Quantum Inf Process (2015) 14:4211–4224
DOI 10.1007/s11128-015-1103-0

Secret sharing of a known arbitrary quantum state with noisy environment

Ming-Ming Wang[1,2] · Wei Wang[1] · Jin-Guang Chen[1] · Ahmed Farouk[3]

Received: 5 June 2015 / Accepted: 20 August 2015 / Published online: 29 August 2015

Abstract We study quantum state sharing (QSTS) with noisy environment in this paper. As an example, we present a QSTS scheme of a known state whose information is hold by the dealer and then investigate the noisy influence process of the scheme. Taking the amplitude-damping noise and the phase-damping noise as typical noisy channels, we show that the secret state can be shared among agents with some information lost. Our research connects the areas of quantum state sharing and remote state preparation.

Keywords Quantum state sharing · Amplitude-damping noise · Phase-damping noise · Fidelity

1 Introduction

Entanglement is a special resource in quantum information processing, and one of the most astonishing applications is quantum teleportation [1]. Bennett et al. [1] demonstrated that an unknown quantum state can be teleported to a spatially separated place via Einstein–Podolsky–Rosen channels. If a quantum state is known to the sender, there is another way to transfer the quantum state without qubit transmission, which is known as remote state preparation (RSP) [2–4]. With shared quantum resource and additional classical information, RSP can be performed with simpler measurements

✉ Ming-Ming Wang
bluess1982@126.com

1 College of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China

2 Nanjing University of Information Science & Technology (NUIST), Nanjing 210044, China

3 Information Technology Department, Al-Zahra College for Women, Muscat, Oman

and less classical communication costs than quantum teleportation. Since its first appearance, different kinds of RSP schemes have been proposed, such as oblivious RSP [5], continuous variable RSP [6], RSP in higher dimension space [7]. In recent years, RSP schemes that include many participants have also been proposed, like joint RSP (JRSP) [8–10] and controlled RSP (CRSP) [11,12]. The difference between JRSP and CRSP is what the roles did the preparers played. In a JRSP scheme, each sender is a information carrier who holds partial information of a prepared state and all senders jointly prepare the state for a remote receiver. While in a CRSP scheme, there is a controller who does not know the information of the state, but the scheme will not be completed without the controller's consent.

Besides, quantum entanglement has also been used to extend the scope of cryptograph. Applications like quantum key distribution [13], quantum data hiding [14–17] and quantum authentication [18,19] have been proposed based on shared entanglement resource. Quantum secret sharing (QSS) [20] is another application of entanglement resource which enhances the secure level of classical secret sharing. The pioneering work of QSS was introduced by Hillery et al. [20] in 1999. After that, various QSS schemes have been proposed both theoretically [21–26] and experimentally [27–29]. According to the type of shared secret, QSS schemes can be divided into two classes, i.e., QSS of a classical secret and QSS of a quantum state. The latter one is also known as quantum state sharing (QSTS) named by Lance et al. in [30], where a secret state is shared among a set of agents, and only qualified agents groups can cooperate to reconstruct the state. QSTS has strong relationships with quantum teleportation and RSP. Many of the existing QSTS schemes can be regarded as quantum teleportation among multiparty who located at spatially separated places [20,24,31–34], where the secret state is unknown to the dealer. However, if the dealer already known the information of the secret state, the scheme can be performed in a simpler way. In 2014, we pointed out that the application of QSTS can also be achieved by using the idea of RSP [35].

Generally, most applications of entanglement were considered in an ideal condition; i.e., the entangled resources were perfectly generated and transmitted without any interaction with the outside environment. But in real world, a quantum system will unavoidably be affected by the environment. And these interactions are considered as noises. In recent years, some entanglement-based schemes with noisy environments have been studied. Adhikari et al. [36] proposed a QSS protocol of classical information with noisy channels. Xiang et al. [37] presented a RSP protocol for mixed state in depolarizing and dephasing channel. Chen et al. [38] investigated remote preparation of an entangled state through a mixed-state channel in nonideal conditions. Guan et al. [39] investigate the JRSP of an arbitrary two-qubit quantum state in noisy environments.

As is mentioned, we have shown that a QSTS scheme can be achieved by using the idea of RSP in Ref. [35], which is simpler and more efficient than by the idea of quantum teleportation. But like most of other QSTS schemes, our schemes were discussed with ideal environment and no outside noise was considered. One may ask how a QSTS scheme will be affected by the noise and how much information will be lost in the process? In this paper, we are going to discuss these problems. The organization of the paper is as follows. In Sect. 2, we present our multiparty QSTS scheme of an arbitrary known qubit state with ideal environment. Then, we investigate

our QSTS scheme with the amplitude-damping noise and the phase-damping noise in Sects. 3 and 4, respectively. We discuss their security issues and their relationships with quantum teleportation and RSP in Sect. 5. The paper is concluded in Sect. 6.

2 State sharing scheme with ideal environment

To begin with, we are going to present a multiparty state sharing scheme of an arbitrary qubit state, which is a specific instance of our schemes in Ref. [35]. Let us suppose that Alice wants to distribute a secret state between two agents Bob and Charlie in such a way that only if two agents work together can they recover the state. Generally, an arbitrary single-qubit state has the form

$$|\phi\rangle = a_0 e^{i\theta_0}|0\rangle + a_1 e^{i\theta_1}|1\rangle, \tag{1}$$

where $a_0, a_1 \in \mathcal{R}$, $\theta_0, \theta_1 \in [0, 2\pi]$, with $a_0^2 + a_1^2 = 1$. The parameters a_0, a_1, θ_0 and θ_1 of the secret state are known by Alice. She need not hold the state.

