



**Analysis and Evaluation of Quantum Key
Distribution Protocols**

By

Reza Rouhani

A thesis submitted in partial fulfilment of the
requirements for the degree of Master of Computing

Supervisor: Bahman Sassani (Sarrafpour)

Unitec Institute of Technology, 2020

Abstract

Quantum Key Distribution (QKD) which is the name of cryptography in quantum environment act as the highest developed area in quantum communication and computing technology (QCIT).

QKD is inventive technology which utilize the laws of quantum to create a cryptographic share key to make the communication system secure. The unique feature of QKD assures eavesdropping detectable during quantum communications which is fascinating for a high-level secure environment.

Most of the traditional cryptographic methods which we use currently are based on mathematical scheme or Computational complexity theory which are not completely safe. Using quantum cryptography has been achieved extensive steps in communication security establishment. As the information Unit has been changed from "bit" to Quantum bit (Qubit), a new element has been offered that can guarantee the shared information confidentiality between parties. The confidentiality of system is established via exchanging a secret key through a channel of quantum, the key which we use for encrypting the shared data. This structure has quantum integration which has been developed by physics law and techniques of cryptography.

This thesis has proposed a modified version of QKD protocol, this new protocol will generate a cryptographic share key for a more efficient, lower cost and secure communication between two parties (sender and Receiver). This new protocol principal is similar to BBM92, but the source of photon moved to sender instead of third-party photon generator, following steps will be executed in this Experiment:

- Observe different categories protocols of QKD in details
- The Quantum Mechanics Visualisation Project (QuVis) is the simulation software that has been used for implementing the proposed protocol [BB84 with spin] among the other three (BBM92, B92 and BB84).
- Probability ratio of error will be tested and compared for all protocols, for this experiment 100 to 5000 photons will be sent.

By Analysing collected data in this experiment, it will be determined which one of this four protocols lead the detecting of eavesdropping. Simulation software accomplishes the value of error key probability which receiver can use and should not pass over the range limit of 0.25 & 0.5.

Keywords:

Protocols of QKD, Quantum Cryptography, Distribution Key, Cybersecurity, QuVis, BB84, E91, B92, BBM92.

Acknowledgments

I would like to take this opportunity to express my sincere gratitude to Mr. Bahman Sassani (Sarrafpour) My Supervisor for his invaluable guidance and support. His vision, encouragement, patience, and support are valuable sources in my academic journey and in developing my professional skills.

Also, I would like to Thank to Mr Sam Kolahi my Co-supervisor and all the members of staff at Unitec Institute of Technology who helped me during my time here at Unitec.

Special thanks to UK Institute of Physics and the University of St Andrews for funding the QuVis simulation development and providing it for the learning and teaching of quantum mechanics concepts.

Reza Rouhani

Unitec Institute of Technology
January 2020

List of Figures

Figure 2.1 bit (a) and qubit (b). [12]	4
Figure 2.2 Process of coding & decoding. [12]	6
Figure 2.3 QKD main block diagram [31]	8
Figure 2.4 QKD model illustration. [12]	8
Figure 2.5 Eavesdropper effect on channel of quantum. [12].....	9
Figure 2.6 BB84 Polarization Basis [31]	11
Figure 2.7 BB84 Protocol Illustration of quantum exchange processes [31].....	11
Figure 2.8 BB84 Protocol Implementation on Details [31]	12
Figure 2.9 Polarization basis of BB84. [31]	13
Figure 2.10 Entanglement based QKD basic concepts [31]	13
Figure 2.11 Sphere of Poincare [31]	14
Figure 2.12 DPS design pattern [42]	15
Figure 2.13 Scheme of COW [35].....	166
Figure 3.1 BB84 Result of 100 to 1000 Photons experiment [26]	18
Figure 3.2 B92 result of 100 to 1000 Photons experiment [26]	19
Figure 3.3 Comparison of each protocol N key [31]	21
Figure 3.4 Comparison of N Error Value for each Protocol [31].....	22
Figure 3.5 Value Comparison of N Error/N Key value (Probability Error) on each Protocol [31]	22
Figure 5.1 Sample QuVis Simulation QKD Quantum Environment for BB84 Protocol	277
Figure 6.1 BB84 Np Comparison of Current Evaluation vs Rambu & Rachmana.....	36
Figure 6.2 B92 Np Comparison of Current Evaluation vs Rambu & Rachmana	37
Figure 6.3 Value Comparison of Np value Protocol from Ali Ibnun and Nana Rachmana	41
Figure 6.4 Value Comparison of Np value Protocol in range of 2000 Photons from current experiment.	42
Figure 6.5 N Key Value Comparison of BB84, B92, BBM92 and BB84 with Spin $\frac{1}{2}$ Protocol	45
Figure 6.6 Ne Value Comparison of BB84, B92, BBM92 and BB84 with Spin $\frac{1}{2}$ Protocol.....	46
Figure 6.7 Ne/ Nk Value Comparison of BB84, B92, BBM92 and BB84 with Spin $\frac{1}{2}$ Protocol	48
Figure 6.8 the Entangled States submitted by third party. [44]	49

List of Tables

Table 2.1 QKD Protocols Details [31]	17
Table 3.1 BB84 and B92 error probability ratio [26].....	19
Table 3.2 Simulation results of key and error [31]	21
Table 5.1 Experiment data collection 1 results	28
Table 5.2 Experiment data collection 2 results	29
Table 5.3 Experiment data collection 3 results	30
Table 5.4 Experiment data collection 4 results	31
Table 5.5 Experiment data collection 5 results	32
Table 5.6 Experiment average data collection results.....	33
Table 6.1 BB84 and B92 Error Probability ratio [3].....	34
Table 6.2 Correct data evaluation of NP for B92 protocol.....	35
Table 6.3 Evaluation data results for 1000 photon number for BB84 and B92 protocols.....	35
Table 6.4 Summary of Np value comparison between current evaluation vs Rambu and Rachmana	38
Table 6.5 Simulation results of key and error from Ali Ibnun and Nana Rachmana	39
Table 6.6 Recalculated NP value of Ali Ibnun and Nana Rachmana Evaluation	40
Table 6.7 My evaluation data simulation results of protocols in 2000 photon range (Current experiment).....	40
Table 6.8 Summary of Np value comparison between current and Ali Ibnun and Nana Rachmana	43
Table 6.9 Experiment average data Collection Results of Current Experiment.....	44
Table 6.10 Nk Value comparison summary	46
Table 6.11 Ne Value comparison summary	47
Table 6.12 Np Value comparison summary	48

List of Acronyms

Alice: The party transmitting a secret key	1
BBM92: Bennet 1992 protocol	1
Bob: The party receiving a secret key	1
COW: Coherent One-Way	16
DPS: Differential Phase shift	15
EB: Entanglement Base QKD scheme	10
Eve: A hypothetical eavesdropper	2
FIFA: Fédération Internationale de Football Association	7
HTML5: Hypertext Markup Language Revision 5	26
Ks: Initial generated key	8
MPTL:Multimedia Physics Teaching and Learning.....	26
NE: Number of Error Key	20
NK: Number of generated Key	20
NP: Number of probability Key (Ne/Nk)	20
P&M: Prepare and measure QKD scheme	9
QKD : Quantum Key Distribution	ii
Qubit: Quantum Bit	ii
QuVis: The Quantum Mechanics Visualisation Project.....	ii
S13: Eduin H. Serna introduced S13 in 2013	16
SARG04: Scarani presented SAEG04 in 2004	10
SSP: Six-State Protocol	14

Table of Contents

Abstract	ii
Acknowledgment	iii
List of Figures	iv
List of Tables	v
List of Acronyms	vi
Chapter 1-Introduction	1
1.1 Introduction.....	1
1.2 Problem Statement	1
1.3 Thesis Overview	2
1.4 Motivation.....	2
1.5 Research Contribution.....	3
Chapter 2-Quantum Computing	4
2.1 Quantum Computing.....	4
2.2 Quantum Cryptography	5
2.3 Quantum Key Distribution	7
2.4 Advantages of QKD.....	8
2.5 QKD's Limitations	9
2.6 QKD's Structural Design	10
2.6.1 P&M Type	10
2.6.2 EB Type.....	10
2.7 QKD's Protocols.....	10
2.7.1 BB84	10
2.7.2 E91	13
2.7.3 BBM92	14
2.7.4 B92	14
2.7.5 SSP.....	14
2.7.6 DPS	15
2.7.7 SARG04	15
2.7.8 COW	16
2.7.9 S13	16
Chapter 3-Literature Review	18
3.1 Related Previous Evaluation of QKD Experiment	18
3.1.1 Rambu and Rachmana QKD Evaluation Experiment (2018)	18
3.1.2 Ali Ibnun and Nana Rachmana QKD Evaluation Experiment (2018).....	20

Chapter 4-Methodology	24
4.1 The Methodology	24
4.2 Implementation Methodology	24
4.3 Experimental Metrics	25
Chapter 5-Evaluation and Data Collection Process.....	26
5.1 QuVis Software.....	26
5.1.1 About QuVis	26
5.1.2 QuVis Awards.....	26
5.2 Evaluation.....	27
5.3 The Results	28
5.3.1 Data Collection 1.....	28
5.3.2 Data Collection 2.....	29
5.3.3 Data Collection 3.....	30
5.3.4 Data Collection 4.....	31
5.3.5 Data Collection 5.....	32
5.3.6 Average Value of Collected Data	33
Chapter 6- Analysis, Discussion and Comparison	34
6.1 Comparison with Beatrix Rambu and Nana Rachmana Evaluation.....	34
6.1.1 Probability Key value comparison for BB84 protocol between Current Evaluation vs Rambu and Rachmana Experiment.....	36
6.1.2 Probability Key value comparison for BB84 protocol between Current Evaluation vs Rambu and Rachmana Experiment.....	37
6.2 Comparison with Ali Ibnun and Nana Rachmana Evaluation (2000 Photon range for BB84, B92 and BBM92 Protocols)	39
6.2.1 Np value comparison between Current Evaluation vs Ali Ibnun and Nana Rachmana Experiment (BB84, B92 and BBM92 Protocols).....	41
6.3 Simulation and Results of Current Experiment.....	43
6.4 Generated Keys of Simulation Results (Average Value of Data Collection).....	44
6.5 N Key Value Comparison	45
6.6 N Error Value comparison	46
6.7 N Error / N Key (Np) Value comparison	47
Chapter 7- Conclusion and Future review.....	50
7.1 Summary	49
7.2 Conclusion	50
7.3 Future Review	51
References	52

Chapter1

Introduction

1.1 - Introduction

Imagine that the complex mathematical issues that cannot be solved even by the current fastest supercomputers, can be solve in a blink of an eye by a computer. This is one of the quantum computer characteristics [1]. The design of the quantum computers makes them able to use quantum physics laws to work, the power of processing of this computer are significantly higher than conventional computers. Quantum computers have the capacity of Analysing the large scale of data processing such as the process of high-resolution image for artificial intelligence applications which is almost impossible to perform by normal computers [2].

So the question is if the quantum computer can be a significant milestone in Scientific Human progress? [3] .By the beginning of quantum physic, large number of new fields have been opened for exploration and improvement in the technology and science world [4].

In regular computers, electrical currents are recorded as the numbers of 0 and 1 on tiny electronic circuits. So, if an electrical current is carried by circuit carries it is considered as 1, and it is expressed as 0 when no electrical current carry by circuit. Meanwhile there are 3 different combination of states in quantum computing which are: state (0), state (1) and the third state is the state of (0 and 1). Superposition is the name of this form in quantum physic which is defined as “Qubit” or “Quantum Bit”. This format cannot be changed from the outside by taking energy. The information can be transformed by changing the electrons spin orders by quantum computers working based on this principle.

The researchers have developed the first quantum processor at the South California University which this can be an example of the most up-to-date quantum computing. Microsoft and IBM also have provided their virtual quantum simulation environment for researcher to use [2].

1.2 - Problem Statement

Current quantum protocols have some issues such as complexity and very high cost of installation and setting of Instruments and devices, Therefore, the major motivation will be proposing more effective, simple, efficient, lower cost with less equipment setup protocol. This new method of the proposed protocol will help parties to develop a key securely using single spin $\frac{1}{2}$ particle model, which Alice sends to Bob instead of having a pair of particles generated from the third-party source. The main advantages of this protocol are higher level of efficiency and lower cost of equipment setup. By completing the evaluation and analysing of four protocols (BB84, B92, BBM92 and BB84 with spin) this thesis will have the answers for following questions:

- What could be the differentiation between selected protocols of BB84, B92, BBM92(existing protocols) and BB84 with spin (proposed protocol) in working process such as Key Generating?
- Which one of the protocols generates the higher value of keys? The higher generated key makes the protocol better.
- Which one comes up with less error probability? The less errors determine better profile.
- How the efficiency of current protocols can be improved?
- What are the ways of reducing the cost of equipment and instruments setup?

For this experiment the QuVis simulator software has been used by Implementing 4 protocol in simulator environment.

Eve will be added into this experiment as Eavesdropper to develop the experiment.

1.3 - Thesis Overview

The main structure of this thesis will be as follows:

Chapter 1: Describes general information about quantum computing then discloses my motivation to improve the existing methods of QKD protocols.

Chapter 2: Reviews the quantum computing environment such as its structure design, key distribution, and existing protocols.

Chapter 3: This chapter will review some related previous evaluation experiments.

Chapter 4: Explains the methodology and implementation methodologies that have been used for this research.

Chapter 5: Contains all the collected data also explains QuVis simulation environment.

Chapter 6: In first part of this chapter the analysis, discussion, and comparison of previous experiment with current one with same range of sent photon number has been performed. Then the analysis of current experiment has been presented.

Chapter 7: Concludes the thesis along with future directions for the research.

Acronyms List

References

1.4 - Motivation

The Importance of security protocol in communication is increasing Everyday these days, e.g. for communication over the internet. QKD gives parties (Alice & Bob) the ability of generating secret key sequences of zeros and Ones that can be known only by parties. Both parties never can be sure about the security of their communication as there is a possibility of compromising of the communication by eavesdropper. Quantum computing however makes the communication totally secure. By applying quantum fundamental, parties can detect eavesdrop presents by observing the errors in their measurement of polarization basis [5].

So the differences between Classical and Quantum Cryptography are as below:

Classical Cryptography: Classical cryptography is based on the mathematics and it relies on the computational difficulty of factorizing large number. The security of classical cryptography is based on the high complexity of the mathematical problem for the instance factorization of large number.

Quantum Cryptography: Quantum Cryptography is based on physics and it relies on the laws of quantum mechanics. It is arising technology which emphasizes the phenomena of quantum physics in which two

parties can have secure communication based on the invariability of the laws of the quantum mechanics [6].

The main concern when it comes to quantum protocols are the complexity and very high cost of installation and setting of Instruments and devices to apply them, Therefore, my major motivation will be proposing a protocol with more effective, simple, efficient, lower cost with less equipment setup protocol. This new method can be created by modifying one of the existing protocols, BBM92, by moving the photon generator's source to the sender instead of using a third-party photon generator. This modification will reduce the cost of using third party, setting up the connection tools and network between the third party and Sender, creating more efficiency in cost, more control on the network and security; so in general the aim is

- a) Improving the Np value of BBM92 protocol by using the proposed protocol of BB84 with Spin $\frac{1}{2}$.
- b) reducing the cost of devices and network implementation.

Which with this new proposal protocol the cost will reduced to almost half of the cost of implementation of BBM92 protocol. the proposed protocol will help parties to develop a key securely using single spin $\frac{1}{2}$ particle model, which Alice sends to Bob instead of having a pair of particles generated from the third-party source. The main advantages of this protocol are higher level of efficiency and lower cost of equipment setup.

1.5 - Research Contribution

Now that we know how important the quantum computing is, the achievements of this research and thesis are as follows:

- The main contribution of this research is Innovating a simplified low cost but effective QKD protocol.
- Reviewing the concept of QKD protocols error ratio comparison from a new perspective. So far most studied experiment by sending maximum 2000 Photon, in this thesis 500 photon has been sent.
- Helping to improve quantum cryptography protocols system.
- This research outputs might Assist the future researchers to have a hand on more information and data as there are not many resources available regarding QKD protocols.
- Providing an overview of a developed software simulations called QuVis to other researcher or students.
- Helps students to learn the fundamental of QKD protocols principles of four model of protocols.
- This thesis opens a window to other student, teach and explain them the process of generating a raw key in QKD system.
- This thesis will show the effect of the eavesdropper penetrating during the process of observation.

Chapter 2

Quantum Computing

2.1 – Quantum Computing

Security of information generally is depending on expectations of how long the information will continue to be secure and private for a duration of time [7]. There is a secure network communication need in many different areas such as science, defence, development and Information system which can be provided by QKD [8]. In the late 19th century, foundation of quantum world was laid down with the introduction of Max Planck and black body radiation. In 1905, Albert Einstein discovered the concept of photons [9]. Our successful understanding of quantum computing in last 35 years declared its feature as a new and innovative technology in computing [10].

The Latin word “quantum” has the meaning of “some quantity”. Quantum mechanics is one of the mathematical systems of the physical world [11]. Quantum computing using quantum mechanics features like entanglement, superposition and quantum interference to provide completely secure communication protocols and efficient computation algorithms [12]. The quantum mechanics has started playing a critical role in computing and communication fields [13].

Those computers which use quantum mechanics principles like super-position and quantum - entanglement, applying more complicated data unit called Qubit. In terminology of conventional computer, one qubit can express value of one, zero or the superposition of zero and one together [14]. In a situation in general, (n) classical bits can only show (2^n) type of information per time, meanwhile the (n) qubits can show entire information at the same time [15].

Figure 2.1 illustrates a Qubit.

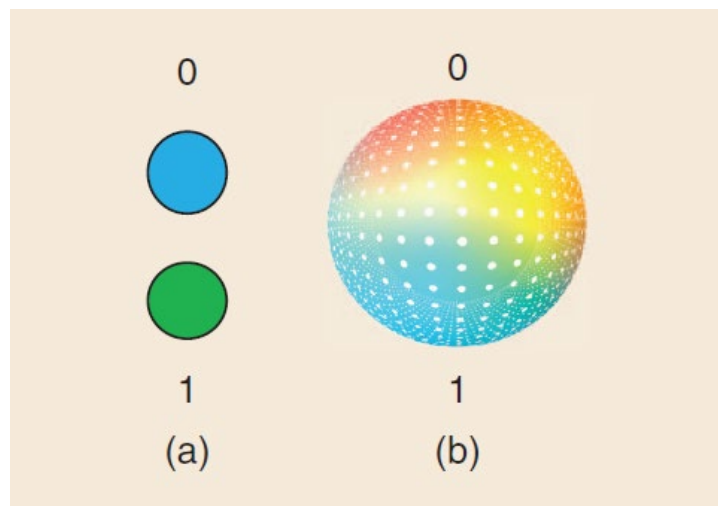


Figure 2.1 bit (a) and qubit (b). [12]

When it comes to computing, a quantum computer can proceed many (ones) and (zeros) combinations at a very high speed simultaneously. However, currently quantum computers use quantum annealing (multiple variables) to find the best problem solution, in fact this is only a subdivision of a quantum computer abilities [13]. A real quantum computer has already existed as many of giant technology are racing to achieve goal [12]. One of the challenges in quantum computing will be the improvement of functional memory in quantum computing in future. Several comprehensive research proposals have been demonstrated with different quantum model of memory [14].

When we consider the possibilities of the quantum computing in future, from the point of view it will affect the deep mankind culture in many areas as it is an unknown technical frontier.

Whenever technology move forward through the unknown, intelligent and smart people will discover some uses which were beyond the previous imagination [16].

If we put the theory aside and focusing on quantum computing application in the real world, we will see that the quantum computing will have major impact on human life in future and will open a new age in human history in many different fields such as:

Climate and weather modelling: With quantum computing the scientists can forecast the patterns of weather perfectly to generate more accurate climate predictions in long term, this day we get poor data collection in weather as the supercomputers process sometimes effected by many variable environmental.

Personalizing the medicine: Decoding the human DNA is critical for doctors in the future to make the drugs that work for human body perfectly.

Exploration of space: Amount of collected data from the space, stars, and planets and so on by telescopes these days are too much for supercomputers to sift and make through discoveries. but with a proper quantum computing and using machine learning, these data can be efficiently processed.

Elementary Sciences: The power of raw computing of quantum computers will help engineers and scientist to develop new materials and chemicals.

Machine Learning: For learning new skills by traditional computers the algorithms of machine learning need a huge amount of assistant data, but quantum computers machine learning software can learn very similar to human and picking up new skills with less amount of data [17].

2.2 – Quantum Cryptography

By the time that Steven Wiesner wrote the “ Conjugate Coding” paper in early seventies, the quantum cryptography was born for the first time, It took him more than ten years to complete the paper [18], his paper did not get that much attention by that time, however when a classic paper was published by Charles Bennett and Gilles Brassard In 1984, that received a great attention for the topic. There was a prediction by scientist that the quantum computer will have the ability of cracking the public key classical cryptography one day [19].

Cryptography is the art of making communication and data secure among two parties even if an adversary exists [20]. Any type of data has different specific feature, so that’s why These data required individual type of cryptographic methods [21].

Traditional cryptography is very clever, but according to methods of encoding in history of code-breaking, it is being phased out. Quantum cryptographies provide secure communication by using quantum mechanics. It enables both parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. By harnessing the unpredictable nature of matter at the quantum level, physicists have figured out a way to exchange information on secret keys. Attaching information to the photons spin is the essence of Quantum Cryptology. In brief, the processes of encoding (cryptography) and decoding (crypto analysis) information or messages (called plaintext) into an otherwise meaningless data (cipher text) combined are cryptology. And when the keys used for this process are photons, it is called Quantum Cryptology. [22]

Cryptography in quantum domain provide us a different system of safe and secure data communication comparing it with current cryptography methods. Quantum Cryptography uses QKD system which we will review it in Detail in next section [23]. The classical cryptography algorithm that we use now days will break down when facing quantum cryptosystem [24].The cryptography aims transmitting data in a unique way which only recipient have access to that data, even though if any other received that data [25].

