Quantum Inf Process (2017) 16:64
DOI 10.1007/s11128-017-1525-y

Dynamic quantum secret sharing by using d-dimensional GHZ state

Huawang Qin[1] · **Yuewei Dai**[1]

Received: 20 January 2016 / Accepted: 8 January 2017 / Published online: 30 January 2017

Abstract Through generating the d-dimensional GHZ state in the Z-basis and measuring it in the X-basis, a dynamic quantum secret sharing scheme is proposed. In the proposed scheme, multiple participants can be added or deleted in one update period, and the shared secret does not need to be changed. The participants can be added or deleted by themselves, and the dealer does not need to be online. Compared to the existing schemes, the proposed scheme is more efficient and more practical.

Keywords Quantum secret sharing · Dynamic quantum secret sharing · d-dimensional GHZ state · Quantum cryptography

1 Introduction

"Secret sharing" can split a secret into several parts (called "shadows" or "shares") and distribute them to several participants. Then only the qualified participants can cooperate to recover the original secret. The first scheme of secret sharing was proposed by Shamir [1] in 1979. In 1999, Hillery et al. [2] combined the classical secret sharing with the quantum theory, and used the Greenberger–Horne–Zeilinger (GHZ) state to propose the fist scheme of quantum secret sharing (QSS). Since then, many kinds of QSS schemes have been proposed. Li et al. [3] proposed a QSS scheme without a trusted party, in which the participants choose their private keys and determine the final secret themselves. Yang et al. [4,5] demonstrated the verifiable QSS schemes. In their schemes, the recovered message can be verified to check whether some dishonest participants provide the fake keys. Gao [6] used the special security check procedure

✉ Huawang Qin
qin_h_w@163.com

[1] School of Automatization, Nanjing University of Science and Technology, Nanjing 210094, China

to design a secure QSS scheme, which can resist the collective eavesdropping. Chen et al. [7] designed an error-correcting QSS scheme. Its main method is the binary search and two-party Cascade protocol. Shi et al. [8] used the Chinese Remainder Theorem to improve the framework of QSS. Guo and Guo [9], Zhang et al. [10] and Sun et al. [11] proposed the QSS schemes without entanglement, and the quantum states used in these schemes are easier to be generated within the present technology. Liu et al. [12] used the symmetric W state of three qubits to propose an efficient QSS scheme, in which only a single-photon measurement and the XOR operation are needed. Lau and Weedbrook [13] used the continuous-variable cluster states to design a QSS, which can share both the classical information and the quantum state.

In a network of secret sharing, the variance of the participants is a usual problem, which has been studied widely in the classical secret sharing. But in QSS, this problem has not got enough attention, and only a few schemes have studied it. For example, Yang et al. [14] used the Lagrange interpolation to design an expansible QSS, and the "expansible" means that new participants can join the old participants. In this scheme, any t out of n old participants can generate a new shadow for a new participant. Sun et al. [15] used the operation of quantum-controlled-not to present another expansible QSS. Yang' scheme and Sun's scheme can only add participants, but cannot delete participants. Jia et al. [16] used the property of a special star-like cluster state (which is constructed by Chen et al. [17], and composed of one center qubit and n surrounding two-qubit) to design a dynamic QSS, in which the dealer can add or delete participant through the entanglement swapping. Hsu et al. [18] used the entanglement swapping on the BELL state to design another dynamic QSS.

In this paper, we will use the d-dimensional GHZ state to propose a new dynamic QSS. In our scheme, the dealer generates a d-dimensional GHZ state in the Z-basis and distributes the particles to the participants. The participants measure their particles in the X-basis and get their shadows. In the protocol of adding participants, the participants can update their shadows according to the measurement results of the d-dimensional GHZ state. In the protocol of deleting participants, the remained participants can update their shadows according to the published shadows of the removed participants. Compared to the existing schemes, our scheme has the following merits:

(1) Multiple participants can be added or deleted through one update period. So our scheme is more efficient.
(2) The participants can be added or deleted by themselves, and the dealer does not need to be online. So our scheme will be more flexible in practice.
(3) The protocol is simple and efficient, and only the single-particle measurement is needed.

The rest of this paper is organized as follows. In Sect. 2, the correlative preliminaries are introduced. Section 3 explicates the design method of the proposed scheme. In Sect. 4, an example is given to explain our scheme more clearly. Section 5 proves the correctness. Section 6 analyzes the security. Section 7 compares our scheme to some of the existing schemes. Finally, in Sect. 8, the conclusion of this paper is given.