Our state sharing scheme of an arbitrary known qubit state in ideal environment can be described as follows.

(1) **Secret splitting phase**

(a) The dealer Alice prepares a GHZ state as shared quantum resource, which can be written as

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}, \tag{2}$$

where subscripts denote qubits of the state. Alice keeps qubit A in her laboratory. She sends qubit B to Bob and qubit C to Charlie through two ideal quantum channels, which means the outside environment will not affect qubits B and C. After qubits transmissions, Alice holds qubit A, Bob holds qubit B, and Charlie holds qubit C.

(b) Alice prepares an ancilla state R in $|0\rangle$, and then, she performs a unitary operation U on qubits AR where

$$U = \begin{pmatrix} U_0 & 0 \\ 0 & U_1 \end{pmatrix}, \quad \text{with } U_i = \begin{pmatrix} a_i & \sqrt{1-a_i^2} \\ \sqrt{1-a_i^2} & -a_i \end{pmatrix}; \quad i = 0, 1. \tag{3}$$

Then, the quantum system becomes

$$\begin{aligned} & U_{AR} \otimes I_{BC}|\Phi\rangle_{ABC}|0\rangle_R \\ &= \frac{1}{\sqrt{2}}(a_0|000\rangle_{ABC} + a_1|111\rangle_{ABC})|0\rangle_R \\ &\quad + \frac{1}{\sqrt{2}}\left(\sqrt{1-a_0^2}|000\rangle_{ABC} + \sqrt{1-a_1^2}|111\rangle_{ABC}\right)|1\rangle_R. \end{aligned} \tag{4}$$

(c) Alice measures qubit R in the computational basis. If she gets the result $|0\rangle$, the quantum system becomes

$$a_0|000\rangle_{ABC} + a_1|111\rangle_{ABC}. \tag{5}$$

While if Alice gets the result $|1\rangle$, she can use the recursive method proposed by Jiang et al. [40,41] to get the above state.

(d) Alice performs a projective measurement on qubit A under the basis $\{|\Lambda_k\rangle; k \in \{0, 1\}\}$ where

$$|\Lambda_0\rangle = \frac{1}{\sqrt{2}}\left(e^{-\mathrm{i}\theta_0}|0\rangle + e^{-\mathrm{i}\theta_1}|1\rangle\right), \tag{6}$$

$$|\Lambda_1\rangle = \frac{1}{\sqrt{2}}\left(e^{-\mathrm{i}\theta_0}|0\rangle - e^{-\mathrm{i}\theta_1}|1\rangle\right). \tag{7}$$

Then, the quantum system can be rewritten as

$$\begin{aligned} &a_0|000\rangle_{ABC} + a_1|111\rangle_{ABC} \\ &= \frac{1}{\sqrt{2}}\Big[|\Lambda_0\rangle_A\left(a_0e^{\mathrm{i}\theta_0}|00\rangle + a_1e^{\mathrm{i}\theta_1}|11\rangle\right)_{BC} \\ &\quad + |\Lambda_1\rangle_A\left(a_0e^{\mathrm{i}\theta_0}|00\rangle - a_1e^{\mathrm{i}\theta_1}|11\rangle\right)_{BC}\Big]. \end{aligned} \tag{8}$$

(e) After the measurement of qubit A, the secret state is distributed between two agents. Here, Alice announces her measurement result $|\Lambda_k\rangle$ as k publicly.

(2) **Secret recovery phase**

(a) In the secret recovery phase, either Bob or Charlie can recover the shared secret state with the help of the other. As an example, suppose that Bob wants to help Charlie to recover the state. Here, Bob performs a single-qubit measurement on qubit B under the basis $\{\left|\hat{0}\right\rangle, \left|\hat{1}\right\rangle\}$ where $\left|\hat{0}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\left|\hat{1}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then, the resource shared among two agents becomes

$$\begin{aligned} &a_0e^{\mathrm{i}\theta_0}|00\rangle_{BC} + (-1)^k a_1e^{\mathrm{i}\theta_1}|11\rangle_{BC} \\ &= \frac{1}{\sqrt{2}}\sum_{k_1=0}^{1}|\hat{k_1}\rangle_B\left(a_0e^{\mathrm{i}\theta_0}|0\rangle + (-1)^{k+k_1}a_1e^{\mathrm{i}\theta_1}|1\rangle\right)_C. \end{aligned} \tag{9}$$

(b) For recovering the secret state, Bob sends his measurement result $|\hat{k}_1\rangle$ as k_1 to Charlie. After receiving k_1, Charlie can recover the secret state $|\phi\rangle$ by performing the unitary operation $\sigma_z^{k+k_1}$ on qubit C. Noted that Bob can also recover the secret state if Charlie agrees to help him, and each agent has the same power for recovering the secret state in the scheme, which means our scheme is symmetric.

3 State sharing scheme with amplitude-damping noisy environment

In the following, we are going to show our scheme with two specific noisy environments. And we start with the amplitude-damping noisy environment.

3.1 The amplitude-damping noise

The amplitude-damping noise is one of the most important decoherence noise which describes the energy-dissipation effects due to loss of energy from a quantum system. The action of amplitude-damping noise can be presented by a set of Kraus operators as follows [42]

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{\lambda} \\ 0 & 0 \end{pmatrix}, \tag{10}$$

where $0 \leq \lambda \leq 1$ indicates the decoherence rate of the amplitude-damping noisy environment. When a quantum state passes through the noisy channel, there is a probability λ that the state will be affected.

