Entangled States as Robust and Re-usable Carriers of Information

Shima Emamipanah [b], Marzieh Asoudeh[b1] and Vahid Karimipour.[a]

[a] Department of Physics, Sharif University of Technology, P.O. Box 11155-9161, Tehran, Iran.
[b]Department of Physics, Azad University, Northern Branch, Tehran, Iran .

Abstract

Entangled states can be used as secure carriers of information much in the same way as carriers are used in classical communications. In such protocols, quantum states are uploaded to the carrier at one end and are downloaded from it in safe form at the other end, leaving the carrier intact and ready for reuse. Furthermore, protocols have been designed for performing quantum state sharing in this way. In this work, we study the robustness of these protocols against two of the most common sources of noise, namely de-phasing and depolarization and show that multiple uses of these carriers do not lead to accumulative errors, rather the error remains constant and under control.

1 Introduction

Conventionally in quantum information processes [1, 2, 3, 4] entanglement is used as a resource which is consumed at the end of a process and has to be renewed for a second use. This is the case for teleportation, measurement-based quantum computation and many other protocols. For example in quantum secret sharing schemes [5, 6, 7, 8, 9, 10], which is the subject of interest in the present work, the highly non-classical correlation in the shared entangled state allows the legitimate parties to establish a random shared key between themselves. Of course there are also cryptographic protocols which are sequential and do not use entanglement at all [11, 12, 14, 15, 16, 17, 18].

The idea of using an entangled state between two remote points, as a reusable carrier of information, first came up in [19] and then extended to quantum secret sharing in [20] by one of the authors. This idea is a natural generalization of the idea behind today's classical communication networks, in the sense that an entangled state between two or more points acts as a secure carrier of information between these points. The sender entangles (uploads) a state to the carrier which is disentangled (downloaded) by the receiver at the other end. The additional feature, due to the quantum properties is that during transmission, the state is hidden from potential adversaries. The hiding effect is a direct result of entanglement of the message state with the carrier state, by which the message state is in a highly mixed state and carrying no information at all by itself. Only in the sender and receiver ends, where the message is uploaded (entangled to the carrier) or downloaded (disentangled from the carrier), the identity of the message is revealed. At the end of each round, the carrier returns to its initial state and is ready for a second round of use. We stress that an entangled state is not used here in the usual sense, i.e. to securely establish a shared random key between the parties[26], but to send a deterministic message from one end to the other. In case of [19] the carrier is a simple Bell state between two parties, while in case of [20], the carrier is a three party entangled state and alternates between two specific forms in consecutive rounds. In this protocol Alice sends a classical or quantum message to Bob and Charlie who can retrieve it only by their collaboration. Note that by classical

---

[1]Corresponding Author

message we mean classical bits which have been encoded into computational states $\{|0\rangle, |1\rangle\}$ and by quantum message we mean an unknown quantum state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$.

We should stress that entanglement in this sense, that is, for sending deterministic messages, has not been reported previously before the two references [19] and [20]. Of course the price of this higher level protocol is the bigger resource that the players have to use, i.e. the multi-party entangled states in the transition stage. These schemes may seem impractical with present technologies, however with the intensive research on quantum networks, they may become potential candidates for the quantum communication methods of tomorrow. Therefore it is important to study these schemes from different points of view. In particular it is important to investigate how resilient these protocols are against noise of the environment. Of particular importance are the de-phasing and depolarizing noise which we study in this paper. We will examine in detail the scheme of [20] for Quantum State Sharing (QSS) and determine how much error the de-phasing and depolarizing noise incur on the transmitted data and states. It is important to determine how much error the noise of environment will incur on the fidelity between the sent and the received q(bits). This will allow the legitimate players to distinguish the noise resulting from the action of an adversary from the environmental noise and help them to reveal the presence of an adversary. Note that our emphasis is on the concept of entangled state as a reusable carrier of information and not on the security of such a protocol against various types of attacks. For discussions on two kinds of attacks on this protocol see [21, 22] and [23, 24]. For generalization of this protocol to polynomial codes and (k, n) threshold schemes, see [25] where further discussions on the performance of the protocol under various outsider attacks and cheating of insiders, shas been made.

An important question is whether or not a noisy carrier, specially when it is continually under the uploading, downloading and Hadamard actions of the players, will keep its shape or will be disrupted after a few rounds and will be completely useless. We will show that this is not the case and the carrier will keep its form and is only mixed by a well-known and controlled state. Here we will study the case where the carrier has been contaminated by noise before the operations start and the time scale of operations in each round are short enough that the additional noise during the operations, either on the carrier or on the encoded states are negligible.

The structure of the paper is as follows: In section (2), we briefly review the protocols of [20] in a self-contained way. The main point of the scheme of [20] is that the three parties involved in the state sharing scheme, have to use two kinds of carriers in alternating rounds and these two carriers are turned into each other by their local action at the end of each round. In sections (3) and section (4) we study the effect of two important types of noise, namely de-phasing and depolarizing noise on this protocol. Although we focus on the three-party case, the idea can be easily generalized to schemes with more than three players. We will briefly discuss this in section (**??**), where we also point out the possibility of error correction schemes for overcoming the effect of aforementioned noise. We end the paper with conclusion and outlook.

2 Entangled states as reusable carriers of information

Consider three parties, Alice (A), Bob (B) and Charlie (C). The goal of Alice is to send a state $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob and Charlie so that they can retrieve it only if they collaborate with each other. We assume that Bob and Charlie are at one location and can affect two qubit gates on the state they receive. In the meantime Alice wants to keep this state from any possible adversaries by entangling it with a carrier which is shared between her and the other two parties. In the end the carrier should be such that it can be used again for sending other qubits. Before proceeding, it is better that we

collect all our notations and conventions and some basic facts and formulas which are easily proved by direct calculations.

