Iranian Journal of Physics Research, Vol. 22, No. 3, 2022
DOI: 10.47176/ijpr.22.3.61463

Stability of entangled carriers against continuous noise

S Emamipanah and M Asoudeh
Department of physics, Azad university, Northern Branch, Tehran, Iran

E-mail: marzieh.asoudeh@gmail.com

(Received 7 June 2022 ; in final form 9 August 2022)

Abstract
Similar to the role of carriers in classical communications as a medium for transmitting messages, entangled states can also be considered a medium that plays the role of the information carrier. In this way, we can define protocols with entangled carriers for quantum communications which can also be used for quantum secret-sharing. The outspread of quantum secret-sharing for many users is the substructure of a quantum internet, so it is essential to study such protocols in terms of their practical implementations. Since protocols are performed in noisy environments without interruption, it is necessary to investigate the performance of protocols under continuous noise. This paper studies the stability of these protocols against dephasing and depolarizing noise. It shows that despite the constant effect of noise, the carrier remains in two types of spaces with the entangled basis, which forms complete spaces for the carrier's qubits. These spaces are compatible with the protocol performance; therefore, the protocol is stable under the noise effect.

Keywords: quantum communication, quantum secret sharing, entangled carriers

1. Introduction

Entanglement is used as a quantum source in most quantum information processes [1-3], such as quantum teleportation and quantum key distribution. In quantum secret sharing schemes [4-8], strong non-classical correlations in entangled states shared between legitimate parties allow them to generate a random key. Of course, there are other cryptographic protocols that do not use entanglement [9-17]. Alice, Bob, and Charlie are the legal parties in these protocols. Alice and Bob want to distribute a secret key between themselves in the quantum key distribution protocol by sharing maximally entangled states and performing specific measurements. Despite eavesdropping, they exchange messages through a communication channel and eventually access an identical and secure key. These keys distributed between Alice and Bob are safe and identical due to the unique features in maximally entangled states.

In addition to the quantum key distribution protocol, we can refer to the secret-sharing protocol, in which Alice wants to send a secret message to Bob and Charlie that they can only read with their contribution. This article explains the secret-sharing protocol in which entanglement is used as a secure carrier of information to send a message. Using entangled states between two distant points as a secure and reusable information carrier was first proposed in 2001 [18], and then expanded to the issue of secret-sharing in 2003 [19]. This idea is, in fact, a quantum extension of the concept that exists in today's classical communications network. The sender uploads the message to the carrier, and at the destination, the recipients download the message and leave the carrier intact for reuse. Carrier's security means that the state of the message during the transmission is hidden from the eavesdropper's point of view. (We call eavesdropper Eve). In this protocol, the message can be classical or quantum. Classical messages are the classical bits encoded in the standard basis $\{|0\rangle,|1\rangle\}$, and the quantum messages are the states encoded in the superposition of these basis:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle . \quad (1)$$

This paper examines the effect of two important types of noise, called dephasing and depolarizing, which continuously affect a secret-sharing protocol. In the article [20], we assumed that before running the protocol, the carrier was disturbed once with noise, and the protocol execution time is such that the added noise

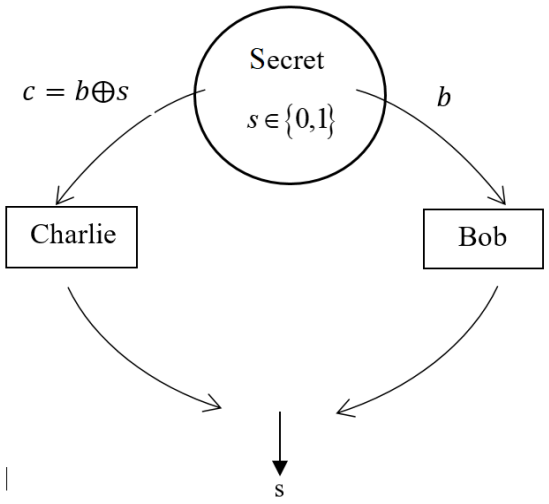

Figure 1. Classical secret-sharing protocol.

can be ignored. In this paper, we will discuss that even if we consider the noise effect not just once but continuously, the carrier remains in two specific spaces with entangled basis that are complete spaces for the carrier qubits and are compatible with the protocol performance. After this introduction, In the second part, we will introduce a classical and quantum secret-sharing protocol. In the third section, we will study a secret-sharing protocol, which considers a different role for the entangled states as the carrier of information. The fourth section will discuss about quantum channels. The fifth section will investigate the effect of dephasing and depolarizing noise on the secret-sharing protocol. In the sixth section, we will see the continuous noise effect on the secret-sharing protocol. Eventually, in the seventh section, we will conclude.

2. Secret-Sharing

2. 1. Classical secret-sharing protocol

In the classical secret-sharing protocol, Alice wants to distribute a classical secret S to Bob and Charlie by sending a portion of the secret to Bob and another to Charlie (S is a bit, $S\in\{0,1\}$). Alice sends the bit b to Bob and the bit c to Charlie (figure 1) so that neither of them can recover the secret on their own. Bob does not know S even though he has b, and Charlie does not know S even though he has c. We call this protocol secret-sharing because Bob and Charlie can recover the secret S only by exchanging their shares.

For this purpose, Alice randomly chooses a bit $b\in\{0,1\}_R$. (R index emphasizes the randomness). Alice adds the secret S with the bit b in mud 2, and calls it the bit c:

$$b \oplus s = c. \tag{2}$$

Whatever S is, due to the randomness of b, the bit c will also be random. From the outside observer's point of view, both bits are random and uniform. When Bob and Charlie add their shares in mud 2, the secret S will be recovered:

$$b \oplus c = b \oplus (b \oplus s) = s. \tag{3}$$

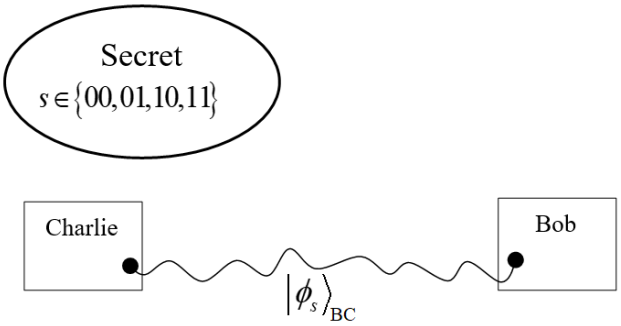

Figure 2. Quantum secret-sharing protocol

In the classical secret-sharing protocol, one bit is shared by two 1-bit shares, but we can do better by using quantum states.