3.2 The scheme with amplitude-damping noise

(1) **Secret splitting phase**

(a) Still, Alice prepares the GHZ state $|\Phi\rangle$ as shared quantum resource. The state can be represented in the form of density matrix as

$$\rho_{ABC} = |\Phi\rangle\langle\Phi|. \tag{11}$$

Alice keeps qubit A and sends qubits B and C to Bob and Charlie through two identical amplitude-damping noisy channels, respectively. The effect of noisy environment can be described by operator sum representation. This process will convert the pure channel state into a mixed one. After qubits transmissions through amplitude-damping noisy channels, the quantum resource used for state sharing becomes

$$\begin{aligned} \epsilon(\rho) &= \sum_{i,j=0,1} E_i^B E_j^C \rho (E_i^B)^\dagger (E_j^C)^\dagger \\ &= \frac{1}{2}\Big[(|000\rangle + (1-\lambda)|111\rangle)(\langle 000| + (1-\lambda)\langle 111|) \\ &\quad + (1-\lambda)\lambda|110\rangle\langle 110| + (1-\lambda)\lambda|101\rangle\langle 101| + \lambda^2|100\rangle\langle 100|\Big], \end{aligned} \tag{12}$$

where superscripts B and C indicate that noise operators act on qubits B and C, respectively. And "$\dagger$" means the conjugate transpose of a matrix.

(b) Alice prepares an ancilla state R in $|0\rangle$, and she performs a unitary operation U on particles AR. Then, the quantum system becomes

$$\rho_1 = U_{AR} \otimes I_{BC} \{\epsilon(\rho)_{ABC} \otimes |0\rangle\langle 0|_R\} U_{AR}^\dagger \otimes I_{BC}, \tag{13}$$

where each subscript indicates a qubit.

(c) Alice measures qubit R in the computational basis. If she gets the result $|0\rangle$, the quantum system becomes

$$\begin{aligned}\rho_2 &= tr_R\left(\frac{M_0\rho_1 M_0^{\dagger}}{tr(M_0 M_0^{\dagger}\rho_1)}\right)\\ &= (a_0|000\rangle + a_1(1-\lambda)|111\rangle)(a_0\langle 000| + a_1(1-\lambda)\langle 111|)\\ &\quad + a_1^2(1-\lambda)\lambda|110\rangle\langle 110| + a_1^2(1-\lambda)\lambda|101\rangle\langle 101| + a_1^2\lambda^2|100\rangle\langle 100|.\end{aligned} \tag{14}$$

where $M_0 = |0\rangle\langle 0|$ is the measurement operator. While if Alice gets the result $|1\rangle$, she needs to use the recursive procedure.

(d) Alice performs a projective measurement on qubit A under the basis $\{|\Lambda_k\rangle; k \in \{0, 1\}\}$. Suppose the measurement result is $|\Lambda_k\rangle$, the quantum system will be rewritten as

$$\begin{aligned}\rho_3 &= \frac{M_{\Lambda_k}\rho_2 M_{\Lambda_k}^{\dagger}}{tr(M_{\Lambda_k} M_{\Lambda_k}^{\dagger}\rho_2)}\\ &= \frac{1}{2}\Big[\Big(a_0|000\rangle + (-1)^k a_1(1-\lambda)e^{-\mathrm{i}\theta_0}e^{\mathrm{i}\theta_1}|011\rangle + (-1)^k a_0 e^{\mathrm{i}\theta_0}e^{-\mathrm{i}\theta_1}|100\rangle\\ &\quad + a_1(1-\lambda)|111\rangle) \times \Big(a_0\langle 000| + (-1)^k a_1(1-\lambda)e^{\mathrm{i}\theta_0}e^{-\mathrm{i}\theta_1}\langle 011|\\ &\quad + (-1)^k a_0 e^{-\mathrm{i}\theta_0}e^{\mathrm{i}\theta_1}\langle 100| + a_1(1-\lambda)\langle 111|\Big)\\ &\quad + a_1^2(1-\lambda)\lambda((-1)^k e^{-\mathrm{i}\theta_0}e^{\mathrm{i}\theta_1}|010\rangle + |110\rangle)((-1)^k e^{\mathrm{i}\theta_0}e^{-\mathrm{i}\theta_1}\langle 010|\\ &\quad + \langle 110|) + a_1^2(1-\lambda)\lambda((-1)^k e^{-\mathrm{i}\theta_0}e^{\mathrm{i}\theta_1}|001\rangle + |101\rangle)((-1)^k e^{\mathrm{i}\theta_0}e^{-\mathrm{i}\theta_1}\\ &\quad \langle 001| + \langle 101|) + a_1^2\lambda^2((-1)^k e^{-\mathrm{i}\theta_0}e^{\mathrm{i}\theta_1}|000\rangle\\ &\quad + |100\rangle)((-1)^k e^{\mathrm{i}\theta_0}e^{-\mathrm{i}\theta_1}\langle 000| + \langle 100|)\Big],\end{aligned} \tag{15}$$

where $M_{\Lambda_k} = |\Lambda_k\rangle\langle\Lambda_k|$ with $k \in \{0, 1\}$ is the measurement operator, which means the quantum system of Bob and Charlie becomes

$$\begin{aligned}\rho_4 &= tr_A(\rho_3)\\ &= a_0^2|00\rangle\langle 00| + (-1)^k a_0 e^{\mathrm{i}\theta_0}a_1 e^{-\mathrm{i}\theta_1}(1-\lambda)|00\rangle\langle 11|\\ &\quad + (-1)^k a_0 e^{-\mathrm{i}\theta_0}a_1 e^{\mathrm{i}\theta_1}(1-\lambda)|11\rangle\langle 00| + a_1^2(1-\lambda)^2|11\rangle\langle 11|\\ &\quad + a_1^2(1-\lambda)\lambda|01\rangle\langle 01| + a_1^2(1-\lambda)\lambda|10\rangle\langle 10| + a_1^2\lambda^2|00\rangle\langle 00|.\end{aligned} \tag{16}$$

