UNC PEMBROKE COPYRIGHT AND AVAILABILITY FORM

Student Name: Pace Lamberton

Title of Project: A study of Quantum Cryptography

Degree (Circle one): [✓ Undergraduate] Masters Doctorate

Date of Graduation (Month Year): 5/2021 Degree Received__________

Major Subject: Applied Physics

Advisor (print name): Quinton Rice

AVAILABILITY OPTION (check one)

☑ Release the work immediately for worldwide access on the Internet.

□ *(Patent Hold)* Secure the work temporarily for patent and/or proprietary purposes, then release the work for worldwide access on the Internet.

□ *(Journal Hold)* Hold the work for one year, then release the work for worldwide access on the Internet. *(One* year extension on request, if needed)*

UNCP COPYRIGHT AGREEMENT

I hereby certify that, if appropriate, I have obtained and attached hereto a written permission statement from the owner(s) of each third party copyrighted matter to be included in my thesis, dissertation, or record of study, allowing distribution as specified below.

I certify that the version I submitted is the same as that approved by my advisory committee.

I hereby grant to UNCP or its agents the non---exclusive license to archive and make accessible, under the conditions specified below, my thesis, dissertation, or record of study in whole or in part in all forms of media, now or hereafter known. FERPA. To the extent this thesis, dissertation, or record of study is an educational record as defined in the Family Educational Rights and Privacy Act (FERPA) (20 USC 1232g),

I consent to disclosure of it to anyone who requests a copy.

I retain all other ownership rights to the copyright of the thesis, dissertation or record of study.

I also retain the right to use in future works (such as articles or books) all or part of this thesis, dissertation, or record of study.

STUDENT AVAILABILITY & COPYRIGHT AGREEMENT

I have read and fully agree to the UNCP copyright agreement regarding my thesis/dissertation. I agree to the thesis/dissertation availability option I selected above. I understand that the availability option is my choice and that there may be publishing consequences to my selection.

Student Signature:

____

Thesis Advisor/Faculty Mentor's Signature

I have discussed the availability choices with my student, and I am aware of the choice my student has made.

Advisor/Mentor's
Signature:______________________________________

(Only One Signature Required)

UNC Pembroke
Electronic Theses and Dissertations (ETDs)

How to Choose an Availability Option

<u>UNCP's Policy</u>

Your Electronic Thesis/Dissertation (ETD) will be made available immediately after graduation worldwide on the Internet via The Mary Livermore Library, unless you choose to delay release for publishing, patent or proprietary reasons.

<u>Why would I choose "Journal Hold"?</u>

If you are (or will be) submitting material to a journal that restricts Internet access to material **prior to publication**, a "Journal Hold" is the option you need to select. This gives you time to get published, and your ETD is released one year after graduation to the Internet. This hold may be extended one additional year if an email is sent before the initial hold ends in order to give you time to finish publishing your material.

<u>What is a "Patent Hold," and when would I choose it?</u>

If you have patent and/or proprietary reasons for having information in your ETD held from the public domain, UNCP will hold your document until your patent has been secured, or the proprietary restriction is no longer necessary.

<u>What if I have more questions about availability options?</u>

If you still have questions or concerns about availability options, please call (910) 521-6834, (910) 521-6369, or email us at anne.coleman@uncp.edu , june.power@uncp,edu

UNC PEMBROKE | MAYNOR HONORS COLLEGE

Study of Quantum Cryptography with a Thorlabs Teaching Apparatus

Senior Project

In partial fulfillment of the requirements for
The Esther G. Maynor Honors College
University of North Carolina at Pembroke

By

Dana Lamberton
Chemistry and Physics
5/1/2019

Dana Lamberton
Dana Lamberton
Honors College Scholar

5/1/19
Date

Quinton Rice, Ph.D.
Faculty Mentor

5/1/19
Date

Teagan Decker, Ph.D.
Senior Project Coordinator

5/1/19
Date

Acknowledgements

I would like to acknowledge the mentorship of Dr. Quinton Rice for his teaching and advice on this project and throughout my educational career.

