Revocation and Reconstruction of Shared Quantum Secrets

Prakash Mudholkar \textsuperscript{*1}, Chiranjeevi Vanarasa \textsuperscript{†1}, Indranil Chakraborty\textsuperscript{†1,2}, and Srinathan Kannan\textsuperscript{§1,2}

\textsuperscript{1}Centre for Security Theory and Algorithmic Research, International Institute of Information Technology, Gachibowli, Hyderabad 500 032, Telangana, India.
\textsuperscript{2}Centre for Quantum Science and Technology, International Institute of Information Technology, Gachibowli, Hyderabad 500 032, Telangana, India.

April 7, 2023

Abstract

In Quantum secret sharing we can share both quantum and classical secrets with a quantum resource. In this article we study the problem of revocation of quantum secret shared by the dealer with two shareholders in a three party scenario. In the existing secret sharing protocols there are no means by which the dealer can retrieve back the secret once he/she finds all the share holders to be semi-honest\textsuperscript{1}. In this work, we are not dealing with shareholders who are dishonest. We state clearly that in our quantum secret sharing protocol, we explicitly deal with shareholders who are semi-honest and not dishonest. Our protocol makes a significant advancement in solving this problem by designing strategy in bringing back the secret in the worst possible situation when all the shareholders/receivers are semi-honest. In our proposed strategy the dealer also possesses a quantum share of the secret which empowers the dealer to bring back the secret even after sharing is done. However the protocol along with the revocation process also ensures the normal reconstruction at the share holder’s location when they are honest. This advantage comes with the expense of extra one qubit on dealer’s side and consequently we require a four qubit resource to start with for 1-dealer and 2-share holder’s scenario. Here in this article we not only give the description of our protocol but also give an example where our protocol is working with the help of a four qubit entangled state. We also explicitly found out the range of parameter for the input state for which the protocol will be successful.

1 Introduction

In classical cryptography, secret sharing is a protocol where some sensitive classical data is distributed among number of people such that sufficiently large subsets of those people can collectively reconstruct the data, but they can gain no information about the sensitive data from their respective individual shares. For instance, a possible application is to share the key for a accessing a joint account controlled by many people. No individual is able to withdraw money, but sufficiently large groups can withdraw the money or access the account. One particular symmetric variety of secret sharing scheme is called

\textsuperscript{1}By semi-honest, we mean that the receivers diligently participate in the protocol, follow and execute the protocol as well, but are curious to know about the secret of the dealer, and also desire to take other parties’ private information, but cannot collude with dishonest or malicious parties\textsuperscript{[1]}. They are different from malicious/dishonest receivers/parties who can easily destroy or alter the secret, thereby making revocation impossible\textsuperscript{[2]}.
a threshold scheme. A \((k,n)\) classical threshold scheme has \(n\) share holders, of which any \(k\) are sufficient to reconstruct the secret, while any set of \(k - 1\) or fewer shares has no information about the secret.

Quantum secret sharing (QSS) \([3, 4]\) deals with the problem of sharing of both classical as well as quantum secrets, however the resources used for secret sharing are purely quantum mechanical in nature. A typical protocol for quantum secret sharing, like many other tasks in quantum cryptography, uses quantum entanglement \([5]\) as a cardinal resource, mostly pure entangled states as quantum entanglement acts as a very useful resource in carrying out various protocols like quantum teleportation \([6, 7]\), quantum cryptography \([8]\) and quantum secret sharing (QSS) \([3]\). Karlsson et al. \([9]\) studied quantum secret sharing protocols using bipartite pure entangled states as resources. Many authors investigated the concept of quantum secret sharing using tripartite pure entangled states and multi-partite states like graph states \([10, 11, 12, 13, 14, 15, 16]\). Q. Li et al. \([17]\) proposed semi-quantum secret sharing protocols taking maximally entangled GHZ state as resource. In a realistic situation however, the secret sharing of classical or quantum information involves transmission of qubits through noisy channels that give rise to mixed states. Several works were done in this context where mixed and noisy entangled states were taken as a resource for the purpose of secret sharing \([18, 19, 20]\). Quantum secret sharing has also been realized in experiments \([21, 22, 23]\).

2 Motivation

In most of the quantum secret sharing scenarios, the protocols ensure security only if some of the share holders are semi-honest instead of all. However these protocols fail to address the security when the dealer after sharing finds all the share holders to be semi-honest. In that situation they can collaborate with each other and reveal the secret without the dealer’s consent. Hence, once the secret is shared, the dealer has no way to bring the secret back to herself/himself.

Definition 1. By semi-honest share holders, we mean that the receivers diligently participate in the protocol, follow and execute the protocol as well, but are curious to know about the secret of the dealer, and also desire to take other parties’ private information, but cannot collude with dishonest or malicious parties \([1]\).

Definition 2. By dishonest share holders, we mean that the receivers may use fake shares in the secret reconstruction phase \([24]\) or try to sabotage the action \([25]\).

In this work, we are not dealing with shareholders who are dishonest. We clearly state that in our quantum secret sharing protocol, that we explicitly deal with shareholders who are ‘semi-honest’ and not ‘dishonest’. It is important to mention here that the secret sharing of classical information is different from the sharing of the quantum information. In case of secret sharing of classical information, if both the receivers are semi honest it is a no-win scenario as they can always clone their classical information on their part and combine to get back the original secret without hampering the original protocol. Now since here the secret is a quantum secret, the no-cloning theorem does not allow at the very first place to clone the secret by the shareholders. So, it becomes necessary to investigate from the dealer’s point of view how to revive the secret if all the shareholders turn out to be semi-honest. The original paper by Mark Hillery \([3]\) on Quantum Secret Sharing talks of dishonest shareholders/receivers although their paper does not talk of the semi-honest shareholders colluding among themselves to know the secret. We also clarify that the secret sharing is not all about authorization. We assume only authorized people are participating in the protocol. The problem is about what is being given to the authorized people/shareholders in the form of the share of the secret.

We address this problem of quantum secrets by taking a simple scenario when there is one dealer Alice and the secret is shared between Bob and Charlie. Here in our protocol we empower the dealer to keep a part of the quantum secret (which we refer to as quantum share) with herself which enables
her to stop the reconstruction of the secret by Bob and Charlie and consequently retrieve the secret when she finds both of them to be semi-honest. This empowerment comes at the cost of one extra qubit with the dealer. So for a three party scenario (one dealer and two additional share holders) we need a four qubit entangled state as a resource for the execution of the protocol. However if the dealer (Alice) is not revoking the secret, then all the shareholders can reconstruct the secret using our protocol at their location. In addition of introducing our protocol, we explicitly work with a class of four qubits pure entangled state as a resource.

In section II we introduce our revocation and reconstruction protocol for one dealer and two shareholders and introduce the concept of quantum share of the secret. In section III we execute our protocol with a four qubit pure entangled state as a resource. In particular we find out the range based on the input state parameters under which both revocation at the dealer’s location and the reconstruction at the share holder’s location will be possible.

3 The Partial Secret Sharing Protocol: Quantum Share Of The Secret

In this section we first discuss what is the difficulty in carrying out this protocol in 3-party, 3-qubit scenario. Further we give an outline of our protocol in general and introduce the concept of quantum share of secret in that process.

3.1 Going Beyond Three Qubit Secret Sharing

In most of the existing Quantum Secret Sharing (QSS) protocols, the dealer (Alice), who is having the secret will first split the quantum information by combining her secret with the resource state and then does a two qubit measurement of the secret qubit and the resource qubit shared with her. In this case Alice, Bob and Charlie (Bob and Charlie are the two parties with whom Alice wants to share the secret) are sharing a three qubit resource among them with each possessing one qubit. The measurement will result in the secret being shared into two quantum qubits with the other two parties, Bob and Charlie. Alice will only have classical outcome of the measurement but not a quantum part of the secret that she has shared. The strength of 3-party, 3-qubit protocol is that if one of the share holders (Bob or Charlie) is semi-honest, he can not reveal the secret. The existing protocol gives full security to it. However if both of them are semi-honest they can collaborate with each other to get hold of the secret, and Alice can not do anything about it. This can allow Bob and Charlie, if semi-honest to collude and reconstruct the exact secret qubit with a probability of $1/4$.

Alice combines her qubit (secret), $\alpha|0\rangle_A + \beta|1\rangle_A$, with her share in the 3-qubit GHZ resource $a, b, c$ such that only Alice has access to $a$, only Bob has access to $b$, and only Charlie has access to $c$ [3]. After measuring the pair in the Bell basis, she now conveys the result of her measurement to Bob or Charlie. Assuming Bob now measures his state in the Hadamard basis, Charlie is able to reconstruct the secret. However he needs two bits of classical information in order to reconstruct the secret. Hence, after Alice now conveys the result of her measurement in Bell basis to Bob or Charlie, Charlie can reconstruct Alice’s state but only with Bob’s assistance [3]. Bob must measure his state and send the result to Charlie. Without Bob’s information, Charlie can not reconstruct Alice’s state. If Alice comes to know that either Bob is semi-honest or Charlie is semi-honest or both are semi-honest, she does not share her results of measurement in the Bell basis with Bob or Charlie. Even then, Bob and Charlie can reconstruct the exact secret without the help of Alice with a probability of $1/4$. However, if Alice comes to know that either Bob is semi-honest or Charlie is semi-honest or both are semi-honest after conveying the results of her measurement in the Bell basis, there is nothing she can do to prevent Bob and Charlie from reconstructing the secret.
To nullify this probability, we introduce the need of one more qubit with Alice, so that she can also hold a share in the quantum form. This we refer as quantum share of the secret. Thus, Bob and Charlie will be unable to reconstruct the secret without the involvement of Alice. More interestingly if Alice finds both the party to be semi-honest, then she can always bring back the secret to her.

