Quantum Inf Process (2017) 16:59
DOI 10.1007/s11128-016-1506-6

Quantum secret sharing using the d-dimensional GHZ state

Chen-Ming Bai[1] · **Zhi-Hui Li**[1] · **Ting-Ting Xu**[1] · **Yong-Ming Li**[2]

Received: 21 September 2016 / Accepted: 19 December 2016 / Published online: 21 January 2017

Abstract We propose a quantum secret sharing scheme that uses an orthogonal pair of n-qudit GHZ states and local distinguishability. In the proposed protocol, the participants use an X-basis measurement and classical communication to distinguish between the two orthogonal states and reconstruct the original secret. We also present $(2, n)$-threshold and generalized restricted $(2, n)$-threshold schemes that enable any two cooperating players from two disjoint groups to always reconstruct the secret. Compared to the existing scheme by Rahaman and Parker (Phys Rev A 91:022330, 2015), the proposed scheme is more general and the access structure contains more authorized sets.

Keywords Quantum secret sharing · Local distinguishability · GHZ state · Orthogonal pair

1 Introduction

Secret sharing, first introduced by Shamir [1] and Blakley [2], plays a significant role in the cryptography. It is an important protocol to distribute a piece of secret information (called the secret) among a finite set of players $\mathcal{P}$ such that only qualified

✉ Zhi-Hui Li
lizhihui@snnu.edu.cn

Yong-Ming Li
liyongm@snnu.edu.cn

[1] College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710119, China

[2] College of Computer Science, Shaanxi Normal University, Xi'an 710119, China

subsets can collaboratively recover the secret. Traditionally, both secret and shares were classical information. Several researchers [3–6] extended the classical protocol to the quantum field. Quantum secret sharing (QSS) is also a cryptographic protocol to distribute a secret among a group of players $\mathcal{P}$ such that only authorized subsets of $\mathcal{P}$ can reconstruct the secret. While the secret in a quantum scheme may be either an unknown quantum state or a classical one, in this case the players are comprised of quantum systems and quantum communication is allowed between the dealer and the players. Compared to the classical secret sharing, QSS is more secure due to the excellent properties of quantum theory.

In 1999, Hillery et al. [3] firstly introduced a protocol of QSS by using GHZ states. At the same year, Karlsson et al. [7] showed how a QSS protocol can be implemented using two-particle quantum entanglement and discussed how to detect eavesdropping or a dishonest participant. In 2004, Xiao et al. [8] generalized the QSS of Hillery et al. into arbitrary multiparty. From then on, various QSS schemes have been proposed [9–21]. For example, Liao et al. [22] used the GHZ state to design a dynamic quantum secret sharing protocol. Rahaman and Parker [23] proposed the quantum secret sharing based on local distinguishability (LOCC-QSS). Gheorghiu and Sander [24] constructed accessing quantum secret via local operations and classical communication. Moreover, with the development and application of quantum communication, it is a good idea for quantum communication to design the protocol with high-dimensional quantum systems, such as quantum secure direct communication [25] and controlled teleportation [26]. For QSS, Tavakoli et al. [27] introduced the secret sharing with a single d-level quantum system. Qin and Dai [28] considered a verifiable (t, n) threshold quantum secret sharing using d-dimensional Bell state. Based on the idea of the previous schemes, we try to combine the d-dimensional GHZ state and the local distinguishability to design a new quantum secret sharing scheme.

In this paper, we propose the quantum secret sharing scheme that uses local operations and classical communication (LOCC) to distinguish between two d-dimensional orthogonal GHZ states (d-LOCC-QSS). In our protocol, we firstly adopt the data block transmission technique [29] and make use of the decoy photon technique [30,31] to assure the security of the transmission. Then we utilize the delayed measurement technique [32]; that is, all participants efficiently make the measurements with X-basis after Alice. At last, the participants can distinguish the orthogonal pair and reconstruct the original secret.

The organization of this paper is as follows: In Sect. 2, we give some preliminaries. In Sect. 3, we propose the quantum secret sharing scheme and show two specific d-LOCC-QSS schemes. Section 4 analyzes the security. Section 5 compares our scheme with the existing scheme. Finally, the conclusion is given in Sect. 6.

2 Preliminaries

In this section, we discuss several distinguishability problems related to an orthogonal pair of n-qudit symmetric state, i.e., the generalized GHZ state, see Refs. [23,28].