The key principle is that two recipients who want to have secure communication will agree upon an encryption (encoding) and decryption (decoding) data methods. Once the method is chosen, then secret key can be shared (encryption key) by communicators that can be used for encrypting and decrypting as shown by Figure 2.2.

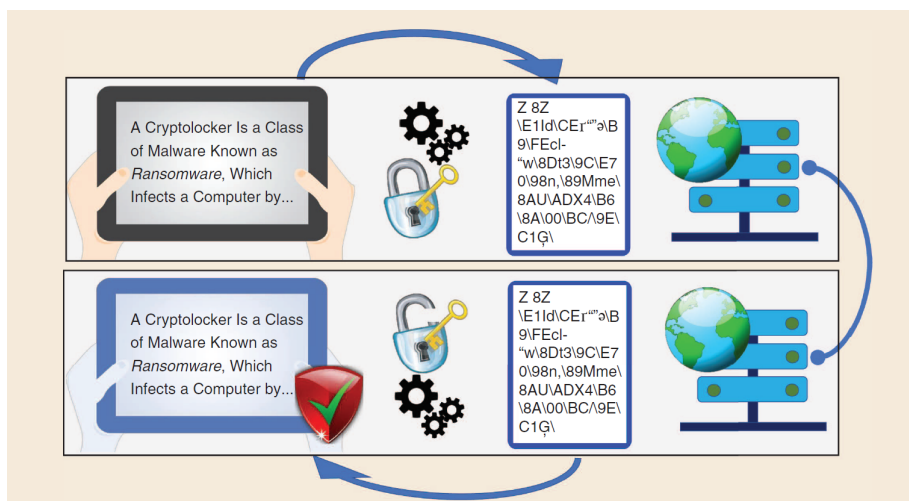


Figure 2.2 Process of coding & decoding. [12]

Following Two facts:

1-Algorithm method used for data encryption-decryption

2-The secret key size

are the main facts that establish the strength of the system security.

This is how the information confidentiality works, first step is the encryption of information or message before sending it to both parties with secret key which both known. How safe will be the secret key within the classical exchange process is our problem here, process, as the matter of fact we cannot be sure that the exchange key process is completely secure. Quantum mechanics is the method than can be apply for key distribution security.

Protocols are the information carrier which involves parties during a communication. Quantum protocols using light properties to carry secret key's information in quantum mechanics, the light nature cannot be duplicated and is very hard to be modified based on superposition result [26].

As an example of one of the first link of encryption fibre quantum we can refer to implementation of this technology in South Africa during the FIFA world cup on 2010, The purpose of setting this system was to provide the security of information and data transmission between the main hub and the Moses Mabhida stadium [27].

2.3 – Quantum Key distribution

Key distribution is one of the most fundamental fact in cryptography, which is a protocol that creates and form a secret shared key between parties who don't have any secret common key, or they have only a small seed initial key [28]. Most sophisticated and developed cryptography application in quantum is the QKD which is indicated an evolutionary mechanism that generates unconditional shared cryptography key security for parties who are physically separated [29]. By using QKD protocols a secret key can be shared by two parties in a complete confidentiality, even if there is an eavesdropper [30].

QKD is a high developed technology in quantum cryptography environment. QKD uses the quantum mechanics models unlike the regular algorithm of cryptography which is depends on mathematics complexity facts for its strength security basis, it has been determined that QKD is able to deliver unconditional security in theory. Figure 2.3 is illustrated the diagram of QKD basic block [31]. The principle of Heisenberg inaccurate and un-clone theory of quantum are two elementary quantum physics properties which they guaranteed the quantum cryptography security [25]. The uncertainty principle (also known as Heisenberg's uncertainty principle) was Introduced in 1927 for the first time by the Werner Heisenberg the German physicist, this principle states that the more precisely the position of some particle is determined, the less precisely its momentum can be predicted from initial conditions, and vice versa [32].

According to nature of quantum communication mechanics, any examination of a quantum state, will collapse its state, so the eavesdropping detection is possible in quantum channel. This attribute makes QKD suitable for achieving a higher level of security application in areas such as government, banking and military fields [29].

As it shown in Figure 2.3 there are two channels in QKD system, public channel, and quantum channel. Transmission and sharing the secret key information which is in the form of qubit uses the quantum channel. To discuss the qubit transmission process, we use the public channel. In general, there are two forms of channels in quantum that can be applied on QKD. One is the fibre optical; the other is free space. Sender (Alice) and Receiver (Bob) and Eavesdropper (Eve) are the identity names that we use in QKD scheme [31].

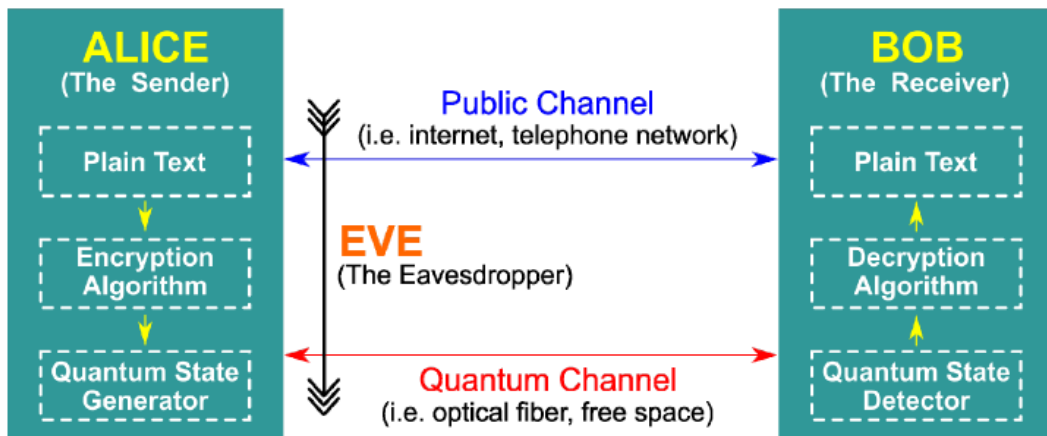


Figure 2.3 QKD main block diagram [31]

2.4 - Advantages of QKD

As we mentioned earlier for secure sharing secret keys or encryption keys, the QKD can be used in the form of qubit over a channel of quantum. This operation is secured by the Heisenberg principle of the uncertainty, that declare that is not possible accurate examine the momentum and position of a particle simultaneously. Based on this principle, even with ideal techniques and instrumentation, the calculation of atomic momentum for a particle is uncertain. QKD's security is established by creating a total secure technique of distribution key, as Figure 2.4 is illustrated [12].

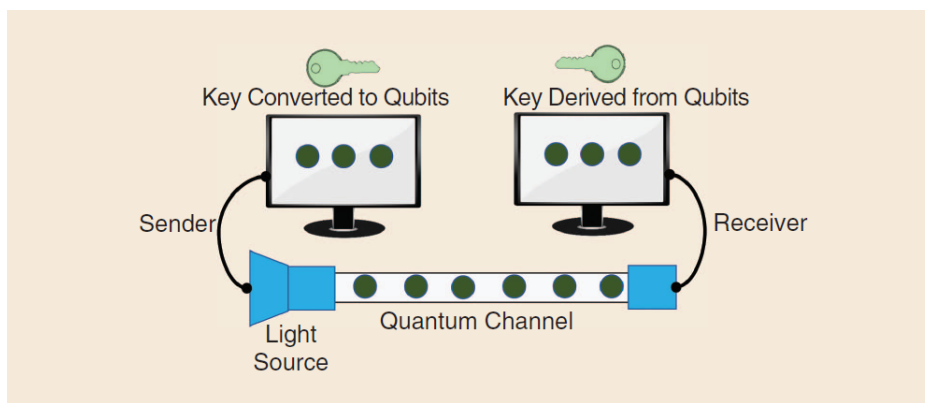


Figure 2.4 QKD model illustration. [12]

As an Example, if parties wish to transfer information securely, Alice need to generate a secret key(K_s) initially, using random numbers. The length of secret key (bit) is vary, the encryption's strength directly depends on key length. Once created, secret key can be converted now to qubit, which can be transmitted via quantum channel. If this channel interrupted by any intruder, like Eve, to steal or eavesdropping the key, an error will be created which changes the transmitted data's state unintentionally according to Heisenberg's principle of uncertainty, Figure 2.5 illustrated the effect of eavesdropper on quantum channel [12].

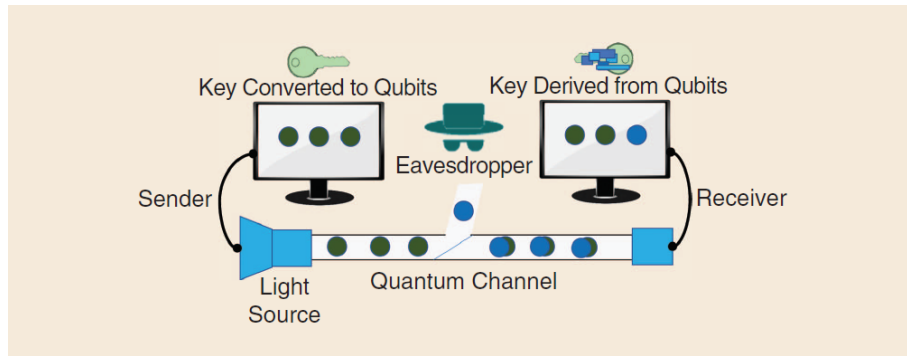


Figure 2.5 Eavesdropper effect on channel of quantum. [12]

Bob the receiver can detect the errors or changes which has been generated by eavesdropper in the form of error transmission. Once the secret key verification is completed then is useable for encryption of data to send and receive the data via classical public channel securely. If Alice detecting any transmission error, the secret key received by Alice will be dropped straight away, Alice will request Bob to restart the key transmission process. However, there is a concern when the secret key is establishing as Eve might still attempting on eavesdropping. On the other hand, as there is no perfect implementation, transmission process might be affected by different natural environment disruptions like noise which can cause error on transmission. Secret-key filtration has been used in this specific case for making a new Key. This can be established by bits error rates calculation; this can deduct the amount of information that Eve might have known. Then recipients (Alice & Bob) can extract a new Ks by using the remaining bits of information [12].

2.5 - QKD's Limitations

If we investigate the quantum information processing, the principal rules of representing the information are completely different than the classical processing system [33].

As we mentioned before, QKD can guaranteed the security of initial exchange secret key. Security strength depends directly on algorithm complexity and key length. Although QKD cannot be interfered or change, it still can be arbitrating if is not properly setup. Below are few different QKD aspects which should be considered:

- 1) The secure channel provided by QKD is not for encryption, then we must use a strong strength secret key. Type of algorithm that we use for encryption–decryption process must also be unbreakable by the existing technology.
- 2) Proper setting is essential for the equipment we use to transmit the secret key. If this equipment causes any change or errors in transmission process, then recipient (Alice & Bob) will continue discard and eliminating secret key.
- 3) Secret Key (Ks) must be kept safe by involved parties (Alice & Bob) in process of exchange to avoid impersonating one of them by Eve.
- 4) To provide a true secret key (Ks) a complete random number must be used by the seed value for generating Ks [12].
- 5) The other challenge that researchers have to face it, is developing of optical devices to be able to generate and detect the single photon, Not expensive devices for commercial territory [34].

2.6 - QKD's Structural Design

QKD Schemes can be classified as two main types, Prepare and Measure (P&M) and Entanglement-Based (EB) designs. P&M model has designed use single qubit and EB type is based on entangle pairs of qubits. Both parties can use either schemes to generate and establish a Key. There are another group of protocols which are based on [coherent-one-way] protocol. This thesis will briefly explain the process of each scheme in the following sections [35].

2.6.1 - P&M Type

With this design, data information encoded to a series states by Alice for example and sent them to Bob through a quantum channel. Then Bob execute measurements of the received states. These results can be shared in data channel which is created by quantum between parties (Alice & Bob). BB84, B92, SARG04 and six-state are some examples of protocols which are using this scheme [35].

2.6.2 - EB Type

This principle is one of the essential quantum principles. Two particles can be entangled on the way that if the property of one particle is measured, the state of opposite particle will be changed simultaneously [36].

This method uses a source of photon generator which creates an entangled quantum state and distributes to Alice and Bob. Then both parties execute measurements on their system. During the process of measurement, they will collect perfect mutual corresponded conclusion which are totally random. As the state prepared by third party source, eavesdropper will not be correlated with this state. This indicates secrecy of key. E91 protocol uses this scheme [35].

2.7 - QKD Protocols

To explain the mechanism of how protocols of QKD work, we need to describe the theory of observing qubit [37]. According to theory of no-cloning, Qubit cannot be amplified or copied without affecting its state. This unique system makes QKD able to identify the eavesdropper existence by measuring error key parameter, these parameters come into sight during the photon transmission process between Alice & Bob [31]. Despite of massive improvement for QKD, Still some problems are exist in theory, regarding complete secure communication under an eavesdropper's observation [38].

This chapter will review nine different QKD protocol which five of them are P&M based and the other four using EB based of QKD protocols [31].

2.7.1-BB84

Bennett and Brassard proposed this protocol in 1984, with the aim of providing two parties the ability of sharing secret key when using quantum mechanics principles like Heisenberg's principle of uncertainty. BB84 is first protocol cryptography of quantum which described the process of using state of polarization photons to carry the secret key information via a quantum transmission channel.

BB84 protocol can be classified under P&M category of QKD protocol [31]. BB84 can be recognized physically by two level of quantum structure and four states of polarization that use for coding [39].

This protocol is using an individual photon to carry and distribute secret key bits randomly. This single photon has the polarization of four different states using one of the two rectangular and diagonal bases, these polarization bases are shown in Figure 2.7 [31].

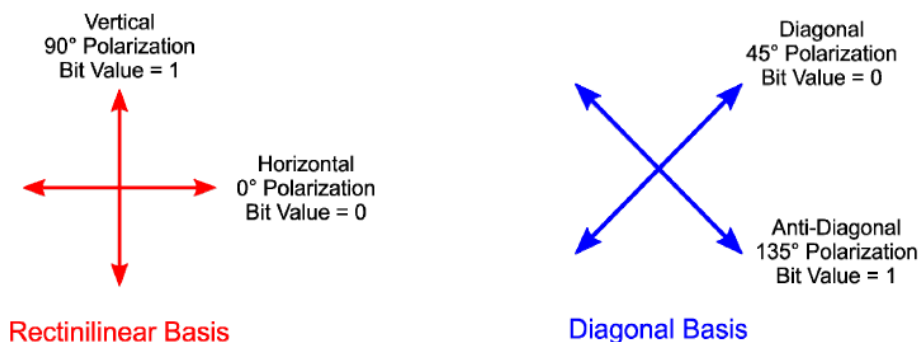


Figure 2.6 BB84 Polarization Basis [31]

Figures 2.8 and 2.9 describe the processes in more details. [31]

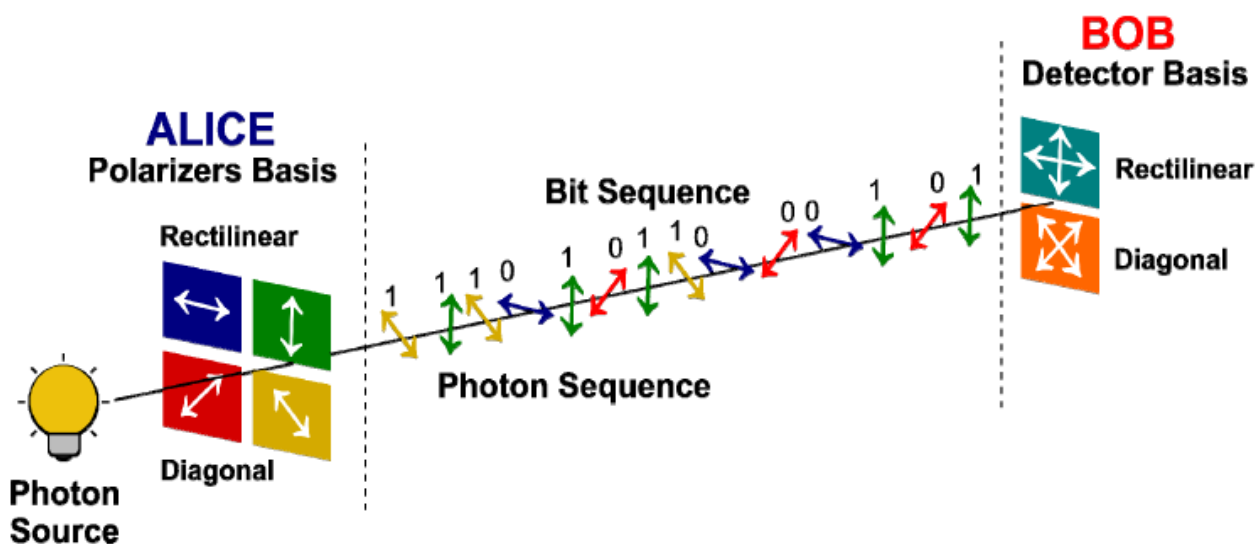


Figure 2.7 BB84 Protocol Illustration of quantum exchange processes [31]

Quantum Exchange															
Alice's random bit	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1
Alice's random basis selection	R	D	R	R	D	D	R	D	R	R	R	D	R	D	D
Polarized photon sent by Alice	↑	↗	↑	↑	↗	↗	↔	↘	↑	↔	↑	↗	↔	↘	↘
Bob's random basis selection	D	R	D	R	D	D	D	D	R	R	R	R	D	D	D
Bob's measured received bits	0	0	1	1	0	0	0	1	1	1	1	1	1	1	1
Bob's basis and Alice's basis agreement?	N	N	N	Y	Y	Y	N	Y	Y	Y	Y	N	N	Y	Y
Public Discussion															
Bob reports basis of received bits	D	R	D	R	D	D	D	D	R	R	R	R	D	D	D
Alice says which basis were correct				√	√	√		√	√	√	√			√	√
Sifted key				1	0	0		1	1	1	1			1	1
Bob reveals some key bits randomly					0						1				
Alice confirm them					√						√				
Outcome															
Remaining Shared Secret Bits				1		0		1	1	1				1	1

Figure 2.8 BB84 Protocol Implementation on Details [31]

Blue R: Represent the rectilinear basis polarization.

Yellow D: Represent the diagonal basis polarization.

Red N: Represent no generated key as the measured polarization basis or value, or both are different.

Green Y: Represent generated key when the measured polarization basis and value are both the same.

Any photons that has been sent by sender (Alice) will be measured randomly by receiver (Bob), from the experimental results can be concluded as below:

- 1) If Alice and Bob use the same basis, but different value the key will not be generated between Alice and Bob.
- 2) If Alice uses a dissimilar base than Bob but same value, the key will not generate between Alice and Bob.
- 3) A key will be generated between Alice and Bob if Alice uses the same base as Bob and same value

In theory, it's been proven that BB84 protocol can provide unconditional security which will be discussed later in this thesis [31].

Figure 2.9 Illustrates the based polarization of BB84.

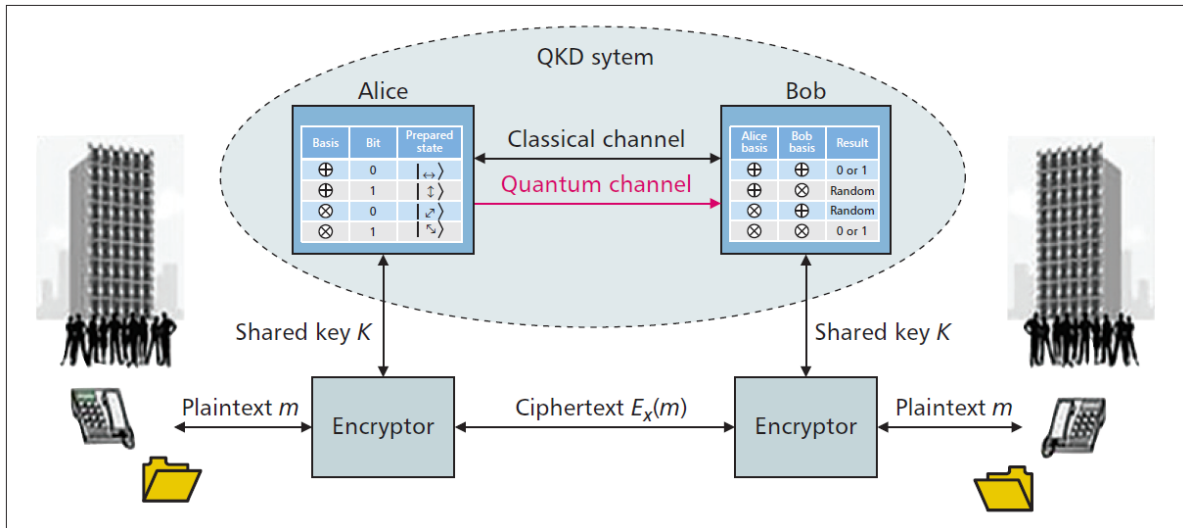


Figure 2.9 Polarization basis of BB84. [31]

Alice & Bob are able to generate a key that can be shared for encryptions, Quantum channel is in use for secure qubit transmission, for facilitating the BB84 protocol, classical channel can be used [29].

2.7.2-E91

This protocol was established by Ekert in 1991, which was designed to use a pair of entangled photons principle, a third-party source can create photons and send them to both Alice & Bob. Figure 2.11 illustrated the QKD model of Entanglement-based.