2. 2. Quantum secret-sharing protocol

In the quantum secret-sharing protocol, Alice wants to share a classical two-bit secret $S\in\{00,01,10,11\}$ using Bell entangled states (figure 2). Bell entangled states are the basis for two-qubit four-dimensional space:

$$\begin{aligned}
|\phi_{00}\rangle_{BC} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\\
|\phi_{01}\rangle_{BC} &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),\\
|\phi_{10}\rangle_{BC} &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),\\
|\phi_{11}\rangle_{BC} &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).
\end{aligned} \tag{4}$$

Alice encodes the secret S into Bell states $|\phi_S\rangle_{BC}$ and by sending qubit B to Bob and qubit C to Charlie, she shares the entangled Bell states between them. Bell states are locally indistinguishable; the reduced density matrix of Bob and Charlie's qubits are in maximally mixed states and therefore does not contain any information about the secret S:

$$\rho_B^S = \rho_C^S = \frac{I}{2}. \tag{5}$$

The role of quantum mechanics in the secret-sharing problem is that a maximally entangled state has maximally mixed subspaces; all the information is in the correlation between two qubits, and each qubit alone has no information.

The quantum state $|\phi_S\rangle_{BC}$ should recover the secret S with a probability of 1. So there must be a measurement that measures $|\phi_S\rangle_{BC}$ and retrieves S. ($|\phi_S\rangle_{BC}$ states should be perpendicular for different S, which they are!). Since Bell states form a perpendicular basis, they are distinguishable. If Bob sends his qubit to Charlie, he can measure his and Bob's qubit in the Bell basis and retrieve the classical bits. So with the help of entanglement, we managed to recover two classical bits by sending one qubit. This quantum protocol is twice as efficient as the classical protocol.

3. Quantum secret-sharing with entangled states

In this section, entangled states have a different role than the last section. In the last section, the message was encoded into the entangled state, but here the message is uploaded to the entangled state. In this new role, entangled states are a medium for conveying the message (figure 3).

To begin the discussion, first, we introduce the CNOT control operator. CNOT operates on a two-qubit state; one is the control qubit and the other the target. If the control qubit were $|0\rangle$, the effect of the CNOT on the target qubit would be the same as the effect of the unit operator. (Does nothing). If the control qubit were $|1\rangle$, the effect of CNOT on the target qubit would be similar to that of the Pauli X operator. (Bit-flip operator).

Using entangled states as a secure information carrier between two points is such that Alice wants to send the message q to Bob using the state $|\phi\rangle_{AB}=(|00\rangle+|11\rangle)/\sqrt{2}$ that is shared as a carrier between Alice and Bob. Alice encodes the message q into state $|q\rangle_1$ (qubit 1 corresponds to message state). She then affects the operator $C_{A,1}$ on the carrier and message state. ($C_{A,1}$ is a CNOT control operator, which control qubit is A, and its target qubit is 1). This is how the message q gets entangled with the carrier:

$$\begin{aligned} &C_{A,1}\left[\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{AB}|q\rangle_1\right] \\ &=\frac{1}{\sqrt{2}}\left(|00q\rangle+|11\bar{q}\rangle\right)_{AB,1}. \end{aligned} \tag{6}$$

($\bar{q}$ is q flipped: $\bar{0}=1$, $\bar{1}=0$). Alice sends qubit 1 to Bob. In the above equation, if one takes a partial trace with respect to A and B, one will see that qubit 1 is in a maximally mixed state during the transfer; that is, from Eve's point of view, the message is uniform and completely random:

$$\rho_1=\frac{1}{2}\left(|q\rangle\langle q|+|\bar{q}\rangle\langle\bar{q}|\right)=\frac{I}{2}, \tag{7}$$

At the destination, Bob receives qubit 1 and affects operator $C_{B,1}$:

$$\begin{aligned} &C_{B,1}\left[\frac{1}{\sqrt{2}}\left(|00q\rangle|00\bar{q}\rangle\right)_{AB,1}\right] \\ &=\frac{1}{\sqrt{2}}\left(|00q\rangle+|11q\rangle\right)_{AB,1} \\ &=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{AB}|q\rangle_1. \end{aligned} \tag{8}$$

As one can see, the message has been separated from the carrier, and Bob has received Alice's message correctly. The carrier is also left intact for reuse.

In secret-sharing schemes, Alice sends a secret message to Bob and Charlie that they can only read the message with their cooperation. We introduce a protocol that uses an entangled state as a carrier between Alice, Bob, and Charlie to send a message. The role of entangled states as a carrier is that Alice can hide the message state from Eve's view by entangling the message with the carrier while transmitting it to Bob and Charlie. It is assumed that Bob and Charlie are in the same place at the destination so that they can read the message together. Before examining how the protocol is implemented, we will first mention conventions.

The even parity and the odd parity for two qubits are as follows:

$$\begin{aligned} |\tilde{0}\rangle&=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right), \\ |\tilde{1}\rangle&=\frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right). \end{aligned} \tag{9}$$

which are summarized as follows:

$$|\tilde{q}\rangle=\frac{1}{\sqrt{2}}\left(|0,q\rangle+|1,\bar{q}\rangle\right). \tag{10}$$

Sometimes we skip normalization coefficients. For example, when we write $(|000\rangle+|111\rangle)$ we mean the normalized state $(|000\rangle+|111\rangle)/\sqrt{2}$. The even parity and the odd parity for three qubits are written as follows:

$$\begin{aligned} |\tilde{0}\rangle_{ABC}&=|0\rangle_A|\tilde{0}\rangle_{BC}+|1\rangle_A|\tilde{1}\rangle_{BC} \\ &=|000\rangle+|011\rangle+|101\rangle+|110\rangle. \\ |\tilde{1}\rangle_{ABC}&=|0\rangle_A|\tilde{1}\rangle_{BC}+|1\rangle_A|\tilde{0}\rangle_{BC} \\ &=|001\rangle+|010\rangle+|100\rangle+|111\rangle. \end{aligned} \tag{11}$$