Let $\mathcal{H}$ be a d-dimensional Hilbert space and a generalized n-qudit GHZ state can be denoted by

$$|\mathrm{GHZ}(u_1, u_2, u_3, \ldots, u_n)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{ju_1} |j, j + u_2, \ldots, j + u_n\rangle,$$

where $\omega = \mathrm{e}^{\frac{2\pi i}{d}}$,$u_1, u_2, \ldots, u_n \in \{0, 1, \ldots, d - 1\}$, and the symbol "+" means the adder modulo d. In particular, for $d = 2$, the general GHZ state can also be described as follows.

$$|\mathrm{GHZ}(u_1, u_2, u_3, \ldots, u_n)\rangle = \frac{1}{\sqrt{2}}[|0, u_2, \ldots, u_n\rangle + (-1)^{u_1}|1, \overline{u_2}, \ldots, \overline{u_n}\rangle]$$

where $u_1, u_2, \ldots, u_n \in \{0, 1\}$, and the bar over a bit value indicates its logical negation.

In the d-dimensional Hilbert space, the generalized X-basis and Z-basis have the following forms:

$$\begin{aligned} X &= \{|j\rangle, j = 0, 1, \ldots, d - 1\} \\ Z &= \{|J_j\rangle, j = 0, 1, \ldots, d - 1\} \end{aligned}$$

where $|J_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle$ and $\omega = \mathrm{e}^{\frac{2\pi i}{d}}$.

Let us define an orthogonal pair with distance r as follows:

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{d}}\Big[|\overbrace{\underbrace{0, 0, \ldots, 0}_{A_0}, \underbrace{0, 0, \ldots, 0}_{A_1}, \ldots, \underbrace{0, 0, \ldots, 0}_{A_{d-1}}}^{n}\rangle + |1, 1, \ldots, 1, 1, \ldots, 1\rangle \\ &\quad + \cdots + |d-1, d-1, \ldots, d-1, d-1, \ldots, d-1\rangle\Big] \\ |\mathrm{GHZ}\rangle_r &= \frac{1}{\sqrt{d}}\Big[|\underbrace{0, 0, \ldots, 0}_{A_0}, \underbrace{1, 1, \ldots, 1}_{A_1}, \ldots, \underbrace{d-1, d-1, \ldots, d-1}_{A_{d-1}}\rangle \qquad (1) \\ &\quad + |1, 1, \ldots, 1, 2, 2, \ldots, 2, \ldots, 0, 0, \ldots, 0\rangle + \ldots \\ &\quad + |d-1, d-1, \ldots, d-1, 0, 0, \ldots, 0, \ldots, d-2, d-2, \ldots, d-2\rangle\Big] \end{aligned}$$

where $r = \max\{|A_k| : k = 0, 1, \ldots, d-1\}$ and $|A_k|(k = 0, 1, \ldots, d-1)$ represents the total number of A_k and satisfies the following: (1) $\sum_{k=0}^{d-1} |A_k| = n$ and (2) there exist at least two nonzero elements in the $\{|A_k|\}_{k=0}^{d-1}$. In particular, for $d = 2$ we can get $r = \max\{|A_0|, |A_1|\}$. It is easy to verify that the orthogonal pair with distance r is consistent with the orthogonal pair of that distance in Ref. [23].

Example 1 We give an example to illustrate the existence of this orthogonal pair with distance r. An orthogonal pair is denoted by:

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{3}}\Big[|000000\rangle + |111111\rangle + |222222\rangle\Big] \qquad (2)$$

$$|\mathrm{GHZ}\rangle_r = \frac{1}{\sqrt{3}}\Big[|011222\rangle + |122000\rangle + |200111\rangle\Big]$$

By the definition, we can get that $r = 3$. Hence, this is a distance-3 orthogonal pair.

Theorem 1 ([23]) *Classical communication is necessary to distinguish any pair of Bell states locally.*

We can understand this theorem as follows. Let Alice and Bob share the following pair of Bell states:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B]$$

Their goal is to distinguish the above pair of Bell states by only local operations (LO) on their respective qubits, and they cannot utilize the classical communication.

Let Alice and Bob be spatially separated and share the known Bell state $|\Phi^{\pm}\rangle$. Bob applies $\mathbb{I}$ or σ_z on his qubit to communicate the message 0 or 1, respectively, and the desired state may change to another orthogonal Bell state as

$$(\mathbb{I}^A \otimes \mathbb{I}^B)|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B] = |\Phi^+\rangle,$$
$$\left(\mathbb{I}^A \otimes \sigma_z^B\right)|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B] = |\Phi^-\rangle$$

If Alice (alone) is able to distinguish the above pair without any communication from Bob, then she can recover Bobs message as well, which is impossible as that would imply signaling (no message can travel faster than the speed of light in a vacuum).

