Hierarchical and probabilistic quantum state sharing via a non-maximally entangled $|\chi\rangle$ state*

Peng Jia-Yin(彭家寅)[a)b)†], Bai Ming-Qiang(柏明强)[a)], and Mo Zhi-Wen(莫智文)[a)]

[a)] College of Mathematics and Software Science, Sichuan Normal University, Chengdu 610066, China
[b)] School of Mathematics and Information Science, Neijiang Normal University, Neijiang 641100, China

(Received 25 April 2013; revised manuscript received 8 June 2013; published 3 December 2013)

A scheme that probabilistically realizes hierarchical quantum state sharing of an arbitrary unknown qubit state with a four-qubit non-maximally entangled $|\chi\rangle$ state is presented in this paper. In the scheme, the sender Alice distributes a quantum secret with a Bell-state measurement and publishes her measurement outcomes via a classical channel to three agents who are divided into two grades. One agent is in the upper grade, while the other two agents are in the lower grade. Then by introducing an ancillary qubit, the agent of the upper grade only needs the assistance of any one of the other two agents for probabilistically obtaining the secret, while an agent of the lower grade needs the help of both the other two agents by using a controlled-NOT operation and a proper positive operator-valued measurement instead of the usual projective measurement. In other words, the agents of two different grades have different authorities to reconstruct Alice's secret in a probabilistic manner. The scheme can also be modified to implement the threshold-controlled teleportation.

Keywords: $|\chi\rangle$ state, hierarchical quantum state sharing, asymmetetric distribution, positive operator-valued measurement

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud **DOI:** 10.1088/1674-1056/23/1/010304

1. Introduction

The immensely successful methodology of quantum secret sharing has provided new applications involving creating private keys among distributed participants. One of the most important branches of the quantum secret sharing is quantum state sharing (QSS),[1,2] which was first introduced by Hillery *et al.* In the original QSS proposal, a secret quantum state is distributed by quantum teleportation[3] from a boss to more than one agents so that any one of them can recover the state with the assistance of the others.

The QSS has extensive applications in quantum information science, such as creating joint checking accounts containing quantum money[4] and secure distributed quantum computation.[5,6] Since the outstanding work of Hillery *et al.*, the QSS has been attracting much attention,[7–30] and a scheme has already been experimentally realized.[31] However, all of the aforementioned QSS schemes are focused on the symmetric case where every partner has the same status, i.e., the same authority for getting the sender's secret. In 2000, Gottesman[8] pointed out that a more general QSS scheme should include an asymmetry between the powers of the different participants, and showed that it is possible to construct an access structure in which some subsets of the shares can be combined to reconstruct the secret quantum state. Recently, an attempt has been made by Wang *et al.* in Refs. [32]–[34] to give a partial answer with the $|\chi\rangle$ state, the graph state, and the cluster state as the quantum channels to the question raised by Gottesman.

Quantum entanglement, one of the most striking features in quantum mechanics, is the center resource for quantum information processing. So far, various entangled states have been extensively explored in QSS protocols, including Greenberger–Horne–Zeilinger (GHZ) states,[21,22] Bell states,[23,24] W states,[25,26] graph states,[27,33] genuine five-qubit states,[28,29] and six-qubit states.[30] However, all of those states in the above literature are the maximally entangled states. In a real communication scenario, an initially maximally entangled state may easily evolve into a non-maximally entangled or mixed state due to the inevitable environmental effect. There have been some probabilistic QSS schemes[35–38] with non-maximally entangled states as the quantum channels. Thus, it is reasonable to surmise that the sender can also share non-maximally entangled channels with the participants. However it often necessary to perform a high-dimensional projective measurement operation[34–36] to restore the original state, which makes the physical realization difficult.

In this paper, by utilizing a proper positive operator-valued measure (POVM)[39–41] instead of the usual projective measurement, we propose an asymmetric QSS scheme with a four-qubit non-maximal entanglement $|\chi\rangle$ channel and the classical communication. Our scheme distributes an unknown quantum state to three distant agents asymmetrically and the agents do not need to perform any nonlocal operation to obtain the original secret. This asymmetric distribution leads to the

*Project supported by the National Natural Science Foundation of China (Grant No. 11071178) and the Research Foundation of the Education Department of Sichuan Province, China (Grant No. 12ZB106).

†Corresponding author. E-mail: pengjiayin62226@163.com

© 2014 Chinese Physical Society and IOP Publishing Ltd

agents having different powers to reconstruct the boss's secret, i.e., their authorities for getting the secret are hierarchized. The $|\chi\rangle$ state, proposed by Yeo and Chua,[42] has many interesting properties and exhibits more clear nonlocality in some aspects than its counterparts of the well-known GHZ and W states.[42,43] In addition, it can be easily verified that at least two single-qubit measurements are required to completely disentangle $|\chi\rangle$. Thus such a state has higher persistency of entanglement than the GHZ state, which can be completely disentangled by only one local measurement. This may lead to the result that our scheme is more robust against decoherence than the schemes in Refs. [1], [44], and [45]. For implementing the same quantum task, the order of matrix of projective measurement is double of the POVM, so our protocol makes real experiments easier and possible.