3.2 Our Protocol: A New Quantum Secret Sharing Protocol

In this subsection we give an outline of our protocol which requires a 4-qubit resource, with two of the qubits with Alice, the third qubit with Bob and the fourth qubit with Charlie.

**Step 1: Splitting of Quantum Information or the sharing phase.** Alice combines her secret, which is in the state $|\psi\rangle_s = \alpha|0\rangle_s + \beta|1\rangle_s$, (where $|\alpha|^2 + |\beta|^2 = 1$) with the 4-Qubit entangled resources $|X\rangle_{abcd}$, where the qubits $a$ and $b$ are with Alice, while $c$ and $d$ are with Bob and Charlie respectively. She measures the secret $s$ and the qubit $a$ in the Bell basis, and she gets one of the four possible outcomes $\{\psi^\pm, \phi^\pm\}$ (Bell states). Corresponding to each measurement outcomes, Alice, Bob and Charlie share three qubit entanglement among each other. The secret is shared in form of three qubit entanglement among these three parties (see Fig 1).

**Step 2: Revocation and Reconstruction of the secret.** Alice then uses her second qubit (quantum share of the resource) to participate in the reconstruction of the secret along with Bob or Charlie. If Charlie needs to reconstruct the secret, Alice and Bob measure their respective particles in the Hadamard basis. At this point, if Alice comes to know that either Bob or Charlie is semi-honest or both are semi-honest, she will not measure her state and the chance that Charlie retrieves the secret is zero. In addition to that Alice can bring back her secret by asking Bob and Charlie to do their measurements in the Hadamard basis. The importance of the protocol is that the dealer Alice holds a quantum share of the secret with herself, which empowers her to stop the revealing of the secret and consequently bring the entire secret back to herself without revealing it even after sharing (see Figure 1).

Figure 1

4 Implementation Of Our Protocol With Four Qubit Resource

In this section we consider a particular class of four qubit state [25] and investigate whether they will be useful to be used as resource states for our protocol. We begin with the first 4-qubit normalized $G_{abcd}$
state:

\[ |G_{abcd} \rangle = \frac{a + d}{2} (|0000\rangle + |1111\rangle) + \frac{a - d}{2} (|1100\rangle + |0011\rangle) + \frac{b + c}{2} (|0101\rangle + |1010\rangle) + \frac{b - c}{2} (|0110\rangle + |1001\rangle) \]

with \( a, b, c \) and \( d \) being complex numbers and the normalization condition being \( |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1 \). Here, the first two qubits are with Alice, the third one with Bob and the last one with Charlie. Here Alice is the dealer who shares the secret with both Bob and Charlie. The secret to be shared by Alice is given by the one qubit state \( |\psi_S\rangle = \alpha|0\rangle + \beta|1\rangle \) where \( |\alpha|^2 + |\beta|^2 = 1 \).

The combined state of the system with the message and the resource is given by:

\[ |\psi_S\rangle \otimes |G_{abcd} \rangle = \{ \alpha|0\rangle + \beta|1\rangle \} \otimes \frac{a + d}{2} (|0000\rangle + |1111\rangle) + \frac{a - d}{2} (|1100\rangle + |0011\rangle) + \frac{b + c}{2} (|0101\rangle + |1010\rangle) + \frac{b - c}{2} (|0110\rangle + |1001\rangle) \]

Our next target is to see how the dealer Alice is revoking back the secret which is already shared with Bob and Charlie with the state \( G_{abcd} \) as a resource. Revocation is important when Alice decides to change the secret or Alice guesses that recipients are no longer trustworthy, or there is an update of secret in higher level application using secret sharing as a subroutine. Now if we rewrite the combined system with the secret qubit \( S \) and the first qubit of Alice in the Bell basis we have

\[ |\psi_S\rangle \otimes |G_{abcd} \rangle = \]

\[ (|\phi^+\rangle)(\frac{a + d}{2\sqrt{2}}(\alpha|000\rangle + \beta|111\rangle) + \frac{a - d}{2\sqrt{2}}(\alpha|011\rangle + \beta|100\rangle) + \frac{b + c}{2\sqrt{2}}(\alpha|101\rangle + \beta|010\rangle) + \frac{b - c}{2\sqrt{2}}(\alpha|110\rangle + \beta|001\rangle) + \]

\[ (|\phi^-\rangle)(\frac{a + d}{2\sqrt{2}}(\alpha|000\rangle - \beta|111\rangle) + \frac{a - d}{2\sqrt{2}}(\alpha|011\rangle - \beta|100\rangle) + \frac{b + c}{2\sqrt{2}}(\alpha|101\rangle - \beta|010\rangle) + \frac{b - c}{2\sqrt{2}}(\alpha|110\rangle - \beta|001\rangle) + \]

Our next target is to see how the dealer Alice is revoking back the secret which is already shared with Bob and Charlie with the state \( G_{abcd} \) as a resource. Revocation is important when Alice decides to change the secret or Alice guesses that recipients are no longer trustworthy, or there is an update of secret in higher level application using secret sharing as a subroutine. Now if we rewrite the combined system with the secret qubit \( S \) and the first qubit of Alice in the Bell basis we have

\[ |\psi_S\rangle \otimes |G_{abcd} \rangle = \]

\[ (|\phi^+\rangle)(\frac{a + d}{2\sqrt{2}}(\alpha|000\rangle + \beta|111\rangle) + \frac{a - d}{2\sqrt{2}}(\alpha|011\rangle + \beta|100\rangle) + \frac{b + c}{2\sqrt{2}}(\alpha|101\rangle + \beta|010\rangle) + \frac{b - c}{2\sqrt{2}}(\alpha|110\rangle + \beta|001\rangle) + \]

\[ (|\psi^-\rangle)(\frac{a + d}{2\sqrt{2}}(\alpha|000\rangle - \beta|111\rangle) + \frac{a - d}{2\sqrt{2}}(\alpha|011\rangle - \beta|100\rangle) + \frac{b + c}{2\sqrt{2}}(\alpha|101\rangle - \beta|010\rangle) + \frac{b - c}{2\sqrt{2}}(\alpha|110\rangle - \beta|001\rangle) + \]

Now Alice measures both the secret qubit and the first qubit of the resource state in the Bell basis. There will be four possible measurement outcomes \( \{\phi^\pm, \psi^\pm\} \) as a result of Alice’s measurement. In correspondence to various measurement outcomes obtained by Alice in the Bell basis, Alice, Bob and
Charlie’s qubits collapse into the states as given in TABLE I. It is important to note that the information about the secret is shared among three parties Alice, Bob, and Charlie and Alice being the dealer also has a hold on the part of the secret. The Alice’s qubit that is shared in form of a three qubit state with Bob and Charlie is the quantum share of the secret. Next we see how the dealer Alice is revoking back the secret which is already shared with Bob and Charlie.

Table 1: Sharing of Quantum Information

| Alice’s Measurement Outcomes | Alice, Bob and Charlie’s Combined State |
|-------------------------------|-----------------------------------------|
| \(|\phi^\pm\rangle\)               | \(\frac{a+d}{\sqrt{2}} [\alpha|000\rangle \pm \beta|111\rangle] + \frac{a-d}{\sqrt{2}} [\alpha|011\rangle \pm \beta|100\rangle] + \frac{b+c}{\sqrt{2}} [\alpha|101\rangle \pm \beta|010\rangle] + \frac{b-c}{\sqrt{2}} [\alpha|110\rangle \pm \beta|001\rangle]\) |
| \(|\psi^\pm\rangle\)               | \(\frac{a+d}{\sqrt{2}} [\alpha|111\rangle \pm \beta|000\rangle] + \frac{a-d}{\sqrt{2}} [\alpha|100\rangle \pm \beta|011\rangle] + \frac{b+c}{\sqrt{2}} [\alpha|010\rangle \pm \beta|101\rangle] + \frac{b-c}{\sqrt{2}} [\alpha|001\rangle \pm \beta|110\rangle]\) |

Revocation of Secret on Alice’s location: Now if we write Bob and Charlie’s qubit in the Hadamard basis, then the combined shared system of Alice, Bob, and Charlie (with Bob’s and Charlie’s qubit are written in \(|+\rangle\) and \(|-\rangle\) basis), when Alice’s initial measurement outcome is \(|\phi^\pm\rangle\), can be rewritten as,

\[
[Y_{\phi^\pm}^{234}] = \frac{a+d}{2\sqrt{2}} [\alpha|0\rangle_A |(+\rangle_B |(-\rangle_C] + \frac{a-d}{2\sqrt{2}} [\alpha|0\rangle_A |(+\rangle_B |(+\rangle_C] + \frac{b+c}{2\sqrt{2}} [\alpha|0\rangle_A |(-\rangle_B |(+\rangle_C] + \frac{b-c}{2\sqrt{2}} [\alpha|0\rangle_A |(-\rangle_B |(-\rangle_C]
\]

And if we write Bob and Charlie’s qubit in the Hadamard basis, then the combined shared system of Alice, Bob, and Charlie, when Alice’s initial measurement outcome is \(|\psi^\pm\rangle\) can be rewritten as,

\[
[Y_{\psi^\pm}^{234}] = \frac{a+d}{2\sqrt{2}} [\alpha|1\rangle_A |(+\rangle_B |(-\rangle_C] + \frac{a-d}{2\sqrt{2}} [\alpha|1\rangle_A |(+\rangle_B |(+\rangle_C] + \frac{b+c}{2\sqrt{2}} [\alpha|1\rangle_A |(-\rangle_B |(+\rangle_C] + \frac{b-c}{2\sqrt{2}} [\alpha|1\rangle_A |(-\rangle_B |(-\rangle_C]
\]