2.1 Notations and conventions

We use the subscripts A, B, and C for the qubits of carrier possessed by Alice, Bob and Charlie and the subscripts 1 and 2 for the two qubits which are being communicated. The qubit 1 is always sent to Bob and qubit 2 is always sent to Charlie. In equations and for the sake of simplicity, we write these subscripts only on the left hand side. The same subscripts are to be understood for the states on the right hand side.

Let q be a bit $\in \{0, 1\}$. $\overline{q}$ is meant to denote the negation of q, i.e. $\overline{0} = 1, \overline{1} = 0$. We define the state

$$|\mathbf{0}_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\mathbf{1}_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{1}$$

to represent respectively the two qubit states of even and odd parity. In close form we write

$$|\mathbf{q}\rangle = \frac{1}{\sqrt{2}}(|0q\rangle + |1\overline{q}\rangle). \tag{2}$$

Remark: *Hereafter and most of the time, we write all states without normalization and assume that they are understood to be properly normalized. Thus, a state like $|000\rangle + |111\rangle$ is to be understood as $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.*

The even and odd parity states can be extended to more than two parties. For three qubits we have

$$\begin{aligned} |\mathbf{0}_3\rangle &= |0\rangle|\mathbf{0}_2\rangle + |1\rangle|\mathbf{1}_2\rangle, \\ |\mathbf{1}_3\rangle &= |0\rangle|\mathbf{1}_2\rangle + |1\rangle|\mathbf{0}_2\rangle. \end{aligned} \tag{3}$$

This can be extended to n parties in the same way by induction on n, although we do not need this here. The subscripts A, B and C are used to denote qubits in possession of the three players conventionally called Alice, Bob and Charlie. The subscripts 1 and 2 are used to denote the qubits which are being transmitted, one to B and the other to C. We write these subscripts only on the left hand side of equations, with the understanding that they also apply to the states on the right hand side, that is

$$|\psi\rangle_{A,B} = |00\rangle + |11\rangle$$

is meant to denote

$$|\psi\rangle_{A,B} = |00\rangle_{A,B} + |11\rangle_{A,B}.$$

When from the context it is clear what types of parity state we are dealing with, we refrain from writing the subscript 2 or 3 on $\mathbf{0}$ or $\mathbf{1}$. For example it is clear that a state $|\mathbf{0}\rangle_{A,B,C}$ is a $|\mathbf{0}_3\rangle$ state and a state like $|\mathbf{0}\rangle_{1,2}$ is a $|\mathbf{0}_2\rangle$ state.

A CNOT operation with control bit X (where $X \in \{A, B, C\}$) and target bit 1 is denoted by C_{X1}. Simple calculation shows that on this encoded states [20], we have the following CNOT operations, Fig. (1)

$$(C_{X,1} \text{ or } C_{X,2}) |q\rangle_X |\mathbf{q}'\rangle_{1,2} = |q\rangle_X |\mathbf{q} + \mathbf{q}'\rangle_{1,2}, \tag{4}$$

and

$$C_{X,1}C_{Y,2}|\mathbf{q}\rangle_{X,Y}|\mathbf{q}'\rangle_{1,2} = |\mathbf{q}\rangle_{X,Y}|\mathbf{q} + \mathbf{q}'\rangle_{12}. \tag{5}$$

Note the difference: In Eq. (4) only one of the CNOTs should be applied, while in Eq. (5) both CNOT's should be applied. Finally we numerate the rounds as $0, 1, 2, \cdots$ The superscript $^{(0)}, ^{(1)}, ^{(2)}, \cdots$ are used to denote the form of the carrier at the start of rounds $0, 1., 2, \cdots$.
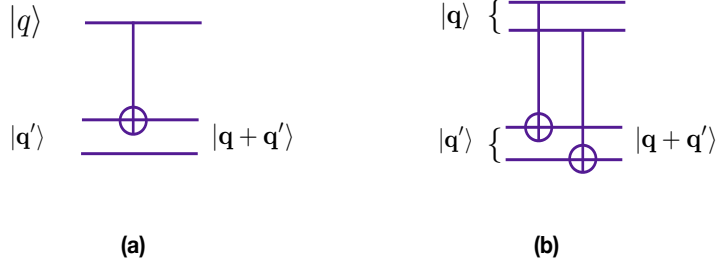
Figure 1: The CNOT operators on encoded states, (a): equation (4), (b): equation (5).

2.2 The QSS scheme in the absence of noise

The three party secret sharing scheme [20], which can easily be extended to $N-$party scheme runs as follows Alice, Bob and Charlie (A,B and C) share a GHZ state

$$|GHZ\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{6}$$

which upon the joint Hadamard action of all three parties $H_A \otimes H_B \otimes H_C$ turns into another carrier

$$|\mathbf{0}\rangle_{A,B,C} = \frac{1}{2}\left(|000\rangle + |110\rangle + |101\rangle + |011\rangle\right), \tag{7}$$

Since $H^2 = I$, we have

$$H_A \otimes H_B \otimes H_C|\mathbf{0}\rangle_{A,B,C} = |GHZ\rangle_{A,B,C}, \qquad H_A \otimes H_B \otimes H_C|GHZ\rangle_{A,B,C} = |\mathbf{0}\rangle_{A,B,C}. \tag{8}$$

Therefore the two types of carriers alternate in even and odd rounds (starting from round 0 with GHZ). Consider now the even rounds 0, 2, 4, $\cdots$, where the carrier is $|GHZ\rangle_{A,B,C}$ and Alice encodes $|q\rangle$ to $|qq\rangle_{1,2}$ and entangles this state to the carrier by the operation $C_{A,1} \otimes C_{A,2}$. The total state becomes

$$|\Psi_{even}\rangle_{A,B,C,1,2} = |000\rangle|qq\rangle + |111\rangle|\overline{qq}\rangle. \tag{9}$$

