Article

Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation

Yuval Bloom ^{1,2} , Ilai Fields ¹ , Alona Maslennikov ³ and Georgi Gary Rozenman ^{1,4,*}

¹ The Raymond and Beverly Sackler School of Physics and Astronomy, Tel Aviv University, Tel Aviv 69978, Israel; yuvalbloom@mail.tau.ac.il (I.B.); ilai.f1456@gmail.com (I.F.)

² The Blavatnik School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel

³ The Raymond and Beverly Sackler Faculty of Exact Sciences, School of Chemistry, Tel Aviv University, Tel Aviv 69978, Israel; maslennikov@mail.tau.ac.il

⁴ The Iby and Aladar Fleischman Faculty of Engineering, Tel Aviv University, Tel Aviv 69978, Israel

* Correspondence: garyrozenman@protonmail.com or georgiro@mail.tau.ac.il

Abstract: Quantum cryptography is a topic of considerable interest. A simple and robust experiment and theory for a senior level undergraduate investigation of quantum key distribution are described. In the proposed experiment, key principles from the BB84 protocol, used in quantum cryptography, are emulated using an optical apparatus and computational scripts independently.

Keywords: quantum; key; distribution; cryptography

Citation: Bloom, Y.; Fields, I.; Maslennikov, A.; Rozenman, G.G. Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation. *Physics* **2022**, *4*, 104–123. <https://doi.org/10.3390/physics4010009>

Received: 7 November 2021

Accepted: 12 January 2022

Published: 25 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Private communication is of critical importance in the present time, which is raising the demand for developing secure methods for message delivery. Encryption by means of secret keys, which is at the core of cryptography, allows a secure exchange of messages through a public channel when a potential adversary exists. Modern cryptography [1–3] not only practices but also studies secure communication techniques between two distant users in the presence of third parties. Its protocols exhibit unidentifiable messages, which are readable only to the sender and the recipient, assuring that an encrypted message sent through a public channel is indecipherable by a third party.

Prior to the digital age [4–6], cryptography has focused on message conversion into an indecipherable form, making it unreadable to interceptors. These days, the field is expanded not only to communication and military secrecy [6,7], but also to integrity checking, identity authentication, secure computation and more [2].

A secure key is required for the sender to encrypt the message and for the recipient to decrypt it [8]. In modern cryptography, the security of a key is based either on complex underlying algorithms, or on practical constraints, such as the factorization of large numbers [3]. One example is the Diffie Hellman key exchange protocol [9,10], which was implemented by using prime numbers and their primitive root modulo. Although key decryption calculations can take an unrealistic period of time for modern computers, there is no way to ensure that a key has not been decrypted by a third party, and so become readable to an eavesdropper.

As computers gain the ability to perform complex calculations, along with the development of quantum computers [11], the decryption of cryptographic algorithms is becoming simpler. This makes former cryptographic protocols irrelevant and strengthens the threat to information security. Nonetheless, many recent studies claim that this issue can be resolved by the utilization of quantum key distribution [12,13]. In other words, secure communication can be achieved with quantum cryptography [11,14].

One of the basic principles of quantum physics states that the measurement of a photon's state necessarily changes it [12,13]. When using a single photon in a specific

state to carry an information bit, it cannot be copied without causing an alteration in its state. This phenomenon is known as the no-cloning theorem in quantum mechanics [15]. Therefore, two users that are willing to exchange a random binary message through a public channel can recognize whether a third party is intercepting this channel before sending the message, that is, any attempt at interception can be identified before the message is sent. Furthermore, by using random number generation [16] that dictates the photon's state, it is possible to generate a random key that will be known only to the sender and the recipient.

This application of quantum cryptography is known as quantum key distribution (QKD) [8], which is the utilization of quantum communication for establishing a key shared between two users, without allowing a third party to learn anything about it. The security of QKD can be proven mathematically [17], without any restrictions on the eavesdropper's ability, unlike in classical key distribution.

Practically, there are some challenges in this technique [18,19] due to transmission distances, rate limitations and accuracy. Nowadays, quantum cryptography is at the forefront of research, and suggests many other applications, such as quantum coin tossing [11].

The first quantum cryptography protocol was developed by Charles Bennet and Gilles Brassard under the name of BB84 [1]. This quantum key distribution scheme is usually referred to as a secure method of sending a private key from one user to another in a one-time pad encryption. Based upon two conditions, this protocol is known to be provably secure [17]; there is an authenticated public classical channel and information gain is possible by interfering with the signal in attempts to distinguish the two states only if they are not orthogonal (i.e., the no-cloning theorem).

Quantum technologies have been implemented rapidly into industry in the past two decades. However, the implementation of quantum cryptography in the market remains limited, as several obstacles prevent the industrial transfer of classical cryptography into quantum cryptography. Previous processes of implementation concepts in optics, such as optical fibers and adaptive optical systems, rely on the development of devices in the industrialization of any optical technology. In fact, quantum key distribution (QKD) devices are no different as there are high costs involved in the integrability of such devices. Current QKD devices often include an optical table, superconducting wire detectors, expensive and fragile single photons sources and precision optics. These components require extensive and constant maintenance and can be operated only by trained experts. Therefore, QKD has many challenges when implemented in standard educational laboratories.

In this paper, an educational experiment for the study of the BB84 quantum cryptography protocol is presented which can be performed without a single photon source or special training for senior undergraduate laboratories. Instead of individual photons, this experiment is carried out with a pulsed laser and while it cannot truly be employed as a perfect encryption system, the sequence of the BB84 protocol is completely identical to a true quantum encryption system. The major difference between this emulation experiment and a true quantum cryptography setup is that genuine safety from interception can only be guaranteed if a single photon source is used. This means that the information of a bit must be transported only by a single photon. If any classical light source is used instead of a single photon source, then Eve cannot be detected. For eavesdropping, all that is required is that Eve separates a portion of the transmitted light for detection, while sending the remainder to Bob unnoticed. The core principle in our emulation is based on the fact that every single light pulse cannot be split into smaller portions and travels as a single quantity of light. Under this condition, the simulation for single photons completely replicates the experimental results.

2. Theory of Experiment

2.1. One-Time Pad

The one-time pad [20,21] is a classical encryption technique, which is assisted by quantum physics to meet the method's requirements, and is considered 100% secure in principle. While the desired message consists of a non-random sequence of 0 s and 1 s,

the one-time pad is a single-use key consisting of a random sequence of 0 s and 1 s. A binary addition [22,23] of the message to the key results in another sequence of random bits, which is then sent as the encrypted message. The addition rules for the bits are:

$$0 + 0 = 0; 1 + 0 = 1; 0 + 1 = 1; 1 + 1 = 0. \quad (1)$$

When applying a binary addition with the secure key, which is generated by the BB84 protocol, to the original message, the sender can encrypt the message. By applying a binary addition with the secure key to the encrypted message, the receiver can decrypt it and obtain the original message. An example is shown in Figure 1.

