*, vol. 13, pp. 334–338, 2019.

[86] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, p. 150501, Apr 2005.

[87] T. Honjo, S. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, "Long-distance entanglement-based quantum key distribution over optical fiber," *Optics express*, vol. 16, pp. 19118–26, 12 2008.

[88] M. Mafu, C. Sekga, and M. Senekane, "Loss-tolerant prepare and measure quantum key distribution protocol," *Scientific African*, vol. 14, p. e01008, 2021.

[89] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[90] D. Enzer, P. Hadley, R. Hughes, C. Peterson, and P. Kwiat, "Entangled-photon six-state quantum cryptography," *New Journal of Physics*, vol. 4, p. 45, 07 2002.

[91] M. Lucamarini, G. Vallone, I. Gianani, P. Mataloni, and G. Di Giuseppe, "Device-independent entanglement-based bennett 1992 protocol," *Phys. Rev. A*, vol. 86, p. 032325, Sep 2012.

[92] L. C. Alvarez and P. C. Caiconte, "Comparison and analysis of bb84 and e91 quantum cryptography protocols security strengths," *International Journal of Modern Communication Technologies and Research*, vol. 4, 9 2016.

[93] L. Li, H. Li, C. Li, X. Chen, Y. Chang, Y. Yang, and J. Li, "The security analysis of e91 protocol in collective-rotation noise channel," *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, p. 1550147718778192, 2018.

[94] A. Villar *et al.*, "Entanglement demonstration on board a nano-satellite," *Optica*, vol. 7, pp. 734–737, Jul 2020.

[95] K. Durak and M. Pahalı, "A system and method for quantum key distribution with entangled photon pairs," 01 2022.

[96] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, "Experimental quantum key distribution based on a bell test," *Phys. Rev. A*, vol. 78, p. 020301, Aug 2008.

[97] M. Fujiwara *et al.*, "Modified e91 protocol demonstration with hybrid entanglement photon source," *Optics express*, vol. 22, pp. 13616–13624, 06 2014.

[98] A. Parakh, P. Verma, and M. Subramaniam, "Improving efficiency of quantum key distribution with probabilistic measurements," *International Journal of Security and Networks*, vol. 11, p. 37, 01 2016.

[99] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New Journal of Physics*, vol. 11, 04 2009.

[100] M. Pahalı, K. Durak, and U. Tefek, "Cryptographic security concerns on timestamp sharing via a public channel in quantum-key-distribution systems," *Phys. Rev. A*, vol. 106, p. 012611, Jul 2022.

[101] J. Jogenfors, A. Elhassan, J. Ahrens, M. Bourennane, and J.- Larsson, "Hacking the bell test using classical light in energy-time entanglement-based quantum key distribution," *Science Advances*, vol. 1, pp. e1500793–e1500793, 12 2015.

[102] S. Meraner, R. Chapman, S. Frick, R. Keil, M. Prilmüller, and G. Weihs, "Approaching the tsirelson bound with a sagnac source of polarization-entangled photons," *SciPost Physics*, vol. 10, 01 2021.

[103] W. Rosenfeld, M. Weber, J. Volz, F. Henkel, M. Krug, A. Cabello, M. Zukowski, and H. Weinfurter, "Towards a loophole-free test of bell's inequality with entangled pairs of neutral atoms," *Advanced Science Letters*, vol. 2, 12 2009.

[104] M. S. Rzeszotarski, "The aapm/rsna physics tutorial for residents," *RadioGraphics*, vol. 19, no. 3, pp. 765–782, 1999. PMID: 10336202.

[105] D. Wang, A. Gauthier, A. Siegmund, and K. Hunt, "Bell inequalities for entangled qubits: Quantitative tests of quantum character and nonlocality on quantum computers," *Physical Chemistry Chemical Physics*, vol. 23, 01 2020.

[106] K. D. Jöns, L. Schweickert, M. A. M. Versteegh, D. Dalacu, P. J. Poole, A. Gulinatti, A. Giudice, V. Zwiller, and M. E. Reimer, "Bright nanoscale source of deterministic entangled photon pairs violating bell's inequality," *Scientific reports*, vol. 7, p. 1700, May 2017.

[107] J. G. Rarity and P. R. Tapster, "Experimental violation of bell's inequality based on phase and momentum," *Phys. Rev. Lett.*, vol. 64, pp. 2495–2498, May 1990.

[108] J. Tang, Q. Zeng, Y. Zhang, and T. Qiu, "Some major studies in experimental verifications of bell inequality," *Journal of Physics: Conference Series*, vol. 2230, p. 012003, mar 2022.

[109] X. Ma, A. Qarry, J. Kofler, T. Jennewein, and A. Zeilinger, "Experimental violation of a bell inequality with two different degrees of freedom of entangled particle pairs," *Physical Review A*, vol. 79, p. 042101, 2009.

[110] H.-X. Lu, L.-Z. Cao, J.-Q. Zhao, Y.-D. Li, and X.-Q. Wang, "Extreme violation of local realism with a hyper-entangled four-photon-eight-qubit greenberger-horne-zelinger state," *Scientific reports*, vol. 4, p. 4476, 03 2014.

[111] M. Pahalı, K. Durak, and U. Tefek, "Optimal photon budget allocation in E91 protocol," 12 2022.

VITA

2018 - 2022	PhD, Dept. of Electrical and Electronics Eng., Özyeğin University, Turkey
2014 - 2017	MSc, Dept. of Physics Eng., Istanbul Technical University, Turkey
2013 - 2014	Scientific Preparation for the MSc, Istanbul Technical University, Turkey
2004 - 2009	BSc, Dept. of Meteorological Eng., Istanbul Technical University, Turkey