We start the protocol execution with even rounds (0,2,4,…) in these rounds, Alice, Bob, and Charlie share the entangled state $|GHZ\rangle=(|000\rangle+|111\rangle)_{ABC}/\sqrt{2}$ as a carrier. Qubits A, B, and C are respectively the share qubits of Alice, Bob, and Charlie from the carrier. In even rounds, Alice encodes the message $|q\rangle$ into the product state $|q,q\rangle_{1,2}$ and entangles it to the carrier with operator $C_{A,1}C_{A,2}$:

$$\begin{aligned} &\left(C_{A,1}C_{A,2}\right)\left[\left(|000\rangle+|111\rangle\right)_{ABC}|q,q\rangle_{1,2}\right] \\ &=\left(|000\rangle|q,q\rangle+|111\rangle|\bar{q},\bar{q}\rangle\right)_{ABC,1,2} \end{aligned} \tag{12}$$

Alice sends qubit 1 to Bob and qubit 2 to Charlie. These qubits are in a maximally mixed state during transfer; they are completely random and uniform from Eve's point of view. At the destination, with affecting operator $C_{B,1}$, Bob can independently detach $|q\rangle_1$ from the carrier and read the message sent by Alice:

$$\begin{aligned} &C_{B,1}\left(|000\rangle|q,q\rangle+|111\rangle|\bar{q},\bar{q}\rangle\right)_{ABC,1,2} \\ &=\left(|000\rangle|q,q\rangle+|111\rangle|q,\bar{q}\rangle\right)_{ABC,1,2} \\ &=\left(|000\rangle|q\rangle+|111\rangle|\bar{q}\rangle\right)_{ABC,2}|q\rangle_1. \end{aligned} \tag{13}$$

Charlie can also affect operator $C_{C,2}$, and detach $|q\rangle_2$ from the carrier and read the message independently:

$$\begin{aligned} &C_{C,2}\left(|000\rangle|q\rangle+|111\rangle|\bar{q}\rangle\right)_{ABC,2} \\ &=\left(|000\rangle+|111\rangle\right)_{ABC}|q\rangle_2. \end{aligned} \tag{14}$$

At the end of even rounds, Alice, Bob, and Charlie each individually affect the Hadamard operator H on their shares of carrier and turn it from state $|GHZ\rangle_{ABC}$ to state $|\tilde{0}\rangle_{ABC}$:

$$\left(H_A\otimes H_B\otimes H_C\right)|GHZ\rangle_{ABC}=|\tilde{0}\rangle_{ABC} \tag{15}$$

To get the above equation, we used our conventions and the following:

$$\begin{aligned} &H|0\rangle=|+\rangle,\ H|1\rangle=|-\rangle.\\ &|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle).\\ &|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle). \end{aligned} \tag{16}$$

The carrier of odd rounds $(1,3,5,\ldots)$ is an entangled state $|\tilde{0}\rangle_{ABC}$ Alice encodes the message $|q\rangle$, in an entangled state $|\tilde{q}\rangle_{1,2}$, and entangles it with operator $C_{A,1}$ or $C_{A,2}$ to the carrier. (It does not matter which operator Alice chooses):

$$\begin{aligned} &C_{A,1}\left[|\tilde{0}\rangle_{ABC}|\tilde{q}\rangle_{1,2}\right]\\ &=|0\rangle_A|\tilde{0}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{1}\rangle_{BC}|\tilde{\tilde{q}}\rangle_{1,2} \end{aligned} \tag{17}$$

Alice sends qubit 1 to Bob and qubit 2 to Charlie. qubit 1 and qubit 2 are individually in a maximally mixed state during the transfer. At the destination, Bob and Charlie, after receiving qubits 1 and 2, collaborate to affect the operator $C_{B,1}C_{C,2}$ and separate the message from the carrier:

$$\begin{aligned} &\left(C_{B,1}C_{C,2}\right)\left[|0\rangle_A|\tilde{0}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{1}\rangle_{BC}|\tilde{\tilde{q}}\rangle_{1,2}\right]\\ &=|\tilde{0}\rangle_{ABC}|\tilde{q}\rangle_{1,2} \end{aligned} \tag{18}$$

In the above equation, the control space of CNOT operators is on qubits B and C. The target space is on qubits 1 and 2. Since $|\tilde{0}\rangle_{BC}$ is an even parity of two qubits, and $|\tilde{1}\rangle_{BC}$ is an odd parity of two qubits, $|\tilde{q}\rangle_{1,2}$ does not change when $|\tilde{0}\rangle_{BC}$ is 0 in control, but $|\tilde{\tilde{q}}\rangle_{1,2}$ is flipped and transformed in $|\tilde{q}\rangle_{1,2}$ when $|\tilde{1}\rangle_{BC}$ is in control. Because $H^2=I$, at the end of odd rounds, Alice, Bob, and Charlie return the carrier's state from $|\tilde{0}\rangle_{ABC}$ to $|GHZ\rangle_{ABC}$, by acting Hadamard on their carrier's share.

Since Bob and Charlie can read the message independently in even rounds, Alice sends extra qubits that do not contain important information in these rounds. Instead, she sends secret messages only in odd rounds where Bob and Charlie collaborate to read the message. The question may be asked, why do we not use only odd rounds? The answer is that the presence of the Hadamard operator, which converts the carrier between rounds, makes Eve separated from the carrier if she wants to entangle herself with it. To prove, suppose that Eve has entangled herself with the carrier of even and odd rounds as follows:

$$\begin{aligned} &\left|\begin{matrix}GHZ_{ABC},E\rangle\\ \tilde{0}_{ABC},E\rangle\end{matrix}\right.=|000\rangle\eta_{000}+|111\rangle\eta_{111}\\ &=|000\rangle\xi_{000}+|011\rangle\xi_{011}+|101\rangle\xi_{101}+|110\rangle\xi_{110}. \end{aligned} \tag{19}$$