2 Preliminaries

In the d-dimensional Hilbert space, we define the Z-basis and X-basis as follows.

$$Z = \{|j\rangle, j = 0, 1, \ldots, d-1\}, \quad X = \{|J_j\rangle, j = 0, 1, \ldots, d-1\} \tag{1}$$

where $|J_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle$ and $\omega = e^{\frac{2\pi i}{d}}$. Then the d-dimensional GHZ state in the Z-basis can be represented as

$$\Psi = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n} \tag{2}$$

If each particle in Ψ is measured in the X-basis, and we use $a_1, a_2, \ldots, a_n \in \{0, 1, \ldots, d-1\}$ to denote the measurement results $|J_j\rangle$ ($j \in \{0, 1, \ldots, d-1\}$) of the n particles, then we can obtain that

$$a_1 + a_2 + \cdots + a_n = 0 \tag{3}$$

where the symbol "+" means the add modulo d.

3 The proposed scheme

3.1 The basic scheme

We first introduce the basic scheme. The dealer Alice will share a classical secret among n participants $\{\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n\}$. The protocol is described as follows.

(1) Alice generates a d-dimensional GHZ state $\Psi = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n+1}$ in the Z-basis. When Ψ is measured in the X-basis, Alice and all the participants agree to use $a_1, a_2, \ldots, a_{n+1} \in \{0, 1, \ldots, d-1\}$ to denote the measurement results $|J_j\rangle$ ($j \in \{0, 1, \ldots, d-1\}$) of the $n+1$ particles.
(2) Alice measures one particle of Ψ in the X-basis, and we assume the measurement result is a_{n+1}. Then Alice sets the secret as $S = d - a_{n+1}$.
(3) Alice sends the rest n particles of Ψ to the n participants, each participant holds a particle. Alice uses the detecting particles to check the eavesdropping as steps (4)–(5).
(4) Alice prepares some detecting particles which are random in the Z-basis or X-basis. She inserts the transmitted particle into the detecting particles and keeps a record of the insertion position and the initial states of the detecting particles. Then Alice sends these particles to the participant.
(5) After confirming the participant has received the particles, Alice publicly announces the positions and basis of the detecting particles and asks the participant to measure these particles in the$Z$-basis or X-basis according to their basis. The participant publishes his measurement results. Alice can compute the error rate through comparing the measurement results and the initial states. If the

error rate exceeds the threshold value (according to the existing results [19–23], the error rate of one qubit caused by the noise is about from 2 to 8.9%.), Alice asks the participant to abort the process and starts a new one. Otherwise, the participant accepts the received particle.

(6) After all the participants have received the particles of Ψ, each participant measures his particle in the X-basis. We assume the measurement results of these n participants are $a_1, a_2, \ldots, a_n$. Then Bob_i $(i = 1, 2, \ldots, n)$ sets his shadow as $k_i = a_i$. According to the property of GHZ state in Sect. 2, we can know that $k_1 + k_2 + \cdots + k_n = S$, where the symbol "+" means the add modulo d. So Alice has shared the secret S among the n participants.

3.2 Add participants

We assume m participants $\{\text{Bob}_{n+1}, \text{Bob}_{n+2}, \ldots, \text{Bob}_{n+m}\}$ want to join the old n participants $\{\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n\}$. The protocol of adding participants is described as follows.

(1) The participants randomly select one participant from themselves, and we assume this selected participant is Bob_i $(i \in \{1, 2, \ldots, n+m\})$. Then Bob_i generates a d-dimensional GHZ state $\Psi' = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n+m}$ in the Z-basis.

(2) Bob_i holds one particle of Ψ'. Then he sends the rest $n + m$-1 particles to the other participants, and each participant will get a particle. Bob_i uses the detecting particles to check the eavesdropping as the steps (4)–(5) of Sect. 3.1.

(3) Every participant (including old and new participants) measures his particle in the X-basis, and we assume the measurement results are $a_1, a_2, \ldots, a_{n+m}$.

(4) The participant Bob_i $(i = 1, 2, \ldots, n + m)$ updates his shadow as $k_i' = k_i + a_i$, where the symbol "+" means the add modulo d, k_i' is his new shadow, and k_i is his old shadow (if Bob_i is a new participant, then his old shadow is 0). Then all the $n + m$ participants will share the original secret S.

3.3 Delete participants

Without loss of generality, we assume the original participants are $\{\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n\}$, and m participants $\{\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_m\}$ want to leave. The protocol of deleting participants is described as follows.

(1) Each of the m participants publishes his shadow k_i, $i \in \{1, 2, \ldots, m\}$.

(2) The remained participants randomly select one participant from themselves, and we assume this selected participant is Bob_j.