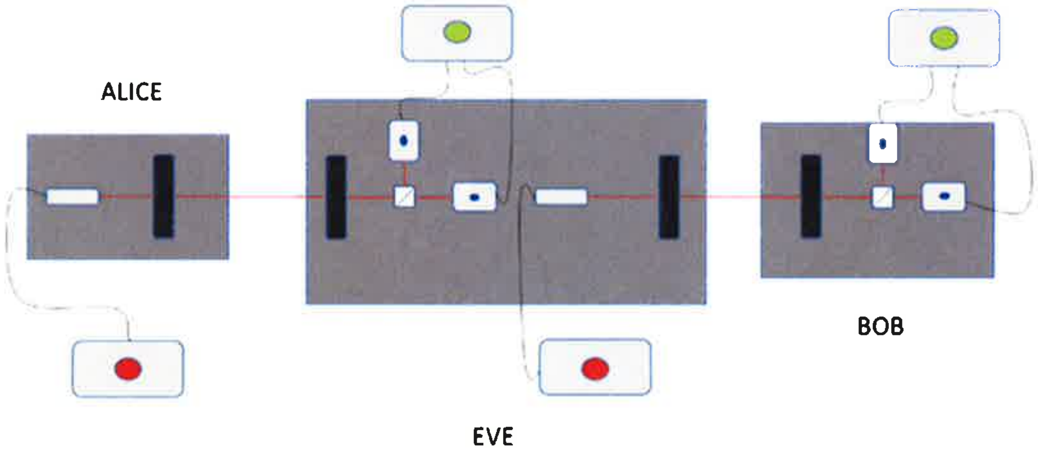
I would like to acknowledge a number of other professors and personal mentors for their encouragement to pursue research in my educational career, including: Dr. Bill Brandon, Dr. Roland Stout, Dr. Paul Flowers, Dr. Siva Mandjiny, Dr. Meredith Storms, Dr. Tom Dooling, Dr. Scott Hicks, and Dr. José D'Arruda.

I would also like to acknowledge a number of people who encouraged and prepared me to study science and engineering prior to college, including Mrs. Beverly McGougan, Mr. Al Buie, Mrs. Faith Jackson, Mr. Tommy Williams, Mr. Steve Hagen, Mrs. Patricia Hayes, Mrs. Mirla Rodriguez, my parents, grandparents, and other family members.

Finally, I would like to acknowledge Dr. Teagan Decker, Dr. Mark Milewicz, and Mr. Gordon Byrd for making my time at UNCP and a part of the Maynor Honors College both challenging and enjoyable.

Abstract

A pseudo-quantum system consisting of laser diodes, wave retarders, beamsplitters, and photodetectors was employed to study encryption of data through binary transmission. The Jones vectors for each optical element can be represented in matrix notation and operated on through linear algebra computation. The laser diodes emit polarized photon pulses which can be represented by 2 x 1 matrices which are treated as transmitted bits. Because of the inherent randomness of polarized photons through a beamsplitter any intermediate detection and subsequent transmission of bits by a third party can immediately be detected. In this study, a total error rate of 25% was calculated for a 20-bit key and 52-bit protocol when the transmitted signal was intercepted in agreement with theory.

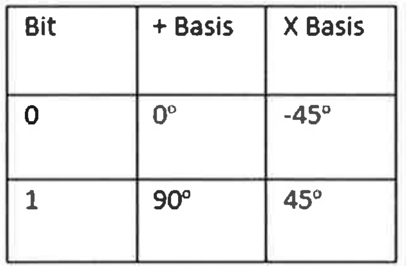


Study of Quantum Cryptography with a Thorlabs Teaching Apparatus

Introduction

Through history it has been important for one to be able to transmit information without interception by another party, particularly in times of war. As people developed increasingly clever ways to encrypt information, the field of cryptography was born. Cryptography holds particular importance in the present information age, where sensitive data like banking information is being transmitted electronically [1]. Computers rely on encryption using complex algorithms and pseudorandom code generation. Since this coding is not truly random it can be compromised when computers employ "brute-force" methods, where they break down the code. Quantum cryptography can eliminate the possibility of these brute-force attacks, as it creates both a truly random code and alerts the senders that an "eavesdropper" is present [2]. Both these perks are derived from the fundamentals of quantum mechanical properties. The first is the ability of generating a truly random key [1]. For example, when a diagonally polarized photon passes through a polarizing beamsplitter, it must "decide" which way to be transmitted. This either reflection or transmission cannot be predicted, since the diagonal polarization is a superposition of both the horizontal and vertical states there is 50% chance that either reflection or transmission could take place. This is one case of true random behavior in nature.

