TEL AVIV UNIVERSITY

Using Quantum Mechanics For Secure Communication

Alon Shaaltiel,[1] Oren Kereth,[1] and Georgi Gary Rozenman[1,2]

[1] *Raymond and Beverly Sackler School of Physics and Astronomy, Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 69978, Israel*

[2] *School of Electrical Engineering, Iby and Aladar Fleischman Faculty of Engineering, Tel Aviv University, Tel Aviv 69978, Israel*

(Dated: July 5, 2022)

Using linearly polarized light we execute the BB84 protocol for quantum cryptography. The protocol is examined when no eavesdropper is present and a key is transmitted securely between two users. The results are compared with a simulation of the system. As the BB84 protocol uses quantum mechanics, an eavesdropper cannot measure the signal without altering it and so they are detected. Detection of an eavesdropper under the BB84 is also examined and the results are compared with a simulation of the system.

Introduction

Historical Review

The first documented use of cryptography is from Egypt dating 4000 years ago [1]. Cryptography is the science of writing in secret code, which is necessary when communicating over any untrusted medium [2]. Most cryptographic protocols make use of "keys" to encrypt and decrypt data [3]. The idea of quantum cryptography, which utilizes quantum mechanics in cryptographic protocols, was first proposed in the 1970s by Stephan Wiesner, Charles H.Bennet and Gilles Brassard [4]. Based on this idea, the protocol we use in this experiment, BB84, was invented. BB84 allows its users to securely create an encryption key and to detect eavesdroppers [5]. Since its invention, BB84 was proven to be secure both theoretically and experimentally [6, 7]. With the advancements of technology, practical implementations of BB84 are being tested. Among these implementations are satellite-to-ground quantum communication using BB84 encryption over a distance of 1200km [8], underwater communication[9, 10] and more. In the near future, BB84 could be used worldwide due to its secure nature and the improvement of technology over time.

Theoretical Review

A key that will be used to encrypt data is formed from a sequence of '0's and '1's . In this experiment the polarization of light transmitted between the two communicating users, "Alice" and "Bob", is used to signify 0 and 1. The light can be polarized and measured in two different bases, + and ×. In the + basis, light can be linearly polarized at either 0° or 90°, denoted by $|0°\rangle$ and $|90°\rangle$ respectively. These polarizations are by definition orthogonal and therefore $|0°\rangle$ can denote '1' and $|90°\rangle$ can denote '0' without the two mixing. In the × basis, light can be polarized at either 45° or −45°, denoted similarly by $|45°\rangle$ and $|-45°\rangle$ respectively. These polarizations are orthogonal too, and so $|45°\rangle$ denotes '1' and $|-45°\rangle$ denotes '0' when the light is measured in this basis. Using linear algebra it can be shown that

$$\left|45°\right\rangle = \frac{1}{\sqrt{2}}(\left|0°\right\rangle + \left|90°\right\rangle); \left|-45°\right\rangle = \frac{1}{\sqrt{2}}(\left|0°\right\rangle - \left|90°\right\rangle) \quad (1)$$

and similarly from these relations it can be shown that

$$\left|0°\right\rangle = \frac{1}{\sqrt{2}}(\left|45°\right\rangle + \left|-45°\right\rangle); \left|90°\right\rangle = \frac{1}{\sqrt{2}}(\left|45°\right\rangle - \left|-45°\right\rangle) \quad (2)$$

Based on the quantum mechanical treatment of the polarizations, the relations above indicate that measuring the polarization of light that was polarized in the × basis in the + basis has an equal probability of yielding either '0' or '1', and vise-versa.

BB84

The BB84 encryption protocol makes use of the two different bases that share the relations in equations 1 and 2. The protocol is as follows: one of the communicating users, Alice, chooses a basis (either + or ×) at random. Alice then chooses a bit in that basis (either 0 or 1) and transmits a photon with the corresponding polarization in the basis she has chosen. Independently, the second user, Bob, chooses a basis at which he measures the polarization of the transmitted photon. Upon measurement, Bob documents the result (either 0 or 1) and the basis at which he chose to measure the polarization, while Alice documents the basis and bit she chose to transmit. The two users repeat this step many times. Alice and Bob then go through their measurements and compare the bases they have chosen for each measurement. They then discard the measurements in which Alice and Bob have chosen different bases and keep only those that have the same basis. Alice and Bob then publicly compare bits from a sample group chosen at random from the remaining measurements. In an ideal communication channel that is not eavesdropped on, they expect all the bits to be the same (i.e if Alice sent a 1 in × basis and Bob chose to measure in the × basis he is guaranteed to get a 1 too) and thus from the remaining bits that they have not compared they will form the key with which they will now encrypt and decrypt data from each other. However, if there