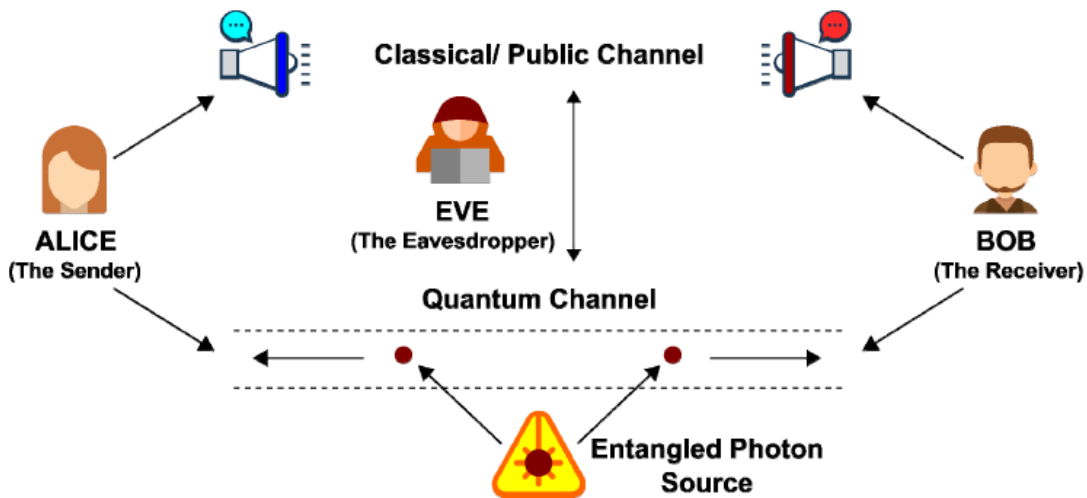


Figure 2.10 Entanglement based QKD basic concepts [31]

Figure 2.10 presents a pair of entangle photons that have been released by photon generator source to both Alice and Bob. In E91 protocol random basis measurement will be executed by both parties (Alice and Bob) which works in the same way as BB84 protocol process, they will exchange the random protocols via classical channel. Bell's inequality test is used by E91 protocol for detecting the Eavesdropper Existence. [The experimental violation of Bell's inequalities confirms that a pair of entangled photons separated by hundreds of metres must be considered a single non-separable object, it is impossible to assign local physical reality to each photon] [40]. E91 is considered under EB category of QKD system [31].

2.7.3-BBM92

BBM92 has similar main structure as BB84, like basis key exchange technique, sifting of key process plus amplification of privacy. BBM92 can be consider as EB category of BB84, which BB84 protocol can be classified under P&M category of QKD protocol [29]. BB84 can be recognized physically by two level of quantum structure and four states of polarization that use for coding [37]. This protocol is using an individual photon to carry and distribute secret key bits randomly. This single photon has the polarization of four different states using one of the two rectangular and diagonal bases, BBM92 using entangled states and It was developed in 1992 by Brassard, Bennett and Mermin after a short time that E91 was proposed by Ekert [31].

2.7.4-B92

B92 is modified type of BB84 to make a simple protocol, Bennett introduced it in 1992. The difference between these two protocols is that B92 use only one of the two states of polarization while the BB84 protocol use one out of four states of polarization photon. Bennett believed that the encoding and decoding the QKD can be done even with one single basis and still the system is able to detect any eavesdropping activity. B92 protocol can be classified as P&M based of QKD protocol [31].

2.7.5-SSP (Six-State Protocol)

SSP protocol established and introduced by Gisin and Pasquucci in 1999. SSP protocol has three basis measurement and six states of polarization. SSP protocol is considered as BB84 protocol with an extra basis. Figure 2.11 illustrates Poincare sphere, if we represent the BB84 protocol on the Poincare sphere will show us 4 spin of 1/2 polarization states that containing of directions of $\pm x$ and $\pm y$. In SSP protocols there are two additional states polarization of $\pm z$, which in total become six states [$\pm x$, $\pm y$, and $\pm z$] within the Poincare sphere. One of the advantages of SSP compare to BB84 is the higher level of symmetry. SSP is under P&M based of QKD System [31].

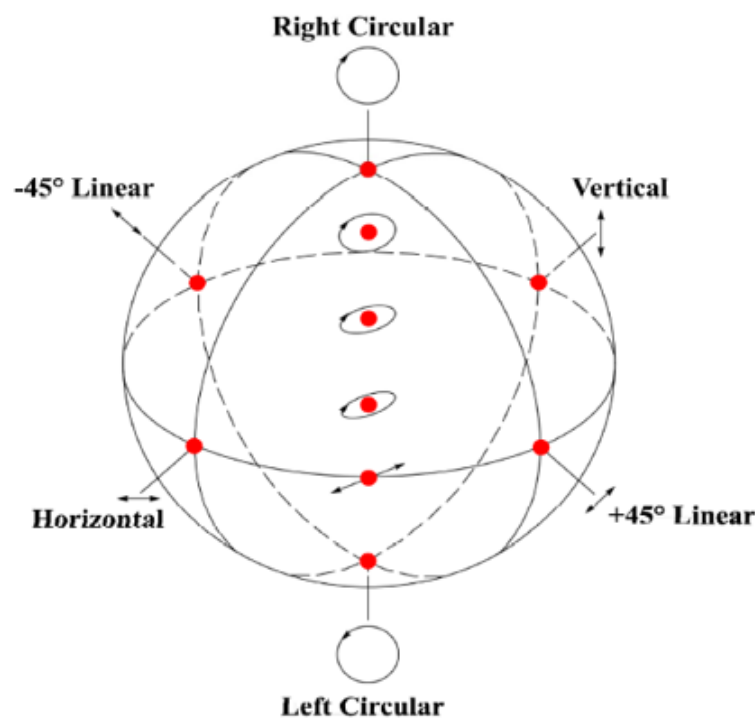


Figure 2.11 Sphere of Poincare [31]

2.7.6-DPS

Differential phase shift (DPS) is one of the unique protocols in QKD system [41], it was developed and proposed at Osaka and NTT University in 2003. Coherent pulse train is used instead of single photons as in traditional protocols of QKD system. Security in this protocol comes from the fact that the difference phase of coherent pulse train highly-attenuated can't be fully measured [42].

In DPS Protocol a coherent pulse is sent by Alice in modulated phase of $(0, \pi)$ per each pulse which has the attenuated of 0.1 to 0.2 photon per pulse, after attenuating the light to make the number less than 1 photon per pulse, then light will be sent to Bob (receiver) [43].

Bob receives the pulse by delay of one-bit. Bob will inform Alice the detection time of photon after completing the transmission, one key bit has generated from difference phase of pulses. Below are some of the specification of DPS Protocol:

- Unlike the other QKD protocols in DPS there is no procedure selection basis
- Implementation required a very simple configuration
- Speed of key creation is very high
- Robust against PNS (Photon Number Splitting) attack.

DPS protocol scheme and setup has been shown in Figure 2.12 [42].

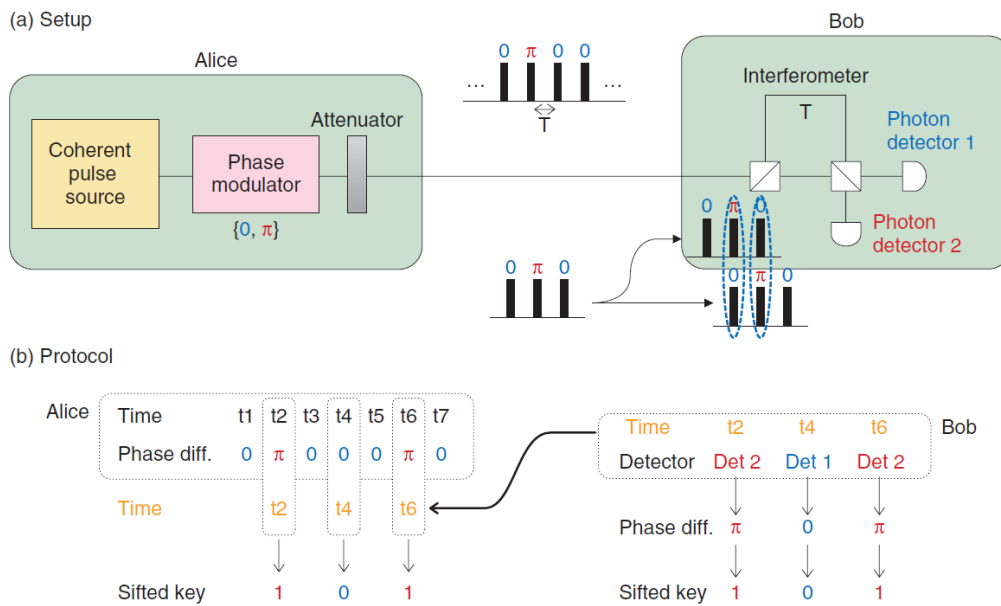


Figure 2.12 DPS design pattern [42]

DPS has some advantages i.e. simple configuration, strong against PSN attack, uses the domain time efficiently. This protocol can be considered under EB category [42].

2.7.7-SARG04

Scarani presented SAEG04 in 2004. In this protocol instead of single photon source, attenuated laser pulse is in use. SARG04 has identical scheme as BB84 protocol in first phase. But second phase is different, Alice the sender uses one of non-orthogonal state of her basis for encoding her bit instead of directly announcing her bases. Bob will measure the exact state if he uses appropriate basis, and he will not get the bit if choose the wrong basis. SARG04 protocol is under P&M based protocol of QKD [31].

2.7.8-COW

Nicolas Gisin presented the COW (Coherent One-Way) protocol in year 2004. COW using the entanglement photon principle. The advantages of COW Protocol are high level of efficiency on secret bits distilled on qubit, is tough against PSN (photon number splitting) attack. Figure 2.13 illustrates the COW model, in COW data encrypted in function of time. COW is under EB category of QKD [31].

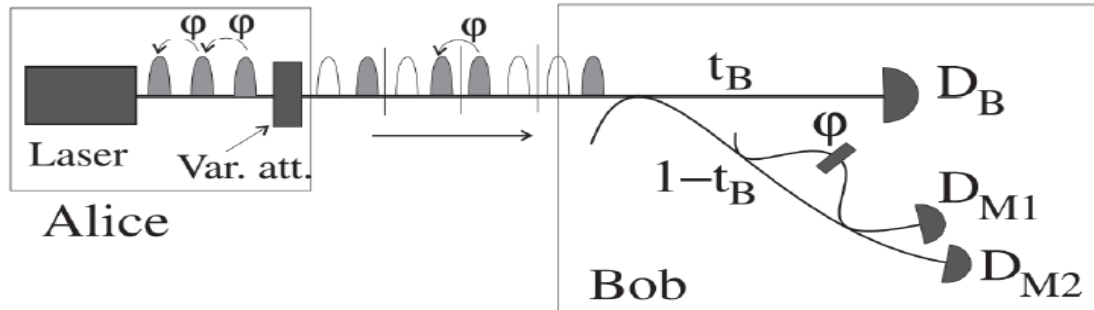


Figure 2.13 Scheme of COW [35]

2.7.9-S13

Eduin H. Serna introduced S13 in 2013. S13 is very similar to BB84 with this difference that a random asymmetric and seed cryptography [31]. The purpose of designing this protocol was avoid losing any data in data transfer process between parties. Because the mechanism of this protocol is based on a random seed and asymmetric cryptography, they can process in multiple exchanges. The one-time-pad is guaranteed to be secured if the secret key is random and contains the same length of the plain text. Therefore, the S13 protocol was designed to match the one-time-pad by generating a secret key with zero losses [44].

Table 2.1 shows the list and some specification of discussed protocols in this thesis such as Principles base and the year of introductions.

No.	Year	Name of Protocol	Principle Base
1	1984	BB84	Heisenberg's Uncertainty Principles
2	1991	E91	Quantum Entanglement
3	1992	BBM92	Quantum Entanglement
4	1992	B92	Heisenberg's Uncertainty Principles
5	1999	SSP	Heisenberg's Uncertainty Principles
6	2003	DPS	Quantum Entanglement
7	2004	SARG04	Heisenberg's Uncertainty Principles
8	2004	COW	Quantum Entanglement
9	2013	S13	Heisenberg's Uncertainty Principles

Table 2.1 QKD Protocols Details [31]

An extensive time search for possible recent QKD protocols found limited information only on one new proposed protocol, named AK15 protocol that was presented at IEEE LISAT conference in 2015. AK15 protocol was developed to stand against the common quantum attacks as well as providing an authentication link before starting any exchanges. The proposed protocol was designed to include two quantum channels. One of these channels is an EPR channel that is based on initiating an entangled state [57]. The other channel is a quantum channel, where the sender and the receiver can submit the data to create a secret key [44].

Chapter 3

Literature Review

This chapter will enclose some basic concepts of QKD which are required for reader for better understanding of the thesis. Then will review some related previous evaluation of QKD experiments.

3.1 - Related Previous Evaluation of QKD Experiment

There are two related previous experiment study about the comparison of probability Error on QKD protocols which have been performed in 2018, this thesis will go through them with details.

3.1.1- Beatrix Rambu and Nana Rachmana (2018)

Rambu and Rachmana (2018), had a research on testing and analysing the error probability of two protocols of QKD model which are BB84 and B92 protocols, QuVis Software simulator has been used for this experiment to continue work of previous research. Following experiment setups have been used for both BB84 and B92 protocols by author:

1. Random Basis has been used for sending polarization photons by Alice and Bob on both protocols.
2. Random base was in used by Eavesdropper (Eve) which placed between Alice and Bob for translating the basis send by Alice to Bob.
3. The fast Forward of 100 photons polarization option was used for sending photons.
4. The experiment was executed by sending range of 100 to 1000 photons.
5. This Experiment performed the probability error ratio comparison for any photon delivery.

Figures 3.1 and 3.2 show the experimental result of 100 to 1000 photons probability keys [26]

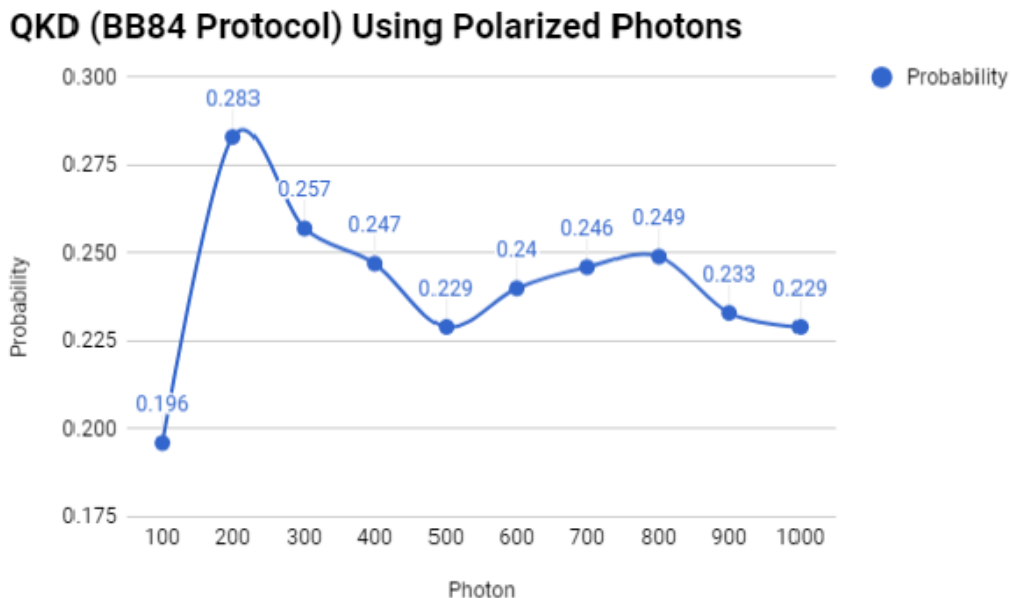


Figure 3.1 BB84 result of 100 to 1000 photons experiment [26]

QKD (B92 Protocol) Using Polarized Photons

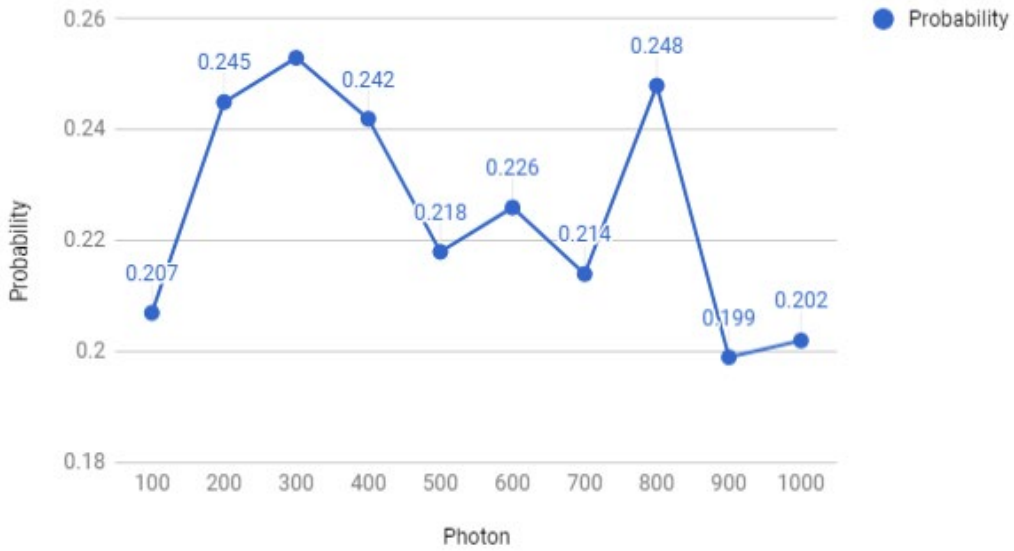


Figure 3.2 B92 result of 100 to 1000 photons experiment [26]

Using the similar experimental setup for both protocols generated the probability error statistics as shown in Table 3.1 below:

Photon (N_{tot})	BB84			B92		
	N_{key}	N_{err}	N_{err} / N_{key}	N_{key}	N_{err}	N_{err} / N_{key}
100	46	9	0.196	29	6	0.207
200	99	28	0.283	53	13	0.245
300	136	35	0.257	75	19	0.253
400	182	45	0.247	95	23	0.242
500	240	55	0.229	119	26	0.218
600	279	67	0.24	146	33	0.226
700	325	80	0.246	173	37	0.214
800	374	93	0.249	196	39	0.248
900	421	98	0.233	223	45	0.199
1000	463	106	0.229	246	48	0.202

Table 3.1 BB84 and B92 error probability ratio [26]

Based on collected data result from simulator the generated error key probability in B92 is less than the BB84 as it uses only 2 bases compare to BB84 which has 4 bases, bases difference between these two protocol cases many of few keys agreed between the receiver and sender.

This approached by the Authors concluded as below:

- The B92 protocol is a simplified form of BB84 protocol
- This simplification can be noticed from bases difference between these two QKD protocols.
- The basis difference can determine that key generated for Bob (receiver) is %50 on BB84 and is %25 on B92.
- B92 generated a smaller number of probability discard key (K_E) compare to BB84 (Fig 3.1 and Fig 3.2) [26].

3.1.2- Ali Ibnun and Nana Rachmana (2018)

Ali Ibnun and Nana Rachmana (2018) have done another survey on QKD protocols. The authors discussed all of the QKD protocols which have been developed since 1984 (BB84) to 2013(S13) in first part of their survey, In second section authors perfumed three QKD protocol simulation consisting an entanglement based protocol (BBM92) and two P&M based protocols (BB84 and B92), The authors used a quantum simulator called QuVis same as first evaluation experiment [31].

Authors set up the experiment as Below:

- Three protocols (BB84, B92 and BBM92) are involved in this simulation experiment.
- Passive eavesdropping manages to be involved in this experiment testing.
- Both sender (Alice) and receiver (Bob) use basis randomly for sending each experiment polarized photon.
- Basis is in use also randomly by eavesdropper to translate the polarization photons between Alice and Bob.
- Fast forwarded option of 100 photons has been planned for this experiment activation.
- This experiment has been executed by sending 100 to 2000 photons.
- The measure parameters have values of N Error (N_E), N Key (N_K), and N_E / N_K (N_P) for all the protocols [31].

The data result of this experiment has been shown in table 3.2, Figure 3.3 presents the N Key (N_K) value for all three protocols, Figure 3.4 presented the N Error (N_E) value for each protocol and Figure 3.5 shows the value of $N_E/N_K = (N_P)$. As it shown in Figure 3.3 The highest number of generated keys is 1004 keys out of 2000 photons that have been sent by BBM92, and less keys, 16 out of 100 has been generated by B92. The higher generated keys, the better [31].