The other employment of a quantum mechanical property is in the detection of an eavesdropper. When taking a measurement at the quantum mechanical level, it is impossible to do so without changing the state of that which is being measured [1]. In order to take a measurement of a photon, it must be interacted with in some way, which will destroy the photon.[2] Since the collection of the information also destroyed it, it can no longer be transmitted to the receiver. The eavesdropper must generate a new photon for the receiver to collect, but he does not know the exact polarization state which the sender delivered to him. A new photon must be sent with an assumed polarization state. It is statistically impossible over even a short key for the eavesdropper to randomly guess the correct polarization states, so his presence will inevitably be detected [2]. Data is transmitted from the sender (Alice) to the receiver (Bob) with this apparatus via the BB84 protocol. This protocol utilizes two bases in order to generate a secure key, which determine the orientation of the half-wave plates and then the corresponding binary bits. An example is shown in Figure 1.



Bit	+ Basis	X Basis
0	0°	-45°
1	90°	45°

Figure 1

Theory

The polarization states of each photon can be represented using Dirac matrix notation. Vertically and horizontally polarized photons can be represented as shown in Eq. 1:

$$|0°\rangle = \begin{bmatrix}0\\1\end{bmatrix} \qquad |90°\rangle = \begin{bmatrix}1\\0\end{bmatrix} \tag{1}$$

Scalar matrix multiplication is used to describe the probability of photons interacting with polarizers.

$$\langle 90°|0°\rangle = \begin{bmatrix}1 & 0\end{bmatrix} * \begin{bmatrix}0\\1\end{bmatrix} = 0 \tag{2}$$

$$|0|^2=0$$

This describes the interaction of a horizontally polarized photon interacting with a vertically oriented polarizer. There is a 0% chance that the photon will be transmitted.

Diagonally polarized photons can be expressed as a linear combination of horizontally and vertically polarization states.

$$|45°\rangle = \frac{1}{\sqrt{2}}|90°\rangle + \frac{1}{\sqrt{2}}|0°\rangle \qquad |-45°\rangle = \frac{1}{\sqrt{2}}|90°\rangle - \frac{1}{\sqrt{2}}|0°\rangle \tag{3}$$

Another behavior which is described through linear algebra is the interaction of a photon with a half-wave plate.

The matrix in equation 4 represents a half-wave plate, with θ representing the orientation [4].

$$HWP = e^{\frac{-i\pi}{2}} \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\sin(2\theta) \end{bmatrix} \tag{4}$$

The probability of a horizontally polarized photon being transmitted through two half-wave plates oriented at angles $\theta_1 = 0°$ and $\theta_2 = 0°$, given by:

$$\begin{aligned} &((HWP_1 * HWP_2 * H)^T * H)^2 = 1 \\ &|1|^2 = 1 \end{aligned} \tag{5}$$

The square of the scalar product indicates there is a 100% chance a horizontally polarized photon will result from this half-wave plate combination.

Experimental Procedure

Signals were sent by Alice via polarized pulses of light from a diode laser. In order to sent data,she choses a wave plate orientation based on the intended bit to be sent. Bob then receives a bit based on the orientation of his wave plate. The signal then passes through a horizontal beamsplitter, where it is transmitted into one of two detectors. The detector the light is transmitted or reflected into one of the two detectors. The detector which receives the signal will blink and LED. The detector which lights up indicates whether the bit was a 1 or a 0. In order to create a secure key the bases are chosen at random by Alice and Bob and not shared with one another until after the information to create the key has been transmitted. Then, the bases are shared publicly. [1]