(2) **Secret recovery phase**

(a) In the beginning of this phase, Bob and Charlie's quantum system is ρ_4. Suppose that Bob agrees to help Charlie to recover the secret state. Here, Bob performs a single-qubit measurement under the basis $\{|\hat{0}\rangle, |\hat{1}\rangle\}$. Bob's measurement result $|\hat{k_1}\rangle$ is represented as a cbit k_1. Then, the state shared by Charlie becomes

$$\begin{aligned}\rho_C &= tr_B\left(\frac{M_{B_{k_1}}\rho_4 M_{B_{k_1}}^{\dagger}}{tr(M_{B_{k_1}}M_{B_{k_1}}^{\dagger}\rho_4)}\right)\\ &= (a_0^2+a_1^2\lambda)|0\rangle\langle 0|+a_1^2(1-\lambda)|1\rangle\langle 1|+(-1)^{k+k_1}a_0e^{\mathrm{i}\theta_0}a_1e^{-\mathrm{i}\theta_1}(1-\lambda)|0\rangle\langle 1|\\ &\quad+(-1)^{k+k_1}a_0e^{-\mathrm{i}\theta_0}a_1e^{\mathrm{i}\theta_1}(1-\lambda)|1\rangle\langle 0|,\end{aligned} \tag{17}$$

where $M_{B_{k_1}} = |\hat{k_1}\rangle\langle\hat{k_1}|$ with $k_1 \in \{0, 1\}$ is Bob's measurement operator.

(b) Bob sends his measurement result k_1 to Charlie. Then, Charlie recover the secret state by performing $\sigma_z^{k+k_1}$ on qubit C. The recovery state has the form

$$\begin{aligned}\rho_{out} &= \sigma_z^{k+k_1}\rho_C(\sigma_z^{k+k_1})^{\dagger}\\ &= (a_0^2+a_1^2\lambda)|0\rangle\langle 0|+a_1^2(1-\lambda)|1\rangle\langle 1|+a_0e^{\mathrm{i}\theta_0}a_1e^{-\mathrm{i}\theta_1}(1-\lambda)|0\rangle\langle 1|\\ &\quad+a_0e^{-\mathrm{i}\theta_0}a_1e^{\mathrm{i}\theta_1}(1-\lambda)|1\rangle\langle 0|.\end{aligned} \tag{18}$$

3.3 Fidelity

Since the shared quantum resource has been affected by the noisy environment and become a mixed state in the secret splitting phase. The recovered state ρ_{out} will not be the same as $|\phi\rangle$. Generally, the difference between the two states can be measured by the fidelity as follows

$$\begin{aligned}F_{\mathrm{AD}} &= \langle\phi|\rho_{out}|\phi\rangle\\ &= a_0^4+a_0^2a_1^2(2-\lambda)+a_1^4(1-\lambda).\end{aligned} \tag{19}$$

As is shown in the above, the fidelity F_{AD} for the amplitude-damping noise depends on the amplitude factors of the prepared state a_0, a_1 and the decoherence rate λ, but has nothing to do with the phase parameters θ_0 and θ_1. When $F_{\mathrm{AD}} = 1$, it is means that $\rho_{out} = |\phi\rangle\langle\phi|$; i.e., the noise has no effect on the output shared state, and there is no information lost (in ideal condition that $\lambda = 0$ or sharing a specific state $e^{i\theta_0}|0\rangle$ where $a_0 = 1$). While if $F_{\mathrm{AD}} < 1$, it means that $\rho_{out} \neq |\phi\rangle\langle\phi|$; i.e., some information has been lost since the affection of noise. The relationship among F_{AD}, λ and a_0 is shown in Fig. 1 (noted that $a_1^2 = 1 - a_0^2$).

4 State sharing scheme with phase-damping noisy environment

4.1 The phase-damping noise

The phase-damping noise is another important decoherence noise which describes the loss of quantum information without energy dissipation. The Kraus operators of a phase-damping noisy channel are [42]

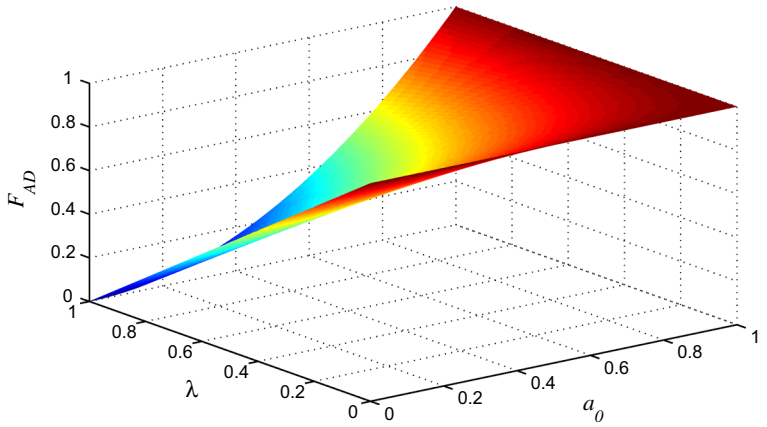

Fig. 1 Relationship among F_{AD}, λ and a_0

$$E_0 = \sqrt{1-\eta}I, \quad E_1 = \sqrt{\eta}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \sqrt{\eta}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{20}$$

where $0 \leq \eta \leq 1$ is the error probability of the phase-damping noisy environment.