Phot-on Number	BB84			B92			BBM92		
	N_k	N_e	N_p	N_k	N_e	N_p	N_k	N_e	N_p
100	52	12	0.231	16	4	0.25	47	12	0.255
200	95	25	0.263	43	11	0.256	99	20	0.202
300	140	39	0.279	68	16	0.235	146	39	0.267
400	192	56	0.292	90	23	0.256	201	53	0.264
500	249	78	0.313	117	26	0.222	250	69	0.276
600	249	88	0.301	146	29	0.199	288	78	0.271
700	292	99	0.289	178	35	0.197	344	91	0.265
800	342	112	0.289	214	44	0.207	395	100	0.253
900	388	126	0.287	239	49	0.205	444	116	0.261
1000	439	139	0.281	265	58	0.219	498	132	0.265
1100	495	159	0.288	288	65	0.226	545	147	0.27
1200	552	171	0.284	310	74	0.239	601	161	0.268
1300	603	180	0.277	334	82	0.246	653	171	0.262
1400	700	187	0.267	361	92	0.255	705	184	0.261
1500	744	200	0.269	394	103	0.261	752	198	0.263
1600	792	209	0.264	416	108	0.26	800	218	0.273
1700	845	226	0.267	443	112	0.253	854	233	0.273
1800	901	237	0.263	470	120	0.255	910	246	0.27
1900	939	246	0.262	491	122	0.248	958	262	0.237
2000	999	257	0.257	511	125	0.245	1004	272	0.271

Table 3.2 Simulation results of key and error [31]

N Key Value Comparison

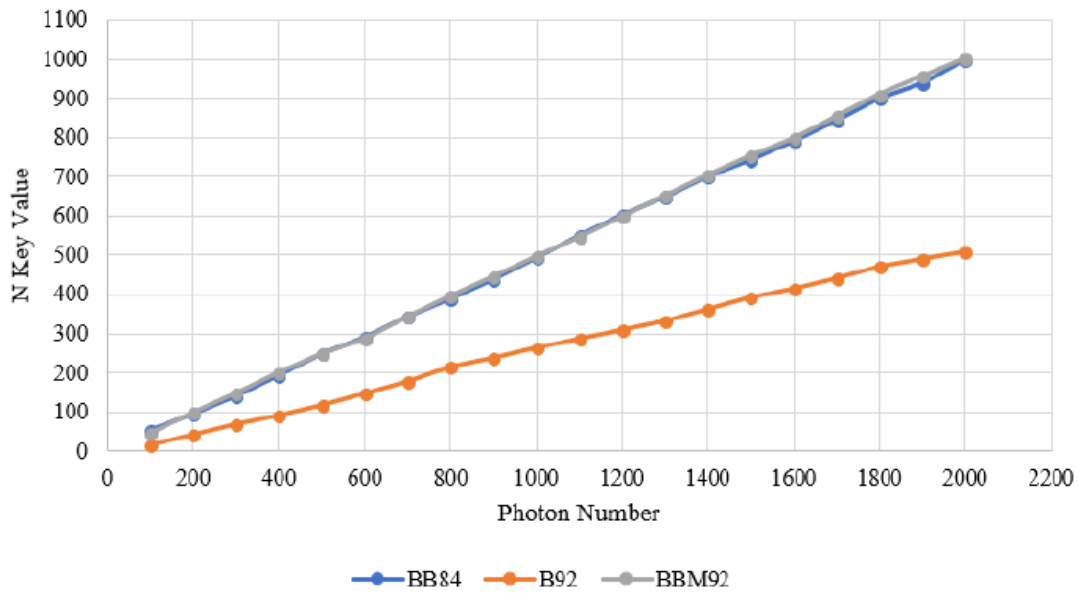


Figure 3.3 Comparison of each protocol N key [31]

N Error Value Comparison

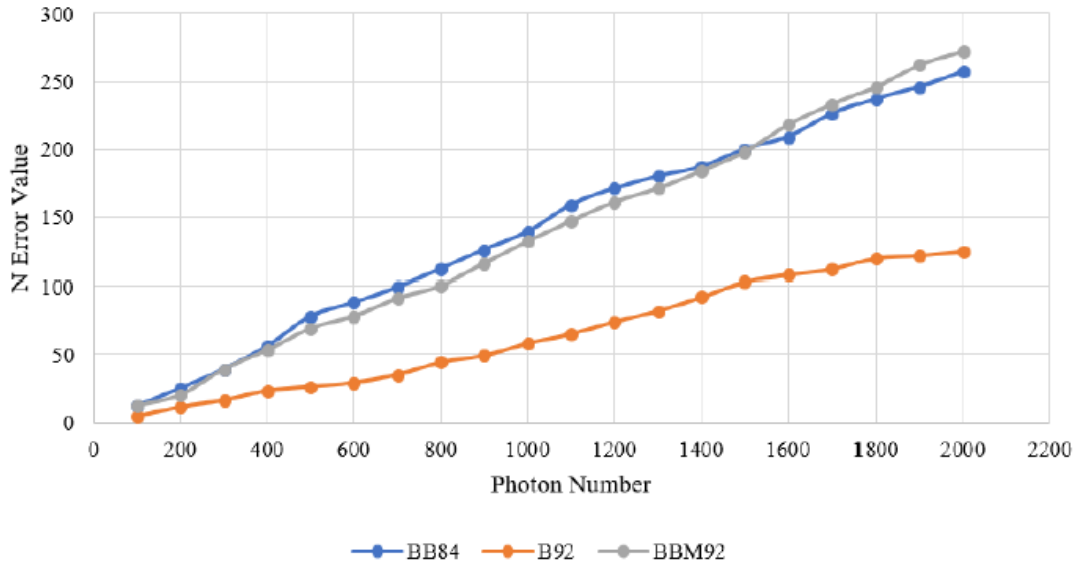


Figure 3.4 Comparison of N error value for each protocol [31]

As shown in Figure 3.4 highest key error generated number is 272 whit 2000 photons that has been sent by BBM92 protocol, while the lowest error generated key is 4 by sending 100 of photons by B92. The smaller error number is better [31].

N Error/ N Key Value Comparison

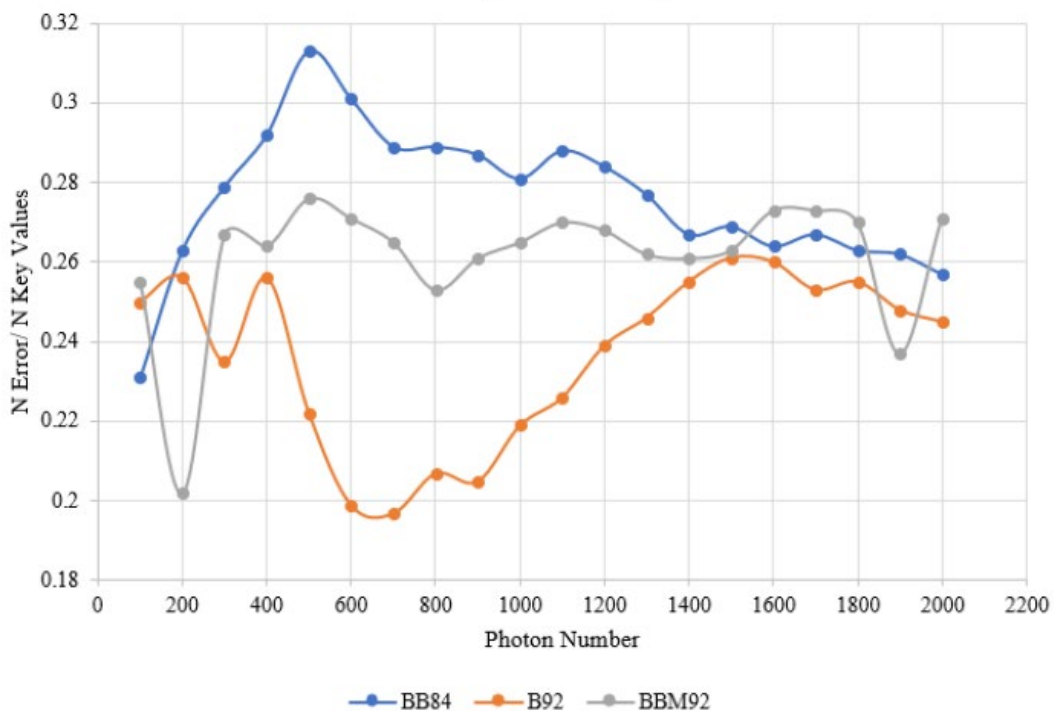


Figure 3.5 Value comparison of N error/N key value (Probability error) on each protocol [31]

Figure 3.5 shows that the lowest amount of error probability belongs to B92 protocol, the range of %19.9 (0.199) to %25.6 (0.256). In theory the value of error in B92 can be %25 which the result can be affected by environment, Setup condition or design. In other hand the result of error probability for BB84 has the

largest value in range of %23.1(0.231) to %31.3 (0.313). The highest value of error for of BB84 is 0.5 (50%) in theory. Meantime we can see that error probability (N_p) of BBM92 is between the other two protocols error probabilities of BB84 and B92, the range of 0.202 (20.2%) to 0.276 (27.6%).

Based on the experiment results, the authors concluded their research as below:

- The B92 has the smallest value of N_{error}/N_{key} (N_p), which means this protocol has smallest error probability compare to other two protocols.
- B92 is best protocol compare to another two protocols (BB84 and BBM92) Referring to error parameter, however when it comes to network implementation of QKD there are many other facts that needs to be considered like the rate of secret key, cost of setup, robustness and distance, etc.

Chapter 4

Methodology

4.1 - The Methodology

Researchers usually have three options of method basics to choose when doing a research as expressed by Kowalczyk (2016), which is directly depends on many facts which are involved in any individual research project. One method is called “quantitative research method” which tests hypotheses and come up with a prediction as using collected data and illustrate an operation by utilizing those data [5].

Researchers use numbers in form of statistic in this method to assure the collected results have a statistical liaison, they describe their finding by using numbers. Researchers also might use the other method which called “qualitative research method”, in this method researcher define the type and nature of the subject by describing an action. Researcher using text to define their discovery in qualitative method. Researchers give the audience a big intellectual picture of what the researcher is detecting. Sometimes researcher choose to apply a combination of both qualitative and quantitative methods to express an action completely. Based on Creswell (2003) the choosing a method by researcher is based on:

- (a) Problem of research
- (b) Experience of researcher
- (c) Reporting audience
- (d) Type of collected data (text or numeric) (Creswell, 2003) [5]

This thesis will use a combination methods of research, The quantitative method has been used for collecting and analysing the test data results with statistics help, Qualitative method is used for testing and develop hypothesis while processing [5].

The schemes of this thesis are to understand and know the concepts and process of QKD methods by using QuVis software simulator. Implementation of four protocols in simulation environment are involved in this experiment, Eavesdropper also has been added in process of this experiment. Therefore, this research tested the QuVis and continue the previous research by analysing the error probability of B92, BBM92, BB84 and BB84 with Spin 1/2 protocols.

4.2 – Implementation Methodology

Data collection have been executed five times for this experiment and analysis and discussion will be based on average value of collected data, following are the steps of the experiment:

1. For this experiment QuVis software environment has been used as simulator.
2. Four protocols have been implemented in simulation environment.
3. Eve will be added into this experiment as eavesdropper to develop the experiment.
4. A random basis has been used to send polarization photons by sender and receiver in every individual protocol.
5. The Eve also uses random basis for translating sender basis sent to receiver.
6. The method of “fast forward 100 photons” has been used for sending polarization photons.

7. 100 to 5000 photons have been sent to perform the examination.
8. The ratio rates of error probability of photons will be examined in this observation.

4.3 - Experimental Metrics

The new protocol will be setup in a QuVis simulator from St. Andrews university and will evaluate Number of probability key (N_p) by using below metrics:

- N_{key} : Total value of selected keys.
- N_{err} : Total value of error keys.
- N_p : Total value of probability key

Following formula has been used to determine the number of probability errors:

$$N_p = N_{err} / N_{key}$$

Analysing generated probability keys of selected protocols will determine variation of these four protocols. The error detection level can be determining the status change of quantum by eavesdropping.

Chapter 5

Evaluation and Data Collection Process

5.1 – QuVis Software

5.1.1- About QuVis

QuVis is created by a group of simulation mostly research based with the purpose of teaching the concepts of quantum mechanics for the range of high school level student to advanced level of university undergraduates. This simulation has been developed based on current research educational and aiming quantum mechanics areas of difficulty for helping student with better understanding. Development is announced by student input, Then the activities and simulations are modifying constantly based on feedback from students observation sessions, These simulations have been created and designed to assist students to analyse the quantities and relationship between them on different representations, and multiple situations.

All the simulations can be downloaded and run through the website. There are new HTML5 version of simulations that can be run on either desktop computers or tablet-based devices. The Flash type simulations are not supported on touchscreen devices. Web browser can be used to run the Flash type of simulations, but Adobe flash player installation is required. Stand-alone player can be downloaded by users if they like to run these simulations as a stand-alone application, (Flash Player Projector from the Adobe website).

QuVis acknowledges the funding from the UK Higher education academy, UK Institute of physics, and the University of St Andrews for the development of these recourses [45].

5.1.2- QuVis Awards

QuVis earned the 2015 Multimedia educational resources from Physics Classics award for teaching and learning online (MERLOT, www.merlot.org). Every year an outstanding resource selected by MERLOT Editorial Boards to receive the MERLOT Classics Award. MERLOT considers this learning material an exemplary online learning resource and recognises it as such on its website.

QuVis also received the excellence award of the “MPTL” (Multimedia Physics Teaching and Learning) in 2014. Quantum physics was the multimedia materials topic for 2014 [46].

Figure 5.1 is a sample of QuVis quantum environment for BB84 protocol, this software was used to perform the experiment and collect the data values for all four protocols.

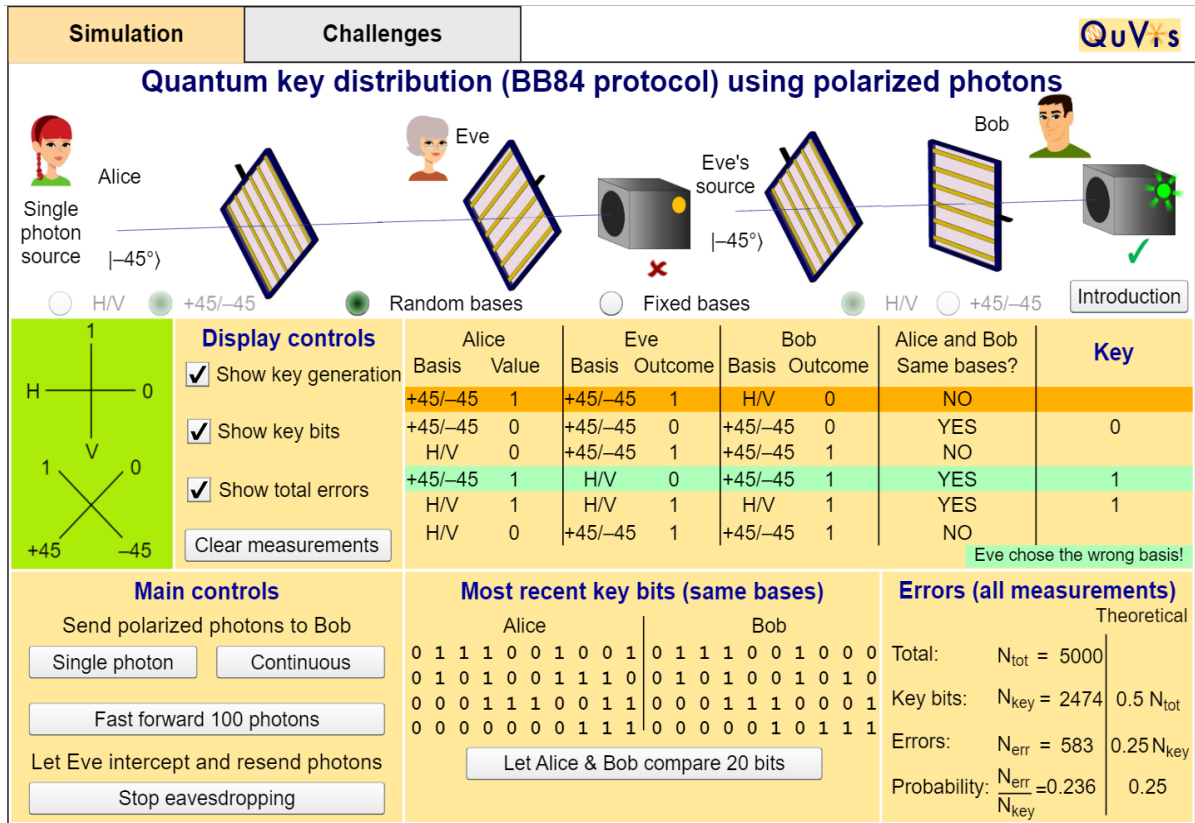


Figure 5.1 Sample QuVis simulation quantum environment for BB84 protocol

5.2 – Evaluation

Following our data collection processes, QuVis software simulator was used to Implement four protocols in simulation environment (B92, BBM92, BB84 and BB84 Spin protocols). For more accuracy of collected data in this experiment, data collection process has been executed five times, and the average value of each collected data has been calculated. final analysis was performed based on final average value of collected data, the data collection results of this experiment have been shown in table 5.1 to 5.5.

5.3 - The Results

This chapter contains the data collection results from QuVis simulation software.

5.3.1- Data Collection 1

First data collection process was performed in QuVis platform and the results are shown in data collection 1 below on Table 5.1.

Photon Number	BB84			B92			BBM92			BB84 with Spin 1/2		
	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np
100	50	16	0.320	19	5	0.263	51	18	0.353	38	14	0.368
200	105	30	0.286	49	11	0.224	100	25	0.250	84	25	0.298
300	153	43	0.281	70	17	0.243	143	35	0.245	131	37	0.282
400	208	61	0.293	88	23	0.261	191	47	0.246	178	46	0.258
500	267	74	0.277	121	29	0.240	242	58	0.240	226	57	0.252
600	326	88	0.270	150	36	0.240	297	69	0.232	280	71	0.254
700	375	101	0.269	173	43	0.249	347	85	0.245	335	84	0.251
800	428	117	0.273	203	55	0.271	405	101	0.249	378	97	0.257
900	483	127	0.263	231	61	0.264	456	112	0.246	421	112	0.266
1000	534	136	0.255	255	67	0.263	506	127	0.251	477	123	0.258
1100	576	146	0.253	281	76	0.270	557	135	0.242	530	136	0.257
1200	625	156	0.250	304	86	0.283	609	149	0.245	573	150	0.262
1300	676	166	0.246	329	95	0.289	653	159	0.243	626	167	0.267
1400	726	170	0.234	353	99	0.280	706	170	0.241	678	172	0.254
1500	779	176	0.226	381	105	0.276	755	183	0.242	721	182	0.252
1600	824	191	0.232	404	111	0.275	805	201	0.250	772	195	0.253
1700	873	204	0.234	426	114	0.268	860	212	0.247	821	207	0.252
1800	924	216	0.234	457	118	0.258	905	221	0.244	866	219	0.253
1900	975	226	0.232	480	123	0.256	954	230	0.241	922	234	0.254
2000	1020	241	0.236	509	127	0.250	1000	244	0.244	975	255	0.262
2100	1078	254	0.236	533	132	0.248	1051	250	0.238	1032	267	0.259
2200	1136	267	0.235	556	139	0.250	1095	261	0.238	1080	277	0.256
2300	1180	280	0.237	578	142	0.246	1152	277	0.240	1126	287	0.255
2400	1234	299	0.242	595	143	0.240	1199	285	0.238	1179	307	0.260
2500	1280	306	0.239	618	149	0.241	1251	301	0.241	1231	319	0.259
2600	1323	313	0.237	645	155	0.240	1295	313	0.242	1281	332	0.259
2700	1377	325	0.236	659	157	0.238	1339	327	0.244	1351	350	0.259
2800	1428	338	0.237	681	163	0.239	1388	339	0.244	1397	360	0.258
2900	1481	355	0.240	708	171	0.242	1440	349	0.242	1450	374	0.258
3000	1531	369	0.241	735	177	0.241	1486	359	0.242	1492	386	0.259
3100	1584	386	0.244	762	184	0.241	1525	368	0.241	1548	396	0.256
3200	1646	408	0.248	788	191	0.242	1573	386	0.245	1591	408	0.256
3300	1697	433	0.255	808	198	0.245	1622	401	0.247	1650	424	0.257
3400	1745	443	0.254	839	210	0.250	1672	418	0.250	1706	438	0.257
3500	1797	454	0.253	859	214	0.249	1724	429	0.249	1754	446	0.254
3600	1849	466	0.252	883	226	0.256	1775	449	0.253	1808	460	0.254
3700	1909	479	0.251	909	231	0.254	1814	459	0.253	1853	475	0.256
3800	1954	486	0.249	934	239	0.256	1865	470	0.252	1902	488	0.257
3900	2007	503	0.251	951	243	0.256	1914	485	0.253	1957	498	0.254
4000	2061	515	0.250	976	247	0.253	1960	494	0.252	2010	515	0.256
4100	2106	529	0.251	1005	252	0.251	2012	501	0.249	2056	528	0.257
4200	2157	542	0.251	1032	257	0.249	2065	512	0.248	2119	547	0.258
4300	2202	559	0.254	1056	266	0.252	2113	526	0.249	2172	559	0.257
4400	2253	571	0.253	1077	271	0.252	2158	536	0.248	2215	567	0.256
4500	2297	578	0.252	1109	276	0.249	2218	554	0.250	2266	576	0.254
4600	2349	591	0.252	1138	284	0.250	2267	565	0.249	2312	581	0.251
4700	2406	606	0.252	1165	292	0.251	2323	580	0.250	2358	596	0.253
4800	2449	619	0.253	1186	302	0.255	2375	593	0.250	2413	607	0.252
4900	2494	634	0.254	1209	308	0.255	2428	612	0.252	2465	620	0.252
5000	2549	642	0.252	1233	314	0.255	2476	626	0.253	2514	630	0.251

Table 5.1 Experiment data collection 1 results

5.3.2- Data Collection 2

The second round of data collection process was performed in QuVis platform and the results are shown in data collection 2 below on Table 5.2.