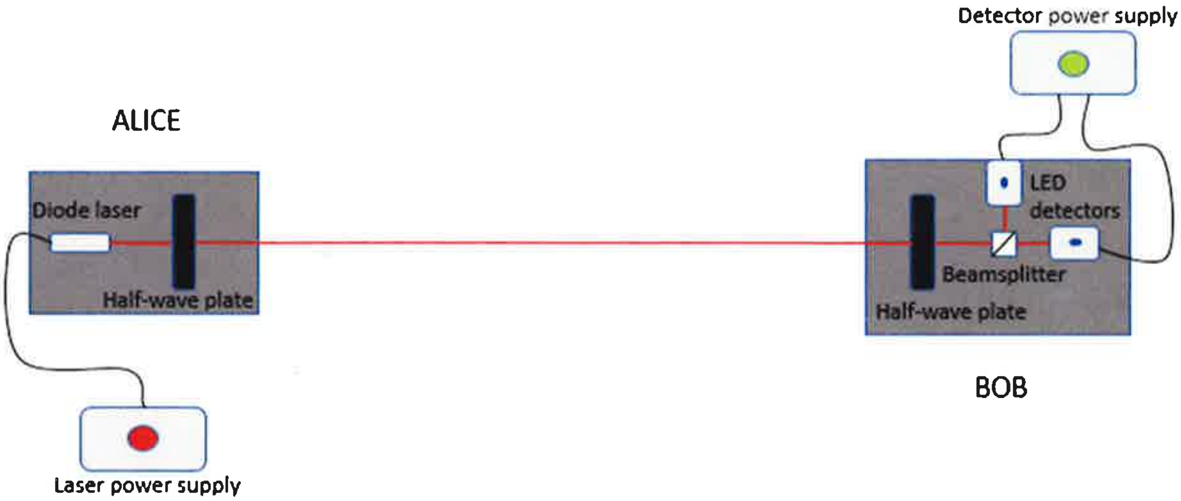


Figure 2

After data was successfully transmitted between Alice and Bob an eavesdropper (Eve) was added. Eve consists of all of the same components of both Alice and Bob, as she must both receive and then transmit signals. Eve chooses her bases at random. She receives the correct bit only 75% of the time. There will be an average discrepancy among 25% of the transmitted data between Alice and Bob when Eve is present.

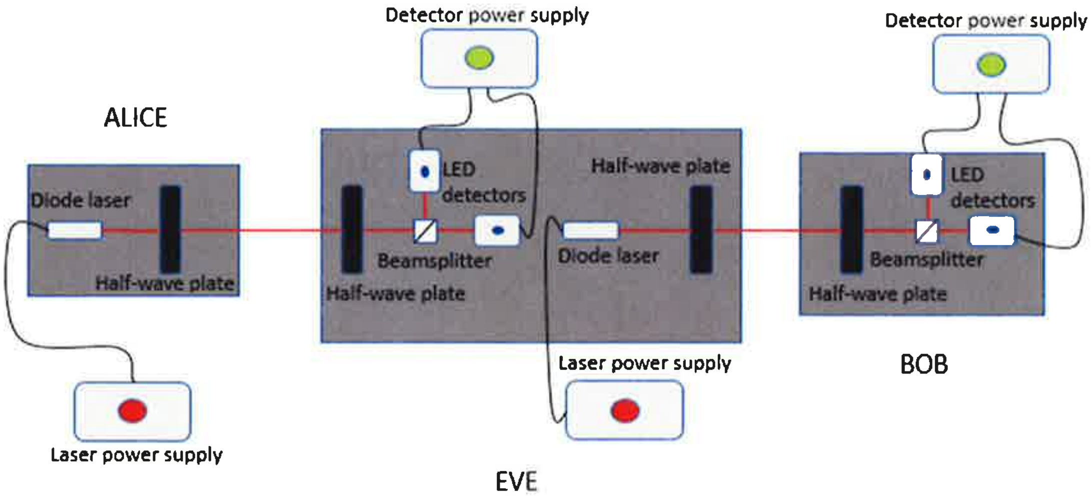


Figure 3

Figure 4 demonstrates a horizontally polarized beam passing through a half wave plate oriented at 45° and then a polarizing beamsplitter. The beamsplitter transmits the horizontal photons and relflects the vertical photons. These photons are distributed evenly between the two detectors. If this were a single photon, it would have a 50% chance of interacting with either detector.