is an eavesdropper, "Eve", spying on their communication, she will inevitably interfere with the transmission, allowing us to intercept her. Suppose Eve is eavesdropping on the communication between Alice and Bob. Eve receives the polarized photon from Alice. Suppose that Bob and Alice have both chosen the same basis in that measurement, + and that Alice transmitted a 1. At a probability of 50% Eve will choose the + basis, leading to a correct measurement of the polarization. She will then replicate the result by choosing the basis with which she has measured the polarization, to transmit to Bob a photon polarized in that basis at a state corresponding to the bit she measured. In this case, she will transmit the exact same polarization to Bob, which will then receive exactly what Alice tried to transmit, leaving Eve undetected in this case. In the other 50% of the cases, Eve will choose the wrong basis, ×. She will then transmit the photon with a polarization in that wrong basis, therefore, when Bob will measure the polarization in 50% of the cases he will get a 1 and on the remaining 50% of the cases he will get a 0. Therefore, despite choosing the exact same basis as Alice, in $50\% \times 50\% = 25\%$ of the cases he will measure the wrong bit because of Eve. Consequently, if 25% of the compared bits turn out to be different from each other, Bob and Alice can detect Eve and cease communication on that channel. As we have shown here, BB84 allows its users to either detect an eavesdropper or to safely form a key with which they will communicate safely.

Half-Wave Plate

As we have seen above, the protocol heavily relies on the ability of its users to transmit and measure photons with different polarizations. In this experiment this will be done using half-wave plates, also known as a "polarization rotator". A polarization rotator rotates the polarization of the incident light by double the physical rotation angle of the wave plate, denoted by θ (see Figure 1).

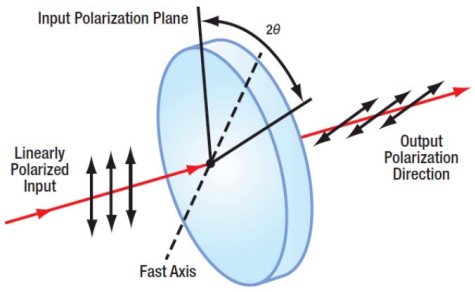

Figure 1: A schematic of a polarization rotator. θ is the physical rotation angle of the wave plate. Incident polarized light that passes through the polarization rotator has its polarization rotated by 2θ.

For example, if the incident light is in the state $|0°\rangle$ and the polarization rotator is rotated by 45°, the light will be rotated to the $|90°\rangle$ state.

Experimental Setup

The experiment consists of two parts. The first part contains only Alice and Bob communicating a key to each other without the existence of an eavesdropper on the channel. For the second part we add Eve, the eavesdropper. We then check if the BB84 protocol enables us to detect Eve.

First Part

The experimental setup of the first part consists of two units. The first unit 'belongs' to Alice and is capable of transmitting light with different linear polarizations according to the two bases $+, \times$. The second unit belongs to Bob and is capable of detecting the light and measuring its polarization (see Figure 2).

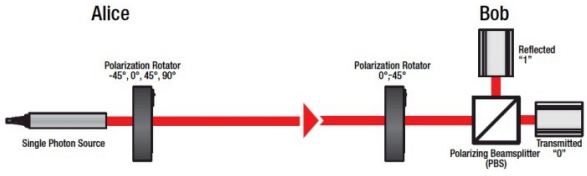

Figure 2: The experimental setup of the first part. On the left- Alice's unit which transmits the bits via polarized light. On the right- Bob's unit which detects the light and measures its polarization.

Alice's unit uses a single photon source that produces vertically polarized light ($|0°\rangle$). The light then goes through a polarization rotator which can change the polarization of light to one of four angles at the two different bases: + ($|0°\rangle, |90°\rangle$) and × ($|45°\rangle, |-45°\rangle$). In this method Alice is capable of transmitting bits of information in the two bases required for the protocol. Bob then chooses a basis of measurement by rotating the polarization of the incident light at either 0° or −45°. The polarized light then goes through a polarizing beamsplitter (PBS) that transmits the horizontal component of polarization ($|90°\rangle$) and reflects the vertical component ($|0°\rangle$). This allows Bob to measure the polarization in the two different bases. For example, if Alice transmits $|45°\rangle$ (a 1 bit in the × basis) and Bob rotates the polarization by −45° (measuring in × basis) the light will turn to $|0°\rangle$. It will then be reflected by the PBS and Bob will measure a 1 as required. If Bob measures in the + basis the polarization of the light will not change. Because $|45°\rangle$ consists of vertical and horizontal components in equal magnitude (according to equation 1) half the time Bob will mea-

sure a 1 and in the other half he will measure a 0. We have thus shown that the composition of Bob's unit allows him to perform all the operations required of him according to the BB84 protocol. In this part of the experiment Alice sends to Bob three sequences of bits with varying lengths (18,50 and 100 bits), the bits that were sent and received with the same basis form the key, upon comparison we expect no errors as the system is ideal with no eavesdropper.

