Quantum Computing and CyberSecurity

Nix Brandon Correia

Department of Computer Science

Swansea University

This Dissertation is submitted for the degree of

Master of Cybersecurity

December 2023

Declaration

This work has not been previously accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed Nix Brandon Correia

Date 15/12/2022

Statement 1

This thesis is the result of my own investigations, except where otherwise stated. Other resources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed Nix Brandon Correia

Date 15/12/2022

Statement 2

I hereby give my consent for my thesis, if accepted, to be made available for photocopying and inter-library loan, and for the title and summary to be made available to outside organizations.

Signed Nix Brandon Correia

Date 15/12/2022

Acknowledgements

I would like to thank my Academic Mentor, Dr. Bertie Müller, for his guidance during the duration of this project.

Abstract

Modern Cryptography algorithms alone form the basis for the current internet, however with the evolution of cryptanalysis tools they are projected to become obsolete within a few decades. A few decades may not seem to be a small amount of time, however it would be possible to break encryption of a piece of data at a later date by saving its state. The evolution of tools being referred to is the development of quantum computing technology. The algorithms that can run on these tools can break the current classical computing based cryptographic algorithms within a reasonable timeframe. The difficulty of most encryption is a benefit of a mathematical operation that is difficult to reverse, this however stands true only for classical computers which operate on a different set of rules. The goal of this paper will be to compare various factors of different Quantum key distribution algorithms(BB84, E91) , with widely used classical algorithms (RSA, 3DES, ECDH). These factors include the average speed of algorithm execution, memory usage, security features and other venues of attack.

Table of Contents

Chapter 1

1.1 Introduction

a) Project Overview

Encryption is believed to provide complete and unfettered security for a set of data. This however is a gross overestimation of the concept. The data is not locked away forever but, is garbled in a way that can only be read using the key. The security of the algorithm thereby relies wholly upon the key used. Encryption algorithms can be broadly classified into Symmetric and Asymmetric encryption. Both these categories however require some form of transfer of the key. This arises the need for a secure channel. Since encrypting the key itself will lead to a type of dilemma, different methods need to be used. These methods rely heavily upon hard-to-reverse mathematical operations and concepts. Quantum cryptography takes a different path. It relies upon the laws of physics and quantum mechanics to prove its security, which in an ideal world seems unbreakable.

b) Motivation

The future impact of Quantum computing was made apparent by the popularization of the Shors algorithms. The emergence of an algorithm that can break most web security poses a major risk to the internet. With the field merging with other technologies like mobile networks and the production of simulators that make it easier to interact with quantum computers, it is much easier to explore the subject.

Along with the risks that present themselves are also solutions that provide perfectly secure cryptosystems with further research. Some form of Quantum cryptography algorithms might be the future of cryptography itself. A proper analysis of the cryptosystem will identify any problems that may have been overlooked. It also increases the understanding of the inner workings of the cryptosystem.

c) Project Aims

This project aims to implement and analyse the BB84 and E91 Quantum cryptographic algorithms. Certain aspects that will be analysed are Time Usage, Memory usage, Security, Attacks and comparison with classical algorithms like RSA and Elliptic Curve Diffie Helman. Other aspects of Quantum cryptography, such as the theorems surrounding security. Concepts such as Quantum teleportation and Shor’s Algorithm will also be briefly explored. The data will be presented in a visual format and conclusions are to be drawn from it.

d) Objectives

To understand and verify the security measures implemented in quantum cryptosystems. Find any aspects that might reduce trust in these algorithms, while discovering how a boom in quantum technology might affect classical cryptosystems and the Web. To determine the viability of quantum cryptosystems as a replacement for current technology.

c) Problems Faced

Quantum computing being a relatively recent technology is fraught with unique challenges. Quantum computing hardware is difficult to attain. IBM offers remote execution of instructions on their quantum computer but, it is on a token basis and therefore allows very few runs. This makes it difficult to obtain a large data set for the analysis of parameters. Thereby requiring the use of simulators. These however require large amounts of computational power which scales with the number of qubits used and certain operations such as Quantum entanglement.

1.2 Foundations of Quantum Computation

a) Theorems and Principles

Heisenberg Uncertainty Principle

The principle states that, out of a pair of properties, it is impossible to know both with complete certainty. Measurement of a simple property will effectively change the other to some random value[23].

Non-Orthogonal States cannot be distinguished perfectly

A property of quantum mechanical double state system that describes that the states do not necessarily have to be either $|1\rangle$ or $|0\rangle$. It is in a superposition of $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

where $|\alpha|^2 + |\beta|^2 = 1$.

The laws of quantum mechanics ensure that it is impossible to distinguish between 2 unmeasured states [14]

$$|\phi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$$

$$|\phi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$$

Unless States $|\phi_1\rangle$ and $|\phi_2\rangle$ are mutually orthogonal.

Theorem-1: No-Cloning Theorem

The theorem states that it is nigh impossible to replicate an unknown state. Let us consider unknown Quantum states |ϕ> and |***Ψ***>. Let these be orthogonal bases, thereby they cannot be properly distinguished by any measurement. This also means that there will always be some probability of an error occurring. However if it was possible to make multiple copies of the unknown state then the probability of error could be made smaller and almost negligible. This is prevented by the no cloning theorem, single unitary operators can only copy mutually orthogonal states. To understand this further, let us assume the existence of an unitary operator that can copy unknown quantum states U [22].

$$|\varphi\rangle \otimes |0\rangle \, Ucl - \rightarrow |\varphi\rangle \otimes |\varphi\rangle.$$

$$|\psi\rangle \otimes |0\rangle \, Ucl - \rightarrow |\psi\rangle \otimes |\psi\rangle$$

This means that <φ | ψ > can be 0 or 1

$$|\varphi\rangle|0\rangle U - \rightarrow |\varphi\rangle|\varphi\rangle = (a|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

$$.=\alpha^2|00\rangle+\beta\alpha|10\rangle+\alpha\beta|01\rangle+\beta^2|11\rangle$$

Using the simple algebraic expression of $(a+b)(a+b)=a^2+ab+ba+b^2$.

We can then try to use U to further clone the expansion of $|\varphi\rangle$.

$$(\alpha|0\rangle+\beta|1\rangle)|0\rangle\xrightarrow{U}\alpha|00\rangle+\beta|11\rangle$$

When cloning we end up with a whole different state. No cross terms exist here and thereby we end up with a contradiction [14]. A single unitary operator that can clone an unknown state can therefore not exist. Cross terms refer to the x and y terms in $(x+y)(x+y)$. It is however entirely possible to clone a known state such as $|0\rangle$ or $|1\rangle$.

Theorem 2: Local Hidden variable Theory

The local hidden variable theory developed to explain quantum correlations states that $|C|\leqslant 2$. A local hidden variable theory is defined as a proposal to provide an explanation for a quantum mechanical phenomenon through use of hypothetical entities that is consistent with local realism, i.e. it can only be influenced by objects in its locality. Bell's Theorem however states that “no physical theory of local hidden variables can ever reproduce all the predictions of quantum mechanics.”[8]

Quantum Teleportation

Quantum particles can entangle with each other regardless of the physical distance between them. Entanglement means that, when a property has been measured in one of the entangled particles, a correlated property will change in the others [Upon inducing a change in one of the entangled particles, The second particle will explicably change regardless of distance from its counterpart [4].

Let us consider a 2-qubit register in the state of $\langle|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}$. The system is in the state

$$\frac{1}{\sqrt{(2)}}\langle a|0\rangle(|00|+|11|)+\langle a|0\rangle(|00|+|11|)=\frac{1}{\sqrt{(2)}}\begin{bmatrix}a\\0\\0\\a\\b\\0\\0\\b\end{bmatrix}$$

To move further, the CNOT operation needs to be performed on the quantum state.

Upon performing the operation, the state changes to,

$$\frac{1}{\sqrt{(2)}}\langle a|0\rangle(|00|+|11|)+\langle a|0\rangle(|10|+|01|)=\frac{1}{\sqrt{(2)}}\begin{bmatrix}a\\0\\0\\a\\0\\b\\b\\0\end{bmatrix}$$

The Hadamard (H) gate is then applied to the state, allowing for the superposition of $|0\rangle$ and $|1\rangle$. Given a matrix

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \quad (1)$$

H is then applied into the previous system to obtain

At the point the Qubits can be visualized on a Bloch sphere as shown below

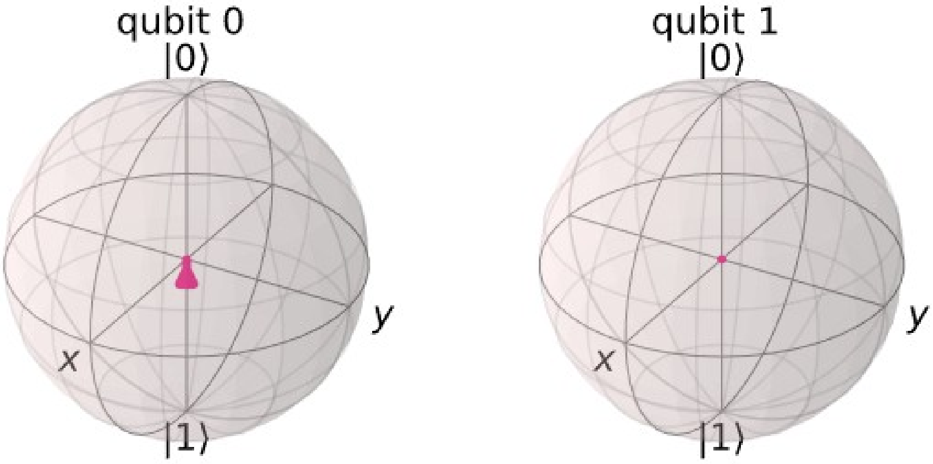


Figure 1: Qubits in entangled states after H-Gate applied (Generated by Qiskit)

$$|\varphi\rangle=\frac{1}{\sqrt{(2)}}[\frac{1}{\sqrt{(2)}}a(|0\rangle+|1\rangle)(|00\rangle+|11\rangle)+\frac{1}{\sqrt{(2)}}a(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)]=\frac{1}{\sqrt{(2)}}\begin{bmatrix}a\\a\\b\\b\\a\\-b\\-b\\a\end{bmatrix}$$

This Equation can be rewritten as

$$\begin{bmatrix} \begin{bmatrix} a \\ a \end{bmatrix} \\ \begin{bmatrix} b \\ b \end{bmatrix} \\ \begin{bmatrix} a \\ -b \end{bmatrix} \\ \begin{bmatrix} -b \\ a \end{bmatrix} \end{bmatrix} = \frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle + b|1\rangle) + |11\rangle(a|1\rangle + b|0\rangle)]$$

This can be simplified into

$$\frac{1}{2}\left[|00\rangle\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}|\psi\rangle + |01\rangle\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}|\psi\rangle + |10\rangle\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}|\psi\rangle + |11\rangle i\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}|\psi\rangle\right]$$

It can be observed that the matrices are Pauli spin matrices, upon substituting the matrices with their respective operators I, X, Y, Z :

$$\frac{1}{2}[|00\rangle I|\psi\rangle + |01\rangle X|\psi\rangle + |10\rangle Z|\psi\rangle + |11\rangle iY|\psi\rangle]$$

$$|\varphi\rangle = \frac{1}{2}[|00\rangle I|\psi\rangle + |01\rangle X|\psi\rangle + |10\rangle Z|\psi\rangle + |11\rangle XY|\psi\rangle]$$

Upon measuring the first and second qubit, two classical bits are obtained. These bits can be used to identify the transformation applied to the third bit. This is possible since the 2-qubit states of Qubit 1 and 2 differs each term.

The third qubit can be fixed by either applying X, Z, Both X and Z or Neither. Using electrons A and B as an example, Their state is prepared such that they are considered a single entity unable to be separated. One of these is a singlet state

$$|\psi_S\rangle = \frac{1}{\sqrt{(2)}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) = \frac{1}{\sqrt{(2)}}(|01\rangle - |10\rangle)$$

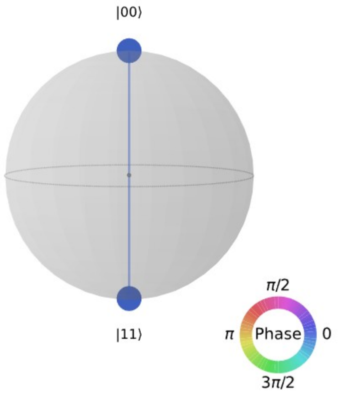


Figure 2: Depiction of State Vector for entangled Qubit (Generated by Qiskit)

The State vector can be visualized as above:

$|0\rangle$ and $|1\rangle$ are used to denote the state along with the spin of the electron, along the +ve or -ve direction of the z-axis. The projection onto the direction $\vec{n}=(n_x, n_y, n_z)$ denoted by

$$\vec{n}.\vec{\sigma}=n_x X+n_y Y+n_z Z$$

$\sigma=(X, Y, Z)$ X,Y,Z being the Pauli matrices. For the qubits A and B, it can be observed that $(\vec{a}.\vec{\sigma})_A \otimes (\vec{b}.\vec{\sigma})_B$ describes the combined measurement of their respective spin projections onto directions $\vec{a}$ and $\vec{b}$. This can be simplified to obtain $\langle(\vec{a}.\vec{\sigma})_A \otimes (\vec{b}.\vec{\sigma})_B\rangle \psi_s=-\vec{a}.\vec{b}$ (2)

CHSH Inequality

Upon measuring the Pauli observables X and Z for some qubit A and $W=\frac{1}{\sqrt{(2)}}(X+Z)$ and $V=\frac{1}{\sqrt{(2)}}(-X+Z)$ for qubit B. Combined measurements of these observables, gives

$$\langle X \otimes W\rangle_{\psi_s}=-\frac{1}{\sqrt{(2)}}, \langle X \otimes V\rangle_{\psi_s}=\frac{1}{\sqrt{(2)}}$$

$$\langle Z \otimes W\rangle_{\psi_s}=-\frac{1}{\sqrt{(2)}}, \langle Z \otimes V\rangle_{\psi_s}=-\frac{1}{\sqrt{(2)}}$$

These values can be used to obtain the *Clauser-Horne-Shimony-Holt (CHSH) correlation value* © *[8]*, which is written as:

$$C=\langle X \otimes W\rangle-\langle X \otimes V\rangle-\langle Z \otimes W\rangle-\langle Z \otimes V\rangle=-2\sqrt{2}$$

It can be noted that $C=-2\sqrt{2}$ which does not satisfy $|C| \leqslant 2$. This provides a generalized form of Bells inequality.

The benefit of the CHSH correlation value will be discussed in the observations in further detail.