(3) Bob_j computes $k = k_1 + k_2 + \cdots + k_m$ and updates his shadow as $k_j' = k_j + k$, where the symbol "+" means the add modulo d, k_j' is his new shadow, and k_j is his old shadow. Then the remained participants can still use their shadows to share the original secret S.

In the above process, we must assume the removed participants will publish their shadows honestly. In fact, every participant should be honest in QSS scheme with the

(n, n) structure, and any dishonest participant will destroy the recovery of the secret. So our assumption is reasonable.

4 Example

In order to explain our scheme more clearly, we will give an example in the following. We assume there are four participants $\{\text{Bob}_1, \text{Bob}_2, \text{Bob}_3, \text{Bob}_4\}$, and $d = 6$. In the basic protocol, the dealer Alice generates a six-dimensional five-particle GHZ state $\Psi = \frac{1}{\sqrt{5}}(|00000\rangle + |11111\rangle + |22222\rangle + |33333\rangle + |44444\rangle + |55555\rangle)$ in the Z-basis. Ψ will be measured in the X-basis, and the measurement results $\{|J_0\rangle, |J_1\rangle, |J_2\rangle, |J_3\rangle, |J_4\rangle, |J_5\rangle\}$ are denoted as $\{0, 1, 2, 3, 4, 5\}$ respectively. Alice measures one particle of Ψ in the X-basis, and we assume the measurement result is $a_5 = 3$. Then Alice sets the secret as $S = d - a_5 = 3$. Alice sends the other four particles to the participants, and each participant gets a particle. Every participant measures his particle in the X-basis, and we assume the measurement results are $a_1 = 4$, $a_2 = 3$, $a_3 = 3$ and $a_4 = 5$. Then Bob_1 sets his shadow as $k_1 = a_1 = 4$, Bob_2 sets his shadow as $k_2 = a_2 = 3$, Bob_3 sets his shadow as $k_3 = a_3 = 3$, and Bob_4 sets his shadow as $k_4 = a_4 = 5$. We can see that $k_1 + k_2 + k_3 + k_4 = 3 = S$, where the symbol "+" means the add modulo d.

In the protocol of adding participants, we assume two participants $\{\text{Bob}_5, \text{Bob}_6\}$ want to join the original participants $\{\text{Bob}_1, \text{Bob}_2, \text{Bob}_3, \text{Bob}_4\}$. The participants randomly select one participant from themselves, and we assume this selected participant is Bob_1. Then Bob_1 generates a six-dimensional six-particle GHZ state $\Psi' = \frac{1}{\sqrt{5}}(|000000\rangle + |111111\rangle + |222222\rangle + |333333\rangle + |444444\rangle + |555555\rangle)$ in the Z-basis. Bob_1 holds one particle of Ψ' and sends the rest five particles to the other participants. Every participant measures his particle in the X-basis, and we assume the measurement results are $a_1 = 3$, $a_2 = 2$, $a_3 = 4$, $a_4 = 0$, $a_5 = 2$ and $a_6 = 1$. Then Bob_1 updates his shadow as $k_1' = k_1 + a_1 = 1$, Bob_2 updates his shadow as $k_2' = k_2 + a_2 = 5$, Bob_3 updates his shadow as $k_3' = k_3 + a_3 = 1$, Bob_4 updates his shadow as $k_4' = k_4 + a_4 = 5$, Bob_5 updates his shadow as $k_5' = k_5 + a_5 = 2$, and Bob_6 updates his shadow as $k_6' = k_6 + a_6 = 1$. We can see that $k_1' + k_2' + k_3' + k_4' + k_5' + k_6' = 3 = S$.

In the protocol of deleting participants, we assume two participants $\{\text{Bob}_1, \text{Bob}_2\}$ want to leave from the original four participants $\{\text{Bob}_1, \text{Bob}_2, \text{Bob}_3, \text{Bob}_4\}$. $\{\text{Bob}_1, \text{Bob}_2\}$ publish their shadows $k_1 = 4$, $k_2 = 3$. The remained participants randomly select one participant from themselves, and we assume this selected participant is Bob_3. Then Bob_3 computes $k = k_1 + k_2 = 1$ and updates his shadow as $k_3' = k_3 + k = 4$. Bob_4 does not change his shadow, so his shadow is $k_4' = k_4 = 5$. We can see that $k_3' + k_4' = 3 = S$.