4.2 The scheme with phase-damping noise

(1) **Secret splitting phase**

(a) Alice prepares the GHZ state $\rho = |\Phi\rangle\langle\Phi|$. She keeps particle A and sends particle B to Bob and particle C to Charlie through two phase-damping noisy channels. After interactions with the noises, the quantum system becomes

$$\begin{aligned}\epsilon(\rho) &= \sum_{i,j=0}^{2} E_i^B E_j^C \rho (E_i^B)^\dagger (E_j^C)^\dagger \\ &= \frac{1}{2}\Big[|000\rangle\langle 000| + |111\rangle\langle 111| + (1-\eta)^2(|000\rangle\langle 111| + |111\rangle\langle 000|)\Big].\end{aligned} \tag{21}$$

(b) Alice prepares an ancilla state R in $|0\rangle$, and then, she performs a unitary operation U on particles AR. The quantum system becomes

$$\rho_1 = U_{AR} \otimes I_{BC} \left\{\epsilon(\rho)_{ABC} \otimes |0\rangle\langle 0|_R\right\} U_{AR}^\dagger \otimes I_{BC}. \tag{22}$$

(c) Alice measures qubit R in the computational basis. If she gets the result $|0\rangle$, the quantum system becomes

$$\begin{aligned}\rho_2 = tr_R\left(\frac{M_0\rho_1 M_0^\dagger}{tr(M_0 M_0^\dagger \rho_1)}\right) = \frac{1}{2}\Big[a_0^2|000\rangle\langle 000| \\ + a_1^2|111\rangle\langle 111| + a_0 a_1(1-\eta)^2(|000\rangle\langle 111| + |111\rangle\langle 000|)\Big].\end{aligned} \tag{23}$$

While if Alice gets the result $|1\rangle$, she performs the recursive procedure.

(d) Alice measures qubit A under the basis $\{|\Lambda_k\rangle; k \in \{0, 1\}\}$. Suppose the measurement result is $|\Lambda_k\rangle$, the quantum system can be rewritten as

$$\begin{aligned}\rho_3 &= \frac{M_{\Lambda_k}\rho_2 M_{\Lambda_k}^{\dagger}}{tr(M_{\Lambda_k}M_{\Lambda_k}^{\dagger}\rho_2)} \\ &= \frac{1}{2}\Big[a_0^2\left(|000\rangle + (-1)^k e^{i\theta_0}e^{-i\theta_1}|100\rangle\right)\left(\langle 000| + (-1)^k e^{-i\theta_0}e^{i\theta_1}\langle 100|\right) \\ &\quad + a_1^2\left((-1)^k e^{-i\theta_0}e^{i\theta_1}|011\rangle + |111\rangle\right)\left((-1)^k e^{i\theta_0}e^{-i\theta_1}\langle 011| + \langle 111|\right) \\ &\quad + a_0a_1(1-\eta)^2\left(|000\rangle + (-1)^k e^{i\theta_0}e^{-i\theta_1}|100\rangle\right) \\ &\quad \times \left((-1)^k e^{i\theta_0}e^{-i\theta_1}\langle 011| + \langle 111|\right) \\ &\quad + a_0a_1(1-\eta)^2\left((-1)^k e^{-i\theta_0}e^{i\theta_1}|011\rangle + |111\rangle\right) \\ &\quad \times \left(\langle 000| + (-1)^k e^{-i\theta_0}e^{i\theta_1}\langle 100|\right)\Big].\end{aligned} \tag{24}$$

And Bob and Charlie's quantum system becomes

$$\begin{aligned}\rho_4 &= tr_A(\rho_3) \\ &= a_0^2|00\rangle\langle 00| + a_1^2|11\rangle\langle 11| + (-1)^k a_0 e^{i\theta_0}a_1 e^{-i\theta_1}(1-\eta)^2|00\rangle\langle 11| \\ &\quad + (-1)^k a_0 e^{-i\theta_0}a_1 e^{i\theta_1}(1-\eta)^2|11\rangle\langle 00|.\end{aligned} \tag{25}$$

(2) **Secret recovery phase**

(a) Here, Bob performs a single-qubit measurement under the basis $\{\left|\hat{0}\right\rangle, \left|\hat{1}\right\rangle\}$. Bob's measurement result $|\hat{k_1}\rangle$ is represented as a cbit k_1. Then, the resource hold by Charlie becomes

$$\begin{aligned}\rho_C &= tr_B\left(\frac{M_{B_{k_1}}\rho_4 M_{B_{k_1}}^{\dagger}}{tr(M_{B_{k_1}}M_{B_{k_1}}^{\dagger}\rho_4)}\right) \\ &= a_0^2|0\rangle\langle 0| + a_1^2|1\rangle\langle 1| + (-1)^{k+k_1}a_0 e^{i\theta_0}a_1 e^{-i\theta_1}(1-\eta)^2|0\rangle\langle 1| \\ &\quad + (-1)^{k+k_1}a_0 e^{-i\theta_0}a_1 e^{i\theta_1}(1-\eta)^2|1\rangle\langle 0|.\end{aligned} \tag{26}$$

(b) Bob sends k_1 to Charlie. After receiving k_1, Charlie performs $\sigma_z^{k+k_1}$ on qubit C. Then, the secret state in Charlie's side has the form

$$\begin{aligned}\rho_{out} &= \sigma_z^{k+k_1}\rho_C(\sigma_z^{k+k_1})^{\dagger} \\ &= a_0^2|0\rangle\langle 0| + a_1^2|1\rangle\langle 1| + a_0 e^{i\theta_0}a_1 e^{-i\theta_1}(1-\eta)^2|0\rangle\langle 1| \\ &\quad + a_0 e^{-i\theta_0}a_1 e^{i\theta_1}(1-\eta)^2|1\rangle\langle 0|.\end{aligned} \tag{27}$$