Eigenstates

The properties of vectors dictate that new vector results from the multiplication of a Matrix and a vector. Given *M* is a matrix and $|v\rangle$ is the vector.

$$M|v\rangle=|v'\rangle$$

For certain vectors and matrices, multiplication by a vector is the same as performing multiplication with a scalar. $M|v\rangle=\lambda|v\rangle$ (Where λ is a scalar). These states are known as Eigenvectors of the Matrix. The eigenvectors of the *Z* Pauli matrix are $|0\rangle$ and $|1\rangle$ [10], Thereby

$$Z|0\rangle=|0\rangle$$

$$Z|1\rangle=-|1\rangle$$

These are often called eigenstates, since the vectors represent quantum states. Similarly, the eigenstates of the X gate are called $|+\rangle$ and $|-\rangle$ such that

$$|+\rangle=\frac{1}{\sqrt{(2)}}(|0\rangle+|1\rangle)=\frac{1}{\sqrt{(2)}}\begin{bmatrix}1\\1\end{bmatrix}$$

$$|-\rangle=\frac{1}{\sqrt{(2)}}(|0\rangle-|1\rangle)=\frac{1}{\sqrt{(2)}}\begin{bmatrix}1\\-1\end{bmatrix}$$

These are relevant in the Quantum entanglement section since they are outputs of the Hadamard gate. (Equation 1)

Orthonormal Basis

Two vectors are called orthonormal if they are both orthogonal and normalized. Orthogonal vectors are at right angles. The Normalized term refers to their magnitudes being 1. Upon considering that the vectors $|0\rangle$ and $|1\rangle$ are Orthonormal vectors. The vectors $|0\rangle$, $|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle$ are linearly independent. That means that it is not possible to describe in terms of. Due to this fact, the vectors and $|1\rangle$ can be used to generate any vector in 2D space. Thereby the vectors and form a basis called the orthonormal basis [18].

Bayes's theorem

The Bayes theorem is used to determine conditional probability. Created by the mathematician Thomas Bayes. Conditional probability can be defined as the probability of an event occurring given that a prior event has occurred in a similar environment. The theorem states that the conditional property of an event based on another event is equal to the probability of the second event. The probability of the occurrence of the prior event is called a prior probability whereas the current event being measured for is known as the posterior probability. The Posterior probability of calculated by taking some new data into account and thereby is used to provide a better value than the prior calculation [2]. The theorem is given as

$$P(A|B)=\frac{P(A\,intersect\,B)}{p(B)}=\frac{P(A).P(B|A)}{P(B)}$$

Probabilities of the occurrence of event A and event B are defined as P(A) and P(B). P(A|B) is the probability of occurrence of A given B occurs. P(B|A) is vice-versa. P(A intersect B) is the probability of both occurring.

Quantum Fourier transform

Upon inputting a single number into the QFT, it outputs a superposition of all other numbers weighted by certain amounts. The weights form a rough sin wave upon being plotted, the frequency of said sin wave corresponds to the number inputted. Larger numbers will result in a higher frequency sin wave. However, Upon providing the QFT with a superposition of numbers, it outputs a superposition of superposition's. The sin waves of said superposition's can either Constructively or destructively interfere [22].

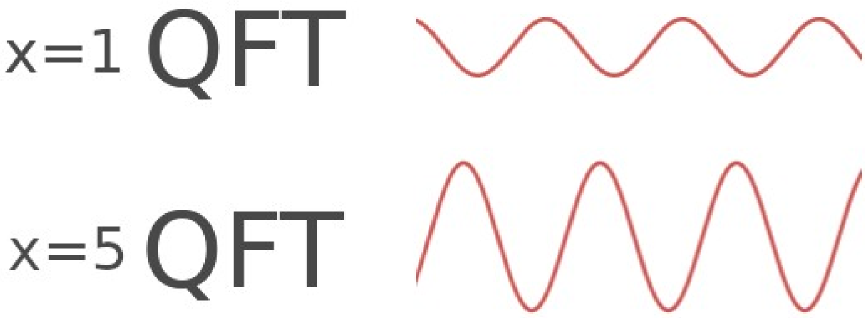


Figure 3: Quantum fourier transform on simple numbers

b) Quantum Computing Basics

Classical computing and Quantum computing run on totally different rules and thereby require different building blocks. This section intends to provide an overview of fundamental concepts such as gates, Spaces and Qubits. The basis of classical computers at the lowest level relies upon Transistors, which rely on the properties of semiconductors. Semiconductors, however, require the understanding of Quantum computing to explain. There is simply no explanation based on classical physics that can explain its working. Thereby, classical computers themselves are in some form quantum mechanical. However, they cannot utilize some of the key Features of quantum computing. A classical bit needs to be in either a state of 1 or 0, whereas a qubit is in both those states at the same time. This is called a superposition and forms the basis for quantum computing.

Let's consider a qubit that always outputs a 0 such that $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$ (3) and a corresponding qubit that always measures into a 1 $|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$ (4).

Each Qubit is denoted using $|$ and $\rangle$. This is referred to as the bra-ket notation, it is used since each qubit is considered to be a vector. The bra section of the notation refers to the row vectors, and the column vectors are named kets. A complete bra-ket vector is written as $\langle a|a\rangle$ As can be seen in the above examples, each vector is equivalent to some matrix space that consists of states that it can be in [21].

Thereby for two bits, there are 4 states i.e. it is in a superposition such that

$$|\psi\rangle=a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle$$

Suppose that $a=d=0$ and $b=c=1/\sqrt{(2)}$, this is Einsteins-podolski-Rosen state(EPR)[5]

The EPR state forms the basis for the E91 Cryptographic algorithm, described in further detail below. It also violates the Bell inequality theorem. This property and a few others differentiate quantum mechanics from classical physics, as the fundamental laws of physics do not seem to apply to it. Classical computers use logic gates as the basis for all logical and mathematical operations. All classical gates other than the NOT gate are irreversible. Any operation can be defined as a series of gates. These cannot be used in Quantum mechanics as they are, therefore some of the base gates are modified to fit into quantum computing.

The Bloch Sphere

As seen above, the state of a qubit ($|q\rangle$) can be defined as $|q\rangle=\alpha|0\rangle+\beta|1\rangle$

Wherein α and β are complex numbers. Upon confining these to real numbers and introducing n additional variable to measure the phase difference between the two states ($e^{i\phi}$). The state definition changes to

$|q\rangle=\alpha|0\rangle+e^{i\phi}\beta|1\rangle$ (5)

The State then needs to be normalized to increase the probability of obtaining the proper measurement. It is performed as shown below

$\sqrt{(\alpha^2+\beta^2)}=1$

Given the fact that $\sqrt{(\sin^2 x+\cos^2 x)}=1$, the complex numbers α and β can be describes as

$\alpha=\cos\frac{\theta}{2},\beta=\sin\frac{\theta}{2}$ Therefore, all qubits having the variables θ and ϕ conform to the below equation[21[

$|q\rangle=\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta}{2}|1\rangle$

The variables θ and ϕ can be used to plot the Bloch sphere for a given qubit. The Bloch sphere is a graphical representation of the complex state vector of a qubit. Upon using the variables as spherical coordinates, it is possible to plot a single qubit onto the surface of a sphere. An example of the same can be seen below

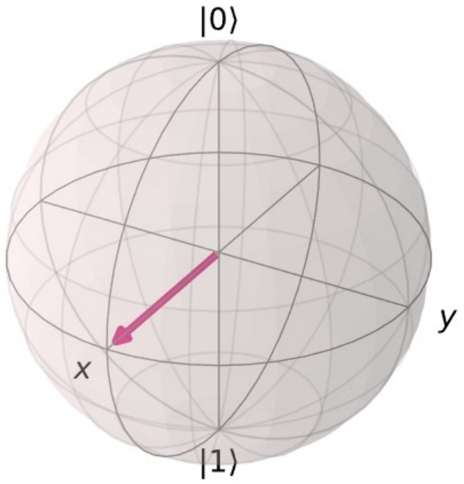


Figure 4: Bloch sphere for undecided Qubit

Hilbert's Spaces

A Hilbert Space provides a method for the description of concepts, processes and laws of a quantum mechanical system. The Pure states can be considered as vectors of the Hilbert space of the system the Hilbert space belongs to. The use of these spaces to formulate quantum mechanics was one of the major milestones of Quantum computing.

Let $l_2(D)$ be the Hilbert space for a finite countable set *D*.

$$l_2(D)=\{x \vee x: D \rightarrow C_1 \left(\sum_{e \in D} x(i) x^*(i) \right)^{\frac{1}{2}} < \infty \}$$

To define the Hilbert space in terms of the inner product we can state that

$$\langle x_1 | x_2 \rangle = \sum_{e \in D} x^*{}_1(i) x_2(i)$$

The Elements belonging to a Hilbert space are vectors.

There is a more prominent definition of a Hilbert space that states that an inner product space of *H* is made up of complex vectors with an inner product ($\langle | \rangle$) $H \times H \rightarrow C$. These must satisfy the following conditions, $\forall$ vectors $\phi, \psi, \phi_1, \phi_2 \in H$ and $\forall c_1, c_2 \in C$.

$$\langle \phi | \psi \rangle = \langle \psi | \phi \rangle^*$$

$\langle \psi | \psi \rangle = 0$ and $\langle \psi | \psi \rangle = 0$ if and only if $\psi = 0$

$$\langle \psi | c_1 \phi_1 + c_2 \phi_2 \rangle = c_1 \langle \psi | \phi_1 \rangle + c_2 \langle \psi | \phi_2 \rangle$$

The inner product also adds onto *H* the norm such that

$$|| \psi || = \sqrt{(\langle \psi | \psi \rangle)}$$

These unit vectors of the norm are called Pure states of the inner product Space *H*. A complete inner product space is then called a Hilbert space. A complete inner product space is one that has an element ϕ such that $\lim_{i \rightarrow \infty} || \phi - \phi_i || = 0$ with properties $\lim_{i,j \rightarrow \infty} || \phi_i - \phi_j || = 0$.

Quantum Gates

The base gates NOT, AND, XOR can be used to make any complex gates. These gates have their correspondents in the quantum system.

The equivalent to the classical XOR gate is the CNOT gate (Also known as the Controlled NOT gate). Its logic table is the same as a classical XOR, gate and can be drawn as

Table 1: CNOT gate Truth Table

Control(A)	Target(B)	Result	
0	0	0	0
1	0	1	1
0	1	0	1
1	1	1	0

Unlike irreversible gates, their counterparts require a control bit and a target bit. The target bit has a different operation performed on it based on the state of the control bit. The CNOT gate works similarly to an XOR gate. It checks whether the bits are different and returns a 1 if they are. Consequently, it returns a 0 if they aren't.[21]

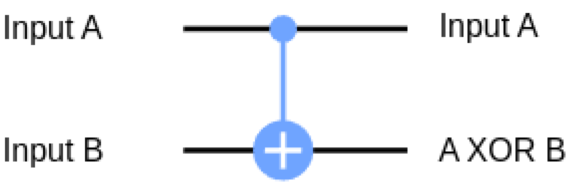


Figure 5: CNOT Gate Circuit

A simpler explanation for the Control and target bit functioning is that a NOT is performed on the target bit when the control bit is 1. The control bit thereby acts as a switch.

The Quantum teleportation theorem describes Pauli matrices. Each of the Pauli matrices corresponds to a single qubit gate. The CNOT gate however is a multi-Qubit Gate. Given below are some Single qubit gates.

X-Gate

Corresponding to the Pauli Matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$. The qubit is changed by multiplying its state vector with the X Pauli Matrix [6]. Such that

$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$ as given in **(4)(3)**

Upon plotting the state of a vector that has the X gate applied to it the following Bloch sphere is obtained

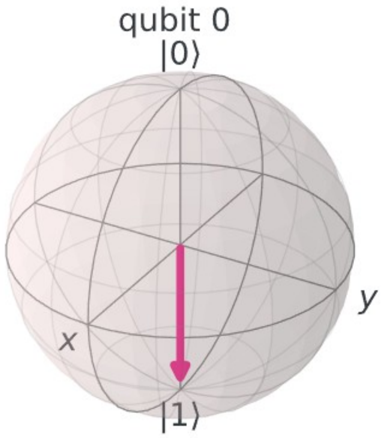


Figure 6: Bloch Sphere depicting Qubit in State |1>

The figure depicts that the qubit is in state $|1\rangle$ as can be seen from the previous equation. Due to its properties the X gate is usually called the NOT gate since it performs a similar function.

Y and Z Gates

Unsurprisingly, the Y and Z gates operate similarly to the above. They each refer to the matrices

$$Y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}=-i|0\rangle\langle 1|+i|1\rangle\langle 0|$$

$$Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=|0\rangle\langle 0|+|1\rangle\langle 1|$$

They are applied to the Qubit in the same method as the X gate by using Matrix multiplication [6].

The Hadamard Gate

The H gate is used for the production of superpositions of States. Therefore is classified as a fundamental gate for quantum computing. It is fundamental to the E91 Cryptographic algorithm. It has the matrix

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$\langle H|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}=|+\rangle$$ From **Eigenvectors**

$$\langle H|1\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix}=|-\rangle$$ From **Eigenvectors**

The concept of Quantum entanglement and how the Hadamard gate plays a part of explained in detail in the Quantum teleportation Section. The H gate also helps to connect the different Pauli gates. Suppose some superposition needs to be measured on the X basis, but the system is only capable of measuring on the Z basis. Upon sandwiching the Z gate between 2 H gates it functions similar to an X gate. Measuring on the Z basis removes all certainty of measuring the same on the X basis [21].

The P-Gate

The Phase Gate takes a parameter ϕ that changes its working. The param ϕ needs to be a real number, and the gate can be written as the Matrix

$$P(\phi)=\begin{bmatrix}1 & 0\\ 0 & e^{i\phi}\end{bmatrix}$$

The $e^{i\phi}$ can be recognized from an earlier definition **(5)** wherein it is introduced to find the difference between the phases of 2 states of a qubit. The Gate performs a rotation of ϕ in the Z direction [6]. The Z-Gate can also be defined as a special variant of the P-Gate with a $\phi=\pi$, similarly there are Three other variants. Two of these are discussed below as they are relevant to the later section.