Now if Bob and Charlie carry out the measurement in Hadamard basis, the resultant state on Alice’s side is given by the following:

Bob and Charlie’s joint measurement outcome when Alice’s initial measurement outcome is \(|\phi^\pm\rangle\):
When Bob and Charlie measure in the Hadamard Basis $|+\rangle|+$, Alice’s resultant state is as follows:
\[ \sqrt{2}(aa \pm b\beta)|0\rangle + \sqrt{2}(ba \pm a\beta)|1\rangle. \]
When Bob and Charlie measure in the Hadamard Basis: $|+\rangle|-$, Alice’s resultant state is as follows:
\[ \sqrt{2}(da \pm c\beta)|0\rangle - \sqrt{2}(ca \pm d\beta)|1\rangle. \]
When Bob and Charlie measure in the Hadamard Basis $|-\rangle|+$, Alice’s resultant state is as follows:
\[ \sqrt{2}(da \mp c\beta)|0\rangle + \sqrt{2}(ca \mp d\beta)|1\rangle. \]
When Bob and Charlie measure in the Hadamard Basis $|-\rangle|-\rangle$, Alice’s resultant state is as follows:
\[ \sqrt{2}(aa \mp b\beta)|0\rangle - \sqrt{2}(ba \mp a\beta)|1\rangle. \]

Bob and Charlie’s joint measurement outcome when Alice’s initial measurement outcome is $|\psi^\pm\rangle$:
When Bob and Charlie measure in the Hadamard Basis $|+\rangle|+$, Alice’s resultant state is as follows:
\[ \sqrt{2}(ba \pm a\beta)|0\rangle + \sqrt{2}(aa \pm b\beta)|1\rangle. \]
When Bob and Charlie measure in the Hadamard Basis: $|+\rangle|-$, Alice’s resultant state is as follows:
\[ \sqrt{2}(da \mp c\beta)|0\rangle - \sqrt{2}(ca \mp d\beta)|1\rangle. \]
When Bob and Charlie measure in the Hadamard Basis $|-\rangle|+$, Alice’s resultant state is as follows:
\[ -\sqrt{2}(ca \mp d\beta)|0\rangle - \sqrt{2}(da \mp c\beta)|1\rangle. \]
When Bob and Charlie measure in the Hadamard Basis $|-\rangle|-\rangle$, Alice’s resultant state is as follows:
\[ -\sqrt{2}(ba \mp b\beta)|0\rangle - \sqrt{2}(aa \mp b\beta)|1\rangle. \]

Now if Bob and Charlie send their measurement outcomes inform of two qubits with the encoding $|+\rangle \rightarrow |0\rangle$, $|-\rangle \rightarrow |1\rangle$, Alice will be able to revive the secret with the applications of appropriate Pauli operator. However this will not be possible for all values of $a, b, c, d$. There will be certain range of the input parameters for which revocation will be possible. Next in the form of following theorem, we give the range of input parameters for which Alice will be able to revive the secret.

**Theorem 1.** For a Quantum Secret Sharing protocol to be implemented using the $G_{abcd}$ state, the necessary conditions for Alice to retrieve the secret are as follows:

1. If $a$ and $c$ are chosen as real numbers, then we have $b$ and $d$ as purely imaginary numbers such that:
   \[ a^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq a \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad d \neq b \text{ or } d \neq -b \text{ or } \frac{1}{2} - d^2 \geq 0 \]

2. If $a$ and $d$ are chosen to be real numbers, then we have $b$ and $c$ as purely imaginary numbers such that:
   \[ a^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq a \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad d^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq d \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad c \neq b \text{ or } c \neq -b \text{ or } \frac{1}{2} - c^2 \geq 0 \]

3. If $b$ and $c$ are chosen to be real numbers, then we have $a$ and $d$ as purely imaginary numbers such that:
   \[ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad d^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq d \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad a \neq b \text{ or } a \neq -b \text{ or } \frac{1}{2} - a^2 \geq 0 \]

4. If $b$ and $d$ are chosen to be real numbers, then we have $a$ and $c$ as purely imaginary numbers such that:
   \[ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad d^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq d \leq \frac{1}{\sqrt{2}} \quad \text{and} \quad c \neq b \text{ or } c \neq -b \text{ or } \frac{1}{2} - c^2 \geq 0 \]

The union of conditions 1, 2, 3 and 4 stated in Theorem 1 given above gives all the necessary values of $a, b, c$ and $d$ for Alice to retrieve the secret.
in the Hadamard basis, then the combined shared

tuple $(a, b, d)$, for which $c$ will have two possible values.
The Figure 2 above represents all possible values
of $(a, b, d)$ for condition 2 in theorem 1. For each
tuple $(a, b, d)$, $c$ will have two possible values as per
the normalization condition of the $G_{abcd}$ state. For
the protocol to be successful, the reconstruction at
the shareholder’s place should be possible in the
normal scenario when all the share holder’s are not
semi-honest. Next we consider the reconstruction
of the secret at the Charlie’s place (say). The same
procedure can be repeated for Bob also.

Reconstruction of Secret on Charlie’s location:
Now if we write Alice and Bob’s qubit
in the Hadamard basis, then the combined shared
system of Alice, Bob and Charlie, when Alice’s
initial measurement is $|\phi^\pm\rangle$ can be rewritten as:

$$|Y_{234}^\pm\rangle = \frac{a + d}{2\sqrt{2}} |\alpha[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|0\rangle|c] + \\
\frac{a - d}{2\sqrt{2}} |\alpha[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|0\rangle|c] + \\
\frac{b + c}{2\sqrt{2}} |\alpha[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|0\rangle|c] + \\
\frac{b - c}{2\sqrt{2}} |\alpha[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle + |\rangle)A(|+\rangle + |\rangle)B|0\rangle|c]$$

The combined shared system, when Alice’s initial
measurement is $|\psi^\pm\rangle$ is given by

$$|Y_{234}^\pm\rangle = \frac{a + d}{2\sqrt{2}} |\alpha[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|0\rangle|c] + \\
\frac{a - d}{2\sqrt{2}} |\alpha[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|0\rangle|c] + \\
\frac{b + c}{2\sqrt{2}} |\alpha[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|0\rangle|c] + \\
\frac{b - c}{2\sqrt{2}} |\alpha[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|1\rangle|c] \pm \\
\beta[(|+\rangle - |\rangle)A(|+\rangle - |\rangle)B|0\rangle|c]$$

Alice and Bob’s joint measurement outcomes when Alice’s initial measurement outcome is $|\phi^\pm\rangle$:

When Alice and Bob measure in the Hadamard Basis $|+\rangle|+\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c + d)\alpha \pm (a + b + c - d)\beta]|0\rangle + [(a + b - c - d)\alpha \pm (a + b + c - d)\beta]|1\rangle$$

When Alice and Bob measure in the Hadamard Basis $|+\rangle|-\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c + d)\alpha \pm (a - b + c - d)\beta]|0\rangle + [(a - b + c + d)\alpha \pm (a + b - c - d)\beta]|1\rangle$$

When Alice and Bob measure in the Hadamard Basis $|-\rangle|+\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c + d)\alpha \pm (-a + b + c + d)\beta]|0\rangle + [(a + b + c + d)\alpha \pm (-a + b - c - d)\beta]|1\rangle$$

When Alice and Bob measure in the Hadamard Basis $|-\rangle|-\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c + d)\alpha \pm (-a - b + c + d)\beta]|0\rangle + [(a - b + c + d)\alpha \pm (a + b - c + d)\beta]|1\rangle$$

Alice and Bob’s joint measurement outcomes when Alice’s initial measurement outcome is $|\psi^\pm\rangle$:

When Alice and Bob measure in the Hadamard Basis $|+\rangle|+\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c - d)\alpha \pm (a + b + c + d)\beta]|0\rangle + [(a + b - c + d)\alpha \pm (a + b + c + d)\beta]|1\rangle$$

When Alice and Bob measure in the Hadamard Basis $|+\rangle|-\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c - d)\alpha \pm (a - b + c + d)\beta]|0\rangle + [(a - b + c + d)\alpha \pm (a + b - c + d)\beta]|1\rangle$$

When Alice and Bob measure in the Hadamard Basis $|-\rangle|+\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c - d)\alpha \pm (-a + b + c + d)\beta]|0\rangle + [(a - b - c + d)\alpha \pm (a + b + c + d)\beta]|1\rangle$$

When Alice and Bob measure in the Hadamard Basis $|-\rangle|-\rangle$, Charlie’s resultant state is as follows:

$$\frac{1}{\sqrt{2}}[(a + b + c - d)\alpha \pm (-a - b + c + d)\beta]|0\rangle + [(a - b - c + d)\alpha \pm (a + b - c + d)\beta]|1\rangle$$
When Alice and Bob measure in the Hadamard Basis \(|+\rangle\rangle -\rangle), Charlie’s resultant state is as follows:
\[ \frac{1}{\sqrt{2}} \left[ \left( a - b - c - d \right) \alpha \pm \left( a - b + c + d \right) \beta \right] |0\rangle + \left( a + b - c - d \right) \alpha \pm \left( a - b - c + d \right) \beta |1\rangle. \]
When Alice and Bob measure in the Hadamard Basis \(|-\rangle\rangle +\rangle), Charlie’s resultant state is as follows:
\[ \frac{1}{\sqrt{2}} \left[ \left( a + b + c + d \right) \alpha \pm \left( a - b + c + d \right) \beta \right] |0\rangle + \left( a + b - c - d \right) \alpha \pm \left( a - b - c - d \right) \beta |1\rangle. \]
When Alice and Bob measure in the Hadamard Basis \(|-\rangle\rangle -\rangle), Charlie’s resultant state is as follows:
\[ \frac{1}{\sqrt{2}} \left[ \left( a - b - c + d \right) \alpha \pm \left( a + b + c + d \right) \beta \right] |0\rangle + \left( a + b - c - d \right) \alpha \pm \left( a - b + c - d \right) \beta |1\rangle. \]

Now if Alice and Bob send their measurement outcomes inform of two qubits with the same encoding \(|+\rangle\rangle \rightarrow |0\rangle, |-\rangle\rangle \rightarrow |1\rangle), Charlie can reconstruct the initial secret by applying appropriate Pauli operators on his obtained state. Just like in the case of revocation, here reconstruction of the secret will not be possible for all values of \(a, b, c, d\). There will be certain range of the input parameters for which the reconstruction will take place. Next in the form of following theorem, we give the range of input parameters for which Charlie will be able to revive the secret.