5 Correctness

Theorem 1 *If each particle of the Z-basis GHZ state $\Psi = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n}$ is measured in the X-basis, and the measurement results $|J_j\rangle$ ($j \in \{0, 1, \ldots, d-1\}$) of the n*

particles are denoted as $a_1, a_2, \ldots, a_n \in \{0, 1, \ldots, d-1\}$, *then* $a_1+a_2+\cdots+a_n = 0$, *where "+" means the add modulo d.*

Proof We know that the Z-basis and the X-basis can be expressed as $Z = \{|j\rangle, j = 0, 1, \ldots, d-1\}$, $X = \{|J_j\rangle, j = 0, 1, \ldots, d-1\}$, where $|J_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle$ and $\omega = e^{\frac{2\pi i}{d}}$. So if Ψ is measured in the X-basis, and the measurement results are denoted as $a_1, a_2, \ldots, a_n \in \{0, 1, \ldots, d-1\}$, then Ψ can be written as

$$\Psi = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle \right)^{\otimes n} = \frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} \omega^{j \sum_{i=1}^{n} a_i} |a_1 a_2 \ldots a_n\rangle \quad (4)$$

where $a_1, a_2, \ldots, a_n \in \{0, 1, \ldots, d-1\}$.

We can see that, if $\sum_{i=1}^{n} a_i \neq 0$, that is $\omega^{\sum_{i=1}^{n} a_i} \neq 1$, then

$$\begin{aligned} \frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} \omega^{j \sum_{i=1}^{n} a_i} &= \frac{1}{(\sqrt{d})^{n+1}} \frac{1 - \omega^{d \sum_{i=1}^{n} a_i}}{1 - \omega^{\sum_{i=1}^{n} a_i}} = \frac{1}{(\sqrt{d})^{n+1}} \frac{1 - e^{\frac{2\pi i}{d} d \sum_{i=1}^{n} a_i}}{1 - e^{\frac{2\pi i}{d} \sum_{i=1}^{n} a_i}} \\ &= \frac{1}{(\sqrt{d})^{n+1}} \frac{1-1}{1 - e^{\frac{2\pi i}{d} \sum_{i=1}^{n} a_i}} = 0 \end{aligned} \quad (5)$$

If $\sum_{i=1}^{n} a_i = 0$, that is $\omega^{\sum_{i=1}^{n} a_i} = 1$, then

$$\frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} \omega^{j \sum_{i=1}^{n} a_i} = \frac{1}{(\sqrt{d})^{n-1}} \quad (6)$$

where "$\sum$" means the serial add modulo d. So in the X-basis, we can get

$$\Psi = \frac{1}{(\sqrt{d})^{n-1}} \sum_{\substack{a_1+a_2+\cdots+a_n=0 \\ a_1, a_2, \ldots, a_n \in \{0,1,\ldots,d-1\}}} |a_1 a_2 \ldots a_n\rangle \quad (7)$$

We can see the measurement results will satisfy $a_1 + a_2 + \cdots + a_n = 0$.

Lemma 1 *In the basic protocol* (Sect. 3.1), *the shared secret S satisfies* $S = k_1 + k_2 + \cdots + k_n$, *where* k_i *is the shadow of the participant* Bob_i, $i \in \{1, 2, \ldots, n\}$.

Proof We know that $k_i = a_i$ (step (6) of Sect. 3.1), so according to Theorem 1, we can get that

$$k_1 + k_2 + \cdots + k_n + a_{n+1} = 0 \quad (8)$$

Then we know

$$k_1 + k_2 + \cdots + k_n = d - a_{n+1} \quad (9)$$

where a_{n+1} is the measurement result of Alice. We know that $S = d - a_{n+1}$ (step (2) of Sect. 3.1). So

$$S = k_1 + k_2 + \cdots + k_n \tag{10}$$

Lemma 1 is proved. □

Lemma 2 *In the protocol of adding participants* (Sect. 3.2)*, the shared secret S satisfies $S = k'_1 + k'_2 + \cdots + k'_{n+m}$, where k'_i is the new shadow of the participant Bob_i, $i \in \{1, 2, \ldots, n+m\}$.*

Proof After the participants measure the particles of Ψ' and get the measurement results $a_1, a_2, \ldots, a_{n+m}$, according to Theorem 1, we can get that

$$a_1 + a_2 + \cdots + a_{n+m} = 0 \tag{11}$$

We know that $k'_i = k_i + a_i$ (step (4) of Sect. 3.2), $i \in \{1, 2, \ldots, n+m\}$. So we can get

$$\begin{aligned} k'_1 + k'_2 + \cdots + k'_{n+m} &= (k_1 + k_2 + \cdots + k_{n+m}) + (a_1 + a_2 + \cdots + a_{n+m}) \\ &= k_1 + k_2 + \cdots + k_{n+m} \end{aligned} \tag{12}$$

We also know that $k_i = 0$ when $i \in \{n+1, n+2, \ldots, n+m\}$ (step (4) of Sect. 3.2), so

$$k'_1 + k'_2 + \cdots + k'_{n+m} = k_1 + k_2 + \cdots + k_n = S \tag{13}$$

Lemma 2 is proved.