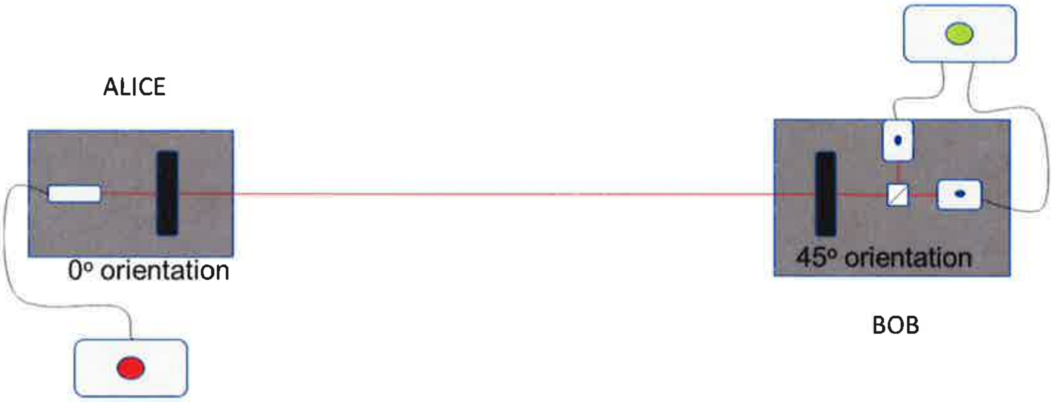
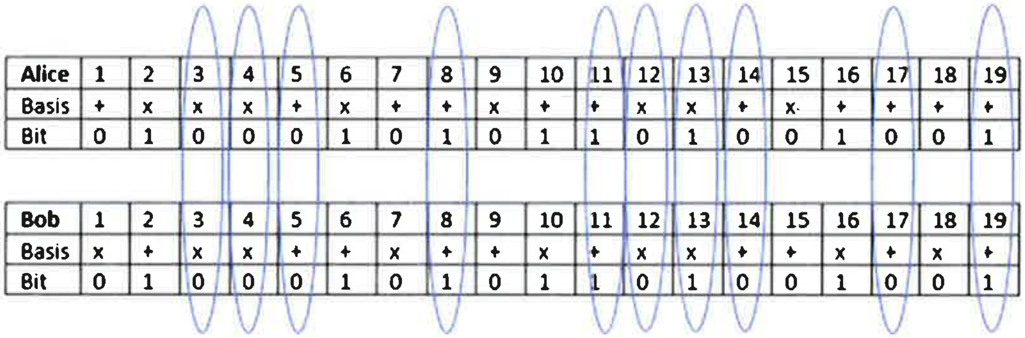


Figure 4

Results

A one-time pad (key) was created, as shown in Figure 5. The bases and bits were randomly chosen by Alice, while only the bases were randomly chosen by Bob, and the resulting transmitted bits were recorded. In all places where the bases between Alice and Bob matched the information was recorded, otherwise it was discarded.

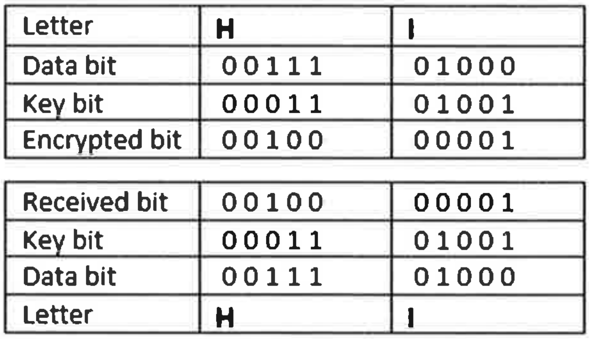


Alice	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Basis	+	x	x	x	+	x	+	+	x	+	+	x	x	+	x	+	+	+	+
Bit	0	1	0	0	0	1	0	1	0	1	1	0	1	0	0	1	0	0	1

Bob	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Basis	x	+	x	x	+	+	x	+	+	x	+	x	x	+	+	x	+	x	+
Bit	0	1	0	0	0	1	0	1	0	1	1	0	1	0	0	1	0	0	1

Figure 5

An example below of the encoding of a message which was transmitted via the Thorlabs apparatus, and then retrieved and decoded.