The S-Gates

The S gate is a variant of the P-gate with a $\phi=\pi/2$, Sometimes called the $\sqrt{(Z)}$ gate. It performs a quarter turn around the Bloch sphere. It differs from every gate before it since it is not its own inverse. Thereby the matrix of the S gate is

$$S=\begin{bmatrix}1 & 0\\0 & e^{\frac{i\pi}{2}}\end{bmatrix}$$

$$S'=\begin{bmatrix}1 & 0\\0 & e^{-\frac{i\pi}{2}}\end{bmatrix}$$

The name $\sqrt{(Z)}$ gate is used since two S gates in series function the same as a Z gate (Since the Z gate is a P gate with $\phi=\pi$ whereas the S gate has a $\phi=\pi/2$)

The T-Gate

The T-Gate is a P-Gate with a $\phi=\pi/4$, thereby it follows a similar thread as the S-Gate. Therefore four T-Gates in succession Equate to 1 Z gate and two Equate to an S-Gate. Similar to the gate it is not the inverse of itself. It differs such that the phase difference is $e^{\frac{i\pi}{4}}$ [6]. Therefore the Matrix is written as

$$T=\begin{bmatrix}1 & 0\\0 & e^{\frac{i\pi}{4}}\end{bmatrix}$$

$$T'=\begin{bmatrix}1 & 0\\0 & e^{-\frac{i\pi}{4}}\end{bmatrix}$$

Some gates are not discussed as they are irrelevant to the project. These consist of the I-gate which is an identity matrix and therefore does nothing. It is only used for proofs of inverse. The U-Gate that is a highly generalized gate that takes in parameters θ , ϕ and λ [6]. It can be moulded into a P-gate or H-gate based on the parameters given. Thereby the U-gate can give rise to a near infinite number of gates.

1.3 Background Research

a) Quantum Cryptography

A major problem with Symmetric key cryptography is that the initial key exchange between parties is difficult to achieve securely. The go-to method for the former is to transport the keys via a previously authenticated channel, the problem lies therein that the security is now fully dependent on the encryption applied to the channel. This can be overcome by the use of non-Symmetric keys, this method however requires the existence of a trusted third party. The major problem with public key algorithms is that they rely on mathematically difficult problems for their security, which in turn means that these algorithms are susceptible to cryptanalysis attacks from a quantum computer running Shor's algorithm. The problems in this method become evident, a break in the algorithm at a lower level compromises every higher level as well. As a solution to this problem, Quantum Key Distribution algorithms were introduced which allowed for secure transfer of Symmetric keys between parties without possibility of a proper breach. The former method used for secret key sharing over an unsecure channel was the Diffie-Hellman key exchange. The algorithm however was found to be insecure when matched against an adequate adversary. This led to the adoption of RSA as the new standard in communications across hosts. RSA itself is prone to a number of attacks, disregarding factoring of the primes that make up the algorithm. An efficient path of attack other than the Shor's algorithm has yet to be found, most attacks abuse bad parameters and system restrictions to break the encryption. Data encrypted by RSA can be decrypted by multiple keys if the primes used are not strong, i.e. $\frac{(p-1)}{2}$ and $\frac{(q-1)}{2}$ are primes; these numbers get scarcer as the number of digits increases.

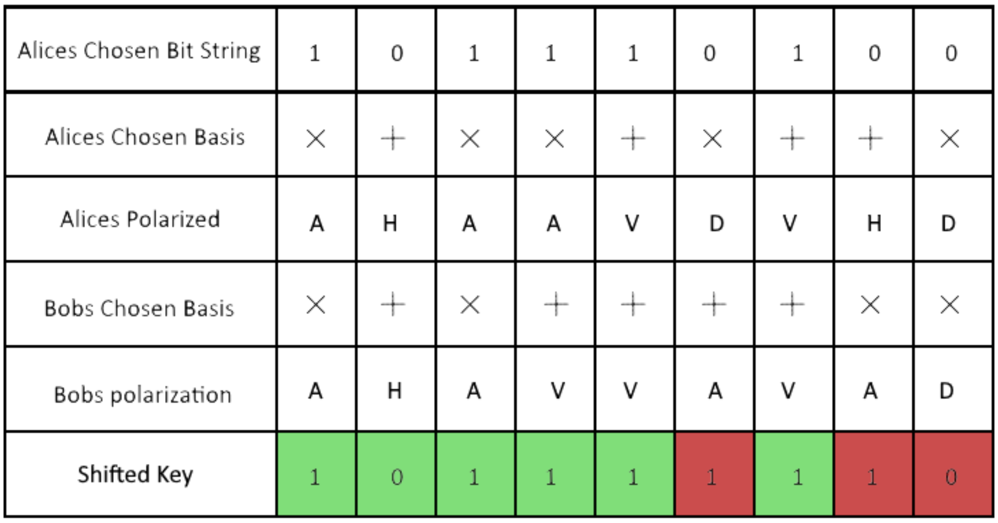
b) BB84(Bennet and Brassard 1984) Protocol

BB84 is one of the earliest Quantum key distribution protocols to be widely publicized. Named after its creators Bennet and Brassard. While classical cryptography algorithms rely upon mathematically difficult problems for their security, Quantum algorithms rely on the laws of quantum mechanics that are built into reality itself. Consequently, The security for BB84 relies upon the Heisenberg Uncertainty principle (Theorem 1), It states that determining both the speed and position of a particle at the same time is impossible. As one value begins to get clearer, the other becomes more obscure, this works both ways. Thereby, we cannot gain a single value, we do however obtain a wave function that represents the probabilities of where we would find the particle and its speed. The BB84 protocol uses a photon for the transmission of a secret key from one party to another(Alice and Bob) and the No-cloning theorem protects said secret key from replication by a third party(Eve).

The no-cloning theorem simply states that it is impossible to replicate an unknown state that has yet to be measured(Theorem 3).

The theorem relies upon the fact that all operations done on a quantum state need to be unitary linear transformation. Any attempt towards the measurement of the secret key will disturb the system and Bob will be alerted. This works perfectly given that the track is not prone to errors, this is usually not the case since the transmission of photons requires a medium such as optical fibre. Since direct line of sight limits the range of the technology, it would be much better to consider the use of optical fibre mediums as the default. Errors in the track will increase the chances of Eve staying undetected, this is caused by a concept called noise in quantum mechanics. Noise, as the word implies, stands for disturbances in the system that can muddle the final measurement of the state and throw the values into disarray, however this is also the reason Eve cannot possibly intercept the key.

The BB84 protocol uses photons (Particles/Waves that represent light) as qubits, the implementation depends on the polarization property of the photons. Polarization oscillates the light wave on a single plane when it passes through a polarizing material. Linear polarization is used as the standard method, allowing for 4 states for each photon. These states can be defined as Horizontal $(|H\rangle)$, Vertical $(\,|\,V\rangle)$, Diagonal $(\,|\,D\rangle)$ and Anti-diagonal $(\,|\,A\rangle)$. Observations will be made on the X and Z axis. 0°, 45° are set as binary 0 and 90°, 135° are set as binary 1. The actual communication will be performed over two separate channels, A quantum channel and a classical channel. The Quantum channel is meant to be a private channel and the other will act as a public channel. The opening steps will be performed on the Quantum channel. Alice will go on to randomly select two bit strings of equal length ($X=x_0,x_1,x_2....,x_n$ and $Y=y_0,y_1,y_2....,y_n$, $X_i,Y_i\in\{1,0\}$), X is the Bit string Alice wishes to send over to Bob and Y will act as the Basis that will encode the corresponding bit. Alice will then prepare n qubits, such that $|\psi_{x1y1}\rangle,|\psi_{x2y2}\rangle...|\psi_{xnyn}\rangle$ She will then send these qubits as a set of photons, one at a time polarized in their corresponding bases, by passing them through a polarization filter to Bob. Considering that there is no noise or eavesdropping Bob will receive the exact sequence $|\psi_{x1y1}\rangle,|\psi_{x2y2}\rangle...|\psi_{xnyn}\rangle$ from Alice [8]. Bob will then generate a randomly uniform string of the m , this string will act as Bobs guess of the Basis chosen by Alice Y' . Measurement with the proper basis i.e. $y_i'=y_i$ then $x_i'=x_i$ (Bob obtains the same bit sent by Alice),in the other case however i.e. $y_i'\neq y_i$, x_i' will have no correspondence to x_i (x_i' will be completely random). Bob will then use a public channel to communicate the bases $(Y^{'})$ used to Alice. Alice will then compare against Y and reply with the bases that Bob chose correctly. The strings $X^{'}$ and X are not revealed. Both will then go on to discard $\forall x_i \, where \, y_i^{'} \neq y_i$ and the remaining bit strings i.e. $\tilde{X}$ and $\tilde{X}^{'}$ will be similar for both. $\tilde{X}$ will then act as a shared secret key.



Alices Chosen Bit String	1	0	1	1	1	0	1	0	0
Alices Chosen Basis	×	+	×	×	+	×	+	+	×
Alices Polarized	A	H	A	A	V	D	V	H	D
Bobs Chosen Basis	×	+	×	+	+	+	+	×	×
Bobs polarization	A	H	A	V	V	A	V	A	D
Shifted Key	1	0	1	1	1	1	1	1	0

Figure 7: Comparison Table for Alice and Bob

In a real situation there will always be some noise in the system and there is a need to identify the presence of an attacker (Eve). Bob and Alice will proceed to calculate the Bit Error Rate, i.e. find the percentage of bits in $\tilde{X}$ that do not match $\tilde{X}^{'}$ [18]. They will publicly forward a set of bits from the shifted key, since it is a shared key it is expected to be similar on both sides. These bits are then discarded from both secret keys, the remaining bits are expected to have a proportional error rate as those checked. Next, the error rates need to be reduced, this can be done at the cost of a few more bits from the secret key, given that the error rate is not exceptional high. Using the Bit error rate estimation, Alice and Bob can guess the amount of information Eve might have obtained from their transaction. Quantum mechanics dictates that changes in the state is directly related to the amount of information obtained, Using this principle we can link the bit error rate to the information that Eve might potentially know. The honest parties can then use privacy-amplification methods from classical cryptography to replace their strings with shorter strings that Eve has no knowledge of. Another method Eve might use to listen in on this conversation is the general coherent attack [14], Where in Eve builds a whole Quantum system E of her own and allows for the unitary interaction between the qubits sent by Alice and system E. Finally E will be measured to try and obtain some bits, this can be postponed till after the agreement of the secret key over the public channel. Privacy Amplification techniques still provide sufficient security against this or any other attack that is within the laws of physics.

In a case where the presence of Eve is identified, the procedure needs to be repeated using a different quantum channel. There is however a rather miniscule chance that Eve can stay hidden throughout the procedure. Eve has no knowledge whatsoever regarding the bases used by Alice and therefore is forced to guess. If she manages to guess the correct base then no information is lost, in the other case however all information from the unchosen bases will be irreversibly lost. Thereby if n-bits are being used then Eve has $n^{\frac{3}{4}}$ chances to escape undetected [14]. Therefore, the security is higher when using a larger number of bits. Alice and Bob will use the secret key as a One time pad and use it to encrypt their messages. As stated by the Information Theory, a protocol that uses One time pad and does not reuse a secret key for message encryption cannot be possibly broken by an attacker. Thereby, in theory BB84 is Uncrackable.. One of the principles governing the security of BB84 is The No-Cloning theorem.

c) Eckert 1991 (E91) Protocol

E91 or Eckert91 named after its creator Artur Eckert and the year it was created, 1991 respectively. The main security feature in the protocol is the entanglement property of quantum particles and the Bell theorem, which in simple terms allow for the teleportation of information over seemingly infinite distance.

$$\langle(\vec{a}.\vec{\sigma})_A \otimes (\vec{b}.\vec{\sigma})_B\rangle \, \psi_s = -\vec{a}.\vec{b} \quad \underline{(2)}$$

Given the above equation that is a simplified version of the equation for the states of entangled qubits A and B. Give that Both Are measured using the same spin projection both A and B will result in opposite bits [20].

E91 Procedure

Given particles A and B in a superposition. Albeit it is know that one particle is spinning up and the other down, it is impossible to determine which is which until measurement. Alice and Bob need to choose one of three coplanar axis to measure the incoming particles. Pairs of spin 1/2 particles are emitted in singlet states in the form $\phi=\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle+|\downarrow\uparrow\rangle)$. The aforementioned bases can be defined by writing the vectors for Alice and Bob respectively $a_i(i=1,2,3)$ and $b_j(j=1,2,3)$. In the case the particles travel along the z direction, a_i and b_j are located on the x-y plane, perpendicular to the particle trajectory. Using the vertical x-axis to measure the angles, a_i and b_j are described by $\phi_1^a=0^\circ$, $\phi_2^a=45^\circ$, $\phi_3^a=90^\circ$ and $\phi_1^b=45^\circ$, $\phi_2^b=90^\circ$ and $\phi_3^b=135^\circ$.

It can be noticed that Alice and Bob have a 1/3 chance of randomly choosing a compatible basis to measure the particle. In the case that a compatible base is chosen, If Alice measures a Spin up particle, the quantum system collapses into the first state from ϕ . Thereby, Bob will inevitably measure a spin down particle (Due to the particles being entangled).

In the latter case wherein incompatible bases are chosen, Given that Alice measures first. Bobs measurement will be totally random. e.g. If Alice measures using 45° basis, Bob can either measure a spin-up or spin-down particle with equal probability in the 90° basis. This serves to imply that the particle measured by Bob somehow knows that its counterpart(Alice’s particle) has been measured, and fixes its orientation accordingly. This phenomena defies the classical rules of locality and realism. Since this can occur over any distance the information is propagated faster than the speed of light, thereby contradicting the theory that c is the universal speed limit.

To further refine the key, the imcompatible bases need to be discarded. To do so they need to announce the bases they used to each other over a public channel. They can then discard any incompatible bases while keeping the actual key a secret. This process reduced the key size by roughly 30% of its orignal size. The obtained key with the sin-up and spin-down states can be replaced with the bits 1 and 0 respectively, leaving Alice and Bob with a shared secret key.

Since the system collapses into either state after a measurement has been made, trying to gain any information prior to this is impossible, as it simply does not exist. Eve can be identified in a similar method to BB48. When Alice and Bob choose a compatible basis, if Alice measures a spin-up particle Bob should expect a Spin-down particle, if any discrepancy is observed it can be concluded that either Eve has interfered or Noise exists in the quantum channel.

For Eve to effectively eavesdrop on the channel she needs to measure the particle using a random basis, effectively destroying it in the process. She will proceed to send to recreate the particle and send it to Bob. The orientation of the particle Bob receives will be totally random due to Eves intervention. If the Spin Bob observes does not correlate to Alice's measurement then Bob knows an error has occurred. Unlike BB84 the E91 protocol makes use of 6 states, The additional 2 states are used to detect an eavesdropper without announcing any information about the key, like in BB84.