Photon Number	BB84			B92			BBM92			BB84 with Spin 1/2		
	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np
100	50	16	0.320	19	5	0.263	51	18	0.353	38	14	0.368
200	105	30	0.286	49	11	0.224	100	25	0.250	84	25	0.298
300	153	43	0.281	70	17	0.243	143	35	0.245	131	37	0.282
400	208	61	0.293	88	23	0.261	191	47	0.246	178	46	0.258
500	267	74	0.277	121	29	0.240	242	58	0.240	226	57	0.252
600	326	88	0.270	150	36	0.240	297	69	0.232	280	71	0.254
700	375	101	0.269	173	43	0.249	347	85	0.245	335	84	0.251
800	428	117	0.273	203	55	0.271	405	101	0.249	378	97	0.257
900	483	127	0.263	231	61	0.264	456	112	0.246	421	112	0.266
1000	534	136	0.255	255	67	0.263	506	127	0.251	477	123	0.258
1100	576	146	0.253	281	76	0.270	557	135	0.242	530	136	0.257
1200	625	156	0.250	304	86	0.283	609	149	0.245	573	150	0.262
1300	676	166	0.246	329	95	0.289	653	159	0.243	626	167	0.267
1400	726	170	0.234	353	99	0.280	706	170	0.241	678	172	0.254
1500	779	176	0.226	381	105	0.276	755	183	0.242	721	182	0.252
1600	824	191	0.232	404	111	0.275	805	201	0.250	772	195	0.253
1700	873	204	0.234	426	114	0.268	860	212	0.247	821	207	0.252
1800	924	216	0.234	457	118	0.258	905	221	0.244	866	219	0.253
1900	975	226	0.232	480	123	0.256	954	230	0.241	922	234	0.254
2000	1020	241	0.236	509	127	0.250	1000	244	0.244	975	255	0.262
2100	1078	254	0.236	533	132	0.248	1051	250	0.238	1032	267	0.259
2200	1136	267	0.235	556	139	0.250	1095	261	0.238	1080	277	0.256
2300	1180	280	0.237	578	142	0.246	1152	277	0.240	1126	287	0.255
2400	1234	299	0.242	595	143	0.240	1199	285	0.238	1179	307	0.260
2500	1280	306	0.239	618	149	0.241	1251	301	0.241	1231	319	0.259
2600	1323	313	0.237	645	155	0.240	1295	313	0.242	1281	332	0.259
2700	1377	325	0.236	659	157	0.238	1339	327	0.244	1351	350	0.259
2800	1428	338	0.237	681	163	0.239	1388	339	0.244	1397	360	0.258
2900	1481	355	0.240	708	171	0.242	1440	349	0.242	1450	374	0.258
3000	1531	369	0.241	735	177	0.241	1486	359	0.242	1492	386	0.259
3100	1584	386	0.244	762	184	0.241	1525	368	0.241	1548	396	0.256
3200	1646	408	0.248	788	191	0.242	1573	386	0.245	1591	408	0.256
3300	1697	433	0.255	808	198	0.245	1622	401	0.247	1650	424	0.257
3400	1745	443	0.254	839	210	0.250	1672	418	0.250	1706	438	0.257
3500	1797	454	0.253	859	214	0.249	1724	429	0.249	1754	446	0.254
3600	1849	466	0.252	883	226	0.256	1775	449	0.253	1808	460	0.254
3700	1909	479	0.251	909	231	0.254	1814	459	0.253	1853	475	0.256
3800	1954	486	0.249	934	239	0.256	1865	470	0.252	1902	488	0.257
3900	2007	503	0.251	951	243	0.256	1914	485	0.253	1957	498	0.254
4000	2061	515	0.250	976	247	0.253	1960	494	0.252	2010	515	0.256
4100	2106	529	0.251	1005	252	0.251	2012	501	0.249	2056	528	0.257
4200	2157	542	0.251	1032	257	0.249	2065	512	0.248	2119	547	0.258
4300	2202	559	0.254	1056	266	0.252	2113	526	0.249	2172	559	0.257
4400	2253	571	0.253	1077	271	0.252	2158	536	0.248	2215	567	0.256
4500	2297	578	0.252	1109	276	0.249	2218	554	0.250	2266	576	0.254
4600	2349	591	0.252	1138	284	0.250	2267	565	0.249	2312	581	0.251
4700	2406	606	0.252	1165	292	0.251	2323	580	0.250	2358	596	0.253
4800	2449	619	0.253	1186	302	0.255	2375	593	0.250	2413	607	0.252
4900	2494	634	0.254	1209	308	0.255	2428	612	0.252	2465	620	0.252
5000	2549	642	0.252	1233	314	0.255	2476	626	0.253	2514	630	0.251

Table 5.2 Experiment data collection 2 results

5.3.3- Data Collection 3

Table 5.3 below shows the further result of third data collection obtained from QuVis simulation software.

Photon Number	BB84			B92			BBM92			BB84 with Spin 1/2		
	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np
100	52	12	0.231	26	5	0.192	53	9	0.170	48	11	0.229
200	106	28	0.264	51	12	0.235	99	18	0.182	96	30	0.313
300	152	41	0.270	80	19	0.238	149	36	0.242	143	42	0.294
400	200	53	0.265	100	23	0.230	195	50	0.256	192	53	0.276
500	248	63	0.254	126	28	0.222	245	62	0.253	248	65	0.262
600	300	77	0.257	143	35	0.245	302	80	0.265	304	79	0.260
700	353	89	0.252	165	37	0.224	361	100	0.277	350	90	0.257
800	407	104	0.256	193	42	0.218	415	115	0.277	404	106	0.262
900	455	114	0.251	218	46	0.211	461	125	0.271	445	111	0.249
1000	503	124	0.247	233	50	0.215	507	139	0.274	505	122	0.242
1100	545	132	0.242	262	57	0.218	562	151	0.269	554	127	0.229
1200	591	143	0.242	291	64	0.220	605	163	0.269	607	143	0.236
1300	644	153	0.238	310	70	0.226	651	175	0.269	658	156	0.237
1400	693	166	0.240	333	72	0.216	699	185	0.265	712	164	0.230
1500	738	181	0.245	360	79	0.219	754	197	0.261	768	173	0.225
1600	795	196	0.247	384	87	0.227	799	206	0.258	821	182	0.222
1700	851	214	0.251	410	90	0.220	848	218	0.257	874	200	0.229
1800	907	232	0.256	434	96	0.221	889	227	0.255	924	209	0.226
1900	964	245	0.254	462	103	0.223	943	244	0.259	982	219	0.223
2000	1005	261	0.260	481	109	0.227	1000	252	0.252	1035	234	0.226
2100	1058	275	0.260	510	121	0.237	1046	269	0.257	1081	242	0.224
2200	1106	289	0.261	544	127	0.233	1101	279	0.253	1119	254	0.227
2300	1147	298	0.260	573	133	0.232	1159	295	0.255	1171	263	0.225
2400	1192	305	0.256	597	138	0.231	1210	307	0.254	1224	278	0.227
2500	1249	318	0.255	621	145	0.233	1257	315	0.251	1274	288	0.226
2600	1293	329	0.254	645	150	0.233	1306	325	0.249	1324	302	0.228
2700	1340	341	0.254	670	156	0.233	1354	335	0.247	1368	313	0.229
2800	1391	356	0.256	692	162	0.234	1396	342	0.245	1419	327	0.230
2900	1443	370	0.256	724	165	0.228	1446	359	0.248	1472	338	0.230
3000	1496	384	0.257	754	175	0.232	1496	373	0.249	1516	351	0.232
3100	1544	392	0.254	786	185	0.235	1545	381	0.247	1568	367	0.234
3200	1595	401	0.251	812	189	0.233	1593	394	0.247	1623	379	0.234
3300	1642	411	0.250	834	194	0.233	1644	405	0.246	1678	385	0.229
3400	1697	426	0.251	856	201	0.235	1701	420	0.247	1724	402	0.233
3500	1738	432	0.249	877	208	0.237	1748	430	0.246	1776	416	0.234
3600	1782	441	0.247	902	213	0.236	1794	443	0.247	1827	424	0.232
3700	1832	453	0.247	926	223	0.241	1846	458	0.248	1880	440	0.234
3800	1876	460	0.245	949	230	0.242	1898	471	0.248	1927	454	0.236
3900	1921	470	0.245	972	235	0.242	1952	483	0.247	1976	468	0.237
4000	1963	482	0.246	995	245	0.246	1996	492	0.246	2026	480	0.237
4100	2008	494	0.246	1017	250	0.246	2045	507	0.248	2080	497	0.239
4200	2062	505	0.245	1046	254	0.243	2090	516	0.247	2122	511	0.241
4300	2116	520	0.246	1064	257	0.242	2148	529	0.246	2171	524	0.241
4400	2157	527	0.244	1094	265	0.242	2196	537	0.245	2216	538	0.243
4500	2204	540	0.245	1115	267	0.239	2237	555	0.248	2269	554	0.244
4600	2253	551	0.245	1141	274	0.240	2287	569	0.249	2328	568	0.244
4700	2306	562	0.244	1164	277	0.238	2337	577	0.247	2380	580	0.244
4800	2352	585	0.249	1181	282	0.239	2382	586	0.246	2421	592	0.245
4900	2400	599	0.250	1200	290	0.242	2436	602	0.247	2474	603	0.244
5000	2452	610	0.249	1230	297	0.241	2484	611	0.246	2522	613	0.243

Table 5.3 Experiment data collection 3 results

5.3.4- Data Collection 4

The fourth round of data collection process was performed in QuVis platform and Table 5.4 shows the results of this data collection.

Photon Number	BB84			B92			BBM92			BB84 with Spin 1/2		
	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np
100	51	8	0.157	22	1	0.045	48	7	0.146	55	16	0.291
200	101	18	0.178	44	5	0.114	92	20	0.217	110	37	0.336
300	154	35	0.227	74	12	0.162	141	38	0.270	157	50	0.318
400	202	40	0.198	97	16	0.165	180	47	0.261	209	62	0.297
500	258	57	0.221	120	21	0.175	216	64	0.296	262	80	0.305
600	301	65	0.216	142	28	0.197	266	75	0.282	309	96	0.311
700	344	75	0.218	164	38	0.232	315	85	0.270	357	110	0.308
800	390	84	0.215	185	44	0.238	360	99	0.275	403	123	0.305
900	442	98	0.222	213	49	0.230	415	114	0.275	440	130	0.295
1000	491	107	0.218	234	51	0.218	466	130	0.279	502	147	0.293
1100	536	122	0.228	258	55	0.213	521	143	0.274	546	157	0.288
1200	592	133	0.225	284	61	0.215	568	161	0.283	591	173	0.293
1300	635	146	0.230	306	67	0.219	612	170	0.278	651	165	0.253
1400	682	157	0.230	326	69	0.212	657	184	0.280	697	176	0.253
1500	738	168	0.228	352	79	0.224	708	195	0.275	757	190	0.251
1600	788	183	0.232	381	83	0.218	760	206	0.271	808	203	0.251
1700	838	190	0.227	405	94	0.232	813	220	0.271	861	218	0.253
1800	891	202	0.227	432	100	0.231	865	227	0.262	910	226	0.248
1900	943	221	0.234	457	109	0.239	919	241	0.262	960	246	0.256
2000	994	235	0.236	483	113	0.234	966	253	0.262	1013	260	0.257
2100	1051	249	0.237	503	117	0.233	1017	263	0.259	1065	276	0.259
2200	1106	271	0.245	529	124	0.234	1064	277	0.260	1108	289	0.261
2300	1161	285	0.245	567	129	0.228	1106	287	0.259	1156	303	0.262
2400	1212	300	0.248	590	133	0.225	1158	304	0.263	1214	322	0.265
2500	1262	314	0.249	614	143	0.233	1209	313	0.259	1270	342	0.269
2600	1311	330	0.252	642	148	0.231	1257	328	0.261	1322	355	0.269
2700	1368	343	0.251	667	153	0.229	1304	346	0.265	1377	369	0.268
2800	1420	357	0.251	695	158	0.227	1349	357	0.265	1421	384	0.270
2900	1463	364	0.249	715	163	0.228	1405	372	0.265	1473	397	0.270
3000	1513	379	0.250	736	169	0.230	1455	385	0.265	1524	410	0.269
3100	1553	392	0.252	757	176	0.232	1496	393	0.263	1575	416	0.264
3200	1602	408	0.255	783	181	0.231	1548	405	0.262	1625	426	0.262
3300	1650	417	0.253	813	191	0.235	1600	423	0.264	1668	437	0.262
3400	1701	426	0.250	834	197	0.236	1643	436	0.265	1710	448	0.262
3500	1748	442	0.253	851	205	0.241	1691	456	0.270	1760	466	0.265
3600	1798	456	0.254	878	214	0.244	1748	479	0.274	1813	478	0.264
3700	1845	467	0.253	892	217	0.243	1797	492	0.274	1856	489	0.263
3800	1893	478	0.253	912	222	0.243	1852	504	0.272	1900	497	0.262
3900	1948	492	0.253	935	227	0.243	1904	510	0.268	1946	514	0.264
4000	2002	505	0.252	963	235	0.244	1950	523	0.268	2000	529	0.265
4100	2058	517	0.251	990	243	0.245	1995	538	0.270	2048	537	0.262
4200	2108	523	0.248	1014	249	0.246	2047	549	0.268	2105	554	0.263
4300	2159	536	0.248	1043	258	0.247	2107	563	0.267	2162	571	0.264
4400	2201	547	0.249	1076	263	0.244	2155	576	0.267	2223	586	0.264
4500	2250	559	0.248	1104	272	0.246	2204	593	0.269	2281	600	0.263
4600	2298	569	0.248	1125	277	0.246	2255	609	0.270	2327	615	0.264
4700	2344	578	0.247	1155	284	0.246	2305	618	0.268	2385	621	0.260
4800	2392	588	0.246	1179	290	0.246	2358	634	0.269	2428	637	0.262
4900	2449	602	0.246	1200	293	0.244	2408	642	0.267	2490	652	0.262
5000	2496	615	0.246	1225	299	0.244	2467	654	0.265	2542	671	0.264

Table 5.4 Experiment data collection 4 results

5.3.5- Data Collection 5

Then the fifth and final round of data collection process was performed in QuVis platform and collected data illustrated by table 5.5 below:

Photon Number	BB84			B92			BBM92			BB84 with Spin 1/2		
	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np
100	41	8	0.195	24	5	0.208	51	15	0.294	53	15	0.283
200	90	23	0.256	45	11	0.244	108	31	0.287	98	23	0.235
300	140	36	0.257	68	12	0.176	158	42	0.266	151	29	0.192
400	198	47	0.237	93	17	0.183	204	51	0.250	207	44	0.213
500	249	62	0.249	122	26	0.213	264	68	0.258	256	55	0.215
600	302	76	0.252	151	31	0.205	312	79	0.253	307	68	0.221
700	351	95	0.271	175	36	0.206	371	94	0.253	356	84	0.236
800	391	106	0.271	200	43	0.215	422	107	0.254	401	96	0.239
900	443	120	0.271	219	49	0.224	484	120	0.248	447	110	0.246
1000	488	129	0.264	251	59	0.235	547	137	0.250	503	123	0.245
1100	534	144	0.270	279	65	0.233	593	148	0.250	559	135	0.242
1200	585	152	0.260	303	70	0.231	634	159	0.251	615	145	0.236
1300	638	161	0.252	335	76	0.227	680	172	0.253	667	153	0.229
1400	689	177	0.257	362	83	0.229	733	185	0.252	713	167	0.234
1500	744	189	0.254	383	88	0.230	778	192	0.247	762	176	0.231
1600	796	209	0.263	409	93	0.227	830	209	0.252	808	182	0.225
1700	848	225	0.265	432	98	0.227	886	216	0.244	854	194	0.227
1800	896	245	0.273	455	102	0.224	935	226	0.242	904	213	0.236
1900	953	256	0.269	480	113	0.235	983	236	0.240	948	224	0.236
2000	1005	272	0.271	503	118	0.235	1032	247	0.239	999	241	0.241
2100	1052	288	0.274	525	126	0.240	1080	259	0.240	1051	248	0.236
2200	1103	298	0.270	550	131	0.238	1130	274	0.242	1100	263	0.239
2300	1150	311	0.270	579	143	0.247	1179	287	0.243	1150	281	0.244
2400	1204	329	0.273	606	149	0.246	1224	297	0.243	1198	295	0.246
2500	1244	338	0.272	628	158	0.252	1280	311	0.243	1240	308	0.248
2600	1304	357	0.274	655	165	0.252	1330	324	0.244	1286	317	0.247
2700	1348	367	0.272	677	172	0.254	1376	334	0.243	1340	330	0.246
2800	1402	380	0.271	703	177	0.252	1429	346	0.242	1394	349	0.250
2900	1457	396	0.272	729	184	0.252	1473	357	0.242	1439	362	0.252
3000	1506	411	0.273	756	188	0.249	1532	369	0.241	1493	374	0.251
3100	1559	426	0.273	778	194	0.249	1579	377	0.239	1541	386	0.250
3200	1621	443	0.273	806	202	0.251	1629	392	0.241	1591	397	0.250
3300	1673	456	0.273	837	209	0.250	1681	402	0.239	1647	407	0.247
3400	1720	470	0.273	860	216	0.251	1735	414	0.239	1696	421	0.248
3500	1776	484	0.273	887	224	0.253	1784	424	0.238	1749	430	0.246
3600	1835	500	0.272	919	234	0.255	1836	433	0.236	1800	445	0.247
3700	1880	513	0.273	953	237	0.249	1889	446	0.236	1851	460	0.249
3800	1929	530	0.275	980	240	0.245	1940	461	0.238	1901	467	0.246
3900	1976	539	0.273	999	244	0.244	1988	472	0.237	1957	486	0.248
4000	2031	553	0.272	1018	251	0.247	2039	485	0.238	2005	500	0.249
4100	2080	569	0.274	1037	254	0.245	2074	496	0.239	2053	511	0.249
4200	2130	584	0.274	1063	260	0.245	2130	512	0.240	2100	525	0.250
4300	2179	596	0.274	1093	264	0.242	2180	525	0.241	2156	540	0.250
4400	2232	617	0.276	1119	270	0.241	2231	536	0.240	2208	558	0.253
4500	2285	627	0.274	1149	273	0.238	2281	547	0.240	2258	573	0.254
4600	2343	638	0.272	1171	278	0.237	2334	564	0.242	2309	588	0.255
4700	2399	658	0.274	1199	285	0.238	2376	574	0.242	2355	600	0.255
4800	2450	667	0.272	1225	291	0.238	2425	587	0.242	2396	612	0.255
4900	2498	676	0.271	1258	297	0.236	2472	599	0.242	2443	630	0.258
5000	2549	686	0.269	1287	304	0.236	2524	611	0.242	2501	651	0.260

Table 5.5 Experiment data collection 5 results

5.3.6- Average Value of Collected Data

In this stage the average value of each data collected was calculated based on collected data from Table 5.1 to Table 5.5, The analysis and analysis charts have been created base on average value of data shown below, the average value of collected data shown in Table 5.6 below:

Photon Number	BB84			B92			BBM92			BB84 with Spin 1/2		
	Nk	Ne	Np	Nk	Ne	Np	Nk	Ne	Np	NK	Ne	Np
100	50	12	0.238	22	5	0.209	51	12	0.235	48	13	0.282
200	102	25	0.250	47	10	0.219	101	24	0.241	95	27	0.285
300	152	39	0.253	74	16	0.212	149	38	0.256	145	37	0.254
400	204	50	0.246	96	20	0.210	196	50	0.253	196	49	0.248
500	258	63	0.245	125	26	0.212	244	63	0.258	248	62	0.251
600	309	75	0.244	149	33	0.223	295	76	0.257	298	76	0.254
700	360	88	0.246	174	40	0.229	350	90	0.257	348	88	0.254
800	408	102	0.249	200	47	0.235	400	105	0.262	396	101	0.255
900	459	113	0.247	225	53	0.234	452	118	0.260	440	112	0.254
1000	508	124	0.244	250	58	0.234	507	133	0.262	496	124	0.250
1100	553	136	0.247	276	65	0.237	557	144	0.258	547	134	0.245
1200	603	146	0.243	300	73	0.243	603	158	0.261	597	148	0.247
1300	654	158	0.241	324	79	0.245	650	169	0.260	649	156	0.240
1400	702	170	0.242	349	83	0.239	701	182	0.259	699	166	0.238
1500	755	180	0.239	373	90	0.241	750	193	0.257	751	176	0.235
1600	804	196	0.244	399	96	0.242	800	207	0.259	801	186	0.232
1700	855	209	0.245	422	102	0.242	851	218	0.256	851	199	0.234
1800	907	224	0.247	450	107	0.238	901	228	0.254	899	211	0.234
1900	960	236	0.246	473	115	0.243	951	240	0.253	950	224	0.235
2000	1008	251	0.249	498	120	0.241	1001	252	0.252	1002	240	0.240
2100	1063	264	0.249	523	127	0.243	1050	263	0.251	1052	250	0.238
2200	1116	279	0.250	549	134	0.244	1099	276	0.251	1099	263	0.239
2300	1163	291	0.250	577	140	0.243	1149	290	0.252	1147	275	0.240
2400	1213	305	0.252	601	145	0.242	1198	302	0.252	1201	290	0.241
2500	1263	317	0.251	623	152	0.245	1250	315	0.252	1252	305	0.244
2600	1312	331	0.252	651	159	0.244	1300	327	0.252	1301	318	0.245
2700	1362	344	0.252	674	164	0.243	1346	341	0.253	1356	333	0.245
2800	1414	357	0.253	698	169	0.242	1394	351	0.252	1404	348	0.248
2900	1464	371	0.254	723	175	0.242	1446	365	0.252	1456	360	0.248
3000	1514	385	0.254	748	181	0.242	1496	377	0.252	1505	374	0.249
3100	1563	399	0.255	774	189	0.244	1539	386	0.251	1556	386	0.248
3200	1618	413	0.255	799	194	0.243	1588	400	0.252	1606	398	0.248
3300	1668	426	0.255	824	201	0.244	1638	413	0.252	1659	410	0.247
3400	1717	438	0.255	849	210	0.247	1689	426	0.252	1709	424	0.248
3500	1766	450	0.255	871	217	0.249	1739	439	0.252	1757	437	0.248
3600	1817	465	0.256	897	226	0.252	1794	455	0.254	1811	449	0.248
3700	1867	477	0.255	921	231	0.251	1842	467	0.254	1860	463	0.249
3800	1914	487	0.255	944	237	0.251	1893	480	0.254	1909	474	0.248
3900	1964	500	0.254	966	242	0.250	1944	490	0.252	1960	488	0.249
4000	2015	512	0.254	990	248	0.251	1990	501	0.252	2013	503	0.250
4100	2063	525	0.254	1016	255	0.251	2037	514	0.252	2062	516	0.250
4200	2115	536	0.254	1043	261	0.250	2087	525	0.251	2114	532	0.251
4300	2164	551	0.255	1067	266	0.250	2141	538	0.252	2166	544	0.251
4400	2214	563	0.254	1094	272	0.249	2189	550	0.251	2216	557	0.252
4500	2262	574	0.254	1122	278	0.248	2237	564	0.252	2269	571	0.252
4600	2314	586	0.253	1146	284	0.248	2288	577	0.252	2318	583	0.252
4700	2367	598	0.253	1174	291	0.248	2339	588	0.252	2368	595	0.251
4800	2413	612	0.254	1195	297	0.248	2390	602	0.252	2414	608	0.252
4900	2462	625	0.254	1219	303	0.248	2441	615	0.252	2466	622	0.252
5000	2512	635	0.253	1246	309	0.248	2493	627	0.251	2517	636	0.253

Table 5.6 Experiment average data collection results

Chapter 6

Analysis, Discussion and Comparison

This chapter will perform a comparison between this thesis data collection with following previous QKD survey experiment:

- 1) Beatrix Rambu and Nana Rachmana (2018) with 1000 sent photon range
- 2) Ali Ibum and Nana Rachmana (2018) with same range of 2000 photon sent

This will give a better understanding on analysing of generated probability key of selected protocols. The error detection level can be determining if there is any improvement in the generated error probability key of QKD by increasing the photon range to 5000 in existing protocols and evaluating the new protocol of BB84 with Spin $\frac{1}{2}$

6.1 – Comparison with Beatrix Rambu and Nana Rachmana Evaluation (1000 Photon range for BB84 and B92 Protocols)

