Applications of No-Cloning Theorem: Approximate Cloning Machines and Quantum Protocols

A Major Qualifying Project
Submitted to the Faculty of
WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the
Degree of Bachelor of Science in

Physics
and
Mathematical Sciences
by:

Daniil Volkov
Yonglong Zhan

March 2022

Physics Advisor: Professor P.K. Aravind

Math Advisor: Professor Darko Volkov

Abstract

This report studies a number of quantum cloning machines, motivated by their relevance to the field of quantum cryptography. Following a review of basic notions, the report looks at the Buzek-Hillery cloning machine and its generalizations using an approach due to Werner. With this background, an attack on the BB84 protocol by a particular type of cloning machine is considered and a security criterion for the protocol under such an attack is derived.

Acknowledgements

Our sincere gratitude goes to all of our friends in the physics lounge in Olin Hall that endured our bickering about the math even though that clearly distracted them from their work. All the late nights we had worked on this project were that much more manageable due to the incredible support from Ryan Hanna, Patrick O'Mullan, Ana "Gaby" Cano and Morgan Kaler for which we are incredibly grateful. Additional thanks goes to Dana White who provided entertainment every Saturday of the pandemic allowing a sense of normalcy to remain.

Most importantly, we would like to express our deepest gratitude to Professor P.K. Aravind for taking us on this fantastic journey of Quantum Mechanics since sophomore year. His incredible patience allowed us to create work that we can be proud of and it definitively would not have been possible without his advice. His efforts to push us to improve in every single aspect of scientific writing have made a great impact for which we are extremely grateful.

Table of Contents

List of Figures

List of Tables

1 Introduction

The discovery of Shor's algorithm[12] in 1994 has proven the value of quantum mechanics in the field of cryptography. Shor's algorithm, with its ability to efficiently factor large numbers into primes, could jeopardise the security of current encryption schemes. However, at the same time that it makes conventional cryptography unsafe, quantum mechanics is also capable of encrypting data, with the security being guaranteed by the laws of physics. It is the purpose of this project to convey some understanding of how this can be done.

One of the main tasks of quantum cryptography is to allow two distant parties to create a secret key by exchanging quantum particles. The information is encoded in the values of the spin of the particles, where the measuring of the spin allows the receiving party to create a series of bits of 0s and 1s (for spin 1/2 particles). This key can then be used to encrypt and decrypt messages in the usual way.

In conventional cryptography, an eavesdropper who can intercept information in transit can copy it without being detected and use that information to extract the secret key. Quantum mechanics is governed by the no-cloning theorem, which states that it is impossible to produce a perfect clone of an arbitrary quantum state. It is important to note that the no-cloning theorem does not imply that it is impossible to clone an arbitrary state, only that it is impossible to clone it perfectly. An eavesdropper therefore cannot decipher the information encoded in the state perfectly, and at the same time also disturbs it in an uncontrollable way and thus risks detection. An understanding of how all this comes about is conveyed in this report.

This report will study the $1 \to 2$ cloning machine by Buzek and Hillery [2], which allows an arbitrary state of a qubit to be reproduced as two identical, but imperfect, copies of the original. Following this, a $N \to M$ cloning machine for qudits (or d-state quantum systems) is explored using an approach originally discovered by Werner [6] concluding with the calculation of the clones' fidelity.

Quantum key distribution is a successful technique because it is possible to detect and correct for the presence of an eavesdropper. This is possible because there is no such thing as a passive observation on a quantum system. On the contrary, an observation generally changes the state of the system without a way to recover the original state. Quantum mechanics suggests ways of quantifying the disturbance caused by an eavesdropper, and provided this disturbance does not exceed a critical value there are ways of correcting for it and obtaining a secure key. This report will examine a particular protocol for key exchange developed by Bennett and Brassard [1] and see how secure it is under a particular type of attack.

The plan of this report is as follows. Ch.2 reviews some basic notions related to qubits and systems of qubits that are used in the rest of the report. Ch.3 introduces the Bennett-Brassard protocol for quantum key exchange (also known as BB84) that is in wide use today. Ch.4 gives two different proofs of the no-cloning theorem

that demonstrates the impossibility of cloning an arbitrary quantum state perfectly. Ch.5 discusses a family of approximate cloning machines that are generalizations of the $1 \rightarrow 2$ machine proposed originally by Buzek and Hillery. Ch.6 discusses a number of attacks that can be launched on the BB84 protocol using a simple type of cloning machine and examines how secure it is under each of the attacks. Finally Ch.7 contains some concluding remarks.

2 Review on Qubits and Other Basic Concepts

2.1 Qubits and Bloch Sphere

In information theory, the bit is a binary digit that represents the smallest amount of data that can be stored in a computer. In this chapter we will introduce a similar concept in the quantum theory, the qubit. The difference between a qubit and a classical bit is that a classical bit can only be one of the two distinct states 1 or 0, whereas, a qubit can be in a superposition of such states with complex amplitudes. Let $|0\rangle$ and $|1\rangle$ be an orthonormal pair of states satisfying the conditions such that $\langle i|j\rangle = \delta_{i,j}$, then, the most general quantum state can be written in terms of them as:

$$\begin{aligned} &|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,,\ a,b \in \mathbb{C} \\ &|a|^2 + |b|^2 = 1. \end{aligned} \tag{2.1}$$

Let us introduce spherical coordinates $\varphi \in [0, 2\pi)$ and $\theta \in [0, \pi]$. We can connect θ and φ to the complex amplitudes a and b via the following equation: $a = \cos\frac{\theta}{2}$, $b = \sin\frac{\theta}{2}e^{i\varphi}$. For the normalization in Eq.(2.1), we set $a \in \mathbb{R}$ and therefore, $0 \leq a \leq 1$. With this parameterization, the state Eq.(2.1) can be represented by the point with spherical coordinates (θ,φ) on a unit sphere, known as the Bloch sphere.

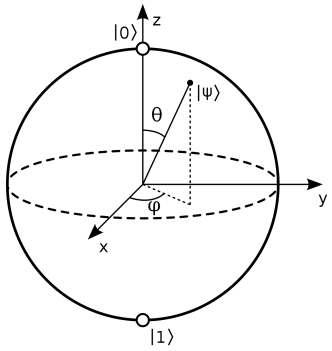

Figure 1: The position of the vector $|\psi\rangle$ in the Bloch sphere is defined by θ and φ.

It may seem counterintuitive that the half angle $\frac{\theta}{2}$ occurs in the expressions for a and b, but it is necessary in order to have a unique correspondence between the states in Eq.(2.1) and points on the Bloch sphere.

2.2 Pauli Operators

The spin operator of a spin-half particle has the components $S_i = \frac{\hbar}{2}\sigma_i$, i=x,y,z, where the Pauli matrices occurring in this expression are given by:

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.2}$$

$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{2.3}$$

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.4}$$

These matrices all have eigenvalues of +1 or -1, and their eigenstates corresponding to these eigenvalues are shown in the table below.

Pauli Matrices	Eigenvectors
σ_x	$\lvert+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $\lvert-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
σ_y	$\lvert\uparrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \end{pmatrix}$, $\lvert\downarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \end{pmatrix}$
σ_z	$\lvert 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\lvert 1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Table 1: Pauli Matrices and their corresponding eigenvectors.

As an application, we will calculate the average spin along the Z axis of the arbitrary state Eq.(2.1).

$$\begin{aligned} \langle Z \rangle &= \langle \psi | \, \sigma_z \, | \psi \rangle \\ &= \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= |a|^2 - |b|^2 \\ &= P_+ - P_- \end{aligned} \tag{2.5}$$

the final line of the Eq.(2.5) is the probability of finding the particle spin up along the Z-axis minus the probability of spin down, which is exactly the definition of the average spin along the Z axis (in units of $\frac{\hbar}{2}$). In fact, one can calculate the average value of the spin along the unit vector $\hat{u}$ for a particle in the state Eq.(2.1) as the expectation value of the operator:

$$\vec{\sigma} \cdot \hat{u} = u_x \sigma_x + u_y \sigma_y + u_z \sigma_z. \tag{2.6}$$

For any pure state, like in Eq.(2.1), one can define density matrix, $\boldsymbol{\rho}$, via the equation $\boldsymbol{\rho} = |\phi\rangle\langle\phi|$. Using Eq.(2.1) and a bit of algebra, one can show that the density matrix $\boldsymbol{\rho}$ can be written as:

$$\boldsymbol{\rho} = \frac{1}{2}(I + \vec{s} \cdot \vec{\sigma}) \tag{2.7}$$

where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is a vector composed of the Pauli matrices, I is a 2x2 identiy matrix and $\hat{s} = (\sin(\theta)\cos(\phi), \sin(\theta)\sin(\phi), \cos(\theta))$ is a unit vector. Note that $\hat{s}$ picks a point on the Bloch sphere to represent a pure state, and its Cartesian components represents the average values of the spin along the coordinates axes in this state.

Now that we have a general operator that measures the average spin in an arbitrary direction, we can derive the operator that measures the probability of finding spin up state. We can use Eq.(2.5) to calculate the average value of the spin in an arbitrary direction and the probability of finding the spin up or down along that direction when the particle is in the state Eq.(2.1). We find that:

$$\begin{aligned}
&\langle S\rangle = \langle\psi|\,\vec{\sigma}\cdot\hat{u}\,|\psi\rangle = P_+ - P_- \\
&P_- = 1 - P_+, \text{ because the sum of the probabilities is unity} \\
&\langle\psi|\,\sigma\cdot u\,|\psi\rangle = 2P_+ - 1 \\
&P_+ = \frac{\langle\psi|\,\vec{\sigma}\cdot\hat{u}\,|\psi\rangle + 1}{2} = \langle\psi|\,\frac{I + \vec{\sigma}\cdot\hat{u}}{2}\,|\psi\rangle
\end{aligned} \tag{2.8}$$

P_- follows exactly the same, so we get

$$P_- = \langle\psi|\,\frac{1 - \vec{\sigma}\cdot\hat{u}}{2}\,|\psi\rangle\,. \tag{2.9}$$

There are two more properties of Pauli matrices that one will find useful later in the report:

$$\sigma_i^2 = I \tag{2.10}$$

$$\sigma_i \cdot \sigma_j = \delta_{ij} I + i\varepsilon_{ijk}\delta_k. \tag{2.11}$$

Notice that i is imaginary number $(0, i)$ while ε_{ijk} is a three dimension Levi-Citiva symbol, such that $\varepsilon_(ijk) = 1$ when $(i, j, k) = (1, 2, 3), (2, 3, 1) or (3, 1, 2)$, $\varepsilon_(ijk) = -1$ when $(i, j, k) = (3, 2, 1), (1, 3, 2) or (2, 1, 3)$ and $\varepsilon = 0$ when $i = j, j = k$ or $k = i$.

2.3 Two Qubit System

We now introduce a system of two qubits, which plays an important role in the later chapters of this report.

We can use the basis of the individual qubits to create a basis for the entire system by applying the notion of tensor product. The most general pure state of a two qubit system can be expressed as:

$$|\psi\rangle = c_{00}\,|00\rangle + c_{01}\,|01\rangle + c_{10}\,|10\rangle + c_{11}\,|11\rangle\,, \tag{2.12}$$

where $|00\rangle = |0\rangle_A\,|0\rangle_B$ is the tensor product of the state $|0\rangle$ of qubit A and the state $|0\rangle$ of qubit B, with the state $|01\rangle$, $|10\rangle$, and $|11\rangle$ being similarly interpreted. These four states form the computational basis for a system of two qubits, and any pure state of two qubits can be expressed as a superposition of them with arbitrary coefficients, as in Eq.(2.12).

An alternative basis for a system of two qubits is the Bell basis defined below:

$$\begin{aligned}
\left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
\left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
\left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
\left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned} \tag{2.13}$$

We could rewrite the state from Eq.(2.12) in the Bell basis with different coefficients:

$$|\psi\rangle = b_{00}\left|\Phi^+\right\rangle + b_{10}\left|\Phi^-\right\rangle + b_{01}\left|\Psi^+\right\rangle + b_{11}\left|\Psi^-\right\rangle. \tag{2.14}$$

Unlike Eq.(2.12), the states of the Bell basis are all entangled states. An entangled state of two qubit is one in which the properties of the qubits are tightly correlated. The Bell basis offers an advantage over the computational basis in the analysis of some problems, as we will see later in this report.

2.4 Mixed States

A pure state of a qubit is any state that can be expressed in the form of Eq.(2.1), but there is an even more general expression for quantum system, the mixed state. One way in which a mixed state can arise is if we prepare the system in a probabilistic combination of pure states. Unlike in the case of pure states, it is impossible to assign a single state vector to such an ensemble.

