Quantum Cryptography

Emily Gillott*
[redacted]

Third year laboratory report
(Dated: May 22, 2022)

In this experiment a classical analogue of the BB84 protocol was conducted to investigate the effect of eavesdropping. The data collected showed that in an eavesdropped system $27 \pm 8\%$ of the key was incorrectly measured where the Monte Carlo simulation gave $25 \pm 1.3\%$.

I. INTRODUCTION

Cryptography, derived from the Greek words kryptos (hidden) and graphein (writing), is a method of protecting the contents of a message as it was delivered from one person to another. Different forms of cryptography have been used throughout history from Egyptians using non-standard hieroglyphs, the Caesar Shift Cipher, and the famously known enigma code[1] [2].

In modern times cryptography has become increasingly important with digital communication with regards to security. Cryptography protects a message from theft, alteration and can also be used for authentication (to ensure that the receiver is the intended receiver)[3].

Quantum cryptography uses the laws of quantum mechanics to securely share a key used to encrypt a message (a process known as quantum key distribution or QKD). Unlike the mathematical algorithms which are currently used, quantum cryptography is safe from attack in advancement of quantum computers [4].

In this experiment the BB84 protocol was investigated to determine the effect of eavesdropping on QKD.

II. THEORY

A. Cryptography

In symmetric cryptography both the sender and the receiver use the same secret key. The sender converts a plain text message to binary, then uses the key to encrypt the message which should render the message unintelligible to anyone without the key. The message is then sent over a public channel (which anyone can access). The receiver then uses the key to decrypt the message and convert the binary back into text. [5].

Quantum cryptography uses QKD to securely share a key and alert the sender if the signal has been intercepted. There are two main methods of sending a key, one uses entangles particles and the other single photons of a specific polarisation state [2]. In this experiment only the latter will be investigated.

Three characters, Alice, Eve and Bob, will be used to simplify the theory of QKD. Alice, the sender, is trying to share a secure key with Bob, the receiver. Eve is trying in intercept the key (or "eavesdrop") without Alice and Bob detecting her presence.

B. BB84 protocol

The Bennet-Brussard (BB84) protocol uses the polarisation states of single photons. Two orthogonal basis are chosen, a diagonal ($\times$) and a rectilinear ($+$), in each basis a 0 and a 1 are defined [2] [6].

Alice sends single photons to Bob randomly choosing between the $\times$ and $+$ basis each time. Bob also selects a random basis and measured the polarisation state of the photons. If Alice and Bob have selected the same basis, the bit is successfully transmitted. If they are in different basis, the photon will be forced into a state in Bob's basis due to the collapse of the wave function and he will have a 50% chance of detecting either a 1 or a 0 [2] [6]. The case where Alice sends a 0 in both the $+$ and $\times$ basis has been summarised in Table I.

TABLE I. Table showing all the possible combinations when Alice sends a 0 bit to Bob in a non-eavesdropped system. This can be extended when Alice sends a 1. When the basis are unaligned there is an equal chance of detecting a 1 or a 0.

Alice basis	Alice bit	Bob basis	Bob bit
+	0	+	0
+	0	x	1 or 0
x	0	+	1 or 0
x	0	x	0

Once the Key has been sent Alice and Bob compare the basis they chose for each measurement and discard the bits where the basis were unaligned. Assuming perfect communication, Alice and Bob are left with the same sequence of random numbers used as the key. A

* This experiment was performed in collaboration with Antonin Rat ([redacted]).