At the end of even rounds, when Alice, Bob, and Charlie apply Hadamard operators, the carrier becomes as follows:

$$\begin{aligned} &H^{\otimes 3}|GHZ,E\rangle\\ &=|+++\rangle\eta_{000}+|---\rangle\eta_{111}\\ &=\left(|\tilde{0}\rangle_{ABC}+|\tilde{1}\rangle_{ABC}\right)\eta_{000}+\left(|\tilde{0}\rangle_{ABC}-|\tilde{1}\rangle_{ABC}\right)\eta_{111}\\ &=|\tilde{0}\rangle_{ABC}(\eta_{000}+\eta_{111})+|\tilde{1}\rangle_{ABC}(\eta_{000}-\eta_{111}). \end{aligned} \tag{20}$$

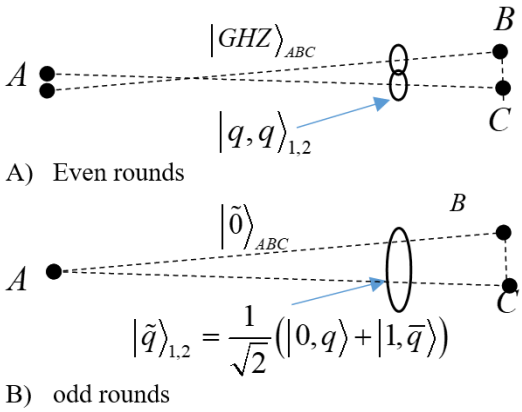

Figure 3. The secret-sharing protocol using the entangled carriers.

After applying the Hadamard operators, even rounds carrier must be turned into $|\tilde{0}\rangle_{ABC}$. So we should have, $\eta_{000}=\eta_{111}$ which causes Eave to get separated from the carrier in the even rounds. For equality of equations (14) and (15), it must be $\xi_{000}=\xi_{011}=\xi_{101}=\xi_{110}$, in which case Eve also get separated from the odd rounds carrier.

We saw how Alice could send the standard basis (classical message) to Bob and Charlie. Any superposition of basis states is a quantum message $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$. Due to the linearity of this process, Alice can send the quantum messages as $|\phi'\rangle=\alpha|00\rangle+\beta|11\rangle$ in even and as $|\phi''\rangle=\alpha|\tilde{0}\rangle+\beta|\tilde{1}\rangle$ in odd rounds.

4. Noise

4. 1. Quantum channels

Suppose we have a quantum system in an arbitrary state ρ. The state ρ may change due to a physical process. There are different dynamics for quantum systems. The simplest dynamic assumes that the system does not interact with the external environment. Or in other words, the system is closed. According to the principles of quantum mechanics, the dynamics of a closed system is characterized by unitary operators:

$$\rho\rightarrow U\rho U^{+}. \tag{21}$$

Now the question is, if the system is not closed and interacts with its surroundings, what is the dynamic of the system state. Another point is that the change induced by measurement on a quantum system can also be Considered a quantum dynamic. It is also possible for a quantum dynamic to be a combination of unitary transformation and measurement. Depending on the conditions of the problem, a quantum dynamic is called a quantum map or quantum channel. The effect of the surrounding environment on a quantum system is called noise. In quantum information, noise is considered a channel that affects the quantum state. The most general evolution of the quantum system ρ is written as follows:

$$\rho\rightarrow\sum_{e}V_e\rho V_e^{+}. \tag{22}$$

In the above equation, V_e is called the Kraus operator, which applies in the following condition:

$$I = \sum_e V_e^+ V_e. \tag{23}$$

4. 2. Dephasing channel

For examining the dephasing noise, consider a qubit in a pure state $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$. In this linear combination, basis states $(|0\rangle,|1\rangle)$ are in a relative phase. The dephasing channel gradually eliminates the relative phase of these two states and eventually creates a mixed state. To model this noise, we assume that an operation $R_Z(\theta)$ makes phase difference θ on the states $|0\rangle,|1\rangle$. It irregularly affects the initial state with a Gaussian distribution and converts it as follows:

$$|\psi\rangle\langle\psi| \to \int p(\theta) R_Z(\theta)|\psi\rangle\langle\psi|R_Z^+(\theta)d\theta \tag{24}$$

4.3. Depolarizing channel

The depolarizing channel maintains the initial quantum state ρ with probability (1–P), and erases all the information with the error probability P; converts the state into a maximally mixed state, which is an entirely random and uniform state:

$$\rho \to (1-p)\rho + p\frac{I}{2} \tag{25}$$

The above equation is written for a qubit channel, which the maximally mixed state is $I/2$. The equation gets arranged using the following relation:

$$2I = \rho + X\rho X + Y\rho Y + Z\rho Z \tag{26}$$

X, Y, and Z are Pauli operators. Therefore, the depolarizing channel transforms a qubit state as follows:

$$\rho \to \frac{1-3P}{4}\rho + \frac{P}{4}X\rho X + \frac{P}{4}Y\rho Y + \frac{P}{4}Z\rho Z \tag{27}$$

The above equation shows that X, Y, and Z errors occur with equal probability in a depolarizing channel.

5. Secret-sharing protocol with noisy carriers

5. 1. The effect of dephasing noise

Consider a pure state $|GHZ\rangle=(|000\rangle+|111\rangle)/\sqrt{2}$; a linear combination of two basis states $(|000\rangle,|111\rangle)$ with a certain relative phase. The dephasing noise acts on the qubits as random phase kicks, gradually vanishing the relative phase and eventually creating a mixed state. Suppose that irregular phase kicks on the qubit j cause a phase difference θ_j:

$$\begin{aligned} Z|0\rangle = |0\rangle \to e^{i\theta_j Z}|0\rangle = e^{i\theta_j}|0\rangle, \\ Z|1\rangle = -|1\rangle \to e^{i\theta_j Z}|1\rangle = e^{-i\theta_j}|1\rangle. \end{aligned} \tag{28}$$

The effect of phase kicks on three qubits is as follows:

$$\begin{aligned} & e^{i\theta_1 Z}e^{i\theta_2 Z}e^{i\theta_3 Z}|000\rangle \\ & = e^{i(\theta_1+\theta_2+\theta_3)}|000\rangle = e^{i\theta}|000\rangle. \\ & e^{i\theta_1 Z}e^{i\theta_2 Z}e^{i\theta_3 Z}|111\rangle \\ & = e^{-i(\theta_1+\theta_2+\theta_3)}|111\rangle = e^{-i\theta}|111\rangle. \end{aligned} \tag{29}$$

The effect of the dephasing noise on the state $|GHZ\rangle\langle GHZ|$ is obtained as follows:

$$\frac{1}{2}\int p(\theta)\begin{bmatrix} |000\rangle\langle 000| + e^{2i\theta}|000\rangle\langle 111| \\ +e^{-2i\theta}|111\rangle\langle 000| + |000\rangle\langle 000| \end{bmatrix} d\theta \tag{30}$$

In the above equation, we assume that the phase kicks are symmetric around zero, and the probability distribution function is even. We set the integral of this function equal to the value $(1-2P)$:

$$\begin{aligned} & (1-2P)|GHZ\rangle\langle GHZ| \\ & +P\left(|GHZ\rangle\langle GHZ| + |GHZ'\rangle\langle GHZ'|\right) \end{aligned} \tag{31}$$

In the above equation, we defined the state $|GHZ'\rangle=(|000\rangle-|111\rangle)/\sqrt{2}$. Due to the dephasing noise, with the probability (1–P), the $|GHZ\rangle$ state does not change, but with the probability of an error P, it changes into the $|GHZ'\rangle$ state:

$$\begin{aligned} & |GHZ\rangle\langle GHZ|_{ABC} \to \\ & (1-P)|GHZ\rangle\langle GHZ|_{ABC} \\ & +P|GHZ'\rangle\langle GHZ'|_{ABC} \end{aligned} \tag{32}$$

Therefore, the noisy even rounds carrier is written as follows:

$$\begin{aligned} \rho^{even} &= (1-P)|GHZ\rangle\langle GHZ|_{ABC} \\ &+P|GHZ'\rangle\langle GHZ'|_{ABC}. \end{aligned} \tag{33}$$

How does the noisy carrier work in even rounds? $|GHZ\rangle$ part of a carrier works as well as before, but we have to check the performance of $|GHZ'\rangle$ part. In even rounds, the message is encoded in the product state $|q,q\rangle_{1,2}$ (figure 4) and the CNOT operators used by Alice, Bob, and Charlie to upload and download the message are $\Omega^{even}=C_{B,2}C_{B,1}C_{A,2}C_{A,1}$. In delivering the message $|GHZ'\rangle$ works as follows:

$$\begin{aligned} & \Omega^{even}\left(|000\rangle-|111\rangle\right)_{ABC}|q,q\rangle_{1,2} \\ & = \left(|000\rangle-|111\rangle\right)_{ABC}|q,q\rangle_{1,2} \end{aligned} \tag{34}$$

$|GHZ'\rangle$ is acting as well as $|GHZ\rangle$, because at the end of the round, the message is correctly separated from the carrier. Alice, Bob, and Charlie apply the Hadamard operators on the carrier, turning it into the carrier of the odd rounds. We know that $H^{\otimes 3}|GHZ\rangle_{ABC}=|\tilde{0}\rangle_{ABC}$, but we should check the effect of Hadamard operators on $|GHZ'\rangle$:

$$\begin{aligned} & (H_A\otimes H_B\otimes H_C)\left(|000\rangle-|111\rangle\right)_{ABC} \\ & = \left(|{+}{+}{+}\rangle-|{-}{-}{-}\rangle\right)_{ABC} \\ & = \left(|001\rangle+|010\rangle+|100\rangle+|111\rangle\right)_{ABC} \\ & = |0\rangle_A|\tilde{1}\rangle_{BC}+|1\rangle_A|\tilde{0}\rangle_{BC} = |\tilde{1}\rangle_{ABC}. \end{aligned} \tag{35}$$

Therefore, the odd rounds noisy carrier is as follows:

$$\rho^{odd} = (1-P)|\tilde{0}\rangle\langle\tilde{0}|_{ABC} + P|\tilde{1}\rangle\langle\tilde{1}|_{ABC}. \tag{36}$$

In odd rounds (figure 4), the message is encoded in an entangled state $|\tilde{q}\rangle_{1,2}$. How does the noisy carrier deliver the message? We already know that $|\tilde{0}\rangle_{ABC}$ part of the carrier is working well, but we have to check the

performance of $|\tilde{1}\rangle_{ABC}$ part. Alice uploads the message to the carrier by operator $C_{A,1}$ or $C_{A,2}$:

$$\begin{aligned} &C_{A,1}\left(|\tilde{1}\rangle_{ABC}|\tilde{q}\rangle_{1,2}\right)\\ &=C_{A,1}\left[\left(|0\rangle_A|\tilde{1}\rangle_{BC}+|1\rangle_A|\tilde{0}\rangle_{BC}\right)\left(|0,q\rangle+|1,\bar{q}\rangle\right)_{1,2}\right]\\ &=|0\rangle_A|\tilde{1}\rangle_{BC}\underbrace{\left(|0,q\rangle+|1,\bar{q}\rangle\right)_{1,2}}_{|\tilde{q}\rangle_{1,2}}\\ &+|1\rangle_A|\tilde{0}\rangle_{BC}\underbrace{\left(|1,q\rangle+|0,\bar{q}\rangle\right)_{1,2}}_{|\tilde{\bar{q}}\rangle_{1,2}}. \end{aligned} \tag{37}$$

Alice sends qubit 1 to Bob and qubit 2 to Charlie. The above equation shows that these qubits are in a maximally mixed state during transmission. At the destination, Bob and Charlie have to contribute to download the message from the carrier:

$$\begin{aligned} &\left(C_{B,1}C_{C,2}\right)\left[|0\rangle_A|\tilde{1}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{0}\rangle_{BC}|\tilde{\bar{q}}\rangle_{1,2}\right]\\ &=|0\rangle_A|\tilde{1}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{0}\rangle_{BC}|\tilde{\bar{q}}\rangle_{1,2}\\ &=\underbrace{\left(|0\rangle_A|\tilde{1}\rangle_{BC}+|1\rangle_A|\tilde{0}\rangle_{BC}\right)}_{|\tilde{1}\rangle_{ABC}}|\tilde{\bar{q}}\rangle_{1,2}. \end{aligned} \tag{38}$$

In the above equation, the message is separated from the carrier but delivered in a flipped form. The total CNOT operators in odd rounds are $\Omega^{odd}=C_{B,1}C_{C,2}C_{A,1}$. So the performance of $|\tilde{1}\rangle_{ABC}$ in the delivery of the message is as follows:

$$\Omega^{odd}|\tilde{1}\rangle_{ABC}|\tilde{q}\rangle_{1,2}=|\tilde{1}\rangle_{ABC}|\tilde{\bar{q}}\rangle_{1,2}. \tag{39}$$

The dephasing noise effect on the secret-sharing protocol can be summarized as follows: In even rounds in which the message q is encoded in a product state $|q,q\rangle_{1,2}$, the carrier $|GHZ\rangle$ get mixed with state $|GHZ'\rangle$ which works as well as $|GHZ\rangle$ state in delivering the message. In odd rounds, message q is encoded in an entangled state $|\tilde{q}\rangle_{1,2}$, and the carrier $|\tilde{0}\rangle_{ABC}$ get mixed with $|\tilde{1}\rangle_{ABC}$ state which flips the message. The message is received correctly with probability (1–P) and is flipped with the probability of error P.

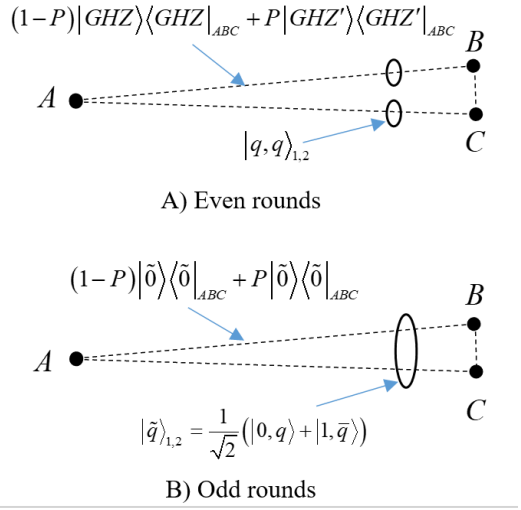

Figure 4. The effect of dephasing noise on the secret-sharing protocol with entangled carriers

5.2. The effect of depolarizing noise

Due to the depolarizing noise, the carrier $|GHZ\rangle_{ABC}$ does not change with probability (1–P), but each of its qubits happens into a maximally mixed state with the error probability P:

$$\begin{aligned} &|GHZ\rangle\langle GHZ|_{ABC}\rightarrow\\ &(1-P)|GHZ\rangle\langle GHZ|_{ABC}+P\left(\frac{I_A}{2}\otimes\frac{I_B}{2}\otimes\frac{I_C}{2}\right). \end{aligned} \tag{40}$$

Three qubits are in an eight-dimensional space. We can consider the following entangled states as the basis of eight-dimensional space:

$$\begin{aligned} |GHZ_1\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle).\\ |GHZ'_1\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle).\\ |GHZ_2\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|110\rangle+|001\rangle).\\ |GHZ'_2\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|110\rangle-|001\rangle).\\ |GHZ_3\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|101\rangle+|010\rangle).\\ |GHZ'_3\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|101\rangle-|010\rangle).\\ |GHZ_4\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|011\rangle+|100\rangle).\\ |GHZ'_4\rangle_{ABC}&=\frac{1}{\sqrt{2}}(|011\rangle-|100\rangle). \end{aligned} \tag{41}$$

The above states form a complete space for the carrier's qubits:

$$I_{ABC}=\sum_{i=1}^{4}|GHZ_i\rangle\langle GHZ_i|_{ABC}+|GHZ'_i\rangle\langle GHZ'_i|_{ABC}. \tag{42}$$

Note that $|GHZ_1\rangle$ is indeed $|GHZ\rangle$ state. Therefore, the even rounds noisy carrier is written as follows:

$$\begin{aligned} \rho^{even}&=(1-P)|GHZ_1\rangle\langle GHZ_1|_{ABC}\\ &+\frac{P}{8}\sum_{i=1}^{4}|GHZ_i\rangle\langle GHZ_i|_{ABC}+|GHZ'_i\rangle\langle GHZ'_i|_{ABC} \end{aligned} \tag{43}$$

$|GHZ_i\rangle$ and $|GHZ'_i\rangle$ are the components of the noisy carrier in even rounds (figure 5). To evaluate the carrier performance, we must examine the performance of each these components in delivering the message:

$$\begin{aligned} &\Omega^{even}|GHZ_1\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ_1\rangle_{ABC}|q,q\rangle_{1,2}.\\ &\Omega^{even}|GHZ'_1\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ'_1\rangle_{ABC}|q,q\rangle_{1,2}.\\ &\Omega^{even}|GHZ_2\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ_2\rangle_{ABC}|q,\bar{q}\rangle_{1,2}.\\ &\Omega^{even}|GHZ'_2\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ'_2\rangle_{ABC}|q,\bar{q}\rangle_{1,2}.\\ &\Omega^{even}|GHZ_3\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ_3\rangle_{ABC}|\bar{q},q\rangle_{1,2}.\\ &\Omega^{even}|GHZ'_3\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ'_3\rangle_{ABC}|\bar{q},q\rangle_{1,2}.\\ &\Omega^{even}|GHZ_4\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ_4\rangle_{ABC}|\bar{q},\bar{q}\rangle_{1,2}.\\ &\Omega^{even}|GHZ'_4\rangle_{ABC}|q,q\rangle_{1,2}=|GHZ'_4\rangle_{ABC}|\bar{q},\bar{q}\rangle_{1,2}. \end{aligned} \tag{44}$$

In the above equation, in all cases, at the end of the round, the message is separated from the carrier. The state $|q,q\rangle_{1,2}$ is delivered correctly with the probability 1–3P/4, but one or both of its qubits get flipped with the error probability 3P/4. (Remember that no secret message is sent in even rounds). At the end of rounds,

due to the Hadamard operators, $|GHZ_i\rangle_{ABC}$ states turn into $|\tilde{0}_i\rangle_{ABC}$ states, and $|GHZ'_i\rangle_{ABC}$ states turn into $|\tilde{1}_i\rangle_{ABC}$ states:

$$\begin{aligned}
&|\tilde{0}_1\rangle_{ABC} = |000\rangle + |011\rangle + |101\rangle + |110\rangle.\\
&|\tilde{1}_1\rangle_{ABC} = |111\rangle + |100\rangle + |010\rangle + |001\rangle.\\
&|\tilde{0}_2\rangle_{ABC} = |000\rangle - |011\rangle - |101\rangle + |110\rangle.\\
&|\tilde{1}_2\rangle_{ABC} = |111\rangle - |100\rangle - |010\rangle + |001\rangle.\\
&|\tilde{0}_3\rangle_{ABC} = |000\rangle - |011\rangle + |101\rangle - |110\rangle.\\
&|\tilde{1}_3\rangle_{ABC} = |111\rangle - |100\rangle + |010\rangle - |001\rangle.\\
&|\tilde{0}_4\rangle_{ABC} = |000\rangle + |011\rangle - |101\rangle - |110\rangle.\\
&|\tilde{1}_4\rangle_{ABC} = |111\rangle + |100\rangle - |010\rangle - |001\rangle.
\end{aligned} \tag{45}$$

The above entangled states also form a complete space for the three qubits carrier. (The space basis can be converted with unitary operators, Here, the Hadamard operators that parties apply at the end of the rounds play this role):

$$I_{ABC} = \sum_{i=1}^{4} |\tilde{0}_i\rangle\langle\tilde{0}_i|_{ABC} + |\tilde{1}_i\rangle\langle\tilde{1}_i|_{ABC}. \tag{46}$$

Therefore, the noisy carrier of the odd rounds is as follows:

$$\begin{aligned}
\rho^{odd} &= (1-P)|\tilde{0}_1\rangle\langle\tilde{0}_1|_{ABC}\\
&+ \frac{P}{8}\sum_{i=1}^{4} |\tilde{0}_i\rangle\langle\tilde{0}_i|_{ABC} + |\tilde{1}_i\rangle\langle\tilde{1}_i|_{ABC}.
\end{aligned} \tag{47}$$

Notice that $|\tilde{0}_1\rangle_{ABC}$ is the same as $|\tilde{0}\rangle_{ABC}$ state, and $|\tilde{1}_1\rangle_{ABC}$ is also the same as $|\tilde{1}\rangle_{ABC}$ state. To examine the noisy carrier performance in odd rounds (figure 5), we should analyze the performance of its components, which include $|\tilde{0}_i\rangle_{ABC}$ and $|\tilde{1}_i\rangle_{ABC}$ states:

$$\begin{aligned}
&\Omega^{odd}|\tilde{0}_1\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{0}_1\rangle_{ABC}|\tilde{q}\rangle_{1,2}.\\
&\Omega^{odd}|\tilde{1}_1\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{1}_1\rangle_{ABC}|\bar{\tilde{q}}\rangle_{1,2}.\\
&\Omega^{odd}|\tilde{0}_2\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{0}_2\rangle_{ABC}|\tilde{q}\rangle_{1,2}.\\
&\Omega^{odd}|\tilde{1}_2\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{1}_2\rangle_{ABC}|\bar{\tilde{q}}\rangle_{1,2}.\\
&\Omega^{odd}|\tilde{0}_3\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{0}_3\rangle_{ABC}|\tilde{q}\rangle_{1,2}.\\
&\Omega^{odd}|\tilde{1}_3\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{1}_3\rangle_{ABC}|\bar{\tilde{q}}\rangle_{1,2}.\\
&\Omega^{odd}|\tilde{0}_4\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{0}_4\rangle_{ABC}|\tilde{q}\rangle_{1,2}.\\
&\Omega^{odd}|\tilde{1}_4\rangle_{ABC}|\tilde{q}\rangle_{1,2} = |\tilde{1}_4\rangle_{ABC}|\bar{\tilde{q}}\rangle_{1,2}.
\end{aligned} \tag{48}$$

In the above equation, in all cases, at the end of the round, the message gets detached from the carrier. In cases $|\tilde{0}_i\rangle_{ABC}$ (three qubits even parity), the message is received correctly, and in cases $|\tilde{1}_i\rangle_{ABC}$ (three qubits odd parity), the message is delivered in a flipped form. In odd rounds, with the probability (1–P/2) the message is delivered correctly, and with the error probability P, the message is received as a flipped form.

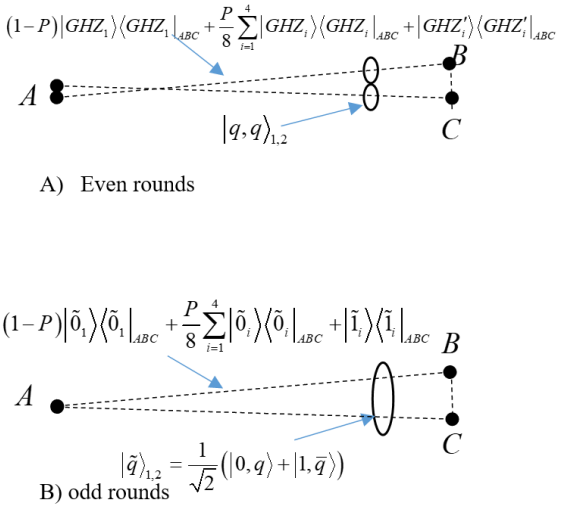

Figure 5. The effect of depolarizing noise on the secret-sharing protocol with entangled carriers.