At the other end, Bob and Charlie disentangle the state $|qq\rangle$ by operations $C_{B,1}$ and $C_{C,2}$, returning the carrier to the $|GHZ\rangle$ state, and read the message bit q independently. In these rounds, the sequence of operations can be collected in the form

$$\Omega^{even} = C_{C,2}C_{B,1}C_{A,2}C_{A,1}. \tag{10}$$

At the end of even rounds, all three parties act by their Hadamard operation on their share and turn the carrier to the state $|\mathbf{0}\rangle_{A,B,C}$. In the odd rounds 1, 3, 5, $\cdots$, where the carrier is $|\mathbf{0}\rangle_{A,B,C} =$
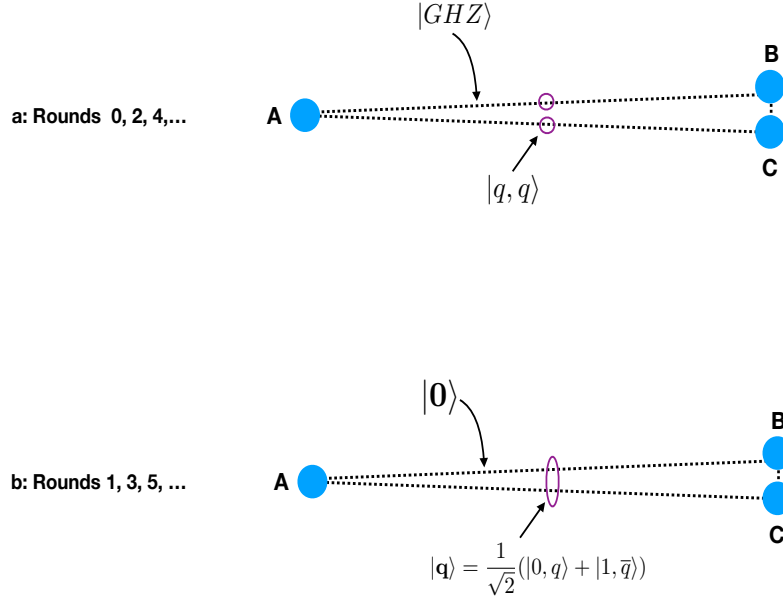
Figure 2: In even rounds $0, 2, 4, \cdots$, the carrier is $|GHZ\rangle$ and q is encoded into a product state $|q, q\rangle$. In odd rounds $1, 3, 5, \cdots$ the carrier is $H^{\otimes 3}|GHZ\rangle = |\mathbf{0}\rangle$ and q is encoded into an entangled state $|\mathbf{q}\rangle_{1,2}$. In the even rounds, where Bob and Charlie can retrieve the bit independently, Alice can send redundant bits which carry no information.

$|0\rangle_A|\mathbf{0}\rangle_{B,C} + |1\rangle_A|\mathbf{1}\rangle_{B,C}$, Alice encodes the state $|q\rangle$ into $|\mathbf{q}\rangle_{1,2}$ and entangles this state to the carrier by her operation $C_{A,1}$ on only one of the qubits (see Eq.(4)). This changes the total state to

$$|\Psi_{odd}\rangle_{A,B,C,1,2} = |0\rangle_A|\mathbf{0}\rangle_{B,C}|\mathbf{q}\rangle_{1,2} + |1\rangle_A|\mathbf{1}\rangle_{B,C}|\overline{\mathbf{q}}\rangle_{1,2}. \qquad (11)$$

Again the state in travel is a mixture of $|\mathbf{q}\rangle$ and $|\overline{\mathbf{q}}\rangle$ and is hidden from any adversary. At the destination, Bob and Charlie perform the operation $C_{B,1}C_{C,2}$ to disentangle the state from the carrier (download it) (see (Eq. 5)). In these rounds, the sequence of operations can be collected in the form

$$\Omega^{odd} = C_{C,2}C_{B,1}C_{A,1}. \qquad (12)$$

But this time the state can be decoded only if Charlie and Bob collaborate with each other (i.e. Acting by $C_{1,2}$ on the received state). It has already been shown in [20] that Eve cannot entangle herself with the carrier state, since the joint Hadamard operation effectively throws her out by revealing her presence to the legitimate parties.

Remark: *Any basis state $|q\rangle$ can be sent by Alice and retrieved by the receivers by encoding and decoding it differently in even and in odd rounds. Therefore by linearity of the process, this is also true for any linear combination of these basis states, i.e. for any unknown quantum state $|\psi\rangle_{1,2} = \alpha|0\rangle + \beta|1\rangle$ which is encoded to $|\overline{\psi}\rangle_{1,2} = \alpha|0,0\rangle + \beta|1,1\rangle$ in even rounds and to $|\overline{\psi}\rangle_{1,2} = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$ in odd rounds. Note that the even rounds is not used for sharing data between*

5

Bob and Charlie and in fact Alice can spare these rounds and send sensitive data only in odd rounds where the receivers should collaborate to retrieve the data. The answer to the question why the parties do not always use the odd-type carrier is that the Hadamard operations are necessary for the security of the protocol [20] and the action of these Hadamard operations inevitably changes the carrier in alternate rounds.