Theorem 2 *An orthogonal pair of generalized GHZ states* (1) *can always be exactly distinguished by any two cooperating LOCC parties, one from the part of A_j and the other from the part of A_k, where $k, j \in \{0, 1, \ldots, d-1\}$ and $j \neq k$.*

Proof The proof is simple. Both cooperating parties (one from the part of A_j and the other from the part of $A_k (j \neq k)$) measure their own qudit in the basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ locally, and if both of them get the same result, the shared state was $|\mathrm{GHZ}\rangle$, otherwise the state was $|\mathrm{GHZ}\rangle_r$. □

3 Quantum scheme for secret sharing

3.1 The *d*-LOCC-QSS scheme

Now we propose our scheme in some steps: Alice is going to share her secret information among Bob$_k$ ($k = 1, 2, \ldots, n$) such that some of them must collaborate to reconstruct Alice's secret. In this protocol, we adopt the following techniques: the

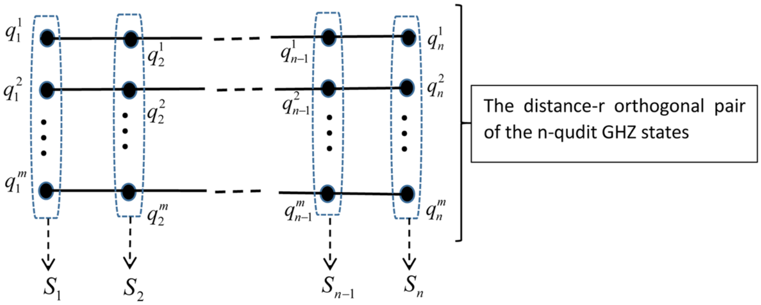

Fig. 1 The qudits distribution of our QSS scheme and the arranged particle sequences

data block transmission [29], the decoy photon technique [30,31] and the delayed measurement technique [32].

Step 1 (S1) Alice first prepares a sequence of m entangled states, $(q_1^j q_2^j \dots q_n^j)$ $j = 1, 2, \dots, m$, chosen randomly from a specified distance-r orthogonal pair of the n-qudit GHZ states in Eq. (1) according to the access structure. Then, Alice divides the sequence into n strings, as given in Fig. 1, and these strings can be denoted by:

$$\begin{aligned} S_1 &= \left\{q_1^1, q_1^2, \dots, q_1^m\right\}, \\ S_2 &= \left\{q_2^1, q_2^2, \dots, q_2^m\right\}, \\ &\dots \\ S_n &= \left\{q_n^1, q_n^2, \dots, q_n^m\right\}, \end{aligned} \tag{3}$$

where $q_1^j, q_2^j, \dots, q_n^j$ are the ordered particles in jth entangled state in the main sequence $j = 1, 2, \dots, m$.

Step 2 (S2) In order to prevent the dishonest participants, Alice now prepares, at random, a different sequence, $r_k = \Pi_k(1, 2, 3, \dots, m)$ $(k = 1, 2, \dots, n)$, where Π_k is an arbitrary permutation of the sequence $(1, 2, 3, \dots, m)$. Alice makes use of the r_k to disrupt the order of S_k and produces a new sequence S'_k $(k = 1, 2 \dots, n)$.

Step 3 (S3) In this step, Alice uses the checking photon technique in order to guarantee the security of transmission and randomly chooses some checking single photons from the X-basis and Z-basis. These photons are denoted by

$$C_k = \left\{p_k^1, p_k^2, \dots, p_k^l\right\}, k = 1, 2, \dots, n.$$

the single photons of C_k are put randomly between the particles of S'_k, $k = 1, 2, \dots, n$. At last, Alice shuffles the particles in the sequences and obtains new sequences $S''_1, S''_2, \dots, S''_n$.

Step 4 (S4) In this case, for each $k = 1, 2, \dots, n$, Alice sends S''_k to Bob$_k$. Note that Alice only sends the qudits and not the information about Π_k. Hence, except Alice, no one has the information about Π_k.

Step 5 (S5) After confirming that $\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_n$ have received their own sequences, Alice announces the positions and measuring base of checking photons in each sequence. All players take some measures to their corresponding checking photons in specific bases and resend the results to Alice. According to all participants' results, Alice can evaluate the error rate. If the error rate is higher than threshold value, then she must abort the protocol and start again with a new set of resources.