**Theorem 2.** For a Quantum Secret Sharing protocol to be implemented using the \(G_{abcd}\) state, the necessary conditions for Charlie to reconstruct the secret are as follows:

1. If \(a\) and \(c\) are chosen as imaginary numbers, and \(b\) and \(d\) are chosen as imaginary numbers, then we have:
   \[ (a)\ a = c \text{ and } b = d \ (b)\ a^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq a \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |b|^2 = \frac{1}{2} - a^2 \ (e)\ |d|^2 = \frac{1}{2} - c^2 \]

2. If \(a\) and \(d\) are chosen as imaginary numbers, and \(b\) and \(c\) are chosen as imaginary numbers, then we have:
   \[ (a)\ a = -d \text{ and } b = -c \ (b)\ a^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq a \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |b|^2 = \frac{1}{2} - a^2 \ (e)\ |c|^2 = \frac{1}{2} - |d|^2 \]

3. If \(b\) and \(c\) are chosen as real numbers, and \(a\) and \(d\) are chosen as imaginary numbers, then we have:
   \[ (a)\ b = c \text{ and } a = d \ (b)\ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |a|^2 = \frac{1}{2} - b^2 \ (e)\ |d|^2 = \frac{1}{2} - c^2 \]

4. If \(b\) and \(d\) are chosen as real numbers, and \(a\) and \(c\) are chosen as imaginary numbers, then we have:
   \[ (a)\ b = -d \text{ and } a = -c \ (b)\ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |a|^2 = \frac{1}{2} - b^2 \]

5. If \(a\) and \(c\) are chosen as real numbers, and \(b\) and \(d\) are chosen as imaginary numbers, then we have:
   \[ (a)\ b = -d \text{ and } a = -c \ (b)\ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |a|^2 = \frac{1}{2} - b^2 \]

6. If \(a\) and \(d\) are chosen as real numbers, and \(b\) and \(c\) are chosen as imaginary numbers, then we have:
   \[ (a)\ b = c \text{ and } a = d \ (b)\ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |a|^2 = \frac{1}{2} - b^2 \]

7. If \(b\) and \(d\) are chosen as real numbers, and \(a\) and \(c\) are chosen as imaginary numbers, then we have:
   \[ (a)\ a = -d \text{ and } b = -c \ (b)\ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |a|^2 = \frac{1}{2} - b^2 \]

8. If \(b\) and \(d\) are chosen as real numbers, and \(a\) and \(c\) are chosen as imaginary numbers, then we have:
   \[ (a)\ a = c \text{ and } b = d \ (b)\ b^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}} \ (c)\ c^2 \leq \frac{1}{2} \text{ or } -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \ (d)\ |a|^2 = \frac{1}{2} - b^2 \]

For the proposed protocol to be successful there will be common range of the values of \(a, b, c, d\) for which both revocation and reconstruction will be possible which we get by the union of conditions 1, 2, 3, 4, 5, 6, 7 and 8 in theorem 2 given above.
The intersection of the plane and the cylinder in the Figure 3 above gives all possible values of the tuple \((a, b, d)\) for condition 2 in theorem 2, and where \(c\) will have a unique value.

5 Conclusion:

In this article we address the revocation and reconstruction of quantum secret for 1-dealer and 2-share holders scenario using 4-qubit entangled states. Here Alice, (the dealer) also possesses a quantum share of the secret and can always bring back her secret with the help of that quantum share when she finds other shareholders to be semi honest. The protocol ensures the normal reconstruction of the secret at shareholder’s location otherwise. The actual advantage of the protocol is, it prevents the shareholders from any possibility of reconstructing the secret if they are semi honest. We not only give the basic idea of the protocol but also exemplify with the help of four qubit state. In particular, we find out the explicit ranges based on the input state parameter for which our protocol will be successful. Our protocol will ensure an additional level of security to the normal quantum secret sharing protocols when all the shareholders are semi honest.

Note: For proof of Theorem 1 and Theorem 2, please see the Appendix.

References

[1] Zhang, Cai et al. (2020), doi:10.1038/s41598-020-77579-w
[2] Sazim, S. and Chiranjeevi, V. and Chakrabarty, I. and Srinathan, Quant. Inf. Proc. Volume 14, Issue 12, pp 4651-4664 (2015)
[3] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A 59, 1829 (1999);
[4] R. Cleve et.al, Phys.Rev.Lett. 83 (1999) 648-651
[5] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. 47, 777 (1935);
[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. 70, 1895 (1993).
[7] D. Bouwmeester, J-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Experimental quantum teleportation, Nature 390, 575-579 (1997).
[8] N. Gisin, G. Ribordy, W. Tittel, and H.Zbinden, Rev. Mod. Phys. 74, 145 (2002)
[9] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A 59, 162 (1999).
[10] S. Bandyopadhyay, Phys. Rev. A 62, 012308 (2000);
[11] S. Bagherinezhad, and V. Karimipour, Phys. Rev. A 67, 044302 (2003).
[12] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. 92, 177903 (2004).
[13] G. Gordon, and G. Rigolin, Phys. Rev. A
Appendix 1: (Proof of Theorem 1)

For Alice to successfully retrieve the secret, Bob and Charlie must measure their respective qubits in the Hadamard Basis. We show how Alice can retrieve her message by enlisting down the respective local operations corresponding to Bob’s and Charlie’s measurement outcomes.

If Bob and Charlie’s joint measurement outcome in Hadamard Basis $|++\rangle$, the resultant state on Alice’s side is given by the following (when Alice’s initial measurement outcome is $|φ^+\rangle$):

$$\sqrt{2}\{(aα + bβ)|0\rangle + (bα + aβ)|1\rangle\}$$

Condition of normalization of the above Alice’s resultant state is as follows:

$$|a|^2 + |b|^2 + (a\bar{b} + b\bar{a})(α\bar{β} + β\bar{α}) = \frac{1}{2}$$

In order to find Alice’s Local Operations state for retrieving the secret, we proceed by taking a Unitary Matrix as follows:

$$U = \begin{bmatrix}
    a_1 + ib_1 & c_1 - id_1
    c_1 + id_1 & -a_1 + ib_1
\end{bmatrix}$$

such that $\text{det}(U) = -1$

We need to find $a_1, b_1, c_1, d_1$ by the solving the following equation for Alice to retrieve the secret:

$$\begin{bmatrix}
    a_1 + ib_1 & c_1 - id_1
    c_1 + id_1 & -a_1 + ib_1
\end{bmatrix} \begin{bmatrix}
    \sqrt{2}(aα + bβ) \\
    \sqrt{2}(bα + aβ)
\end{bmatrix} = \begin{bmatrix}
    α \\
    β
\end{bmatrix}$$

As $a, b, α$ and $β$ are complex numbers, we write $a = x_1 + iy_1, b = x_2 + iy_2, α = x_3 + iy_3, β = x_4 + iy_4$.

The above equation transforms as follows:

$$\begin{bmatrix}
    a_1 + ib_1 & c_1 - id_1
    c_1 + id_1 & -a_1 + ib_1
\end{bmatrix} \begin{bmatrix}
    \sqrt{2}(λ_1 + iλ_2) \\
    \sqrt{2}(λ_3 + iλ_4)
\end{bmatrix} = \begin{bmatrix}
    α \\
    β
\end{bmatrix}$$
Where we have:

\[
\begin{align*}
\lambda_1 &= x_1 x_3 + x_2 x_4 - y_1 y_3 - y_2 y_4 \\
\lambda_2 &= x_3 y_1 + x_1 y_3 + x_2 y_4 + x_4 y_2 \\
\lambda_3 &= x_2 x_3 + x_1 x_4 - y_1 y_4 - y_2 y_3 \\
\lambda_4 &= x_3 y_2 + x_4 y_1 + x_2 y_3 + x_1 y_4
\end{align*}
\]

Such that:

\[
\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 = |a|^2 + |b|^2 + (\bar{a}b + a\bar{b})(\alpha\beta + \alpha\bar{\beta}) = \frac{1}{2}
\]