As this evaluation was reviewed on chapter 3, Rambu and Rachmana evaluation results of probability error data for BB84 and B92 protocols are shown in Table 6.1 as below:

Photon (N _{tot})	BB84			B92		
	N _{key}	N _{err}	N _{err} /N _{key}	N _{key}	N _{err}	N _{err} /N _{key}
100	46	9	0.196	29	6	0.207
200	99	28	0.283	53	13	0.245
300	136	35	0.257	75	19	0.253
400	182	45	0.247	95	23	0.242
500	240	55	0.229	119	26	0.218
600	279	67	0.24	146	33	0.226
700	325	80	0.246	173	37	0.214
800	374	93	0.249	196	39	0.248
900	421	98	0.233	223	45	0.199
1000	463	106	0.229	246	48	0.202

Table 6.1 BB84 and B92 Error Probability ratio [3]

During the reviewing of data collection some inaccurate data calculation of N_p for B92 protocol for photon Numbers of 800,900 and 1000 were found, which have been marked on Table 6.1, Below are the correct value of N_p that have been recalculated, Table 6.2 shows the correct N_p data results:

Photon Number	Nk	Ne	Np
800	196	39	0.199
900	223	45	0.202
1000	246	48	0.195

Table 6.2 Correct data evaluation of NP for B92 protocol

Data results for same environment and photon number of 1000 photons for these two protocols by this thesis shown in Table 6.3:

Photon Number	BB84			B92		
	NK	Ne	Np	NK	Ne	Np
100	50	12	0.238	22	5	0.209
200	102	25	0.250	47	10	0.219
300	152	39	0.253	74	16	0.212
400	204	50	0.246	96	20	0.210
500	258	63	0.245	125	26	0.212
600	309	75	0.244	149	33	0.223
700	360	88	0.246	174	40	0.229
800	408	102	0.249	200	47	0.235
900	459	113	0.247	225	53	0.234
1000	508	124	0.244	250	58	0.234

Table 6.3 Evaluation data results for 1000 photon number for BB84 and B92 protocols

6.1.1- Probability Key value comparison for BB84 protocol between Current Evaluation vs Rambu and Rachmana Experiment

BB84 Protocol Comparison

Figure 6.1 shows the comparison results of this thesis vs Rambu and Rachmana for BB84 Protocol using 1000 Polarized photons:

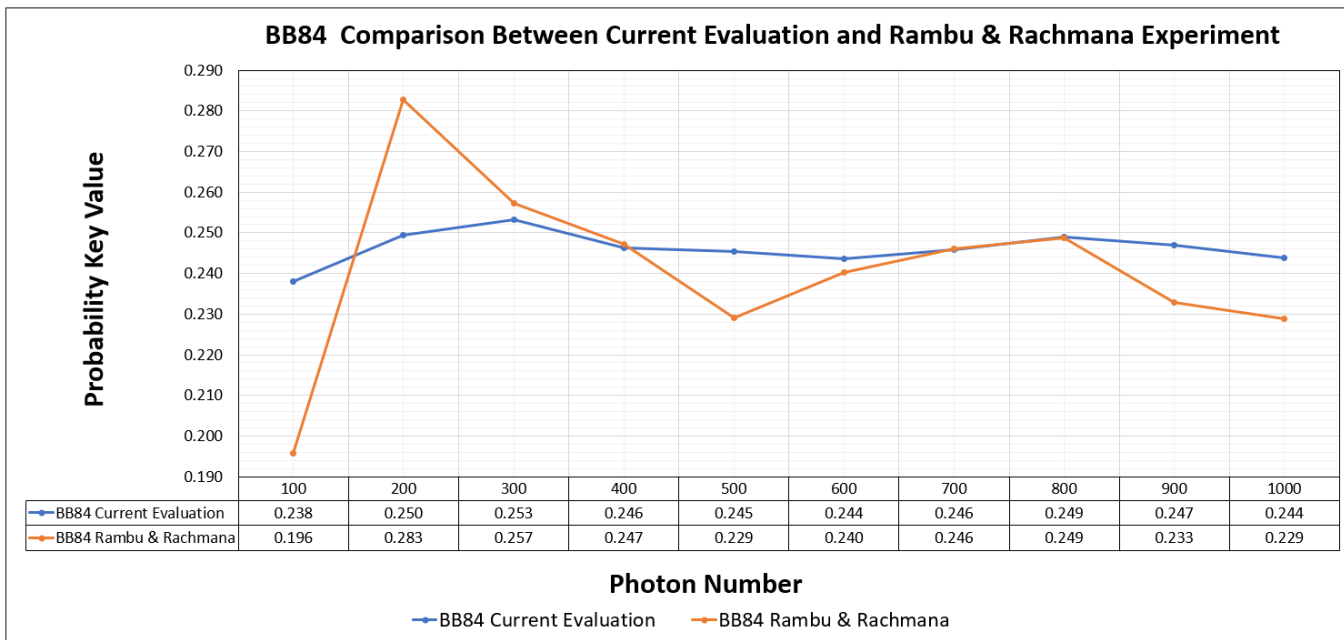


Figure 6.1 BB84 Np Comparison of current evaluation vs Rambu & Rachmana

According to figure 6.1 the N_p value for BB84 protocol has the values of Lowest 0.196 (%19.6) and highest value of 0.283 (%28.3) with average value of 0.241 (%24.1)

Current evaluation by this thesis has the values of Lowest 0.238 (% 23.8), highest of 0.253 (%25.3) and average value of 0.246 (%24.6), higher rates of error probability in current are in photon numbers of 100 to 150 also from 400 to 1000 photons. also has higher rate between 800 to 1000 photon number which determined current evaluation has more accuracy results as we repeated the evaluation five times. In average the current evaluation rate with 0.246 is higher than average N_p of 0.241 from Rambu and Rachana.

6.1.2- Probability Key value comparison for B92 protocol between Current Evaluation vs Rambu and Rachmana Experiment

B92 Protocol Comparison

Figure 6.2 shows this thesis experimental comparison results vs Rambu and Rachmana for B92 protocol using 1000 polarized photons:

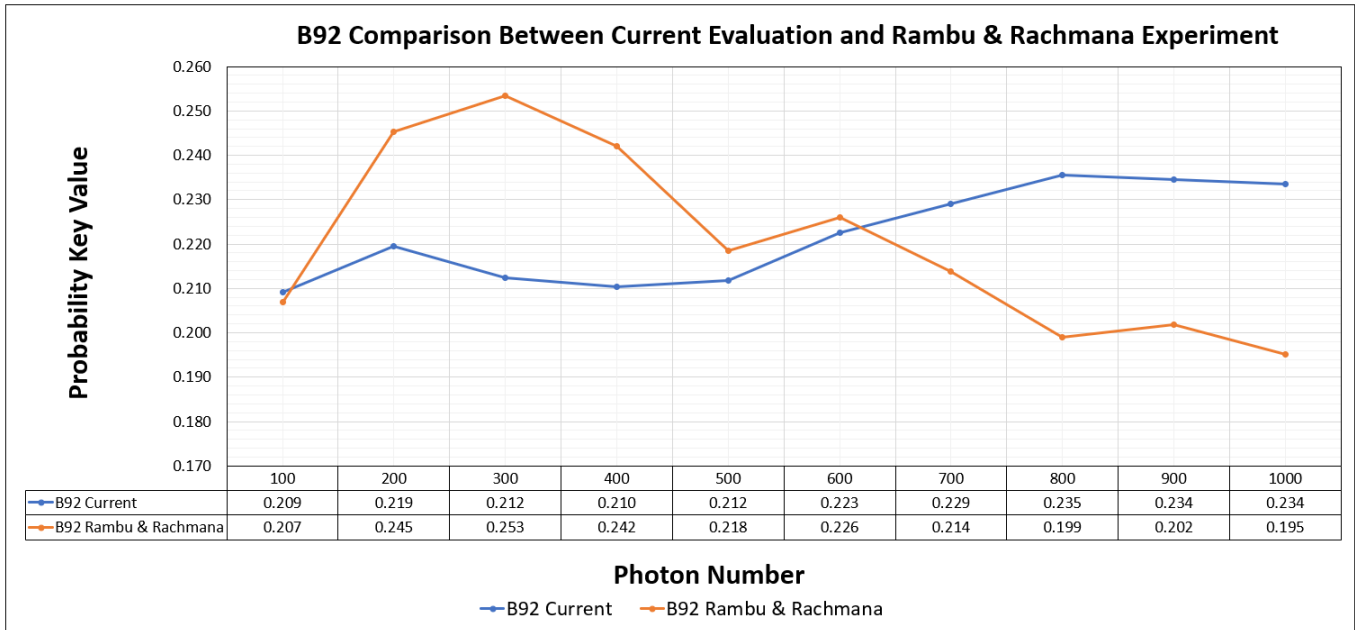


Figure 6.2 B92 N_p comparison of current evaluation vs Rambu & Rachmana

Based on Figure 6.2 the key values of B92 protocol are as lowest 0.199 (%19.9), highest of 0.253 (%25.3) and based on this thesis calculation the average amount of 0.220 (%22.0) for Rambu and Rachana experiment.

This thesis experiment N_p values are as lowest 0.209 (%20.9), highest value of 0.235 (%23.5) and average amount of 0.222 (%22.2) Current evaluation data has higher level of error probability in range of 650 to 1000 photon also in 100 to 120 photons, the difference between lowest: 0.209 to highest 0.235 in current evaluation is less than the difference in previous experiment which determined that the current evaluation has more precise data results.

Current experiment average result of N_p (0.222) is higher than average N_p of 0.220 from Rambu and Rachana for B92 protocol.

Table 6.4 illustrate a summary of N_p value comparison between Rambu and Rachmana Evaluation and current experiment data collection.

BB84	Rambu and Rachmana Evaluation	Np (L)	0.196 (%19.6)
		Np (H)	0.283 (%28.3)
		Np (avg.)	0.241 (%24.1)
	Current Evaluation	Np (L)	0.238 (% 23.8)
		Np (H)	0.253 (%25.3)
		Np (avg.)	0.246 (%24.6)
B92	Rambu and Rachmana Evaluation	Np (L)	0.199 (%19.9)
		Np (H)	0.253 (%25.3)
		Np (avg.)	0.220 (%22.0)
	Current Evaluation	Np (L)	0.209 (%20.9)
		Np (H)	0.235 (%23.5)
		Np (avg.)	0.222 (%22.2)

Table 6.4 Summary of Np value comparison between current evaluation vs Rambu and Rachmana Evaluation

Based on data on Table 6.4 the average value of Np for both protocols of B92, BB84 by running 1000 polarized photons in current evaluation have higher value than Rambu and Rachmana evaluation which this might be again related to simulation environment, Network setup or the other facts as this experiments are based on random polarization sent photons, but in general this thesis experiment results are more accurate as the process of data collection has been repeated five times and final analysis have been performed based on average value of each collected data.

6.2 – Comparison with Ali Ibnun and Nana Rachmana Evaluation (2000 Photon range for BB84, B92 and BBM92 Protocols)

This evaluation experiment has been performed with range of 2000 photon polarization for BB84, B92 and BBM92 protocols as we reviewed it on Chapter 3.

Table 6.5 shows the simulation data collection result of keys generation as below:

Phot-on Number	BB84			B92			BBM92		
	N_k	N_e	N_p	N_k	N_e	N_p	N_k	N_e	N_p
100	52	12	0.231	16	4	0.25	47	12	0.255
200	95	25	0.263	43	11	0.256	99	20	0.202
300	140	39	0.279	68	16	0.235	146	39	0.267
400	192	56	0.292	90	23	0.256	201	53	0.264
500	249	78	0.313	117	26	0.222	250	69	0.276
600	249	88	0.301	146	29	0.199	288	78	0.271
700	292	99	0.289	178	35	0.197	344	91	0.265
800	342	112	0.289	214	44	0.207	395	100	0.253
900	388	126	0.287	239	49	0.205	444	116	0.261
1000	439	139	0.281	265	58	0.219	498	132	0.265
1100	495	159	0.288	288	65	0.226	545	147	0.27
1200	552	171	0.284	310	74	0.239	601	161	0.268
1300	603	180	0.277	334	82	0.246	653	171	0.262
1400	700	187	0.267	361	92	0.255	705	184	0.261
1500	744	200	0.269	394	103	0.261	752	198	0.263
1600	792	209	0.264	416	108	0.26	800	218	0.273
1700	845	226	0.267	443	112	0.253	854	233	0.273
1800	901	237	0.263	470	120	0.255	910	246	0.27
1900	939	246	0.262	491	122	0.248	958	262	0.237
2000	999	257	0.257	511	125	0.245	1004	272	0.271

Table 6.5 Simulation results of key and error from Ali Ibnun and Nana Rachmana evaluation (2000 photon polarization) [31]

During the review of the collected data of this evaluation some inaccurate data calculation has been found in N_p for BB84 protocol for photon number range of 600 to 1300 which have been marked on Table 6.5. The correct N_p Values have been recalculated. Table 6.6 shows the correct values:

Photon Number	BB84		
	Nk	Ne	N_p
600	249	88	0.353
700	292	99	0.339
800	342	112	0.327
900	388	126	0.325
1000	439	139	0.317
1100	495	159	0.321
1200	552	171	0.310
1300	603	180	0.299

Table 6.6 Recalculated NP value of Ali Ibnun and Nana Rachmana Evaluation

Table 6.7 shows the current experiment data result for same photon range of 2000 photons for below three protocols:

Photon Number	BB84			B92			BBM92		
	Nk	Ne	N_p	Nk	Ne	N_p	Nk	Ne	N_p
100	50	12	0.238	22	5	0.209	51	12	0.235
200	102	25	0.250	47	10	0.219	101	24	0.241
300	152	39	0.253	74	16	0.212	149	38	0.256
400	204	50	0.246	96	20	0.210	196	50	0.253
500	258	63	0.245	125	26	0.212	244	63	0.258
600	309	75	0.244	149	33	0.223	295	76	0.257
700	360	88	0.246	174	40	0.229	350	90	0.257
800	408	102	0.249	200	47	0.235	400	105	0.262
900	459	113	0.247	225	53	0.234	452	118	0.260
1000	508	124	0.244	250	58	0.234	507	133	0.262
1100	553	136	0.247	276	65	0.237	557	144	0.258
1200	603	146	0.243	300	73	0.243	603	158	0.261
1300	654	158	0.241	324	79	0.245	650	169	0.260
1400	702	170	0.242	349	83	0.239	701	182	0.259
1500	755	180	0.239	373	90	0.241	750	193	0.257
1600	804	196	0.244	399	96	0.242	800	207	0.259
1700	855	209	0.245	422	102	0.242	851	218	0.256
1800	907	224	0.247	450	107	0.238	901	228	0.254
1900	960	236	0.246	473	115	0.243	951	240	0.253
2000	1008	251	0.249	498	120	0.241	1001	252	0.252

Table 6.7 My evaluation data simulation results of protocols in 2000 photon range (Current experiment).

6.2.1- N_p value comparison between Current Evaluation vs Ali Ibnun and Nana Rachmana Experiment (BB84, B92 and BBM92 Protocols)

This section will have a N_p value comparison of Rambu and Rachmana experiment and current evaluation, Figure 6.3 shows the value comparison of N_p from previous experiment from Rambu and Rachmana for three protocols of BB84, B92 and BBM92 in range of 2000 photons:

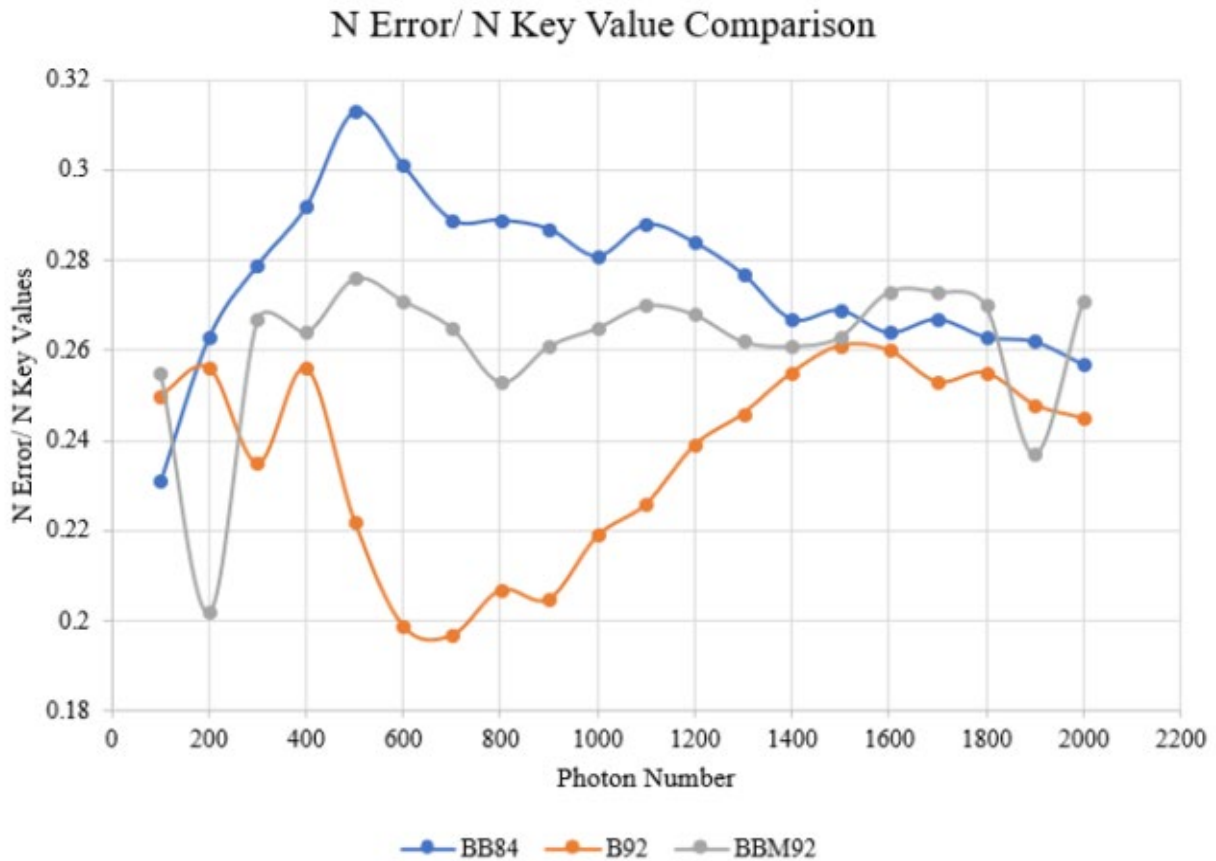


Figure 6.3 Value comparison of N error/ N key value (Probability error) on each protocol from Ali Ibnun and Nana Rachmana experiment [31]

B92 Protocol Comparison

Based on figure 6.3 the lowest amount of N_p comes from B92 protocol in range of 0.199 (%19.9) to 0.256 (%25.6). theoretically this value can be up to %25 for B92 protocol, this result can be influenced by design, setup, or environment. The average amount of B92 N_p has the amount of 0.237 (%23.7) according to this thesis calculations.

In current evaluation the amount of N_p for B92 protocol shows the range of 0.209 (%20.9) to 0.243 (%24.3) which is under %25 of theory value, The average value of N_p for B92 protocol based on current experiment is 0.231 (%23.1) which seems current data collection are more accrue as the process of data collection has been repeated five times.

Figure 6.4 illustrate the value comparison of N error/ N key value (Probability error) on each protocol by current evaluation.

Probability Value Comparison

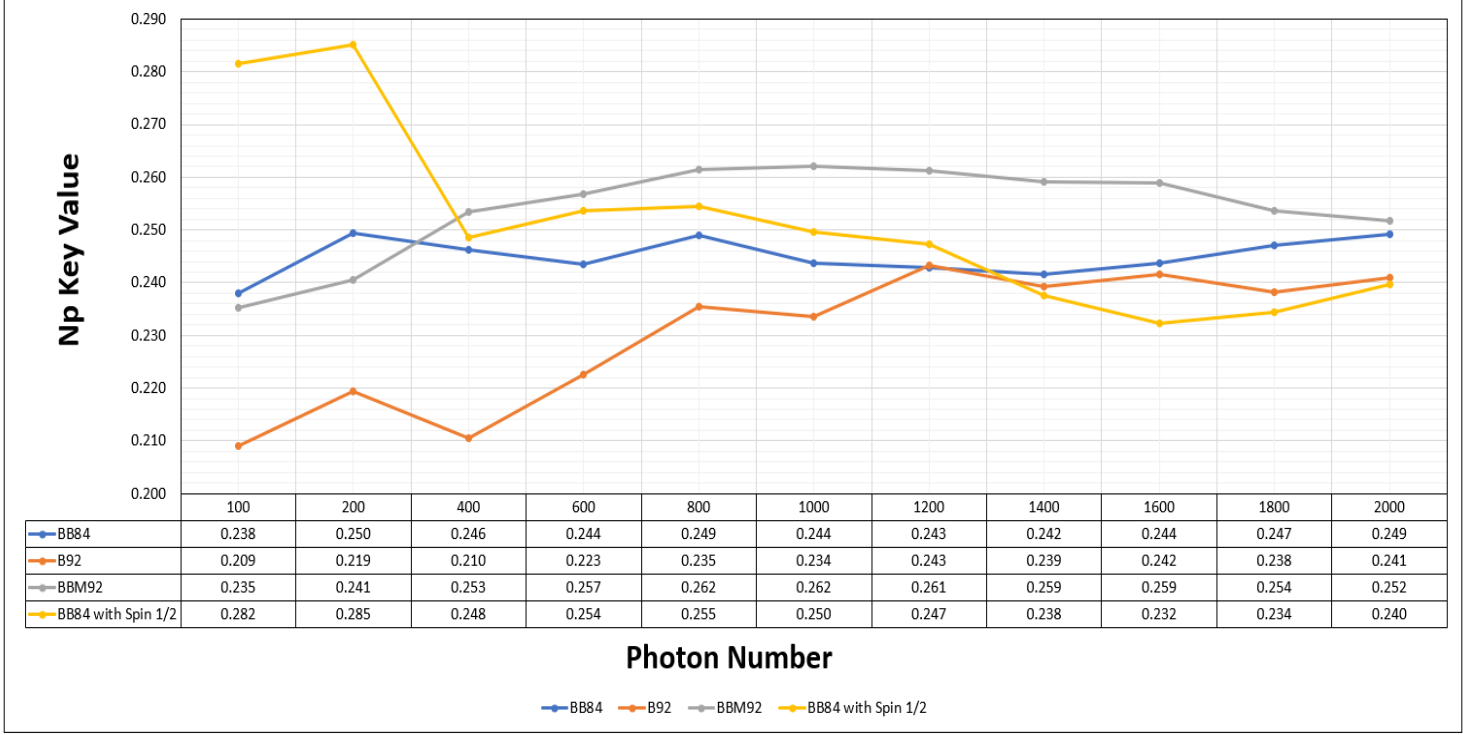


Figure 6.4 Value Comparison of N Error/N Key value (Probability Error) on each Protocol in range of 2000 Photons from current experiment.