Step 6 (S6) If no eavesdropper is detected, Alice announces the sequence r_k to Bob_k, respectively. After receiving the sequence r_k, Bob_k measures his particles in the sequence S''_k with the X-basis. Through cooperation among the participants, they can distinguish between $|GHZ\rangle$ and $|\mathrm{GHZ}\rangle_r$, which $|\mathrm{GHZ}\rangle_r(|\mathrm{GHZ}\rangle)$ represents the secret $a(=0/1)$. The relation between classical bit value and orthogonal entangled pair is fixed and communicated, securely, from Alice to all Bobs in advance.

3.2 The specific d-LOCC-QSS scheme

In Ref. [23], Rahaman and Parker proposed the restricted $(2, n)$-threshold LOCC-QSS scheme. From the perspective of the graph access structure [33], the access structure in the LOCC-QSS scheme is a complete bipartite graph. In this section, we discuss the choice of states (S1) for different threshold scenarios and give the standard $(2, n)$-threshold d-LOCC-QSS scheme and the generalized restricted $(2, n)$-threshold d-LOCC-QSS scheme.

3.2.1 The $(2, n)$-threshold d-LOCC-QSS scheme

Here considering the case when $r = 1$, that is, $|A_k| = 1 (k = 0, 1, \ldots, d-1)$, we propose the $(2, n)$-threshold d-LOCC-QSS scheme ($n = d$). For this scheme, it is a standard threshold scheme; that is, the access structure can be written as

$$\Gamma = \{P_j P_k : j, k = 0, 1, \ldots, d-1 \text{ and } j \neq k\}.$$

S1. Alice first prepares the states, each chosen randomly from a distance-1 orthogonal pair of n-qudit GHZ states (4).

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{d}}\Big[|0,0,\ldots,0\rangle + |1,1,\ldots,1\rangle + \cdots + |d-1,d-1,\ldots,d-1\rangle\Big] \\ |\mathrm{GHZ}\rangle_1 &= \frac{1}{\sqrt{d}}\Big[|0,1,\ldots,d-1\rangle + |1,2,\ldots,0\rangle + \cdots + |d-1,0,\ldots,d-2\rangle\Big] \end{aligned} \tag{4}$$

S2, S3, S4 and S5 can be carried out in accordance with the above steps in Sect. 3.1.

S6. If no eavesdropper is detected, Alice announces the sequence r_k to Bob_k, respectively. According to Theorem 2, Bobs make use of the X-basis to measure their particles, and any two cooperating players can perfectly distinguish the above pair (4). If both are the same measurement, then the state is $|\mathrm{GHZ}\rangle$, otherwise the state is $|\mathrm{GHZ}\rangle_1$. Hence, they are able to recover the secret.

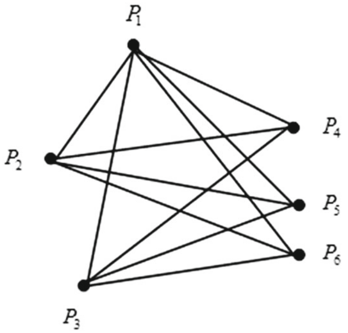

Fig. 2 The graph of the access structure Γ

3.2.2 *The generalized restricted* $(2, n)$*-threshold* d*-LOCC-QSS scheme*

In Sect 3.2.1, we have already discussed the $(2, n)$-threshold d-LOCC-QSS scheme, i.e., $r = 1$. Thus here we only consider the case when $r \geq 2$ and give the generalized restricted $(2, n)$-threshold d-LOCC-QSS scheme. For this scheme, the access structure is a complete multipartite graph.

S1. Alice first prepares the states, each chosen randomly from a distance-r orthogonal pair of n-qudit GHZ states, as given in Eq. (1).

S2, S3, S4 and S5 can be carried out in accordance with the same steps in Sect. 3.1.

S6. If no eavesdropper is detected, Alice announces the sequence r_k to Bob$_k$, respectively. According to Theorem 2, Bobs make use of the X-basis to measure their particles, and any two cooperating players, i.e., one from the part of A_k and the other from the part of $A_j (k \neq j)$, can perfectly distinguish the pair (1). If both are the same measurement, then the state is $|\mathrm{GHZ}\rangle$, otherwise the state is $|\mathrm{GHZ}\rangle_r$. Hence, they are also able to recover the secret.

Example 2 In this example, the access structure can be written as

$$\Gamma = \{P_1P_2, P_1P_3, P_1P_4, P_1P_5, P_1P_6, P_2P_4, P_2P_5, P_2P_6, P_3P_4, P_3P_5, P_3P_6\},$$

where the P_k is said to Bob$_k$. From the access structure, we can know that the graph of Γ is a complete tripartite one (Fig. 2).