Lemma 3 *In the protocol of deleting participants* (Sect. 3.3)*, the shared secret S satisfies $S = k'_{m+1} + k'_{m+2} + \cdots + k'_n$, where k'_i ($i \in \{m+1, m+2, \ldots, n\}$) are the shadows of the remained participants.*

Proof After the m participants $\{\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_m\}$ are moved, the selected participant Bob_j ($j \in \{m+1, m+2, \ldots, n\}$) will compute $k = k_1 + k_2 + \cdots + k_m$ and update his shadow as $k'_j = k_j + k$ (step (3) of Sect. 3.3). The shadows of the other remained participants are not changed. So

$$k'_{m+1} + k'_{m+2} + \cdots + k'_n = k_1 + k_2 + \cdots + k_n = S \tag{14}$$

Lemma 3 is proved.

6 Security

6.1 Confidentiality

From the proof of Theorem 1, we can know that the Z-basis GHZ state $\Psi = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n+1}$ can be written as $\Psi = \frac{1}{(\sqrt{d})^n} \sum_{\substack{a_1+a_2+\cdots+a_{n+1}=0 \\ a_1,a_2,\ldots,a_{n+1} \in \{0,1,\ldots,d-1\}}} |a_1 a_2 \ldots a_{n+1}\rangle$ when it is measured in the X-basis. So we can see that Ψ is a maximal entangled

state when it is in the X-basis, and the probability of each particle being measured as $0, 1, \ldots, d-1$ is $\frac{1}{d}$. Without knowing the secret, the measurement result of each particle cannot be deduced from the other particles.

We assume that n-1 participants have measured their particles. Then the reduced density matrix of the last participant's particle will be

$$\rho = \sum\nolimits_{R\in\{0,1,\ldots,d-1\}} \frac{1}{d}|d-R+S\rangle\langle d-R+S| \tag{15}$$

where R is the sum of the measurement results of the n-1 participants. We can see that, without knowing the secret S, the state of the last participant's particle cannot be deduced from the measurement results of the n-1 particles. Thus, if the participants want to recover the secret, all the n participants must provide their measurement results. We can see that our scheme can meet the confidentiality.

6.2 Security of particles transmission

The security of particles transmission in our scheme is based on the detecting particles, which are random in the Z-basis or X-basis. If the eavesdropper measures the detecting particle, the probability of the eavesdropper selecting wrong basis is $\frac{1}{2}$. If the eavesdropper selects the wrong basis, the state of the detecting particle will be changed, the correct rate (that is the receiver can get the right state) is only $\frac{1}{d}$, and the error rate is $\frac{d-1}{d}$. Therefore, for one detecting particle, the error rate caused by the eavesdropping is $\frac{1}{2}\times\frac{d-1}{d}=\frac{d-1}{2d}$, which is larger than the error rate caused by the noise (2–8.9%). Therefore, the eavesdropper cannot hide his attack into the noise. For l detecting particles, the eavesdropping will be detected with the probability $1-(\frac{d+1}{2d})^l$. When l is large enough, the probability will converge to 1.

The eavesdropper can use a unitary operation U_E to entangle an ancillary particle on the transmitted particle, and then measures the ancillary particle to steal secret information. Assume that the ancillary particle is $|E\rangle$. If the detecting particle is in the Z-basis, the effect of the unitary operation U_E performed on the detecting particle can be shown as follows.

$$U_E|0\rangle|E\rangle = \alpha_{00}|0\rangle|e_{00}\rangle + \alpha_{01}|1\rangle|e_{01}\rangle + \cdots + \alpha_{0(d-1)}|d-1\rangle|e_{0(d-1)}\rangle \tag{16}$$

$$U_E|1\rangle|E\rangle = \alpha_{10}|0\rangle|e_{10}\rangle + \alpha_{11}|1\rangle|e_{11}\rangle + \cdots + \alpha_{1(d-1)}|d-1\rangle|e_{1(d-1)}\rangle \tag{17}$$

$$\cdots$$

$$U_E|d-1\rangle|E\rangle = \alpha_{(d-1)0}|0\rangle|e_{(d-1)0}\rangle + \alpha_{(d-1)1}|1\rangle|e_{(d-1)1}\rangle + \cdots + \alpha_{(d-1)(d-1)}|d-1\rangle|e_{(d-1)(d-1)}\rangle \tag{18}$$

where $|e_{ij}\rangle$ $(i, j \in \{0, 1, \ldots, d-1\})$ are the states determined by the unitary operation U_E, and