Looking back at the Correlation coefficient it was proved that $S \leqslant 2$. Quantum mechanics however contradicts this with $S=2\sqrt{2}$. By publicly announcing the values

Alice and Bob measured with an incompatible basis a value for S can be calculated. If there was no disturbance in the channel then the calculated value should be $2\sqrt{2}$. If the value of S is proper then Alice and Bob conclude that their values are anti-correlated and their shared key is secure [13]. S However will rarely be exactly the same as $2\sqrt{2}$, due to noise in the channel which will sway the value, but this will be slight.

Error correction will then be performed over a public channel in a similar way to BB84. Upon comparison of the shared secret key, a QBER(Quantum Bit Error Rate) value can be obtained. A QBER of 15% is a safe bet that an eavesdropper [14] is present in the system. Since all this occurs over a public channel some information about the key might get leaked. Thereby privacy amplification is applied to increase security of the key.

d) Privacy Amplification

The idea was introduced by the founders of BB84 algorithm, and is applied to E91 as well. Alice will proceed to choose a random pair of bits and compute their XOR value. Alice will announce which bits were chosen, but not what the computed XOR was. Bob will then find said bits in his secret Key, Both Alice and Bob will replace the bits with their XOR value. Alice and Bob will proceed to XOR sections of their shared key, making the key shorter in the process [14].

If Eve wishes to know a value in the final key, then she would need to have knowledge of both Alice's and Bob Key before the XOR Operations were performed.

e) Shors Algorithm

Shor’s Algorithm is the main reason quantum computing is considered a threat to modern cryptography algorithms. In essence, it is an algorithm for factoring integers that leverages the properties of quantum physics. The best prime factorization algorithm that can run on classical computers is called The number field sieve algorithm, it is however inefficient when it comes to factoring large numbers such as those used in RSA. These methods effectively guess the factors of a number and check whether their product equals the number in question, this process is repeated till the proper numbers are found. In 2009, researchers spent an equivalent of 2000 years of computational power on a 2.2Ghz processor with 2GB or RAM, to factor a 768 bit(232 digit decimal) Coprime number.

Shor’s algorithm can factor an integer in polynomial time. Factorization of a Number N would require $2+\frac{3}{2}\log_2 N$ qubits to perform the operation.

In brief terms, Shor’s algorithm guesses a number that might share a factor with the required number, this however will most likely not be true. It will then go on to find a better guess that is more viable. This is possible on classical computers, but it is extremely time consuming. However the same process is exponentially faster on quantum computers.

Given a number N that is a Co-prime number i.e. factor of two unique prime numbers. A number g is chosen such that $g<N$. g in itself doesn't need to be a factor of *N* itself, it can also have common factors with $N(N=a.c,g=a.b)$. These numbers can be used due to Euclid's algorithm, that allows one to find shared factors between two numbers $gcd(N,g)=a$. It is however very unlikely for a guess to share a factor with *N*, this in itself will be used to deduce a better guess. Instead Shor’s algorithm generates a pair of guesses that are more likely to share a factor with *N [12]*.

For a pair of whole numbers *A* and *B* that do not share factors, multiplying one of them but itself some arbitrary number of time, will equate to a Whole number B plus 1 i.e. $A^{p}=m.B+1$ for some p and Some multiple m.

Substituting *A* and *B* for *g* and *N* respectively,

$$g^{P}=m.N+1$$

$$g^{P}-1=m.N$$

$$(g^{\frac{P}{2}}+1).(g^{\frac{P}{2}}-1)=m.N$$

Proof:

$$(g^{\frac{P}{2}}+1).(g^{\frac{P}{2}}-1)$$

$$=g^{\frac{P}{2}}(\frac{g^{P}}{(2)}-1)+1(g^{\frac{P}{2}}-1)$$

$$=g^{\frac{P}{2}}.g^{\frac{P}{2}}-g^{\frac{P}{2}}+g^{\frac{P}{2}}-1$$

$$=g^{\frac{P}{2}+g^{\frac{P}{2}}}-1$$

$$=g^{P}-1$$

We are now left with a product of some arbitrary numbers $(g^{\frac{P}{2}}+1).(g^{\frac{P}{2}}-1)$ = product of N with another arbitrary number. The former are the improved guesses mentioned in the above process.

Since the right-hand side contains some multiple of N, the numbers on the left-hand side i.e

$g^{\frac{P}{2}} \pm 1$ can be multiples of factors of *N*, rather than the required factors.

Eg. Given $g=7$, $N=15$ and $P=4$

$7^{\frac{4}{2}}+1=50$

$7^{\frac{4}{2}}-1=48$ Neither 48 or 50 is a factor of 15

However we can find shared factors by circling back to Euclid's algorithm. $gcd(50{,}15)=5$ and $gcd(48{,}15)=3$ [10].

Upon finding those shared factors the algorithm can be broken.

A few problems however are present: One of the new guesses in itself might be a multiple of N, therefore the other would be a factor of m.

P might also be an odd number, thereby $\frac{P}{2}$ would not be a whole number. Thereby $g^{\frac{P}{2}}$ would also not be a whole number. thereby making it useless.

However for a random guess g these problems do not occur 37.5% of the time. Thereby it is worth repeating the algorithm, as there is 99% probability that the factors will be found in less than 10 guesses.

The final problem however is a tricky one, finding a number *P* such that $g^P=m.N+1$ is extremely inefficient on a classical computer, as it needs to sequentially compute the result $g^{\frac{P}{2}}$ for each power *P* till it equals $m.N\pm1$. For extremely large numbers, this process in itself might take more time than factoring the number N by brute force.

This problem is solved by using the quantum superposition quality of quantum mechanics. A quantum computation can simultaneously calculate a large set of results for a single input using superposition, however upon measurement it will return a single value, the returned value will be completely random. The key method is to arrange a quantum superposition that computes all the values but the non required values destructively interfere with each other. Thereby reducing the probability of those values being returned upon measurement [12]. Thereby the result of such an arranged computation will most likely be the desired output.

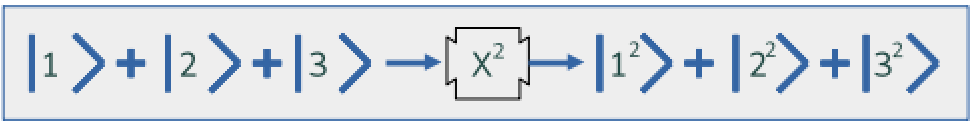


Figure 8: Example of Computations on Superposition

Shor’s algorithm does exactly this. A quantum mechanical computer needs to be set up such that give an input x it raises some number *g* to the power of *x*. There is a need to keep track of both *x* and g^x ($\langle x|g^x\rangle$). The computer is then required to take the result of the previous operation and calculate how much larger g^x is against $m.N$ (multiple of N). Let the result of this operation be known as *r* (remainder) ,since remainder is required to be 1.

A superposition of numbers is to be sent to a Quantum computer that will result in a superposition of g raised to the power of all the numbers, and after the second computation will result in a superposition of all the respective values for *r [12].*

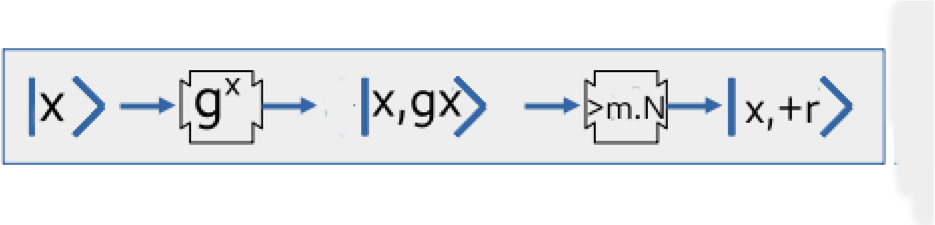


Figure 9: Visual representation of Shor's Algorithm final section

A measurement cannot be performed on this superposition, as it would just return a random result. Therefore destructive interference needs to be implemented for the proper functioning of the algorithm.

This can be done using the simple mathematical observation that is

$$g^x = m.N + r_x$$

|

V

$$g^{x+P} = m_2.N + r_x$$

If P was known, we could get $m.N+1$, however given a random value (*x*) for *P* we would get arbitrary number r such that $r \neq 1$. However as can be seen in the above observation, when P is added to the x, the r value remains the same. the same goes for any multiple of P.

Proof: $g^{P+x}=g^{P}.g^{x}=(m.N+1)(m_1.N+r_1)$

$$=m.m_1N^2+r_1mN+m_1N+r_1$$

$$=(m.m_1N+3m+m_1).N+r_1$$

Therefore for any P the equation can be written in the form $g^{x+P}=m_2.N+r_x$

The required number P thereby has a repeating property such that for any multiple of *P*, g^x, g^x+P, g^x-P will always have the same remainder *r [10]*.

The repeating property can therefore be used since computation can be performed on superpositions of powers.

Such that given the superposition of all possible powers P. Upon measuring the remainder r more than a multiple of n, will output a random r_1 . Thereby the remaining superposition should be made up of all powers P that result in a remainder of r_1 . This is one of the properties of quantum computation, i.e. given a superposition, if upon measurement the observed result could have been obtained from multiple values in the superposition then the superposition resulting from the measurement is made up of purely those values.

In the case of Shor's algorithm, the resulting superposition will contain all powers that are P apart from each other. Thereby it can be said that these numbers repeat with a frequency of $\frac{1}{P}$ ($Frequency = \frac{1}{Period}$). Therefore to find P we first need to find the frequency, this can be done by applying a mathematical concept called a Fourier transform. In simple terms, a Fourier transform allows for the conversion of a wave to a graph depicting the frequencies of the wave. There also exists a quantum version of the Fourier transform(QFT). Upon applying the QFT to the superposition obtained from the previous measurement that repeats with a frequency of $\frac{1}{P}$, all the non-existent frequencies destructively interfere with each other and results in a single quantum state i.e. $\frac{1}{P}$. Which upon measurement lets us calculate the value of P. Reflecting back on the previous example where the numbers repeat with a period of P, All the sin waves constructively interfere to result in $\frac{1}{P}$.

Thereby Given P is even and not an exact multiple of *N*, A number that shares factors with N is obtained and the factors can be obtained using Euclid's algorithm. Once these factors are found the encryption can be cracked [12]. Current quantum technology is however in the very early stages of development and can only hold a few bits. More complex algorithms exist that can perform a similar computation with fewer bits such as Adiabatic Quantum computation that can factor numbers up to 6 digits using around 3 qubits of memory. These would still require at least a few hundred times more memory to factor numbers used in current cryptographic algorithms.

Chapter 2

2.1 Attacks on Quantum Cryptography

The goal of both algorithms is to produce a one-time pad that can be used to encrypt messages between 2 parties. Thereby attacks on the protocols rely on eavesdropping on the key exchange, Since it is assumed that Eve is fully isolated from Alice and Bob. The attacks do not consider Eve to be limited by the technological limitations of the current time, this is a necessity when building ultimately proofs for the safety of cryptosystems. Eve can perform any action as far as it is permitted by the laws of physics, Thereby unitary actions on one or several qubits are permitted. Eve is required to use methods that have a QBER lower than 20% [12]. Some of the attacks that Eve can use is not an ideal and non-ideal system will be discussed.

a) Individual and collective Attacks

Multiple eavesdropping methods have been theorized, Taking into account the vulnerabilities due to building constraints. These can be widely classified into two types based on the attack method. Given that Eve attaches probes to the qubits used by Alice or Bob and measures the probes in sequence it is called an individual attack. The simple intercept and resend attack referenced in the implementation belongs to this category, also known as in-coherent attacks. The other broad category is Coherent attacks, The allow for the attacker to perform simultaneous measurement of several qubits. Two subcategories can be found within this category, Joint attacks and Collective attacks. It is assumed that Eve acts only after the privacy amplification phase has been completed. For individual attacks, Eve begins measuring after the first communication over the public channel, i.e. Base reconciliation [14].

Each has its own merits and demerits, thereby there is no clear winner for efficiency.

b) Simple intercept and resend attack

These attacks follow the same methodology as Man In The Middle attacks. They can be applied to most cryptosystems. These attacks have had a very low impact recently as most cryptosystems are designed such that it is impossible to break the encryption using these. This however does not rule out the possibility of an attacker storing the request and decrypting it in the future. Albeit it seems impossible at the moment this is the exact reason Shors algorithm and fully functional quantum computers pose such a large threat to current cryptosystems. Quantum systems however make it very difficult to utilise without being discovered. This method allows Eve to guess the correct bit with a probability of 75%.

The averaged probability of entropy decrease can be written as $\sum_r P(r)H(i|r)$ averaged over all possible results that can be obtained by eve.

where $H(i|r)=\sum_i P(i|r)\log(P(i|r))$

Where the entropy decrease for a *bit(i)* can be rewritten using Bayes theorem.

$$P(i|r)=\frac{P(r|i)P(i)}{P(r)}$$

$$P(r)=\sum_i P(r|i)P(i)$$

As explained earlier in the BB84 algorithm, Eve can obtain one of 4 results from her measurement. Thereby the entropy decrease value is $\frac{1}{2}$ corresponding to the amount of information Eve can obtain from each qubit. Eve can also use the intermediate basis for measurement which allows her a higher chance of guessing the correct bit value. The actual probability *(p)* can be defined as $p=\cos(\pi/8)^2=\frac{1}{2}+\frac{\sqrt{(2)}}{4}\approx 0.854$ (This is due to Eves results being deterministic 1/2 of the time), for a QBER of 25% and information gain per bit as 0.399.

c) Symmetric Individual Attacks

The general idea behind this attack is similar to the intercept and resend attack described above. The main difference however is that Eve can obtain the maximum Shannon information for a fixed QBER. Assuming an idealized scenario wherein the single qubit source is perfect and Eve uses individual attacks. The attack is performed on a 4-state BB84 protocol, dissimilar to the 6-State protocol described in Section 1 of this chapter. Eve sets up an isolated system that will function to interact with the qubit while it is in transit. The system must follow the rules of quantum physics described inside a Hilbert space. She can choose an interaction with the qubit defined as a unitary operator.

Let us consider H_{Eve} to be the Hilbert space Eve's chosen system(probe) and C^2 ¿ H_{Eve} to be the combined system with the qubit. let $|\vec{m}\rangle$, $|0\rangle$ and U denote Qubit, the initial state of the system and the unitary operation respectively. Since Eve forward the qubit to Bob the state that bob receives can be written as

$$\rho_{Bob}(\vec{m})=Tr_{H_{Eve}}(U|\vec{m},0\rangle\langle\vec{m},0|U^{!})$$

Assume that Bob's state is somehow related to Alice's by some factor n such that

$$\rho_{Bob}(\vec{m})=\frac{1+n\vec{m}\vec{\sigma}}{2}$$

Any attempts at listening in to the exchange that follows the above equation can be defined as Symmetric attacks since n relies upon the symmetry between Alice and Bob's states. Due to this property and the fact that the qubit can only be in 2 states we can declare the below [14].

$$\langle\varphi_{\uparrow}|\theta_{\downarrow}\rangle+\langle\theta_{\uparrow}|\varphi^{\downarrow}\rangle=0$$

wherein φ is Eves state if Bob obtains an undisturbed qubit (*F*) and θ is when the qubit is disturbed (*D*). *n* can therefore be defined as $n=F-D$.

Looking back at the previous equation and the properties of unitary operators. Given that Alice and Bob use compatible basis for measurement F represents the possibility of Bob obtaining the proper result. Thereby *F* can be the Fidelity and *D* the QBER.

Symmetric individual attacks depend fully on 2 real parameters: $\cos(x)\equiv\langle\varphi_{\uparrow}\vee\varphi_{\downarrow}\rangle$ and $\cos(y)\equiv\langle\theta_{\uparrow}|\theta_{\downarrow}\rangle$.

Given that Alice sends a qubit in the state $|\uparrow\rangle$ and Bob performs a measurement in the $\{\uparrow,\downarrow\}$ (else the qubit will be discarded). Since Eve knows the Basis, her probe must be in one of 2 mixed states

$$\rho_{Eve}(\uparrow)=FP(\varphi_{\uparrow})+DP(\theta_{\uparrow})$$ Or

$$\rho_{Eve}(\downarrow)=FP(\varphi_{\downarrow})+DP(\theta_{\downarrow})$$

Eve then needs to distinguish two pure states using either overlapping $\cos(x)$ or $\cos(y)$ (Defined Above) . This is made possible because the two subspaces $\rho_{Eve}(\downarrow)$ and $\rho_{Eve}(\uparrow)$ are mutually orthogonal. An optimal measurement distinguishing the two states will leave Eve with a $\frac{1+\sin(x)}{2}$ probability of getting the correct guess. Thereby the Maximum information about a qubit Eve can obtain in an ideal situation is given by

$$I=F.(1-h(\frac{1+\sin(x)}{2}))$$

$$+D.(--h(\frac{1+\sin(y)}{2}))$$

Given that $h(p)=-plog_2(p)-(1)\log_2(1-p)$ for some QBER *D*. The Maximal value can be obtained when x = y.

Substituting x = y we obtain

$$I = F.(1 - h(\frac{1+\sin(x)}{2})) + D.(h(\frac{1+\sin(x)}{2}))$$

$$I = (1 - h(\frac{1+\sin(x)}{2}))(F.D)$$

Given that $F = \frac{1+\cos(y)}{2-\cos(x)+\cos(y)}$

and $D = \frac{1-\cos(x)}{2}$

Since x = y

$$F = \frac{1+\cos(x)}{2-\cos(x)+\cos(x)}$$

$$= \frac{1+\cos(x)}{2}$$

therefore

$$F + D = \frac{1+\cos(x)}{2} + \frac{1-\cos(x)}{2}$$

$$= \frac{1+\cos(x)+1-\cos(x)}{2}$$

$$= \frac{1+1}{2}$$

$$= 1$$

$$I_{max} = (1 - h(\frac{1+\sin(x)}{2}))(F + D)$$

$$I_{max} = (1 - h(\frac{1+\sin(x)}{2}))$$

For an x of 0, both the resulting QBER(*D*) and Information(*F*) are 0. for an $x = \pi/2$ however the QBER results in $1/2$ and the Information gain is 1.

The QBER and Information follow a linear growth relationship for small increases such that [14]

$$I^{max}(A, E) = \frac{2}{\ln(2)} D + O(D)^2 \approx 2.9D$$

A and E represent the classical values obtained after the procedure by Alice and Eve respectively.

Let us also consider a var B for Bob's classical random. Alice and Bob can agree to the key after performing Error correction and Privacy amplification only if $I(A,B)>I(A,E)$ or $I(A,B)>I(B,E)$ meaning that Shannon information for Alice and Bob should be greater than that obtained by Eve [11].

Thereby the Security criteria against individual attacks for BB84 protocols are written as

$$BB84_{Secure}\Leftrightarrow D<D_0\equiv\frac{1-1/\sqrt{(2)}}{2}\approx 15\%$$

For some QBER larger than D_0 , Alice and Bob can't obtain a secure key even with the use of Error correction and Privacy Amplification.

2.2 Attacks on BB84

Although a properly thought-out quantum cryptographic algorithm is protected by the laws of physics itself, it remains vulnerable to certain methods of attack due to limitations in technology. There have been multiple attempts to break BB84 to date and the algorithm has evolved to prevent these attacks. As seen above, a simple interpretation of the man-in-the-middle attack will be ineffective since it introduces a QBER of 25% or more. However, since photons are used as a transmission medium certain attacks can be performed. The improper generation and measurement of photons create a vulnerability in the system. The Phase-Mapping attack can, in theory, use these insecurities to attack the algorithm. This attack allows Eve to reduce the QBER to 19.7% which is slightly lower than 20% which is the security standard for identification of eavesdropping. Due to limitations in polarization and phase instabilities over long distances bi-Directional QKD schemes have been developed. One such method is the 'plug-and-play'' structure, wherein Bob sends a pair of streams of photons (Signal pulse and reference pulse) to Alice. The reference pulse is used to synchronise her phase modulator. Alice then modulates the phase of the signal pulse and sends back both pulses as single photons to Bob. Bob then chooses a basis for measurement by using the reference pulse returned by Alice [14].

Since Alice allows signals to enter and leave her device, it allows for a potential backdoor. Practical phase modulators have a finite response time, as shown in the figure below. In an ideal case, Bob's signal pulse should pass through Alice's phase modulator in the middle of the modulation signal and would thereby undergo a proper modulation $\left(time\, t_0\right)$.

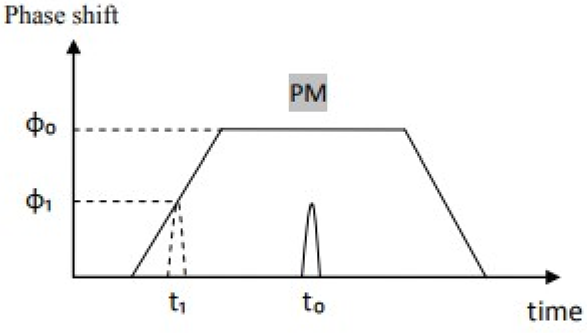


Figure 10: Phase modulation diagram[1]

But given that Eve changes the time difference between both the signal and reference pulse thereby causing the signal pulse to pass through the phase modulator at a different time causing the encoding phase to be different from intended by Bob. Consider Alice wishes to use the bases

$0,\pi/2,\pi,3\pi/2$ to encode the bits $0_1,0_2,1_1,1_2$ respectively. Following the remapping attack by Eve, Alice's phase $0,\pi/2,\pi,3\pi/2$ will be mapped to $0,\phi_1,\phi_1+\phi_2,\phi_1+\phi_2+\phi_3$ where ϕ_i is the new phase difference between the adjacent states. The value of ϕ_i depends on the time difference that is introduced by Eve and the phase modulation [11].

Eve can intercept Bob's Reference pulse and forward a slightly time-shifted pulse to Alice through her device. Eve's strategy depends upon distinguishing $\{0_1\}$ or $\{1_2\}$ from the phase $\{0_2,1_1,1_2\}$ and $\{1_1,0_1,0_2\}$ respectively with the least amount of errors possible to prevent increasing the QBER. To do so, Eve induces a phase-shift of $\{\phi_1+\phi_2\}$ or $\{\phi\}$ using her phase modulator to change the reference pulse sent through by Alice and then measures the interference. Based on the results, Eve decides to either send a standard BB84 state to Bob or discard it.

Assuming that Eve uses the phase $\{\phi_1+\phi_2\}$ to distinguish $\{0_1\}$ and Alice sends the phase $\{0_1,0_2,1_1,1_2\}$.

Let the probabilities for Eve successfully distinguishing the State be $\{P_{0_1},P_{0_2},P_{1_1},P_{1_2}\}=\{\sin^2\left(\frac{\phi_1+\phi_2}{2}\right),\sin^2\left(\frac{\phi_2}{2}\right),0,\sin^2\left(\frac{\phi_3}{2}\right)\}$

After the attack, the probability of an error being introduced into the system can be given as $\{0,1/2,1,1/2\}$.

Given this information the QBER can be calculated as follows:

$$QBER_{\phi_1+\phi_2}=\frac{\frac{\sin^2(\frac{\phi_2}{2})}{2}+\frac{\sin^2(\frac{\phi_3}{2})}{2}}{\frac{\sin^2(\frac{\phi_2+\phi_1}{2})}{2}+\frac{\sin^2(\frac{\phi_2}{2})}{2}+\frac{\sin^2(\frac{\phi_3}{2})}{2}}$$

$$QBER_{\phi_1}=\frac{\frac{\sin^2(\frac{\phi_1}{2})}{2}+\frac{\sin^2(\frac{\phi_2}{2})}{2}}{\frac{\sin^2(\frac{\phi_3+\phi_2}{2})}{2}+\frac{\sin^2(\frac{\phi_2}{2})}{2}+\frac{\sin^2(\frac{\phi_1}{2})}{2}}$$

Assuming that Eve set ϕ such that $\phi_1=\phi_2=\phi_3=\phi$, a Total QBER can be calculated

$$\overline{QBER}=\frac{QBER_{\phi_1}+QBER_{\phi_1+\phi_2}}{2}=\frac{\sin^2(\frac{\phi_2}{2})}{\sin^2(\phi)+2\sin^2(\frac{\phi}{2})}$$

BB84 is also vulnerable to the photon number-splitting attack. Due to the limitations in the generation of the photons for the transmission, most implementations of BB84 use phase-randomized weak coherent pulses. Thereby on rare occasions, more than one photon might be sent through to Bob, Since both photons sent are encoded the same one of these could be measured by Eve while the other is forwarded to Bob [4]. Thereby, if Eve splits the photon pair, she can obtain the same information as Bob. This will also not disturb the state of Bob's photon, and Eve would remain undetected by Alice and Bob when comparing the bits of their shared key. Albeit split photons become less prevalent as the number of photons transmitted increases, Eve might be able to obtain some information on the message being transmitted. Certain modifications to BB84 have been suggested that effectively negate these situations.

The phase-mapping attack can be fixed by proper monitoring of the phase difference between the reference pulse and signal pulse to make sure there is no delay between the pulses. If any delay is found by Alice, then she can conclude that Eve has phase-shifted the pulses and the communication has been compromised.

The Photon splitting attack can be mitigated by using a decoy state. In a paper titled "Decoy State Quantum Key Distribution," the authors suggest an improvement to the BB84 protocol that is meant to allow Alice and Bob to detect the presence of eve in the case of a photon-splitting attack. This is done using a decoy signal that is mixed in with the proper signals. The signals can be identified based on their intensity however, this also increases the chances of a split photon occurring, but it allows Alice to detect Eve's interference on the channel. To avoid altering the state of the photons, Eve can only measure the number of photons received at a certain point in time during the attack phase [11]. This method however has a very low yield and would therefore tip off the honest parties regarding the intrusion.

a) Trojan Horse attacks

The previous strategies discussed above try to obtain the highest amount of information possible for some arbitrary fixed QBER. Eve can however choose to take a different approach to the attack. Eve chooses to send signals to Bob and Alice over a quantum channel. Consider a scenario where Eve sends photon pulses over an optical medium to both Alice and Bob. She then observes the reflected light to obtain some information (Similar to sending an SYN packet to a host). In theory, Eve could determine the laser used, the detector fired or even the settings of the phase modulator. Similar to the previous example with SYN packets, the channel needs to be open for communication with honest parties [14]. Thereby, it is not possible to use a shutter or blocking medium to prevent this. Plug and Play models of Quantum cryptosystems are especially vulnerable to these attacks due to using mirrors to send signals to Bob. Thereby, Eve can send strong photon pulses to Alice and effectively decipher the phase shift applied.

Since Alice cannot close the connection, she can force Eve to send her probing pulse at the same moment as Bob. Bob sends macroscopic pulses and Alice then converts them into a single photon level. Thereby, if Eve wants to get a single photon from the reflection, then she needs to compensate for the attenuator (Converts Macroscopic pulse to a single photon). Given that Alice can detect a spike in the intensity of the pulses, then she can identify the presence of Eve [14].

The Existence of trojan-horse attacks provides a very compelling argument against the security of QC algorithms. It needs to be taken into account that these only occur due to technological limitations and can therefore be fixed as the system gets closer to an ideal one. However, they prove that the algorithms have different attacks that cannot be protected by the laws of quantum mechanics.

Chapter 3

3.1 Methodologies

The project roughly followed an action research approach. Data was collected from multiple runs of a set consisting of Quantum security algorithms and another with Classical cryptosystems. Data visualization was performed with the use of automated tools provided by python. Certain hypothesises were produced upon the results of each set of tests. The number of runs was increased by a factor of 10 each time. The algorithm was modified as needed to observe different Parameters. The evolution of the data set was analysed to find inconsistencies or peculiar observations to help produce a better inference. Using the methodology allowed for much fewer outliers in the Data. A simple peer review was performed on the inference to prevent unintended bias towards certain data.

3.2 Implementation

a) BB84 Model

The implementation models a run of BB84 with Alice and Bob acting as the conversing parties. The first run remains uninterrupted by Eve. The second however models Eve's interference and how it affects the overall QBER and Secret key. The implementations are written in python using a quantum computing simulation library known as Qiskit, provided by IBM that can run on IBM's quantum computer remotely. Some other novel libraries used are numpy, tracemalloc, time and csv. The Novel libraries function to process and store clean data into easily iterable forms. Alice produces an initial key using a sequence of random bits "0" and "1". She then picks a sequence of Polarization eigenstates that she will use to encode the sequence of bits. After going through the normal process of the BB84 Alice and Bob will sift their key to discard errors.

Upon introducing Eve to the equation, she makes a candidate key using Alice's intercepted bits and forwards it to Bob.

Key sharing in the implementation will be simulated by 3 different quantum circuits for all participants(Alice, Bob, Eve). 16 qubits are used for the implementation, thereby let *n* be 16. Alice's quantum circuit is built using n qubits and n classical bits for measurement. a random 16-bit number is generated and used as the key by Alice. The key is then encoded into the qubits to either of the states $\{|0\rangle|1\rangle\}$ depending on the binary representation of the chosen key. A random rotation is then applied to these states, and the array of basis is stored for verification.

A separate quantum circuit is initialized for bob, his initial state is set to Alice's output state. This is done using a function called sendState that retrieves the Quantum Assembly language(qasm) code of a circuit and extracts the gates applied to it. These gates are used to initialize a different circuit. This can be performed since the qasm instructions for each circuit are stored as a dictionary in the object and can be accessed using the dot operator. Upon creation of Bob's circuit that has Alice's output state, we can consider that Bob has received Alice's Basis. However, the received state is considered unknown information and Bob proceeds to use a random basis to measure each qubit and store it in a comparison array. Alice and Bob then sift the key based on their respective key arrays, and the final key can be used as an OTP. The percentage of discarded bits can be seen in figures *20* and *21*.

Given the fact that bob chooses the wrong basis 50% of the time, a verification check can be performed, by checking if the theoretical probability is replicated. It is also known that Bob can end up choosing the wrong basis but can arrive at the right eigenstate 50 % of the time. Thereby Bob can get roughly 3/4ths of the Bits correct. In the real world however due to noise in quantum channels it is rare to get a key similarity of 100%. The key similarity usually ranges between 75% and 100%. Anything that does not fit the range can be considered to be invalid, as an eavesdropping attempt might have disturbed the channel. Here a cutoff of 90% is applied to check the validity of the key.

Eve is modelled similarly to Bob. It is assumed that Eve has intercepted the qubits sent by Alice, this is implemented by using the sendState function to initiate Eve's quantum circuit using Alice's state. Eve doesn't know the bases used for encoding and therefore uses random basis from the measurement of the qubits. Using her measurements, Eve generates her own Candidate Key. Due to Eve's unwarranted measurement of the qubits, they collapse into different eigenstates. This cannot be easily simulated since results are stored in classical registers, while the Qubits themselves don't change. Therefore, Eve's qubits are manually set to their corresponding altered states,, The results of Eve's measurements are used as the initial state. The operations Eve performed for measurement are then reversed (A complimentary basis is used). Eve's Altered state is used to initialise Bob's circuit using the sendState function.

Alice and Bob then go through the same procedure as earlier by comparing their Measurement basis arrays and discarding mismatching bits. A discrepancy will arise upon verifying the theoretical properties since it is almost certain that Bob will get less than 90% of the bits correct due to Eve's interference.

b) E91 Model

Initialization

The E91 implementation is a practical model of the E91 protocol, built using the same packages as the BB84 model. The E91 protocol requires the definition of a quantum register(qr) with 2 qubits and a Classical register(cr) with 4 bits. Assume Alice and Bob use qr[0] and qr[1] respectively. Their measurement results are stored in cr[0] and cr[1]. the final 2 bits in the classical register are reserved for Eve's measurements of Alice and Bob's qubit.

A singlet is then initialized using qr and cr. After the creation of the state, the CNOT gate is applied to both qr[0] and qr[1] Qubit. The Hadamard gate is then applied to qr[0]. After which, a controlled not operation using the qr[0] as the Control bit and qr[1] as the target qubit. To form a circuit as shown in the figure below.

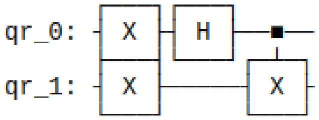


Figure 11: Quantum circuit for Qubit entanglement (From Qiskit)

Measurement

The qubits in the Quantum register are now entangled. the qubits are then delivered to Alice and Bob respectively. Circuits $A(\vec{a}_i)$ and $B(\vec{b}_i)$ are defined as $\vec{a}_i.\sigma$ and $\vec{b}_i.\sigma$ respectively for the measurement of respective qubits. A_1 has the Hadamard gate applied to it. A_2 Has the Sequence of S -> H -> T -> H . B1 and B3 have the same configuration as A2. These are meant to act as detectors to measure the X, W, Z and V measurable. The Detectors are then placed in the earlier circuit. Alice and Bob select a random set of bases using a random choice function.

Results

The circuit is then executed, and the results are stored in a variable. The results are made up of 4 digits corresponding to the Classical register. Recalling that the first and second bits contain Alice's and Bob's measurements. Alice and Bob need to record their measurements, this is performed by setting up Regular instructions for each of the possible patterns. These patterns are then used to fill Alice's and Bobs Strings with the results.

Revealing Bases

An empty array is assigned for Alice and Bob's key. For each Measurement of the i'th singlet, the output of the measurement is stored in k[i]. Alice stores a_i whereas Bob stores $-a_i$. 500 singlet states are used, and thereby the process is iterated through 500 times. Since the keys have been set up for both Alice and Bob, they need to be sifted. A simple check is run that iterates through the key checking for inequalities. The check however cannot be performed on the whole key in a real-world scenario. It would need to be done using random sampling on parts of the key and discarding them thereafter. A large enough sample will provide a value that is close to the number of expected errors in the whole key.

Verification

Verification of the run is performed by calculating the CSHS correlation value (*CHSH*) using the results from the measurements of the spin projections from $a_1/b_1, a_1/b_3, a_3/b_1$ and a_3/b_3 directions. These can be equated to X or W, X or V, Z or W and Z or V respectively.

The Equation for the joint measurement of A and B can be written as :

$$\langle A\otimes B\rangle_{\psi}=\sum_{jk}(j,k)a_j b_k P_{(\psi)}(A|=a_j,B|=b_k)=\sum_{jk}(j,k)a_j b_k P_{\psi}(a_j,b_k) \quad (6)$$

A and B refer to the spin projection observables. The corresponding eigenvalues are $a_j, b_k=\pm 1$.

Thereby, For $A(\vec{a}_i)$ and $B(\vec{b}_j)$ and the singlet state $|\psi\rangle_s$ we can simplify (Equation 6) as

$$\langle A(a_i)\otimes B(b_j)\rangle=P(-1,-1)-P(1,-1)-P(-1,1)+P(1,1)$$

in the implementation, the right side can be written as follows.

$$P(a_j,b_k)=\frac{n_{a_j,b_k}(A\vee B)}{N(A\vee B)} \quad (7)$$

The Numerator contains the number of results obtained via measurements of $(A\otimes B)$. The denominator is the total number of measurements of the observables $(A\otimes B)$.

The expectation values are calculated using (Equation 7), (Equation 6) and (*CSCH*)

Since Eve is not involved in the first run of the model, the CHSH Corr value should be close to $-2\sqrt{(2)}\approx -2.828$. There should also be no mismatching bits in Alice's and Bob's keys, since noise does not play a role in the simulation. Given the fact that 9 combinations of measurements can be performed on the qubits. 2 of these provide any relevant results, thereby the key size should be near $2/9$.

Eve's Model

An intercept-resend is modelled such that Eve intercepts one or both the entangled qubits from the source. She then measures them before sending newly prepared qubits based on her measurement results, to Alice and Bob.

$$E(n_A)=n_A.\phi$$

$$E(n_B)=n_B.\phi$$

Represent the observables similar to the ones defined for Alice and Bob. Eve needs to choose n_A and n_B such that $n_A=a_2,a_3$ and $n_b=b_1,b_2$ since these are the only directions that can be used for the creation of a secret key. These 2 directions refer to the W and Z basis. Eve will choose randomly between these 2 basis for her measurement $W\otimes W$ and $Z\otimes Z$.

Eves circuit is then added to the previous model and the whole system is executed and measured. All 3 then record their results, Alice and Bob using the previous regular expression, whereas a new array of regex is made for Eve that checks the final 2 bits of the classical register. These results are then made into secret keys using the bits obtained after the measurement of $W\otimes W$ and $Z\otimes Z$. The keys are iterated through to find inconsistencies, Eve's key is checked against both Alice's and Bob's. We then check Eve's knowledge of both keys using the data obtained. We then calculate the Corr Value.

The Corr value for the eavesdropper model strays quite far from the actual value it should be i.e. $-2\sqrt{(2)}$ (*CHSH*) Alice and Bob would notice this and would thereby invalidate the process. As given in **CHSH** *Section* the value will be $-\sqrt{(2)}\leq C\leq\sqrt{(2)}$,

C being the CHSH correlation value. The higher Eve's knowledge is of the keys the higher this value will increase. There will also be mismatched bits in Alice's and Bob's keys, since upon eves measurement Eve obtains either *-1,1* or *1,-1* randomly (Equation). Depending on which value she obtained, Eve prepares and sends $|\varphi_1\rangle=|01\rangle$ or $|\varphi_2\rangle=|01\rangle$ (This is automatically provided by a measurement in the Z basis for Alice's and Bobs Detector) and sends it to Alice and Bob. Upon Alice and Bob Measuring on W or W they get a random result with the probability $P_{\varphi_n}(a_i,b_j)$.

Chapter 4

4.1 Observations

a) Memory Usage:

Each implementation was wrapped with a check using the tracemalloc python library. Which allowed for checking the Memory usage before and after the implementation, the difference was then exported as a csv. The record file was then plotted into a histogram for better viewing of the memory usage. Each algorithm was run 100, 1000 and 5000 times(left to right) to reduce outliers. The following are the observations obtained:

BB84:

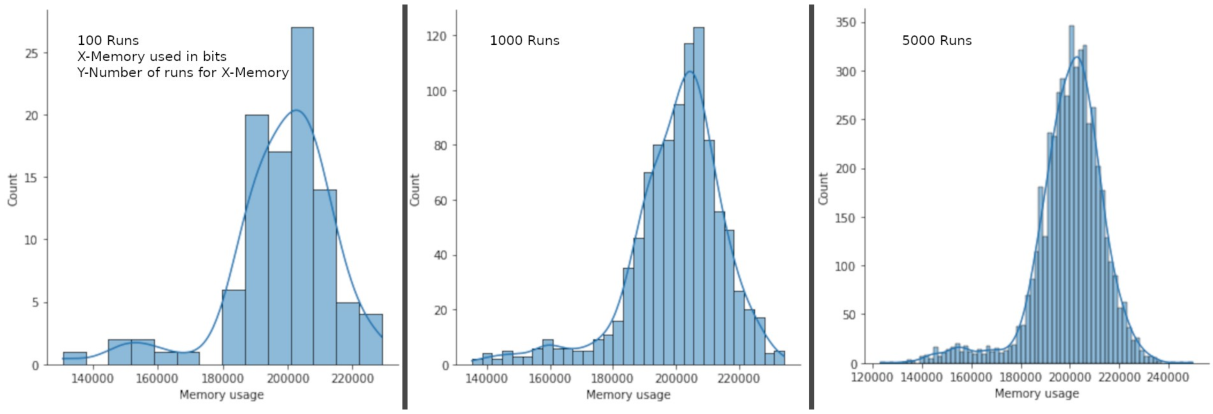


Figure 12: BB84 Memory Usage per Run

E91:

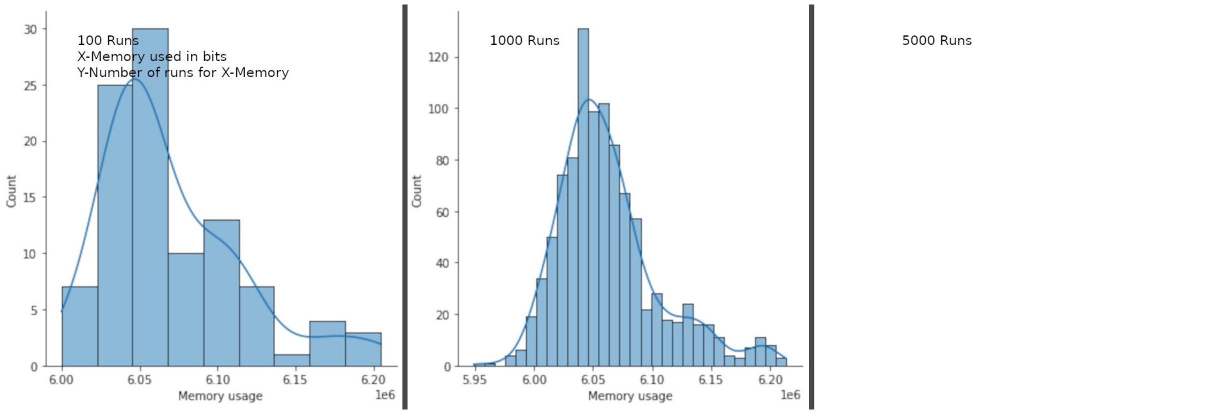


Figure 13: E91 Memory Usage per Run

RSA:

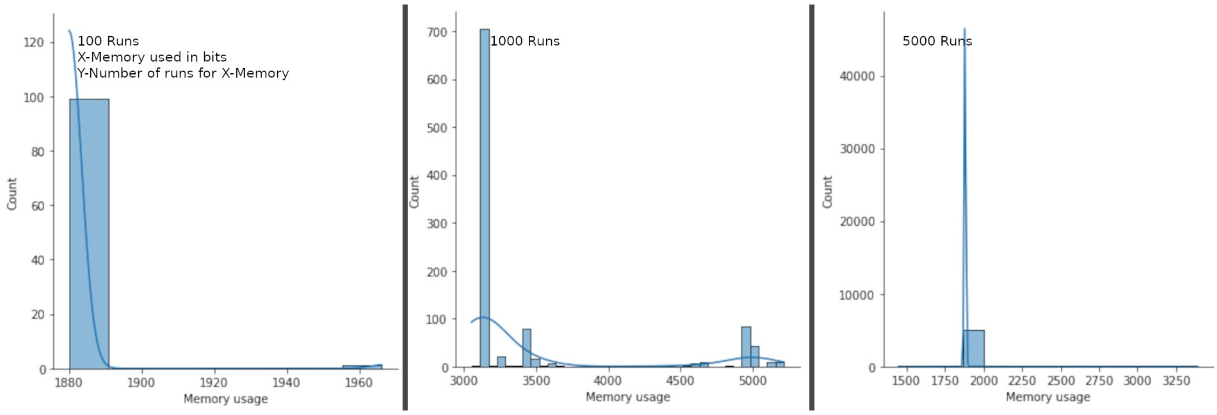


Figure 14: RSA Memory Usage per Run

ECDH:

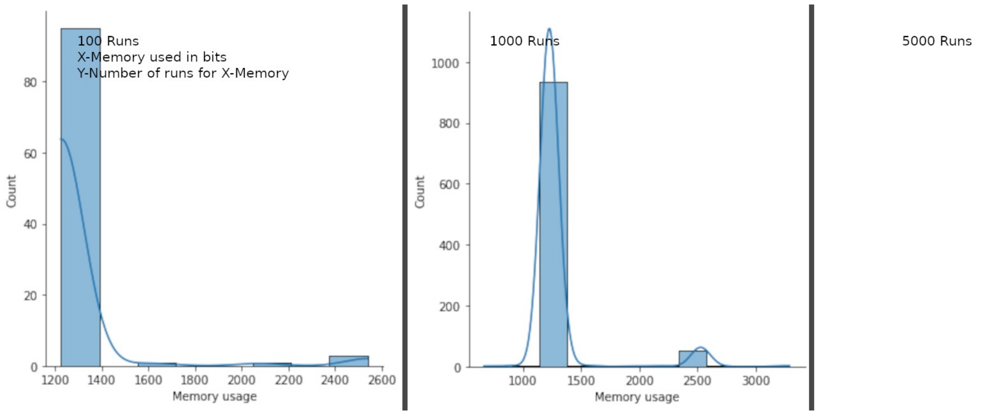


Figure 15: ECDH Memory Usage per Run

It can be observed that the quantum algorithms use exponentially more memory than the classical algorithms. This stems from having to simulate quantum physics using a classical computer. Since each qubit hold 4 bits of information, the simulation requires a larger amount of memory. Furthermore, Each Quantum register can also be in a quantum superposition. Which uses more resources due to performing operations on all elements at the same time.

b) Time Usage:

- * Y-Axis: Number of times an algorithm used x-Time
- * X-Axis: Time in milliseconds used by an implementation

BB84:

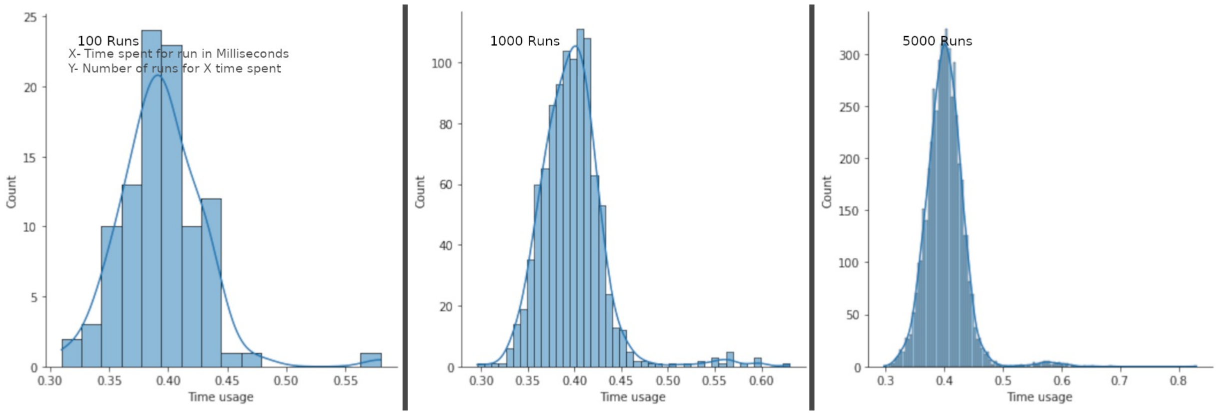


Figure 16: BB84 Time Usage per Run

E91:

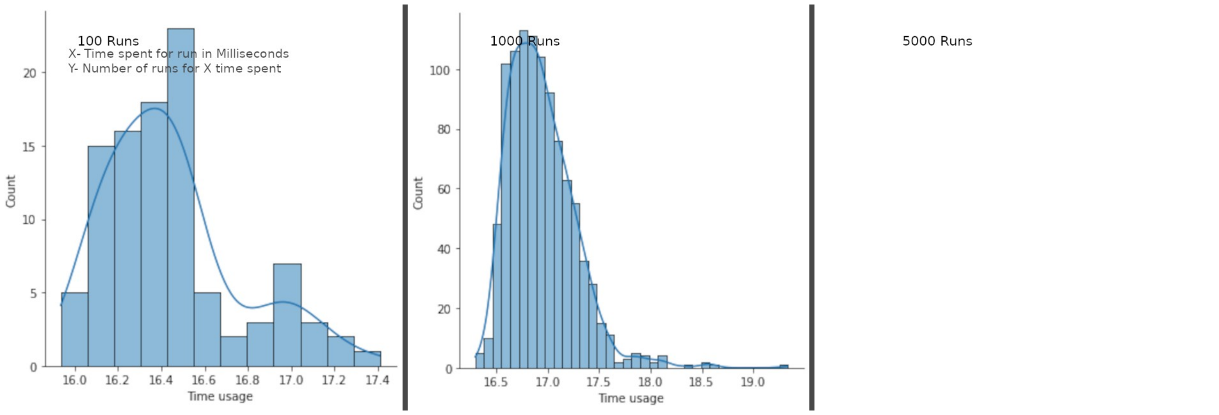


Figure 17: E91 Time Usage per Run

RSA:

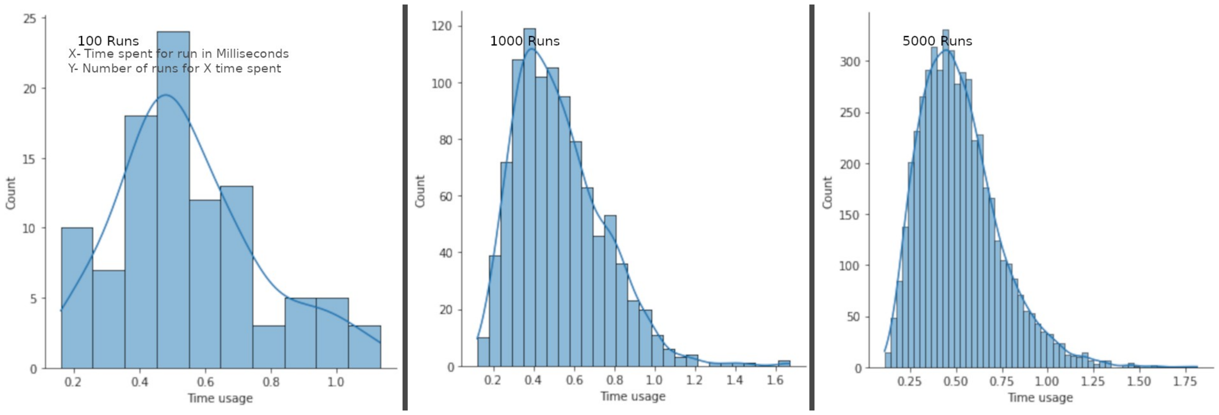


Figure 18: RSA Time Usage per Run

ECDH:

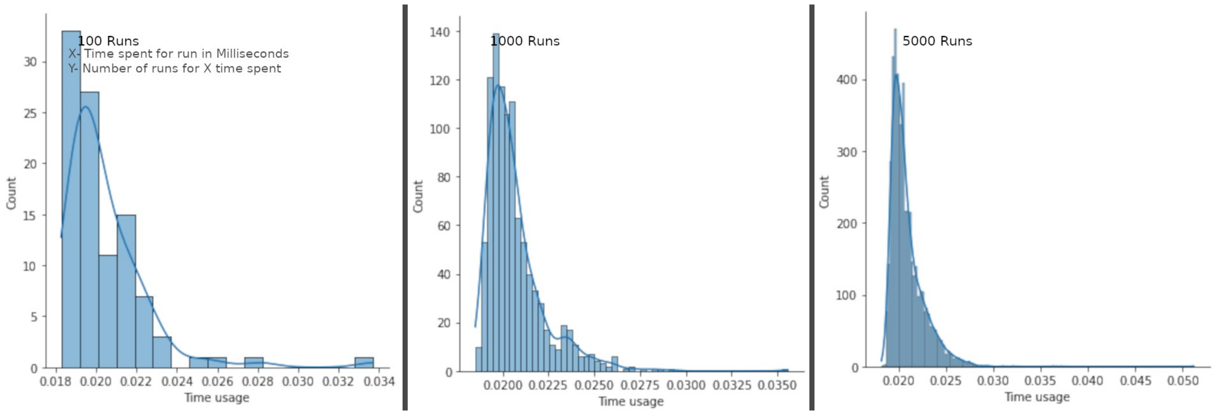


Figure 19: ECDH Time Usage per Run

The time for each implementation tends to vary greatly within the algorithm itself, partly due to the randomness in these algorithms. However similarly to the memory test the classical algorithms perform much better than the quantum algorithms. With ECDH being the Fastest, followed by BB84, RSA and E91 being the slowest. The implementation of E91 is the slowest due to it performing a quantum superposition in 2 Quantum registers. However, RSA and ECDH use 2048 bit Keys, wherein the quantum algorithms only use 4 qubits, since that is close to the upper limit possible with current technology.

c) BB84 Percent of Discarded Bits(Without Eve):

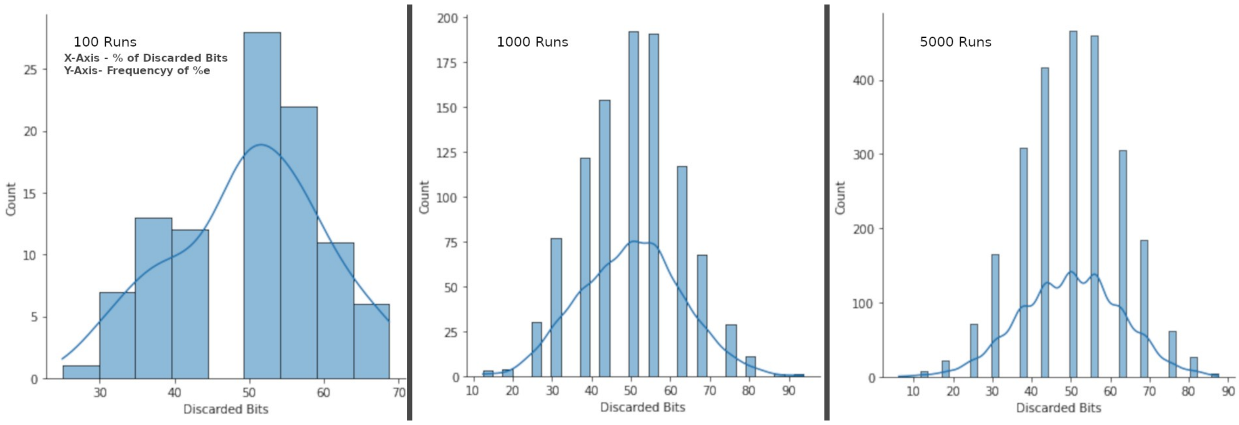


Figure 20: Discared Bits Without Eve for BB48

d) BB84 Percent of Discarded Bits(With Eve):

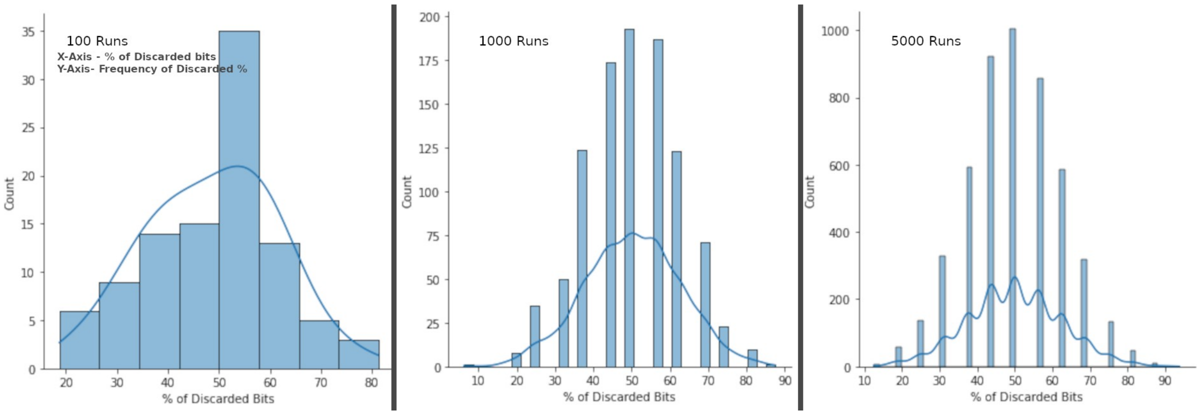


Figure 21: Discarded bits during sifting phase(With Eve)

e) E91 correlation Variation(Without Eve):

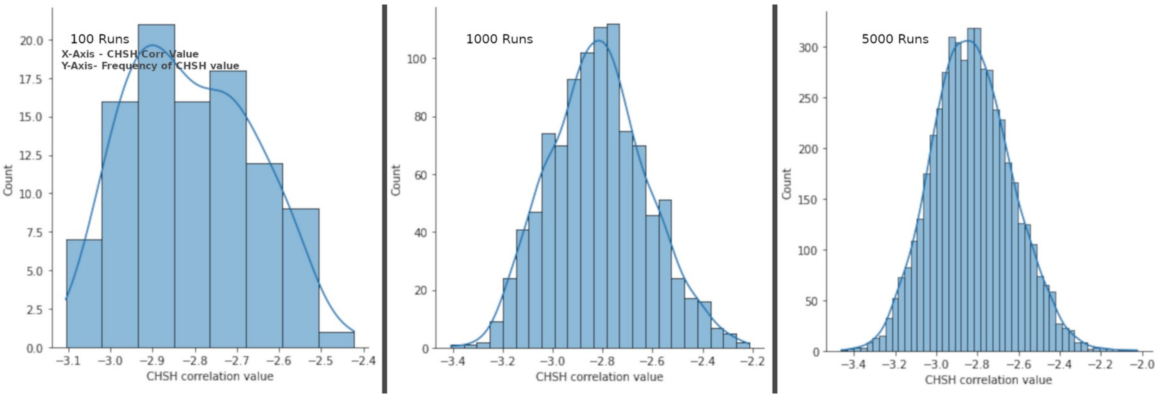


Figure 22: E91 CHSH Corr Values per run (Without Eve)

A very clear begins to emerge as the number of runs increases, the pattern mentioned is a normal distribution curve. Also called a bell curve. The corr value should roughly equal -2.8 for a valid run without Eve. This can be clearly seen in the graphs. Although there are some outliers the highest probability i.e. the peak of the curve is at -2.8 thereby we can verify that the runs are valid. At the worst case, it begins moving toward -2.2. As can be seen in other graphs below, there are some outliers that reach -2.2 corr value. Thereby, a valid corr value should be at least 2.6 and above to reduce the possibility of Eve remaining undetected to the minimum.

f) E91 correlation Variation(With Eve):

The Graphs verify the fact that Eve can rarely ever go undetected by Alice and Bob. The curve gets infinitely closer to a Bell curve. Therefore, the probability distribution dictates that Eve has a very small probability of inducing a very small QBER and therefore obtaining a CHSH correlation value of 2.2. Since 2.2 is not equivalent to 2.8 it can be concluded that the probability that Eve can induce a CHSH value of 2.8 is extremely rare. The probability also decreases with the use of a larger Key.

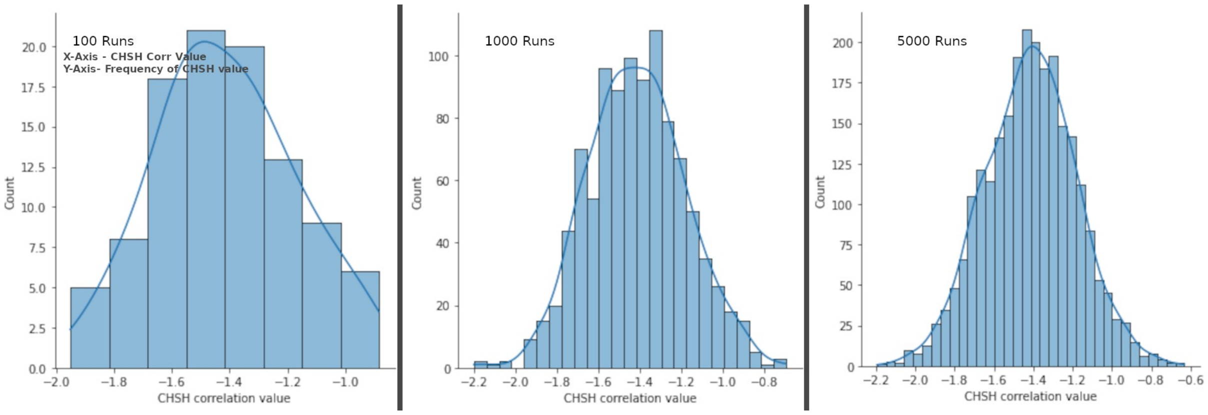


Figure 23: E91 CHSH Corr Values per run (With Eve)

g) Knowledge gained by Eve(E91):

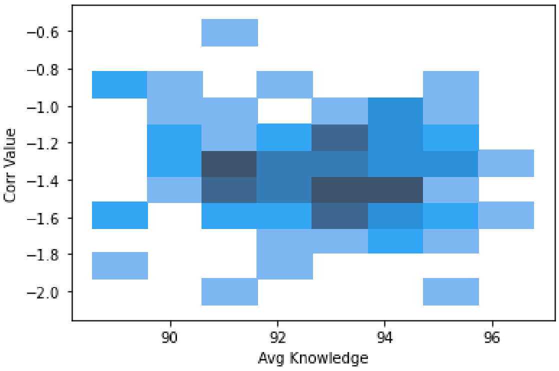


Figure 24: 100 Runs for CHSH Corr Value vs Eves Knowledge -E91

It is known that the Corr value should hover around (2.828) for a Valid Run. Here it can be seen that as Eve's knowledge of the key increases, the corr value also strays further from the proper corr value.

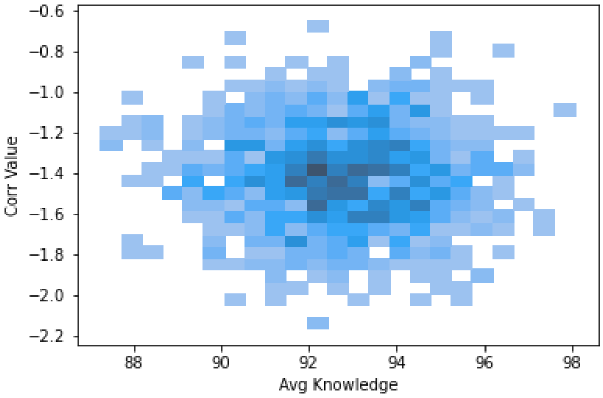


Figure 26: 1000 Runs for CHSH Corr Value vs Eves Knowledge -E91

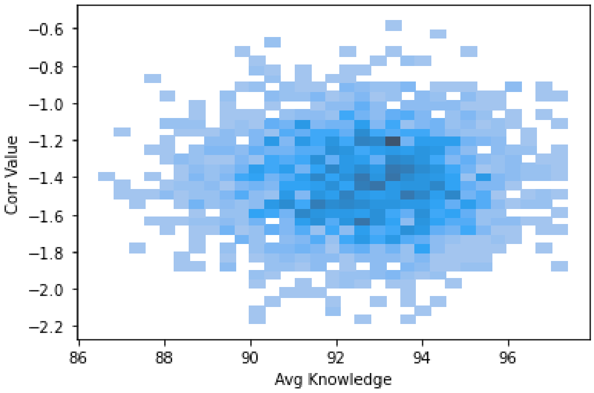


Figure 25: 5000 Runs for CHSH Corr Value vs Eves Knowledge -E91

In the latter 2 graphs, it can be seen that some outliers exist wherein for large amounts of knowledge the Corr Value starts straying toward the proper value. However, does not cross -2.2. There is still an extremely rare possibility that Eve can go undetected, however it remains almost unattainable. The final graph is an accumulation of 5000 runs. It shows a wide spread of knowledge vs Corr Values. Albeit no proper pattern can be seen, it was expected since there is a large amount of randomness in the choices of Eve, Alice and Bob. Thereby, a pattern would be difficult to obtain.

h) Knowledge Gained by Eve(BB84):

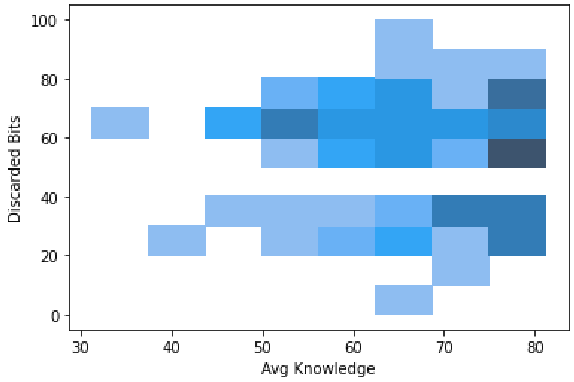
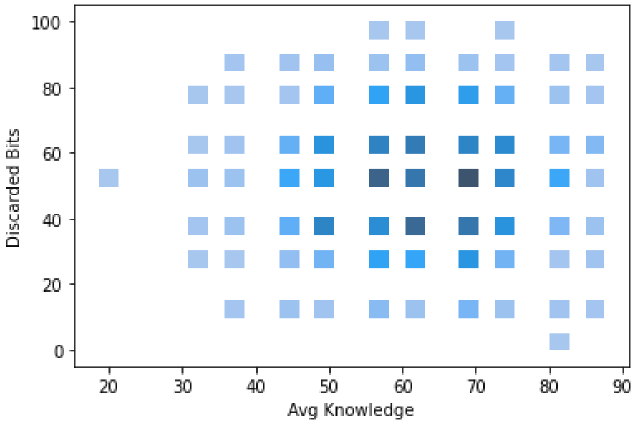


Figure 27: 500 Runs for Discarded Bits vs Eves Knowledge -BB84



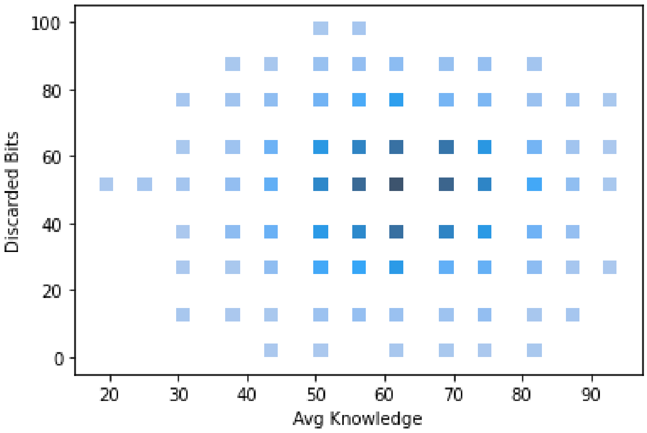


Figure 29: 1000 Runs for Discarded Bits vs Eves Knowledge -BB84

Figure 28: 2500 Runs for Discarded Bits vs Eves Knowledge -BB84

A peculiar situation is seen in the graph. There are clear areas in the graph. This is due to the number of qubits used in the implementation. Since the number of qubits used is 8, and the Size of the sifted key is divided by it, certain probabilities are excluded. Since there should be no noise in the system. We can see that for very rare cases, there are almost no discarded bits for high amounts of Knowledge gain. This is due to the small number of qubits used.

4.2 Results

The data depicts a clear picture regarding the differences between Classical computing algorithms, along with a verification of the security measures for their quantum counterparts.

Contrary to expectations, it was found that a simple BB84 implementation ran faster than the RSA implementation, given that the transmission time for the RSA keys was omitted. Expectedly, the Quantum cryptosystems used large amounts of memory, with almost an exponential difference. It can be inferred from Fig.23 and Fig.21 that the security conditions for both the chosen cryptosystems hold fast against intercept resend attacks. The average amount of discarded bits increases by a noticeable amount when Eve begins to observe the channel. Eve's interference with the entangled qubits in the E91 algorithm moves the CHSH value off its valid bounds.

Chapter 5

5.2 Future Scope

Further work can be performed to model other theoretical attacks mentioned in the Attacks on Cryptography section. These can then be analysed to compare the amount of information Eve obtains from each. A better set of data could also be obtained by performing the experiments on a functional quantum computer. Comparisons can be made for the factorization of prime numbers using the Number-Sieve Algorithm and Shor's algorithm. Albeit it has been mathematically proven that the latter is faster, it would help understand the relationship further and quantify it. This remains impossible at the moment, since only 2-digit numbers can be factored by the Shors algorithm on current quantum computers.

5.2 Conclusion

Quantum Cybersecurity is quickly rising to prominence, with Algorithms such as Shor's posing a massive threat to almost all Web security. This has prompted security-focused organizations to move to Quantum-Safe cryptography. Stored encrypted data can be decrypted, after the development of proper technology. Diverging from the use of mathematical problems for security, Quantum Cryptosystems use the rules of physics to secure the algorithms. These security features are enforced by theorems such as the Heisenberg uncertainty principle and the No-Cloning theorem. Quantum computing functions on a different logic from classical computation systems, the boolean model is preserved since results are outputted in a classical format. The operations however differ completely due to its properties of superposition and entanglement. This induces the need for reversible counterparts of classical gates, as well as new gates altogether. They remain unbreakable in an ideal scenario. These cryptosystems aim to produce an OTP, which as dictated by the information theory is unbreakable. The technology is in very early stages and therefore doesn't pose a huge threat. It is estimated that fully working quantum computers will be produced within a few decades, giving a rough deadline for the disruption that will be caused at the time.

References

[1]

C. Pacher *et al.*, ‘Attacks on quantum key distribution protocols that employ non-ITS authentication’, *Quantum Inf Process*, vol. 15, no. 1, pp. 327–362, Jan. 2016, doi: 10.1007/s11128-015-1160-4.

[2]

‘Bayes’ Theorem: What It Is, the Formula, and Examples’, *Investopedia*. https://www.investopedia.com/terms/b/bayes-theorem.asp (accessed Dec. 14, 2022).

[3]

A. Acín, N. Gisin, and V. Scarani, ‘Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks’, *Phys. Rev. A*, vol. 69, no. 1, p. 012309, Jan. 2004, doi: 10.1103/PhysRevA.69.012309.

[4]

Y. Zhao, ‘Development of Quantum Key Distribution and Attacks against It’, *J. Phys.: Conf. Ser.*, vol. 1087, p. 042028, Sep. 2018, doi: 10.1088/1742-6596/1087/4/042028.

[5]

D. Howard, ‘Einstein on locality and separability’, *Studies in History and Philosophy of Science Part A*, vol. 16, no. 3, pp. 171–201, Sep. 1985, doi: 10.1016/0039-3681(85)90001-9.

[6]

A. Barenco *et al.*, ‘Elementary gates for quantum computation’, *Phys. Rev. A*, vol. 52, no. 5, pp. 3457–3467, Nov. 1995, doi: 10.1103/PhysRevA.52.3457.

[7]

F. Xu, B. Qi, and H.-K. Lo, ‘Experimental demonstration of phase-remapping attack in a practical quantum key distribution system’, *New Journal of Physics*, vol. 12, Nov. 2010, doi: 10.1088/1367-2630/12/11/113026.

[8]

Q. C. G. Roorkee IIT, ‘Fundamentals of Quantum Key Distribution — BB84, B92 & E91 protocols’, *Medium*, Sep. 06, 2021. https://medium.com/@qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols-e1373b683ead (accessed Nov. 24, 2022).

[9]

C. Padró, Ed., *Information Theoretic Security*, vol. 8317. Cham: Springer International Publishing, 2014. doi: 10.1007/978-3-319-04268-8.

[10]

J. von Neumann, *Mathematical Foundations of Quantum Mechanics: New Edition*. Princeton University Press, 2018.

[11]

D. Bruß, ‘Optimal Eavesdropping in Quantum Cryptography with Six States’, *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, Oct. 1998, doi: 10.1103/PhysRevLett.81.3018.

[12]

P. W. Shor, ‘Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer’, *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[13]

M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, 10th anniversary ed. Cambridge ; New York: Cambridge University Press, 2010.

[14]

N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, ‘Quantum Cryptography’, *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[15]

N. Datta and D. Cambridge, ‘QUANTUM INFORMATION & COMPUTATION’, p. 8.

[16]

A. Peres and D. R. Terno, ‘Quantum information and relativity theory’, *Reviews of Modern Physics*, vol. 76, no. 1, pp. 93–123, Jan. 2004, doi: 10.1103/revmodphys.76.93.

[17]

M. M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2013.

[18]

MR.Asif, ‘Quantum Key Distribution and BB84 Protocol’, *Quantum Untangled*, May 10, 2022. https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5 (accessed Nov. 07, 2022).

[19]

M. Bourennane, A. Karlsson, G. Bj rk, N. Gisin, and N. J. Cerf, ‘Quantum key distribution using multilevel encoding: security analysis’, *J. Phys. A: Math. Gen.*, vol. 35, no. 47, pp. 10065–10076, Nov. 2002, doi: 10.1088/0305-4470/35/47/307.

[20]

H.-K. Lo, M. Curty, and K. Tamaki, ‘Secure Quantum Key Distribution’, *Nature Photon*, vol. 8, no. 8, pp. 595–604, Aug. 2014, doi: 10.1038/nphoton.2014.149.

[21]

‘The Atoms of Computation’. https://learn.qiskit.org (accessed Dec. 13, 2022).

[22]

D. Gottesman, ‘The Heisenberg Representation of Quantum Computers’. arXiv, Jul. 01, 1998. Accessed: Dec. 12, 2022. [Online]. Available: http://arxiv.org/abs/quant-ph/9807006