Hence, we can give a generalized restricted (2, 6)-threshold d-LOCC-QSS scheme, which Alice prepares in the Step S1 and can be chosen randomly from the pair (2).

S6. If no eavesdropper is detected, Alice announces the sequence r_k to Bob$_k(k = 1, 2, 3, 4, 5, 6)$, respectively. Then Bobs make use of the X-basis to measure their particles, as given in Table 1. According to Table 1, we can get that any two cooperating players which are from the parts of A_k and A_j $(k \neq j,$ and $j, k \in \{0, 1, 2\})$ can perfectly distinguish the pair in the step S1. If both are the same measurement, then the state is $|\mathrm{GHZ}\rangle$, otherwise the state is $|\mathrm{GHZ}\rangle_3$. Hence, they can cooperatively reconstruct the secret.

The rest of the steps are similar to those mentioned in Sect. 3.1.

Table 1 Measurement result performed by Bob$_k$($k = 1, 2, 3, 4, 5, 6$)

	X-basis	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$
A_0	Bob$_1$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$
A_1	Bob$_2$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|1\rangle$	$\|2\rangle$	$\|0\rangle$
	Bob$_3$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|1\rangle$	$\|2\rangle$	$\|0\rangle$
A_2	Bob$_4$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|2\rangle$	$\|0\rangle$	$\|1\rangle$
	Bob$_5$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|2\rangle$	$\|0\rangle$	$\|1\rangle$
	Bob$_6$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|2\rangle$	$\|0\rangle$	$\|1\rangle$
		$\|GHZ\rangle$			$\|GHZ\rangle_3$		

4 Security analysis

It is the most important issue for the quantum communication protocol to assure its security. Then, in this following we mainly analyze the security of our scheme against four primary quantum attacks: the intercept-and-resend attack, entangle-and-measure attack, participant attack and Trojan horse attack.

4.1 Intercept-and-resend attack

In this paper, Alice mainly makes use of the decoy photon technique to check eavesdropper's attacks, in which some sample checking single photons are chosen from the X-basis and Z-basis. Suppose Eve can utilize the intercept-and-resend attack. When Alice sends those sequences $S_1'', S_2'', \ldots, S_n''$ to Bob$_1$, Bob$_2, \ldots,$ Bob$_n$, respectively, Eve intercepts all sequences and measures the particles by the X-basis and Z-basis. After that, she sends the fake particle sequences $S_1^*, S_2^*, \ldots, S_n^*$ to the players. Because the eavesdropper Eve does not know the positions of the decoy photons, she must introduce some errors. If intercept-and-resend attack does not have errors in the checking phase, then Alice can detect eavesdropping with the probability $1 - (\frac{d+1}{2d})^{nl}$. Thus, when the numbers of n and l get larger, the probability is

$$1 - \left(\frac{d+1}{2d}\right)^{nl} \approx 1.$$

Consequently, Eve's eavesdropping will be detected from the higher error rate.

4.2 Entangle-and-measure attack

In this section, we will primarily consider the entangle-and-measure attack. Assume that the eavesdropper Eve implements ancillary system to obtain the information. Suppose that Eve performs the unitary transform U_E on her particles and the auxiliary ones in the following forms,

$$U_E|k\rangle|E\rangle = \sum_{l=0}^{d-1} a_{kl}|k\rangle|e_{kl}\rangle \tag{5}$$

$$\begin{aligned}
U_E|J_j\rangle|E\rangle &= U_E\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}|k\rangle\right)|E\rangle \\
&= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}U_E(|k\rangle|E\rangle) \\
&= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}\left(\sum_{l=0}^{d-1}a_{kl}|l\rangle|e_{kl}\rangle\right) \qquad (6) \\
&= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\sum_{l=0}^{d-1}\omega^{kj}a_{kl}\left(\frac{1}{\sqrt{d}}\sum_{m=0}^{d-1}\omega^{-ml}|J_m\rangle\right)|e_{kl}\rangle \\
&= \frac{1}{d}\sum_{k=0}^{d-1}\sum_{l=0}^{d-1}\sum_{m=0}^{d-1}\omega^{kj-ml}a_{kl}|J_m\rangle|e_{kl}\rangle
\end{aligned}$$

where $|E\rangle$ is the initial state of Eve's ancillary system; $|e_{kl}\rangle$ $(k, l = 0, 1, \ldots, d-1)$ is the pure auxiliary state determined uniquely by the unitary transform U_E, and