2. Hierarchical and probabilistic QSS via non-maximally entangled $|\chi\rangle$ channel

Consider a situation in which Alice, Bob, Charlie, and David possess particles A, B, C, and D, respectively. Alice also wishes to teleport the unknown state of particle A$'$

$$|\phi\rangle_{\mathrm{A}'} = \alpha|0\rangle_{\mathrm{A}'} + \beta|1\rangle_{\mathrm{A}'}, \tag{1}$$

where the coefficients are complex and satisfy normalized condition $|\alpha|^2 + |\beta|^2 = 1$. Suppose that Alice, Bob, Charlie, and David share a four-qubit non-maximally entangled state $|\chi\rangle_{\mathrm{ABCD}}$ as the quantum channel

$$|\chi\rangle_{\mathrm{ABCD}} = a|0\rangle_{\mathrm{A}}|\psi^0\rangle_{\mathrm{BCD}} + b|1\rangle_{\mathrm{A}}|\psi^1\rangle_{\mathrm{BCD}}, \tag{2}$$

where

$$|\psi^0\rangle_{\mathrm{BCD}} = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle + |110\rangle)_{\mathrm{BCD}},$$
$$|\psi^1\rangle_{\mathrm{BCD}} = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)_{\mathrm{BCD}},$$

and a and b are nonzero real numbers satisfying $a^2 + b^2 = 1$. The state of the whole system can be expressed as

$$\begin{aligned}|\tau\rangle &= |\phi\rangle_{\mathrm{A}'} \otimes |\chi\rangle_{\mathrm{ABCD}} \\ &= a\alpha|00\rangle_{\mathrm{A}'\mathrm{A}}|\psi^0\rangle_{\mathrm{BCD}} + b\alpha|01\rangle_{\mathrm{A}'\mathrm{A}}|\psi^1\rangle_{\mathrm{BCD}} \\ &\quad + a\beta|10\rangle_{\mathrm{A}'\mathrm{A}}|\psi^0\rangle_{\mathrm{BCD}} + b\beta|11\rangle_{\mathrm{A}'\mathrm{A}}|\psi^1\rangle_{\mathrm{BCD}}. \end{aligned}\tag{3}$$

Now Alice wants to transfer her original state $|\phi\rangle$ to her three agents so that each of them can recover the secret state with the assistance of some or all of the other agents. None can solely obtain the quantum information. To achieve this scheme, Alice performs a Bell-state measurement on her two particles A$'$ and A in the basis $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$, and then informs the outcome to them. The four states of this basis are given by

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

After Alice's measurement, the state of particles B, C and D collapses to one of the following four possible results:

$${}_{\mathrm{A}'\mathrm{A}}\langle\Phi^\pm|\tau\rangle = \frac{1}{\sqrt{2}}(a\alpha|\psi^0\rangle_{\mathrm{BCD}} \pm b\beta|\psi^1\rangle_{\mathrm{BCD}}), \tag{4}$$

$${}_{\mathrm{A}'\mathrm{A}}\langle\Psi^\pm|\tau\rangle = \frac{1}{\sqrt{2}}(b\alpha|\psi^1\rangle_{\mathrm{BCD}} \pm a\beta|\psi^0\rangle_{\mathrm{BCD}}). \tag{5}$$

The non-cloning theorem[46] allows only one qubit to be in state $|\phi\rangle$, so one of Bob, Charlie, and David, but not all, can recover this state.

First, suppose that David is assigned to recover the original state $|\phi\rangle$. We rewrite ${}_{\mathrm{A}'\mathrm{A}}\langle\Phi^\pm|\tau\rangle$ and ${}_{\mathrm{A}'\mathrm{A}}\langle\Phi^\pm|\tau\rangle$ as follows:

$$\begin{aligned}{}_{\mathrm{A}'\mathrm{A}}\langle\Phi^\pm|\tau\rangle &= \frac{1}{2\sqrt{2}}[(|00\rangle_{\mathrm{BC}} + |11\rangle_{\mathrm{BC}})(a\alpha|0\rangle \pm b\beta|1\rangle)_{\mathrm{D}} \\ &\quad - (|01\rangle_{\mathrm{BC}} + |10\rangle_{\mathrm{BC}})(a\alpha|1\rangle \mp b\beta|0\rangle)_{\mathrm{D}}] \\ &= \frac{1}{2}[|+_{\mathrm{B}}+_{\mathrm{C}}\rangle(a\alpha|-_{\mathrm{D}}\rangle \pm b\beta|+_{\mathrm{D}}\rangle) \\ &\quad - |-_{\mathrm{B}}-_{\mathrm{C}}\rangle(a\alpha|+_{\mathrm{D}}\rangle \mp b\beta|-_{\mathrm{D}}\rangle)], \end{aligned}\tag{6}$$