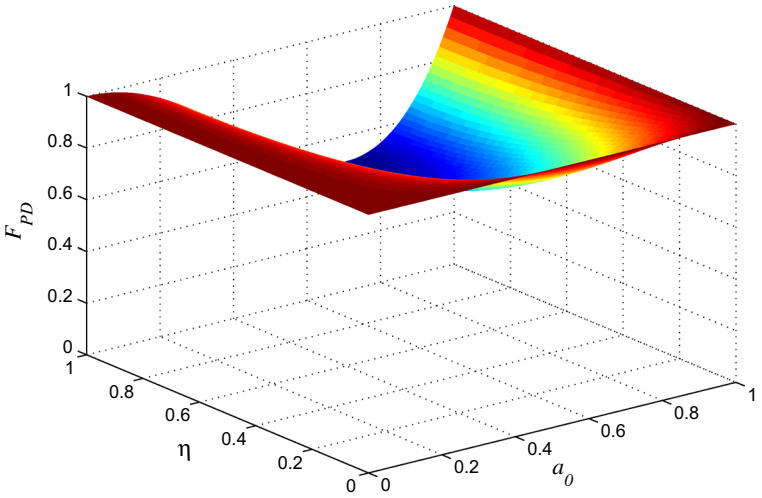

Fig. 2 Relationship among F_{PD}, η and a_0

4.3 Fidelity

The fidelity of the output state can be calculated as

$$\begin{aligned} F_{PD} &= \langle\phi|\rho_{out}|\phi\rangle \\ &= a_0^4 + a_1^4 + 2(1-\eta)^2 a_0^2 a_1^2. \end{aligned} \tag{28}$$

As is shown in the above, the fidelity F_{PD} for phase-damping noise depends on the amplitude factors a_0, a_1 and the decoherence rate η, but has nothing to do with the phase parameters. The relationship among F_{PD}, λ and a_0 is shown in Fig. 2. As is shown, the Fidelity is 1 when $\eta = 0$ (no noise) or $a_0 = 1, 0$ (sharing a specific state $e^{i\theta_0}|0\rangle$ or $e^{i\theta_1}|1\rangle$). The minimum fidelity is $F_{PD} = \frac{1}{2}$ when $\eta = 1$ and $a_0 = \frac{1}{\sqrt{2}}$.

5 Discussions

5.1 Security

There are two kinds of threats in a QSS scheme. The first is that some dishonest agents may try to obtain the secret state without the cooperation of others from a qualified agents group, which is also called "participant attack." The second is that an outside eavesdropper Eve may attempt to find the secret without being detected. Participant attack, firstly proposed by Gao et al [43], emphasizes that the attacks from dishonest users are generally more powerful since they can obtain more information than the eavesdropper Eve. This attack has attracted much attention in the cryptanalysis of quantum cryptography [44–46]. Qin and Gao [47] have pointed out that a QSS scheme is secure against the outside Eve if it is secure against inside dishonest agents, which

means we only need to pay our attention to participant attack when studying the security of a QSS scheme.

A key security issue of our QSTS schemes is that the message carrier GHZ states have to be securely distributed among the dealer Alice and all the agents. The ways for sharing a sequence of GHZ states securely among remote players have been discussed in Refs. [20,21,26,47,48]. Alice can prepare the GHZ states and then use these methods to securely share the GHZ states with all the agents in the first step of the secret splitting phase. But noted that the error rate caused by the noise have to be lower than the detection probability, so that a malicious attack can be distinguished from noise. In other words, honest participants will not find the attack if the noise rate is too large since they cannot distinguish the attack from the noise; i.e., the attack is covered by the noise.

There is no qubit transmission in the recovery phase of our scheme. One may worry about that some dishonest agents may try to recover the secret state privately before the recovery phase. As is shown in Eq. (9), the system of Bob and Charlie has the form

$$a_0 e^{\mathrm{i}\theta_0}|00\rangle_{BC} + (-1)^k a_1 e^{\mathrm{i}\theta_1}|11\rangle_{BC}, \tag{29}$$

which means the partial trace of Bob has the form

$$tr_C(a_0 e^{\mathrm{i}\theta_0}|00\rangle + (-1)^k a_1 e^{\mathrm{i}\theta_1}|11\ldots1\rangle) = a_0^2|0\rangle\langle 0|_B + a_1^2|1\rangle\langle 1|_B, \tag{30}$$

while the partial trace of Charlie has the same form. From the above equation, we conclude that any unqualified agents group cannot recover the secret state by any general operations on their sides. Though they have the amplitude information, it is not sufficient since the phase information is not available. All in all, this QSTS scheme can be made to be secured.

5.2 State sharing of a known state

By a "known" quantum state, we mean that the information of the state is already known to the dealer. But noted that the secret information of the state is unknown to all the agents in the beginning of the schemes, which means our schemes meet the definition of the secret sharing. Each agent will get a share of the secret in the distribution phase, and authorized agents can cooperatively recover the secret state in the recovery phase. QSTS of a known qubit is similar to the QSS of classical bits. As is shown in Eq. (1), a general qubit $|\phi\rangle$ state has four parameters a_0, a_1, θ_0 and θ_1. The task of QSTS of $|\phi\rangle$ is to share these four parameters. Usually, a QSS of classical bits usually shares a real number secret, while our proposed protocols can share four real numbers each time, which means our quantum protocols have more information capacity.