$$\sum_{l=0}^{d-1}|a_{kl}|^2 = 1(k = 0, 1, \ldots, d-1) \tag{7}$$

In order to avoid introducing the error rate for the states, Eve has to set: $a_{kl} = 0$, where $k \neq l$ and $k, l \in \{0, 1, \ldots, d-1\}$. Therefore, Eqs. (5) and (6) can be simplified as follows:

$$U_E|k\rangle|E\rangle = a_{kk}|k\rangle|e_{kk}\rangle \tag{8}$$

$$U_E|J_j\rangle|E\rangle = \frac{1}{d}\sum_{k=0}^{d-1}\sum_{m=0}^{d-1}\omega^{k(j-m)}a_{kk}|J_m\rangle|e_{kk}\rangle \tag{9}$$

Similarly, Eve can obtain that $\sum_{k=0}^{d-1}\omega^{k(j-m)}a_{kk}|e_{kk}\rangle = 0$, where $m \in \{0, 1, \ldots, d-1\}$ and $m \neq j$. Then for any $j \in \{0, 1, \ldots, d-1\}$, we can get $d-1$ equations. According to these $d-1$ equations, we can compute that

$$a_{00}|e_{00}\rangle = a_{11}|e_{11}\rangle = \cdots = a_{d-1,d-1}|e_{d-1,d-1}\rangle. \tag{10}$$

To obtain useful information about the secret, without loss of generality, Eve uses the unitary transform U_E on the last particle of the n-qudit $|GHZ\rangle = \frac{1}{\sqrt{d}}\Big[|0, 0, \ldots, 0\rangle + |1, 1, \ldots, 1\rangle + \cdots + |d-1, d-1, \ldots, d-1\rangle\Big]$, then we can have that

$$(I^{\otimes^{n-1}} \otimes U_E)|GHZ\rangle = \frac{1}{\sqrt{d}}(a_{00}|0,0,\ldots,0\rangle|e_{00}\rangle \\ + \cdots + a_{d-1,d-1}|d-1,d-1,\ldots,d-1\rangle|e_{d-1,d-1}\rangle) \quad (11)$$

According to Eq. (10), Eq. (11) can be changed to

$$(I^{\otimes^{n-1}} \otimes U_E)|GHZ\rangle = \frac{1}{\sqrt{d}}(|0,0,\ldots,0\rangle \\ + \cdots + a_{d-1,d-1}|d-1,\ldots,d-1\rangle) \otimes (a_{00}|e_{00}\rangle) \quad (12)$$

In Eq. (12), it implies that Eve has no effect on the whole system of QSS if she wants to eavesdrop without being detected, that is, she cannot steal secret information. So the entangle-and-measure attack is unsuccessful.

4.3 Participant attack

For the QSS scheme, the participant attack is also of great importance because it is always easier and more powerful than external attack and the participants can get more useful information than a fourth eavesdropper. In the step S6, after receiving the sequence r_k, Bob$_k$ measures his particles in the sequence S''_k with the X-basis. Supposing that Bob$_1$ is a dishonest participant and gets other people's measurements by cheating, he compares his measurements with others to recover the secret. The successful probability, however, is quite small because Alice has disrupted the order of S_k with the random Π_k ($k = 1, 2 \ldots, n$) before sending these particles. Bob$_1$ does not know the position of these and guesses the probability of Π_k is $\frac{1}{m!}$. Thus, he cannot exactly distinguish any pair of the orthogonal states $|\text{GHZ}\rangle_r$ or $|\text{GHZ}\rangle$. It means that he cannot obtain any information. Therefore, the participant attack is unsuccessful.

4.4 Trojan horse attack

In this section, we will primarily consider another important attack—Trojan horse attack [34–41]. The proposed protocol used the photons that may be insecure against the two kinds of Trojan horse attacks: the delay photon attack [38] and the invisible photon attack [36,37]. In these studies, they give some ways to defeat these attacks. Therefore, we can modify our protocol slightly and make use of the similar way to overcome the Trojan horse attack. In order to prevent the delay photon attack, the participants can pick up a portion of the photons and split each particle by the technology of photon number splitter (PNS). Then, they measure the photons with the X-basis and Z-basis. If the multiphoton rate is much higher than the desired value, then the presence of the delay photon attack is detected. At that time, Alice must stop the transmission of the scheme and begin with a new set of resources. For stopping the invisible photon attack, the participants should install a wavelength optical device that filters out the invisible photons. Through this optical device, the operable photons will be allowed to come in, and the eavesdropper's invisible photons will be eliminated.