$$\begin{aligned}{}_{\mathrm{A}'\mathrm{A}}\langle\Psi^\pm|\tau\rangle &= \frac{1}{2\sqrt{2}}[(|00\rangle_{\mathrm{BC}} + |11\rangle_{\mathrm{BC}})(b\alpha|1\rangle \pm a\beta a|0\rangle)_{\mathrm{D}} \\ &\quad + (|01\rangle_{\mathrm{BC}} + |10\rangle_{\mathrm{BC}})(b\alpha|0\rangle \mp a\beta a|1\rangle)_{\mathrm{D}}] \\ &= \frac{1}{2}[|+_{\mathrm{B}}+_{\mathrm{C}}\rangle(b\alpha|+_{\mathrm{D}}\rangle \pm a\beta|-_{\mathrm{D}}\rangle) \\ &\quad - |-_{\mathrm{B}}-_{\mathrm{C}}\rangle(b\alpha|-_{\mathrm{D}}\rangle \mp a\beta|+_{\mathrm{D}}\rangle)], \end{aligned}\tag{7}$$

where $|\pm_j\rangle = (|0_j\rangle \pm |1_j\rangle)/\sqrt{2}$ (j = B, C, D). In order to assist David reconstructing the original state $|\phi\rangle$, after Alice publishes her measurement results via a classical channel, the other agents Bob and Charlie are asked to measure their qubits through a suitable basis and broadcast their results. According to Eqs. (6) and (7), if Bob and Charlie measure their qubits with the basis $\{|+\rangle, |-\rangle\}$, their outcomes are always correlated, i.e., anyone's result can deduce the other's. This implies that one of them is sufficient to help David recover the original state. Without loss of generality, suppose that Alice's measurement result is $|\Phi^-\rangle_{\mathrm{A}'\mathrm{A}}$, and the measurement result of one of Bob and Charlie, say, Bob, is $|+_{\mathrm{B}}\rangle$, then David obtains the state of his qubit

$$\frac{1}{2}(a\alpha|-_{\mathrm{D}}\rangle - b\beta|+_{\mathrm{D}}\rangle). \tag{8}$$

David then performs the corresponding operation $U = \mathrm{i}\sigma_y H$ on his qubit D, where σ_y is the Pauli operator, and $H = (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)/\sqrt{2}$ is the Hardamard transformation. It transforms as

$$|\tau'\rangle = \frac{1}{2}(a\alpha|0\rangle_{\mathrm{D}} + b\beta|1\rangle_{\mathrm{D}}). \tag{9}$$

Let $U'_j \in \{I, \sigma_z, \sigma_x, \mathrm{i}\sigma_y\}$, where σ_k ($k = x, y, z$) are the usual Pauli matrices, and I is the identity matrix. The outcomes of the measurements performed by Alice and Bob, the state obtained by David, and the corresponding collective operation $U_j = U'_j H$ are listed in Table 1.

Table 1. Relationship among Alice's measurement results (AR), Bob's measurement results (BR), states obtained by David, and the corresponding collective operation U_j.

AR	BR	State obtained by David	U_j
$\|\Phi^+\rangle_{A'A}$	$\|+_B\rangle$	$(a\alpha\|-_D\rangle+b\beta\|+_D\rangle)/2$	$\sigma_x H$
$\|\Phi^-\rangle_{A'A}$	$\|+_B\rangle$	$(a\alpha\|-_D\rangle-b\beta\|+_D\rangle)/2$	$i\sigma_y H$
$\|\Phi^+\rangle_{A'A}$	$\|-_B\rangle$	$(a\alpha\|+_D\rangle-b\beta\|-_D\rangle)/2$	$\sigma_z H$
$\|\Phi^-\rangle_{A'A}$	$\|-_B\rangle$	$(a\alpha\|+_D\rangle+b\beta\|-_D\rangle)/2$	H
$\|\Psi^+\rangle_{A'A}$	$\|+_B\rangle$	$(b\alpha\|+_D\rangle+a\beta\|-_D\rangle)/2$	H
$\|\Psi^-\rangle_{A'A}$	$\|+_B\rangle$	$(b\alpha\|+_D\rangle-a\beta\|-_D\rangle)/2$	$\sigma_z H$
$\|\Psi^+\rangle_{A'A}$	$\|-_B\rangle$	$(b\alpha\|-_D\rangle-a\beta\|+_D\rangle)/2$	$i\sigma_y H$
$\|\Psi^-\rangle_{A'A}$	$\|-_B\rangle$	$(b\alpha\|-_D\rangle+a\beta\|+_D\rangle)/2$	$\sigma_x H$

After that, the state of qubit D transforms into one of the following states:

$$\frac{1}{2}(a\alpha|0\rangle_D+b\beta|1\rangle_D),\ \ \frac{1}{2}(b\alpha|0\rangle_D+a\beta|1\rangle_D).$$