For example, consider the following system that has a probability of $\frac{1}{2}$ to be in state up along z and probability of $\frac{1}{2}$ to be down along z:

$$\phi_{mixed} = (P = \frac{1}{2}) \left|0\right\rangle + (P = \frac{1}{2}) \left|1\right\rangle . \tag{2.15}$$

It is very easy to confuse this system with a simple state vector:

$$\left|+x\right\rangle = \frac{1}{\sqrt{2}} \left|0\right\rangle + \frac{1}{\sqrt{2}} \left|1\right\rangle . \tag{2.16}$$

Indeed, the average spin along z of systems described in Eq.(2.15) and Eq.(2.16) are the same:

$$\begin{aligned} &< \sigma_z >_{mixedstate} = \frac{1}{2} \left\langle 0\right| \sigma_z \left|0\right\rangle + \frac{1}{2} \left\langle 1\right| \sigma_z \left|1\right\rangle = \frac{1}{2} - \frac{1}{2} = 0 \\ &< \sigma_z >_{+x} = (\frac{1}{\sqrt{2}} \left\langle 0\right| + \frac{1}{\sqrt{2}} \left\langle 1\right|)|\sigma_z|(\frac{1}{\sqrt{2}} \left|0\right\rangle + \frac{1}{\sqrt{2}} \left|1\right\rangle) = \frac{1}{2} - \frac{1}{2} = 0 \end{aligned} \tag{2.17}$$

The difference between Eq.(2.15) and Eq.(2.16) described above is that $\left|+x\right\rangle$ is an eigenstate of the σ_x operator and will always produce eigenvalue of 1. Let us now try to find a similar direction for the mixed state. To keep matters simple, we will use inner product to calculate the probabilities and show that the average spin will remain 0 in any direction.

First, we will calculate the probability of getting the particle spin up in a random direction.

$$\begin{aligned} &\left|\psi_{random}\right\rangle = a \left|0\right\rangle + b \left|1\right\rangle \\ &P(+) = \frac{1}{2}|(\left\langle 0\right| (a \left|0\right\rangle + b \left|1\right\rangle))|^2 + \frac{1}{2}|(\left\langle 1\right| (a \left|0\right\rangle + b \left|1\right\rangle))|^2 = \\ &\frac{1}{2}|a|^2 + \frac{1}{2}|b|^2 = \frac{1}{2} \end{aligned} \tag{2.18}$$

The total probability is unity, so the probability of getting the particle spin down is $1 - \frac{1}{2} = \frac{1}{2}$. Notice this number is independent of the choice for a or b, so it will remain constant for any possible pure state vector. Hence, the average value of the spin is going to remain $1 \cdot \frac{1}{2} - 1 \cdot \frac{1}{2} = 0$, which is what we were trying to show.

We can also express mixed states on the Bloch sphere in a similar way to the pure states. The difference is that the mixed states will be inside of the Bloch sphere instead of being on the surface.
We can see the result of Eq.(2.18) without any calculations by using Bloch Sphere representation and notice that the average spin will be 0 in any direction simply based on the fact that $\forall \vec{u} : \vec{u} \cdot \vec{0} = 0$.

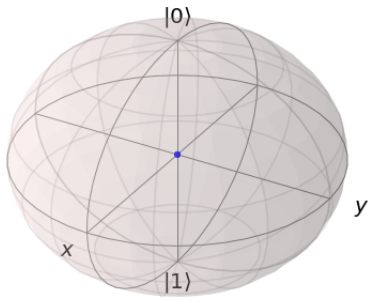

Figure 2: Bloch sphere with the point in the origin representing Eq.(2.15)

As shown earlier, there cannot be a pure state vector that would work with system Eq.(2.15). Instead, we will use the operator form also known as density matrix or tensor:

$$\boldsymbol{\rho} = \frac{1}{2}\left|0\right\rangle\!\left\langle 0\right| + \frac{1}{2}\left|1\right\rangle\!\left\langle 1\right| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.19}$$

Now we can use the density matrix to show another way of calculating the average value of spin. Mathematically, the operations are equivalent, but the Eq.(2.19) uses linear algebra to simplify some steps.

$$\begin{aligned} &\left|\psi\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle \\ &\left\langle\psi\right|\boldsymbol{\rho}\left|\psi\right\rangle = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \\ &= \frac{1}{2}|a|^2 + \frac{1}{2}|b|^2 = \frac{1}{2} \end{aligned} \tag{2.20}$$

the rest of the argument will follow the same steps of the Eq.(2.18).

Having defined the notion of a mixed state, let us list all the properties of the density operator for such a state. These properties will be needed in the chapters to follow.

1. As shown earlier we can create a mixed state by combining multiple pure states with assigned probabilities, in addition, we can do that with mixed states as well, and the result will remain a mixed state:

$$\boldsymbol{\rho} = \sum_{i=1}^{j}\left|\psi_i\right\rangle\!\left\langle\psi_i\right| + \sum_{k=1}^{l}\boldsymbol{\rho}_k.$$

2. Density matrix will have a form of 2 x 2 Hermitian matrix with a unit trace.

3. Density matrix in the space of a single qubit will have two eigenvalues, each greater than or equal to zero. If it has only a single eigenvalue (equal to 1) it is a pure state, whereas if it has two nonzero eigenvalues it is a mixed state.

4. For a mixed state, the eigenvalues of the density matrix define a pair of probabilities and their eigenvectors as a pair of orthogonal pure states. The mixed state can be regarded as a mixture of the pure states (corresponding to the eigenvectors), weighted by their probabilities (the eigenvalues).

5. We saw earlier that a pure state is represented by a point on the Bloch sphere. A similar calculation shows that a mixed state is represented by a point in the interior of the Bloch sphere.

6. The expectation value of the observable A in the mixed state described by the density operator $\boldsymbol{\rho}$ is given by $< A >= \mathrm{Tr}(\boldsymbol{\rho} A)$

3 Quantum Cryptography Protocols BB84

3.1 Background on BB84

Most modern cryptographic protocols rely on the use of a secret key to encrypt and decrypt messages in a secure fashion known only to the two parties involved. Establishing a secret key is the most challenging aspect of this scheme and that is where the unique features of quantum mechanics can be used to advantage.

The first quantum protocol for establishing a secret key between two parties was proposed by Charles Bennett and Gilles Brassard [1] in 1984 and is now known after them as BB84. This protocol allows two separated parties, Alice and Bob, to establish a secret key known only to them and a way to detect infiltrators.

3.2 Process of BB84

Alice begins the protocol by generating two random strings of bits, the basis string and the parent string. The parent string is a series of 0s and 1s, and the basis string is a series of Zs and Xs.

For each choice of entries in the basis and parent strings, Alice encodes her qubit in the manner indicated in the table blow.

basis	parent	qubit state
Z	0	$\|0\rangle$
Z	1	$\|1\rangle$
X	0	$\|+\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
X	1	$\|-\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$

Table 2: The correlating relationship between prepared by Alice for transmission to Bob.

Then table (3) below illustrates how the protocol works, beginning with Alice's preparation of her qubits (the first three rows of the table), then Bob's measurements (next two rows) and finally his attempt to reconstructing Alice's parent string (last three rows).

Alice's Basis String	Z	Z	X	Z	X	X	Z	Z	Z
Alice's Parent String	1	1	0	1	1	0	1	0	0
Qubit States	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
Bob's Basis String	X	Z	X	X	Z	Z	Z	X	Z
Bob's Result	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
Bob's Parent String	0	1	0	1	0	0	1	0	0
Right Basis?	No	Yes	Yes	No	No	No	Yes	No	Yes
Key String N/A	N/A	1	0	N/A	N/A	N/A	1	N/A	0

Table 3: An Example of BB84 Protocol. In this particular case the key will consist of just four elements out of the nine elements in Alice's parent string.

Once Bob gets Alice's qubits, he measures each according to a random sequence of Zs and Xs that he chooses for his basis string. If he guesses the basis correctly, then he will be guaranteed to get the correct parent bit. However, if he selected the wrong measurement basis for the qubit, he would still have a 50 percent chance of getting the right parent bit.

Bob then communicates with Alice over a public channel, telling her his choice of basis for each of the measurements and Alice tells him which measurements were done correctly. Bob will then discard the measurements done in the incorrect basis and the portion of Alice's parent string he infers from the remaining measurements match her string perfectly. However, one sees that Bob discards some correct key bits in this process. Unfortunately, the discarded bits cannot be used since it is impossible to guarantee their accuracy.

3.3 General comments on BB84

Security protocols are created to minimize the risk of the information being obtained by an adversary. So how does BB84 hold up? Well, if an interceptor, we shall call her Eve, gets access to the qubits, could she not just copy the qubits and wait for Alice to reveal the correct basis before she measures them? It turns out that it is impossible to make a perfect copy of an unknown qubit (we will discuss this in detail in the next chapter) and that any attempt to do so will disturb it in an unpredictable way. Eve's interference inevitably leads to errors in the secret key. Knowing that, Alice and Bob have a reliable way of detecting interference and correcting for it.

4 No-Cloning Theorem

In this chapter we will discuss a fundamental theorem of quantum cryptography that has deep implications for the security of quantum key-distribution protocols, the no-cloning theorem. The no-cloning theorem states that it is impossible to produce a perfect clone of an arbitrary quantum state while also preserving the original state undisturbed.

4.1 First Proof of No Cloning Theorem

The is a proof by contradiction and it was first discovered by Wootters and Zurek[13]. The proof is based on the linearity of unitary transformations. So let us assume that a perfect cloning machine $|M\rangle$ exists that is able to produce copies of the two orthogonal states $|0\rangle$ and $|1\rangle$ of a qubit. The entire machine consists of three parts: the qubit to be copied, a qubit in a blank state $|B\rangle$ and the machine in its original state $|M_B\rangle$. If the state $|1\rangle$ is put into the machine to be copied, the machine will perform the following transformation:

$$|1\rangle\,|B\rangle\,|M\rangle \longrightarrow |1\rangle\,|1\rangle\,|M(1)\rangle\,. \tag{4.1}$$

If we feed the state $|0\rangle$ into the machine it yields the output:

$$|0\rangle\,|B\rangle\,|M\rangle \longrightarrow |0\rangle\,|0\rangle\,|M(0)\rangle\,. \tag{4.2}$$

Note that $|M(0)\rangle$ and $|M(1)\rangle$ are different states, because the final state of the machine must reflect the difference in inputs.

If one feeds the state $|+x\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ (i.e. the spin up state along x axis) into the machine, the linearity of unitary transformations along with Eq.(4.2) and Eq.(4.3) predict that the output of the machine will be:

$$\begin{aligned} |+x\rangle\,|B\rangle\,|M\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,|B\rangle\,|M\rangle \\ &= \frac{1}{\sqrt{2}}\,|0\rangle\,|B\rangle\,|M\rangle + \frac{1}{\sqrt{2}}\,|1\rangle)\,|B\rangle\,|M\rangle \\ &\to \frac{1}{\sqrt{2}}\,|0\rangle\,|0\rangle\,|M(0)\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|1\rangle\,|M(1)\rangle\,. \end{aligned} \tag{4.3}$$

But the state $|+x\rangle$ is also a pure state, so the perfect cloning machine should be able to clone it directly:

$$\begin{aligned} |+x\rangle\,|B\rangle\,|M\rangle &\to |+x\rangle\,|+x\rangle\,|M(+x)\rangle \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|M(+x)\rangle\,. \end{aligned} \tag{4.4}$$

In the last line of Eq.(4.4), we used Eq.(2.16) to expand $|+x\rangle$ in the standard z basis representation.

Clearly Eq.(4.3) have two more terms than Eq.(4.4), which means that there are two more possible outcomes than the latter. Therefore, the perfect cloning machine does not work. We see that even if a cloning machine is able to clone two orthogonal states perfectly, linearity prevents it from cloning an arbitrary superposition of these states perfectly.

4.2 Second Proof of No Cloning Theorem

The second proof was discovered by Dieks[4], and it shows a contradiction by attempting to clone non-orthogonal states, so let $|\psi\rangle$ and $|\phi\rangle$ be two states such that

$$0 < \langle\phi|\psi\rangle < 1. \tag{4.5}$$

In the larger Hilbert space that also includes the blank qubit and the state of the machine, these states will have the form:

$$\begin{aligned} |\Psi\rangle &= |\psi\rangle\,|B\rangle\,|M\rangle \\ |\Phi\rangle &= |\phi\rangle\,|B\rangle\,|M\rangle\,, \end{aligned} \tag{4.6}$$

where $|B\rangle$ is the blank qubit and $|M\rangle$ is the initial state of the cloning machine.

We are assuming that a perfect cloning machine exists that can apply the same unitary transformation U_c to clone any initial state. Thus, it will transform the two different input states in Eq.(4.6) as follows:

$$\begin{aligned} |\Psi'\rangle &= U_c\,|\Psi\rangle = |\psi\rangle\,|\psi\rangle\,|M_\psi\rangle \\ |\Phi'\rangle &= U_c\,|\Phi\rangle = |\phi\rangle\,|\phi\rangle\,|M_\phi\rangle\,. \end{aligned} \tag{4.7}$$

From Eq.(4.6) it follows that $|\langle\Phi|\Psi\rangle| = |\langle\phi|\psi\rangle|$. As U_c is a unitary operators, it reserves inner products. So we see from Eq.(4.7) that it is equivalent to Eq.(4.6):

$$|\langle\Psi'|\Phi'\rangle| = |\langle\Psi|\Phi\rangle| = |\langle\psi|\phi\rangle|. \tag{4.8}$$

However, if we expand the first inner product in Eq.(4.8) using the final expression of Eq.(4.7) we find that:

$$|\langle\Psi'|\Phi'\rangle| = |\langle\psi|\phi\rangle|^2|\langle M_\psi|M_\phi\rangle| \leq |\langle\psi|\phi\rangle|^2 < |\langle\psi|\phi\rangle|. \tag{4.9}$$

The third step in Eq.(4.9) follows because $|\langle M_\phi | M_\psi \rangle| \leq 1$ and the last step follows because $x^2 < x$ if $x \in (0,1)$. However, Eq.(4.9) is in disagreement with Eq.(4.8), which demonstrates that a perfect cloning machine is impossible for states satisfying $|\langle \phi | \psi \rangle|^2 < 1$. Perfect cloning is possible only if $|\langle \phi | \psi \rangle|^2 = 0$ or 1, that is, the states are either identical or orthogonal.

5 Approximate Cloning Machines

In this chapter, we will introduce various cloning machines, particularly, the Buzek Hillary optimal $1 \rightarrow 2$ cloning machine as well as a generalization of it introduced by Werner.

In chapter 4 we showed that a perfect cloning machine of arbitrary state is not possible. However, there is no reason why approximate cloning machines cannot exist, and they in fact have interesting applications so we will explore them in this chapter. A good measure of the quality of a cloning machine is its fidelity, defined as:

$$\begin{aligned} F_j &= \langle \Psi | \, \boldsymbol{\rho}_j \, | \Psi \rangle \\ j &= 1, 2, .., M \end{aligned} \tag{5.1}$$

here Ψ is the original input to be cloned, $\boldsymbol{\rho}_j$ is the density matrix of one of the identical clones that is produced.

5.1 Trivial Cloning

Before we discuss more complicated procedures of partially replicating quantum states, let us introduce a simple way of making a copy of a given state that might be called trivial cloning [9]. Trivial cloning will be done by randomly choosing a direction, measuring the spin of the unknown state along that direction and creating two states that are both identical to the output of that measurement.

Let us suppose that we are trying to clone the pure state $|\psi\rangle$, in which the particle has its spin up along $\hat{a}$ on the Bloch sphere. This state is an eigenvector of $\hat{a} \cdot \vec{\sigma}$ with the eigenvalue $+1$. Our cloning strategy is to measure the spin along the arbitrary direction $\hat{b}$ and to prepare the qubit in the spin-up or spin-down state along this direction. Let us denote the eigenstates of $\hat{b} \cdot \vec{\sigma}$ with eigenvalues $+1$ and -1 as ϕ_+ and ϕ_-, respectively:

$$\begin{aligned} (\hat{a} \cdot \vec{\sigma}) \, |\psi\rangle &= |\psi\rangle \\ (\hat{b} \cdot \vec{\sigma}) \, |\phi_+\rangle &= |\phi_+\rangle \\ (\hat{b} \cdot \vec{\sigma}) \, |\phi_-\rangle &= - \, |\phi_-\rangle \, . \end{aligned} \tag{5.2}$$

We will now use Eq.(2.8) particle to calculate the probability of finding the particle in the spin up state along b:

$$
\begin{aligned}
P_+ &= \langle\phi_+| \frac{I + \hat{a}\cdot\vec{\sigma}}{2} |\phi_+\rangle \\
&= \frac{1}{2} + \langle\phi_+| \frac{\hat{a}\cdot\vec{\sigma}}{2} |\phi_+\rangle \\
&= \frac{1}{2} + \langle\phi_+| \frac{(\hat{a}\cdot\vec{\sigma})(\hat{b}\cdot\vec{\sigma})}{2} |\phi_+\rangle \\
&= \frac{1}{2} + \frac{\langle\phi_+| (\hat{a}\cdot\hat{b}) I |\phi_+\rangle}{2} + i\frac{\langle\phi_+| (\hat{a}\times\hat{b})\cdot\vec{\sigma} |\phi_+\rangle}{2} \\
&= \frac{1+\hat{a}\cdot\hat{b}}{2}
\end{aligned}
\tag{5.3}
$$

where we used Eq.(2.11) to expand $(\hat{a}\cdot\vec{\sigma})(\hat{b}\cdot\vec{\sigma})$. Second term in the fourth line will produce $\hat{a}\cdot\hat{b}$ and the third term is 0, because it is equivalent to measuring the average spin in a perpendicular direction, which is always 0. We can use the same procedure to derive the probability for $|\phi_-\rangle$:

$$
P_- = \frac{1-\hat{a}\cdot\hat{b}}{2}. \tag{5.4}
$$

Now we are ready to calculate fidelity of the copy using Eq.(5.1). For pure states it simplifies down to the inner product, so for given $\hat{a}, \hat{b}$.

$$
\begin{aligned}
F &= F_+P_+ + F_-P_- \\
&= \Big(\frac{1-\hat{a}\cdot\hat{b}}{2}\Big)^2 + \Big(\frac{1+\hat{a}\cdot\hat{b}}{2}\Big)^2 \\
&= \frac{1-\hat{a}\cdot\hat{b}+(\hat{a}\cdot\hat{b})^2+1+\hat{a}\cdot\hat{b}+(\hat{a}\cdot\hat{b})^2}{4} \\
&= \frac{1+(\hat{a}\cdot\hat{b})^2}{2}
\end{aligned}
\tag{5.5}
$$

We will need to integrate over all possible values of on the Bloch sphere and average it out. So we get the fidelity equal to:

$$
\begin{aligned}
F_{average} &= \int F_b dp_b = \int \frac{1+(\hat{a}\cdot\hat{b})^2}{2} dp_b \\
&= \frac{1}{2}\int dp_b + \frac{1}{8\pi}\int (\hat{a}\cdot\hat{b})^2 d\Omega \\
&= \frac{1}{2} + \frac{1}{8\pi}\int (\hat{a}\cdot\hat{b})^2 d\Omega.
\end{aligned}
\tag{5.6}
$$

We are varying b, so let us first introduce spherical angles on the Bloch Sphere, such that $\hat{a} = (\theta_0, \phi_0), \hat{b} = (\theta, \phi)$. We now will express the variables $\hat{a}, \hat{b}$ through the two polar angles in Cartesian coordinates to then evaluate the dot product and the integral:

$$
\begin{aligned}
\hat{a} &= < cos(\theta_0), sin(\theta_0)sin(\phi_0), sin(\theta_0)cos(\phi_0) > \\
\hat{b} &= < cos(\theta), sin(\theta)sin(\phi), sin(\theta)cos(\phi) > \\
F_{average} &= \frac{1}{2} + \frac{1}{8\pi}\int (\hat{a}\cdot\hat{b})^2 d\Omega \\
&= \frac{1}{2} + \frac{1}{8\pi}\int_0^{2\pi}\int_0^{\pi} \Big(cos(\theta)cos(\theta_0) + \sin(\theta)\sin(\theta_0)\cos(\phi-\phi_0)\Big)^2 \sin(\theta)\ d\theta d\phi \\
&= \frac{1}{2} + \frac{1}{8\pi}\int_0^{2\pi}\int_0^{\pi} \cos^2(\theta)\cos^2(\theta_0)\sin(\theta)\ d\theta d\phi \\
&+ \frac{1}{8\pi}\int_0^{2\pi}\int_0^{\pi} 2\cos(\theta)\cos(\theta_0)\sin(\theta)\sin(\theta_0)\cos(\phi-\phi_0)\sin(\theta)\ d\theta d\phi \\
&+ \frac{1}{8\pi}\int_0^{2\pi}\int_0^{\pi} \sin^2(\theta)\sin^2(\theta_0)\cos^2(\phi-\phi_0)\sin(\theta)\ d\theta d\phi \\
&= \frac{1}{2} + \frac{1}{8\pi}\frac{4\pi}{3}cos^2(\theta_0) + 0 + \frac{1}{8\pi}\frac{4\pi}{3}sin^2(\theta_0) \\
&= \frac{1}{2} + \frac{1}{6} \\
&= \frac{2}{3}.
\end{aligned}
\tag{5.7}
$$

This result could have been obtained more simply by taking $\theta_0 = 0$ before doing the averaging. The reason this works is due to the isotropy of the Bloch sphere.

5.2 Buzek-Hillery(BH) Cloning Machine

In this subsection we will introduce the Buzek-Hillery cloning machine [2]. It is a $1 \to 2$ cloning machine that performs a unitary transformation of the input state, with the blank and the machine states entangling them in such a way that gives out two approximate copies of the input state. We will first examine the operation with a slight generalization of the Buzek-Hillery cloning machine as this will give us a better feeling for the performance of the actual Buzek-Hillery cloning machine.

5.2.1 Generalized Buzek-Hillery Cloning Machine

We can define generalized Buzek-Hillery cloning machine by specifying how it transforms the basis states: $|0\rangle$, and $|1\rangle$. When the cloning machine takes in the state $|0\rangle$, it transforms it in the following way:

$$|0BM\rangle \to \cos(\theta)\,|001\rangle - \sin(\theta)\,\left|\psi^+\right\rangle|0\rangle\,. \tag{5.8}$$

On the other hand, if we input $|1\rangle$ into the cloning machine, its action is described by:

$$|1BM\rangle \to -\cos(\theta)\,|110\rangle + \sin(\theta)\,\left|\psi^+\right\rangle|1\rangle\,. \tag{5.9}$$

In Eq.(5.8) and Eq.(5.9), $|B\rangle$ represents the blank state, $|M\rangle$ is the initial state of the cloning machine and the bell state $|\psi^+\rangle$ was defined earlier in Eq.(2.13). Further, θ represents an arbitrary parameter that we placed in $\cos(\theta)$, $\sin(\theta)$ to make sure that the cloning machine is unitary and trace preserving.

We can now use linearity to examine the cloning process of a general quantum state $|\psi\rangle$, as defined in Eq.(2.1), which transform according to the equation below:

$$\begin{aligned}|\psi BM\rangle &\to \cos(\theta)[a\,|001\rangle - b\,|110\rangle] - \frac{\sin(\theta)}{\sqrt{2}}[a(|110\rangle + |010\rangle) - b(|101\rangle + |110\rangle)] \\ &= \cos(\theta)\,|\phi_1\rangle - \sin(\theta)\,|\phi_2\rangle\,,\end{aligned} \tag{5.10}$$

where $|\phi_1\rangle = a\,|001\rangle - b\,|110\rangle$ and $|\phi_2\rangle = \dfrac{a(|110\rangle + |010\rangle) - b(|101\rangle + |011\rangle)}{\sqrt{2}}$.

The last line of Eq.(5.10) is the output of the cloning machine, and the density matrix corresponding to it will be

$$|\psi BM\rangle\langle\psi BM| = \boldsymbol{\rho} = \cos^2\theta\,|\phi_1\rangle\langle\phi_1| + \sin^2\theta\,|\phi_2\rangle\langle\phi_2| + \cos(\theta)\sin(\theta)(\langle\psi_1|\psi_2\rangle + \langle\psi_2|\psi_1\rangle). \tag{5.11}$$

Now we can evaluate the reduced density matrix in the space of A and B by taking partial trace over standard basis $|0\rangle$ and $|1\rangle$ of qubit M:

$$\boldsymbol{\rho}_{AB} = Tr_M\boldsymbol{\rho} = \langle 0|\,\boldsymbol{\rho}\,|0\rangle + \langle 1|\,\boldsymbol{\rho}\,|1\rangle\,. \tag{5.12}$$

If one expands Eq.(5.12):

$$\boldsymbol{\rho}_{AB} = \cos^2\theta[|\beta|^2|11\rangle\langle 11| + |\alpha|^2|00\rangle\langle 00|] + \sin^2\theta\left|\phi^+\right\rangle\left\langle\phi^+\right| + \sin(\theta)\cos(\theta)[(\alpha^*\beta\,|11\rangle + \alpha\beta^*\,|00\rangle)\left\langle\psi^+\right| + \left|\psi^+\right\rangle(\alpha\beta^*\,\langle 11| + \alpha^*\beta\,\langle 00|)]. \tag{5.13}$$

Eq.(5.13) is a joint density matrix in the space of qubits A and B; however, to evaluate the fidelity of an individual qubit, we need to use partial trace on Eq.(5.13) in the space of A or B. If one looks closely at the expression in Eq.(5.13), one will see that if qubit A and B were switched, the form of the equation does not change. Thus, $\boldsymbol{\rho}_A = \boldsymbol{\rho}_B$.

We will calculate $\boldsymbol{\rho}_A$ by taking a partial trace over the space of qubit B:

$$\begin{aligned}\boldsymbol{\rho}_A &= \langle 0|\,\boldsymbol{\rho}_{AB}\,|0\rangle + \langle 1|\,\boldsymbol{\rho}_{AB}\,|1\rangle \\ &= \cos^2\theta[|\beta|^2|1\rangle\langle 1| + |\alpha|^2|0\rangle\langle 0|] + \frac{1}{2}\sin^2\theta[|1\rangle\langle 1| + |0\rangle\langle 0|] \\ &+ \frac{1}{\sqrt{2}}\sin(\theta)\cos(\theta)[\alpha^*\beta\,|1\rangle\langle 0| + \alpha\beta^*\,|0\rangle\langle 1|].\end{aligned} \tag{5.14}$$

We can rewrite Eq.(5.14) as $\boldsymbol{\rho}_A = \frac{1}{2}(I + \vec{m}\cdot\vec{\sigma})$, where the $i = x, y, z$ components of $\vec{m}$ are given by the equation $\mathrm{Tr}(\sigma_i\boldsymbol{\rho}_A)$:

$$\begin{aligned}m_x &= \mathrm{Tr}(\sigma_x\boldsymbol{\rho}_A) \\ m_x &= \mathrm{Tr}\begin{pmatrix}\sqrt{2}\alpha\beta^*\cos(\theta)\sin(\theta) & \dfrac{2\cos^2(\theta)|\alpha|^2 + \sin^2(\theta)}{2} \\ \dfrac{2\cos^2(\theta)|\beta|^2 + \sin^2(\theta)}{2} & \sqrt{2}\beta\alpha^*\cos(\theta)\sin(\theta)\end{pmatrix}, \\ m_x &= \sqrt{2}\sin(\theta)\cos(\theta)(\alpha\beta^* + \alpha^*\beta)\end{aligned} \tag{5.15}$$

$$
\begin{aligned}
m_y &= Tr(\sigma_y \boldsymbol{\rho}_A) \\
m_y &= Tr \begin{pmatrix} -\sqrt{2}i\alpha\beta^* \sin(\theta)\cos(\theta) & i\dfrac{-\sin^2(\theta) - 2\cos^2(\theta)|\alpha|^2}{2} \\ i\dfrac{\sin^2(\theta) + 2\cos^2(\theta)|\beta|^2}{2} & \sqrt{2}i\beta\alpha^* \sin(\theta)\cos(\theta) \end{pmatrix} \\
m_y &= i\sqrt{2}\sin(\theta)\cos(\theta)(\alpha\beta^* - \alpha^*\beta),
\end{aligned}
\tag{5.16}
$$

$$
\begin{aligned}
m_z &= Tr(\sigma_z \boldsymbol{\rho}_A) \\
m_z &= Tr \begin{pmatrix} \dfrac{2\cos^2(\theta)|\beta|^2 + \sin^2(\theta)}{2} & \sqrt{2}\beta\alpha^* \sin(\theta)\cos(\theta) \\ -\sqrt{2}\alpha\beta^* \sin(\theta)\cos(\theta) & \dfrac{-2\cos^2(\theta)|\alpha|^2 + \sin^2(\theta)}{2} \end{pmatrix} \\
m_z &= \cos^2\theta(|\alpha|^2 - |\beta|^2).
\end{aligned}
\tag{5.17}
$$

If we let $\alpha = \cos\dfrac{(\vartheta)}{2}$ and $\beta = e^{i\varphi}\sin\dfrac{(\vartheta)}{2}$, then Eq.(5.15), Eq.(5.16) and Eq.(5.17) become:

$$m_x = \sqrt{2}\cos(\theta)\sin(\theta)\cos\vartheta\sin\varphi, \tag{5.18}$$

$$m_y = \sqrt{2}\cos(\theta)\sin(\theta)\sin\vartheta\sin\varphi, \tag{5.19}$$

$$m_z = \cos^2\theta\cos\vartheta. \tag{5.20}$$

Note θ is the angle defined in Eq.(5.10) and ϑ is an angle related to the input state ψ.

To calculate the fidelity of this clone, we use Eq.(5.1):

$$
\begin{aligned}
F &= \langle\psi|\,\boldsymbol{\rho}_A\,|\psi\rangle \\
&= \frac{1}{2} + \frac{1}{2}\left(\cos\left(\frac{\vartheta}{2}\right)e^{i\phi}\sin\left(\frac{\vartheta}{2}\right)\right) m_x\sigma_x \left(\cos\left(\frac{\vartheta}{2}\right)e^{i\phi}\sin\left(\frac{\vartheta}{2}\right)\right) \\
&+ \frac{1}{2}\left(\cos\left(\frac{\vartheta}{2}\right)e^{i\phi}\sin\left(\frac{\vartheta}{2}\right)\right) m_y\sigma_y \left(\cos\left(\frac{\vartheta}{2}\right)e^{i\phi}\sin\left(\frac{\vartheta}{2}\right)\right) \\
&+ \frac{1}{2}\left(\cos\left(\frac{\vartheta}{2}\right)e^{i\phi}\sin\left(\frac{\vartheta}{2}\right)\right) m_z\sigma_z \left(\cos\left(\frac{\vartheta}{2}\right)e^{i\phi}\sin\left(\frac{\vartheta}{2}\right)\right).
\end{aligned}
\tag{5.21}
$$

Simplifying the expression for the fidelity allows it to be expressed as:

$$F = \frac{1+m}{2} = \frac{1}{2}[1 + \sqrt{m_x^2 + m_y^2 + m_z^2}]$$
$$= \frac{1}{2} + \frac{\cos(\theta)\sqrt{2\sin^2(\theta)\sin^2(\vartheta) + \cos^2(\theta)\cos^2(\vartheta)}}{2}. \tag{5.22}$$

The graph of the Eq.(5.22) is shown below. Fidelity is a function of two variables: θ describes the nature of the transformation performed by the machine and ϑ characterizes the input state to be copied.

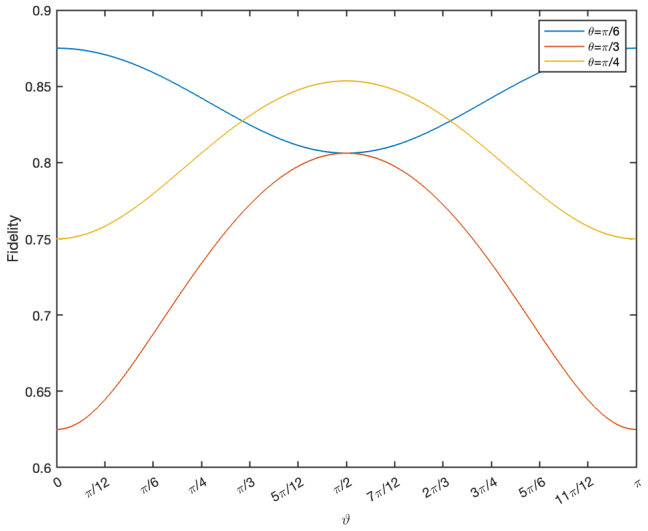

Figure 3: This plot shows the fidelity rate of three different cloning machines when $\theta = \frac{\pi}{3}, \frac{\pi}{4}, \frac{\pi}{6}$. When $\theta = \frac{\pi}{3}$, the cloning machine clones better states that are close to the z-axis, whereas, when $\theta = \frac{\pi}{4}$ and $\theta = \frac{\pi}{6}$ clones better states that are closet o the x axis.

For Eq.(5.22), we consider the three following cases:

1. if $\sin(\theta), \cos(\theta) \neq 0$ and $\cos(\vartheta), \sin(\vartheta) \neq 0$, then

$$\frac{\cos(\theta)\sqrt{2\sin^2(\theta)\sin^2(\vartheta) + \cos^2(\theta)\cos^2(\vartheta)}}{2} \neq 0.$$

We know that cosine and sine functions are differentiable functions and $t \to \sqrt{t}$ in $(0, +\infty)$ must also be differentiable. Therefore, $F : [0 : \pi] \to \mathbb{R}$ is differentiable. In addition, F is πperiodic from $\mathbb{R} \to \mathbb{R}$, then there must be a local maximum and minimum value of F occur at points where F'=0.

2. if $cos(\theta) = 0$ then $F = \frac{1}{2}$

3. if $sin(\theta) = 0$ then $cos(\theta) = \pm 1$, the right hand element is $\frac{1}{2} \pm \frac{|cos(\vartheta)|}{2}$. Unfortunately this function is not differentiable at $\vartheta = \frac{\pi}{2}$, but we can still circumvent that by noticing that $|\cos\vartheta|$ is bound between 0 and 1, so for those specific values of θ, ϑ our fidelity will be equal $\frac{1}{2}, 1$ respectively.

Having dealt with the differentiability of the Eq.(5.22) we can now consider a more general case for θ that is not equal to one of the cases above. To find the critical points we will take the partial derivative with the respect to the parameter and set it equal to 0:

$$\frac{\partial F}{\partial \vartheta} = \frac{\cos(\theta)(4\sin^2(\theta)\sin(\vartheta)\cos(\vartheta) - \cos^2(\theta)\sin(2\vartheta))}{4\sqrt{2\sin^2(\theta)\sin^2(\vartheta) + \cos^2(\theta)\cos^2(\vartheta)}} = 0. \tag{5.23}$$

By direct application of the extreme value theorem it is easy to see that the critical points of Eq.(5.22) are found at $\vartheta = 0$, and $\frac{\pi}{2}$ respectively. It can be checked by simple substitution of the values into Eq.(5.22) that:

$$F_{max}(\vartheta = 0) = \frac{1}{2}[1 + \frac{\sin(2\theta)}{\sqrt{2}}] \tag{5.24}$$

$$F_{min}(\vartheta = \frac{\pi}{2}) = \frac{1}{2}[1 + \cos^2(\theta)]. \tag{5.25}$$

Eq.(5.24) and Eq.(5.25) demonstrate that this cloning machine works best for the qubits prepared along the z axis and the worst for the qubits prepared on the x-y plane.

5.2.2 Cloning using Optimal Buzek-Hillery Cloning Machine

We are looking for the cloning machine that has the greatest possible fidelity while remaining consistent. One can see that it is achieved by setting $\theta = \cos^{-1}(\sqrt{\frac{2}{3}})$ in Eq.(5.10)

$$\begin{aligned} |0\rangle |B\rangle |M\rangle &\rightarrow \sqrt{\frac{2}{3}} |0\rangle |0\rangle |1\rangle - \sqrt{\frac{1}{3}} |\Psi^+\rangle |0\rangle \\ (-|1\rangle) |B\rangle |M\rangle &\rightarrow \sqrt{\frac{2}{3}} |1\rangle |1\rangle |0\rangle - \sqrt{\frac{1}{3}} |\Psi^+\rangle |1\rangle , \end{aligned} \tag{5.26}$$

where $|B\rangle$ stands for a blank qubit, $|M\rangle$ stands for the machine, and $|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|10\rangle + |01\rangle]$.

Using linearity, let us use Eq.(5.26) to clone the general quantum state Eq.(2.1):

$$\begin{aligned}
|\psi\rangle\,|B\rangle\,|M\rangle =& a\,|0\rangle\,|B\rangle\,|M\rangle + b\,|1\rangle\,|B\rangle\,|M\rangle \\
\rightarrow& a\sqrt{\frac{2}{3}}\,|0\rangle\,|0\rangle\,|1\rangle - \sqrt{\frac{1}{3}}\,\left|\Psi^+\right\rangle|0\rangle - b\sqrt{\frac{2}{3}}\,|110\rangle + b\sqrt{\frac{1}{3}}\,\left|\Psi^+\right\rangle|1\rangle \\
=& \sqrt{\frac{2}{3}}[a\,|001\rangle - b\,|110\rangle] - \sqrt{\frac{1}{3}}[a\,\left|\Psi^+\right\rangle|0\rangle - b\,\left|\Psi^+\right\rangle|1\rangle] \\
=& \sqrt{\frac{2}{3}}[a\,|001\rangle - b\,|110\rangle] - \sqrt{\frac{1}{6}}[a(|110\rangle + |010\rangle) - b(|101\rangle + |011\rangle)]
\end{aligned} \tag{5.27}$$

We will introduce the perpendicular vector of our general quantum state $\left|\Psi^\perp\right\rangle = b^*\,|0\rangle - a^*\,|1\rangle$ with the goal of rewriting the last line of Eq.(5.27) using only $|\Psi\rangle$ and $\left|\Psi^\perp\right\rangle$:

$$\begin{aligned}
|\psi\rangle\,|\psi\rangle\,\left|\psi^\perp\right\rangle =& \\
& -\alpha^2\beta^*\,|000\rangle + \alpha|\alpha|^2|001\rangle - \alpha|\beta|^2|010\rangle + |\alpha|^2\beta\,|011\rangle \\
& -\alpha|\beta|^2|100\rangle + |\alpha|^2\beta\,|101\rangle - \beta|\beta|^2|110\rangle + \beta^2\alpha^*\,|111\rangle
\end{aligned} \tag{5.28}$$

$$\begin{aligned}
|\psi\rangle\,\left|\psi^\perp\right\rangle\,|\psi\rangle =& \\
& -\alpha^2\beta^*\,|000\rangle + \alpha|\alpha|^2|010\rangle - \alpha|\beta|^2|001\rangle + |\alpha|^2\beta\,|011\rangle \\
& -\alpha|\beta|^2|100\rangle + |\alpha|^2\beta\,|110\rangle - \beta|\beta|^2|101\rangle + \beta^2\alpha^*\,|111\rangle
\end{aligned} \tag{5.29}$$

$$\begin{aligned}
\left|\psi^\perp\right\rangle\,|\psi\rangle\,|\psi\rangle =& \\
& -\alpha^2\beta^*\,|000\rangle + \alpha|\alpha|^2|100\rangle - \alpha|\beta|^2|010\rangle + |\alpha|^2\beta\,|100\rangle \\
& -\alpha|\beta|^2|001\rangle + |\alpha|^2\beta\,|101\rangle - \beta|\beta|^2|011\rangle + \beta^2\alpha^*\,|111\rangle\,.
\end{aligned} \tag{5.30}$$

Now we add Eq.(5.29) and Eq.(5.30):

$$\begin{aligned}
&|\psi\rangle\,\left|\psi^\perp\right\rangle\,|\psi\rangle + \left|\psi^\perp\right\rangle\,|\psi\rangle\,|\psi\rangle \\
&\quad = -2\alpha^2\beta^*\,|000\rangle - 2\alpha|\beta|^2|001\rangle + \alpha(|\alpha|^2 - |\beta|^2)\,|010\rangle + \beta(|\alpha|^2 - |\beta|^2)\,|011\rangle \\
&\quad + \alpha(|\alpha|^2 - |\beta|^2)\,|100\rangle + \beta(|\alpha|^2 - |\beta|^2)\,|101\rangle + 2|\alpha|^2\beta\,|110\rangle + 2\beta^2\alpha^*\,|111\rangle\,.
\end{aligned} \tag{5.31}$$

Rewriting Eq.(5.27) with equations above:

$$|\psi\rangle|B\rangle|M\rangle = \sqrt{\frac{1}{6}}[2|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle - (|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle + |\psi^{\perp}\rangle|\psi\rangle|\psi\rangle)]. \tag{5.32}$$

One can verify that Eq.(5.32) is identical to Eq.(5.27).

5.2.3 Fidelity of the Buzek Hillery Cloning Machine

Now we calculate the fidelity of this cloning machine. The first step is to simplify Eq.(5.32):

$$|\psi\rangle|B\rangle|M\rangle = \sqrt{\frac{2}{3}}|\chi_1\rangle|\psi^{\perp}\rangle - \sqrt{\frac{1}{6}}|\chi_2\rangle|\psi\rangle \tag{5.33}$$

Where $|\chi_1\rangle = |\psi\rangle|\psi\rangle$ and $|\chi_2\rangle = |\psi\rangle|\psi^{\perp}\rangle + |\psi^{\perp}\rangle|\psi\rangle$.

We will need the density matrix of Eq.(5.33) to examine the fidelity of the copy:

$$\begin{aligned}\boldsymbol{\rho} =& \frac{2}{3}(|\chi_1\rangle\langle\chi_1|)(|\psi^{\perp}\rangle\langle\psi^{\perp}|) + \frac{1}{6}(|\chi_2\rangle\langle\chi_2|)(|\psi\rangle\langle\psi|) \\ &- \frac{1}{9}[(|\chi_1\rangle\langle\chi_2|)(|\psi^{\perp}\rangle\langle\psi|) + (|\chi_2\rangle\langle\chi_1|)(|\psi\rangle\langle\psi^{\perp}|)].\end{aligned} \tag{5.34}$$

The next step is to take a partial trace of this expression over the space of qubit M. Even though the trace can be taken in any basis, we would like to take it over $|\psi\rangle$ and $|\psi^{\perp}\rangle$ because it will simplify the math:

$$\begin{aligned}\boldsymbol{\rho}_{AB} = Tr_M\boldsymbol{\rho}_{AB} &= \langle\psi|\boldsymbol{\rho}|\psi\rangle + \langle\psi^{\perp}|\boldsymbol{\rho}|\psi^{\perp}\rangle \\ &= \frac{1}{6}(|\psi^{\perp}\rangle\langle\psi^{\perp}| + |\psi\rangle\langle\psi|) + \frac{2}{3}|\psi\rangle\langle\psi| \\ &= \frac{1}{6}|\psi^{\perp}\rangle\langle\psi^{\perp}| + \frac{5}{6}|\psi\rangle\langle\psi|.\end{aligned} \tag{5.35}$$

$\boldsymbol{\rho}_A$ can be calculated by taking a partial trace over the space of qubit B using the basis of $|\psi\rangle$ and $|\psi^{\perp}\rangle$

$$\begin{aligned}\boldsymbol{\rho}_A = Tr_B\boldsymbol{\rho}_{AB} &= \langle\psi|\boldsymbol{\rho}_A|\psi\rangle + \langle\psi^{\perp}|\boldsymbol{\rho}_A|\psi^{\perp}\rangle \\ &= \frac{1}{6}(\langle\psi|\chi_2\rangle\langle\chi_2|\psi\rangle + \langle\psi^{\perp}|\chi_2\rangle\langle\chi_2|\psi^{\perp}\rangle) + \frac{2}{3}(\langle\psi|\chi_1\rangle\langle\chi_1|\psi\rangle + \langle\psi^{\perp}|\chi_1\rangle\langle\chi_1|\psi^{\perp}\rangle).\end{aligned} \tag{5.36}$$

Eq.(5.36) can be refined to:

$$\boldsymbol{\rho}_A = \frac{1}{6}(|\psi^{\perp}\rangle\langle\psi^{\perp}| + |\psi\rangle\langle\psi|) + \frac{2}{3}|\psi\rangle\langle\psi| = \frac{1}{6}|\psi^{\perp}\rangle\langle\psi^{\perp}| + \frac{5}{6}|\psi\rangle\langle\psi|. \tag{5.37}$$

By the definition of fidelity provided in Eq.(5.1) we can now derived the fidelity of the Buzek-Hillery Machine:

$$F_{BH} = \langle\psi|\, \boldsymbol{\rho}_A \,|\psi\rangle = \frac{5}{6}. \tag{5.38}$$

The fidelity Eq.(5.38) is the same for all input states $|\psi\rangle$, showing that the Buzek-Hillery machine is a universal one. To confirm this, we revisit Eq.(5.22) and put $\theta = \cos^{-1}(\sqrt{\frac{2}{3}}) \approx 35.3^\circ$ in it, and plot the fidelity for a range of input states with θ varying from 0 to π to get the curve shown in Fig.(4) below:

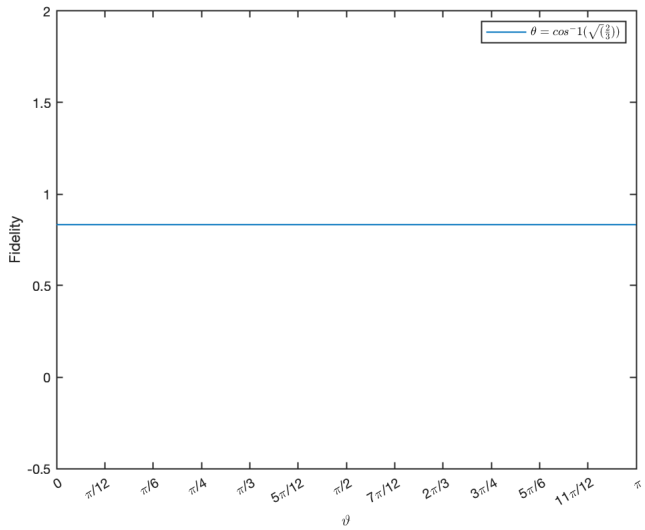

Figure 4: Plot of Eq.(5.21) for $\theta = 35.3^\circ$ and a continuous range of input states with θ varying from 0 to π. The constant value of the fidelity shows this to be a universal cloning machine.

If we compare Fig.3 and Fig.4 we see that Buzek-Hillery cloning machine will produce the same fidelity clones regardless of the input state. In addition, we can conclude that if the angle θ is less than $\cos^{-1}(\sqrt{\frac{2}{3}})$, the machine will be better at cloning states that are closer to the Z axis and if θ is larger than $\cos^{-1}(\sqrt{\frac{2}{3}})$ the machine will clone better at states that are closer to the X axis.

5.3 Werner's Approach

5.3.1 $1 \rightarrow 2$ Cloning Machine using Werner's approach

Our goal is to create a symmetric and universal cloning machine[6]. We can use our experience with the Buzek-Hillary cloning machine to state some basic features that we would like the machine to have:

1. The Hilbert space must include both the input state and the output states.
2. The machine will use unitary transformation to transform the input state into the clones it produces.
3. The output states of the machine will be a mixed state in the space of the clones, since there is an entanglement between them and the internal state of the machine.
4. We want all the clones produced by the machine to be identical (this defines a "symmetric" cloning machine).
5. We want the machine to clone all input states with the same fidelity (this defines a "universal" cloning machine).

In order to accomplish (1), we will embed the input state in a larger Hilbert space of $dim(\mathbb{H}) = 4$, which is the joint space of the original qubit and the blank qubit in which a copy will be made. The output of the machine will be a density operator in the space of the input and blank qubits. Next step is to project this state onto the symmetric subspace of the total Hilbert space which will yield the two identical clones produced by the machine.

For $dim(\mathbb{H}) = 4$, let us first introduce symmetric and anti-symmetric basis vectors. For symmetric basis vectors we have that $|\psi_{A,B}\rangle = |\psi_{B,A}\rangle$ and for anti-symmetric basis vectors $|\psi_{A,B}\rangle = -|\psi_{B,A}\rangle$. Using the additional condition that $\langle\psi_i|\psi_j\rangle = \delta_{i,j}$ it is easy to see that a choice for such basis would be:

$$\begin{aligned} |\psi_1\rangle &= |00\rangle \\ |\psi_2\rangle &= |11\rangle \\ |\psi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\psi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{5.39}$$

The first three states constitute a basis for the symmetric subspace of the total Hilbert space, whereas the last is a basis for the one-dimensional antisymmetric subspace.

We can use this basis and completeness of Hilbert spaces to create a projection operator from z to the symmetric subspace:

$$
\begin{aligned}
S_2 &= |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3| \\
&= |00\rangle\langle 00| + |11\rangle\langle 11| + \frac{1}{2}(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|).
\end{aligned} \tag{5.40}
$$

Notice this is not a unitary operator, because the symmetric subspace is smaller than the entire space.

Let us take an arbitrary state as defined in Eq.(2.1) and represent it through a density matrix:

$$
\begin{aligned}
|\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\
\boldsymbol{\rho} &= |\psi\rangle\langle\psi| = (\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha^*\,\langle 0| + \beta^*\,\langle 1|) \\
&= |\alpha|^2\,|0\rangle\langle 0| + |\beta|^2\,|1\rangle\langle 1| + \alpha\beta^*\,|0\rangle\langle 1| + \alpha^*\beta\,|1\rangle\langle 0|\,.
\end{aligned} \tag{5.41}
$$

Now we will embed this state in a 4-dimensional Hilbert space using a totally unpolarized state I^2 in the space of the blank qubit

$$
\begin{aligned}
\boldsymbol{\rho}_{AB} = \boldsymbol{\rho} \otimes I^2 &= (|\alpha|^2\,|0\rangle\langle 0| + |\beta|^2\,|1\rangle\langle 1| + \alpha\beta^*\,|0\rangle\langle 1| + \alpha^*\beta\,|1\rangle\langle 0|) \otimes (\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \\
&= \frac{1}{2}((|\alpha|^2\,|00\rangle\langle 00| + |\beta|^2\,|10\rangle\langle 10| + \alpha\beta^*\,|00\rangle\langle 10| + \alpha^*\beta\,|10\rangle\langle 00|) \\
&+ \frac{1}{2}((|\alpha|^2\,|01\rangle\langle 01| + |\beta|^2\,|11\rangle\langle 11| + \alpha\beta^*\,|01\rangle\langle 11| + \alpha^*\beta\,|11\rangle\langle 01|).
\end{aligned} \tag{5.42}
$$

Next step is to project this density matrix onto the symmetric subspace. As mentioned earlier, this projection is not a unitary operator. We will have to re-normalize the system such that the trace of the system remains one, so that the output will represent a real physical system

$$
\begin{aligned}
\boldsymbol{\rho}_{symmetry} &= CS_2\boldsymbol{\rho}_{AB}S_2 \\
&= |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3|\,\boldsymbol{\rho}_{AB} \\
&= C\frac{1}{2}(|\alpha|^2\,|\psi_1\rangle\langle\psi_1| + \frac{|\beta|^2}{2}\,|\psi_3\rangle\langle\psi_3| + \frac{\alpha\beta^*}{\sqrt{2}}\,|\psi_1\rangle\langle\psi_3| + \frac{\alpha^*\beta}{\sqrt{2}}\,|\psi_3\rangle\langle\psi_1| \\
&+ \frac{|\alpha|^2}{2}\,|\psi_3\rangle\langle\psi_3| + |\beta|^2\,|\psi_2\rangle\langle\psi_2| + \frac{\alpha\beta^*}{\sqrt{2}}\,|\psi_3\rangle\langle\psi_2| + \frac{\alpha^*\beta}{\sqrt{2}}\,|\psi_2\rangle\langle\psi_3|),
\end{aligned} \tag{5.43}
$$

where C is a re-normalization constant to ensure the output as a valid density tensor. C is defined as following:

$$
\begin{aligned}
C = Tr(\boldsymbol{\rho}_{symmetry})^{-1} &= \langle\psi_1|\,\boldsymbol{\rho}_{symmetry}\,|\psi_1\rangle + \langle\psi_2|\,\boldsymbol{\rho}_{symmetry}\,|\psi_2\rangle + \langle\psi_3|\,\boldsymbol{\rho}_{symmetry}\,|\psi_3\rangle \\
&= (\frac{1}{2} * (|\alpha|^2 + |\beta|^2 + \frac{1}{2}(|\alpha|^2 + |\beta|^2)))^{-1} \\
&= \frac{3}{4}^{-1} = \frac{4}{3}.
\end{aligned} \tag{5.44}
$$

With C established, we carry it into Eq.(5.43):

$$\begin{aligned}\boldsymbol{\rho}_{symmetry} = \frac{2}{3}(|\alpha|^2 |\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_3\rangle\langle\psi_3| + \frac{\alpha\beta^*}{\sqrt{2}}|\psi_1\rangle\langle\psi_3| + \frac{\alpha^*\beta}{\sqrt{2}}|\psi_3\rangle\langle\psi_1| \\ + |\beta|^2 |\psi_2\rangle\langle\psi_2| + \frac{\alpha\beta^*}{\sqrt{2}}|\psi_3\rangle\langle\psi_2| + \frac{\alpha^*\beta}{\sqrt{2}}|\psi_2\rangle\langle\psi_3|).\end{aligned} \tag{5.45}$$

So we are in position to recover the density matrices for the clones by taking the partial trace over the space of qubit 1 or qubit 2. Since we are working in the symmetric subspace, $\boldsymbol{\rho}_1 = \boldsymbol{\rho}_2$. $\boldsymbol{\rho}_1$ is calculated as follows:

$$\begin{aligned}\boldsymbol{\rho}_1 &= \langle 0_1|\boldsymbol{\rho}_{symmetry}|0_1\rangle + \langle 1_1|\boldsymbol{\rho}_{symmetry}|1_1\rangle \\ &= \frac{2}{3}(|\alpha|^2|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{\alpha\beta^*}{2}|0\rangle\langle 1| + \frac{\alpha^*\beta}{2}|1\rangle\langle 0| + \frac{1}{4}|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| + \frac{\alpha\beta^*}{2}|0\rangle\langle 1| + \frac{\alpha^*\beta}{2}|1\rangle\langle 0| \\ &= (\frac{2}{3}|\alpha|^2 + \frac{1}{6})|0\rangle\langle 0| + (\frac{2}{3}|\beta|^2 + \frac{1}{6})|1\rangle\langle 1| + \frac{2}{3}\alpha\beta^*|0\rangle\langle 1| + \frac{2}{3}\alpha^*\beta|1\rangle\langle 0|.\end{aligned} \tag{5.46}$$

Now we shall use the Eq.(5.46) to evaluate the fidelity using Eq.(5.1):

$$\begin{aligned}F_{1,2} &= \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix} * \begin{pmatrix}\frac{2}{3}|\alpha|^2 + \frac{1}{6} & \frac{2}{3}\alpha\beta^* \\ \frac{2}{3}\alpha^*\beta & \frac{2}{3}|\beta|^2 + \frac{1}{6}\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} \\ &= (\frac{2}{3}|\alpha|^2 + \frac{1}{6})|\alpha|^2 + \frac{2}{3}|\alpha|^2|\beta|^2 + (\frac{2}{3}|\alpha|^2 + \frac{1}{6})|\alpha|^2 + \frac{2}{3}|\alpha|^2|\beta|^2 \\ &= \frac{2}{3}|\alpha|^2(|\alpha|^2 + |\beta|^2) + \frac{1}{6}|\alpha|^2 + \frac{2}{3}|\beta|^2(|\alpha|^2 + |\beta|^2) + \frac{1}{6}|\beta|^2 \\ &= \frac{2}{3} + \frac{1}{6} = \frac{5}{6}.\end{aligned} \tag{5.47}$$

Eq.(5.47) shows that we obtain the fidelity of $\frac{5}{6}$ by Werner's approach, which is the same as in the optimal Buzek-Hillery cloning machine. The advantage of the Werner's approach is that we can generalize this construction to $N \to M$ cloning machines.

5.3.2 N→M Cloning machine

We now generalize the treatment of the previous section by considering a machine that takes N identical copies of an arbitrary pure state of a qudit (a d-state quantum system) and transforms it into M identical clones, where $M > N$. The machine works by combining the input state with the identity operator in an M dimensional space and then projecting into the symmetric subspace of this composite

system. The dimension of this symmetric subspace is given by the expression:

$$d[M] = dim(\mathbb{H}_{+d}^{\otimes(M)}) = \begin{pmatrix} d+M-1 \\ \\ M \end{pmatrix}. \tag{5.48}$$

If we specialize this to the case for M=2, d=2 which is the space used for the $1 \to 2$ process, we find that the symmetric subspace does indeed have dimension 3, as we found before:

$$\begin{pmatrix} 2+2-1 \\ \\ 1 \end{pmatrix} = \frac{3!}{1!\,(3-1)!} = 3. \tag{5.49}$$

We will use a procedure similar to that we used earlier when constructing a generalized cloning machine with Werner's approach:

1. Represent the input N original states as $\boldsymbol{\rho}_N = |\psi\rangle\langle\psi|^{\bigotimes N}$
2. Combine the input state $\boldsymbol{\rho}_N$ with the identity operator in an (M-N) Hilbert space to produce a state in an M-dimensional Hilbert space.
3. Project the state in (2) to the symmetric subspace of the M-dimensional space
4. Re-normalize the state in (3) and evaluate its reduced density matrix to determine the states of the individual clones.

Altogether that will look like the following:

$$\begin{aligned} \boldsymbol{\rho}_{symmetry} &= C^{-1} * S_M(\boldsymbol{\rho}_N \otimes I^{(M-N)})S_M \\ C &= Tr(S_M(\boldsymbol{\rho}_N \otimes I^{(M-N)})S_M), \end{aligned} \tag{5.50}$$

where S_M is the projector onto the symmetric subspace of the M-dimensional space and C is the normalization constant.

We will now calculate the value of C by expanding $\boldsymbol{\rho}_N$ in terms of the individual projectors $\boldsymbol{\rho}_k$ in the symmetric subspace S_N. S_M will kill off all the non-symmetric components, so we can rewrite Eq.(5.50):

$$\begin{aligned} \boldsymbol{\rho}_N &= \sum_k c_k P_k \\ P_k &= |\psi_k\rangle\langle\psi_k|\,, \psi_k \in \mathbb{H}_{+d}^N \\ C &= \sum_k Tr(S_M(P_k \otimes I^{(M-N)})S_M). \end{aligned} \tag{5.51}$$

Now let us evaluate $Tr(S_M(P_k \otimes I^{(M-N)}S_M)$. This quantity is the same for all k, so:

$$
\begin{aligned}
&\mathrm{Tr}(S_M(P_k \otimes I^{(M-N)})S_M) \\
&= \frac{1}{d[N]}\mathrm{Tr}(S_M(\sum_{k=1}^{N} P_k \otimes I^{(M-N)})S_M) \\
&= \frac{1}{d[N]}\mathrm{Tr}(S_M(S_N \otimes I^{(M-N)})S_M), \text{ by definition of } S_N \\
&= \frac{1}{d[N]}(\mathrm{Tr}(S_M(I_N \otimes I^{(M-N)}S_M)) + \mathrm{Tr}(S_M([S_N - I_N] \otimes I^{(M-N)})S_M)).
\end{aligned}
\tag{5.52}
$$

The $S_N - I_N$ term is not totally symmetric and it will be cancelled out when sandwiched between the two S_M operators, so:

$$
\frac{1}{d[N]}\,\mathrm{Tr}(S_M I_M S_M) = \frac{1}{d[N]}\,\mathrm{Tr}(S_M) = \frac{d[M]}{d[N]}. \tag{5.53}
$$

With the help of this result we can rewrite Eq.(5.50) as follows:

$$
\boldsymbol{\rho}_{symmetry} = \frac{d[N]}{d[M]} S_M(\boldsymbol{\rho}_N \otimes I^{(M-N)})S_M. \tag{5.54}
$$

Now we will derive the fidelity of a single copy. In order to do so we will use the following equation:

$$
F = Tr(\boldsymbol{\rho}_{clone}\boldsymbol{\rho}). \tag{5.55}
$$

We introduce the operators $\sigma = |\psi\rangle\langle\psi| \in \mathbb{H}_{+d}$ and $\sigma^{(k)} = I^{\otimes k-1} \otimes \sigma \otimes I^{\otimes(M-k)}$. Where the second operator is the density matrix of the k^{th} clone. Therefore, we calculate the fidelity of a single clone as:

$$
\begin{aligned}
F = \mathrm{Tr}(\boldsymbol{\rho}_{clone}\boldsymbol{\rho}) &= \mathrm{Tr}(\sigma^{(k)}\boldsymbol{\rho}_{symmetry}) \\
&= \frac{1}{M}\sum_{k=1}^{M} \mathrm{Tr}(\sigma^{(k)}\frac{d[N]}{d[M]} S_M(\boldsymbol{\rho}_N \otimes I^{(M-N)}S_M) \\
&= \frac{1}{M}\frac{d[N]}{d[M]}\sum_{k=1}^{M} \mathrm{Tr}(\sigma^{(k)} S_M(\boldsymbol{\rho}_N \otimes I^{(M-N)})S_M.
\end{aligned}
\tag{5.56}
$$

We used the fact that the clones are identical and therefore will have the same fidelity to get the second line of Eq.(5.56).

Unlike $\boldsymbol{\rho}$, we choose σ to be a totally symmetric quantity (it exists only in the symmetric subspace), $\sigma^{(k)}S_N = S_N\sigma^{(k)}$. We can use the same trick that we used earlier when dividing $\boldsymbol{\rho}$ into symmetric and non-symmetric parts. Notice that the non-symmetric part will be killed off by the operator S_N. Using that as well as cyclic properties of the trace operator we will rewrite Eq.(5.56) as follows:

$$
\begin{aligned}
F &= \frac{1}{M}\frac{d[N]}{d[M]}\sum_{k=1}^{M}\mathrm{Tr}(S_M\sigma^{(k)}(\sigma^{\otimes N}\otimes I^{(M-N)})S_M) \\
&= \frac{1}{M}\frac{d[N]}{d[M]}\mathrm{Tr}(S_M\sum_{k=1}^{M}\sigma^{(k)}(\sigma^{\otimes N}\otimes I^{(M-N)})S_M).
\end{aligned}
\tag{5.57}
$$

Now it is important to see exactly how $\sigma^{(k)}(\sigma^{\otimes N}\otimes I^{(M-N)})$ operates. We will use the following properties:

$$
\begin{aligned}
&I\sigma = \sigma \\
&\sigma\sigma = |\psi\rangle\langle\psi|\,|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \sigma.
\end{aligned}
\tag{5.58}
$$

Let's divide the problem into two parts, for k less than or equal to N and k greater than N:

$$
\begin{aligned}
\forall k \le N:\ &\sigma^{(k)}\sigma^{\otimes N}\otimes I^{(M-N)} \\
&= (I^{\otimes k-1}\otimes\sigma\otimes I^{\otimes(M-k)})(\sigma^{k-1}\otimes\sigma\otimes\sigma^{\otimes(N-k)}\otimes I^{(M-N)}) \\
&= \sigma^{\otimes N}\otimes I^{(M-N)}.
\end{aligned}
\tag{5.59}
$$

Now for k greater than N:

$$
\begin{aligned}
\forall k > N:\ &\sigma^{(k)}\sigma^{\otimes N}\otimes I^{(M-N)} \\
&= (I^{\otimes k}\otimes\sigma\otimes I^{\otimes(M-k)})(\sigma^{\otimes N}\otimes I^{\otimes(k-1-N)}\otimes I\otimes I^{\otimes(M-k)}) \\
&= \sigma^{\otimes(N+1)}I^{\otimes(M-N-1)}.
\end{aligned}
\tag{5.60}
$$

Now we can use these in Eq.(5.57) and once again using cyclic properties of trace:

$$
F = \frac{1}{M}\frac{d[N]}{d[M]}\Big[\sum_{k=1}^{N}\mathrm{Tr}(S_M(\sigma^{\otimes N}\otimes I^{(M-N)})S_M + \sum_{k=1+N}^{M}\mathrm{Tr}(S_M(\sigma^{\otimes N+1}\otimes I^{(M-N-1)})S_M\Big].
\tag{5.61}
$$

We are now in the position to evaluate fidelity, because we were able to get rid of the k dependence. We can also use Eq. (5.52) to evaluate the terms in the summations. Doing so gets us the following:

$$
\begin{aligned}
F &= \frac{1}{M}\frac{d[N]}{d[M]}(N\frac{d[M]}{d[N]} + (M-N)\frac{d[M]}{d[N+1]}) \\
&= \frac{N}{M} + \frac{M-N}{M}\frac{d[N]}{d[N+1]} \\
&= \frac{N}{M} + \frac{M-N}{M}\frac{N+1}{N+d}.
\end{aligned}
\tag{5.62}
$$

Just to check if this more general calculation agrees with the $1\to 2$ calculations we can plug N=1, M=2, d=2:

$$
F(1,2,2) = \frac{1}{2} + \frac{1}{2}\times\frac{2}{3} = \frac{5}{6}.
\tag{5.63}
$$

The equation for the fidelity of general universal and symmetric cloning machine gives us several key insights into how the cloning machines will operate. It is not a surprise that for a large number of copies, the fidelity of each individual clone rapidly decreases, but what is interesting is that d=2 is the best for the purposes of cloning. That opens up avenues to using particles with a larger spin for ensuring greater security in cryptographic transmissions.

6 Security Analysis of BB84

6.1 Basic principles of Information theory

In the previous chapters of this report we discussed the quantum mechanical aspects of exchanging a secret key. In this chapter we will focus on the classical information theory needed to analyze the security of quantum key exchange schemes.

So let us first define the concept of classical entropy. It's purpose is to quantify the amount of information gained from a measurement in terms of the average number of binary questions that must be asked to determine the outcome of the measurement. Consider the following experiment: we want to find a ball that can be in M possible locations with equal probability:

$$\begin{aligned} p &= \frac{1}{M}, \\ H &= \log_2 M. \end{aligned} \tag{6.1}$$

The probability with which it can be found in any location is $p = \frac{1}{M}$ and we define the amount of information we get on learning where the ball actually is as the Shannon entropy $H = \log_2 M$. For example, if M = 16 then H = 4, which is the number of binary (yes/no) questions we must ask to determine the location of the ball if we eliminate half the possibilities with each question.

We can generalize the expression above for entropy to a distribution that does not involve exclusively equally likely outcomes. The main idea is to consider a large number of equally likely outcomes and group them together into sets of different sizes that occur with different probabilities, and use a modification of the earlier approach to calculate the entropy of this set. Assume that there are $N \in \mathbb{N}$ equally likely outcomes and we can spread them across a collection of sets, denoted as X, each including n_x of the elements. There are two different ways in which we can determine the outcome of an experiment on such a system. The first, which we will denote Z, is to use the method described above to determine which of the N equally likely outcomes occurs, and the entropy associated with this method is $\log_2(N)$. The other way is to first identify the set and then the element within the set. Both methods uniquely identify one of N equally likely outcomes, so equating the entropies obtained by these two methods gives

$$
\begin{aligned}
H(Z) = \log_2 N &= H(X) + \sum_x p(x)\log_2(n_x) \\
\text{or } \; H(X) &= \log_2 N - \sum_x p(x)\log_2(n_x) \\
&= \log_2 N - \sum_x p(x)\log_2(p_x N) \\
\text{since } p_x = \frac{n_x}{N} &= \log_2 N - \sum_x p(x)\log_2(p_x) - \sum_x p(x)\log_2(N) \\
&= -\sum_x p(x)\log_2(p_x).
\end{aligned}
\tag{6.2}
$$

This formula allows the entropy of any random event to be calculated, given that the probabilities of all the outcomes are known. We now wish to generalize this formula so that it applies to quantum systems.

The closest quantum analogy to the discrete variable with equally possible outcomes is the totally unpolarized state as described in Eq.(2.15). In that equation we used d=2 for the mixed state, but we can do this for a general dimensionality d. The Quantum entropy, also known as the von Neumann entropy[10], for a completely mixed state in d dimension is:

$$S = \log_2(d), \tag{6.3}$$

for an arbitrary quantum state described by the density matrix $\boldsymbol{\rho}$, the formula that replaces Eq.(6.3) is

$$S = -Tr(\boldsymbol{\rho})\log_2(\boldsymbol{\rho}). \tag{6.4}$$

The trace operation is the easiest to evaluate in the eigenbasis of the density matrix, so using that we can rewrite the expression above as:

$$S(Q) = -\sum_k p_k \log_2 p_k. \tag{6.5}$$

Clearly this is just the Shannon's entropy calculated for the probabilities p_k of the different mutually orthogonal pure states present in the mixed state described by $\boldsymbol{\rho}$ on the BB84 protocol.

6.2 Incoherent attack

As discussed in chapter 3, Alice and Bob continue the BB84 protocol by announcing the bases they ran and keep those that were correct. While Alice and Bob eventually reach a shared and secret key, they need to see if their key is valid and safe. To do so, they will measure the percentage of error in the bit string they share after the sifting phase. If the percentage exceeds a certain critical value D, they acknowledge that the key either had too much noise in it or it was compromised by Eve. On the other hand, if the percentage of error is below the critical value D, they can shrink their key by a factor R to obtain a secret key. While D and R are both dependent on the attack Eve launches, the security criterion given by Csiszar and Korner[3] determines the value of R as:

$$R = I(A:B) - \min\{I(A:E), I(B:E)\}, \tag{6.6}$$

where (X,Y) is the mutual information shared between individuals X and Y. (A=Alice, E=Eve, and B=Bob)

The quantity I(X:Y) is defined by the equation:

$$I(X:Y) = H(X) + H(Y) - H(XY), \tag{6.7}$$

where H(X), H(Y), and H(XY) are the Shannon entropies of the respective elements.

The critical error rate D is determined implicitly by Eq.(6.6) when R=0. Let us first consider the quantity I(A:B) in Eq.(6.6), which is the mutual information shared among Alice and Bob on average over all the runs. In our discussion of the BB84 protocol, Bob simply guesses the bases that Alice uses in each run. The possibility of Bob guessing it correctly can be denoted as p_{AB}, and the corresponding Shannon entropy Eq.(6.2)

$$H(P_{AB}) = -p_{AB}\log(p_{AB}) - (1-p_{AB})\log(1-p_{AB}). \tag{6.8}$$

The mutual information that Alice and Bob have about the exchanged qubit can be written as

$$\begin{aligned} I(A:B) &= H(A) + H(B) - H(AB) \\ &= H(p=1) + H(p=\frac{1}{2}) - H(p_{AB}) \\ &= 1 - H(p_{AB}). \end{aligned} \tag{6.9}$$

We have taken $H(A) = H(p=1)$ and $H(B) = H(p=\frac{1}{2})$ because Alice knows the bit she is sending, whereas Bob is completely ignorant about the key.

To see that Eq.(6.9) makes sense, let us consider the two limiting cases. If Bob follows the protocol of BB84, his probability of guessing the bases correctly is $\frac{1}{2}$

making $p_{AB} = \frac{1}{2}$. If we put $p_{AB} = \frac{1}{2}$ into Eq.(6.8), then $H_{AB} = 1$ and $I(A : B) = 0$ which implies that there is no information shared between Bob and Alice prior to the protocol. On the other end of the spectrum, assume that Bob knows exactly what Alice is going to send, then his success rate of guessing the bases are 100%. This leads to $p_{AB} = 1$, therefore, $H_{AB} = 0$ and $I(A : B) = 1$ which shows that Bob and Alice have communicated prior to their participation in the protocol.

$I(A : E)$ is very similar $I(A : B)$, but instead of Bob it quantifies the mutual information between Alice and Eve.

Finally, $I(B : E)$ is the mutual information shared among Bob and Eve. In comparison to $I(A : B)$ and $I(A : E)$, Bob and Eve's mutual information represents their knowledge of a bit sent by a third person Alice. Therefore, $I(B : E)$ is a function of the probability that Bob's and Eve's measurement of the spin agrees, and this probability is given by $p_{BE} = p_E(+1)p_B(+1) + p_E(-1)p_B(-1)$. Note that Bob and Eve's mutual information does not depend on how precisely they know Alice's bit but only the extent to which their guesses about it is agree.

6.3 Optimal Incoherent Attack without an ancilla

In this section we will consider the optimal incoherent attack without an ancilla, and the corresponding issues. In this attack, Eve makes two copies of each original qubit, one of which she sends on to Bob and the other of which she keeps for herself. Eve knows that Alice and Bob are using a variation of BB84 protocol, so all of the states that she attempts to clone will have the following form where ϕ is a parameter:

$$|\psi(\phi)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle). \tag{6.10}$$

Eve uses a type of cloning machine, known as the phase covariant cloning machine to make her two clones. It is better than the universal cloning machine for the purposes of an attack on BB84, because it specializes in replicating the states $|\pm x\rangle$, and $|\pm z\rangle$ used in the protocol. The space of the first qubit is the space of the original and that is the copy that Bob will receive. The second qubit is the clone that Eve will try to use to steal the information[8].

All phase covariant cloning machines have the following form with the parameter η which will be established later such that the cloning machine suits Eve's purposes best:

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |10\rangle &\rightarrow \cos(\eta)|10\rangle + \sin(\eta)|01\rangle . \end{aligned} \tag{6.11}$$

To make the algebra easier, let us study what happens when Alice sends the state $|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Eve's cloning machine will entangle the input state with the blank state (originally $|0\rangle$) producing the following state:

$$|\Gamma_{BE}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + \cos(\eta)\,|10\rangle + \sin(\eta)\,|01\rangle). \tag{6.12}$$

Using Eq.(6.12) the density matrix of the copy that Bob receives can be expressed as:

$$\begin{aligned}\rho_B &= \mathrm{Tr}_E(|\Gamma_{BE}\rangle\,\langle\Gamma_{BE}|) \\ &= \frac{1}{2}(\mathbb{1} + \sin^2(\eta)\sigma_z + \cos(\eta)\sigma_x).\end{aligned} \tag{6.13}$$

If Bob makes a measurement along z axis, this qubit is later discarded in accordance to the BB84 protocol. So we only need to consider the case in which Bob measures along the x axis, in which case the probability that Bob gets the same value for the spin as Alice is:

$$p_{AB} = \langle +x|\,\rho_b\,|+x\rangle = \frac{1}{2}(1 + \cos(\eta)). \tag{6.14}$$

This establishes the p_{AB} in our Eq.(6.9). Moving forward to Alice and Eve, Eve'e qubit will be in the state of:

$$\begin{aligned}\rho_E &= \mathrm{Tr}_B(|\Gamma_{BE}\rangle\,\langle\Gamma_{BE}|) \\ &= \frac{1}{2}(\mathbb{1} + \cos^2(\eta)\sigma_z + \sin(\eta)\sigma_x).\end{aligned} \tag{6.15}$$

Eve waits to measure her qubit until Alice and Bob declare which basis they agree on, so that she can follow Bob. Therefore, she will also only measure the qubit along the x axis and the probability that she gets the spin value that Alice intended is:

$$p_{AE} = \langle +x|\,\rho_E\,|+x\rangle = \frac{1}{2}(1 + \sin(\eta)). \tag{6.16}$$

From Eq.(6.14) we can calculate the mutual information between Alice and Bob. The meaning of mutual information between Eve and Bob, I(B:E) is slightly different. It is still the information they share, but in this context p_{BE} is the probability that they agree on their measurements. With that in mind the expression for p_{BE} is:

$$\begin{aligned}p_{BE} &= |\langle +x, +x|\psi_{BE}\rangle|^2 + |\langle -x. - x|\psi_{BE}\rangle| \\ &= p_{AB}p_{AE} + (1 - p_{AB})(1 - p_{AE}) \\ &= \frac{1}{2}(1 + \sin(\eta))\frac{1}{2}(1 + \cos(\eta)) + \frac{1}{2}(1 - \sin(\eta))\frac{1}{2}(1 - \cos(\eta)) \\ &= \frac{1}{4}(2 + 2\sin(\eta)\cos(\eta)) \\ &= \frac{1}{2}(1 + \frac{1}{2}\sin(2\eta)).\end{aligned} \tag{6.17}$$

Let us use this information in the security criterion Eq.(6.6). Eve wants to make the value of the fraction R as small as she can (ideally equal to 0) so that she renders

the key useless. She can do this by adjusting the value of η suitably. The obvious way to do this is by increasing the values of both I(A:E) and I(B:E) as much as she can. The joint probabilities Eq.(6.15), Eq.(6.16) and Eq.(6.17) allow I(A:B), I(A:E) and I(B:E) to be calculated and used in Eq.(6.6) to calculate the value of R. The figure below shows plots of I(A:B), I(A:E) and I(B:E) as functions of η. As is clear from the plot, I(A:B) is always greater than the minimum of I(A:E) and I(B:E), and this allows a secret key to be generated as long as I(A:B) exceeds a certain threshold.