6. Secret-sharing with continuous noise

6. 1. The effect of continuous dephasing noise

To investigate the effect of dephasing noise uninterruptedly, we assume that it is round 1, and the noise has been applied once, so the carrier is written in the form of equation (36). (We can also start from the equation (33), it does not affect the discussion). If the dephasing noise is to enter the carrier continuously, we must calculate its effect on all possible parts of the carrier. According to the calculations detailed in section 5.1, we will have:

$$\begin{aligned}
&|\tilde{0}_i\rangle\langle\tilde{0}_i| \to (1-P)|\tilde{0}_i\rangle\langle\tilde{0}_i| + \frac{P}{3}\left[\sum_{j\neq i}|\tilde{0}_j\rangle\langle\tilde{0}_j|\right]\\
&|\tilde{1}_i\rangle\langle\tilde{1}_i| \to (1-P)|\tilde{1}_i\rangle\langle\tilde{1}_i| + \frac{P}{3}\left[\sum_{j\neq i}|\tilde{1}_j\rangle\langle\tilde{1}_j|\right]
\end{aligned} \tag{49}$$

According to the above equation, the effect of continuous dephasing noise on each $|\tilde{0}_i\rangle_{ABC}$ is such that it is maintained in its type with probability (1–P), and becomes the linear combination of the other three types with the error probability P/3. (The same argument applies to $|\tilde{1}_i\rangle_{ABC}$). The noise does not remove the carrier from the $|\tilde{0}_i\rangle_{ABC}$ and $|\tilde{1}_i\rangle_{ABC}$ space, no matter how many times it is applied. Since the performance of the protocol is compatible with this space, the added noise does not remove the protocol from its defined function. To enter the next round, parties affect Hadamard operators, the carrier becomes a linear combination of $|GHZ_i\rangle_{ABC}$ and $|GHZ'_i\rangle_{ABC}$. Therefore, we should calculate the dephasing noise for $|GHZ_i\rangle_{ABC}$ and $|GHZ'_i\rangle_{ABC}$ in the same way described in section 5.1:

$$\begin{aligned}
&|GHZ_i\rangle\langle GHZ_i| \to\\
&(1-P)|GHZ_i\rangle\langle GHZ_i| + P|GHZ'_i\rangle\langle GHZ'_i|.\\
&|GHZ'_i\rangle\langle GHZ'_i| \to\\
&(1-P)|GHZ'_i\rangle\langle GHZ'_i| + P|GHZ_i\rangle\langle GHZ_i|.
\end{aligned} \tag{50}$$

Due to the continuous dephasing noise, $|GHZ_i\rangle_{ABC}$ states are preserved with probability (1–P), and turned into $|GHZ'_i\rangle_{ABC}$ states with the error probability P. (A Similar argument applies to $|GHZ'_i\rangle_{ABC}$ states). Since the noise does not remove the carrier from $|GHZ_i\rangle_{ABC}$ and $|GHZ'_i\rangle_{ABC}$ space, as many times as it acts, and since the protocol performance is compatible with this space, the added noise does not remove the protocol from its defined function.

6. 2. The effect of continuous depolarizing noise

The depolarizing channel effect is such that it preserves the original state with probability (1−P), and destroys all the information; turning it into a uniform and completely random state with the error probability P. To study the continuous effect of depolarizing noise, each time we want to apply the noise, we have to consider the linear combination of the carrier state and the maximally mixed state. (Because the carrier consists of three qubits, we should consider the maximally mixed state for three qubits: I/8). When the carrier is in $|GHZ_i\rangle_{ABC}$ and $|GHZ'_i\rangle_{ABC}$ space, we have to expand I as an equation (42). But when the carrier state is in $|\tilde{0}_i\rangle_{ABC}$ and $|\tilde{1}_i\rangle_{ABC}$ space, we must expand I according to equation (46). With this account, the noisy carrier remains in $|GHZ_i\rangle_{ABC}$ and $|GHZ'_i\rangle_{ABC}$ or $|\tilde{0}_i\rangle_{ABC}$ and $|\tilde{1}_i\rangle_{ABC}$ spaces. Since these spaces are compatible with the protocol performance, the continuous depolarizing noise does not remove the structure of the protocol.

7. Conclusions

This paper investigates the stability of the secret-sharing protocols with entangled carriers against the continuous dephasing and depolarizing noises. In this protocol, entangled states are shared as information carrier between the sender and receivers. It acts as a medium to which the sender uploads the message on one side, and the recipients download the message from which on the other side. The message is in a maximally mixed state during the transmission; It is hidden from the eavesdropper. We showed that despite the continuous noise, the carrier does not leave its space. Instead, it remains in two distinct spaces with the entangled basis that forms complete spaces for the carrier qubits. Since this protocol uses the entangled states as a medium of conveying the message, it seems that the strong correlations in entangled states, which are here the texture of the protocol, preserve it against noise.

Acknowledgment

We are grateful for the complementary and constructive comments of Dr. Vahid Karimipour.

References

1. C Bennett, *et all*., *Phys. Rev. Lett.* **70** (1993) 1895.
2. C Bennett and S Wiesner, *Phys. Rev. Lett.* **69**, 20 (1992) 2881.
3. R Raussendorf and H Briegel, *Phys. Rev. Lett*. **86**, 22 (2001) 5188.
4. A Broadbent, J Fitzsimons, and E Kashefi, *50th Annual IEEE Symposium on Foundations of Computer Science*, Atlanta GA USA (2009)
5. M Hillery, V Bužek, and A Berthiaume, *Phys. Rev.* A **59**, 3 (1999) 1829.
6. A Karlsson, M Koashi, and N Imoto, *Phys. Rev.* A **59**, 1 (1999) 162.
7. Li Xiao, *et all*., *Phys. Rev.* A **69**, 5 (2004) 052307.
8. Z Zhang and Z Man, *Phys. Rev*. A **72**, 2 (2005) 022303.
9. Y Wu, *et all*., *Phys. Rev*. A **93**, 2 (2016) 022325.
10. C Bennett and G Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York (1984)
11. A Ekert, *Phys. Rev. Lett.* **67** (1991) 661.
12. H Bechmann Pasquinucci, and N Gisin, *Phys. Rev.* A **59**, 6 (1999) 4238.
13. D Bruss and C Macchiavello, *Phys. Rev. Lett.* **88**, 12 (2002) 127901.
14. C Schmid, *et all*., *Phys. Rev. Lett.* **95**, 23 (2005) 230505.
15. Z Zhang, Y Li, and Z Man, *Phys. Rev.* A **71**, 4 (2005) 044301.
16. A Tavakoli, *et all*., *Phys. Rev.* A. **92**, 3 (2015) 030302.
17. V Karimipour and M Asoudeh, *Phys. Rev*. **92**, 3 (2015) 030301
18. Y Zhang, C Li, and G Guo, *Phys. Rev.* A **64**, 2 (2001) 024302.
19. S Bagherinezhad and V Karimipour, *Phys. Rev.* A **67**, 4 (2003) 044302.
20. Sh Emamipanah, M Asoudeh, and V Karimipour, *Quantum information processing* **19** (2020) 357.