Solving the above equation by comparing real and imaginary parts on both sides to get:

\[
\begin{align*}
a_1 &= \frac{\lambda_1 x_3 + \lambda_2 y_3 - \lambda_3 x_4 - \lambda_4 y_4}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_1 x_3 + \lambda_2 y_3 - \lambda_3 x_4 - \lambda_4 y_4) \\
b_1 &= \frac{\lambda_1 y_3 - \lambda_2 x_3 + \lambda_3 y_4 - \lambda_4 x_4}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_1 y_3 - \lambda_2 x_3 + \lambda_3 y_4 - \lambda_4 x_4) \\
c_1 &= \frac{\lambda_1 x_4 + \lambda_2 y_4 + \lambda_3 x_3 + \lambda_4 y_3}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_1 x_4 + \lambda_2 y_4 + \lambda_3 x_3 + \lambda_4 y_3) \\
d_1 &= \frac{\lambda_4 x_3 - \lambda_3 y_3 + \lambda_1 y_4 - \lambda_2 x_4}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_4 x_3 - \lambda_3 y_3 + \lambda_1 y_4 - \lambda_2 x_4)
\end{align*}
\]
Using equations (9), (10), (11) and (12), we obtain the Unitary matrix as follows:

\[
\begin{bmatrix}
\sqrt{2}\{(\tilde{a} - (\tilde{a} + a)|\beta|^2 + (\tilde{b} - b)|\alpha|^2\} & \sqrt{2}\{b + (\tilde{a} + a)|\alpha\beta + (\tilde{b} - b)|\alpha|^2\} \\
\sqrt{2}\{\tilde{b} + (\tilde{a} + a)|\alpha\beta - (\tilde{b} - b)|\alpha|^2\} & \sqrt{2}\{-a + (\tilde{a} + a)|\beta|^2 + (\tilde{b} - b)|\alpha|^2\}
\end{bmatrix}
\]

Since the elements of the matrix need to be independent of \(\alpha\) and \(\beta\), we have the following conditions:

\(\tilde{a} + a = 0\) \hspace{1cm} (13)
\(\tilde{b} - b = 0\) \hspace{1cm} (14)

From eq (13) we have \(a\) to be purely imaginary and from eq (14) we have \(b\) to be purely real. After the imposition of the above conditions eq (13) and (14), the Unitary Matrix reduces to:

\[
U = \begin{bmatrix}
\sqrt{2}\tilde{a} & \sqrt{2}b \\
\sqrt{2}b & -\sqrt{2}a
\end{bmatrix}
= \begin{bmatrix}
-\sqrt{2}a & \sqrt{2}b \\
\sqrt{2}b & -\sqrt{2}a
\end{bmatrix}
\]

Where we made use of eq (14) and eq (15) above, \(\tilde{a} + a = 0\) or \(\tilde{a} = -a\) and \(\tilde{b} - b = 0\) or \(\tilde{b} = b\)

\[\text{det}(U) = 2a^2 - 2b^2 = -1 \text{ or } 2b^2 - 2a^2 = 1\]

Using the above matrix, Alice successfully retrieves the secret as follows:

\[
\begin{bmatrix}
-\sqrt{2}a & \sqrt{2}b \\
\sqrt{2}b & -\sqrt{2}a
\end{bmatrix}
\begin{bmatrix}
\sqrt{2}(a\alpha + b\beta) \\
\sqrt{2}(b\alpha + a\beta)
\end{bmatrix}
= \begin{bmatrix}
2(-a^2\alpha - ab\beta + b^2\alpha + ab\beta) \\
2(ab\alpha + b^2\beta - ab\alpha - a^2\beta)
\end{bmatrix}
= \begin{bmatrix}
2(b^2 - a^2)\alpha \\
2(b^2 - a^2)\beta
\end{bmatrix}
= \begin{bmatrix}
\alpha \\
\beta
\end{bmatrix}
\]

Expressing the above matrix in terms of Pauli Matrices, we have \(U = \sqrt{2}(-aI + b\sigma_x)\)

Now as \(2b^2 - 2a^2 = 1\), we have \(a^2 = b^2 - \frac{1}{2}\)

Since \(a\) is purely imaginary, we must have \(b^2 \leq \frac{1}{2}\) or \(-\frac{1}{\sqrt{2}} \leq b \leq \frac{1}{\sqrt{2}}\). Now from the condition of normalization of Alice’s resultant state, we have:

\[|a|^2 + |b|^2 + (\tilde{a}b + a\tilde{b})(\alpha\beta + \tilde{\alpha}\tilde{\beta}) = \frac{1}{2}\]

As \(b = \tilde{b}\), the above equation reduces to:

\[|a|^2 + |b|^2 + b(\tilde{a} + a)(\alpha\beta + \tilde{\alpha}\tilde{\beta}) = \frac{1}{2}\]

And as \(\tilde{a} + a = 0\), the above equation further reduces to:

\[|a|^2 + |b|^2 = \frac{1}{2}\]
As $b$ is a real number, $b^2 = |b|^2$ and so we have:

$$|a|^2 + b^2 = \frac{1}{2}$$

or

$$|a|^2 = \frac{1}{2} - b^2$$

**Appendix 2: (Proof of Theorem 1)**

If Bob and Charlie’s joint measurement outcome in Hadamard Basis is $|+−\rangle$, the resultant state on Alice’s side is given by the following (when Alice’s initial measurement outcome is $|\phi^+\rangle$):

$$\sqrt{2}\{(d\alpha + c\beta)|0\rangle - (c\alpha + d\beta)|1\rangle\}$$

Condition of normalization of the above Alice’s resultant state is as follows:

$$|c|^2 + |d|^2 + (\bar{c}d + d\bar{c})(\bar{\alpha}\beta + \alpha\bar{\beta}) = \frac{1}{2}$$

In order to find Alice’s Local Operations state for retrieving the secret, we proceed by taking a Unitary Matrix as follows:

$$U = \begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix}$$

such that $\det(U) = -1$

We need to find $a_1, b_1, c_1, d_1$ by the solving the following equation for Alice to retrieve the secret:

$$\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \sqrt{2}(d\alpha + c\beta) \\ -\sqrt{2}(c\alpha + d\beta) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

As $a, b, \alpha$ and $\beta$ are complex numbers, we write $d = x_1 + iy_1, c = x_2 + iy_2, \alpha = x_3 + iy_3, \beta = x_4 + iy_4$. The above equation transforms as follows:

$$\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \sqrt{2}(\lambda_1 + i\lambda_2) \\ -\sqrt{2}(\lambda_3 + i\lambda_4) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Where we have:

$$\lambda_1 = x_1x_3 + x_2x_4 - y_1y_3 - y_2y_4$$
$$\lambda_2 = x_3y_1 + x_1y_3 + x_2y_4 + x_4y_2$$
$$\lambda_3 = x_2x_3 + x_1x_4 - y_1y_4 - y_2y_3$$
$$\lambda_4 = x_3y_2 + x_4y_1 + x_2y_3 + x_1y_4$$
Solving the above equation by comparing real and imaginary parts on both sides to get:

\[ \lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 = |a|^2 + |b|^2 + (\tilde{a}b + a\tilde{b})(\alpha\beta + \tilde{\alpha}\tilde{\beta}) = \frac{1}{2} \quad (15) \]

Using equations (16), (17), (18) and (19), we obtain the Unitary matrix as follows:

\[
\begin{bmatrix}
\sqrt{2}(\tilde{d}(d - \tilde{d})|\beta|^2 + (c + \tilde{c})|\alpha|^2) & \sqrt{2}(c - (d - \tilde{d})\alpha\beta - (\tilde{c} + c)|\alpha|^2) \\
\sqrt{2}(\tilde{c} + (d - \tilde{d})\tilde{\alpha}\beta + (\tilde{c} + c)|\alpha|^2) & \sqrt{2}(-d + (d - \tilde{d})|\beta|^2 - (c + \tilde{c})\tilde{\alpha}\beta)
\end{bmatrix}
\]
Since the elements of the matrix need to be independent of $\alpha$ and $\beta$, we have the following conditions:

$$d - \tilde{d} = 0 \quad (20)$$

$$c + \tilde{c} = 0 \quad (21)$$

From eq (20) we have $d$ to be purely real and from eq (21) we have $c$ to be purely imaginary. After the imposition of the above conditions eq (20) and (21), the Unitary Matrix reduces to:

$$U = \begin{bmatrix} \sqrt{2}d & \sqrt{2}c \\ \sqrt{2}\tilde{c} & -\sqrt{2}\tilde{d} \end{bmatrix} = \begin{bmatrix} \sqrt{2}\tilde{d} & \sqrt{2}c \\ -\sqrt{2}c & -\sqrt{2}\tilde{d} \end{bmatrix}$$

Where we made use of eq (20) and eq (21) above, $d - \tilde{d} = 0$ or $d = \tilde{d}$ and $c + \tilde{c} = 0$ or $c = -\tilde{c}$.

$$\det(U) = 2c^2 - 2d^2 = -1 \text{ or } 2d^2 - 2c^2 = 1$$

Using the above matrix, Alice successfully retrieves the secret as follows:

$$\begin{bmatrix} \sqrt{2}d & \sqrt{2}c \\ \sqrt{2}\tilde{c} & -\sqrt{2}\tilde{d} \end{bmatrix} \begin{bmatrix} \sqrt{2}(d\alpha + c\beta) \\ -\sqrt{2}(c\alpha + d\beta) \end{bmatrix} = \begin{bmatrix} 2(d^2 - c^2)\alpha \\ 2(d^2 - c^2)\beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Expressing the above matrix in terms of Pauli Matrices, we have $U = \sqrt{2}(d\sigma_x + ic\sigma_y)$

Now as $2d^2 - 2c^2 = 1$, we have $c^2 = d^2 - \frac{1}{2}$

Since $c$ is purely imaginary, we must have $d^2 \leq \frac{1}{2}$ or $-\frac{1}{\sqrt{2}} \leq d \leq \frac{1}{\sqrt{2}}$. Now from the condition of normalization of Alice’s resultant state, we have:

$$|d|^2 + |c|^2 + (\tilde{d}c + d\tilde{c})(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}$$

As $d = \tilde{d}$, the above equation reduces to:

$$|d|^2 + |c|^2 + d(c + \tilde{c})(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}$$

And as $\tilde{c} + c = 0$, the above equation further reduces to:

$$|d|^2 + |c|^2 = \frac{1}{2}$$

As $d$ is a real number, $d^2 = |d|^2$ and so we have:

$$|c|^2 + d^2 = \frac{1}{2}$$

or

$$|c|^2 = \frac{1}{2} - d^2$$
Appendix 3: (Proof of Theorem 1)

For Alice to successfully retrieve the secret, Bob and Charlie must measure their respective qubits in the Hadamard Basis. We show how Alice can retrieve back her message by enlisting down the respective local operations corresponding to Bob’s and Charlie’s measurement outcomes.