Moreover, in the proposed QSS protocol, all same photons are sent only one time to these participants. Therefore, the protocol itself can prevent the Trojan horse attack.

5 Comparison

We compare our protocol with Rahaman and Parker [23] in Table 2. The information efficiency η , see Ref. [42], is defined as $\eta = \frac{c}{q}$, where c is the total number of shared classical bits and q is the total number of particles used in the protocol.

Suppose Alice wants to choose m entangled states in form (1) and nl single photons as the secret and the checking photons. Then Alice uses $n(m+l)$ photons for sharing m-bit information among n participants. Then the information efficiency of the proposed scheme is $\frac{m}{n(m+l)}$.

In Rahaman and Parker's scheme, L GHZ states are used to share $m(< L)$ secret bits because $(L - m)$ states are used to check eavesdropping. Then the information efficiency of their scheme is $\frac{m}{nL}(L > m)$. If this efficiency is the same as that of our protocol, we will have that $l = L - m$ and it implies that the number of particles checking eavesdropping is the same in both schemes. From the point of view of resources, our scheme uses the single quantum states, but Rahaman and Parker's utilizes GHZ states. Comparison of two kinds of quantum states, obviously, it is easier to make a single quantum state than GHZ, and the cost will be lower.

In addition, Rahaman and Parker [23] proposed the restricted $(2, n)$-threshold LOCC-QSS scheme. The access structure corresponding to their scheme is a complete bipartite graph, so it is not a standard $(2, n)$-threshold scheme. In our protocol, we give the standard $(2, n)$-threshold scheme with the n-qudit GHZ states. Furthermore, we propose the generalized restricted $(2, n)$-threshold d-LOCC-QSS scheme, and the graph for the access structure is a complete multipartite one.

6 Conclusions

We have proposed here a quantum secret sharing scheme that uses an orthogonal pair of n-qudit GHZ states and local distinguishability. In the proposed protocol,

Table 2 Comparison of Rahaman and Parker's scheme [23] with our proposed one

	Rahaman and Parker's scheme	Our proposed scheme
Basic principle	Local distinguishability	Local distinguishability
Quantum state	n-qubit GHZ state	n-qudit GHZ state
Checking state	n-qubit GHZ state	Single photon
Information efficiency	$\frac{m}{nL}(L > m)$	$\frac{m}{n(m+l)}$
Specific LOCC-QSS scheme with the GHZ state	Restricted $(2, n)$-threshold	$(2, n)$-threshold scheme; Generalized restricted $(2, n)$-threshold
Graph of the access structure	Complete bipartite graph	Complete graph; complete multipartite graph

the participants use an X-basis measurement and classical communication to distinguish between the orthogonal states to reconstruct the original secret. We also presented $(2, n)$-threshold and generalized restricted $(2, n)$-threshold schemes that enable any two cooperating players from two disjoint groups to always reconstruct the secret. Comparing the scheme of Rahaman and Parker with ours, we note that their scheme has a complete bipartite graph access structure, while ours is complete multipartite. Because our scheme is the more general, its access structure contains more authorized sets. Moreover, we showed that our protocol is secure against the intercept-and-resend attack, entangle-and-measure attack, participant attack, and Trojan horse attack. Table 2 offers a summary comparison of the two schemes.

Acknowledgements We want to express our gratitude to anonymous referees for their valuable and constructive comments. This work was sponsored by the National Natural Science Foundation of China under Grant Nos. 61373150 and 61602291, and Industrial Research and Development Project of Science and Technology of Shaanxi Province under Grant No. 2013k0611.