BB84 Protocol comparison

The result for BB84 protocol based on Figure 6.3 shows the N_p lowest amount of 0.231 (%23.1) and highest amount of 0.353 (%35.3). The average amount of N_p based on this thesis calculation shows 0.291 (%29.1).

Current evaluation results based on Figure 6.4 show the lowest value of 0.238 (%23.8) and highest of 0.253 (%25.3) and the average amount of 0.245 (%24.5), both experiments shows the value under (%50) which can be the highest amount of error probability by theory. In average my experiment has lower value of Error probability.

BBM92 Protocol comparison

BBM92 protocol has the result of lowest value of 0.202 (%20.2) and highest value of 0.276 (%27.6) based on figure 6.3 with the average value of 0.263 (%26.3).

The values for this protocol based on Figure 6.4 on current evaluation shows lowest value of 0.235 (%23.5), highest value of 0.262 (%26.2) and average value based on this thesis calculation comes up as 0.255 (%25.5).

Table 6.8 is a summary of N_p comparison collected data of Ali Ibnun and Nana Rachmana Evaluation and the current Evaluation:

B92	Ali Ibnun and Nana Rachmana Evaluation	Np (L)	0.199 (%19.9)
		Np (H)	0.256 (%25.6)
		Np (avg.)	0.237 (%23.7)
	Current Evaluation	Np (L)	0.209 (%20.9)
		Np (H)	0.243 (%24.3)
		Np (avg.)	0.231 (%23.1)
BB84	Ali Ibnun and Nana Rachmana Evaluation	Np (L)	0.231 (%23.1)
		Np (H)	0.353 (%35.3)
		Np (avg.)	0.291 (%29.1)
	Current Evaluation	Np (L)	0.238 (%23.8)
		Np (H)	0.253 (%25.3)
		Np (avg.)	0.245 (%24.5)
BBM92	Ali Ibnun and Nana Rachmana Evaluation	Np (L)	0.202 (%20.2)
		Np (H)	0.276 (%27.6)
		Np (avg.)	0.263 (%26.3)
	Current Evaluation	Np (L)	0.235 (%23.5)
		Np (H)	0.262 (%26.2)
		Np (avg.)	0.255 (%25.5)

Table 6.8 Summary of Np value comparison between current evaluation and Ali Ibnun and Nana Rachmana Evaluation (2000 Photons range)

According to data on Table 6.8 the average value of NP for all three protocols of B92, BB84 and BBM92 by running 2000 photon polarization in current evaluation have lower value than Ali Ibnun and Nana Rachmana evaluation experiment, this might be related to simulation environment, Network setup or other facts as this experiments are based on random polarization photons, but in general current experiment results are more accurate as the process of data collection has been repeated five times and final analysis have been performed base on average value of each collected data.

6.3 – Simulations and Results of Current Experiment

This section simulated four QKD protocols including of two P&M based protocols (BB84 and B92), and two entanglement-based protocol (BBM92 and BB84 with Spin 1/2). This Experiment has been performed in QuVis simulation environment. The experiment setup are as follows:

- Four protocols are involved in this experiment simulation which are: BB84, B92, BBM92 and BB84 with Spin 1/2 protocols.
- The experiment is organized and carried out by involvement of the passive eavesdropping.
- Alice (sender) and Bob(receiver) both use a random basis to send polarized photon for each protocol experiments.
- Eavesdropper also uses the random base to decode and translate the base polarization photon of Alice.
- This experiment using the “fast forward 100 photons” feature of the QuVis.
- The experiments executed by sending 100 to 5000 photons.
- N_{key} (N_k), N_{error} (N_e), and N_{error}/N_{key} (N_p) are the measured value parameters in this experiment for each protocol.

6.4 – Generated Keys of Simulation Results (Average Value of Data Collection)

Data collection Process for this Experiment has been executed five times in QuVis simulation environment, then the average data value for each individual data has been calculated, Table 6.9 below shows this thesis data value collection results of N_k (Key generated value), N_e (Error key generated value) and N_p (Error probability key generated value) for BB84, B92, BBM92 and BB84 with Spin $\frac{1}{2}$ protocols.

Data Collection Results (Average)

Photon Number	BB84			B92			BBM92			BB84 with Spin $\frac{1}{2}$		
	N_k	N_e	N_p	N_k	N_e	N_p	N_k	N_e	N_p	N_k	N_e	N_p
100	50	12	0.238	22	5	0.209	51	12	0.235	48	13	0.282
200	102	25	0.250	47	10	0.219	101	24	0.241	95	27	0.285
300	152	39	0.253	74	16	0.212	149	38	0.256	145	37	0.254
400	204	50	0.246	96	20	0.210	196	50	0.253	196	49	0.248
500	258	63	0.245	125	26	0.212	244	63	0.258	248	62	0.251
600	309	75	0.244	149	33	0.223	295	76	0.257	298	76	0.254
700	360	88	0.246	174	40	0.229	350	90	0.257	348	88	0.254
800	408	102	0.249	200	47	0.235	400	105	0.262	396	101	0.255
900	459	113	0.247	225	53	0.234	452	118	0.260	440	112	0.254
1000	508	124	0.244	250	58	0.234	507	133	0.262	496	124	0.250
1100	553	136	0.247	276	65	0.237	557	144	0.258	547	134	0.245
1200	603	146	0.243	300	73	0.243	603	158	0.261	597	148	0.247
1300	654	158	0.241	324	79	0.245	650	169	0.260	649	156	0.240
1400	702	170	0.242	349	83	0.239	701	182	0.259	699	166	0.238
1500	755	180	0.239	373	90	0.241	750	193	0.257	751	176	0.235
1600	804	196	0.244	399	96	0.242	800	207	0.259	801	186	0.232
1700	855	209	0.245	422	102	0.242	851	218	0.256	851	199	0.234
1800	907	224	0.247	450	107	0.238	901	228	0.254	899	211	0.234
1900	960	236	0.246	473	115	0.243	951	240	0.253	950	224	0.235
2000	1008	251	0.249	498	120	0.241	1001	252	0.252	1002	240	0.240
2100	1063	264	0.249	523	127	0.243	1050	263	0.251	1052	250	0.238
2200	1116	279	0.250	549	134	0.244	1099	276	0.251	1099	263	0.239
2300	1163	291	0.250	577	140	0.243	1149	290	0.252	1147	275	0.240
2400	1213	305	0.252	601	145	0.242	1198	302	0.252	1201	290	0.241
2500	1263	317	0.251	623	152	0.245	1250	315	0.252	1252	305	0.244
2600	1312	331	0.252	651	159	0.244	1300	327	0.252	1301	318	0.245
2700	1362	344	0.252	674	164	0.243	1346	341	0.253	1356	333	0.245
2800	1414	357	0.253	698	169	0.242	1394	351	0.252	1404	348	0.248
2900	1464	371	0.254	723	175	0.242	1446	365	0.252	1456	360	0.248
3000	1514	385	0.254	748	181	0.242	1496	377	0.252	1505	374	0.249
3100	1563	399	0.255	774	189	0.244	1539	386	0.251	1556	386	0.248
3200	1618	413	0.255	799	194	0.243	1588	400	0.252	1606	398	0.248
3300	1668	426	0.255	824	201	0.244	1638	413	0.252	1659	410	0.247
3400	1717	438	0.255	849	210	0.247	1689	426	0.252	1709	424	0.248
3500	1766	450	0.255	871	217	0.249	1739	439	0.252	1757	437	0.248
3600	1817	465	0.256	897	226	0.252	1794	455	0.254	1811	449	0.248
3700	1867	477	0.255	921	231	0.251	1842	467	0.254	1860	463	0.249
3800	1914	487	0.255	944	237	0.251	1893	480	0.254	1909	474	0.248
3900	1964	500	0.254	966	242	0.250	1944	490	0.252	1960	488	0.249
4000	2015	512	0.254	990	248	0.251	1990	501	0.252	2013	503	0.250
4100	2063	525	0.254	1016	255	0.251	2037	514	0.252	2062	516	0.250
4200	2115	536	0.254	1043	261	0.250	2087	525	0.251	2114	532	0.251
4300	2164	551	0.255	1067	266	0.250	2141	538	0.252	2166	544	0.251
4400	2214	563	0.254	1094	272	0.249	2189	550	0.251	2216	557	0.252
4500	2262	574	0.254	1122	278	0.248	2237	564	0.252	2269	571	0.252
4600	2314	586	0.253	1146	284	0.248	2288	577	0.252	2318	583	0.252
4700	2367	598	0.253	1174	291	0.248	2339	588	0.252	2368	595	0.251
4800	2413	612	0.254	1195	297	0.248	2390	602	0.252	2414	608	0.252
4900	2462	625	0.254	1219	303	0.248	2441	615	0.252	2466	622	0.252
5000	2512	635	0.253	1246	309	0.248	2493	627	0.251	2517	636	0.253

Table 6.9 Experiment average data Collection Results of Current Experiment

6.5 – N_k Value Comparison

The value of N_{key} (N_k) result data collections of this simulation are presented in Figure 6.5, as we can see from this figures the most number key generated is 2517 keys for 5000 photons sent using BB84 with Spin ½ protocol, while the least number key generated is 22 keys for 100 photons sent using B92 protocol, The reason is because the B92 protocol used only 2 polarized bases as the other there protocols used 4 polarized bases. This differences in bases used between these four protocols also causes few or many keys agreed by sender and receiver. This determines the level of error detection or due to a change in the status of quantum by eavesdropping. In general, the greater number of keys generated, the better.

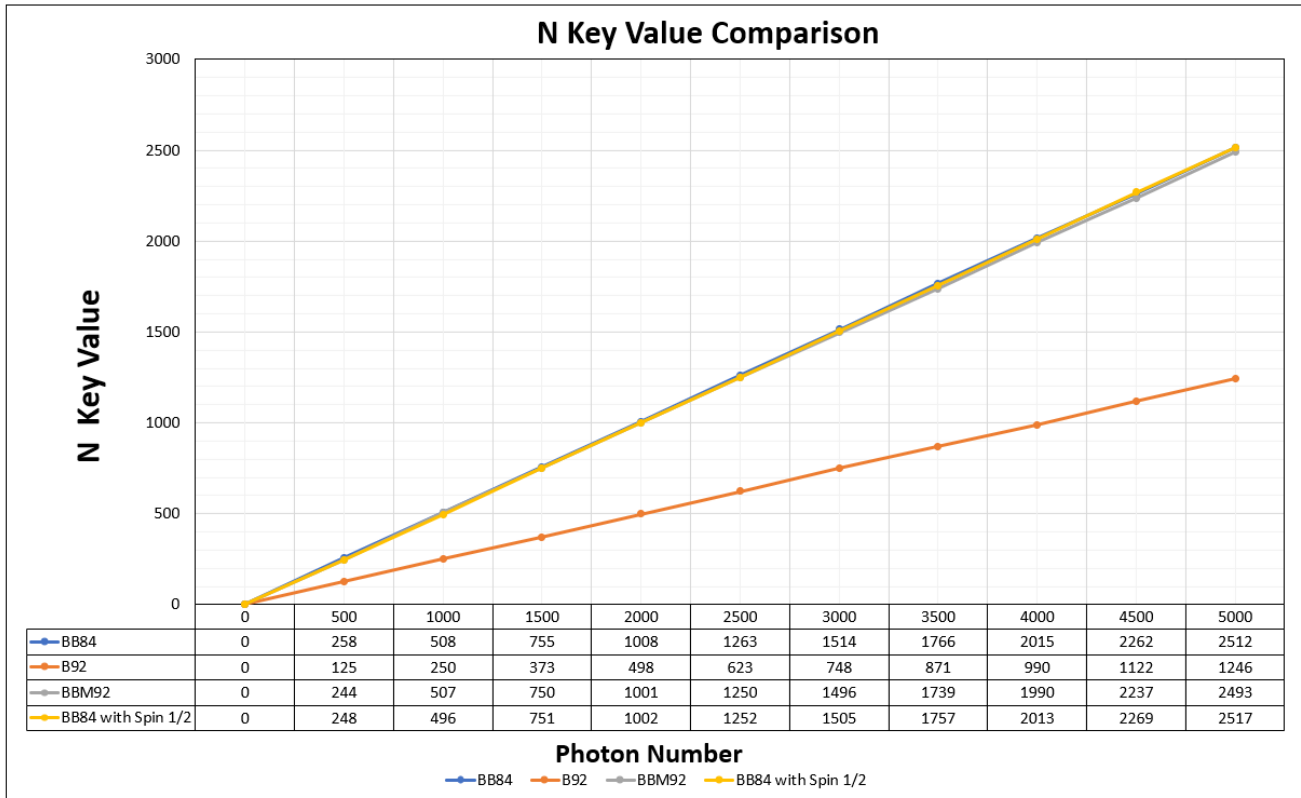


Figure 6.5 N Key Value Comparison of BB84, B92, BBM92 and BB84 with Spin ½ Protocol

Table 6.10 shows the summary of N_k Comparison, as we can see the BB84 with Spin ½ has the highest value of 1279.56 on N_k in Average.

	Nk (L)	50
BB84	Nk (H)	2512
	Nk (avg.)	128.80
	Nk (L)	22
B92	Nk (H)	1246
	Nk (avg.)	635.01
	Nk (L)	51
BBM92	Nk (H)	2493
	Nk (avg.)	1270.69
	Nk (L)	48
BB84 with Spin 1/2	Nk (H)	2517
	Nk (avg.)	1279.56

Table 6.10 Nk Value comparison summary

6.6 – Ne Value comparison

In Figure 6.6 is shown that the most number error obtained is 636 errors for 5000 photons sent using BB84 with Spin $\frac{1}{2}$ protocol which is slightly higher than the value of 635 by BB84 protocol, while the least number error obtained is 5 errors for 100 photons sent using B92 protocol. The fewer number of errors obtained, the better.

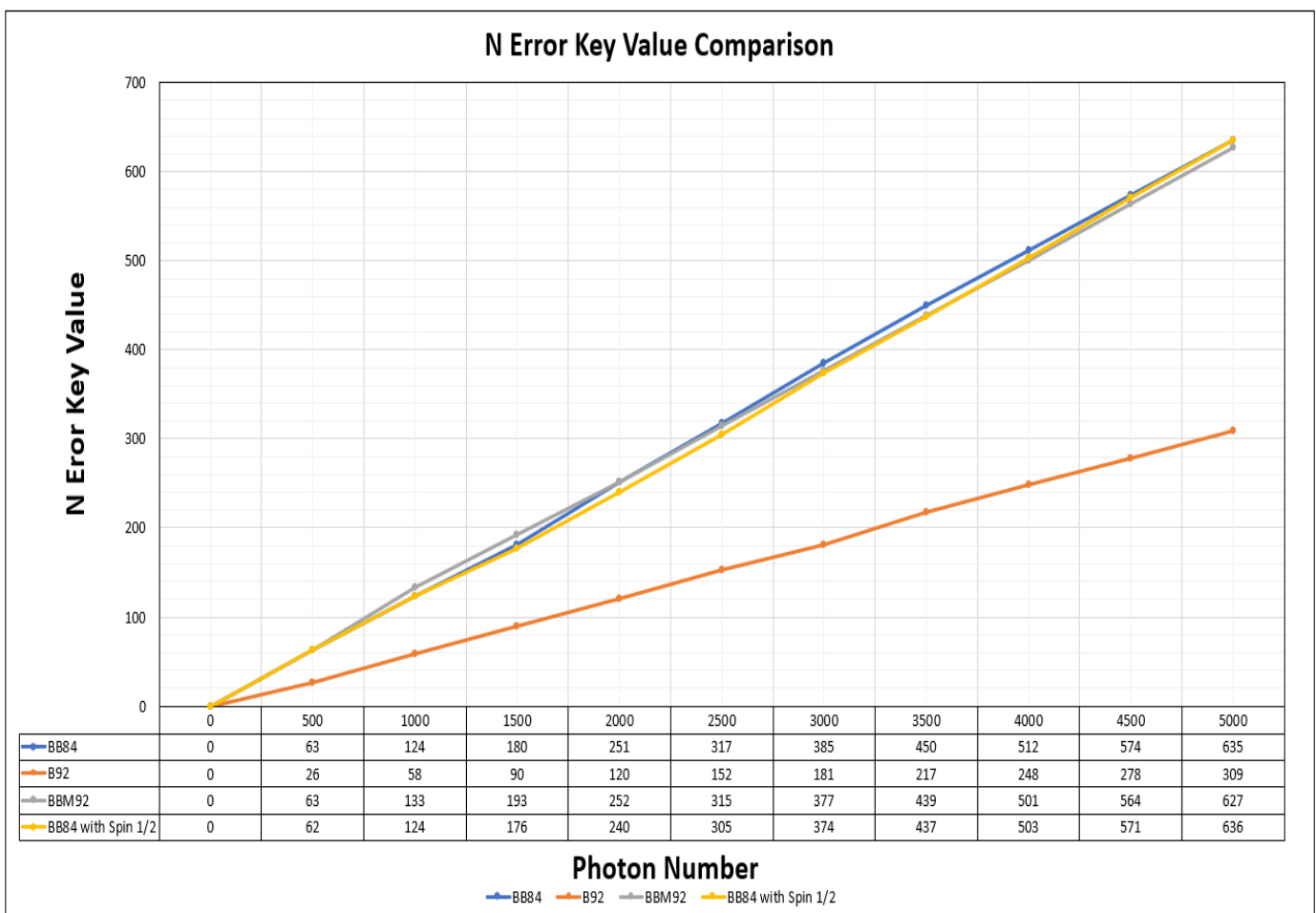


Figure 6.6 Ne Value comparison of BB84, B92, BBM92 and BB84 with Spin $\frac{1}{2}$ protocol

Table 6.11 shows the summary of Ne comparison, as we can see the BB84 with Spin $\frac{1}{2}$ has the lowest value of 316.83 Nk in Average compare to BB84 and BBM92, These three protocols use 4 base of polarization, However the B92 has the value of 155.94 Nk in average as this Protocol use only two bases of polarization. BB84 with spin $\frac{1}{2}$ is the better Protocol in average value of Ne compare to BB84 and BBM92.

	Ne (L)	12
BB84	Ne (H)	635
	Ne (avg.)	324.32
	Ne (L)	5
B92	Ne (H)	309
	Ne (avg.)	155.94
	Ne (L)	12
BBM92	Ne (H)	627
	Ne (avg.)	321.22
	Ne (L)	13
BB84 with Spin 1/2	Ne (H)	636
	Ne (avg.)	316.83

Table 6.11 Ne Value comparison summary

6.7 – Np Value Comparison

According to Figure 6.7 the smallest probability of error belongs to B92 protocol by the range of 0.209 (20.9%) to 0.252 (25.2%). In theory the limit of highest error value of B92 protocol is 25%, however in non-ideal setup condition, design or environment can affected the value result. Instead, the largest probability of error is obtained by different protocol in different range, For example BB84 with spin $\frac{1}{2}$ has highest value in range of 100 to 200 ranged from 0.282 (28.2%) to 0.285 (28.5%). In range of 300 to 2700 photons BBM92 protocol has the highest value from 0.251 (25.1%) to 0.262 (26.2%). In range of 2800 to 4900 photons BB84 protocol has the highest value from 0.253 (25.3%) to 0.256 (25.6%), and in 5000 photons BB84 and BB84 with Spin $\frac{1}{2}$ have the highest value of 0.253 (25.3%).

In theory the maximum error value of BB84, BBM92 and BB84 with Spin $\frac{1}{2}$ protocols is 0.5 (50%). Calculated average value of Np for all four protocols shows that BBM92 protocol has the highest average value of 0.253 (25.3%), BB84 protocol is next with 0.250 (25.0%) then BB84 with Spin $\frac{1}{2}$ protocol which has the value of 0.248 (24.8%) and the lowest average value of Np belongs to B92 of 0.241 (24.1%).