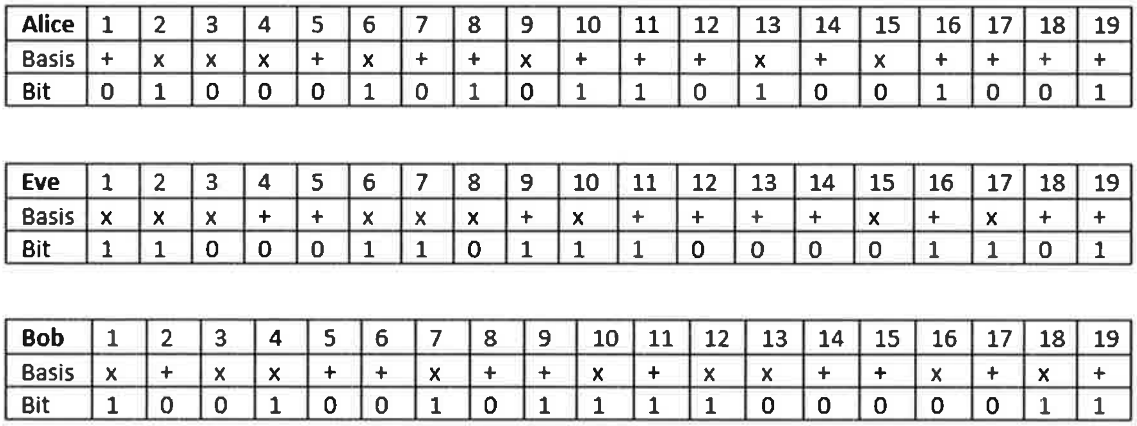
Letter	H	I
Data bit	00111	01000
Key bit	00011	01001
Encrypted bit	00100	00001

Received bit	00100	00001
Key bit	00011	01001
Data bit	00111	01000
Letter	H	I

Figure 6

Messages are encoded and decoded using binary addition.

Figure 7 is an example of an attempt to create a key with an eavesdropper present. It was shown that in some transmissions, such as columns 4 and 8, there are places where the bases match while the bit does not. This is evidence of an eavesdropper's presence. This occurs because Eve is forced to randomly choose bases, as Alice only shares her bases after the data has been transmitted.



Alice	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Basis	+	x	x	x	+	x	+	+	x	+	+	+	x	+	x	+	+	+	+
Bit	0	1	0	0	0	1	0	1	0	1	1	0	1	0	0	1	0	0	1

Eve	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Basis	x	x	x	+	+	x	x	x	+	x	+	+	+	+	x	+	x	+	+
Bit	1	1	0	0	0	1	1	0	1	1	1	0	0	0	0	1	1	0	1

Bob	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Basis	x	+	x	x	+	+	x	+	+	x	+	x	x	+	+	x	+	x	+
Bit	1	0	0	1	0	0	1	0	1	1	1	1	0	0	0	0	0	1	1

Figure 7

When an eavesdropper is detected as above, no more information will be sent between Alice and Bob.

Discussion

The employment of quantum cryptography and the BB84 protocol ensures a secure transmission of data. After the data bits are transmitted and the bases are shared between Alice and Bob, they see which bases match one another and confirm that the bits match. If the transmitted bits do not match, then they are aware of the presence of an eavesdropper and stop communtication. This is especially secure when Eve measures the photon transmitted by Alice, it is then destroyed. It cannot be copied or passed on if a measurement of the photon is taken. Eve is forced to generate a new photon to send to Bob. But, since the bases have not been shared by Alice yet, she must guess the bases to use when she transmits to Bob. Bob will receive data bits and compare the chosen bases and the bits received. If there are places in which the bases match and the bits do, then Alice and Bob know that an eavesdropper is present. Once the key has been established, then an eavesdropper will not be able to interpret the encoded messages which will be sent. It is also near impossible for the eavesdropper to guess at the key due to the inherent randomness of photon behavior.

Conclusion

This system employs a pulse of light from the laser rather than a single photon, it is not a quantum system but rather a psuedoquantum system. A single photon transmission is required if it were to be a true quantum system. Nevertheless, Quantum Cryptography shows promising potential for the future of cryptography. If it could be employed commercially it would be an asset to those who require the secure transmission of information. The interent randomness of photon behavior and the inability to copy a photon ensures for the secure transmission of data. The challenge that lies ahead is with the transmission of a single photon. This proves to be both difficult and expensive, especially over long distances. Photons are sensitive and easily destroyed, so the transmission of a single one carrying a piece of data has proven to be difficult..

References

1 – Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*. CRC Press. 1997

2 – Bennet, C. H., & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. 2014

3 – Pedrotti, F. L., Pedrotti, L. M., & Pedrotti, L. S. Introduction to optics(4th ed.). Cambridge: *Cambridge University Press*. 2018

4 – ThorLabs Quantum Cryptography Demonstration Kit Manual EDU-QCRY1. 2017

5 – Larson, Ron; Elementary Linear Algebra. *Cengage Learning*. 2017