Definition 1 *By the complete channel Φ between the sender Alice and one of the receivers, say Bob, we mean the channel which consists of encoding an initial state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to either $|\psi_{even}\rangle = \alpha|00\rangle + \beta|11\rangle$ or $|\psi_{odd}\rangle\alpha|\mathbf{0}_2\rangle + \beta|\mathbf{1}_2\rangle)$, sending it through the quantum channel described above and then decoding to the initial state $|\psi\rangle$ by the collaboration of Bob and Charlie. In the absence of noise, this channel is an identity qubit channel, i.e. $\Phi(\rho) = \rho$.*

We are now ready to study the robustness of this scheme first under De-phasing and then under global depolarizing noise. In other words, we want to find out what happens to the complete channel defined above, when the carriers are noisy and are not pure states any more.

3 Effect of de-phasing noise

A ubiquitous form of noise is De-phasing which maps the carrier state $|GHZ\rangle$ into the following

$$\rho_{A,B,C}^{(even)} = (1 - 2p)|GHZ\rangle\langle GHZ| + p|000\rangle\langle 000| + p|111\rangle\langle 111|. \tag{13}$$

Such a state is the result of random phase kicks on the three qubits. In fact random operation of a product operator

$$U_{A,B,C} = e^{i\theta_1\sigma_z} \otimes e^{i\theta_2\sigma_z} \otimes e^{i\theta_3\sigma_z}$$

with probability $P(\theta_1, \theta_2, \theta_3)$ produces a state in the form

$$\int dU\ U|GHZ\rangle\langle GHZ|U^\dagger, \tag{14}$$

where $dU = P(\theta_1, \theta_2, \theta_3)d\theta_1 d\theta_2 d\theta_3$. A simple calculation shows that this produces the state in (13) with the following parameter p

$$p = \frac{1}{2}\Big[1 - \int d\theta_1 d\theta_2 d\theta_3 e^{2i(\theta_1+\theta_2+\theta_3)} P(\theta_1, \theta_2, \theta_3)\Big]. \tag{15}$$

Here we have used the plausible assumption that the random kicks are acting on qubits as single gates, although their probability need not be uncorrelated. Moreover we have assumed that the probability distribution function is an even function of its arguments, that is, the phase kicks are symmetric around zero.

As we will see in the sequel, it is convenient if we define another GHZ state in the form

$$|GHZ'\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle). \tag{16}$$

We can then rewrite the noisy state $\rho^{(0)}$ in the form

$$\rho_{A,B,C}^{(even)} = (1 - p)|GHZ\rangle\langle GHZ| + p|GHZ'\rangle\langle GHZ'|. \tag{17}$$

6

The main concern is that, with the operations of the three parties (i.e. the uploading, downloading and Hadamard operations), the shape of the carrier may continually changes in each round and becomes useless for transmission of states after a few rounds. However as we will show in the sequel, this is not the case. To see this we first note from (9) and (17) that in even rounds both carriers $|GHZ\rangle$ and $|GHZ'\rangle$ are equally effective in delivering a state $|qq\rangle$ from A to B and C in safe form. Thus, in the even rounds de-phasing noise has no detrimental effect on the scheme. At the end of these rounds, the state is acted upon by the Hadamard operations $H_A \otimes H_B \otimes H_C$ and turns into

$$\rho_{A,B,C}^{(odd)} = (1-p)|\mathbf{0}\rangle\langle\mathbf{0}| + p|\mathbf{1}\rangle\langle\mathbf{1}|. \tag{18}$$

To analyze the performance of this carrier, we need only study the carrier $|\mathbf{1}\rangle_{ABC}$ and then combine the results, since we already know that the carrier $|\mathbf{0}\rangle_{ABC}$ delivers the state $|\mathbf{q}\rangle$ in safe form. In odd rounds, the operations of the players is given by $\Omega^{odd} = C_{C,2} C_{B,1} C_{A,1}$. This operation is shown in circuit diagram of Fig. (6). We have to affect this operator on

$$|\mathbf{1}\rangle_{A,B,C}|\mathbf{q}\rangle_{1,2} \equiv X_A X_B X_C |\mathbf{0}\rangle_{A,B,C}|\mathbf{q}\rangle_{1,2}. \tag{19}$$

To affect this, we note from Fig. (6) that

$$\Omega^{odd} X_A X_B X_C = X_2 X_A X_B X_C \Omega^{odd}$$

which in combination with (19) and the fact that $X_2|\mathbf{q}\rangle = |\overline{\mathbf{q}}\rangle$, shows that in odd rounds

$$|\mathbf{1}\rangle_{A,B,C}|\mathbf{q}\rangle_{1,2} \longrightarrow |\mathbf{1}\rangle_{A,B,C}|\overline{\mathbf{q}}\rangle_{1,2}. \tag{20}$$

This means that in even rounds the message state being encoded as $|qq\rangle$ is delivered in safe form and in odd rounds the message state encoded as $|\mathbf{q}\rangle$ is delivered with probability $(1-p)$ in safe form as $|\mathbf{q}\rangle$ and with error probability equal to p as $|\overline{\mathbf{q}}\rangle$. The important point is that the sequence of operations do not change the carriers anymore except the Hadamard operations at the end of each round which turn the carriers into each other, Fig (3). At the end of this round the carrier will be in the state (18) and after the Hadamard operation again turns into (17) or equivalently (13) and will be ready for the next round.