Probability Value Comparison

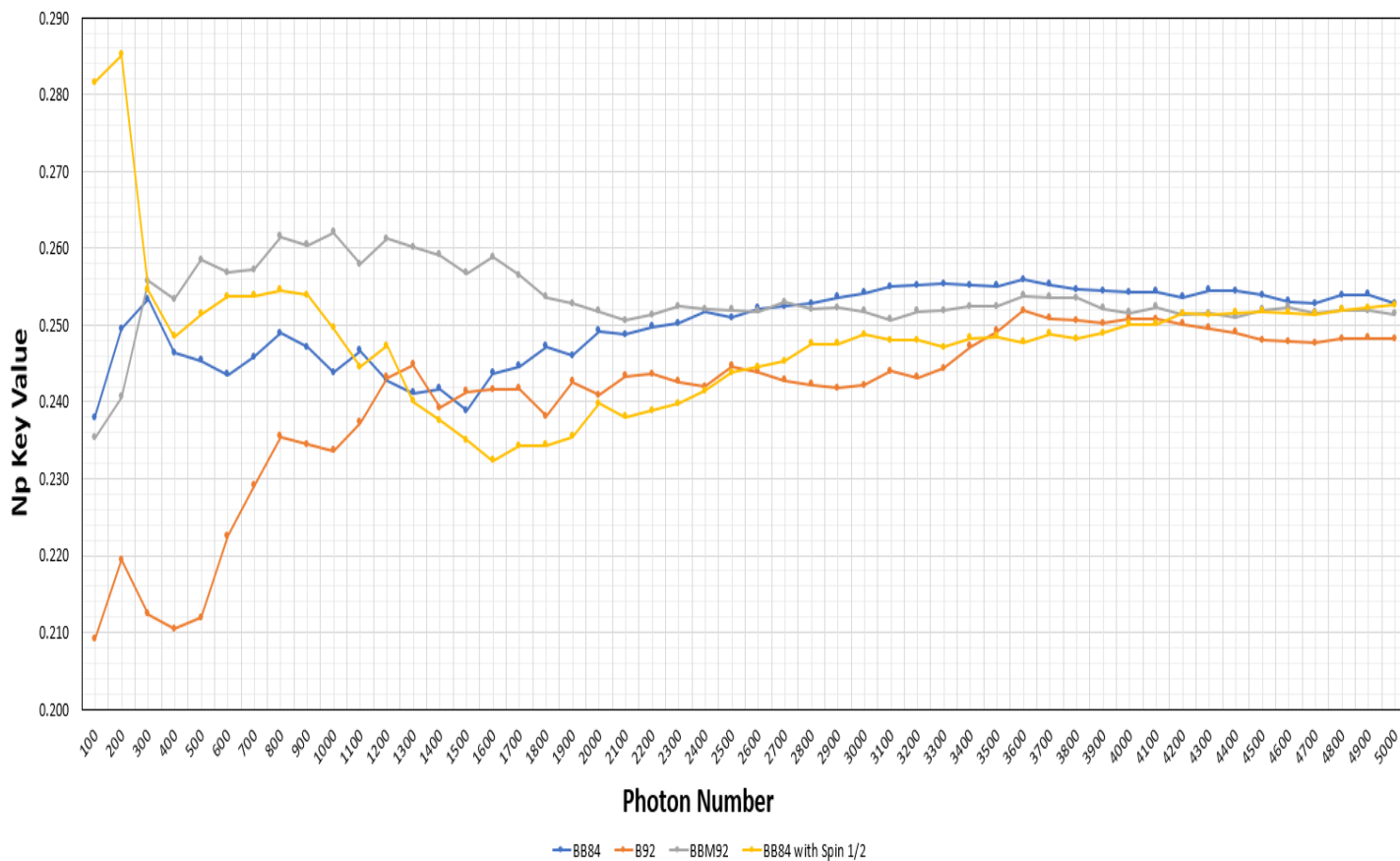


Figure 6.7 Ne/ Nk Value comparison of BB84, B92, BBM92 and BB84 with Spin 1/2 protocol

Table 6.12 shows the summary of Np comparison between these four QKD protocols:

	Np (L)	0.238
BB84	Np (H)	0.256
	Np (avg.)	0.250
	Np (L)	0.209
B92	Np (H)	0.252
	Np (avg.)	0.241
	Np (L)	0.235
BBM92	Np (H)	0.262
	Np (avg.)	0.253
	Np (L)	0.232
BB84 with Spin 1/2	Np (H)	0.285
	Np (avg.)	0.248

Table 6.12 Np Value comparison summary

Chapter 7

Conclusion and Future review

7.1 – Summary

According to result of my experiment on P&M based protocols (BB84, B92) and the protocols with EB based (BBM92, BB84 with Spin 1/2) that presented in tables (6.9, 6.10, 6.11 and 6.12) and Figures (6.5, 6.6 and 6.7) B92 Protocol has the smaller value of N_p ($N_{\text{error}}/ N_{\text{key}}$) compare to other three protocols (%24.1), This makes sense as the B92 protocol uses only two photon polarization bases and the other protocols use four bases of photon polarization, so that means the B92 protocol is still the best protocol out of these four protocols. This thesis proposal protocol BB84 with Spin $\frac{1}{2}$ has the second place in average of N_p value error probability with average value of %24.8.

The proposal protocol by this thesis is the simplified version of BBM92 protocol which instead of using the third party as the source for submitting entangled states, Sender will be the source provider of photon entangled states, some of the challenges with the third party as a source will be as below:

- 1) A trusted and accepted security provider needed as a third party.
- 2) The third party need to have the essential infrastructure to provide and establish the availability of any type of communications at all the time.
- 3) The most important fact will be the security of environment created by Third party.
- 4) All above facts will increase the cost of establishing the system of submitting Entangled states [47].

Figure 6.8 shows the third party of submitting photon entangled states:

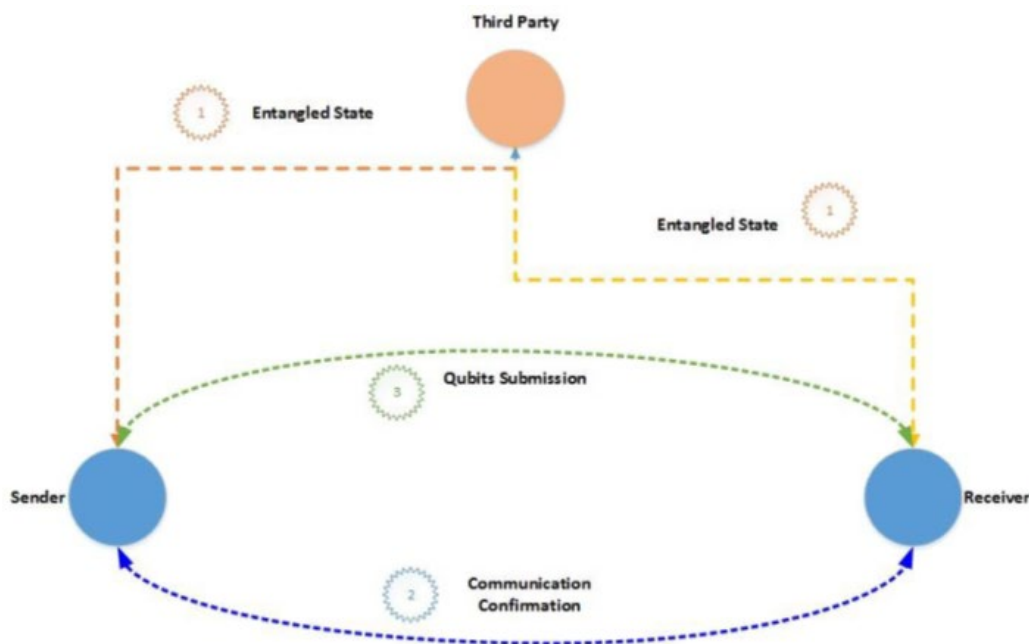


Figure 6.8 the Entangled States submitted by third party. [44]

By using BB84 with Spin $\frac{1}{2}$ there is no need of using the third party and setting up the connection tools and network between the third party and Alice (Sender), This can decrease the cost of using the third party also cost of the implementation significantly and create more efficiency in cost, More control on our network and security, so in general The N_p value of BBM92 protocol has been improved by using the proposed protocol of BB84 with Spin $\frac{1}{2}$, also the cost of devices and network implementation reduced to almost half of the cost we need for BBM92 protocol. However, if we refer to error parameter, QKD network implementation has some factors such as distance, Rate of secret key, robustness, and setup cost etc. which need to be considered delicately.

7.2 – Conclusion

This thesis presents the QKD protocols in a time that can be considered as a converted point in the history of computer science. this thesis demonstrates what has been done so far, and the different between several developed QKD protocols. The most important point about these QKD protocols is that they are all still under experimental work and study and none of them has been completed [44].

There are many difficulties when it comes to QKD system implementation, and it is very easy to reject them from the market as being too expensive to build or too infeasible for wide adoption. In general, according to their current design and capabilities the security is still an issue with physical implementations of QKD systems based on hardware level vulnerabilities. However, these hardships should not make us have any doubt about the complete secure QKD systems possibility. Rather, they should encourage more further research and funding to discover a solution for the issues with physical networks of QKD systems. These experiments research required huge amounts of money, time and effort from different technical community such as security, quantum physics and computer engineering. Nevertheless, the promise of perfect secure encryption and secure communication is absolutely worthy of such a massive enormous resources investment [48].

This thesis described the principles of QKD protocols in brief and presented an overview of the most outstanding QKD protocols in the literature including BB84 protocol and it's variation model of it which Heisenberg's Uncertainty Principle derive their security from, as well as Eckert's approach using quantum entanglement used by B92 and out proposal protocol BB84 with Spin $\frac{1}{2}$ [47]. QKD protocols are based on principles from quantum physics and information theory. QKD is clearly an unconditionally secure means of establishing secret keys. Combined with unconditionally secure authentication, and an unconditionally secure cryptosystem [49]. This thesis also had discussion about new model of QKD protocol that uses sender as the source of photon generator and has more efficiency in using the resource states input [50].

Below are the main results of this experiment:

- The proposal protocol by this thesis (BB84 with Spin $\frac{1}{2}$) is the simplified version of BBM92 protocol which instead of using the third party as the source for submitting Entangled states, Sender will be the source provider of photon entangled states
- BB84 with Spin $\frac{1}{2}$ protocol requires significantly lower cost for implementation and creates more efficiency as there is no need of using third party for submitting Entangled states compare to BBM92 protocol.
- Refer to error parameter, QKD network implementation has some factors such as distance, Rate of secret Key, robustness, and setup cost etc. which need to be considered delicately.

- B92 protocol has the smaller value of N_p ($N_{\text{error}}/ N_{\text{key}}$) compare to other three protocols, This is based on the facts that B92 protocol uses only two photon polarization bases and the other protocols use four bases of photon polarization, so that means the B92 protocol is still the best protocol out of these four protocols.
- The proposal protocol BB84 with Spin $\frac{1}{2}$ has the second place in average of N_p ($N_{\text{error}}/ N_{\text{key}}$) value error probability after B92.

7.3 – Future Review

QKD protocol field is a large-scale area with many different specifications that can be considered as a subject for further research and investigation including quantum cryptography, quantum information, quantum architecture and quantum memory.

All these areas in quantum environment need to be developed and improved to have an efficient system that works perfectly [44]. Two previous research experiments were performed a survey on QKD protocols based on sending numbers of photons of 100 to 1000 in one research for two protocols and 100 to 2000 photons for three QKD protocols, This thesis executed the experiment with rang of photons from 100 to 5000 photons, This thesis can be continue with higher range of sending photons also modification of any protocols and perform the survey between other QKD protocols with different challenges such as different network setup, using more advanced transmission of key devices to process for better investigation [26].

References

- [1] I. F. Dr. Arthur Herman, "Quantum Computing:How to Address the National Security Risk," Hudson Institute, Washington,D.C., 2018.
- [2] S. S. M. U. S. A. Bilgehan Arslan, "A study on the use of Quantum computers,Risk assessment and Security Problems," IEEE, Ankara, 2018.
- [3] E. P. DeBenedictis, "A Role for IEEE in Quantum Computing," in *THE I E E E C O M P U T E R S O C I E T Y*, 2018.
- [4] V. M. Arun G, "A REVIEW ON QUANTUM COMPUTING AND COMMUNICATION," IEEE, SVNIT, Surat, 2014.
- [5] V. P. Techo, *Research Methods-Quantitive, Qualitive, and Mixed Methods*, Paris: ResearchGate, 2016.
- [6] S. G. D. S. S. B. Sandeep Jain, "Differences between Classical and Quantum Cryptography," Geeksfor Geeks, 29 04 2019. [Online]. Available: <https://www.geeksforgeeks.org/>. [Accessed 2019].
- [7] C. D. L. D. N. F. Lisa O'Connor, "Cryptography in a Post-Quantum World," in *Cryptography in a Post-Quantum World*, Accenture, 2018.
- [8] K. S. J. P. S. P. R. A. R. B. Sayantan Gupta, *Quantum Computation of Perfect Time-Eavesdropping in Position-Based Quantum Cryptography*, KolKata: IEEE, 2017.
- [9] J. S. a. M. Singh², "Evolution in Quantum Computing," in *2016 International Conference System Modeling & Advancement in Research Trends*, Moradabad, India, 2016.
- [10] E. P. DeBenedictis, "A Role for IEEE," in *REBOOTING COMPUTING, THE I E E E C O M P U T E R S O C I E T Y* 001 8, 2018, pp. 52-55.
- [11] D. C. Marinescu, "The Promise of Quantum Computing and Quantum Information Theory - Quantum Parallelism," in *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium*, Orlando, 2005.
- [12] D. P. S. P. M. a. U. C. Ashish Nanda, "A Computing Perspective on Quantum Cryptography," *Energy and Security*, vol. 10.1109/MCE.2018.2851741, no. IEEE Consumer Electronics Magazine, p. 59, 2018.
- [13] V. M. Arun G, *A REVIEW ON QUANTUM COMPUTING AND COMMUNICATION*, Surat: IEEE, 2014.
- [14] G. C. J. E. J. D. H. T. J. N. P. R. P. K. L. a. B. C. B. Y.-W. Cho, *Highly efficient and long-lived optical quantum memory with cold atoms*, Canberra: IEEE, 2017.
- [15] J. W. †. ,. X. Y. Dongyang Wang, "Optical Quantum Computing," *Optical Quantum Computing*, no. 978-1-4673-7679-2/15/, 2015.

- [16] H. Seddiqi, "Why is quantum computing important?," Quora, 12 April 2016. [Online]. Available: <https://www.quora.com/Why-is-quantum-computing-important>.
- [17] D. Tal, "Quantum Run," Quantum Special Series, 2018. [Online]. Available: <https://www.quantumrun.com/prediction/how-quantum-computers-will-change-world-future-computers>.
- [18] M. S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System," in *2009 Sixth International Conference on Information Technology: New Generations*, Nova Southeastern University, 2009.
- [19] K. E. a. F. A. Remah Alshinina, "A Highly Efficient and Secure Shared Key for Direct Communications Based on Quantum Channel," in *2015 Wireless Telecommunications Symposium (WTS)*, New York, NY, USA, 2015.
- [20] M. M. H. Heshem A. El Zouka, "On the Power of Quantum Cryptography and Computers," in *2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Alexandria, Egypt, 2014.
- [21] D. D. G. H. Harshad R. Pawar, *Classical and Quantum Cryptography for Image Encryption & Decryption*, Badnera, India: IEEE, 2018.
- [22] M. & A. A. & T. S. & N. G. Bhatt, "Classical Cryptography v/s Quantum Cryptography A Comparative Study," *International Journal of Electronics and Computer Science Engineering*, 2012.
- [23] G. Mogos, "Cubic Quantum Security," in *2014 International Conference on Computational Science and Computational Intelligence*, Riobamba, Ecuador, 2014.
- [24] G. R. Abishek Madaan, *Analysis of Quantum Cryptosystems using key Distribution and Attacking strategies over Security Protocols*, Uttar Pradesh: IEEE, 2018.
- [25] A. D. Rishi Dutt Sharma, "A New Secure Model for Quantum Key Distribution Protocol," in *2011 6th International Conference on Industrial and Information Systems, ICIS 2011, Aug. 16-19, 2011*, Sri Lanka, 2011.
- [26] B. R. Hada, "An Evaluation of Quantum Key Distribution in QuVis Simulation Software," IEEE, Bandung Indonesia, 2018.
- [27] F. P. Yaseera ISMAIL, "The Race Towards Quantum Security," in *IST-Africa 2018 Conference Proceedings*, Durban, South Africa, 2018.
- [28] M. R. a. K. M. Svore, "Quantum Computing: Codebreaking and Beyond," IEEE, Washington, 2018.
- [29] M. R. G. J. M. C. D. D. H. R. D. E. C. V. M. a. G. B. Logan O. Mailloux, "Quantum Key Distribution: Examination of the Decoy State Protocol," *Quantum Key Distribution: Examination of the Decoy State Protocol*, Vols. 163-6804/15, no. IEEE Communications Magazine, p. 31, 2015.
- [30] S. M. Gabriella Cincotti, "Planar Optical Quantum Computing: Current Status and Future Challenges," IEEE, Rome, Italy, 2007.
- [31] N. R. S. Ali Ibnun Nurhadi, *Quantum Key Distribution (QKD) Protocols: A Survey*, Vols. 978-1-5386-6163-5/18, Bandung, Indonesia: IEEE, 2018, p. 10.

- [32] Wikipedia, "Uncertainty principle, Wikipedia," 2019. [Online]. Available: https://en.wikipedia.org/wiki/Uncertainty_principle.
- [33] D. P. DiVincenzo, *The Memory Problem of Quantum Information Processing*, vol. 103, Achen, Germany: IEEE, 2015, pp. 1417-1425.
- [34] M. S. Sharbaf, *Quantum Cryptography: An Emerging Technology in Network Security*, Northridge: IEEE, 2011.
- [35] M. M. a. M. Senekane, *Security of Quantum Key Distribution Protocols*, London: IntechOpen, 2018.
- [36] A. L, "Survey of Most Prominent Quantum Key Distribution Protocols," *International Research Journal of Engineering and Technology (IRJET)*, vol. 03, no. 05, pp. 1330-1333, 2016.
- [37] R. Goodfellow, *Quantum Key Distribution: Leveraging the Laws of Physics for Perfectly Secure One-Time Pad Encryption*, 2016.
- [38] M. M. a. M. Senekane, "Security of Quantum Key Distribution Protocols," in *Advanced Technologies of Quantum Key Distribution*, IntechOpen, 2018, p. Cha.
- [39] L.-x. Z. K. W. K.-b. W. Hui-fang LI, "The Improvement of QKD Scheme Based on BB84 Protocol," in *IEEE*, Shaanxi, 2016.
- [40] A. Aspect, "Nature," *NatureResearch*, 1999. [Online]. Available: <https://www.nature.com/articles/18296>.
- [41] K. Inoue, "Differential Phase-Shift Quantum Key Distribution Systems," *Differential Phase-Shift Quantum Key Distribution Systems*, vol. 21, no. 3, p. 7, 2015.
- [42] T. H. Kyo Inoue, "DPS Quantum key distribution and related technologies," *Proceedings of SPIE - The International Society for Optical Engineering*, pp. 1-10, January 2009.
- [43] T. H. Yasuhiro Tokura, "Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments," *Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments*, vol. 9, p. 5, 2011.
- [44] K. E. Abdulbast Abushgra, "QKDP's Comparison Based upon Quantum," in *Computer Science & Engineering Department*, Bridgeport, 2017.
- [45] A. Kohnle, "The Quantum Mechanics Visualisation Project," University of St. Andrews, 2018. [Online]. Available: <https://www.st-andrews.ac.uk/physics/quvis/>.
- [46] U. o. S. Andrews, "The QuVis Team," University of St Andrews, [Online]. Available: <https://www.st-andrews.ac.uk/physics/quvis/about.html>.
- [47] M. Haitjema, "Washington University in St.Louis," MCKELVEY SCHOOL OF ENGINEERING, 2 December 2007. [Online]. Available: <https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/>.
- [48] R. Goodfellow, *Quantum Key Distribution: Leveraging the Laws of Physics for Perfectly Secure One-Time Pad Encryption*, 2016.
- [49] D. G. A. S. Hitesh Singh, "Quantum Key Distribution Protocols: A Review," in *IOSR Journal of Computer Engineering (IOSR-JCE)*, Sultanpur, UP, India, 2014.

- [50] A. P. L. a. T. C. Ralph, "Efficient Coherent State Quantum Computing by Adaptive Measurements," in *Centre for Quantum Computer Technology, Department of Physics University of Queensland, St Lucia, Queensland, Queensland, 2006.*
- [51] C. Erven, "On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source," *On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source* , vol. 251970951, no. University of Bristol, p. 68, 2014.
- [52] A. A. Abushgra, *A NEW QKD PROTOCOL BASED UPON AUTHENTICATION BY EPR ENTANGLEMENT STATE*, BRIDGEPORT: THE SCHOOL OF ENGINEERING UNIVERSITY OF BRIDGEPORT, 2017.
- [53] IBM, "Newsroom.ibm.com," IBM, 2019. [Online]. Available: <https://newsroom.ibm.com/2019-04-25-Leading-universities-partner-with-IBM-to-accelerate-joint-research-and-drive-educational-opportunities-in-quantum-computing>.
- [54] Q. C. Report, "Quantum Computing Report," 2019. [Online]. Available: <https://quantumcomputingreport.com/news/> .
- [55] "CRYPViz," WebFusion, 2019. [Online]. Available: <https://crypviz.io/knowledge-database/quantum-resistance/>.
- [56] M. Safronova, "The World of Quantum Information," *The World of Quantum Information*, no. University of Delaware Department of Physics and Astronomy, 2015.
- [57] A. Malik, "NetManias," HFR.Inc, 03 March 2018. [Online]. Available: <https://netmanias.com/en/post/blog/12995/cloud-sdn-nfv/quantum-computing-opens-new-front-in-cloud>.
- [58] C. Smith, "BGR," 5th April 2018. [Online]. Available: <https://bgr.com/2018/04/05/ibm-q-network-quantum-computing-startups/>.
- [59] Medicina, "Emaze," Amazing Production, 2018. [Online]. Available: <https://www.emaze.com/@AQIRIWZR>.
- [60] M. Brodie, "YouTube," Institute for Quantum Computing, 2010. [Online]. Available: <https://www.youtube.com/watch?v=cWpqlgF7uEA&list=LLN2CByeZM1vCrF0SLmAZz2Q&index=11&t=62s>.
- [61] Y. Chavanne, "ICT Journal," 1st August 2019. [Online]. Available: <https://www.ictjournal.ch/news/2019-01-08/ibm-degaine-le-premier-ordinateur-quantique-tout-en-un-destine-aux-entreprises>.
- [62] "The Quantum Mechanics Visualisation Project," University Of St Andrews, 2019. [Online]. Available: <https://www.st-andrews.ac.uk/physics/quvis/>.
- [63] S. Chen, "WIRED," 12 December 2018. [Online]. Available: <https://www.wired.com/story/quantum-computing-needs-you-to-help-solve-its-core-mystery/>.
- [64] C. Barnatt, "Explaining Computers," EC, July 2019. [Online]. Available: <https://www.explainingcomputers.com/quantum.html>.

- [65] "Interactive simulations for quantum key distribution," in *School of Physics and Astronomy, University of St Andrews*, St Andrews,, 2016.
- [66] G. A. P. V. R. D N Kartheek, *SECURITY IN QUANTUM COMPUTING USING QUANTUM KEY DISTRIBUTION PROTOCOLS*, Tirupathi: IEE, 2013.