If Bob and Charlie’s joint measurement outcome in Hadamard Basis is \(|++\rangle\), the resultant state on Alice’s side is given by the following (when Alice’s initial measurement outcome is \(|\phi^-\rangle\)):

\[
\sqrt{2}\{(d\alpha - c\beta)|0\rangle - (c\alpha - d\beta)|1\rangle\}
\]

Condition of normalization of the above Alice’s resultant state is as follows:

\[
|c|^2 + |d|^2 + (\tilde{c}d - d\tilde{c})(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}
\]

In order to find Alice’s Local Operations state for retrieving the secret, we proceed by taking a Unitary Matrix as follows:

\[
U = \begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix}
\]

such that \(\det(U) = -1\)

We need to find \(a_1, b_1, c_1, d_1\) by the solving the following equation for Alice to retrieve the secret:

\[
\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \sqrt{2}(d\alpha - c\beta) \\ -\sqrt{2}(c\alpha - d\beta) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}
\]

As \(a, b, \alpha\) and \(\beta\) are complex numbers, we write \(d = x_1 + iy_1, c = x_2 + iy_2, \alpha = x_3 + iy_3, \beta = x_4 + iy_4\).

The above equation transforms as follows:

\[
\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \sqrt{2}(\lambda_1 + i\lambda_2) \\ \sqrt{2}(\lambda_3 + i\lambda_4) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}
\]

Where we have:

\[
\begin{align*}
\lambda_1 &= x_1x_3 - x_2x_4 - y_1y_3 + y_2y_4 \\
\lambda_2 &= x_3y_1 + x_1y_3 - x_2y_4 - x_4y_2 \\
\lambda_3 &= -x_2x_3 + x_1x_4 - y_1y_4 + y_2y_3 \\
\lambda_4 &= -x_3y_2 + x_4y_1 - x_2y_3 + x_1y_4
\end{align*}
\]

Such that:

\[
\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 = |d|^2 + |c|^2 + (\tilde{c}d + d\tilde{c})(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}
\]  (22)
Using equations (23), (24), (25) and (26), we obtain the Unitary matrix as follows:

\[
\begin{align*}
\alpha & = \frac{\lambda_1 x_3 + \lambda_2 y_3 - \lambda_3 x_4 - \lambda_4 y_4}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_1 x_3 + \lambda_2 y_3 - \lambda_3 x_4 - \lambda_4 y_4) \\
b_1 & = \frac{\lambda_1 y_3 - \lambda_2 x_3 + \lambda_3 y_4 - \lambda_4 x_4}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_1 y_3 - \lambda_2 x_3 + \lambda_3 y_4 - \lambda_4 x_4) \\
c_1 & = \frac{\lambda_1 x_4 + \lambda_2 y_4 + \lambda_3 x_3 + \lambda_4 y_3}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_1 x_4 + \lambda_2 y_4 + \lambda_3 x_3 + \lambda_4 y_3) \\
d_1 & = \frac{\lambda_4 x_3 - \lambda_3 y_3 + \lambda_1 y_4 - \lambda_2 x_4}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} = \sqrt{2}(\lambda_4 x_3 - \lambda_3 y_3 + \lambda_1 y_4 - \lambda_2 x_4)
\end{align*}
\]

Solving the above equation by comparing real and imaginary parts on both sides to get:

\[
\begin{align*}
\alpha &= \frac{\sqrt{2}(\lambda_1 x_3 + \lambda_2 y_3 - \lambda_3 x_4 - \lambda_4 y_4)}{\sqrt{2}(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)} \\
b_1 &= \sqrt{2}(\lambda_1 y_3 - \lambda_2 x_3 + \lambda_3 y_4 - \lambda_4 x_4) \\
c_1 &= \sqrt{2}(\lambda_1 x_4 + \lambda_2 y_4 + \lambda_3 x_3 + \lambda_4 y_3) \\
d_1 &= \sqrt{2}(\lambda_4 x_3 - \lambda_3 y_3 + \lambda_1 y_4 - \lambda_2 x_4)
\end{align*}
\]

\[
\begin{align*}
a_1 &= \sqrt{2}\{(\lambda_1 - i\lambda_2)\alpha - (\lambda_3 + i\lambda_4)\beta\} \\
&= \sqrt{2}\{(d\tilde{\alpha} - c\tilde{\beta})\alpha - (d\beta - c\alpha)\beta\} \\
&= \sqrt{2}\{(d - (d + \tilde{d})\alpha\beta + (c - \tilde{c})\alpha\beta)\}
\end{align*}
\]

Using equations (23), (24), (25) and (26), we obtain the Unitary matrix as follows:

\[
\begin{bmatrix}
\sqrt{2}\{(d - (d + \tilde{d})\alpha\beta + (c - \tilde{c})\alpha\beta)\} & \sqrt{2}\{-c + (d + \tilde{d})\alpha\beta + (c - \tilde{c})\alpha\beta\} \\
\sqrt{2}\{-\tilde{c} + (d + \tilde{d})\alpha\beta + (c - \tilde{c})\alpha\beta\} & \sqrt{2}\{-d + (d + \tilde{d})\beta^2 + (c - \tilde{c})\beta\}\end{bmatrix}
\]

Since the elements of the matrix need to be independent of \(\alpha\) and \(\beta\), we have the following conditions:

\[
\begin{align*}
d + \tilde{d} &= 0 \\
c - \tilde{c} &= 0
\end{align*}
\]

19
From eq (27) we have \( d \) to be purely imaginary and from eq (28) we have \( c \) to be purely real. After the imposition of the above conditions eq (27) and (28), the Unitary Matrix reduces to:

\[
U = \begin{bmatrix}
\sqrt{2} \tilde{d} & -\sqrt{2} c \\
-\sqrt{2} c & \sqrt{2} \tilde{d}
\end{bmatrix}
\]

Where we made use of eq (27) and eq (28) above, \( d + \tilde{d} = 0 \) or \( d = -\tilde{d} \) and \( c - \tilde{c} = 0 \) or \( c = \tilde{c} \)

\[\det(U) = 2d^2 - 2c^2 = -1 \text{ or } 2c^2 - 2d^2 = 1\]

Using the above matrix, Alice successfully retrieves the secret as follows:

\[
\begin{bmatrix}
-\sqrt{2} d & -\sqrt{2} c \\
-\sqrt{2} c & -\sqrt{2} d
\end{bmatrix}
\begin{bmatrix}
\sqrt{2}(d\alpha - c\beta) \\
\sqrt{2}(c\alpha - d\beta)
\end{bmatrix}
\]

\[
= \begin{bmatrix}
2(-d^2\alpha + cd\beta + c^2\alpha - cd\beta) \\
2(-c\alpha + c^2\beta + c\alpha - d^2\beta)
\end{bmatrix}
\begin{bmatrix}
2(c^2 - d^2)\alpha \\
2(c^2 - d^2)\beta
\end{bmatrix}
\]

Expressing the above matrix in terms of Pauli Matrices, we have \( U = -\sqrt{2}(dI + c\sigma_x) \)

Now as \( 2c^2 - 2d^2 = 1 \), we have \( d^2 = c^2 - \frac{1}{2} \)

Since \( d \) is purely imaginary, we must have \( c^2 \leq \frac{1}{2} \) or \( -\frac{1}{\sqrt{2}} \leq c \leq \frac{1}{\sqrt{2}} \) Now from the condition of normalization of Alice’s resultant state, we have:

\[|d|^2 + |c|^2 + (\tilde{d}c + d\tilde{c})(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}\]

As \( c = \tilde{c} \), the above equation reduces to:

\[|d|^2 + |c|^2 + c(\tilde{d} + d)(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}\]

And as \( \tilde{d} + d = 0 \), the above equation further reduces to:

\[|d|^2 + |c|^2 = \frac{1}{2}\]

As \( c \) is a real number, \( c^2 = |c|^2 \) and so we have:

\[|d|^2 + c^2 = \frac{1}{2}\]

or

\[|d|^2 = \frac{1}{2} - c^2\]
Appendix 4: (Proof of Theorem 1)

For Alice to successfully retrieve the secret, Bob and Charlie must measure their respective qubits in the Hadamard Basis. We show how Alice can retrieve back her message by enlisting down the respective local operations corresponding to Bob’s and Charlie’s measurement outcomes.

If Bob and Charlie’s joint measurement outcome in Hadamard Basis $|++\rangle$, the resultant state on Alice’s side is given by the following (when Alice’s initial measurement outcome is $|\psi^+\rangle$):

$$\sqrt{2}\{(b\alpha + a\beta)|0\rangle + (a\alpha + b\beta)|1\rangle\}$$

Condition of normalization of the above Alice’s resultant state is as follows:

$$|a|^2 + |b|^2 + (\tilde{a}b + \tilde{a}\tilde{b})(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}$$

In order to find Alice’s Local Operations state for retrieving the secret, we proceed by taking a Unitary Matrix as follows:

$$U = \begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix}$$

such that $\det(U) = -1$

We need to find $a_1, b_1, c_1, d_1$ by solving the following equation for Alice to retrieve the secret:

$$\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \sqrt{2}(b\alpha + a\beta) \\ \sqrt{2}(a\alpha + b\beta) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

As $a, b, \alpha$ and $\beta$ are complex numbers, we write $a = x_1 + iy_1, b = x_2 + iy_2, \alpha = x_3 + iy_3, \beta = x_4 + iy_4$.