Since this protocol is linear, it can be used for quantum state sharing. A quantum state like $|\phi\rangle = a|0\rangle + b|1\rangle$ can be encoded as $|\tilde{\phi}\rangle_{1,2} = a|0,0\rangle + b|1,1\rangle$ in even rounds and as $|\tilde{\phi}\rangle_{1,2} = a|\mathbf{0}\rangle + b|\mathbf{1}\rangle$ in odd rounds and communicated to the receivers who retrieve it in the original form with some error. As mentioned before, only odd rounds are used for sharing states, and the retrieved state is given by $\rho_\phi = (1-p)|\phi\rangle\langle\phi| + pX|\phi\rangle\langle\phi|X$. Therefore in view of the definition of the complete channel in definition (1), we have now proved the following:

The overall effect of de-phasing noise on the complete channel: If the carrier is spoiled by noise as in (13), the complete quantum channel between the players Φ changes to

$$\Phi(\rho) == \begin{cases} \rho & \text{even rounds} \\ (1-p)\rho + \sigma_x \rho \sigma_x & \text{odd rounds} \end{cases} \tag{21}$$

$$(1-p)|GHZ\rangle\langle GHZ| + p|GHZ'\rangle\langle GHZ'|_{ABC}$$

a: Even rounds

A

B

C

$$(1-p)|\mathbf{0}\rangle\langle\mathbf{0}|_{ABC} + p|\mathbf{1}\rangle\langle\mathbf{1}|_{ABC}$$
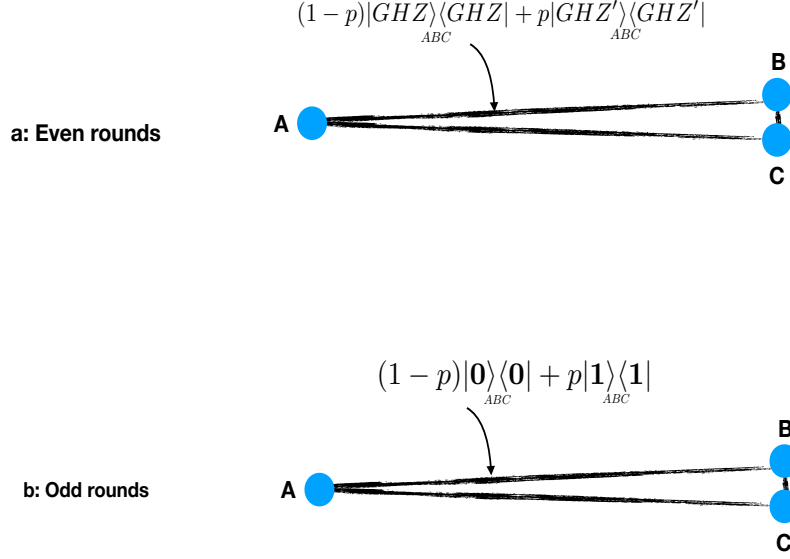
b: Odd rounds

A

B

C

Figure 3: In even rounds, where q is encoded into a product state $|qq\rangle_{1,2}$ the carrier $|GHZ\rangle_{A,B,C}$ is contaminated by $|GHZ'\rangle_{A,B,C}$ which acts as good as $|GHZ\rangle_{A,B,C}$. In odd rounds where q is encoded into an entangled state $|\mathbf{q}\rangle$, the carrier $|\mathbf{0}\rangle_{A,B,C}$ is contaminated by $|\mathbf{1}\rangle_{A,B,C}$ which flips the state to $|\bar{\mathbf{q}}\rangle$. The two kinds of carriers turn into each other after each round.

4 Effect of depolarizing noise

We now consider another important type of noise, namely a global depolarizing noise which affects the carrier as follows:

$$\rho_{A,B,C}^{(even)} = (1-p)|G_0\rangle\langle G_0| + \frac{p}{8}I, \tag{22}$$

where for simplicity of notation, we have denoted the standard GHZ state, simply as G_0. The full set of GHZ states which form a basis for the space of three qubits are:

$$|G_0\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \qquad |G_0'\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle),$$

$$|G_A\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \qquad |G_A'\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle),$$

$$|G_B\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle), \qquad |G_B'\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle),$$

$$|G_C\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle), \qquad |G_C'\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle). \tag{23}$$

These states form an ortho-normal basis, and have the following relations with each other

$$|G_i\rangle_{A,B,C} = X_i|G_0\rangle_{A,B,C}, \qquad |G_i'\rangle_{A,B,C} = X_i|G_0'\rangle_{A,B,C}, \tag{24}$$

where $i = 0, A, B, C$ and $X_0 = I$. And they are complete

$$I_{A,B,C} = \sum_{i=0,A,B,C} |G_i\rangle_{A,B,C}\langle G_i| + |G'_i\rangle_{A,B,C}\langle G'_i|. \tag{25}$$

In order to see how the protocol runs in this case, we have to decompose the carrier in terms of the above collection of GHZ states

$$\rho^{(even)}_{A,B,C} = (1-p)|G_0\rangle_{A,B,C}\langle G_0| + \frac{p}{8}\Big[\sum_{i=0,A,B,C} |G_i\rangle_{A,B,C}\langle G_i| + |G'_i\rangle_{A,B,C}\langle G'_i|\Big]. \tag{26}$$

Using Eq. (24), the relations $H^{\otimes 3}|G_0\rangle = |\mathbf{0}\rangle$ and $ZH = HX$, we also find

$$H^{\otimes 3}|G_i\rangle_{A,B,C} = Z_i|\mathbf{0}\rangle_{A,B,C}, \qquad H^{\otimes 3}|G'_i\rangle_{A,B,C} = Z_i|\mathbf{1}\rangle_{A,B,C}, \tag{27}$$

where $Z_0 = I$ and the above relations are correct modulo a global $\pm$ sign.