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + \cdots + |\alpha_{0(d-1)}|^2 = 1 \tag{19}$$

$$|\alpha_{10}|^2 + |\alpha_{11}|^2 + \cdots + |\alpha_{1(d-1)}|^2 = 1 \tag{20}$$

$$\cdots$$
$$|\alpha_{(d-1)0}|^2 + |\alpha_{(d-1)1}|^2 + \cdots + |\alpha_{(d-1)(d-1)}|^2 = 1 \tag{21}$$

In order to avoid the eavesdropping check, the eavesdropper has to set

$$\alpha_{01} = \alpha_{02} = \cdots = \alpha_{0(d-1)} = 0 \tag{22}$$
$$\alpha_{10} = \alpha_{12} = \cdots = \alpha_{1(d-1)} = 0 \tag{23}$$
$$\cdots$$
$$\alpha_{(d-1)0} = \alpha_{(d-1)1} = \cdots = \alpha_{(d-1)(d-2)} = 0 \tag{24}$$

Therefore, the effect of U_E performed on the detecting particle can be simplified as follows.

$$U_E|0\rangle|E\rangle = \alpha_0|0\rangle|e_0\rangle \tag{25}$$
$$U_E|1\rangle|E\rangle = \alpha_1|1\rangle|e_1\rangle \tag{26}$$
$$\cdots$$
$$U_E|d-1\rangle|E\rangle = \alpha_{d-1}|d-1\rangle|e_{d-1}\rangle \tag{27}$$

where $\alpha_0 = \alpha_{00}; \alpha_1 = \alpha_{11}; \ldots; \alpha_{d-1} = \alpha_{(d-1)(d-1)}$ and $e_0 = e_{00}; e_1 = e_{11}; \ldots; e_{d-1} = e_{(d-1)(d-1)}$.

If the detecting particle is in the X-basis, the effect of the unitary operation U_E performed on the detecting particle can be shown as follows.

$$\begin{aligned} U_E|J_j\rangle|E\rangle &= U_E\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}|k\rangle\right)|E\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}U_E|k\rangle|E\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}\alpha_k|k\rangle|e_k\rangle \end{aligned} \tag{28}$$

where $j \in \{0, 1, \ldots, d-1\}$.

We know that $|j\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{-kj}|J_k\rangle$, so

$$\begin{aligned} U_E|J_j\rangle|E\rangle &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}\alpha_k|e_k\rangle\left(\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}\omega^{-ik}|J_i\rangle\right) \\ &= \frac{1}{d}\left(|J_0\rangle\sum_{k=0}^{d-1}\omega^{k(j-0)}\alpha_k|e_k\rangle + |J_1\rangle\sum_{k=0}^{d-1}\omega^{k(j-1)}\alpha_k|e_k\rangle\right. \\ &\quad \left. + \cdots + |J_{d-1}\rangle\sum_{k=0}^{d-1}\omega^{k(j-(d-1))}\alpha_k|e_k\rangle\right) \end{aligned} \tag{29}$$

In order to avoid the eavesdropping check, the eavesdropper has to set $\sum_{k=0}^{d-1}\omega^{k(j-i)}\alpha_k|e_k\rangle = 0$, where $i \in \{0, 1, \ldots, d-1\}$ and $i \neq j$. Then for any $j \in \{0, 1, \ldots, d-$

1}, we can get d-1 equations. According to these d-1 equations, we can obtain that $\alpha_0|e_0\rangle = \alpha_1|e_1\rangle = \cdots = \alpha_{d-1}|e_{d-1}\rangle$. Therefore, no matter what the state of the useful particle is, the eavesdropper will get the same information from the ancillary particle, and cannot steal secret information. So the entangle-and-measure attack is unsuccessful.

6.3 Security for Trojan horse attack

If the particles used in our scheme are the photons, then the proposed protocol may be insecure against the two kinds of Trojan horse attacks [24,25]: the delay photon attack and the invisible photon attack. We need to modify our protocol slightly to defeat the Trojan horse attack. In order to prevent the delay photon attack, the participants should have the ability to distinguish whether there exists a multi-photon signal, that is, they must judge each received photon is a single-photon or a multi-photon. We can use the technology of PNS (photon number splitter) to realize it. The participants will randomly select a subset of the received photon signals as sample signals and split each sampling signal with a PNS. Then they measure the two signals with the Z-basis or X-basis randomly. If the multi-photon rate is unreasonably high, the transmission should be terminated and be repeated from the beginning. For stopping the invisible photon attack, the participants should add a filter before their devices. The filter only allows the photon signals whose wavelengths are close to the operating one to come in. So the eavesdropper's invisible photons will be moved out.