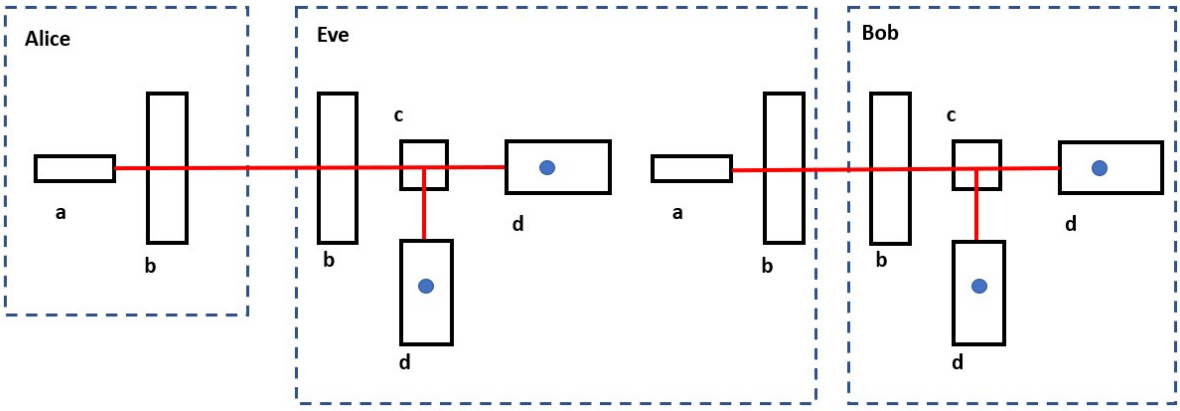

FIG. 1. Diagram of the experimental setup of Alice, Bob and Eve. When the system is not being eavesdropped the apparatus is the same as pictured above with Eve removed. a is a laser, b are half wave plates, c is a beam splitter and d are diode detectors.

sample from the key is chosen and the bits are compared, all of the bits should match [2].

If Eve is present, she also picks a random basis to measure the photon Alice sends. If she measured the photon in the correct basis, she can send a photon in the same state to Bob, as if she was not present. However, if she measures the photon in the wrong basis, she has no choice but to send Bob the photon she detected. If Alice and Bob are in the same basis but Eve is in the other basis, there is a chance that Bob will measure a different bit to the one Alice sent. The case where Alice sends a 0bit in the + basis has been shown in TABLE II. Alice and Bob then compare the basis over a public channel and discard the bits where they don't match as before. A sample of the key is taken and, due to the interference from Eve, there will be a 25% error rate [2].

TABLE II. Table showing all the possibilities of detection when Alice sends a 0 + bit while the channel has been intercepted by Eve. This can be extended for bot sending a 1 or using the × basis.

Alice basis	Alice bit	Eve Basis	Eve bit	Bob basis	Bob bit
+	0	+	0	+	0
				x	Rand
		x	Rand	+	Rand
				x	Same

In real applications of QKD there will always be errors transmitting photons for a number of reasons including, detector inefficiencies, birefringent materials, photon scattering and absorption and noise. If the error is sufficiently small, the QKD would not be impacted. However, if the transmission error becomes comparable to the error produced by eavesdropping, detecting Eve becomes problematic as it cannot be determined whether the errors were caused by Eve's presence or from the transmission [2].

III. METHOD

In this experiment a classical analogue of a quantum experiment was conducted. In place of using single photons to transmit the key, a laser was used to produce pulses of light. QKD does not work using laser pulses as it is possible to "steal" some of the beam without being detected.

A laser, half wave plates, beam splitters and photon detectors were set up as shown in FIG 1. The half wave plates were used to select the basis, the beam splitter splits the orthogonal polarizations of light to allow the detection of 0 and 1. When Alice and Bob are in different basis, light polarized in both directions are present and are incident on both detectors whereas in the quantum experiment there would only be one polarization. To remedy this, the detectors were connected to a system which randomly chose one to light up, acting as if one polarization passed through.

Firstly, 52 bits were sent from Alice to Bob (without Eve). This was repeated 10 times. Then the same was done with Eve. In both cases a sample of the key was taken and compared to see if Eve had interfered with the communication. Then a Monte Carlo simulation was run to produce more data.

Lastly neutral density filters of varying attenuation strengths were placed in the path of the laser to try and introduce errors such as incorrect bits or missed bits from the detectors.

IV. RESULTS

For the non-eavesdropped transmissions from Alice to Bob, it was found that 0 % of the bits in the key were incorrectly measured.