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612 (1979)
2. Blakley, G.R.: In: Proceedings of the National Computer Conference (AFIPS, 1979), pp. 313–317 (1979)
3. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
4. Cleve, R., Gottesman, D., Lo, H.-K.: How to share a quantum secret. Phys. Rev. Lett. **83**, 648 (1999)
5. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A **61**, 042311 (2000)
6. Deng, F.G., Zhou, H.Y., Long, G.L.: Circular quantum secret sharing. J. Phys. A Math. Gen. **39**, 14089–14099 (2006)
7. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162 (1999)
8. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 052307 (2004)
9. Dehkordi, M.H., Fattahi, E.: Threshold quantum secret sharing between multiparty and multiparty using Greenberger–Horne–Zeilinger state. Quantum Inf. Process. **12**(2), 1299–1306 (2013)
10. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Tripartite quantum state sharing. Phys. Rev. Lett. **92**, 177903 (2004)
11. 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)
12. Gordon, G., Rigolin, G.: Generalized quantum-state sharing. Phys. Rev. A **73**, 062316 (2006)
13. Qin, H.W., Zhu, X.H., Dai, Y.W.: (t, n) Threshold quantum secret sharing using the phase shift operation. Quantum Inf. Process. **14**, 2997–3004 (2015)
14. Qin, H.W., Dai, Y.W.: Proactive quantum secret sharing. Quantum Inf. Process. **14**, 4237–4244 (2015)
15. Li, X.H., Zhou, P., Li, C.Y., Zhou, H.Y., Deng, F.G.: Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J. Phys. B At. Mol. Opt. Phys. **39**, 1975–1983 (2006)
16. Li, D., Xiu, X.M., GAO, Y.J.: Multiparty quantum state sharing of m-qubit state. Int. J. Mod. Phys. C **18**, 1699 (2007)
17. Zhang, Z., Liu, W., Li, C.: Quantum secret sharing based on quantum error-correcting codes. Chin. Phys. B **20**(5), 050309 (2011)
18. Hsu, L.Y., Li, C.M.: Quantum secret sharing using product states. Phys. Rev. A **71**, 022321 (2005)
19. Maitra, A., De, S.J., Paul, G., Pal, A.K.: Proposal for quantum rational secret sharing. Phys. Rev. A **92**, 022305 (2015)
20. Sarvepalli, P., Raussendorf, R.: Matroids and quantum-secret-sharing schemes. Phys. Rev. A **81**, 052333 (2010)
21. Karimipour, V., Asoudeh, M., Gheorghiu, V., Looi, S.Y., Griffiths, R.B.: Quantum secret sharing and random hopping: using single states instead of entanglement. Phys. Rev. A **92**, 030301(R) (2015)

22. Liao, C.H., Yang, C.W., Hwang, T.: Dynamic quantum secret sharing protocol based on GHZ state. Quantum Inf. Process. **13**(8), 1907–1916 (2014)
23. Rahaman, R., Parker, M.G.: Quantum scheme for secret sharing based on local distinguishability. Phys. Rev. A **91**, 022330 (2015)
24. Gheorghiu, V., Sanders, B.C.: Accessing quantum secrets via local operations and classical communication. Phys. Rev. A **88**(2), 022340 (2013)
25. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**, 044305 (2005)
26. Li, X.H., Deng, F.G., Zhou, H.Y.: Controlled teleportation of an arbitrary multi-qudit state in a general form with d-dimensional Greenberger–Horne–Zeilinger states. Chin. Phys. Lett. **24**, 1151 (2007)
27. Tavakoli, A., Herbauts, I., Zukowski, M., Bourennane, M.: Secret sharing with a single d-level quantum system. Phys. Rev. A **92**, 030302(R) (2015)
28. Qin, H., Dai, Y.: Verifiable (t, n) threshold quantum secret sharing using d-dimensional Bell state. Inf. Process. Lett. **116**(5), 351–355 (2016)
29. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
30. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with Bell states and local unitary operations. Chin. Phys. Lett. **22**, 1049 (2005)
31. Li, C.Y., Li, X.H., Deng, F.G., et al.: Efficient quantum cryptography network without entanglement and quantum memory. Chin. Phys. Lett. **23**, 2896 (2006)
32. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin. Phys. Lett. **21**, 2097 (2004)
33. Blundo, C., De Santis, A., Stinson, D.R., Vaccaro, U.: Graph decompositions and secret sharing schemes. J. Cryptol. **8**(1), 39–64 (1995)
34. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145 (2002)
35. Gisin, N., Fasel, S., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key distribution systems. Phys. Rev. A **73**, 022320 (2006)
36. Deng, F., Li, X., Zhou, H., Zhang, Z.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
37. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1), 23–25 (2006)
38. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**, 054302 (2006)
39. Lin, J., Hwang, T.: New circular quantum secret sharing for remote agents. Quantum Inf. Process. **12**(1), 685–697 (2013)
40. Lin, J., Yang, C.W., Tsai, C.W., Hwang, T.: Intercept-resend attacks on semi-quantum secret sharing and the improvements. Int. J. Theor. Phys. **52**(1), 156–162 (2013)
41. Lin, J., Yang, C.W., Hwang, T.: Quantum private comparison of equality protocol without a third party. Quantum Inf. Process. **13**(2), 239–247 (2014)
42. Yang, C.W., Hwang, T., Luo, T.: Enhancement on quantum blind signature based on two-state vector formalism. Quantum Inf. Process. **12**(1), 109–117 (2013)