Equipped with these relations we now investigate how the protocol runs if the carrier is not a pure GHZ states but a mixture of different GHZ states in Eq. (23). As performed for the de-phasing noise, we consider one of the GHZ states, run the protocol with this carrier and combine the results at the end. Let the carrier be $|G_i\rangle$. The state to be shared is $|q,q\rangle$, and the full actions of the players is given by $\Omega^{even} = C_{C,2}C_{B,1}C_{A,2}C_{A,1}$, shown in the circuit diagram (5). Using the relation $C_{i,j}X_i = X_iX_jC_{i,j}$ shown in Fig. (5), we find

$$\begin{aligned}\Omega^{(even)}X_A &= X_AX_1X_2\Omega^{(even)}, \\ \Omega^{(even)}X_B &= X_BX_1\Omega^{(even)}, \\ \Omega^{(even)}X_C &= X_CX_2\Omega^{(even)}.\end{aligned} \tag{28}$$

Running the protocol on $|G_i\rangle_{A,B,C}|q,q\rangle_{1,2}$, using (28) and the above relations, we find

$$\Omega^{(even)}_{A,B,C}|G_i\rangle_{A,B,C}|q,q\rangle_{1,2} = |G_i\rangle_{A,B,C}X^{(i)}|q,q\rangle_{1,2}, \tag{29}$$

where

$$X^{(0)} = I \ , \ X^{(A)} = X_1X_2 \ , \ X^{(B)} = X_1 \ , \ X^{(C)} = X_2. \tag{30}$$

It is obvious that exactly the same relations hold when the carrier $|G_i\rangle$ is replaced with $|G'_i\rangle$. Combining all the relations we find that when the protocol is run on the noisy carrier (26), the result is:

$$\begin{aligned}\rho^{(even)}_{A,B,C} \otimes |q,q\rangle_{1,2}\langle q,q| \ \longrightarrow \ & (1-p)|G_0\rangle\langle G_0| \otimes |q,q\rangle\langle q,q| \\ & + \ \frac{p}{8}\sum_i \Big[(|G_i\rangle\langle G_i| + |G'_i\rangle\langle G'_i|) \otimes X^{(i)}|q,q\rangle\langle q,q|X^{(i)}\Big].\end{aligned} \tag{31}$$

Therefore with probability $P = 1 - p + \frac{p}{4} = 1 - \frac{3p}{4}$, the state $|q,q\rangle$ is transmitted in correct form. With probability $\frac{3p}{4}$ it is transmitted in a form where one or both of the qubits have been flipped. Thus the error probability for even rounds is equal to $P^{(even)}_{error} = \frac{3p}{4}$.

Consider now the odd rounds. The carrier is now given by

$$\rho^{(odd)}_{A,B,C} = (1-p)|\mathbf{0}\rangle\langle\mathbf{0}| + \frac{p}{8}\Big[\sum_{i=0,A,B,C} Z_i\big(|\mathbf{0}\rangle\langle\mathbf{0}| + |\mathbf{1}\rangle\langle\mathbf{1}|\big)Z_i\Big], \tag{32}$$

9

$$(1-p)|G_0\rangle\langle G_0| + \frac{p}{8}\left[\sum_i |G_i\rangle\langle G_i| + |G_i'\rangle\langle G_i'|\right]$$

a: Even rounds

A   B   C

$$(1-p)|\mathbf{0}\rangle\langle\mathbf{0}| + \frac{p}{8}\left[\sum_{i=0,A,B,C} Z_i(|\mathbf{0}\rangle\langle\mathbf{0}| + |\mathbf{1}\rangle\langle\mathbf{1}|)Z_i\right]$$
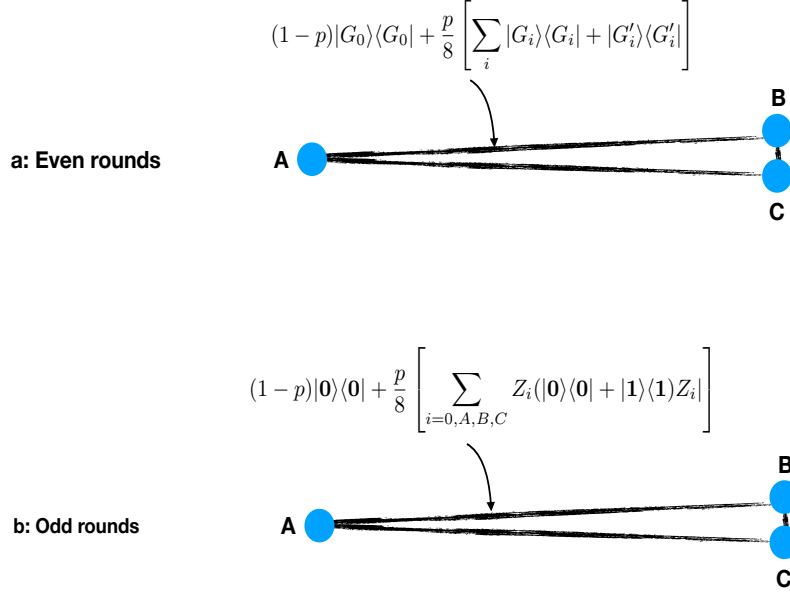
b: Odd rounds

A   B   C

Figure 4: Under a global depolarizing noise, the carrier alternates between the above two forms in even and odd rounds.

obtained by the Hadamard actions of the players on (26), Fig (4). Note that since $H^2 = I$ and $HZ = XH$, the carriers in the even and odd rounds turn into each other by the Hadamard action of the players.