For the eavesdropped case, the number of bits Bob measured to be different to Alice was recorded. The data taken found an average of 27 % with a standard deviation of 8 % from the whole key. A sample of half of the key was taken and it gave an average of 25 % with a standard deviation of 17 %.

In the Monte Carlo simulation a 5000 bit code was sent and a sample of 1250 bits were taken from the key to determine if Eve was detected. This was repeated 1000 times to generate the histogram shown in Fig 2. The data has a mean 25.0% and a standard deviation of 1.3%. A Gaussian was fit to the histogram. The fit gives the centre as 25.0% and a standard deviation of 1.3%.

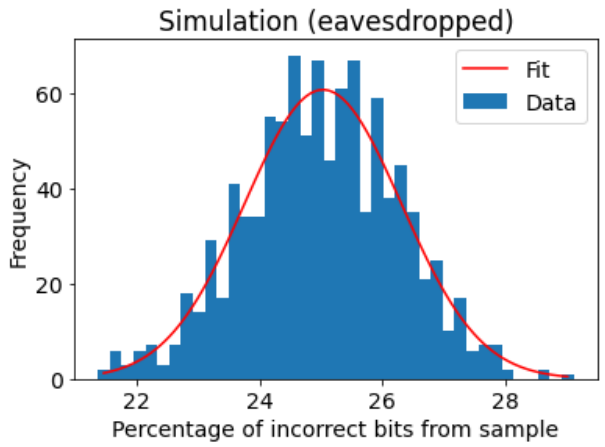

FIG. 2. Histogram showing the percentage of incorrect bits in a 1250 sample of the key.

The chi-square was calculated by summing the squares of the difference between the expected values and the values from the data then dividing by the number of degrees of freedom (taken to be the number of bins in the histogram). The fit has a chi-square value of 84.

It was found that the density filters didn't affect the detection of the light until a density of 0.4 was used. It was found that almost only 0s were being detected.

V. DISCUSSION

In the non-eavesdropped case the results were as expected with 0 % incorrect bits. However, in real applications of QKD the signal may be disrupted meaning some bits could be incorrectly measured despite the fact that the channel not being eavesdropped.

For the eavesdropped case, the experimental value of $27 \pm 8\%$ is consistent with the expected value of 25% but the data has a very large spread. This is due to the fact that the data collection was a slow process so only 10 keys were sent meaning that the data may not reflect the true statistics of the BB84 protocol.

The Monte Carlo simulation's detected $25 \pm 1.3\%$ of incorrect bits in the final key which is consistent with the expected value and has a much smaller spread than the experimental data. The chi-square value of the fit (84) suggests that the fit does not accurately represent the data, as the desired value is 1; this may be due to the noisy nature of the data.

The density filter was not a successful method of introducing random errors to the system as the sudden stop in the detection of 1s implies that the photon signal had become lower than the detector threshold.

VI. CONCLUSION

In summary, the BB84 protocol of QKD was conducted to investigate the effect of eavesdropping on the distribution of a key. It was found that in a channel with perfect communication 100% of the bits were successfully transmitted between Alice and Bob. When Eve was present, it was found that $27 \pm 8\%$ of the resulting key was incorrect which would alert Alice and Bob of her presence. A Monte Carlo simulation of the key distribution showed that $25 \pm 1.3\%$ of the bits were incorrect. Both of these values are consistent with the expected value from the theory.

[1] T. M. Damico, A brief history of cryptography, Inquiries Journal **1** (2009).

[2] M. A. M. Fox, eng*Quantum optics : an introduction*, Oxford master series in atomic, optical and laserphysics ; 15 (Oxford University Press, Oxford, 2006).

[3] G. C. Kessler, An overview of cryptography, (2003).

[4] Quantumxchange, Quantum cryptography, explained.

[5] G. C. Kessler, An overview of cryptography, (2003).

[6] J. Huang, Y. Wang, H. Wang, Z. Li, and J. Huang, Man-in-the-middle attack on bb84 protocol and its defence, in *2009 2nd IEEE International Conference on Computer Science and Information Technology* (2009) pp. 438–439.