As proposed before, the state taken as the quantum channel is shared among Alice, Bob, Charlie, and David, i.e., David has the completed knowledge of the non-maximally entangled states. Hence, David introduces an auxiliary qubit m in the initial state $|0\rangle$ and performs a controlled-NOT gate operation on the auxiliary qubit m with qubit D as the control qubit. The controlled-NOT gate operation C_{Dm} converts the state of qubits D and m to

$$\begin{aligned}|T\rangle &= C_{Dm}|\tau'\rangle|0\rangle_m\\ &= \frac{1}{2}(a\alpha|00\rangle+b\beta|11\rangle)_{Dm}\\ &= \frac{1}{4}(|E\rangle_D\otimes|F\rangle_m+|G\rangle_D\otimes|H\rangle_m),\end{aligned}\tag{10}$$

where $|E\rangle_D=\alpha|0\rangle_D+\beta|1\rangle_D$, $|F\rangle_m=a|0\rangle_m+b|1\rangle_m$, $|G\rangle_D=\alpha|0\rangle_D-\beta|1\rangle_D$, and $|H\rangle_m=a|0\rangle_m-b|1\rangle_m$. From Eq. (10), David can get states $|E\rangle_D$ and $|G\rangle_D$ of his qubit D provided that states $|F\rangle_m$ and $|H\rangle_m$ are obtained via appropriate measurements on his auxiliary qubit m. Unfortunately, states $|F\rangle_m$ and $|H\rangle_m$ are not orthogonal in general. As a consequence, they cannot be differentiated deterministically. Nevertheless, the discrimination can be achieved in a probabilistic manner by making an optimal POVM operation.[39–41] So David performs an optimal POVM on the auxiliary qubit m. The POVM takes the form

$$\begin{aligned}O_1&=\frac{1}{\omega}|M_1\rangle\langle M_1|,\\ O_2&=\frac{1}{\omega}|M_2\rangle\langle M_2|,\\ O_3&=I-\frac{1}{\omega}\sum_{i=1}^{2}|M_i\rangle\langle M_i|,\end{aligned}\tag{11}$$

where

$$\begin{aligned}|M_1\rangle&=\frac{1}{\sqrt{\varepsilon}}\left(\frac{1}{a}|0\rangle+\frac{1}{b}|1\rangle\right)_m,\\ |M_2\rangle&=\frac{1}{\sqrt{\varepsilon}}\left(\frac{1}{a}|0\rangle-\frac{1}{b}|1\rangle\right)_m,\\ \varepsilon&=\frac{1}{(a)^2}+\frac{1}{(b)^2}=\frac{1}{a^2b^2},\end{aligned}$$

I is an identity operator, and parameter ω, which relates to a and b, should be able to assure O_3 to be a positive operator. To exactly determine ω, the three operators O_1, O_2, and O_3 are rewritten in the following matrix forms:

$$\begin{aligned}O_1&=\frac{1}{\omega\varepsilon}\begin{pmatrix}\frac{1}{a^2}&\frac{1}{ab}\\ \frac{1}{ab}&\frac{1}{b^2}\end{pmatrix},\\ O_2&=\frac{1}{\omega\varepsilon}\begin{pmatrix}\frac{1}{a^2}&-\frac{1}{ab}\\ -\frac{1}{ab}&\frac{1}{b^2}\end{pmatrix},\\ O_3&=\begin{pmatrix}1-\frac{2}{\omega\varepsilon a^2}&0\\ 0&1-\frac{2}{\omega\varepsilon b^2}\end{pmatrix}.\end{aligned}\tag{12}$$

Evidently, to let O_3 be a positive operator, parameter ω should satisfy the inequality $\omega\geq 2\max(a^2,b^2)$. After performing the above POVM on the auxiliary qubit m, David can definitively obtain O_1 and O_2 with the probability

$$\langle T|O_1|T\rangle=\frac{1}{4\omega\varepsilon}=\langle T|O_2|T\rangle.\tag{13}$$

Alternatively, in terms of the POVM value, David can positively conclude the state of qubit m. However, with the probability $1-1/2\omega\varepsilon$, David may get the value of O_3. In this case, David cannot infer the state of qubit m. Once David determines $|F\rangle_m$ or $|H\rangle_m$, he also knows state $|E\rangle_D$ or $|G\rangle_D$. As a consequence, David can reconstruct the original state $|\phi\rangle$ by performing an appropriate unitary operation. That is, if David knows that the state of his qubit D is $|E\rangle_D$ ($|G\rangle_D$), he only needs to perform unitary operation I (σ_z) on particle D.

So far, only the case that Alice's measurement result is $|\Phi^-\rangle_{A'A}$ and Bob's measurement result is $|+_B\rangle$ is considered. As a matter of fact, Bob may obtain $|-_B\rangle$. In this case, by applying the same analysis method, David can also retrieve state $|\phi\rangle$ on his qubit D with the same probability. Thus the total success probability of this QSS scheme is

$$\frac{1}{4\omega\varepsilon}\times 2\times 2=\frac{a^2b^2}{\omega}.\tag{14}$$

Table 2. Relationship among Alice's measurement results (AR), Bob's measurement results (BR), the two operations of POVM (O_i), and the success probability of the corresponding measurements (SP), where $O_3 = I - O_1 - O_2$, $\varepsilon = 1/a^2b^2$, $\omega \geq 2\max(a^2, b^2)$.

AR	BR	O_1	O_2	SP
$\|\Phi^{\pm}\rangle_{A'A}$	$\|\pm\rangle$	$O_1 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{a^2} & \frac{1}{ab} \\ \frac{1}{ab} & \frac{1}{b^2} \end{pmatrix}$	$O_2 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{a^2} & -\frac{1}{ab} \\ -\frac{1}{ab} & \frac{1}{b^2} \end{pmatrix}$	$\frac{a^2b^2}{\omega}$
$\|\Psi^{\pm}\rangle_{A'A}$	$\|\pm\rangle$	$O_1 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{b^2} & \frac{1}{ab} \\ \frac{1}{ab} & \frac{1}{a^2} \end{pmatrix}$	$O_2 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{b^2} & -\frac{1}{ab} \\ -\frac{1}{ab} & \frac{1}{a^2} \end{pmatrix}$	$\frac{a^2b^2}{\omega}$

Now let us make some further discussion on it. As depicted previously, Alice's measurement results can also be one of the other three results, applying a similar analysis method proposed above, David can probabilistically restore state $|\phi\rangle$ on his qubit D. Furthermore, we have worked out the success probability for each case, and the results are summarized in Table 2.

In all, the total success probability of this scheme is

$$\frac{a^2b^2}{\omega} \times 4 = \frac{4a^2b^2}{\omega}. \tag{15}$$

It can be easily verified that when the coefficients are $a = b = 1/\sqrt{2}$ and $\omega = 1$, O_3 is a zero operator, the POVM becomes the common projective measurement and the total success probability of the QSS will be 1. In this case, the present QSS scheme is transformed into the usual standard QSS scheme.

Remark 1 Due to the requirement of the POVM that matrix O_3 in Eq. (12) must be positive, $\omega \geq 2\max(a^2, b^2)$. So the scheme is the optimum strategy if $\omega = 2\max(a^2, b^2)$. The success probability of the optimum scheme can also get the maximum $2a^2b^2/\max(a^2, b^2)$ by $\omega = 2\max(a^2, b^2)$.

Remark 2 It can be seen from Eqs. (6) and (7) that Bob and Charlie can also choose the measurement basis $\{|0\rangle, |1\rangle\}$, then David needs the collaboration of both of them.

In the above discussion, David is assigned to recover the original state $|\phi\rangle$ with the assistance of some of the other agents. Now we further discuss the case in which the recovery needs the assistance of all the other agents. We consider the case that they agree to let Bob possess Alice's secret, i.e., recover the original state $|\phi\rangle$. Then ${}_{A'A}\langle\Phi^{\pm}|\tau\rangle$ and ${}_{A'A}\langle\Psi^{\pm}|\tau\rangle$ can be rewritten as

$$\begin{aligned} {}_{A'A}\langle\Phi^{\pm}|\tau\rangle = \frac{1}{2\sqrt{2}}[&(a\alpha|0\rangle_B \pm b\beta|1\rangle_B)|00\rangle_{CD} \\ &- (a\alpha|1\rangle_B \mp b\beta|0\rangle_B)|01\rangle_{CD} \\ &+ (a\alpha|1\rangle_B \pm b\beta|0\rangle_B)|10\rangle_{CD} \\ &- (a\alpha|0\rangle_B \mp \beta b|1\rangle_B)|11\rangle_{CD}], \end{aligned} \tag{16}$$

$$\begin{aligned} {}_{A'A}\langle\Psi^{\pm}|\tau\rangle = \frac{1}{2\sqrt{2}}[&(b\alpha|1\rangle_B \pm a\beta|0\rangle_B)|00\rangle_{CD} \\ &+ (b\alpha|0\rangle_B \mp a\beta|1\rangle_B)|01\rangle_{CD} \\ &+ (b\alpha|0\rangle_B \pm a\beta|1\rangle_B)|10\rangle_{CD} \\ &- (b\alpha|1\rangle_B \mp a\beta|0\rangle_B)|11\rangle_{CD}]. \end{aligned} \tag{17}$$

From Eqs. (16) and (17), it is found that Bob can obtain the state of his qubit B if and only if both Charlie and David measure their qubits in the basis $\{|0\rangle, |1\rangle\}$ and broadcast their results. In other words, Bob needs the assistance of both the other agents, Charlie and David, to get the state of his qubit B. By ignoring a global factor, the corresponding local operation made by Bob, Alice's Bell-state measurement outcomes, and Charlie's and David's single-qubit measurement results are shown in Table 3.

After that, the state of qubit B in Bob's possession is transformed into one of the following two states:

$$a\alpha|0\rangle_B + b\beta|1\rangle_B, \quad b\alpha|0\rangle_B + a\beta|1\rangle_B.$$

In order to reconstruct the original state $|\phi\rangle$, Bob can probabilistically restore state $|\phi\rangle$ on his qubit B by applying the very similar David's method about introducing an auxiliary qubit, performing the POVM, and making use of the local operations just proposed above. We also work out the success probability for each case, and the results are summarized in Table 4, where c stands for an arbitrary one of Charlie's and David's measurement results in set $M = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Table 3. Relationship among Alice's measurement results (AR), Charlie's and David's measurement results (CDR), Bob's states (BS), and Bob's recovering operations (BP).

AR	CDR	BS	BP
$\|\Phi^+\rangle_{A'A}$	$\|00\rangle$	$a\alpha\|0\rangle_B + b\beta\|1\rangle_B$	I
$\|\Phi^-\rangle_{A'A}$	$\|00\rangle$	$a\alpha\|0\rangle_B - b\beta\|1\rangle_B$	σ_z
$\|\Phi^+\rangle_{A'A}$	$\|01\rangle$	$a\alpha\|1\rangle_B - b\beta\|0\rangle_B$	$i\sigma_y$
$\|\Phi^-\rangle_{A'A}$	$\|01\rangle$	$a\alpha\|1\rangle_B + b\beta\|0\rangle_B$	σ_x
$\|\Phi^+\rangle_{A'A}$	$\|10\rangle$	$a\alpha\|1\rangle_B + b\beta\|0\rangle_B$	σ_x
$\|\Phi^-\rangle_{A'A}$	$\|10\rangle$	$a\alpha\|1\rangle_B - b\beta\|0\rangle_B$	$i\sigma_y$
$\|\Phi^+\rangle_{A'A}$	$\|11\rangle$	$a\alpha\|0\rangle_B - b\beta\|1\rangle_B$	σ_z
$\|\Phi^-\rangle_{A'A}$	$\|11\rangle$	$a\alpha\|0\rangle_B + b\beta\|1\rangle_B$	I
$\|\Psi^+\rangle_{A'A}$	$\|00\rangle$	$b\alpha\|1\rangle_B + a\beta\|0\rangle_B$	σ_x
$\|\Psi^-\rangle_{A'A}$	$\|00\rangle$	$b\alpha\|1\rangle_B - a\beta\|0\rangle_B$	$i\sigma_y$
$\|\Psi^+\rangle_{A'A}$	$\|01\rangle$	$b\alpha\|0\rangle_B - a\beta\|1\rangle_B$	σ_z
$\|\Psi^-\rangle_{A'A}$	$\|01\rangle$	$b\alpha\|0\rangle_B + b\beta\|1\rangle_B$	I
$\|\Psi^+\rangle_{A'A}$	$\|10\rangle$	$b\alpha\|0\rangle_B + a\beta\|1\rangle_B$	I
$\|\Psi^-\rangle_{A'A}$	$\|10\rangle$	$b\alpha\|0\rangle_B - a\beta\|1\rangle_B$	σ_z
$\|\Psi^+\rangle_{A'A}$	$\|11\rangle$	$b\alpha\|1\rangle_B - a\beta\|0\rangle_B$	$i\sigma_y$
$\|\Psi^-\rangle_{A'A}$	$\|01\rangle$	$b\alpha\|1\rangle_B + b\beta\|0\rangle_B$	σ_x

Table 4. Relationship among Alice's measurement results (AR), Charlie's and David's measurement results (CDR), the operations of POVM (O_i), and the success probability of the corresponding case (SP), where $O_3 = I - O_1 - O_2$, $\varepsilon = 1/a^2b^2$, and $\omega \geq 2\max(a^2, b^2)$.

AR	BR	O_i	SP
$\|\Phi^{\pm}\rangle_{A'A}$	$c \in M$	$O_1 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{a^2} & \frac{1}{ab} \\ \frac{1}{ab} & \frac{1}{b^2} \end{pmatrix}$, $O_2 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{a^2} & -\frac{1}{ab} \\ -\frac{1}{ab} & \frac{1}{b^2} \end{pmatrix}$	$\frac{a^2b^2}{4\omega}$
$\|\Psi^{\pm}\rangle_{A'A}$	$c \in M$	$O_1 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{b^2} & \frac{1}{ab} \\ \frac{1}{ab} & \frac{1}{a^2} \end{pmatrix}$, $O_2 = \frac{1}{\omega\varepsilon}\begin{pmatrix} \frac{1}{b^2} & -\frac{1}{ab} \\ -\frac{1}{ab} & \frac{1}{a^2} \end{pmatrix}$	$\frac{a^2b^2}{4\omega}$

The total success probability and the maximum success probability of this scheme are $(a^2b^2)/(4\omega)\times 2\times 8 = 4a^2b^2/\omega$ and $2a^2b^2/\max(a^2,b^2)$, respectively. Value ω and the probability corresponding to the optimum scheme are listed in Table 5.

Table 5. Relationship among Alice's measurement results (AR), Charlie's and David's measurement results (CDR), the optimum scheme value ω (OSV ω), and the success probability of the corresponding optimum scheme (SPOP).

AR	CDR	OSV ω	SPOP
$\|\phi^{\pm}\rangle_{x1}$	$c \in M$	$\omega = 2\max(a^2,b^2)$	$\frac{a^2b^2}{8\max(a^2,b^2)}$
$\|\psi^{\pm}\rangle_{x1}$	$c \in M$	$\omega = 2\max(a^2,b^2)$	$\frac{a^2b^2}{8\max(a^2,b^2)}$

These results are applicable to the case that Charlie is deputed to recover Alice's secret, because $|\chi\rangle_{ABCD}$ is unchanged under the permutation of qubits B and C, which indicates that Bob and Charlie have the same status in the QSS protocol. In a word, for recovering the secret state $|\phi\rangle$, David only needs the help of any one of Bob and Charlie, while Bob (Charlie) needs the assistance of both David and Charlie (Bob). Thus, their authorities for getting the secret are hierarchized, and David is in a higher position relative to Bob and Charlie. It implies that Alice's quantum secret is distributed to Bob, Charlie, and David asymmetrically, naturally, the more information is known, the less collaborations are needed.

The above QSS scheme can also be modified to implement the controlled teleportation[47] if we choose David as the receiver in advance. The protocol in Ref. [47] is a $(2,2)$-threshold controlling protocol where the achievement of teleportation is conditioned on the collaboration of both supervisors, while the present one is a $(1,2)$-threshold controlling protocol in which one of the two supervisors, Bob and Charlie, can help David successfully obtain the quantum secret.

As to the physical realization of the above QSS protocol, we mainly need to consider three points: the preparation of the four-particle non-maximally entangled state $|\chi\rangle$, the Bell-state measurement, and the POVM. Recently, several methods for preparing state $|\chi\rangle$ have been proposed.[48–50] Reference [48] presented a protocol for generating state $|\chi\rangle$ with a well controllable ion-trap setup. Reference [49] showed that a four-photon $|\chi\rangle$ state can be effectively created even with the conventional photon detectors. Reference [50] proposed a scheme for the joint remote preparation of an arbitrary 4-qubit $|\chi\rangle$ state. The Bell-state measurement has been well realized for both atomic and photonic qubits.[51,52] By using measurement-assisted programmable quantum processors[53] and the ensemble approach to polarization optics,[54] the POVM can be realized. All these achievements may contribute to our QSS scheme in physical realization.

Now let us analyze the scheme's security. Two kinds of eavesdroppers are considered in this protocol.

(i) Outside eavesdropper Suppose that there is an illegitimate user named Eve. She wants to gain the quantum information which Alice lets Bob, Charlie, and David share. In order to achieve her goal, she entangles an ancilla with the quantum channel during the particle distribution process. In this case, the security depends completely on whether the four legitimate users have securely shared the entangled $|\chi\rangle$ state which is taken as the quantum channel. Here we briefly review the check method. To measure her qubit, Alice choose randomly one single-qubit measurement basis (MB) from the two MBs $\{|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}\}$ and $\{|0\rangle, |1\rangle\}$ to measure her qubit. After that, Alice tells the other three legitimate users Bob, Charlie, and David which BM she has chosen for her qubit. Bob, Charlie, and David then use the same BM as Alice to measure their respective qubits. Their measurement results should be strongly correlated. If there exists an eavesdropper Eve in the quantum line, her operation will of course introduce some disturbances, which will cause some qubit errors. So, when the legitimate users publicly compare their results, they will find a lack of correlation, which means that the quantum channel is disturbed. Alternatively, there may exist an eavesdropper Eve. In this case, the quantum sharing process is aborted. Incidentally, in our scheme, the state taken as the quantum channel is assumed to be safely shared among legitimate users.

(ii) Inside eavesdropper Suppose one of the three legitimate agents Bob, Charlie, and David, say Bob, is dishonest.

He wants to solely and safely recover Alice's secret without any assistance from the other two agents. To achieve his goal, Bob captures the qubits sent by Alice to Charlie and David, and then sends Charlie and David fake ones prepared before. In this case, only when Alice designates Bob to reconstruct the state, can he successfully obtain state $|\phi\rangle$ and avoid the security detection. However, if Alice does not designate Bob but any one of Charlie and David, say Charlie, to reconstruct the state, then the state reconstructed by Charlie will differ from the state sent by Alice. In this case, if Alice and Charlie publicly compare the state, the eavesdropping can be disclosed. Hence, the success probability for dishonest Bob is only 33.333% in each run. During the whole sharing process, if the amount of check states is large enough, then dishonest Bob will be revealed.

3. Conclusion

Up to now, a number of quantum secret distribution schemes by teleportation with non-maximal entanglement channels have been presented. In those schemes, usually by performing the projective measurement, every agent has the same status to recover the quantum secret with the help of all the other agents. Owing to the $|\chi\rangle$ state being more robust against decoherence than the GHZ state, we have proposed a hierarchical QSS protocol of an arbitrary unknown qubit state with a particular four-qubit non-maximally entangled $|\chi\rangle$ state as the quantum channel. In our scheme, the three agents, i.e., Bob, Charlie, and David, have different authorities for obtaining Alice's (the sender) quantum secret. David only needs the help of any one of the other two agents, Bob and Charlie, for probabilistically recovering Alice's secret, while Bob (Charlie) needs the assistance of both the other partners, David and Charlie (Bob). That is, David has a larger authority than Bob and Charlie to possess the secret. In other words, the authorities of three agents are divided into two grades, and David is in the upper grade while Bob and Charlie are in the lower grade. By incorporating auxiliary qubits and performing the POVM instead of the usual projective measurement, the agents of different grades have different authorities for getting the quantum secret. Our scheme can also be modified to implement the $(1,2)$-threshold controlled teleportation.

References

[1] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[2] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[3] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[4] Wiesner S 1983 *SIGACT News* **15** 77
[5] Loukopoulos K and Browne D E 2010 *Phys. Rev. A* **81** 062336
[6] Ben-Or M, Crépeau C, Gottesnan D, Hassidim A and Smity A 2008 arXiv: 0801. 1544 [quant-ph]
[7] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev. A* **59** 162
[8] Gottesman D 2000 *Phys. Rev. A* **61** 042311
[9] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev. A* **63** 042301
[10] Chau H F 2002 *Phys. Rev. A* **66** 060302
[11] Guo G P and Guo G C 2003 *Phys. Lett. A* **310** 247
[12] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[13] Hsu L Y and Li C M 2005 *Phys. Rev. A* **71** 022321
[14] Han L F, Liu Y M, Shi S H and Zhang Z J 2007 *Phys. Lett. A* **361** 24
[15] Li S S, Nie Y Y, Hong Z H, Yi X J and Huang Y B 2008 *Commun. Threor. Phys.* **50** 633
[16] Wang Z S, Liu G Q and Ji Y H 2009 *Phys. Rev. A* **79** 054301
[17] Li B K, Yang Y G and Wen Q Y 2009 *Chin. Phys. Lett.* **26** 010302
[18] Nie Y Y, Sang M H, Li Y H, Liu J C and Sang M H 2011 *Int. J. Theor. Phys.* **50** 1367
[19] Wu J 2010 *Int. J. Theor. Phys.* **49** 324
[20] Wang Z Y 2011 *Int. J. quantum Inf.* **9** 571
[21] Tu C H, Huang Z H, Zhang S G, Hu M L, Wang Q Y, Li E B, Li Y N and Lu F Y 2011 *Opt. Commun.* **284** 455
[22] Li H K, Zhou P, Li C Y, Zhou H Y and Deng F G 2006 *J. Phys. B* **39** 1975
[23] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev. A* **72** 044301
[24] Yuan H, Liu Y M, Zhang W and Zhang Z J 2008 *J. Phys. B* **41** 145506
[25] Zhang Z J and Cheung C Y 2008 *J. Phys. B* **41** 015503
[26] Xue Z Y, Deng P, Yi Y M and Cao Z L 2006 *Int. J. Quantum Inf.* **4** 749
[27] Markham D and Sanders B C 2008 *Phys. Rev. A* **78** 042309
[28] Muralidharan S and Panigrahi P K 2008 *Phys. Rev. A* **77** 032321
[29] Hou K, Li Y B and Shi S H 2010 *Opt. Commun.* **283** 1961
[30] Choudhury S, Muralidharan S and Panigrahi P K 2009 *J. Phys. A* **42** 115303
[31] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J and Pan J W 2004 *Nature* **430** 54
[32] Wang X W, Xia L X, Wang Z Y and Zhang D Y 2010 *Opt. Commun.* **283** 1196
[33] Wang X W, Zhang D Y, Tang S Q and Xie L J 2011 *J. Phys. B* **44** 035505
[34] Wang X W, Zhang D Y, Tang S Q, Zhan X G and You K M 2010 *Int. J. Theor. Phys.* **49** 2691
[35] Zha X W 2007 *Acta Phys. Sin.* **56** 1875 (in Chinese)
[36] Shangguan L X, Sun H X, Chen X B, Wen Q Y and Zhu F C 2009 *Chin. Phys. Sec.* **58** 1371
[37] Gordon G and Rigolin G 2006 *Phys. Rev. A* **73** 062316
[38] Peng J Y and Mo Z W 2013 *Int. J. Quantum Inf.* **11** 1350004
[39] Cu Y J 2006 *Opt. Commun.* **259** 385
[40] Yan F L and Ding H W 2006 *Chin. Phys. Lett.* **23** 17
[41] Wang Z Y, Wang D, Liu J and Shi S H 2006 *Commun. Theor. Phys.* **46** 859
[42] Yeo Y and Chua W K 2006 *Phys. Rev. Lett.* **96** 060502
[43] Wu C, Yeo Y, Kwek L C and Oh C H 2007 *Phys. Rev. A* **75** 032332
[44] Yan F L and Wang D 2003 *Phys. Lett. A* **316** 297
[45] Agrawal P and Pati A K 2002 *Phys. Lett. A* **305** 12
[46] Wootters W K and Zurek W H 1982 *Nature* **239** 802
[47] Karlsson A and Bourennane M 1998 *Phys. Rev. A* **58** 4394
[48] Wang X W and Yang G J 2008 *Phys. Rev. A* **78** 024301
[49] Wang H F and Zhang S 2009 *Phys. Rev. A* **79** 042336
[50] Luod M X and Deng Y 2012 *Int. J. Theor. Phys.* **51** 3027
[51] Reichle R, Leibfrie D, Knill E, Britton J, Blakestad R B, Jost J D, Langer C, Ozeri R, Seidelin S and Wineland D J 2006 *Nature* **443** 838
[52] Olmschenk S, Matsukevich D N, Maunz P, Hayes D, Duan L M and Monroe C 2009 *Science* **323** 486
[53] Ziman M and Bužek V 2005 *Phys. Rev. A* **72** 022343
[54] Sudha, Gopala A V, Usha Devi A R and Rajagopal A K 2007 arXiv:0704.0147