We now have to consider the carriers $Z_i|\mathbf{0}\rangle$ and $Z_i|\mathbf{1}\rangle$ separately and then combine the results. In odd rounds, the operations of the players is given by $\Omega^{odd} = C_{C,2}C_{B,1}C_{A,1}$. This operation is shown in circuit diagram (6) where we use the relation $Z_iC_{i,j} = C_{i,j}Z_i$, Fig.(6), to find

$$\Omega^{odd}Z_i = Z_i\Omega^{odd}, \tag{33}$$

from which we find

$$\begin{aligned}
\Omega^{(odd)}Z_i|\mathbf{0}\rangle_{ABC}|\mathbf{q}\rangle_{1,2} &= Z_i|\mathbf{0}\rangle_{ABC}|\mathbf{q}\rangle_{1,2}, \\
\Omega^{(odd)}Z_i|\mathbf{1}\rangle_{ABC}|\mathbf{q}\rangle_{1,2} &= Z_i|\mathbf{1}\rangle_{ABC}|\mathbf{\bar{q}}\rangle_{1,2}.
\end{aligned} \tag{34}$$

Combining these equations and using Eq. (32) we find

$$\begin{aligned}
\rho_{A,B,C}^{(odd)} \otimes |\mathbf{q}\rangle_{1,2}\langle\mathbf{q}| \longrightarrow \quad &(1-p)|\mathbf{0}\rangle\langle\mathbf{0}| \otimes |\mathbf{q}\rangle\langle\mathbf{q}| + +\frac{p}{8}\sum_i \left[(Z_i|\mathbf{0}\rangle\langle\mathbf{0}|Z_i) \otimes |\mathbf{q}\rangle\langle\mathbf{q}|\right] \\
&+ \frac{p}{8}\sum_i \left[(Z_i|\mathbf{1}\rangle\langle\mathbf{1}|Z_i) \otimes |\mathbf{\bar{q}}\rangle\langle\mathbf{\bar{q}}|\right].
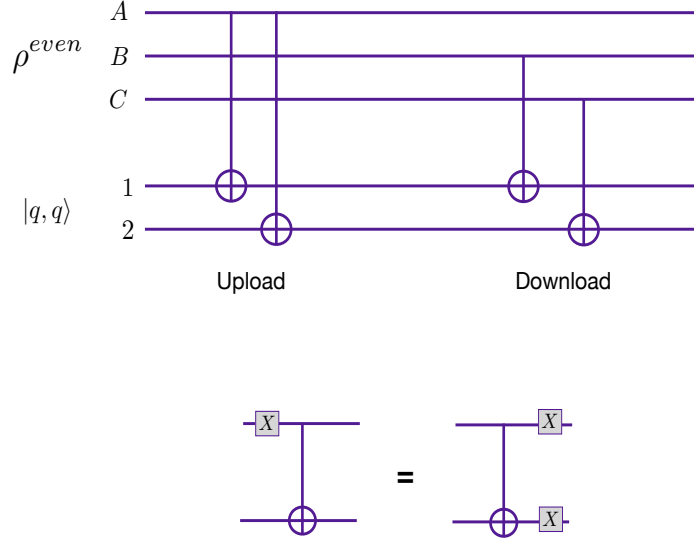\end{aligned} \tag{35}$$

10

Figure 5: The operations of players in even rounds shown in circuit form. The top figure shows encoding of the state $|q\rangle$ and the actions of A, B and C and the bottom figure shows the identity $(C_{i,j}X_i = X_iX_jC_{i,j})$ which is used in deriving (28).

This means that in odd rounds, the states $|\mathbf{q}\rangle$ is transmitted correctly with probability $P = 1 - p + \frac{p}{2} = 1 - \frac{p}{2}$ and in flipped form $|\bar{\mathbf{q}}\rangle$ with probability $P_{error}^{odd} = \frac{p}{2}$. Therefore we have shown the following:

The overall effect of de-polarizing noise on the complete channel: If the carrier is spoiled by depolarizing noise as in (22), the complete quantum channel between the players Φ changes to

$$\Phi(\rho) == \begin{cases} (1 - \frac{3p}{4})\rho + \frac{3p}{4}\sigma_x\rho\sigma_x & \text{even rounds} \\ (1 - \frac{p}{2})\rho + \frac{p}{2}\sigma_x\rho\sigma_x & \text{odd rounds.} \end{cases} \tag{36}$$
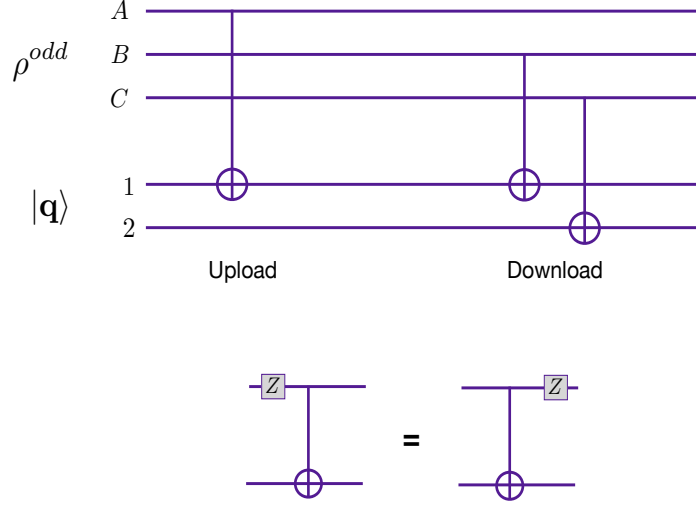
11

Figure 6: The operations of players in odd rounds shown in circuit form. The top figure shows encoding of the state $|q\rangle$ and the actions of A, B and C and the bottom figure shows the identity ($C_{i,j}Z_i = Z_iC_{i,j}$) which is used in deriving (33).

5   Further considerations

In this section we discuss some related problems the first two of them are straightforward and the last one requires further investigation.

5.1   The problem of error correction

What we have shown is that the effect of noisy carriers, when they are affected by de-phased or de-polarized into mixed states is quite simple in the sense that the complete channel of definition (1) becomes a bit-flip channel with different parameters in even and odd rounds as in (21) and (36). Therefore many of the techniques used for quantum error correction, i.e. encoding the states into a larger Hilbert space and using syndrome measurement, can be done to achieve reliable quantum communication.