If the encrypted message is intercepted, the eavesdropper requires the key to decode the message, otherwise the random sequence cannot be interpreted. The binary sequence can be converted to strings using ASCII (American Standard Code for Information Interchange) symbols [24].

Message	T					R					Y				
Binary Message	1	0	1	0	0	1	0	0	1	0	1	1	0	0	1
	+														
Random Key	1	1	0	0	1	0	0	1	0	0	1	1	0	1	0
Encrypted Message	0	1	1	0	1	1	0	1	1	0	0	0	0	1	1
	+														
Random Key	1	1	0	0	1	0	0	1	0	0	1	1	0	1	0
Decrypted Message	1	0	1	0	0	1	0	0	1	0	1	1	0	0	1
Message	T					R					Y				

Figure 1. Example of an encryption of a binary message using a secure key. T, R, Y are alphabetic letters and their corresponding binary codes are the binary message.

While computer-generated pseudo-random numbers are not truly (100%) random [25], the one-time pad requires a completely random selection of the encryption key. Nonetheless, quantum physics offers numerous possibilities for true randomness [16], such as radioactive decay. Quantum random number generators are a key component in quantum cryptography data networks. In practice, a photon that is reflected by a beam-splitter can be interpreted as 1 and a photon that is transmitted by a beam-splitter can be interpreted as 0. Therefore, for conventional light sources with the same intensity [26,27], photon distribution on two single photo-detectors can be considered truly random.

Generally, the BB84 protocol core purpose is generating a secure key between the sender and the receiver.

2.2. Key Distribution

The sending unit ‘Alice’ consists of a pulsed laser source [26,27], which is polarized in a specific direction, and a half-wave plate ($\lambda/2$ with λ being the wave length), which rotates the polarization of the incident light by double the physical rotation angle of the plate; see Table 1. It must be noted that the angle mentioned in here refers to the rotation angle of the polarization, and not of the plate.

Table 1. Legend for choices between the bit and base to the polarization rotator. λ denotes the wave length.

$\lambda/2$	Base	Bit
90°	+	0
0°	+	1
-45°	x	0
45°	x	1

The receiving unit ‘Bob’ consists of a half-wave plate ($\lambda/2$), a polarizing beam-splitter (PBS) and two detectors that indicate whether the light sent by Alice was either reflected or transmitted from the PBS.

Before Alice can send a message to Bob, a secure key must to be generated. If Alice's pulsed source is polarized horizontally, two bases can be defined, "+" and "x", where each contains two light polarizations. Alice can send a random bit of 0 or 1 in the following manner, as shown in Figure 2.

Figure 2. Optical diagram with the bases + (0° and 90°) and x (-45° and 45°). "PBS" defines the polarizing beam-splitter.

The "+" basis consists of 0° and 90° polarizations, whereas the "x" basis consists of -45° and 45° polarizations. In this scheme, either basis can be used to represent a binary bit: "0" for 90° and -45° , and "1" for 0° and 45° .

To create a secure key, Alice randomly selects a basis and a bit, then sends it to Bob by using the scheme above, while rotating the polarization plate accordingly. Bob randomly selects a basis and rotates the polarization plate accordingly (0° or 45°), while recording with the detectors which bit was received.

In this manner, the PBS reflects the 90° component of the incident light, while transmitting the 0° component. Thus, if the polarization of the light sent by Alice is at 90° and her polarization plate is at 90° , the incident pulsed beam will be at 0° , thus transmitted through the beam splitter (designated as event "0"). If Alice's polarization plate is set to rotate the polarization by 0° , the pulsed beam will be reflected by the beam splitter (designated as event "1"). Similarly, Alice can send bits in the "x" basis.

If Bob selects the "+" basis and Alice sends the bit in the "+" basis, Bob obtains an unequivocal result. However, if Bob selects a different basis than Alice, a result polarized by 45° will be sent to the beam-splitter; half of the beam is transmitted and half is reflected by the PBS. Hence, there is a 50% chance that Bob will detect either 0 or 1 for a pulsed beam, and the result is ambiguous. The different cases are shown in Table 2.

After sending the entire random sequence, Alice and Bob compare only the randomly chosen bases through the public channel. If their two bases differ, the measurement is discarded. As can be seen from Table 2, the result is unequivocal only when the bases are the same. The encryption key is derived only from the measurements in which Alice and Bob chose the same basis.

Table 2. Different cases for the basis and bits between Alice and Bob. See text for details.

Alice			Bob				Basis Match
Basis	Angle	Bit	Basis	Angle	Detect 0	Detect 1	
+	90°	0	+	0°	100%	0%	Yes
+	0°	1	+	0°	0%	100%	Yes
x	45°	1	+	0°	50%	50%	No
x	-45°	0	+	0°	50%	50%	No
+	90°	0	x	45°	50%	50%	No
+	0°	1	x	45°	50%	50%	No
x	45°	1	x	45°	0%	100%	Yes
x	-45°	0	x	45°	100%	0%	Yes

Once Alice and Bob have gone through all measurements, the secret key is achieved. Consequently, Alice can encrypt the message and send it in the “+” basis, so that Bob receives it in the “+” basis and decrypts it. If there is no eavesdropper, the number of matching bases should be identical to the number of matching bits. Therefore, the amount of matching bits out of the total bits sent by Alice is 50%.

2.3. Detection of an Eavesdropper

The eavesdropper unit ‘Eve’ is placed between Alice and Bob, as seen in Figure 3, consisting of the same components but in reverse sequence. It is placed in a position that allows to measure the light coming from Alice and transmits the same information to Bob.

Figure 3. Optical diagram (a) and apparatus (b) with the eavesdropper Eve between Alice and Bob.

As Eve cannot copy the pulsed beam transmitted by Alice without altering its state, it must randomly select the basis in which it will transmit it to Bob. Besides that, another random basis should be selected for the bit that is received from Alice. Thus, two random selections are required for Eve’s bases.

There are four possible scenarios in which Alice and Bob can choose the same basis (otherwise, the measurement is discarded):

1. Eve chooses the same basis as Alice and transmits the bit to Bob using the same basis. In this case, Eve correctly measures the signal sent by Alice, thus, Bob receives the bit initially transmitted by her. Eve’s presence is undetected in this case;
2. Eve chooses the same basis as Alice and transmits the bit to Bob in a different basis. In this case, Eve correctly measures the signal sent by Alice, yet transmits it to Bob in a different basis, meaning that he has a 50% chance to detect the original bit that was sent by Alice;
3. Eve chooses a different basis than Alice and transmits the bit to Bob in this basis. In this case, one of Eve’s detectors will randomly respond to the bit transmitted by Alice, meaning that Bob has a 50% chance to detect the original bit that was sent by Alice;

4. Eve chooses a different basis than Alice and transmits the bit to Bob in another different basis. In this case, Eve detects a random bit from Alice, and Bob detects a random bit from Eve, having only 25% chance to detect the original bit that was sent by Alice.

Cases 2–4 produce an error, which allows Alice and Bob to detect Eve's presence. The measurement is not discarded, since both Alice and Bob sent/received the signal on the same basis. However, in cases 2 and 3, one of Eve's basis differs from Alice or Bob, hence one random detection takes place. In case 4, Eve's basis differs and two random detections take place. Either way, Bob can obtain a different bit than the one sent by Alice in the same basis. Such event is impossible without a third party interference. Let us note that in this approach the time interval is 1 s between each bit transmission.

The test for an eavesdropper's presence is carried out following a similar procedure: Alice and Bob compare bases and choose a certain sequence of bits with matching bases to compare in a public channel. If the test bits are identical, there was no eavesdropper in the system. However, if errors occur in approximately 25% of events, the communication was intercepted. In this case, the message was not yet sent, thus Alice and Bob should follow the same procedure in a different channel to generate a new secure key. To note is that in part one, where Alice and Bob are present, it takes only one second to send the pulse from Alice to Bob. In part two, which involves two pulsed lasers and two pulsed laser detections, it takes one second to send the pulse from Alice to Eve; then, Eve prepares the second pulse by mechanically rotating a half wave plate, which takes about two seconds and then it takes another second to send the bit to Bob, resulting in a total time of four seconds.

2.4. Mathematical Description in Dirac Notation

The four polarization states in this experiment are symbolized as $|-45^\circ\rangle$, $|0^\circ\rangle$, $|45^\circ\rangle$, $|90^\circ\rangle$, where $|0^\circ\rangle$, $|90^\circ\rangle$ are the states of the + basis and $|-45^\circ\rangle$, $|45^\circ\rangle$ are the states of the x basis. They are defined using Dirac's notation [28] (i.e., bra-ket notation), where $|v\rangle$ denotes a vector that represents a quantum state, and $\langle f|$ denotes a linear map that maps a vector to a number in the complex plane. Consequently, the linear functional acting on a vector is written as $\langle f|v\rangle$, as corresponds to a scalar product for two states [12,13]. It is important to note that the scalar product of two orthogonal states is: $\langle 90^\circ|0^\circ\rangle = 0$, whereas the squared absolute value of the scalar product represents the probability that a 0° polarized pulsed beam passes through a polarizer oriented in a 90° direction. The scalar product of the same two states is: $\langle 0^\circ|0^\circ\rangle = 1$.

These states can be expressed as linear combinations of the other basis: $|\psi\rangle = \alpha|\phi_1\rangle + \beta|\phi_2\rangle$. According to the fact that the scalar product must be normalized: $\langle\psi|\psi\rangle = 1$, all four states can be expressed by a superposition of the others:

$$\begin{aligned} |45^\circ\rangle &= \frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle, \\ |-45^\circ\rangle &= \frac{1}{\sqrt{2}}|0^\circ\rangle - \frac{1}{\sqrt{2}}|90^\circ\rangle, \\ |0^\circ\rangle &= \frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle, \\ |90^\circ\rangle &= \frac{1}{\sqrt{2}}|45^\circ\rangle - \frac{1}{\sqrt{2}}|-45^\circ\rangle. \end{aligned}$$

Hence, for example, the probability of a 0° polarized pulsed beam passing a 45° oriented polarizer is 50%:

$$|\langle 45^\circ|0^\circ\rangle|^2 = \left| \frac{1}{\sqrt{2}}\langle 45^\circ|45^\circ\rangle + \frac{1}{\sqrt{2}}\langle 45^\circ|-45^\circ\rangle \right|^2 = \frac{1}{2}.$$

The probability for the other states and bases can be derived similarly.

The base operators, which are linear maps that input a ket $|v_1\rangle$ and output a ket $|v_2\rangle$, are introduced to describe a measurement in either one of the bases.

$$\hat{M}_+ = |0^\circ\rangle\langle 0^\circ| - |90^\circ\rangle\langle 90^\circ|, \quad (2)$$

$$\hat{M}_x = |45^\circ\rangle\langle 45^\circ| - |-45^\circ\rangle\langle -45^\circ|. \quad (3)$$

Thereby, the operators act on a given state; if an operator acts on a basis similar to the polarized state, the eigenvalue is the state itself. Note that the eigenvalue of -1 corresponds to the transmission and is assigned as bit 0.

For example:

$$\begin{aligned} \hat{M}_+|0^\circ\rangle &= |0^\circ\rangle\langle 0^\circ|0^\circ\rangle - |90^\circ\rangle\langle 90^\circ|0^\circ\rangle = |0^\circ\rangle \\ \hat{M}_+|90^\circ\rangle &= |0^\circ\rangle\langle 0^\circ|90^\circ\rangle - |90^\circ\rangle\langle 90^\circ|90^\circ\rangle = -|90^\circ\rangle. \end{aligned}$$

The same derivation can be done for $\hat{M}_x$, operating on the x base. However, if an operator acts on the opposite basis, it is possible to show that the transmission probability of a pulsed beam through a polarizer is 50%:

$$\begin{aligned} \hat{M}_+|45^\circ\rangle &= |0^\circ\rangle\langle 0^\circ|45^\circ\rangle - |90^\circ\rangle\langle 90^\circ|45^\circ\rangle = \\ &= |0^\circ\rangle\langle 0^\circ|(\frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle) - |90^\circ\rangle\langle 90^\circ|(\frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle) = \\ &= \frac{1}{\sqrt{2}}|0^\circ\rangle - \frac{1}{\sqrt{2}}|90^\circ\rangle. \end{aligned} \quad (4)$$

Similarly, for the other cases:

$$\hat{M}_+|-45^\circ\rangle = \frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle, \quad (5)$$

$$\hat{M}_x|0^\circ\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle - \frac{1}{\sqrt{2}}|-45^\circ\rangle, \quad (6)$$

$$\hat{M}_x|90^\circ\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle. \quad (7)$$

Figures 4 and 5 exhibit different cases for Alice and Bob with and without an eavesdropper, respectively.

Alice			Eve			Bob		
State	Basis	Bit	Basis	Quantum State	State Sent	Basis	Quantum State	Bit Measured
$ 0^\circ\rangle$	+	1	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	$ 0^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	1
						×	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
			×	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$	$ 45^\circ\rangle$ or $ -45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
						×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$ or $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	0 or 1
$ 90^\circ\rangle$	+	0	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	$ 90^\circ\rangle$	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0
						×	$\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
			×	$\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	$ 45^\circ\rangle$ or $ -45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
						×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$ or $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	0 or 1
$ 45^\circ\rangle$	×	1	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$	$ 0^\circ\rangle$ or $ 90^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$ or $\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0 or 1
						×	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
			×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	$ 45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
						×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	1
$ -45^\circ\rangle$	×	0	+	$\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$	$ 0^\circ\rangle$ or $ 90^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$ or $\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0 or 1
						×	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
			×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	$ -45^\circ\rangle$	+	$\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
						×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	0

- Bases of Alice & Bob are identical : Eve is not Detected
- Bases of Alice & Bob are not identical : Measurement is discarded
- Bases of Alice & Bob are identical; Bits Identical, Eve not Noticed
- Bases of Alice & Bob are identical : Bits Differ, Eve is Uncovered

Figure 4. Alice and Bob basis, bits and measured bit—with Eve.

Alice			Bob		
State	Basis	Bit	Basis	Quantum State	Measured Bit
$ 0^\circ\rangle$	+	1	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	1
			×	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
$ 90^\circ\rangle$	+	0	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0
			×	$\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
$ 45^\circ\rangle$	×	1	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
			×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	1
$ -45^\circ\rangle$	×	0	+	$\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
			×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	0

■ Bases of Alice & Bob are identical : Bit can be used as key bit

■ Bases of Alice & Bob are not identical : Measurement is discarded

Figure 5. Alice and Bob basis, bits and measured bit—without Eve.

3. Experimental Procedure

The light source in the experimental system is a pulsed laser and not a single photon source, meaning that the prevention of an interception cannot be fully guaranteed. Therefore, in order to eavesdrop, Eve must separate a portion of the light transmitted from Alice, then analyze a part of it while sending the remainder to Bob, imperceptibly. However, the sequence of the protocol in this experiment is completely identical to a true quantum encryption system. It must be noted that in order to avoid unbiased randomization, all bases and bits (for Alice, Bob and Eve) should be generated simultaneously. The complete experiment setup is shown in Figure 6.

Figure 6. Optical diagram with Alice, Bob and Eve.

3.1. Calibration

The model of the lasers in the system is CPS635R from Thorlabs [29]; collimated laser diode module: 635 nm, 1.2 mW, Gaussian profile beam. The detectors models are EDU-QCRY1/M by Thorlabs [30].

Before conducting the experiment, the light source and the detectors were calibrated [26,27]. The pulsed laser was calibrated by a polarizer to a horizontal polarization of 90° . The bit

detectors, both for Eve and Bob, were aligned so that the transmitted and reflected light would reach the desirable detector. The detectors were tested both for Eve and Bob for each base and bit.

3.2. Key Transmission—Without Eve

Alice chooses a random basis (+ or x) and a random bit (0 or 1), while Bob randomly chooses his basis (+ or x), and they both set their wave plates accordingly. The random basis and bits were chosen by means of a computational script that is explained later in the paper. Then, the laser pulse is sent through the setup and Bob records whether he measured a 0 or 1 bit.

Next, Alice and Bob compare their bases through a public channel, keeping only the bits that were measured with the same bases, which then define the secret encryption key between them. Using the generated key, Alice can encrypt the message and send it publicly to Bob. Bob can decrypt the message by means of the same generated key.

This experimental Section was conducted on sequences of 18 bits for a 2 letter word, and 52 bits for a 4 letter word. It is important to note that if the generated key is longer than the message, it should be shortened to the message's length in order to allow the binary addition for its encryption.

3.3. Key Transmission—With Eve

Alice chooses a random basis (+ or x) and a random bit (0 or 1), while Bob randomly chooses his basis (+ or x).

Eve randomly chooses two bases (+ or x), the “incident basis” which corresponds to the bit sent by Alice, and the “transmitted basis,” which corresponds to the bit sent by Eve to Bob. All units set their wave plates accordingly. First, a laser pulse is sent from Alice, and Eve records whether it measured a 0 or 1 bit. Next, Eve sends the bits received in the randomly chosen base to Bob, who records whether he measured a 0 or 1 bit.

For example: Alice sent bit 1 by choosing basis $|+\rangle$ for the state $|0^\circ\rangle$ (the 0° polarized light passes a polarization plate with 90°), Eve intercepted it by using the basis + (polarization plate with 0°), and then sent the state $|0^\circ\rangle$. Bob measured this state by using basis + (polarization plate with 0°) then had the measured bit 1.

Alice and Bob compare their bases again through a public channel and keep only the bits that were measured in the same base. In this Section, Alice and Bob compare a sample of the transmitted bits that were measured. If errors occur in approximately 25% of events, the eavesdropper is detected and the secure key is erased.

The goal of this Section is to confirm the existence of Eve and it was conducted in sequences of 10, 18, 30 and 52 bits.

A step-by-step evaluation of the experiment shown in Figure 6 and includes the following steps:

Step 1: The pulsed laser is polarized to 90° using a polarizer.

Step 2: Alice turns her polarization plate to 45° , which is the x base, and sends a pulsed laser, emulating a single photon source. Alice sends a randomly chosen bit, simulated by the pulsed laser, which can be chosen using the python simulation. Let us assume Alice sends the bit “0”.

Step 3: Eve randomly turns her incident base. The random base can be chosen using the python simulation explained in the computational procedure Section 4. Let us assume Eve's incident base is +, which is 90° opposite to Alice's base.

Step 4: There is a 50% chance for Eve's detector to show bit “1” or bit “0”. For this scenario let us assume that Eve receives the bit “1”.

Step 5: Eve randomly turns her transmitted base. The random base can be chosen using the python simulation explained in the computational procedure Section 4. Let us assume Eve's transmitted base is x.

Step 6: Another pulsed laser, transmitted by Eve, emulates Eve sending bit “1” to Bob.

Step 7: Bob chooses his base randomly, as explained above. Let us assume Bob's base is x . Bob assumes that the received bit was from Alice. Bob's base is the same as Eve's transmitted base, so Bob receives the bit "1".

Step 8: Alice continues sending bits by proceeding back to step 1 for every assigned bit in her message.

4. Computational Procedure

To compare the experimental results with the theory, a Python script was computed for the simulation of the BB84 protocol, using modules such as numpy, endecrypt and more; see Appendix A for general functions of the simulation and code, and for full script at GitHub, see available materials.

For a genuine comparison between the experimental results and the simulation, all the randomly generated bits and bases (Alice: bits and base, Eve: incident and transmitted bases, Bob: base) were generated using the Python script. Consequently, the key simulation and the experimental procedure had the same randomly chosen bits and bases for the units.

In the presence of an eavesdropper, the code performs the sequence to detect whether Eve is eavesdropping by using randomly chosen bits, in case the bases chosen by the corresponding units are different. If an eavesdropper is not detected, a random key is generated, and the encryption/decryption is computed by the simulation.

In addition to that, a simulation with large numbers of random bits was executed: for 10^3 , 10^4 , 10^6 and 10^7 bits using the Python code. The convergence of matching bits in the presence of Eve should be roughly 25% of the total bits sent by Alice to Bob. For each sequence, the average simulation running time was measured for 10 different executions and recorded for the analysis of its complexity.

5. Results

All results tables for each part, including the random generated bases and bits, are given in Appendix A.

5.1. Alice & Bob without Eve

In this Section, an encrypted message was transmitted by Alice to Bob, as explained in the experimental Section 3, without an eavesdropper.

5.1.1. 18 Bit

The transmitted message in this Section was "E.M.", hence the key length should be at least 10. The results are shown in Figure A1. The accuracy was calculated as the number of matching bits divided by the number of total bits sent (Table 3). It is important to note that the generated key, both the experimental and simulated, is the bits sequence where the bases of Alice and Bob match. As expected, the accuracy is approximately 50% without an eavesdropper and no errors occur between the matching bases.

Table 3. An 18 bit accuracy for experiment and simulation—without Eve.

18 Bit—Without Eve		
Experiment	Matching Bases	10
	Matching Bits	10
	Accuracy	0.5556
Simulation	Matching Bases	10
	Matching Bits	10
	Accuracy	0.5556

Alice successfully transmitted her message to Bob using the encryption key, and Bob was able to decrypt it using the same key. The transmitted message procedure can be seen in Figure 7. Alice's encrypted message was sent to Bob in the + basis.

Message	E					M				
Binary Message	0	0	1	0	1	0	1	1	0	1
Key	0	1	1	1	0	0	0	0	0	0
Alice's Encrypted Message	0	1	0	1	1	0	1	1	0	1
Bob Received	0	1	0	1	1	0	1	1	0	1
Key	0	1	1	1	0	0	0	0	0	0
Bob's Decrypted Binary Message	0	0	1	0	1	0	1	1	0	1
Message	E					M				

Figure 7. An 18 bit transmitted message between Alice and Bob.

5.1.2. 52 Bit

The message transmitted in this Section was “BOHR”, hence the key length should be at least 20. The key distribution procedure was similar to the 18 bit part, and the results for the 52 bits are added in Figure 8. The accuracy was calculated similarly to the previous part, obtaining roughly 50% of the matching bases between Alice and Bob, as expected (Table 4). Alice successfully transmitted her message to Bob (Figure 8).

Message	B					O					H					R				
Binary Message	0	0	0	1	0	0	1	1	1	1	0	1	0	0	0	1	0	0	1	0
Shorten Key	1	0	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0
Alice's Encrypted Message	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0
Bob Received	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0
Shorten Key	1	0	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0
Bob's Decrypted Binary Message	0	0	0	1	0	0	1	1	1	1	0	1	0	0	0	1	0	0	1	0
Message	B					O					H					R				

Figure 8. A 52 bit transmitted message between Alice and Bob.

Table 4. A 52 bit accuracy for experiment and simulation—without Eve.

52 Bit—Without Eve		
Experiment	Matching Bases	33
	Matching Bits	33
	Accuracy	0.6346
Simulation	Matching Bases	33
	Matching Bits	33
	Accuracy	0.6346

5.2. Alice and Bob with Eve

In this Section, Eve was placed between Alice and Bob, as explained in the experimental Section 3. Alice transmitted bits to Bob in order to detect the eavesdropper.

5.2.1. 10 Bit

Alice sent 10 bits to Bob after randomly choosing the bases and bits as explained previously. The results can be seen in Figure A3. The accuracy was calculated as the number of matching bits divided by total bits sent. As expected, in the presence of a third party in the public channel, the accuracy is approximately 25–30% and both Alice and Bob know that an eavesdropper is present (Table 5). It is important to note that a 10 bits sequence is a short sample; even in the presence of an eavesdropper and after the base comparison, Alice and Bob record the same bit. Therefore, they are unaware of Eve's presence, even though the accuracy is 30%.

Table 5. A 10 bit accuracy for experiment and simulation—with Eve.

10 Bit—With Eve		
Experiment	Matching Bases	3
	Matching Bits	3
	Accuracy	0.3
Simulation	Matching Bases	3
	Matching Bits	3
	Accuracy	0.3

5.2.2. 18 Bit

Alice sent 18 bits to Bob after randomly choosing the bases and bits as explained previously. The results can be seen in Figure A4. The accuracy was calculated similarly to the previous part. As expected, in the presence of a third party in the public channel, the accuracy is approximately 25% and both Alice and Bob know that an eavesdropper is present (Table 6).

Table 6. An 18 bit accuracy for experiment and simulation—with Eve.

18 Bit—With Eve		
Experiment	Matching Bases	10
	Matching Bits	5
	Accuracy	0.2777
Simulation	Matching Bases	10
	Matching Bits	5
	Accuracy	0.2777

5.2.3. 30 Bit

Alice sent 30 bits to Bob after randomly choosing the bases and bits as explained previously. The results can be seen in Figure A5. The accuracy was calculated similarly to the previous part. As expected, in the presence of a third party in the public channel the accuracy is approximately 25–30%, and both Alice and Bob know that an eavesdropper is present (Table 7).

Table 7. A 30 bit accuracy for experiment and simulation—with Eve.

30 Bit—With Eve		
Experiment	Matching Bases	13
	Matching Bits	10
	Accuracy	0.3333
Simulation	Matching Bases	13
	Matching Bits	9
	Accuracy	0.3

5.2.4. 52 Bit

Alice sent 52 bits to Bob after randomly choosing the bases and bits as explained previously. The results can be seen in Figure A6. The accuracy was calculated similarly to the previous part. As expected, in the presence of a third party in the public channel

the accuracy is approximately 25%, and both Alice and Bob know that an eavesdropper is present (Table 8).

Table 8. A 52 bit accuracy for experiment and simulation—with Eve.

52 Bit—With Eve		
Experiment	Matching Bases	24
	Matching Bits	13
	Accuracy	0.25
Simulation	Matching Bases	24
	Matching Bits	14
	Accuracy	0.2692

5.3. Alice and Bob with Eve—Large Numbers Simulation

The eavesdropper detection procedure was simulated for long sequences of: 10^3 , 10^4 , 10^6 and 10^7 bits. The results can be seen in Table 9. The accuracy was calculated as the number of matching bits divided by the number of total bits sent, similarly to all previous parts. The accuracy converges to approximately 25–32%.

Table 9. Large number simulations for Alice, Bob and Eve setup, including average running times.

Large Numbers Simulation		
10^3 Bits Sent	Matching Bases	514
	Matching Bits	317
	Accuracy	0.317
	Average Running Time	0.0323 s
10^4 Bits Sent	Matching Bases	4979
	Matching Bits	3077
	Accuracy	0.3077
	Average Running Time	0.2415 s
10^6 Bits Sent	Matching Bases	499,946
	Matching Bits	312,162
	Accuracy	0.3121
	Average Running Time	14.9789 s
10^7 Bits Sent	Matching Bases	5,001,162
	Matching Bits	3,127,547
	Accuracy	0.31275
	Average Running Time	143.7181 s

6. Discussion

Quantum key distribution is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. The proposed experimental apparatus illustrates the key principles of quantum key distribution [1]. In both experiment and simulations, the eavesdropper can be detected. Nonetheless, if there is no eavesdropper, an encrypted message can be sent via a public channel between two parties, using the same procedure.

The experimental procedure does not require any special training and can be conducted by undergraduate students. Furthermore, the experimental setup is affordable and can be built using commercially available optical components. The computational simulation can help students worldwide, especially in developing countries.

The measurements for 18 and 52 bits without an eavesdropper showed an accuracy of approximately 50% of matching bits from the total number of bits sent. This corresponds to the theory according to which Alice and Bob create a secure key for encryption. The measurements for different sequences of bits with an eavesdropper showed an accuracy of roughly 25% of matching bits from the total number of bits sent. As explained previously, such accuracy alerts Alice and Bob that an eavesdropper is present in the system, hence they need to create a new key. Eve's measurements are shown in the results table for educational purposes, and, even without knowing them, it is possible to detect an eavesdropper.

A computer simulation was written along the experiment in order to compare the results. Although the complexity of this simulation is not ideal and at around $\sim O(N^2)$, we believe it introduces quantum cryptography principles, mainly in terms of eavesdropper detection. Rounding errors and computed pseudo-random numbers might affect the accuracy of the simulation, hence we anticipate an accuracy of around 20–30% with the presence of an eavesdropper. Nonetheless, for educational purposes, the script reliably simulates the presence of an eavesdropper as well as key distribution. Let us note that the major difference between this analogous experiment and a true quantum cryptography setup is that genuine security from interception can only be guaranteed if a single photon source is used. Hence, the information of a bit has to be transported only by a single photon. If any classical light source (even a weakened laser) is used instead of a single photon source, Eve cannot be detected. All that is required to eavesdrop is for Eve to separate a portion of the transmitted light for detection/analysis while sending the remainder to Bob unnoticed. Since the detailed experiment in the paper uses a pulsed light source (not a single photon source), it cannot truly be employed as a perfect encryption system. However, the sequence of the protocol is completely identical to a true quantum encryption system.

We believe that this experimental protocol can be easily adapted in other higher education facilities, using the same experimental procedure and simulation. It is worth mentioning that similar experiments have been carried out in the past [31–33], yet due to their complexity were fairly challenging for repetition in undergraduate laboratories. A simplified experimental setup along with the user-oriented computational simulation, described here, can assure an easy implementation while maintaining high educational standards.

Author Contributions: Conceptualization, supervision and methodology, G.G.R.; Software, validation, formal analysis, investigation, writing, Y.B. and I.F.; Project administration, review and editing, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The simulations mentioned in this article are available online: <https://github.com/yuvalbloom/Quantum-Cryptography-BB84-protocol> (accessed on 20 January 2022). Experimental data can be obtained upon a reasonable request from co-authors.

Acknowledgments: We thank Haim Suchowski, Moshe Shmilovich and the school of physics and astronomy for providing us the necessary tools and laboratory equipment to perform this study. G.G.R. is generally thankful for Ady Arie's guidance, wisdom and support. We also thank Thorlabs for the purchased educational kit and the instruction manual.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Additional Figures

	1	2	3	4	5	6	7	8	9
Alice Basis	+	x	+	x	+	+	+	x	+
Alice Bit	0	1	0	1	1	1	1	0	0
Bob Basis	+	x	x	x	x	x	+	x	+
Bob Bit Simulation	0	1	1	1	1	1	1	0	0
Bob Bit Experiment	0	1	0	1	0	1	1	0	0
matching basis									
matching bits									
	10	11	12	13	14	15	16	17	18
+	+	+	+	x	x	+	+	x	+
0	0	1	0	0	0	1	0	1	0
x	+	x	x	+	x	x	+	+	+
1	0	1	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	1	0

Figure A1. 18 bit key distribution results—Alice & Bob.

	1	2	3	4	5	6	7	8	9
Alice Basis	x	x	x	x	+	x	+	+	+
Alice Bit	1	0	0	0	1	0	0	0	0
Bob Basis	x	x	x	+	+	x	+	x	+
Bob Bit Simulation	1	0	0	0	1	0	0	0	0
Bob Bit Experiment	1	0	0	0	1	0	0	1	0
	10	11	12	13	14	15	16	17	18
	x	+	+	+	+	x	+	x	x
	0	1	1	1	1	1	0	1	0
	x	x	+	+	x	+	+	x	+
	0	0	1	1	0	0	0	1	0
	0	0	1	1	0	1	0	1	0
	19	20	21	22	23	24	25	26	27
Alice Basis	x	x	+	x	x	x	+	x	+
Alice Bit	0	0	0	0	0	0	0	0	0
Bob Basis	x	x	+	x	x	+	+	x	x
Bob Bit Simulation	0	0	0	0	0	1	0	0	1
Bob Bit Experiment	0	0	0	0	0	0	0	0	1
	28	29	30	31	32	33	34	35	36
	x	+	x	+	x	x	x	+	+
	0	1	1	1	0	0	1	1	1
	x	x	+	+	x	x	+	+	+
	0	1	1	1	0	0	0	1	1
	0	0	1	1	0	0	1	1	1
	37	38	39	40	41	42	43	44	45
Alice Basis	+	x	x	+	x	+	+	+	+
Alice Bit	0	1	0	1	1	0	0	1	1
Bob Basis	+	+	+	x	+	x	+	+	+
Bob Bit Simulation	0	1	1	1	1	0	0	1	1
Bob Bit Experiment	0	1	0	0	1	1	0	1	1
		46	47	48	49	50	51	52	
		+	+	+	+	+	+	+	
		1	0	0	0	0	1	1	
		+	x	+	x	+	x	+	
matching basis		1	0	0	0	0	1	1	
matching bits		1	1	0	1	0	0	1	

Figure A2. 52 bit key distribution results—Alice & Bob.

	1	2	3	4	5	6	7	8	9	10
Alice Base	+	x	+	x	+	x	x	x	+	x
Alice Bit	0	1	1	0	0	0	1	1	0	0
Eve Base Incident	x	x	+	x	+	+	+	+	x	+
Eve Base Transmitted	+	+	x	+	+	+	+	+	x	x
Bob Base	x	x	x	+	x	x	+	+	+	+
Eve Bit Experiment	1	1	1	0	0	1	1	1	1	1
Bob Bit Experiment	1	1	1	0	0	0	1	1	0	1
Eve Bit Simulation	1	1	1	0	0	0	0	0	1	1
Bob Bit Simulation	1	1	1	0	1	0	0	0	0	1
matching basis										
matching bits										

Figure A3. 10 bit transmission results from Alice to Bob with Eve—experiment and simulation.

	1	2	3	4	5	6	7	8	9
Alice Basis	+	+	+	+	x	+	x	x	+
Alice Bit	0	1	0	0	0	0	0	0	0
Eve Basis Incident	x	x	x	x	+	x	+	+	+
Eve Basis Transmitted	x	+	x	x	x	x	x	x	x
Bob Basis	+	x	x	x	x	x	+	x	x
Eve Bit Experiment	1	1	1	1	1	1	1	1	0
Bob Bit Experiment	1	0	1	1	1	1	0	1	0
Eve Bit Simulation	0	1	1	1	1	1	1	1	0
Bob Bit Simulation	1	0	1	1	1	1	1	1	0
matching basis									
matching bits									
non matching bits									
	10	11	12	13	14	15	16	17	18
	x	x	x	+	+	x	+	x	x
	1	0	1	1	0	0	0	1	0
	x	x	+	+	+	+	+	x	+
	x	x	x	+	+	x	x	x	+
	x	+	x	+	+	x	x	x	x
	1	0	1	1	0	1	0	1	1
	1	1	1	1	0	1	0	1	1
	1	0	0	1	0	0	0	1	0
	1	1	0	1	0	0	0	1	1

Figure A4. 18 bit transmission results from Alice to Bob with Eve—experiment and simulation.

	1	2	3	4	5	6	7	8	9
Alice Basis	x	+	+	x	x	+	+	+	x
Alice Bit	1	0	1	1	0	0	0	0	0
Eve Basis Incident	x	+	+	x	x	x	+	x	+
Eve Basis Transmitted	+	x	+	x	x	+	+	x	+
Bob Basis	+	x	+	+	+	+	+	x	+
Eve Bit Experiment	1	0	1	1	0	1	0	1	1
Bob Bit Experiment	1	0	1	0	0	1	0	1	1
Eve Bit Simulation	1	0	1	1	0	0	0	1	1
Bob Bit Simulation	1	0	1	1	1	0	0	1	1
	10	11	12	13	14	15			
	+	x	x	x	+	x			
	1	0	1	1	0	1			
	x	+	+	x	+	x			
	+	+	+	+	+	x			
	x	x	+	+	+	+			
	1	1	1	1	0	1			
	1	1	1	1	0	0			
	1	0	1	1	0	1			
	1	0	1	1	0	0			
	16	17	18	19	20	21	22	23	24
Alice Basis	+	x	+	+	+	+	+	+	+
Alice Bit	1	1	1	0	1	1	0	0	1
Eve Basis Incident	+	x	x	x	+	+	x	+	x
Eve Basis Transmitted	x	+	+	x	+	x	+	+	+
Bob Basis	+	+	+	+	+	+	x	+	+
Eve Bit Experiment	1	1	1	1	1	1	1	0	1
Bob Bit Experiment	0	1	1	0	1	1	1	0	1
Eve Bit Simulation	1	1	0	1	1	1	1	0	0
Bob Bit Simulation	0	1	0	0	1	0	0	0	0
matching basis									
matching bits									
non matching bits									
			25	26	27	28	29	30	
			+	+	x	+	+	x	
			0	0	1		1	0	
			x	+	+	x	+	+	
			x	+	+	x	x	x	
			x	x	x	x	x	+	
			1	0	1	1	1	1	
			1	0	1	1	1	0	
			1	0	0	1	1	1	
			1	0	1	1	1	1	

Figure A5. 30 bit transmission results from Alice to Bob with Eve—experiment and simulation.

	1	2	3	4	5	6	7	8	9
Alice Basis	x	x	x	+	x	x	x	+	x
Alice Bit	0	0	0	0	1	0	1	1	0
Eve Basis Incident	+	+	+	+	x	x	+	+	x
Eve Basis Transmitted	x	x	+	+	x	x	+	+	x
Bob Basis	x	+	+	+	x	+	+	+	+
Eve Bit Experiment	1	1	1	0	1	0	1	1	0
Bob Bit Experiment	1	0	1	0	1	0	1	1	0
Eve Bit Simulation	0	1	0	0	1	0	0	1	0
Bob Bit Simulation	0	0	0	0	1	0	0	1	0
	10	11	12	13	14	15	16	17	18
	x	+	+	x	x	+	x	+	x
	1	0	1	0	1	1	1	1	1
	+	+	+	+	x	x	+	x	+
	+	x	+	+	x	+	x	+	+
	x	x	+	+	+	+	+	x	x
	1	0	1	1	1	1	1	1	1
	0	0	1	1	0	1	0	1	0
	1	0	1	0	1	0	1	0	1
	0	0	1	0	0	0	1	0	1
	19	20	21	22	23	24	25	26	27
Alice Basis	+	+	+	x	+	x	+	+	+
Alice Bit	1	1	0	1	1	0	0	1	0
Eve Basis Incident	x	x	+	+	x	x	x	+	+
Eve Basis Transmitted	x	x	x	x	x	+	+	x	+
Bob Basis	x	+	+	x	x	x	+	+	x
Eve Bit Experiment	1	1	0	1	1	0	1	1	0
Bob Bit Experiment	1	0	1	1	1	0	1	0	0
Eve Bit Simulation	1	1	0	0	1	0	0	1	0
Bob Bit Simulation	1	1	0	0	1	0	0	0	1
	28	29	30	31	32	33	34	35	36
	x	x	+	+	+	+	+	+	+
	1	0	1	0	0	0	1	1	1
	+	+	+	x	x	x	x	x	x
	+	+	x	+	x	+	x	x	+
	x	+	+	x	x	+	+	+	+
	1	1	1	0	1	1	1	1	1
	1	1	1	0	1	1	0	0	1
	0	1	1	1	1	0	0	0	1
	0	1	0	0	1	0	1	0	1
	37	38	39	40	41	42	43	44	45
Alice Basis	+	x	x	x	+	x	+	+	x
Alice Bit	0	1	0	1	1	0	0	0	1
Eve Basis Incident	x	+	+	+	+	+	x	x	x
Eve Basis Transmitted	+	+	+	x	+	+	x	x	+
Bob Basis	x	x	x	+	x	+	x	x	+
Eve Bit Experiment	1	1	1	1	1	1	1	1	1
Bob Bit Experiment	1	1	1	0	1	1	1	1	1
Eve Bit Simulation	0	1	0	1	1	1	0	0	1
Bob Bit Simulation	1	0	1	0	1	1	0	0	1
	46	47	48	49	50	51	52		
	+	x	x	x	+	+	x		
	1	1	0	0	1	0	0		
	x	+	+	x	+	x	x		
	+	x	x	+	+	x	+		
	x	+	+	+	+	+	+		
	1	1	1	0	1	1	0		
	1	0	0	0	1	0	0		
	0	1	1	0	1	0	0		
	1	0	0	0	1	1	0		
matching basis									
matching bits									
non matching bits									

Figure A6. 52 bit transmission results from Alice to Bob with Eve—experiment and simulation.

References

1. Bennet, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Ferguson, N.; Schneier, B. *Practical Cryptography*; Wiley Publishing, Inc.: New York, NY, USA, 2003.
3. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. *A Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1997. [CrossRef]
4. Kahn, D. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*; Scribner: New York, NY, USA, 1996.
5. Broemeling, D.L. An account of early statistical inference in Arab cryptology. *Am. Stat.* **2011**, *65*, 255–257. [CrossRef]
6. Gannon, J. *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*; Potomac Books, Inc.: Washington, DC, USA, 2001. Available online: <https://muse.jhu.edu/book/28133> (accessed on 10 January 2022).
7. Merkle, R.C. Secure communications over insecure channels. *ACM* **1978**, *21*, 294–299. [CrossRef]
8. Portmann, C.; Renner, R. Cryptographic security of quantum key distribution. *arXiv* **2014**, arXiv:1409.3525.
9. Diffie, W.; Hellman, M.E. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–655. [CrossRef]
10. Diffie, W.; Hellman, M.E. Multiuser cryptographic techniques. In Proceedings of the National Computer Conference and Exposition (AFIPS '76), New York, NY, USA, 7–10 June 1976; American Federation of Information Processing Societies: Montvale, NJ, USA, 1976; pp. 109–112. [CrossRef]
11. Sharbat, M.S. Quantum cryptography: An emerging technology in network security. In Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 15–17 November 2011; pp. 13–19. [CrossRef]
12. Griffiths, D.J.; Schroeter, D.F. *Introduction to Quantum Mechanics*; Cambridge University Press: Cambridge, UK, 2018. [CrossRef]
13. Muller-Kirsten, H.J.W. *Introduction to Quantum Mechanics: Schrodinger Equation and Path Integral*; World Scientific Co. Ltd.: Hackensack, NJ, USA, 2012. [CrossRef]
14. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
15. Zurek, W.H.; Wootters, W.K. A Single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803.
16. Bird, J.J.; Ekert, A.; Faria, D.R. On the effects of pseudorandom and quantum-random number generators in soft computing. *Soft Comput.* **2020**, *24*, 9243–9256. [CrossRef]
17. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [PubMed]
18. Shields, A.J.; Dynes, J.F.; Yuan, Z.L.; Lucamarini, M. Overcoming the rate distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403.
19. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nature Comm.* **2017**, *8*, 15043. [CrossRef] [PubMed]
20. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
21. Bellovin, S.M. Frank Miller: Inventor of the one time pad. *Cryptologia* **2011**, *35*, 203–222. [CrossRef]
22. Bender, A.; Beller, S. Mangarevan invention of binary steps for easier calculation. *Proc. Natl. Acad. Sci. USA* **2014**, *111*, 1322–1327. [CrossRef] [PubMed]
23. Chrisomalis, S. *Numerical Notation: A Comparative History*; Cambridge University Press: Cambridge, UK, 2010. [CrossRef]
24. Mackenzie, C.E. *Coded Character Sets, History and Development*; Addison-Wesley Pub.: Boston, MA, USA, 1979. Available online: https://textfiles.meulie.net/bitsaved/Books/Mackenzie_CodedCharSets.pdf (accessed on 10 January 2022).
25. Barker, E.; Kelsey, J. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015. [CrossRef]
26. Born, M.; Wolf, E. *Principles of Optics*, 7th ed.; Cambridge University Press: Cambridge, UK, 2002. [CrossRef]
27. Fowles, G.R. *Introduction to Modern Optics*; Dover Publications: Mineola, NY, USA, 1989.
28. Dirac, P.A.M. A New notation for quantum mechanics. *Math. Proc. Camb. Philos. Soc.* **1939**, *35*, 416–418. [CrossRef]
29. ThorLabs: Laser Modules: 635 nm. Available online: <https://www.thorlabs.com/thorproduct.cfm?partnumber=CPS635R> (accessed on 10 January 2022).
30. ThorLabs: Quantum Cryptography Analogy Demonstration Kit. Available online: <https://www.thorlabs.com/thorproduct.cfm?partnumber=EDU-QCRY1/M> (accessed on 10 January 2022).
31. Nugraha Utama, A.; Lee, J.; Seidler, M.A. A hands-on quantum cryptography workshop for pre-university students. *Am. J. Phys.* **2020**, *88*, 1094–1102. [CrossRef]
32. Lemelle, D.S.; Almeida, M.P.; Souto Ribeiro, P.H.; Walborn, S.P. A simple optical demonstration of quantum cryptography using transverse position and momentum variables. *Am. J. Phys.* **2006**, *74*, 542–546. [CrossRef]
33. Camargo, A.L.P.; Pereira, L.O.; Balthazar, W.F.; Huguenin, J.A.O. Simulation of the BB84 protocol of quantum cryptography by using an intense laser beam. *Rev. Bras. Ensino Fis.* **2017**, *39*, e2305. [CrossRef]