It is interesting to discuss the relationships among QSTS, RSP and quantum teleportation. Firstly, QSTS is usually defined as sharing an unknown quantum state as a secret among a group of agents, which is similar to multiparty or controlled teleportation [49–51]. Secondly, RSP can be performed with simpler quantum operations and

less classical communication costs than teleportation. Our QSTS schemes are similar to multiparty RSP (MRSP), and they have the same advantages as RSP to teleportation. Thirdly, there are two types of MRSP, which are JRSP [8–10,52–54] and CRSP [11,12,55], and they have close relationships with our QSTS schemes. For one thing, JRSP is similar to the recovery phase of QSTS, where the secret share is already distributed in each of the agents and they can cooperate to reconstruct the secret state. For the other thing, CRSP can be regarded as a specific type of QSTS, i.e., secret sharing of a known state of the dealer. In secret splitting phase, all agents perform measurement or unitary operation on their side to get the classical share. While in recovery phase, authorized agents cooperate to recover the secret state.

6 Conclusions

In summary, we have studied a multiparty QSTS scheme of an arbitrary known qubit with two noisy environments. Starting with the scheme in an ideal condition, we investigated the QSTS scheme with the amplitude-damping noise and the phase-damping noise, respectively. The detailed process of each QSTS is presented. As is shown in our schemes, some information is lost through the noise channels. We use fidelity to describe how close is the final state to the original state, and how much information has been lost in the process. Our study indicates that the fidelity in both two schemes depends on the amplitude factor of the initial state and the decoherence rate, but is independent of the phase parameter.

Our QSTS scheme is symmetric since any agent is able to recover the state with the help of others. Different from a traditional QSTS scheme that shares an unknown quantum state among agents, our results showed that if a quantum state is already known to the dealer, it can be shared among agents in a simpler way by using the idea of RSP. We pointed out that the researches of quantum state sharing and remote state preparation have strong connection with each other.

In this paper, we have presented the impact of noise for the process of a QSTS scheme. To show our method, we consider the case that three participants share a qubit state. For multiparticipants that share a multiqubit or a multiqudit state, this method can also be used. But the calculation seems too tedious to present here. Besides the amplitude-damping noise and the phase-damping noise, it is also possible to consider other noises like depolarizing, bit-flip and bit-phase flip as noisy channels.

Acknowledgments The project is supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2014JQ2-6030), the Scientific Research Program Funded by Shaanxi Provincial Education Department (Program No. 15JK1316), the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), the Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology (CICAEET), the National Natural Science Foundation of China (61201118), and the PhD Start-up Foundation of Xi'an Polytechnic University (No. BS1331).

References

1. Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895–1899 (1993)

2. Lo, H.K.: Classical-communication cost in distributed quantum-information processing: a generalization of quantum-communication complexity. Phys. Rev. A **62**(1), 012313 (2000)
3. Pati, A.K.: Minimum classical bit for remote preparation and measurement of a qubit. Phys. Rev. A **63**(1), 14302–14304 (2000)
4. Bennett, C.H., DiVincenzo, D.P., Shor, P.W., Smolin, J.A., Terhal, B.M., Wootters, W.K.: Remote state preparation. Phys. Rev. Lett. **87**(7), 077902 (2001)
5. Leung, D.W., Shor, P.W.: Oblivious remote state preparation. Phys. Rev. Lett. **90**(12), 127905 (2003)
6. Kurucz, Z., Adam, P., Kis, Z., Janszky, J.: Continuous variable remote state preparation. Phys. Rev. A **72**(5), 052315 (2005)
7. Zeng, B., Zhang, P.: Remote-state preparation in higher dimension and the parallelizable manifold S^{n-1}. Phys. Rev. A **65**(2), 022316 (2002)
8. Xia, Y., Song, J., Song, H.S.: Multiparty remote state preparation. J. Phys. B: At. Mol. Opt. Phys. **40**(18), 3719–3724 (2007)
9. Nguyen, B.A., Kim, J.: Joint remote state preparation. J. Phys. B: At. Mol. Opt. Phys. **41**(9), 095501 (2008)
10. Wang, M.M., Chen, X.B., Yang, Y.X.: Deterministic joint remote preparation of an arbitrary two-qubit state using the cluster state. Commun. Theor. Phys. **59**(5), 568–572 (2013)
11. Luo, M.X., Chen, X.B., Ma, S.Y., Yang, Y.X., Hu, Z.M.: Remote preparation of an arbitrary two-qubit state with three-party. Int. J. Theor. Phys. **49**(6), 1262 (2010)
12. Wang, Z.Y.: Controlled remote preparation of a two-qubit state via an asymmetric quantum channel. Commun. Theor. Phys. **55**(2), 244 (2011)
13. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
14. Terhal, B.M., DiVincenzo, D.P., Leung, D.W.: Hiding bits in Bell states. Phys. Rev. Lett. **86**(25), 5807 (2001)
15. Qu, Z.G., Chen, X.B., Zhou, X.J., Niu, X.X., Yang, Y.X.: Novel quantum steganography with large payload. Opt. Commun. **283**(23), 4782–4786 (2010)
16. Xia, Z., Wang, X., Sun, X., Wang, B.: Steganalysis of least significant bit matching using multi-order differences. Secur. Commun. Netw. **7**(8), 1283–1291 (2014)
17. Xia, Z., Wang, X., Sun, X., Liu, Q., Xiong, N.: Steganalysis of LSB matching using differences between nonadjacent pixels. Multimed. Tools Appl. pp. 1-16 (2014). doi:10.1007/s11042-014-2381-8
18. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Phys. Rev. A **64**(6), 062309 (2001)
19. Guo, P., Wang, J., Li, B., Lee, S.: A variable threshold-value authentication architecture for wireless mesh networks. J. Internet Technol. **15**(6), 929–936 (2014)
20. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)
21. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**(1), 162–168 (1999)
22. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**(3), 648–651 (1999)
23. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A **61**(4), 042311 (2000)
24. Bandyopadhyay, S.: Teleportation and secret sharing with pure entangled states. Phys. Rev. A **62**(1), 012308 (2000)
25. Karimipour, V., Bahraminasab, A., Bagherinezhad, S.: Entanglement swapping of generalized cat states and secret sharing. Phys. Rev. A **65**(4), 042320 (2002)
26. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**(5), 052307 (2004)
27. Tittel, W., Zbinden, H., Gisin, N.: Experimental demonstration of quantum secret sharing. Phys. Rev. A **63**(4), 042301 (2001)
28. Bogdanski, J., Rafiei, N., Bourennane, M.: Experimental quantum secret sharing using telecommunication fiber. Phys. Rev. A **78**(6), 062307 (2008)
29. Schmid, C., Trojek, P., Bourennane, M., Kurtsiefer, C., Zukowski, M., Weinfurter, H.: Experimental single qubit quantum secret sharing. Phys. Rev. Lett. **95**(23), 230505 (2005)
30. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Tripartite quantum state sharing. Phys. Rev. Lett. **92**(17), 177903 (2004)
31. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein–Podolsky–Rosen pairs. Phys. Rev. A **72**(4), 044301 (2005)