5.2   Generalization to n-parties

The original noiseless protocol has been generalized to $(1, n)$ schemes where Alice shares her state with n parties [25]. Although the reader can find all the details of this generalization in [25], here we present a few basic facts which help the reader to reconstruct the whole scheme. First we note that the basic property of alternating carriers between $|GHZ_n\rangle$ state and the even state $|\mathbf{0}_n\rangle$ states by the

action of joint Hadamard actions remains intact, i.e.

$$H^{\otimes n}|GHZ_n\rangle = |\mathbf{0}_n\rangle \qquad H^{\otimes n}|\mathbf{0}_n\rangle = |GHZ_n\rangle, \qquad (37)$$

where $|\mathbf{0}_n\rangle$ is defined by induction as in (3). Furthermore, any state $|\psi\rangle = \alpha|0\rangle + b|1\alpha$ is encoded into $\alpha|0^{\otimes n}\rangle + b|1^{\otimes n}\rangle$ in odd rounds (when the carrier is $|GHZ_n\rangle$) and into $a|\mathbf{0}_n\rangle + b|\mathbf{1}_n\rangle$ in even rounds (when the carrier is $|\mathbf{0}_n\rangle$).

5.3   The problem of security

Unlike quantum key distribution where there are information theoretic proofs of security of the schemes, for quantum secret and state sharing, no general and widely accepted proofs are available [27]. Therefore no scheme can claim to be absolutely secure and any scheme of this sort is prone to attacks and cheating among participants. This is true for the multitude of schemes that are have been reported so far [16, 7, 8, 9, 10]. As for the present scheme, some of these attacks, like an outsider Eve entangling herself with the carrier has been discussed in the original proposal [20] and the following literature [25, 21, 22], where improvements have also been proposed to prevent these attacks. Here we have focused on one important aspect of this scheme to see how the whole communication is affected if the main carriers are no longer pure states and have been contaminated by two common types of noise.

6   Conclusion

The main purpose of this paper is to study the theoretical possibility of using entangled states as reusable carriers of information. Therefore our concern has not been practical or security issues of protocols based on this idea. Rather we have studied the robustness of quantum state sharing protocol with reusable entanglement against de-phasing and depolarizing noise. In this type of protocol, the carrier which is a shared entangled state between the legitimate parties acts as a medium to which message states are entangled and disentangled in the sender and receiver ends. During the transition the state identity, being in a highly mixed state is hidden from adversaries. For security of the protocol, the carrier should alternate between two different types and it is crucial that these carriers are not distorted and destroyed completely by noise and the repeated downloading and uploading operations of the parties. The overall effect is that the channel transmits the basis states with a fixed and known error probability that we have calculated. One can then use quantum error correcting codes to transmit quantum states through this channel with as high fidelity as desired at the expense of lowering the transmission rate. Finally we should mention that we have proved the robustness against the two most common types of noise, namely de-phasing and de-polarizing noises. It remains to be seen to what extent this scheme is robust against a general form of noise.

7   Acknowledgements

References

[1] C. H. Bennett, G. Brassard, C. Crpeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. 70, 18951899 (1993).

[2] C. Bennett, and S. Wiesner, Physical Review Letters. 69 (20), 2881(1992))

[3] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. 86, 5188 (2001).

[4] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation. In Proceedings of the 50th Annual Symposium on Foundations of Computer Science, 517526 (2009).

[5] M. Hillery, V. Buzek and A. Berthiaume Phys. Rev. A 59, 1829 (1999).

[6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A 59, 162 (1999).

[7] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, Phys. Rev. A 59, 1829 (1999).

[8] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, Phys. Rev. A 69, 052307 (2004).

[9] Zhan-jun Zhang and Zhong-xiao Man, Phys. Rev. A 72, 022303 (2005).

[10] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, Phys. Rev. A 93, 022325 (2016).

[11] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984

[12] A. Ekert, Physical Review Letters, 67, pp.661-663, (1991).

[13] H. Bechmann-Pasquinucci, and N. Gisin, Phys. Rev. A 59, 4238-4248, (1999).

[14] D. Bru, and C. Macchiavello, Physical Review Letters, 88(12), 127901 (2002).

[15] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. 95, 230505 (2005).

[16] Zhan-jun Zhang, Yong Li, and Zhong-xiao Man Phys. Rev. A 71, 044301 (2005).

[17] A. Tavakoli, I. Herbauts, M. Zukowski, and M. Bourennane, Phys. Rev. A Rapid Communication 92, 030302, (2015).

[18] Vahid Karimipour, Marzieh Asoudeh, Phys. Rev. A 92, Rapid Communications, 030301 (2015).

[19] Y. S. Zhang, C. F. Li, and G. C. Guo; Phys. Rev. A, 64, 024302 (2001).

[20] S. Bagherinezhad and V. Karimipour, Phys. Rev. A 67, 044302 (2003).

[21] F. Gao, F. Guo, Q. Wu and F. Zhu, Phys. Rev. A, 67, 044302, (2003).

[22] Jian-Zhong Du et al., Phys. Rev. A 67, 044302 (2003).

[23] V. Karimipour, Phys. Rev. A 72, 056301 (2005).

[24] V. Karimipour, Phys. Rev. A 74, 016302 (2006).

[25] V. Karimipour and M. Marvian, Int. Journal of Quantum Information (IJQI), Vol. 10, No. 2 (2012) 1250018.

[26] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).

[27] Ioannis Kogias, Yu Xiang, Qiongyi He, Gerardo Adesso, Phys. Rev. A 95, 012315 (2017).