6.4 Security of adding or deleting participants

In our scheme, the participants can be added or deleted without the dealer. The dealer does not need to be online, and this can avoid the single-point failure (if the dealer is broken, the attacker may get the secret). So our scheme is secure in practice.

When adding participants, the selected participant generates a d-dimensional GHZ state in the Z-basis and sends the particles to the other participants, and then each participant measures his particle in the X-basis and gets his new shadow. According to the analysis of Sect. 6.1, we can know that the property of d-dimensional GHZ state can ensure the confidentiality of our scheme, and any participant cannot know the states of other participants' particles. So the old participants cannot know the states of the new participants' particles and cannot get the new participants' shadows.

When deleting participants, the selected participant updates his shadow according to the published shadows of the removed participants, and then the shadows of the removed participants will be useless.

We must assume that the selected participant is honest. In fact, every participant should be honest in QSS scheme with the (n, n) structure, and any dishonest participant can destroy the recovery of the secret. However, for a secure QSS scheme, we must guarantee that even if some participants are dishonest, they cannot get the shadows of others. According to the above analysis, we can see that our scheme can meet this requirement.

7 Comparisons

Some other schemes have studied the dynamic QSS. Yang et al. [14] used the idea of Shamir's classical secret sharing to design an expansible QSS, in which any t out of n old participants can use the Lagrange interpolation to generate a new shadow for a new participant. Sun et al. [15] designed another expansible QSS, in which the dealer can use the operation of quantum-controlled-not to distribute the shadow to the new participant. Yang' scheme and Sun's scheme can only add new participants, but cannot delete old participants. Jia et al. [16] used the property of a special star-like cluster state to design a dynamic QSS, and the dealer can add or delete participant through performing the entanglement swapping on the star-like cluster state. Hsu et al. [18] used the entanglement swapping on the BELL state to design another dynamic QSS.

In our scheme, in order to share a secret among n participants, the dealer needs to generate a d-dimensional $(n+1)$-particle GHZ state; in order to add m participants into n participants, the selected participant needs to generate a d-dimensional $(n+m)$-particle GHZ state. Without considering the detecting particles, the utilization efficiency of the particles is 100%.

In Yang's scheme, the participants need $(m+tgm)$ particles to add a new participant, where m is the bit number of shadow, t is the threshold, and g is the control parameter. In Sun's scheme, the participants need $(n+m)$ particles to add a new participant, where n is the number of the participant and m is the number of the detecting particles. In Jia's scheme, the dealer needs to generate some three-particle cluster states, in which one is used to generate the shadow and the others are used to detect the eavesdropper. In Hsu's scheme, the participants need to generate $2n$ EPR pares and some detecting particles, where n is the number of the participant. For the utilization of particles, our scheme is more efficient than Yang's, Sun's and Hsu's schemes. Jia's scheme needs fewer particles, but the cluster states are difficult to generate in practice.

In these existing schemes, only one participant can be added or deleted through one update period. If multiple participants need to be added or deleted, then the same operations must be performed repeatedly. Our scheme can add or delete multiple participants through one update period. So our scheme will be more efficient in practice.

In Sun's, Jia's and Hsu's schemes, the update operation is performed by the dealer. But in a general secret sharing scheme, the dealer will not be online after the secret has been distributed, and this can improve the security of the dealer. Therefore, Sun's, Jia's and Hsu's schemes are not practical. In our scheme and Yang's scheme, the participants can be updated by themselves, so our scheme and Yang's scheme will be more practical.

In Yang's scheme, the participants must perform many unitary operations on the particles to generate a new shadow, and the efficiency is low. In Jia's scheme, the star-like cluster state is not a general state and is difficult to generate in practice. In Hsu's scheme, the shared secret will be changed after the update of participants, and this property may influence its application in practice. Besides, Hsu's scheme and Sun's scheme need the entanglement measurement, which is inefficient compared to the single-particle measurement. Compared to these existing schemes, the protocol of our scheme is simpler and more efficient, and our scheme only needs the single-particle measurement.

8 Conclusion

In this paper, we used the d-dimensional GHZ state to propose a dynamic QSS scheme. The d-dimensional GHZ state is generated in the Z-basis and measured in the X-basis, and to generate and update the shadows. In our scheme, multiple participants can be added or deleted through one update period, and the dealer does not need to be online. Compared to the existing schemes, our scheme is more efficient and more practical.