The above equation transforms as follows:

$$\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \sqrt{2}(\lambda_1 + i\lambda_2) \\ \sqrt{2}(\lambda_3 + i\lambda_4) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Where we have:

$$\begin{align*}
\lambda_1 &= x_2x_3 + x_1x_4 - y_1y_4 - y_2y_3 \\
\lambda_2 &= x_3y_2 + x_4y_1 + x_2y_3 + x_1y_4 \\
\lambda_3 &= x_1x_3 + x_2x_4 - y_1y_3 - y_2y_4 \\
\lambda_4 &= x_3y_1 + x_1y_3 + x_2y_4 + x_4y_2
\end{align*}$$

Such that:

$$\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 = |a|^2 + |b|^2 + (\tilde{a}b + \tilde{a}\tilde{b})(\alpha\tilde{\beta} + \tilde{\alpha}\beta) = \frac{1}{2}$$ (29)
Solving the above equation by comparing real and imaginary parts on both sides to get:

\[
\begin{align*}
 a_1 &= \frac{\lambda_1 x_3 + \lambda_2 y_3 - \lambda_3 x_4 - \lambda_4 y_4}{\sqrt{2(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)}} = \sqrt{2}(\lambda_1 x_3 + \lambda_2 y_3 - \lambda_3 x_4 - \lambda_4 y_4) \\
 b_1 &= \frac{\lambda_1 y_3 - \lambda_2 x_3 + \lambda_3 y_4 - \lambda_4 x_4}{\sqrt{2(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)}} = \sqrt{2}(\lambda_1 y_3 - \lambda_2 x_3 + \lambda_3 y_4 - \lambda_4 x_4) \\
 c_1 &= \frac{\lambda_1 x_4 + \lambda_2 y_4 + \lambda_3 x_3 + \lambda_4 y_3}{\sqrt{2(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)}} = \sqrt{2}(\lambda_1 x_4 + \lambda_2 y_4 + \lambda_3 x_3 + \lambda_4 y_3) \\
 d_1 &= \frac{\lambda_4 x_3 - \lambda_3 y_3 + \lambda_1 y_4 - \lambda_2 x_4}{\sqrt{2(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2)}} = \sqrt{2}(\lambda_4 x_3 - \lambda_3 y_3 + \lambda_1 y_4 - \lambda_2 x_4)
\end{align*}
\]

\[
\begin{align*}
 a_1 + ib_1 &= \sqrt{2}\{(\lambda_1 - i\lambda_2)\alpha - (\lambda_3 + i\lambda_4)\beta\} \\
 &= \sqrt{2}\{(\hat{b}\alpha + \hat{a}\beta)\alpha - (aa + b\beta)\beta\} \\
 &= \sqrt{2}\{(\hat{b} - (\hat{b} + b)|\beta|^2 + (\hat{a} - a)\alpha\beta)\} \\
 &= \sqrt{2}\{(a + (\hat{b} + b)\alpha\beta + (\hat{a} - a)|\alpha|^2)\}
\end{align*}
\]

\[
\begin{align*}
 -a_1 + ib_1 &= \sqrt{2}\{- (\lambda_1 + i\lambda_2)\alpha + (\lambda_3 - i\lambda_4)\beta\} \\
 &= \sqrt{2}\{- (\hat{b}\beta + \hat{a}\alpha)\alpha + (\hat{a} + a)\alpha\beta\} \\
 &= \sqrt{2}\{- b + (\hat{b} + b)|\beta|^2 + (\hat{a} - a)\beta\alpha\} \\
 &= \sqrt{2}\{(a + (\hat{b} + b)|\beta|^2 + (\hat{a} - a)|\alpha|^2)\}
\end{align*}
\]

Using equations (30), (31), (32) and (33), we obtain the Unitary matrix as follows:

\[
\begin{bmatrix}
\sqrt{2}\{(\hat{b} - (\hat{b} + b)|\beta|^2 + (\hat{a} - a)\alpha\beta)\} & \sqrt{2}\{(a + (\hat{b} + b)\alpha\beta + (\hat{a} - a)|\alpha|^2)\} \\
\sqrt{2}\{(\hat{a} + (\hat{b} + b)\alpha\beta - (\hat{a} - a)|\alpha|^2)\} & \sqrt{2}\{- b + (\hat{b} + b)|\beta|^2 + (\hat{a} - a)\beta\alpha\}
\end{bmatrix}
\]

Since the elements of the matrix need to be independent of \(\alpha\) and \(\beta\), we have the following conditions:

\[
\hat{b} + b = 0 \quad (34)
\]

\[
\hat{a} - a = 0 \quad (35)
\]
From eq (34) we have \( b \) to be purely imaginary and from eq (35) we have \( a \) to be purely real. After the imposition of the above conditions eq (34) and (35), the Unitary Matrix reduces to:

\[
U = \begin{bmatrix}
\sqrt{2}b & \sqrt{2}a \\
\sqrt{2}\tilde{a} & -\sqrt{2}b
\end{bmatrix} = \begin{bmatrix}
-\sqrt{2}b & \sqrt{2}a \\
\sqrt{2}a & -\sqrt{2}b
\end{bmatrix}
\]

Where we made use of eq (34) and eq (35) above, \( \tilde{a} = a \) or \( \tilde{b} = -b \)

\[
\det(U) = 2b^2 - 2a^2 = -1 \text{ or } 2a^2 - 2b^2 = 1
\]

Using the above matrix, Alice successfully retrieves the secret as follows:

\[
\begin{bmatrix}
\sqrt{2}b & \sqrt{2}a \\
\sqrt{2}\tilde{a} & -\sqrt{2}b
\end{bmatrix} \begin{bmatrix}
\sqrt{2}(\alpha \tilde{b} + \alpha \beta) \\
\sqrt{2}((\alpha + b\beta)
\end{bmatrix} = \begin{bmatrix}
2(-b^2\alpha - ab\beta + a^2\alpha + \alpha b\beta) \\
2(ab\alpha + a^2\beta - ab\alpha - b^2\beta)
\end{bmatrix} = \begin{bmatrix}
2(a^2 - b^2)\alpha \\
2(a^2 - b^2)\beta
\end{bmatrix} = \begin{bmatrix}
\alpha \\
\beta
\end{bmatrix}
\]

Expressing the above matrix in terms of Pauli Matrices, we have \( U = \sqrt{2}(-bI + a\sigma_x) \)

Now as \( 2a^2 - 2b^2 = 1 \), we have \( b^2 = a^2 - \frac{1}{2} \)

Since \( b \) is purely imaginary, we must have \( a^2 \leq \frac{1}{2} \) or \( -\frac{1}{\sqrt{2}} \leq a \leq \frac{1}{\sqrt{2}} \). Now from the condition of normalization of Alice’s resultant state, we have:

\[
|a|^2 + |b|^2 + (\tilde{a}b + ab)(\alpha \tilde{b} + \alpha \beta) = \frac{1}{2}
\]

As \( a = \tilde{a} \), the above equation reduces to:

\[
|a|^2 + |b|^2 + a(\tilde{b} + b)(\alpha \tilde{b} + \alpha \beta) = \frac{1}{2}
\]

And as \( \tilde{b} + b = 0 \), the above equation further reduces to:

\[
|a|^2 + |b|^2 = \frac{1}{2}
\]

As \( a \) is a real number, \( a^2 = |a|^2 \) and so we have:

\[
|b|^2 + a^2 = \frac{1}{2}
\]

or

\[
|b|^2 = \frac{1}{2} - a^2
\]

23
Appendix 5: (Proof of Theorem 2)

For Charlie to successfully reconstruct the secret, Alice and Bob must measure their respective qubits in the Hadamard Basis. We show how Charlie can reconstruct the secret by enlisting down the respective local operations corresponding to Alice’s and Bob’s measurement outcomes.

If Alice and Bob’s joint measurement outcome in Hadamard Basis is $|++\rangle$, the resultant state on Charlie’s side is given by the following (when Alice’s initial measurement outcome is $\phi^+$):

$$\frac{1}{\sqrt{2}}\{|(a + b - c + d)\alpha + (a + b + c - d)\beta\rangle 0\rangle + \frac{1}{\sqrt{2}}\{|(a + b + c - d)\alpha + (a + b - c + d)\beta\rangle 1\rangle\}$$

Denoting $(a + b - c + d)$ as $\lambda_1$ and $(a + b + c - d)$ as $\lambda_2$, the above resultant state can be written as:

$$\frac{1}{\sqrt{2}}(\lambda_1\alpha + \lambda_2\beta) 0\rangle + \frac{1}{\sqrt{2}}(\lambda_2\alpha + \lambda_1\beta) 1\rangle$$

Condition of normalization of the above Charlie’s resultant state is as follows:

$$\frac{1}{2}\{|\lambda_1\alpha + \lambda_2\beta|^2 + |\lambda_2\alpha + \lambda_1\beta|^2\} = 1$$

Simplifying, we get:

$$|\lambda_1|^2 + |\lambda_2|^2 + (\lambda_1\lambda_2 + \lambda_1\lambda_2)(\alpha\beta + \alpha\beta) = 2$$

In order to find Charlie’s Local Operations state for retrieving the secret, we proceed by taking a Unitary Matrix as follows:

$$U = \begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix}$$

such that $\text{det}(U) = -1$

We need to find $a_1, b_1, c_1, d_1$ by the solving the following equation for Alice to retrieve the secret:

$$\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}}(\lambda_1\alpha + \lambda_2\beta) \\ \frac{1}{\sqrt{2}}(\lambda_2\alpha + \lambda_1\beta) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

As $a, b, c, d, \alpha$ and $\beta$ are complex numbers, we write $\lambda_1 = x_1 + iy_1, \lambda_2 = x_2 + iy_2, \alpha = x_3 + iy_3, \beta = x_4 + iy_4$.