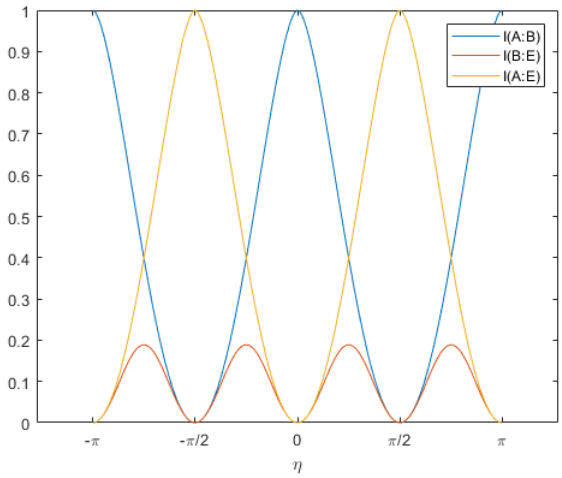

Figure 5: Based on this graph even though there are places where I(A:B)=I(A:E), Alice and Bob still can generate a secret key because I(B:E) is appreciably lower than I(A:E) there, leading to a finite value of R.

6.4 Optimal Incoherent Attack with an Ancilla

The main drawback of the incoherent attack discussed in the previous section is that Eve's knowledge of Bob's bit is too low to prevent the distilling of a key. Eve can overcome this problem by using a cloning machine with an ancilla. That additional qubit will allow Eve to improve $I(B : E)$. To demonstrate this, let Eve make two copies of Alice's qubit by using the following unitary transformation introduced by Niu and Griffiths [7] in their two qubits cloning machine:

$$\begin{aligned} |000\rangle &\rightarrow |000\rangle \\ |100\rangle &\rightarrow \cos(\eta)\,|100\rangle + \sin(\eta)\,|010\rangle \\ |011\rangle &\rightarrow \cos(\eta)\,|011\rangle + \sin(\eta)\,|101\rangle \\ |111\rangle &\rightarrow |111\rangle\,, \end{aligned} \tag{6.18}$$

where the three labels in each ket above refer, respectively, to Alice's qubit, and the two qubits in which she stores information about Alice's and Bob's qubits. After

the cloning machine has acted, the first qubit, which originally belonged to Alice, is sent on by Eve to Bob, and so will be referred to as Bob' qubit, while the other two qubits (the second of which is the ancilla) serve as Eve's record of what Alice and Bob know. Suppose that Alice sends the state $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ to Bob. Eve's cloning machine will entangle the input state with two qubits each initially in the blank state $|0\rangle$ to output the state:

$$\begin{aligned}\left|\Gamma^{\pm}_{BE_1E_2}\right\rangle =& \frac{1}{2}(|000\rangle + \cos(\eta)\,|011\rangle + \sin(\eta)\,|101\rangle \\ & \pm \cos(\eta)\,|100\rangle \pm \sin(\eta)\,|010\rangle \pm |111\rangle).\end{aligned} \tag{6.19}$$

The density matrix of Bob's qubit can be found by taking the partial trace of Eq.(6.19) and is:

$$\rho_B = \mathrm{Tr}_{E_1,E_2}(|\Gamma_{B,E_1,E2}\rangle\langle\Gamma_{B,E_1,E2}|) = \frac{1}{2}(\mathbb{1} \pm \cos(\eta)\sigma_x). \tag{6.20}$$

Now consider a two-qubit unitary transformation that maps the four Bell states defined in Eq.(2.13) into the computation basis states:

$$\begin{aligned}\left|\Phi^+\right\rangle &\to |00\rangle \\ \left|\Phi^-\right\rangle &\to |11\rangle \\ \left|\Psi^+\right\rangle &\to |10\rangle \\ \left|\Psi^-\right\rangle &\to |01\rangle\,.\end{aligned} \tag{6.21}$$

If one performs this transformation on the second and third qubits in Eq.(6.19), which are the ones that Eve keeps for herself, one gets the state:

$$\left|\tilde{\Gamma}^{\pm}\right\rangle = \sqrt{p_{AB}}\,|\pm x\rangle\,|\chi\pm\rangle\,|0\rangle \mp \sqrt{D}\,|\mp x\rangle\,|\chi\mp\rangle\,|1\rangle\,, \tag{6.22}$$

where $p_{AB} = \dfrac{1+\cos\eta}{2}$ is the fidelity of Bob's qubit, $D = 1 - p_{AB}$ is the disturbance caused by Eve, and $|\chi\pm\rangle = \sqrt{F}\,|0\rangle \pm \sqrt{D}\,|1\rangle$. Also, the upper and lower signs in Eq.(6.22) are to be read together.

The state $|\Gamma^+\rangle$ in Eq.(6.22) is the output of Eve's cloning machine if Alice sends the state $|+x\rangle$ while $|\Gamma^-\rangle$ is the output if Alice sends the state $|x-\rangle$

Now let us see how Eve extracts information from her two qubits. She first measures σ_z on her second qubit E_2 and then carries out a measurement on her first qubit E_1 to determine if it is in the state $|x+\rangle$ or $|x-\rangle$. From the combination of the results she gets for these two measurements, she can infer the states that Alice's and Bob's qubit are in, as indicated in table 4. The justification for her conclusions is obvious if one looks at the two terms in Eq.(6.22).

Eve's qubit 1	Eve's qubit 2	Alice's qubit	Bob's qubit
$\|\chi_+\rangle$	$\|0\rangle$	$\|x+\rangle$	$\|x+\rangle$
$\|\chi_-\rangle$	$\|0\rangle$	$\|x-\rangle$	$\|x-\rangle$
$\|\chi_-\rangle$	$\|1\rangle$	$\|x+\rangle$	$\|x-\rangle$
$\|\chi_+\rangle$	$\|1\rangle$	$\|x-\rangle$	$\|x+\rangle$

Table 4: Eve takes measurement on her qubits, and by recording the results of those qubits, she can denote the orientation of Alice's and Bob's qubit in the X basis.

This analysis might seem to suggest that Eve knows the states of both Alice's and Bob's qubits perfectly, but this is not so because Eve's measurement on her qubit E_1 is unable to distinguish between the non-orthogonal states $|\chi_+\rangle$ and $|\chi_-\rangle$ perfectly. The results in table 4 show the inferences she can make about Alice's and Bob's qubits if her measurement of E_1 correctly indicates the state that this qubit is in. However if her measurement returns the wrong state, leading to one row of the table being replaced by another, she will draw the wrong conclusion.

It was shown by Helstrom [5] many years back that the probability with which two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ can be distinguished is $p = \frac{1}{2}(1 + sin(\eta))$. Taking $|\psi_1\rangle = |\chi_1\rangle$ and $|\psi_2\rangle = |\chi_2\rangle$, we can now use this probability to calculate Alice and Eve's mutual information as $I(A:E) = 1 - H(p)$. Since we have established that Eve knows just as much about Bob's bit as Alice's, or I(A:E) = I(B:E), and we also know that $I(A:B) = 1 - H(p_{AB})$, we can use these expressions in Eq.(6.6) along with R=0 to determine the critical error rate. Eq.(6.6) then shows that the critical error rate is achieved when $H(p_{AE}) = H(p_{AB})$. Now p_{AB} can be calculated from the overlap of Bob's reduced density matrix ρ_B with Alice's state and one finds that it becomes equal to p_{AE} for $\eta = \frac{\pi}{4}$. This allows the critical error rate to be calculated as:

$$D = \frac{1}{2}(1 - \sin\Big(\frac{\pi}{4}\Big)) = 0.146 \tag{6.23}$$

In an optimal incoherent attack on the BB84 protocol, the critical error rate that Alice and Bob look for is 14.6%. If Alice and Bob notice that the error rate is larger than 14.6%, they will discard the key as we discussed in BB84. If the error rate is below 14.6%, the protocol continues and will eventually produce the private key. Our analysis was carried out assuming that Alice and Bob both used the x basis. However, identical results are obtained if they both use the same basis along any other direction in the x-y plane.

In conclusion it should be mentioned that we have considered only incoherent attacks, namely, those in which the eavesdropper interacts with each of the qubits individually and in the same manner for all qubits. In a more powerful type of attack, known as a coherent attack, the eavesdropper performs a joint measurement on all her qubits based on the information she gets from Alice and Bob. The virtue of a coherent attack is that it allows a larger amount of information to be obtained about the secret key. Shor and Preskill[11] have analyzed the most general type of coherent attack that can be carried out on BB84 and shown that it will lead to an error rate of at least 11%. Thus, if the error rate is significantly below this value, the protocol can be considered safe.

7 Conclusion

This report has carried out a detailed study of several types of quantum cloning machines. The no-cloning theorem of Wootters, Zurek and Deiks rules out the existence of a perfect cloning machine, so only imperfect machines can be constructed. The most basic machine, due to Buzek and Hillery, produces two imperfect copies of an arbitrary state of a qubit. We carried out an analysis of a slightly generalized version of the Buzek-Hillery machine that gives us a better feeling for its special features.

Following this, we used an approach due to Werner to study more general types of cloning machines that either produce a larger number of copies of the original or allow the original to be a d-state system in an arbitrary state. We showed how Werner's approach allows the fidelity of this class of machines to be calculated without a knowledge of their internal structure.

Finally we studied a third type of cloning machine due to Niu and Griffiths that is useful in mounting an attack on the BB84 protocol. The attack can be of two kinds. In an incoherent attack, the eavedropper interacts with each transmitted qubit in the same way, whereas in a coherent attack, a joint measurement is made on all the copies of the transmitted qubits. We considered only the incoherent attack and showed how the optimum version of it leads to an error rate of 14.6% in the key established by the legitimate users. Thus, if the error rate is less than 14.6%, the key is guaranteed to be safe from this type of attack. A coherent attack, which we did not study in this report but which was analyzed by Shor and Preskill, shows that the maximum error caused by a successful attack is 11%. Thus a much smaller error can be tolerated if the adversary uses this more sophisticated attack.

Other protocols besides BB84, and their security, are topics that might be explored in future projects.

References

[1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[2] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844–1852, 1996.

[3] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[4] D. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

[5] Carl W. Helstrom. *Quantum Detection and estimation theory*. Academic Press, 1976.

[6] M. Keyl and R. F. Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 40(7):3283–3299, 1999.

[7] Chi-Sheng Niu and Robert B. Griffiths. Optimal copying of one quantum bit. *Physical Review A*, 58(6):4377–4393, 1998.

[8] Chi-Sheng Niu and Robert B. Griffiths. Two-qubit copying machine for economical quantum eavesdropping. *Physical Review A*, 60(4):2764–2776, 1999.

[9] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Reviews of Modern Physics*, 77(4):1225–1256, 2005.

[10] Benjamin Schumacher and Michael D. Westmoreland. *Quantum processes, systems, and information*. Cambridge University Press, 2010.

[11] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.

[12] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[13] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.