Second Part

We now add an eavesdropper to the communication channel, Eve. Eve detects the photon transmitted by Alice and measures its bit in a randomly chosen basis. Eve then replicates the measured bit and transmits it to Bob in the same basis she measured in. To perform these operations according to the protocol, Eve's unit is a combination of Alice's and Bob's units (see Figure 3).

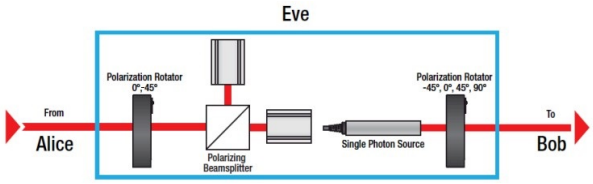

Figure 3: The added unit to the experimental setup for the second part. Eve's unit is a combination of Bob's and Alice's units. Eve is capable of measuring bits from Alice and transmitting the results of her measurement to Bob.

The "Bob part" of Eve's unit allows Eve to detect and measure the bits transmitted to her as explained in the first part and the "Alice part' of Eve's unit allows her to transmit the measurement to Bob in the basis she has chosen. Apart from the addition of Eve to the setup nothing else has changed. In this part of the experiment we will attempt to detect Eve using the protocol with sequences of 18 bits, 50 bits and 100 bits.

Results

First Part

By transmitting sequences of 18,50 and 100 bits from Alice to Bob, forming a key according to the protocol and comparing the results to a simulation the following results have been concluded (see Table I)

———	**Experiment**	**Simulation**
Sequence Length	Key Length(% of bits)	
18	10(56%)	8(44%)
50	27(54%)	27(54%)
100	48(48%)	54(54%)

Table I: First part - results table

As mentioned in a previous section, the length of the key is determined by the number of bits that were transmitted by Alice in the same basis as the one Bob used to measure them, leading to its correct interpretation (meaning that if Alice transmitted a '1' Bob also measured a '1'). According to our model, the probability Alice and Bob chose the same basis for a certain bit is 50%. In both the experiment and simulation it appears that the length of the key is close to the expectancy according to the model (which is half of the sequence length). Moreover, in the experiment and simulation all the bits that were measured and transmitted in the same basis by Bob and Alice respectively were correctly interpreted. This is exactly as the model predicts and as we require for the protocol to work (in its most ideal case, in reality communication errors can and will occur, but the protocol can still allow its users to deduct the existence of a spy).

Second Part

After adding Eve to the setup as shown in 3, sequences of 18, 50 and 100 bits were transmitted from Alice to Bob and the results were analyzed according to the protocol. The bases for each bit measurement were compared and so were the bits corresponding to those measurements. From the comparison the following results have been concluded (see Table II)

Sequence Length	**#SBBs (% of bits)**	**#Errors (% of bits)**
18	8 (44%)	2 (25%)
50	18 (36%)	3 (17%)
100	54 (54%)	13 (24%)

(a) Experimental results. SBBs stands for "same basis bits" (i.e. bits for which Alice and Bob chose the same basis for transmission and measurement).

Sequence Length	**#SBBs(% of bits)**	**#Errors (% of bits)**
18	12 (66%)	3 (25%)
50	24 (48%)	4 (17%)
100	48 (48%)	12 (25%)

(b) Simulation results. SBBs stands for "same basis bits".

Table II: Second part - experimental and simulation results. The percentage of errors was calculated according to the number of SBBs.

As the data shows, upon the insertion of Eve there are errors in SBBs (unlike the first part which had no errors). The percentages of errors for all sequence lengths are close to 25% apart from the 17% errors which was recorded for 50 bits. Figure 4 shows the results from simulations of varying sequence lengths, for longer sequences the percentage of errors converges to 25%, just as the model predicts. Also shown is the variance in the percentage of errors around $x = 50$. Assuming the distance from 25% in each direction is three standard deviations away, the percentage around $x = 50$ is $0.25^{+0.0972}_{-0.0700}$ (1σ in each direction) which makes our measurement 1.1 standard deviations away, well within the desired range.

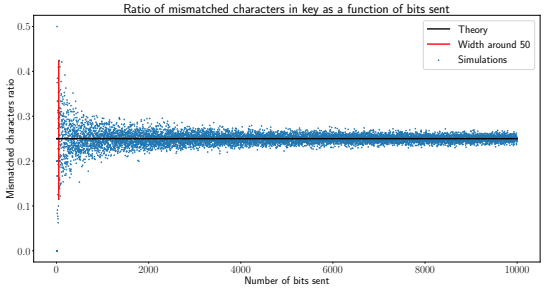

Figure 4: Graph of the percentage of errors in SBBs. The blue dots are simulations, the red line around $x = 50$ shows the width of the points around the black line at $y = 0.25$, which is the theoretical value that the model predicts.

Moreover, Figure 5 shows that according to our model the probability of getting 3 errors for 18 SBBs (which led to the 17% error for the 50 bits case) is greater than 5% (more accurately it is about 17%) and therefore the null hypothesis cannot be rejected and the model remains valid.

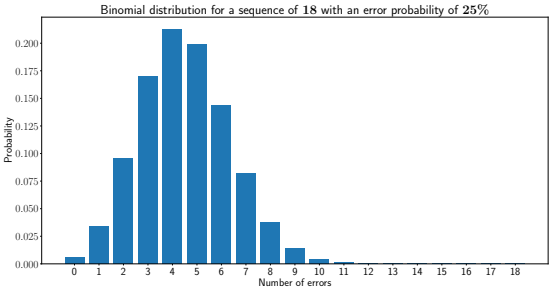

Figure 5: Binomial distribution for a sequence of 18 repetitions (18 SBBs) with a probability of 25% to fail (probability of getting an error at a certain SBB).

The BB84 protocol has therefore allowed us to detect Eve successfully.

Discussion

In this experiment we communicated via the BB84 protocol. In the first part of the experiment there was no eavesdropper, which allowed Alice and Bob to form a key successfully according to the protocol. The key consisted of about half the bits transmitted, in accordance with our theoretical model. Moreover, no errors were spotted in the comparison of SBBs, yet again in accordance with theoretical results for the case of no eavesdropper. The simulation has also demonstrated similar results. In the second part an eavesdropper, Eve, was added. The BB84 protocol allowed us to detect Eve, because for all three sequences transmitted from Alice to Bob there were errors in the comparison of SBBs. For the sequence of 18 and 100 transmitted bits the percentage of errors compared to the number of SBBs was either 25% or close to it. However, for the sequence of 50 bits the percentage was at about 17%, which is not as close to 25%. To assess this result, we used a binomial distribution whose probability of "failure" is 25%, relying on the theoretical model. We have shown that the probability of getting three errors out out of 18 is greater than our set significance level of 5%. In addition the expected variance in the ratio of errors was estimated using simulations and our measurement of 17% is 1.1 standard deviations from 25% which is in the desired range of 3 deviations. Therefore the theoretical model remains valid. We have also shown, using the simulation, that the percentage of errors converges to 25% for longer and longer sequences of transmitted bits, just as the model predicts. The simulation demonstrated similar results that are, too, in agreement with the model. The results we have achieved are in accordance with a previous experiment examining the BB84 protocol. The experiment obtained a percentage of errors close to zero in the absence of an eavesdropper and a percentage close to 25% in the presence of Eve [11]. All in all, we have demonstrated that the BB84 protocol enables secure communication and that it's theoretical model is valid.

[1] Cypher Research Laboratories Pty. Ltd. A brief history of cryptography. http://www.cypher.com.au/crypto_history.htm. Accesed on 14/6/2022.
[2] G. C. Kessler. *An Overview of Cryptography*. 2006.
[3] R. Din J. I. Ahmed and M. Ahmed. *Indonesian Journal of Electrical Engineering and Computer Science*, 12:447–454, 2018.
[4] W. Tittel N. Gisin, G. Ribordy and H. Zbinden. *Review Of Modern Physics*, 74, 2002.
[5] G. Brassard C.H. Bennett. *International Conference on Computers, Systems & Signal Processing*, 1, 1984.
[6] P. W. Shor and J.Preskill. *Physical Review Letters*, 85:441–444, 2000.
[7] N. Lutkenhaus W. Wang. Numerical security proof for decoy-state bb84 and measurement-device-independent qkd resistant against large basis misalignment. August 2021.
[8] S.K. Liao et al. *Nature*, 549:43–47, 2017.

[9] S.Li Z. Feng and Z.Xu. *Optics Express*, 29:8725–8736, 2021.

[10] S. Dong et al. Practical underwater quantum key distribution based on decoy-state bb84 protocol. Mars 2022.

[11] Adarsh Jain, Abhishek Khanna, Jay Bhatt, Parthkumar V Sakhiya, and R K Bahl. Experimental demonstration of free space quantum key distribution system based on the bb84 protocol. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–5, 2020.