The above equation transforms as follows:

$$\begin{bmatrix} a_1 + ib_1 & c_1 - id_1 \\ c_1 + id_1 & -a_1 + ib_1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}}(\nu_1 + i\nu_2) \\ \frac{1}{\sqrt{2}}(\nu_3 + i\nu_4) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Where we have:

$$\nu_1 = x_1x_3 + x_2x_4 - y_1y_3 - y_2y_4$$
$$\nu_2 = x_3y_1 + x_1y_3 + x_2y_4 + x_4y_2$$
$$\nu_3 = x_2x_3 + x_1x_4 - y_1y_4 - y_2y_3$$
$$\nu_4 = x_3y_2 + x_4y_1 + x_2y_3 + x_1y_4$$
Such that:

\[
\nu_1^2 + \nu_2^2 + \nu_3^2 + \nu_4^2 = |\lambda_1|^2 + |\lambda_2|^2 + (\tilde{\lambda}_1\lambda_2 + \lambda_1\tilde{\lambda}_2)(\alpha\beta + \bar{\alpha}\bar{\beta}) = 2
\]  

(36)

Solving the above equation by comparing real and imaginary parts on both sides to get:

\[
a_1 = \frac{\sqrt{2}(\nu_1 x_3 + \nu_2 y_3 - \nu_3 x_4 - \nu_4 y_4)}{\nu_1^2 + \nu_2^2 + \nu_3^2 + \nu_4^2} = \frac{\nu_1 x_3 + \nu_2 y_3 - \nu_3 x_4 - \nu_4 y_4}{\sqrt{2}}
\]

\[
b_1 = \frac{\sqrt{2}(\nu_1 y_3 - \nu_2 x_3 + \nu_3 y_4 - \nu_4 x_4)}{\nu_1^2 + \nu_2^2 + \nu_3^2 + \nu_4^2} = \frac{\nu_1 y_3 - \nu_2 x_3 + \nu_3 y_4 - \nu_4 x_4}{\sqrt{2}}
\]

\[
c_1 = \frac{\sqrt{2}(\nu_1 x_4 + \nu_2 y_4 + \nu_3 x_3 + \nu_4 y_3)}{\nu_1^2 + \nu_2^2 + \nu_3^2 + \nu_4^2} = \frac{\nu_1 x_4 + \nu_2 y_4 + \nu_3 x_3 + \nu_4 y_3}{\sqrt{2}}
\]

\[
d_1 = \frac{\sqrt{2}(\nu_4 x_3 - \nu_3 y_3 + \nu_1 y_4 - \nu_2 x_4)}{\nu_1^2 + \nu_2^2 + \nu_3^2 + \nu_4^2} = \frac{\nu_4 x_3 - \nu_3 y_3 + \nu_1 y_4 - \nu_2 x_4}{\sqrt{2}}
\]

\[
a_1 + ib_1 = \frac{1}{\sqrt{2}} \{((\nu_1 - \nu_2)\alpha - (\nu_3 + \nu_4)\beta)\}
\]

\[
= \frac{1}{\sqrt{2}} \{(\tilde{\lambda}_1\alpha + \tilde{\lambda}_1\beta)\alpha - (\lambda_2\alpha + \lambda_1\beta)\beta\}
\]

\[
= \frac{1}{\sqrt{2}} \{(\tilde{\lambda}_1 - (\lambda_1 + \lambda_1)|\beta|^2 + (\lambda_2 - \lambda_2)\alpha\beta)\}
\]  

(37)

\[-a_1 + ib_1 = \frac{1}{\sqrt{2}} \{-(\nu_1 + \nu_2)\alpha + (\nu_3 - \nu_4)\beta\}
\]

\[
= \frac{1}{\sqrt{2}} \{-(\lambda_1\alpha + \lambda_2\beta)\alpha + (\tilde{\lambda}_2\tilde{\alpha} + \tilde{\lambda}_2\tilde{\alpha})\beta\}
\]

\[
= \frac{1}{\sqrt{2}} \{-\lambda_1 + (\tilde{\lambda}_1 + \lambda_1)|\beta|^2 + (\lambda_2 - \lambda_2)\alpha\beta\}
\]  

(38)

\[c_1 + id_1 = \frac{1}{\sqrt{2}} \{((\nu_1 - \nu_2)\beta + (\nu_3 + \nu_4)\alpha)\}
\]

\[
= \frac{1}{\sqrt{2}} \{(\tilde{\lambda}_1\beta + \tilde{\lambda}_2\alpha)\beta + (\lambda_2\alpha + \lambda_1\beta)\alpha\}
\]

\[
= \frac{1}{\sqrt{2}} \{\lambda_2 + (\tilde{\lambda}_1 + \lambda_1)\alpha\beta - (\tilde{\lambda}_2 - \lambda_2)|\alpha|^2\}
\]  

(39)

\[c_1 - id_1 = \frac{1}{\sqrt{2}} \{((\nu_1 + \nu_2)\beta + (\nu_3 - \nu_4)\alpha)\}
\]

\[
= \frac{1}{\sqrt{2}} \{(\lambda_1\alpha + \lambda_2\beta)\beta + (\tilde{\lambda}_1\tilde{\beta} + \tilde{\lambda}_2\tilde{\alpha})\alpha\}
\]

\[
= \frac{1}{\sqrt{2}} \{\lambda_2 + (\tilde{\lambda}_1 + \lambda_1)\alpha\beta + (\tilde{\lambda}_2 - \lambda_2)|\alpha|^2\}
\]  

(40)
Expressing the above matrix in terms of Pauli Matrices, we have

$$U = \begin{bmatrix} \frac{1}{\sqrt{2}}((\tilde{\lambda} - (\tilde{\lambda}_1 + \lambda_1))|\beta|^2 + (\tilde{\lambda}_2 - \lambda_2)|\alpha|^2) \\ \frac{1}{\sqrt{2}}\{\lambda_2 + (\tilde{\lambda}_1 + \lambda_1)|\alpha\tilde{\beta}| + (\tilde{\lambda}_2 - \lambda_2)|\alpha|^2\} \end{bmatrix}$$

From eq (41) we derived

$$\lambda = \begin{cases} \lambda_1 = \lambda_2 = 0 \\
\lambda_2 - \lambda_2 = 0 \end{cases}$$

Using the above matrix, Alice successfully retrieves the secret as follows:

$$\tilde{\lambda}_1 + \lambda_1 = 0 \quad \text{(41)}$$

$$\tilde{\lambda}_2 - \lambda_2 = 0 \quad \text{(42)}$$

From eq (42) we have $$\lambda_1$$ or $$(a + b - c + d)$$ to be purely imaginary and from eq (43) we have $$\lambda_2$$ or $$(a + b + c - d)$$ to be purely real. After the imposition of the above conditions eq (42) and (43), the Unitary Matrix reduces to:

$$U = \begin{bmatrix} \frac{1}{\sqrt{2}}\tilde{\lambda}_1 & \frac{1}{\sqrt{2}}\lambda_2 \\ \frac{1}{\sqrt{2}}\lambda_2 & -\frac{1}{\sqrt{2}}\tilde{\lambda}_1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}}\lambda_1 & \frac{1}{\sqrt{2}}\lambda_2 \\ \frac{1}{\sqrt{2}}\lambda_2 & -\frac{1}{\sqrt{2}}\lambda_1 \end{bmatrix}$$

From eq (41) we derived $$\lambda_1$$ or $$(a + b - c + d)$$ to be purely imaginary and from eq (42) we derived $$\lambda_2$$ or $$(a + b + c - d)$$ to be purely real, so we have the following conditions of $$a, b, c$$ and $$d$$ from Alice’s retrieval derived in Appendix 1:

**Case:** $$(a + b - c + d)$$ is purely imaginary and $$(a + b + c - d)$$ is purely real

If $$a$$ and $$c$$ are chosen as real numbers, and $$b$$ and $$d$$ are chosen as imaginary numbers, then we have $$a = c$$ and $$b = d$$

If $$a$$ and $$d$$ are chosen as real numbers, and $$b$$ and $$c$$ are chosen as imaginary numbers, then we have $$a = -d$$ and $$b = -c$$

If $$b$$ and $$c$$ are chosen as real numbers, and $$a$$ and $$d$$ are chosen as imaginary numbers, then we have $$b = c$$ and $$a = d$$

If $$b$$ and $$d$$ are chosen as real numbers, and $$a$$ and $$c$$ are chosen as imaginary numbers, then we have $$b = -d$$ and $$a = -c$$

Using equations (38), (39), (40) and (41), we obtain the Unitary matrix as follows:

$$\det(U) = \frac{1}{2}\lambda_2^2 - \frac{1}{2}\lambda_1^2 = -1 \quad \text{or} \quad \frac{1}{2}\lambda_2^2 - \frac{1}{2}\lambda_1^2 = 1$$

Expanding the above matrix in terms of Pauli Matrices, we have $$U = \frac{1}{\sqrt{2}}(-\lambda_1 I + \lambda_2 \sigma_x)$$ or $$U = \frac{1}{\sqrt{2}}[-(a + b + c + d)I + (a + b + c - d)\sigma_x]$$

From eq (41) we derived $$\lambda_1$$ or $$(a + b - c + d)$$ to be purely imaginary and from eq (42) we derived $$\lambda_2$$ or $$(a + b + c - d)$$ to be purely real, so we have the following conditions of $$a, b, c$$ and $$d$$ from Alice’s retrieval derived in Appendix 1: