Int J Theor Phys (2014) 53:1848–1861
DOI 10.1007/s10773-013-1986-4

Asymmetric Quantum Information Splitting of an Arbitrary N-qubit State via GHZ-*like* State and Bell States

Shuang-Yong Kang · Xiu-Bo Chen · Yi-Xian Yang

Received: 25 July 2013 / Accepted: 27 December 2013 / Published online: 12 January 2014

Abstract In this manuscript, a novel and economical scheme for asymmetric quantum information splitting (AQIS) of an arbitrary N-qubit state is investigated. Instead of multi-qubit entangled states, the maximally entangled states, which are made up of a three-qubit GHZ-*like* entangled state and $(N-1)$ sets of Bell states, are used as quantum information carrier. It is shown that the proposed AQIS scheme can be faithfully realized by performing appropriate Bell state measurements (BSMs), single qubit measurements (SMs) and local unitary operations (LUOs), rather than multi-qubit entanglement or multi-particle joint measurements, which make it more convenient and feasible in a practical application than some previous schemes. Furthermore, its intrinsic efficiency for qubits approaches 100 %, and the total efficiency really approaches the maximal value, which is higher than those of some previous symmetric quantum information splitting (QIS) schemes. Finally, the proposed scheme can be proven information-theoretically secure from the views of participant attack and outside attack in detail.

Keywords Asymmetric quantum information splitting · Quantum teleportation · GHZ-*like* state · Bell state measurements · Entropic uncertainty principle

1 Introduction

After the pioneering work of Bennett et al. [1] (BB84), quantum key distribution (QKD) has progressed rapidly, and become one of the most important branch of quantum informa-

S.-Y. Kang · X.-B. Chen (✉) · Y.-X. Yang
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: flyover100@163.com

S.-Y. Kang
e-mail: kangshuangy@163.com

S.-Y. Kang · X.-B. Chen
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

tion [2]. The most advantage of QKD is its unconditional security, which is guaranteed by the principle of quantum mechanics, instead of computational complexity. Besides QKD, some other cryptographic tasks can be realized with quantum mechanics, such as quantum teleportation (QT) [3], quantum secret sharing (QSS) [4] and so on.

Classical secret sharing is a cryptographic task aiming to distribute a secret among a group of parties, and classical secret sharing protocol [5] have been proposed, where classical information is encoded by a mathematical transformation. The protocol can be proven to be information-theoretically secure, i.e., no information about the secret can be obtained by those adversaries even when they have unlimited computational power, if the communication channels between the dealer and the parties are secure.

Following the rapid development of quantum information, the extension of secret sharing to the quantum regime has received much theoretical attention. The objective of QSS is to use the quantum correlations in well-constructed entangled states to securely transmit a set of classical or quantum information to only the access structures. In 1999, Hillery et al. [4] proposed the pioneering QSS scheme for sharing a classical secret among three parties with a three-particle entangled GHZ state. Later, their scheme was generalized by Xiao et al. [6] to many parties. Since then, QSS was attracted widespread attention and there were lots of researches in both its theoretical [7–9] and experimental [10].

Generally speaking, the idea of QSS, in the literature, has been developed to the following three tasks: CC [11] (classical information is shared among parties by distributing QSS states through private secure channels, which are invulnerable to eavesdropping), CQ [9](classical information is shared among parties by distributing QSS states through public insecure channels, which are open for eavesdropping) and QQ [12–18](known as quantum state sharing or quantum information splitting, a secret quantum state is shared among parties by distributing QSS states through public channels). We consider the latter approach in the current paper. The three tasks form a hierarchy of the required resources; i.e., a QQ quantum state can perform all three tasks, and a CQ state can be used for CC, while the reverse is not always true.

To date, lots of QIS schemes have been proposed. Hillery et al.' scheme [4] can be viewed as a typical QIS. Soon later, Cleve and Gottesman et al. [7] have perfectly integrated quantum error correcting code technique for investigating a more general quantum (k, n) threshold QIS. Deng et al. [12] have presented a an arbitrary two-qubit QIS with four sets of EPR pairs as quantum information carrier. And then, instead of EPR pairs, Muralidharan et al. [13] have proposed another QIS via five-qubit Brown state, it have enormously reduced the cost of quantum resource. Yang et al. [14] have found a novel three-qubit GHZ-*like* state in experimental and demonstrated an arbitrary single-qubit state QIS based on Z basis measurement via it among three-party. Meanwhile, Zhang et al. [15] have also designed a similar three-party QIS of an arbitrary n-qubit state by using n sets of GHZ-*like* states as quantum information carrier. Recently, many-party QIS schemes of an arbitrary unknown quantum states have been investigated [16–18].

Inspired by some ideas of Refs. [14, 15, 22, 23], in this manuscript we firstly investigate the AQIS scheme of an arbitrary two-qubit state among three participants by using the maximally entangled states, which are made up of a three-qubit entangled GHZ-*like* state and a Bell state, as quantum information carrier, instead of multi-qubit entangled states. Different from most previous QIS ones, our scheme is claimed an asymmetrical quantum information splitting since that the number of the particles owned by each agent in the secure quantum channel is not necessarily equal except that the quantum information of the receiver is designated in advance. And then, it is generalized to N-qubit scenario. Through deep analysis and research, it can be found that some previous QIS ones exist severely redundancy for

the controller to own more than one particle compared with this AQIS scheme. Moreover, the intrinsic efficiency for qubits of the AIQS scheme approaches 100% by reducing the redundant information, and the total efficiency really approaches the maximal value, which is higher than those of some previous QIS schemes [15].

The rest of this manuscript is organized as follows. In Sect. 2, we briefly introduce the preparation of GHZ-*like* state and then explicitly illustrate the AQIS scheme of an arbitrary two-qubit state. In Sect. 3 we generalize it to N-qubit scenario. In Sect. 4 we analyze the security from the views of participant attack and outside attack in detail. Some discussions and conclusions are given in Sect. 5.

2 AQIS of an Arbitrary Two-Qubit State

In this section, we will briefly introduce the preparation and quantum circuit of the GHZ-*like* state, then explicitly illustrate an economical and efficient AQIS scheme of an arbitrary two-qubit state by using a maximally entangled state, which is made up of the three-qubit GHZ-*like* entangled state and a Bell state, as quantum information carrier.

2.1 Preparation of GHZ-*like* State

As we all known, three-qubit entangled states have been classified into two classes [19]: GHZ-class and W-class. Any one of the two classes cannot be obtained from the other using local operations and classical communication. In accordance with this concept of classification, the GHZ-*like* state

$$\begin{aligned} |G\rangle &= \frac{1}{2}\big(|001\rangle + |010\rangle + |100\rangle + |111\rangle\big) \\ &= \frac{\sqrt{2}}{2}\big(|0\rangle|\psi^+\rangle + |1\rangle|\phi^+\rangle\big) \end{aligned} \tag{1}$$

where Bell states

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle \pm |11\rangle\big), \qquad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle \pm |10\rangle\big) \tag{2}$$

is quite like the W state. However, it belongs to GHZ-class state rather than W-class state and it exists a potential symmetry. This state can be generated by a single photon and an EPR pair as follows [15]:

I. One prepares a single photon $|+\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_1$ and an EPR pair $|\psi^+\rangle_{23} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{23}$. The composite system is formed

$$\begin{aligned} |G_0\rangle_{123} &= |+\rangle_1 \otimes |\psi^+\rangle_{23} \\ &= \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)_1 \otimes \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)_{23} \\ &= \frac{1}{2}\big(|001\rangle + |010\rangle + |101\rangle + |110\rangle\big)_{123} \end{aligned} \tag{3}$$

where the subscript i $(i = 1, 2, 3)$ denotes different particles of $|G_0\rangle_{123}$.

II. One can carry out a control-not (C-NOT) gate operation on $|G_0\rangle_{123}$ with the first particle as the control qubit and the third particle as the target qubit. Then the GHZ-*like* can be generated successfully.

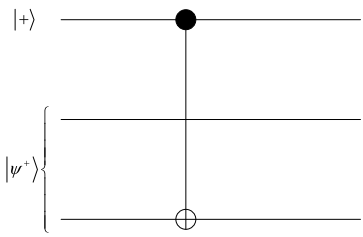

Fig. 1 The quantum circuit for the preparation of GHZ-*like* state

In fact, C-NOT gate operation [20], the generations of single photon and Bell state [21] have already been well demonstrated experimentally. Thus, the preparation of GHZ-*like* state is also feasible and it can be well demonstrated experimentally within the present technology. The quantum circuit for the preparation of GHZ-*like* state is shown in Fig. 1.

2.2 AQIS of an Arbitrary Two-Qubit State

Recently, Yang et al. [14] have devised a symmetric three-party QIS scheme of an arbitrary single-qubit by using only a GHZ-*like* state in Eq. (1) as quantum information carrier. Meanwhile, Zhang et al. [15] have also designed a similar symmetric three-party QIS one via another three-qubit GHZ-*like* state

$$|G\rangle' = \frac{1}{2}\big(|000\rangle + |110\rangle + |101\rangle + |011\rangle\big) \tag{4}$$

In fact, the mentioned above two GHZ-*like* state are the same contrast of the form dissimilarity but essences.

In this manuscript,we wish to construct a QQ scheme by mainly using the GHZ-*like* state as quantum information carrier. In principle, constructing a QQ state is versatile, but the amount of resources can be optimized according to the properties of the shared information and the channels. Moreover, according to Ref. [22] it is shown that using only a GHZ-*like* entangled state can't be utilized for any QIS task of an arbitrary more than two-qubit state. Inspired by some ideas of Refs. [14, 15, 22], we expect to generalize Yang et al.' scheme [4] and research into the AQIS scheme of an arbitrary two-qubit state by using a GHZ-*like* state and a Bell state. Like that in Ref. [14], assume that there are three parties, the boss Alice and two subordinates Bob and Charlie, where Bob is designated as the recover quantum information and Charlie is the controller, as shown in Fig. 2. In other words, Alice wants to transmit the arbitrary unknown quantum information to Bob who is designated to reconstruct it under Charlie's help.

Assume that Alice possesses an arbitrary unknown two-qubit state

$$|\psi\rangle_{xy} = \big(a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle\big)_{xy} \tag{5}$$

where a_i $(i = 0, 1, 2, 3)$ are complex numbers that satisfy the normalization condition $\sum_{i=0}^{3} |a_i|^2 = 1$. The quantum information carrier is the product of a GHZ-*like* state and a Bell state $|\phi^+\rangle$, i.e., it can be described as

$$\begin{aligned} |\Omega\rangle_{12345} &= |G\rangle_{123} \otimes \big|\phi^+\big\rangle_{45} \\ &= \frac{1}{2\sqrt{2}}\big(|001\rangle + |010\rangle + |100\rangle + |111\rangle\big) \otimes \big(|00\rangle + |11\rangle\big) \end{aligned} \tag{6}$$

In this scheme, Alice holds the particles $\{x, y, 1, 4\}$, while particles $\{3, 5\}$ and $\{2\}$ belong to Bob and Charlie, respectively. The basic idea of this QIS scheme is shown in Fig. 2,

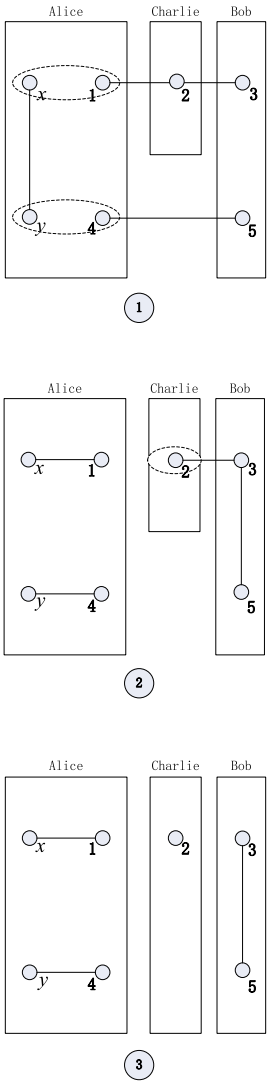

Fig. 2 AQIS of an arbitrary two-qubit state

where the solid lines connect qubits and the dashed lines connect qubits where a BSM is performed.

At the beginning, the whole system

$$\begin{aligned}|Q_2\rangle_{total} &= |\psi\rangle_{xy} \otimes |\Omega\rangle_{12345} = |\psi\rangle_{xy} \otimes |G\rangle_{123} \otimes \left|\phi^+\right\rangle_{45} \\ &= \frac{1}{2\sqrt{2}}\left(a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle\right)_{xy} \\ &\quad \otimes \left(|001\rangle + |010\rangle + |100\rangle + |111\rangle\right)_{123} \otimes \left(|00\rangle + |11\rangle\right)_{45} \end{aligned} \tag{7}$$

is prepared by Alice. The procedure of the AQIS proceeds as follows: Alice initially performs two BSMs on her qubit pairs $\{x, 1\}$ and $\{y, 4\}$ under the orthogonal basis $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$, respectively. It is clear that Alice may acquire one of 16 types of possible measurement re-

Table 1 The correlations between AMR and the corresponding states $|\phi\rangle_{235}$

AMR	$\|\phi\rangle_{235}$
$\|\phi^+\rangle_{x1}\|\phi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|010\rangle + \|100\rangle) \pm a_1(\|011\rangle + \|101\rangle) + a_2(\|000\rangle + \|110\rangle) \pm a_3(\|001\rangle + \|111\rangle)$
$\|\phi^+\rangle_{x1}\|\psi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|011\rangle + \|101\rangle) \pm a_1(\|010\rangle + \|100\rangle) + a_2(\|001\rangle + \|111\rangle) \pm a_3(\|000\rangle + \|110\rangle)$
$\|\phi^-\rangle_{x1}\|\phi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|010\rangle + \|100\rangle) \pm a_1(\|011\rangle + \|101\rangle) - a_2(\|000\rangle + \|110\rangle) \mp a_3(\|001\rangle + \|111\rangle)$
$\|\phi^-\rangle_{x1}\|\psi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|011\rangle + \|101\rangle) \pm a_1(\|010\rangle + \|100\rangle) - a_2(\|001\rangle + \|111\rangle) \mp a_3(\|000\rangle + \|110\rangle)$
$\|\psi^+\rangle_{x1}\|\phi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|000\rangle + \|110\rangle) \pm a_1(\|001\rangle + \|111\rangle) + a_2(\|010\rangle + \|100\rangle) \pm a_3(\|011\rangle + \|101\rangle)$
$\|\psi^+\rangle_{x1}\|\psi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|001\rangle + \|111\rangle) \pm a_1(\|000\rangle + \|110\rangle) + a_2(\|011\rangle + \|101\rangle) \pm a_3(\|010\rangle + \|100\rangle)$
$\|\psi^-\rangle_{x1}\|\phi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|000\rangle + \|110\rangle) \pm a_1(\|001\rangle + \|111\rangle) - a_2(\|010\rangle + \|100\rangle) \mp a_3(\|011\rangle + \|101\rangle)$
$\|\psi^-\rangle_{x1}\|\psi^\pm\rangle_{y4}$	$\|\phi\rangle_{235} = a_0(\|001\rangle + \|111\rangle) \pm a_1(\|000\rangle + \|110\rangle) - a_2(\|011\rangle + \|101\rangle) \mp a_3(\|010\rangle + \|100\rangle)$

sults with equal probability and the remaining qubits may collapse into one of the 16 states $|\phi\rangle_{235}$ after the Bell state measurement. We summarize the possible measurement results and the corresponding states obtained by Bob and Charlie in Table 1, where AMR denotes Alice's measurement result and the normalization factors are omitted for convenience.

Depending on AMR, the state of particles $\{2, 3, 5\}$ obtained by Bob and Charlie evolves to a pure three-particle entangled state. One can see that neither Bob nor Charlie can reconstruct $|\psi\rangle_{xy}$ by performing any general operations on their respective particles without communicating with each other. Whether it is possible for Bob to reconstruct the original state with LUOs on the state $|\phi\rangle_{235}$ depends on Charlie. If Charlie allows Bob to reconstruct $|\psi\rangle_{xy}$, he needs to carry out a SM on his qubit under the Z basis $\{|+z\rangle = |0\rangle, |-z\rangle = |1\rangle\}$ and then informs Bob of his measurement results (CMR) via a classical channel. Having obtained both AMR and CMR, Bob can recover $|\psi\rangle_{xy}$ by carrying out an appropriate local unitary operation on his particles. The correlations among AMR, CMR, the corresponding state $|\phi\rangle_{35}$ of Bob's particles and LUOs are shown in Table 2.

Now we can take an example in order to explicitly illustrate this AQIS principle. WLG, suppose that AMR is $|\phi^+\rangle_{x1}|\psi^-\rangle_{y4}$ on her qubit pairs $\{x, 1\}$ and $\{y, 4\}$, then the remaining qubits $\{2, 3, 5\}$ would collapse into the state

$$\begin{aligned}|\phi\rangle_{235} = {} & a_0\big(|011\rangle + |101\rangle\big) + a_1\big(|010\rangle - |100\rangle\big) \\ & + a_2\big(|001\rangle + |111\rangle\big) + a_3\big(-|000\rangle + |110\rangle\big)\end{aligned} \tag{8}$$

Then Charlie can do a SM on his particle under the basis Z and send CMR to Bob via a classical channel. If it is $|0\rangle$, then Bob needs to perform the LUOs $\sigma_x^3 \otimes (-i\sigma_y)^5$ on his own qubits; otherwise $I^3 \otimes (-i\sigma_y)^5$. Here the LUOs I, σ_x, $-i\sigma_y$ and σ_z are four different Pauli operations and described as

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1|, & \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ -i\sigma_y &= |1\rangle\langle 0| - |0\rangle\langle 1|, & \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1| \end{aligned} \tag{9}$$

3 Generalized AQIS of an Arbitrary N-qubit State

Next, the above-mentioned scheme can be generalized to N-qubit scenario. Firstly, assume that Alice possesses an arbitrary unknown N-qubit entangled state

$$|\phi\rangle_{j_1,j_2,\ldots,j_N} = \sum_{j_1,j_2,\ldots,j_N \in \{0,1\}} a_{j_1,j_2,\ldots,j_N} |j_1, j_2, \ldots, j_N\rangle_{j_1,j_2,\ldots,j_N} \tag{10}$$

Table 2 the correlations among AMR, CMR, $|\phi\rangle_{35}$ and LUOs

AMR	CMR	$\|\phi\rangle_{35}$	$U_i^3 \otimes U_j^5$
$\|\phi^+\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|10\rangle + a_1\|11\rangle + a_2\|00\rangle + a_3\|01\rangle)_{35}$	$\sigma_x^3 \otimes I^5$
$\|\phi^+\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|00\rangle + a_1\|01\rangle + a_2\|10\rangle + a_3\|11\rangle)_{35}$	$I^3 \otimes I^5$
$\|\phi^+\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|10\rangle - a_1\|11\rangle + a_2\|00\rangle - a_3\|01\rangle)_{35}$	$\sigma_x^3 \otimes \sigma_z^5$
$\|\phi^+\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|00\rangle - a_1\|01\rangle + a_2\|10\rangle - a_3\|11\rangle)_{35}$	$I^3 \otimes \sigma_z^5$
$\|\phi^+\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|11\rangle + a_1\|10\rangle + a_2\|01\rangle + a_3\|00\rangle)_{35}$	$\sigma_x^3 \otimes \sigma_x^5$
$\|\phi^+\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|01\rangle + a_1\|00\rangle + a_2\|11\rangle + a_3\|10\rangle)_{35}$	$I^3 \otimes \sigma_x^5$
$\|\phi^+\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|11\rangle - a_1\|10\rangle + a_2\|01\rangle - a_3\|00\rangle)_{35}$	$\sigma_x^3 \otimes (-i\sigma_y)^5$
$\|\phi^+\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|01\rangle - a_1\|00\rangle + a_2\|11\rangle - a_3\|10\rangle)_{35}$	$I^3 \otimes (-i\sigma_y)^5$
$\|\phi^-\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|10\rangle + a_1\|11\rangle - a_2\|00\rangle - a_3\|01\rangle)_{35}$	$(-i\sigma_y)^3 \otimes I^5$
$\|\phi^-\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|00\rangle + a_1\|01\rangle - a_2\|10\rangle - a_3\|11\rangle)_{35}$	$\sigma_z^3 \otimes I^5$
$\|\phi^-\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|10\rangle - a_1\|11\rangle - a_2\|00\rangle + a_3\|01\rangle)_{35}$	$(-i\sigma_y)^3 \otimes \sigma_z^5$
$\|\phi^-\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|00\rangle - a_1\|01\rangle - a_2\|10\rangle + a_3\|11\rangle)_{35}$	$\sigma_z^3 \otimes \sigma_z^5$
$\|\phi^-\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|11\rangle + a_1\|10\rangle - a_2\|01\rangle - a_3\|00\rangle)_{35}$	$(-i\sigma_y)^3 \otimes \sigma_x^5$
$\|\phi^-\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|01\rangle + a_1\|00\rangle - a_2\|11\rangle - a_3\|10\rangle)_{35}$	$\sigma_z^3 \otimes \sigma_x^5$
$\|\phi^-\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|11\rangle - a_1\|10\rangle - a_2\|01\rangle + a_3\|00\rangle)_{35}$	$(-i\sigma_y)^3 \otimes (-i\sigma_y)^5$
$\|\phi^-\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|01\rangle - a_1\|00\rangle - a_2\|11\rangle + a_3\|10\rangle)_{35}$	$\sigma_z^3 \otimes (-i\sigma_y)^5$
$\|\psi^+\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|00\rangle + a_1\|01\rangle + a_2\|10\rangle + a_3\|11\rangle)_{35}$	$I^3 \otimes I^5$
$\|\psi^+\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|10\rangle + a_1\|11\rangle + a_2\|00\rangle + a_3\|01\rangle)_{35}$	$\sigma_x^3 \otimes I^5$
$\|\psi^+\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|00\rangle - a_1\|01\rangle + a_2\|10\rangle - a_3\|11\rangle)_{35}$	$I^3 \otimes \sigma_z^5$
$\|\psi^+\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|10\rangle - a_1\|11\rangle + a_2\|00\rangle - a_3\|01\rangle)_{35}$	$\sigma_x^3 \otimes \sigma_z^5$
$\|\psi^+\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|01\rangle + a_1\|00\rangle + a_2\|11\rangle + a_3\|10\rangle)_{35}$	$I^3 \otimes \sigma_x^5$
$\|\psi^+\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|11\rangle + a_1\|10\rangle + a_2\|01\rangle + a_3\|00\rangle)_{35}$	$\sigma_x^3 \otimes \sigma_x^5$
$\|\psi^+\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|01\rangle - a_1\|00\rangle + a_2\|11\rangle - a_3\|10\rangle)_{35}$	$I^3 \otimes (-i\sigma_y)^5$
$\|\psi^+\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|11\rangle - a_1\|10\rangle + a_2\|01\rangle - a_3\|00\rangle)_{35}$	$\sigma_x^3 \otimes (-i\sigma_y)^5$
$\|\psi^-\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|00\rangle + a_1\|01\rangle - a_2\|10\rangle - a_3\|11\rangle)_{35}$	$\sigma_z^3 \otimes I^5$
$\|\psi^-\rangle_{x1}\|\phi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|10\rangle + a_1\|11\rangle - a_2\|00\rangle - a_3\|01\rangle)_{35}$	$(-i\sigma_y)^3 \otimes I^5$
$\|\psi^-\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|00\rangle - a_1\|01\rangle - a_2\|10\rangle + a_3\|11\rangle)_{35}$	$\sigma_z^3 \otimes \sigma_z^5$
$\|\psi^-\rangle_{x1}\|\phi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|10\rangle - a_1\|11\rangle - a_2\|00\rangle + a_3\|01\rangle)_{35}$	$(-i\sigma_y)^3 \otimes \sigma_z^5$
$\|\psi^-\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|01\rangle + a_1\|00\rangle - a_2\|11\rangle - a_3\|10\rangle)_{35}$	$\sigma_z^3 \otimes \sigma_x^5$
$\|\psi^-\rangle_{x1}\|\psi^+\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|11\rangle + a_1\|10\rangle - a_2\|01\rangle - a_3\|00\rangle)_{35}$	$(-i\sigma_y)^3 \otimes \sigma_x^5$
$\|\psi^-\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|0\rangle_2$	$(a_0\|01\rangle - a_1\|00\rangle - a_2\|11\rangle + a_3\|10\rangle)_{35}$	$\sigma_z^3 \otimes (-i\sigma_y)^5$
$\|\psi^-\rangle_{x1}\|\psi^-\rangle_{y4}$	$\|1\rangle_2$	$(a_0\|11\rangle - a_1\|10\rangle - a_2\|01\rangle + a_3\|00\rangle)_{35}$	$(-i\sigma_y)^3 \otimes (-i\sigma_y)^5$

where $\sum_{j_1,j_2,\ldots,j_N\in\{0,1\}} |a_{j_1,j_2,\ldots,j_N}|^2 = 1$.

In this scheme, the quantum carrier is composed of $(N-1)$ sets of Bell states $|\phi^+\rangle_{i,i+1}(i = 1, 3, \ldots, 2N-3)$ and a GHZ-*like* state $|G\rangle_{2N-1,2N,2N+1}$. Alice holds n pairs of particles $\{j_1, 1\}, \{j_2, 3\}, \ldots, \{j_N, 2N-1\}$, while particles $\{2, 4, \ldots, 2N\}$ and $\{2N+1\}$ belong to Bob and Charlie, respectively. The basic idea of this QIS scheme is shown in Fig. 3.

At the beginning, the whole system

$$|Q_n\rangle_{total} = |\phi\rangle_{j_1,j_2,\ldots,j_N} \otimes |\phi^+\rangle_{1,2} \otimes \cdots \otimes \left|\phi^+\right\rangle_{2N-3,2N-2} \otimes |G\rangle_{2N-1,2N,2N+1} \qquad (11)$$

is prepared by Alice. The procedure proceeds as follows: Firstly, Alice makes n BSMs on her qubit pairs $\{j_1, 1\}, \{j_2, 3\}, \ldots, \{j_N, 2N-1\}$ under the basis $\{|\phi^\pm\rangle, |\psi^\pm\rangle\}$, respectively.

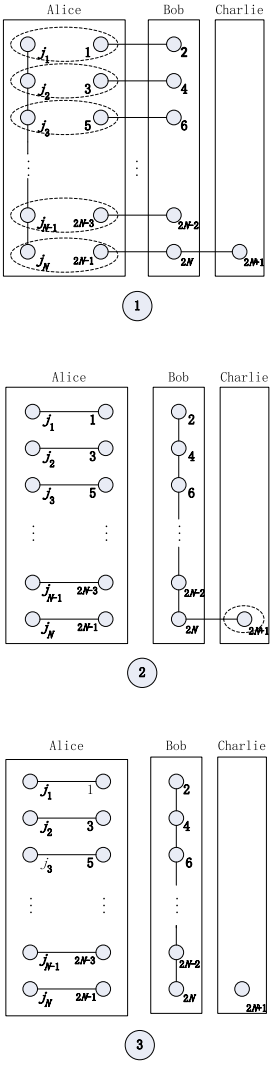

Fig. 3 AQIS of an arbitrary N-qubit state

It is clear that Alice may acquire one of 4^n kinds of possible measurement results with equal probability, and then Alice publicly informs her measurement results of Charlie. Whether it is possible to reconstruct the initial unknown state for Bob with local operations depends on Charlie. If Charlie cooperates with Bob, he carries out a SM on his qubit $\{2N+1\}$ under the Z basis and then conveys his measurement results to Bob. Consequently, Bob's particles will collapse into

$$|\phi\rangle_{2,4,\ldots,2N} = \sum_{j_1,j_2,\ldots,j_N\in\{0,1\}} b_{j_1,j_2,\ldots,j_N}|j_1,j_2,\ldots,j_N\rangle_{2,4,\ldots,2N} \tag{12}$$

where every coefficient $b_{j_1,j_2,\ldots,j_N}$ must be one of the rearrangements of those $a_{j_1,j_2,\ldots,j_N}$, and its value is depended on AMR and CMR. Then Bob can successfully translate $|\phi\rangle_{2,4,\ldots,2N}$ to the original state $|\phi\rangle_{j_1,j_2,\ldots,j_N}$ by performing suitable LUOs on his particles according

to AMR and CMR. Consequently, we perfectly design the AQIS scheme of an arbitrary N-qubit state.

4 Security Analysis

Now we will analyze the security of our scheme in detail and expect our methods could be also utilized for security analysis of other quantum communication schemes. For simplicity, we only consider two-qubit case. Notice that there are two kinds of eavesdropping. The first is that one dishonest participant (Bob or Charlie) try to obtain Alice's secret without cooperating with the other. The second is that a fourth eavesdropper Eve attempts to find Alice's secret without being detected.

Case I Participant attack

Firstly we consider the case of the dishonest participant Charlie, since the participant attack is always more powerful than outsider attack, thus the eavesdropper in this case can obtain more information than a fourth eavesdropper Eve. In the following, we will discuss the participant attack and show that Charlie cannot obtain information on the secret bits without being detectable.

As discussed in Ref. [23], supposed that participant Charlie performs unitary operators attack (P, Q) on the qubits sent from Alice to him and Bob. WLG, P and Q are assumed to share a common probe space $\mathcal{H}_E$. We have the following theorem.

Theorem 1 *For Charlie's attack inducing no error, the final state of Bob's probe should be independent of Charlie's measurement result and therefore Charlie gets no information.*

Proof Denote the qubits sent from Alice to Bob and Charlie by B and C, respectively, and denote Charlie's probe by E. Let us have a look at the evolution of the system $B + C + E$.

1. After Alice's BSMs, the remaining particle become a three-qubit state, denoted by $|\varphi\rangle_{BC}$. Then before Charlie's attack, the state is $|\varphi\rangle_{BC}|0\rangle_E$.
2. After Charlie has performed P, the state evolves to
$$|\varphi\rangle_{BCE} = \sum_{i=0}^{7} \left|\varphi^{(i)}\right\rangle_{BC} |E_i\rangle \tag{13}$$
where $|E_i\rangle$ are un-normalized states of Charlie's probe. In particular, if Charlie does nothing, then $|E_i\rangle = \frac{1}{2\sqrt{2}}|0\rangle$.
3. After Charlie has performed Q. We want to show that after Q having been performed the state of E is independent of Charlie's measurement. For Charlie not being detectable, Q must satisfy the following conditions: for $\forall i$,
$$Q\left|\varphi^{(i)}\right\rangle_{BC} |E_i\rangle = \left|\varphi^{(i)}\right\rangle_{BC} |F_i\rangle \tag{14}$$
It is a key point that Q can not change the state of $B + C$. Otherwise, Alice will detect Charlie's attack with a non-zero probability. For example, suppose that Q changes $|\varphi^{(0)}\rangle_{BC}|E_0\rangle$ to $\sum_{i=0}^{7} |\varphi^{(i)}\rangle_{BC}|F_i'\rangle$. Then, when Bob have made the recover operator on his qubits, Charlie will be brought some errors with probability $\sum_{i\neq 0} \||F_i'\rangle\|^2$.

We can see that, for Charlie's attack inducing no errors, the final state of Charlie's probe is independent of Bob's recover operation (but dependent on his own measurement result). Therefore, we have proved Theorem 1. □

Of course, In the above proof, if the entangling attack (P, Q) was performed by a fourth eavesdropper Eve, Bob and Charlie's measurement results should be strongly correlated since the entanglement is monogamous [24]. We can further show that all $|F_i\rangle$ are equal, which means that the state of outside eavesdropping Eve's probe is independent of Bob and Charlie's measurement results. What's more, we can mainly use the decoy photons technique and the estimation of mutual information, respectively, to prevent from the outsider attack.

Case II Outsider attack

Next we consider the case of outside attacker Eve, who wants to eavesdrop the secret state. Eve intercepts all the participants' photons during the particle distribution process and entangles ancillary particles in order to get the information. If she does obtain Alice's secret information, in the procedure she must inevitably introduce extra error rate which makes her be detected in the process of security checking [1]. In the following, we will provide a more reasonable explanation by means of the decoy photons technique. According to Stingspring dilation theorem [25], Eve's eavesdropping can be described by a unitary operation $\hat{U}_E$ on a larger Hilbert space $Hom(\mathcal{H}_A, \mathcal{H}_E)$. After Eve's eavesdropping, we have the following equations:

$$\begin{aligned} \hat{U}_E|0\rangle|\varepsilon\rangle_E &= |0\rangle|\varepsilon_0\rangle_E + |1\rangle|\varepsilon_1\rangle_E \\ \hat{U}_E|1\rangle|\varepsilon\rangle_E &= |0\rangle|\varepsilon_0'\rangle_E + |1\rangle|\varepsilon_1'\rangle_E \end{aligned} \tag{15}$$

where $|\varepsilon\rangle_E$ is the initial state of Eve's ancilla. Since $\hat{U}_E$ is a unitary operation, these pure ancilla's states $|\varepsilon_0\rangle, |\varepsilon_1\rangle, |\varepsilon_0'\rangle, |\varepsilon_1'\rangle$, thus, must satisfy

$$\begin{aligned} &\langle\varepsilon_0|\varepsilon_0\rangle + \langle\varepsilon_1|\varepsilon_1\rangle = 1, \qquad &&\langle\varepsilon_0'|\varepsilon_0'\rangle + \langle\varepsilon_1'|\varepsilon_1'\rangle = 1 \\ &\langle\varepsilon_1|\varepsilon_0\rangle + \langle\varepsilon_1'|\varepsilon_0'\rangle = 0, \qquad &&\langle\varepsilon_0|\varepsilon_1\rangle + \langle\varepsilon_0'|\varepsilon_1'\rangle = 0 \end{aligned} \tag{16}$$

For the decoy photons $|+\rangle, |-\rangle$, we can rewrite Eq. (15) into

$$\begin{aligned} \hat{U}_E|+\rangle|\varepsilon\rangle_E = \frac{1}{2}\big[&|+\rangle\big(|\varepsilon_0\rangle + |\varepsilon_1\rangle + |\varepsilon_0'\rangle + |\varepsilon_1'\rangle\big) \\ &+ |-\rangle\big(|\varepsilon_0\rangle - |\varepsilon_1\rangle + |\varepsilon_0'\rangle - |\varepsilon_1'\rangle\big)\big] \\ \hat{U}_E|-\rangle|\varepsilon\rangle_E = \frac{1}{2}\big[&|+\rangle\big(|\varepsilon_0\rangle + |\varepsilon_1\rangle - |\varepsilon_0'\rangle - |\varepsilon_1'\rangle\big) \\ &+ |-\rangle\big(|\varepsilon_0\rangle - |\varepsilon_1\rangle - |\varepsilon_0'\rangle + |\varepsilon_1'\rangle\big)\big] \end{aligned} \tag{17}$$

When the pre-shared decoy state is $|0\rangle$ or $|1\rangle$, the action of Eve's eavesdropping will introduce an error rate

$$P_e = \frac{1}{2}\big(\langle\varepsilon_1|\varepsilon_1\rangle + \langle\varepsilon_0'|\varepsilon_0'\rangle\big) \tag{18}$$

Similarly, for the decoy state is $|+\rangle$ or $|-\rangle$, the introduced error rate is

$$P_e' = \frac{1}{2}\big[2 - \big(\langle\varepsilon_1|\varepsilon_0'\rangle + \langle\varepsilon_0|\varepsilon_1'\rangle\big)\big] \tag{19}$$

Supposed that Eve is clever enough to prevent all participants from detecting her eavesdropping by finding the discrepancy in the error rates of quantum states. Eve tries to achieve the eavesdropping without being detected, if and only if both the error rates P_e and P_e' equal

0 in the ideal environment, which means that the quantum channels are noiseless. Thus, according to Eqs. (13), (18), (19) we can get the following equation

$$\begin{aligned}\langle\varepsilon_1|\varepsilon_1\rangle &= \langle\varepsilon_0'|\varepsilon_0'\rangle = 0\\ \langle\varepsilon_0|\varepsilon_0\rangle &= \langle\varepsilon_1'|\varepsilon_1'\rangle = 1\\ \langle\varepsilon_1|\varepsilon_0'\rangle &= \langle\varepsilon_0|\varepsilon_1'\rangle = 1\end{aligned} \tag{20}$$

Then, in essence, If the entanglement of Eve's ancilla with the quantum channel does not introduce any errors into the procedure, then the state of the system is a product of the state and the ancillary particles. It means that Eve gain no information about Alice's original quantum state.

Certainly, except the above decoy photons technique we can also adopt other strategies. Here, we will design an equivalent strategy for the security checking and give the estimation of mutual information. Sender can randomly prepare a Bell state $|\phi^+\rangle$ instead of the decoy photons. Then, she distributes one of the entangled particles to receiver, while keeping the other particle herself. Sender randomly measures each qubit in the mutually unbiased basis X or Z after receiving the confirmation. We can note that this model is originated from the celebrated E91 QKD [26]. It is equivalent to the decoy photons method used in our scheme, and more suitable for the following security proof.

At first, we will introduce the entropic uncertainty principle [27, 28] in order to give a more rigorous proof by estimating the mutual information between Alice and Eve. For POVM measurements X and Z and any density operator $\rho_{ABE} \in End(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$, the inequality

$$H(X|B) + H(Z|E) \geq \log \frac{1}{c(X,Z)} \tag{21}$$

holds, where, $c(X,Z) = \max_{jk} \| \sqrt{X_j}\sqrt{Z_k} \|_\infty^2$, and $\{X_j\}$ and $\{Z_k\}$ are the elements of corresponding POVM measurements. Moreover, for the mutually unbiased basis X and Z, the Eq. (21) equation can be simplified into

$$H(X|B) + H(Z|E) \geq 1 \tag{22}$$

Eve's attack has no effect on the local measurement performed by Alice because of the no-signaling theorem. Thus, the equality

$$H(Z) = 1 \tag{23}$$

holds. Combining both Eq. (22) and Eq. (23), we can compute an upper bound for the mutual information between Alice and Eve

$$I(Z;E) = H(Z) - H(Z|E) \leq H(X|B) \tag{24}$$

It is shown that the above mutual information $I(Z;E)$ will vanish when the uncertainty $H(X|B)$ approaches zero. Thus, what Eve has got is totally disentangled from Bob's system. In a word, any outside attack will be detected with a non-zero probability.

In addition, for a practical quantum channel, there are noise and loss which will threaten the security of quantum communication since Eve can hide her eavesdropping in the noise. Therefore, a security problem for this scheme implementing in an imperfect quantum channel seems to arise. Fortunately, even for a noise channel, with the help of quantum error correction [29–31], and a quantum repeater technique containing entanglement purification [32], and quantum privacy amplification [33, 34], our scheme can also be acted securely.

Of course, this methods of security analysis can be also utilized for security analysis of other quantum communication schemes.

The security of AQIS of an arbitrary N-qubit state is the same as the two-qubit case. In a word, our scheme is secure against participant attack and outside attack.

5 Conclusion and Discussion

In this manuscript, a novel scheme is investigated for AQIS of an arbitrary N-qubit state. Instead of multi-qubit entangled states, the maximally entangled states, which are made up of a three-qubit GHZ-*like* entangled state and $(N-1)$ sets of Bell states, are used as quantum carrier. Same as most existing symmetric QIS schemes, without the help of Charlie, Bob cannot recover the unknown state even though he obtains the measurement results published by Alice, because Bob does not know whether Charlie measure their particles with the Z basis or not. That means, Bob does not know whether his particles still entangle with those controlled by Charlie or not. Thus, the designated recover Bob can reconstruct the unknown N-qubit state with the probability 100 % in principle if he cooperates with the controller Charlie. It is shown that AQIS of an arbitrary N-qubit state can be faithfully realized by performing appropriate BSMs, SMs and LUOs.

For the security of this AQIS scheme, it depends on the process of the secure quantum channel, which is introduced in Ref. [1], by means of the decoy photons technique. However, the ratio of the decoy photons is small and can be ignored in theory. Thus, the intrinsic efficiency for qubits $\eta_q = \frac{q_u}{q_t}$ in our AQIS scheme approaches 100%, where q_u is the number of the useful qubits in AQIS and q_t is the number of qubits transmitted.

In addition, from the point of view of information theory, Cabello [35] proposed a definition of efficiency of a QKD scheme,

$$\eta = \frac{b_s}{q_t + b_t} \tag{25}$$

where b_s , q_t and b_t are the number of bits in the raw key, the qubits transmitted, and the total classical bits exchanged between the participants in the quantum communication, respectively. Here we exploited the definition, and the total efficiency for AQIS can be calculated as follows,

$$\eta_t = \frac{q_s}{q_t + b_t} \tag{26}$$

where q_s is the number of qubits in an unknown quantum state (the secret), q_t and b_t are described as the above. In our AQIS scheme for sharing an arbitrary N-qubit state with two agents, $q_s = N$, $q_t = N+1$, and $b_t = 2N+1$, so $\eta_t = \frac{q_s}{q_t+b_t} = \frac{N}{3N+2}$, which is the maximal value for AQIS theoretically. However, in Ref. [15], for sharing an arbitrary N-qubit state with two agents, $q_s = N$, $q_t = 2N$, and $b_t = 3N$, so $\eta_t = \frac{q_s}{q_t+b_t} = \frac{1}{5}$, which is lower than that of our scheme ($N \geq 2$). Moreover, in our scheme, when finishing one qubit state the principle is the same as Yang et al.' scheme [14], in other words, we perfectly generalizes Yang et al.' scheme by asymmetrically distributing the particles among those participants.

In summary, we have presented an asymmetric QIS scheme of an arbitrary N-qubit state with the maximally entangled states, which are made up of a three-qubit entangled GHZ-*like* state and $(N-1)$ sets of Bell states. It is shown that the proposed AQIS scheme can be faithfully realized by performing appropriate BSMs, Z basis measurement and LUOs, rather than multi-qubit entanglement or multi-particle joint measurements, which make it more convenient in a practical application than some previous schemes. Furthermore, its

intrinsic efficiency for qubits approaches 100 %, and the total efficiency really approaches the maximal value, which is higher than those of some previous symmetric quantum information splitting schemes. Finally, the proposed AQIS scheme can be proven information-theoretically secure from the views of participant attack and outside attack in detail. We mainly adopt the following two strategies: the decoy photons technique and estimating the mutual information via entropic uncertainty principle.

Finally we hope that our scheme can be realized experimentally for the N-qubit case. Working along an arbitrary multi-qubit by using other typical states as quantum information carrier is under way.

Acknowledgements Project supported by NSFC (Grant Nos. 61272514, 61003287, 61170272, 61121061, 61161140320), NCET (Grant No. NCET-13-0681), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 20100005120002), the Fok Ying Tong Education Foundation (Grant No. 131067).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: IEEE Int. Conf. on Computers, Systems, and Signal Processing, pp. 175–179. IEEE Press, New York (1984)
2. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, New York (2002)
3. 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**, 1895–1899 (1993)
4. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
5. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
6. Xiao, L., Long, G.L., Deng, F.G., et al.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 052307 (2004)
7. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret? Phys. Rev. Lett. **83**, 648–651 (1999)
8. Chen, X.B., Xu, G., Su, Y., Yang, Y.X.: Robust variations of secret sharing through noisy quantum channel. Quantum Inf. Comput. **14**, 0589 (2014)
9. Chen, X.B., Niu, X.X., Zhou, X.J., Yang, Y.X.: Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf. Process. **12**, 365–380 (2013)
10. Tittel, W., Zbinden, H., Gisin, N.: Experimental demonstration of quantum secret sharing. Phys. Rev. A **63**, 042301 (2001)
11. Wang, T.Y., Wen, Q.Y., Chen, X.B.: An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt. Commun. **281**, 6130–6134 (2008)
12. 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**, 044301 (2005)
13. Muralidharan, S., Panigrahi, P.K.: Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. Phys. Rev. A **77**, 032321 (2008)
14. Yang, K., Huang, L.S., Yang, W., Quantum, S.F.: Teleportation via GHZ-like state. Int. J. Theor. Phys. **48**, 516–521 (2009)
15. Zhang, Q.Y., Zhan, Y.B., Zhang, L.L., Ma, P.C.: Schemes for splitting quantum information via tripartite entangled states. Int. J. Theor. Phys. **48**, 3331–3338 (2009)
16. Lin, S., Guo, G.D.: Cryptanalysis the security of enhanced multiparty quantum secret sharing of classical messages by using entanglement swapping. Int. J. Theor. Phys. **52**, 3238–3243 (2013)
17. Liu, D., Zong, Z.C., Ma, W.: High-capacity quantum secret sharing with hyperdense coding assisted by hyperentangled photon pairs. Int. J. Theor. Phys. **52**, 2245–2254 (2013)
18. Xiao, H.L., Gao, J.L.: Multi-party d-level quantum secret sharing scheme. Int. J. Theor. Phys. **52**, 2075–2082 (2013)
19. Dur, W., Vidal, G., Cirac, J.I.: Three qubits can be entangled in two inequivalent ways (2000). arXiv:0000.5115v2 [quant-ph]

20. Rieffel, E.G., Polak, W.: An introduction to quantum computing for non-physicists. ACM Comput. Surv. **32**, 300–335 (2000)
21. Englert, B.G., Walther, H.: Preparing a GHZ state, or an EPR state, with the one-atom maser. Opt. Commun. **179**, 283–288 (2000)
22. Muralidharan, S., Karumanchi, S., Narayanaswamy, S., Srikanth, R., Panigrahi, P.K.: In how many ways can quantum information be split (2009). arXiv:0907.3532v2 [quant-ph]
23. Kang, S.Y., Chen, X.B., Yang, Y.X.: Quantum teleportation and state sharing via a generalized seven-qubit brown state. Int. J. Theor. Phys. **52**, 3413–3431 (2013)
24. Coffman, V., Kundu, J., Wootters, W.K.: Distributed entanglement. Phys. Rev. A **61**, 052306 (2000)
25. Stinespring, W., Positive, F.: Functions on C^*-algebras. Proc. Am. Math. Soc. **6**, 211–216 (1955)
26. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
27. Berta, M., Christandl, M., Colbeck, R., Renes, J.M., Renner, R.: The uncertainty principle in the presence of quantum memory. Nat. Phys. (2010). doi:10.1038/nphys1734-1745
28. Coles, P.J., Colbeck, R., Yu, L., Zwolak, M.: Uncertainty relations from simple entropic properties. Phys. Rev. Lett. **108**, 210405 (2012)
29. Calderbank, A.P., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**, 1098–1105 (1996)
30. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**, 793–797 (1996)
31. Bennett, C.H., Divincenzo, D.P., Smolin, J.A., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**, 3824–3851 (1996)
32. Cao, C., Wang, C., He, L.Y., Zhang, R.: Polarization-entanglement purification for ideal sources using weak Cross-Kerr nonlinearity. Int. J. Theor. Phys. **52**, 1265–1273 (2013)
33. Waks, E., Zeevi, A., Yamamoto, Y.: Security of quantum key distribution with entangled photons against individual attacks. Phys. Rev. A **65**, 052310 (2002)
34. Zhu, C.H., Quan, D.X., Zhang, F., Improving, P.C.X.: Key rate of optical fiber quantum key distribution system based on channel tomography. Int. J. Theor. Phys. **52**, 596–603 (2013)
35. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635–5638 (2000)