32. Li, X.H., Zhou, P.: Efficient symmetric multiparty quantum state sharing of an arbitrary m -qubit state. J. Phys. B: At. Mol. Opt. Phys. **39**(8), 1975 (2006)
33. Muralidharan, S., Panigrahi, P.K.: Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. Phys. Rev. A **77**(3), 032321 (2008)
34. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Multi-party quantum state sharing of an arbitrary two-qubit state with Bell states. Quantum Inf. Process. **10**(2), 231–239 (2011)
35. Wang, M.M., Chen, X.B., Chen, J.G., Yang, Y.X.: Quantum state sharing of arbitrary known multi-qubit and multi-qudit states. Int. J. Quantum Inf. **12**(03), 1450014 (2014)
36. Adhikari, S., Chakrabarty, I., Agrawal, P.: Probabilistic secret sharing through noisy quantum channel. Quantum Inf. Comput. **12**(3–4), 253–261 (2012)
37. Xiang, G.Y., Li, J., Yu, B., Guo, G.C.: Remote preparation of mixed states via noisy entanglement. Phys. Rev. A **72**(1), 012315 (2005)
38. Ai-Xi, C., Li, D., Jia-Hua, L., Zhi-Ming, Z.: Remote preparation of an entangled state in nonideal conditions. Commun. Theor. Phys. **46**(2), 221 (2006)
39. Guan, X.W., Chen, X.B., Wang, L.C., Yang, Y.X.: Joint remote preparation of an arbitrary two-qubit state in noisy environments. Int. J. Theor. Phys. **53**(7), 2236–2245 (2014)
40. Jiang, M., Zhou, L.L., Chen, X.P., You, S.H.: Deterministic joint remote preparation of general multi-qubit states. Opt. Commun. **301–302**, 39–45 (2013)
41. Jiang, M., Jiang, F.: Deterministic joint remote preparation of arbitrary multi-qudit states. Phys. Lett. A **377**(38), 2524–2530 (2013)
42. Xian-Ting, L.: Classical information capacities of some single qubit quantum noisy channels. Commun. Theor. Phys. **39**(5), 537 (2003)
43. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the brádler–dušek protocol. Quantum Inf. Comput. **7**(4), 329 (2007)
44. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "Experimental demonstration of a quantum protocol for byzantine agreement and liar detection". Phys. Rev. Lett. **101**(20), 208901 (2008)
45. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys. Lett. A **2**(357), 101–103 (2006)
46. Wang, M.M., Chen, X.B., Yang, Y.X.: Comment on "High-dimensional deterministic multiparty quantum secret sharing without unitary operations". Quantum Inf. Process. **12**(2), 785–792 (2013)
47. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery–Buzcaronek–Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**(6), 062324 (2007)
48. Yu, I.C., Lin, F.L., Huang, C.Y.: Quantum secret sharing with multilevel mutually (un)biased bases. Phys. Rev. A **78**, 12344–12348 (2008)
49. Ishizaka, S., Hiroshima, T.: Quantum teleportation scheme by selecting one of multiple output ports. Phys. Rev. A **79**(4), 42306–42318 (2009)
50. Man, Z.X., Xia, Y.J., An, N.B.: Economical and feasible controlled teleportation of an arbitrary unknown N-qubit entangled state. J. Phys. B: At. Mol. Opt. Phys. **40**(10), 1767–1774 (2007)
51. Zhang, Z.J.: Controlled teleportation of an arbitrary n-qubit quantum information using quantum secret sharing of classical message. Phys. Lett. A **352**(1–2), 55–58 (2006)
52. Hou, K., Wang, J., Lu, Y.L., Shi, S.H.: Joint Remote Preparation of a Multipartite GHZ-class State. Int. J. Theor. Phys. **48**(7), 2005–2015 (2009)
53. Zhan, Y.B.: Joint remote preparation of a four-dimensional quantum state (2010). arXiv:1006.4204v1
54. Luo, M.X., Chen, X.B., Ma, S.Y., Niu, X.X., Yang, Y.X.: Joint remote preparation of an arbitrary three-qubit state. Opt. Commun. **283**(23), 4796–4801 (2010)
55. Chen, X.B., Ma, S.Y., Su, Y., Zhang, R., Yang, Y.X.: Controlled remote state preparation of arbitrary two and three qubit states via the Brown state. Quantum Inf. Process. **11**(6), 1653–1667 (2012)