Acknowledgements Funding was provided by NSF of China (Grant No. 61170250).

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
2. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
3. Li, Q., Long, D.Y., Chan, W.H., Qiu, D.W.: Sharing a quantum secret without a trusted party. Quantum Inf. Process. **10**, 97–106 (2011)
4. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Verifiable quantum (k, n)-threshold secret key sharing. Int. J. Theor. Phys. **50**, 792–798 (2011)
5. Yang, Y.G., Jia, X., Wang, H.Y., Zhang, H.: Verifiable quantum (k, n)-threshold secret sharing. Quantum Inf. Process. **11**, 1619–1625 (2012)
6. Gao, G.: Secure multiparty quantum secret sharing with the collective eavesdropping-check character. Quantum Inf. Process. **12**, 55–68 (2013)
7. Chen, R.K., Zhang, Y.Y., Shi, J.H., Li, F.G.: A multiparty error-correcting method for quantum secret sharing. Quantum Inf. Process. **13**, 21–31 (2014)
8. Shi, R.H., Lv, G.L., Wang, Y., Huang, D.Z., Guo, Y.: On quantum secret sharing via Chinese remainder theorem with the non-maximally entanglement state analysis. Int. J. Theor. Phys. **52**, 539–548 (2013)
9. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247–251 (2003)
10. Zhang, Z.J., Li, Y., Man, Z.X.: Multiparty quantum secret sharing. Phys. Rev. A **71**, 044301 (2005)
11. Sun, Y., Gao, F., Yuan, Z., Li, Y.B., Wen, Q.Y.: Splitting a quantum secret without the assistance of entanglements. Quantum Inf. Process. **11**, 1741–1750 (2012)
12. Liu, L.L., Tsai, C.W., Hwang, T.: Quantum secret sharing using symmetric W state. Int. J. Theor. Phys. **51**, 2291–2306 (2012)
13. Lau, H.K., Weedbrook, C.: Quantum secret sharing with continuous-variable cluster states. Phys. Rev. A **88**, 042313 (2013)
14. Yang, Y.G., Wang, Y., Chai, H.P., Teng, Y.W., Zhang, H.: Member expansion in quantum (t, n) threshold secret sharing schemes. Opt. Commun. **284**, 3479–3482 (2011)
15. Sun, Y., Xu, S.W., Chen, X.B., Niu, X.X., Yang, Y.X.: Expansible quantum secret sharing network. Quantum Inf. Process. **12**, 2877–2888 (2013)
16. Jia, H.Y., Wen, Q.Y., Gao, F., Qin, S.J., Guo, F.Z.: Dynamic quantum secret sharing. Phys. Lett. A **376**, 1035–1041 (2012)
17. Chen, Q., Chen, J., Wang, K., Du, J.: Efficient construction of two-dimensional cluster states with probabilistic quantum gates. Phys. Rev. A **73**, 012303 (2006)
18. Hsu, J.L., Chong, S.K., Hwang, T., Tsai, C.W.: Dynamic quantum secret sharing. Quantum Inf. Process. **12**, 331–344 (2013)
19. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., Zeilinger, A.: Quantum cryptography with entangled photons. Phys. Rev. Lett. **84**, 4729–4732 (2000)
20. Hughes, R.J., Nordholt, J.E., Derkacs, D., Peterson, C.G.: Practical free-space quantum key distribution over 10 km in daylight and at night. New J. Phys. **43**, 1–14 (2002)
21. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., Zbinden, H.: Quantum key distribution over 67 km with a plug&play system. New J. Phys. **41**, 1–8 (2002)
22. Beveratos, A., Brouri, R., Gacoin, T., Villing, A., Poizat, J.P., Grangier, P.: Single photon quantum cryptography. Phys. Rev. Lett. **89**, 187901 (2002)

23. Gobby, C., Yuan, Z.L., Shields, A.J.: Quantum key distribution over 122 km standard telecom fiber. Appl. Phys. Lett. **84**, 3762–3764 (2004)
24. Li, Y.B., Qin, S.J., Sun, Y., Yuan, Z., Huang, W., Sun, Y.: Quantum private comparison against decoherence noise. Quantum Inf. Process. **12**, 2191–2205 (2013)
25. Li, Y.B., Xu, S.W., Wang, Q.L., Liu, F., Wan, Z.J.: Quantum key distribution based on interferometry and interaction-free measurement. Int. J. Theor. Phys. **55**, 98–106 (2016)