Quantum Information Processing (2018) 17:244
https://doi.org/10.1007/s11128-018-1970-2

A dynamic multiparty quantum direct secret sharing based on generalized GHZ states

Yun Song[1] · Zhihui Li[2] · Yongming Li[1]

Received: 6 November 2017 / Accepted: 21 June 2018 / Published online: 7 August 2018

Abstract
This paper proposes a new dynamic multiparty quantum direct secret sharing (DQDSS) using mutually unbiased measurements based on generalized GHZ states. Without any unitary operations, an agent can obtain a shadow of the secret by simply performing a measurement on single photons. In the proposed scheme, multiple agents can be added or deleted and the shared secret need not be changed. Our DQDSS scheme has several advantages. The dealer is not required to retain any photons and can further share a predetermined key instead of a random key to the agents. Agents can update their shadows periodically, and the dealer does not need to be online. Furthermore, the proposed scheme can resist not only the existing attacks, but also cheating attacks from dishonest agents. Hence, compared to some famous DQSS schemes, the proposed scheme is more efficient and more practical. Finally, we establish a mathematical model about the efficiency and security of the scheme and perform simulation analyses with different parameters using MATLAB.

Keywords Dynamic quantum secret sharing · Generalized GHZ state · Multiparty · Security

1 Introduction

Secure multiparty computation is an important branch in modern cryptography. It focuses on the studies of secure computation among the players that do not trust each other. In quantum cryptography, it is also studied extensively as secure multiparty quantum computation (SMQC). The SMQC has been studied from two aspects: (1) the evaluation of classical function with quantum protocol and (2) the evaluation of quantum transformation. Smith [1] proposed a secure multiparty computation of

✉ Yun Song
songyun09@snnu.edu.cn

1 School of Computer Science, Shaanxi Normal University, Xi'an 710062, China

2 School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China

quantum circuit based on a verifiable quantum secret sharing protocol. Later, there were a lot of studies focus on SMQC in both the theoretical [2–5] and applied [6–8] aspects. Quantum secret sharing (QSS) is a kind of basic agreement of secure multiparty quantum computation. A QSS scheme allows a sender to share his/her secret message among several agents by using quantum mechanics in such a way that only the legitimate agents can cooperate to recover the original secret. The first QSS scheme was proposed by Hillery et al. [9] in 1999 for sharing a private key with three-particle and four-particle entangled Greenberger–Horne–Zeilinger (GHZ) state and generalized by Xiao et al. [10] into arbitrary multiparty. Subsequently, Karlsson et al. [11] proposed another QSS scheme with a two-photon polarization entangled state. Afterwards, there were a lot of studies focused on QSS protocols [12–24]. However, most of these QSS schemes do not consider the issue on the joining and deleting of agents when quanta are distributed, which is an essential requirement for all practical setups. A scheme with this feature is referred to as DQSS scheme.

In 2012, Hsu et al. [25] firstly proposed a dynamic quantum secret sharing (DQSS), in which the dealer can add or delete agents through the entanglement swapping on the Bell state. In this scheme, the shared secret will be changed after updating agents. Almost at the same time, Jia et al. [26] also proposed a DQSS scheme using the property of a special star-like cluster state (which is constructed by Chen et al. [27]). In 2013, Wang and Li [28] performed a cryptanalysis of Hsu et al.'s DQSS scheme and showed that the first and the last agents can collude with each other to reveal the sender's secret message. In 2014, Liao et al. [29] proposed a new scheme of DQSS which can resist the collusion attack and dishonest user's attack. In 2017, Qin et al. [30] used the d-dimensional GHZ state to propose a new dynamic QSS. However, all QSS schemes have four constraints: (1) the dealer is required to retain particle sequences. That is, quantum memory cannot be omitted for the dealer. (2) In order to check the security of the scheme, the dealer has to prepare checking sets and insert them into the agents' particle sequences which were previously divided. (3) The above schemes are based on the idea of sharing some sifted keys through the transmission of quantum signals between the dealer and participants. By using the sifted key, participants can encrypt or decrypt the secret messages. That is, the participants are only allowed to build a shared key using their secret shares. (4) The above schemes do not mention the issue of updating the agents' shadows periodically without changing the secret, which is very useful for resisting the mobile attacker. Thus, the mobile attacker must break enough participants within a period of updating. After an updating period, the old shadows will be useless even if they have been stolen by the attacker.

As a practical matter, it may also be the case that, sometimes, the dealer wants to share her secret directly with a group of participants, who can then collaborate together to restore her secret at a later time. Therefore, it is very important to improve the practicability of the DQSS. In this paper, we will propose a practical and efficient multiparty quantum direct secret sharing (DQDSS). We point out the properties of unbiased bases using quantum Fourier transform that has been used to design some quantum cryptographic protocols [31–34]. Then, the quantum correlation between the exclusive-OR value of all agents' possible mea-

surement results with X-basis and the original local unitary operation on the last particle of the generalized GHZ states encoded by the dealer was presented, which brought out an advantage that the dealer can directly share a predetermined secret rather than transmitting a random key to agents. Our scheme only needs to use one n-particle generalized GHZ state to share one classical bit among n agents in contrast to [25,26] that need one $(n+1)$-particle generalized GHZ state. Besides, all agents simply have to perform the measurement of single photons to get shadows without being required to generate any photons, do any local unitary operations, or transmit any classical message except in eavesdropping checks. Two approaches are employed for eavesdropping checkings. The corresponding security of the proposed scheme is presented in detail. Our scheme has the following merits:

1. The dealer can directly share a determinate secret among the participants. Therefore, our scheme is more practical than those schemes that can only share a random secret.
2. In our scheme, the dealer is not required to retain any photons, and thus quantum memory for the dealer can be omitted.
3. Rather than inserting checking sets composed of nonorthogonal states into the agents' particle sequences, the dealer only needs to prepare additional generalized GHZ states at the beginning of the scheme to detect the eavesdropping (Remark 2).
4. Agents can update their shadows periodically, and the dealer does not need to be online. After an updating period, the secret is changeless and the old shadows will be useless even if they have been stolen by an attacker.

The rest of this article is organized as follows. In Sect. 2, we review some preliminaries that are used in this article. Our DQDSS scheme is described in detail in Sect. 3. Section 4 presents the security analysis of the proposed scheme and also gives a comparison to the other DQSS schemes. Section 5 provides conclusions.

2 Mutually unbiased bases measurement for generalized GHZ states

The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states for a two-dimensional Hilbert space C^2; $\{|Z_0\rangle = 0, |Z_1\rangle = 1\}$ is called Z-basis and forms an orthonormal basis for this vector space. By performing the quantum Fourier transform, another orthonormal basis X-basis ($\{|X_0\rangle, |X_1\rangle\}$) for C^2 can be obtained as follows:

$$|X_j\rangle = F|Z_j\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} \mathrm{e}^{\frac{2\pi ijk}{2}}|Z_k\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} \mathrm{e}^{\pi ijk}|Z_k\rangle, \tag{1}$$

where $j \in \{0, 1\}$ and F is the quantum Fourier transform. Then, $|X_0\rangle$ and $|X_1\rangle$ can be computed, thanks to Eq. (1), as

$$|X_0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |X_1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Similarly, by performing the inverse quantum Fourier transform of F, both $|Z_0\rangle = 0$ and $|Z_1\rangle = 1$ can be represented by X-basis as follows:

$$|Z_j\rangle = F^{-1}|X_j\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} \mathrm{e}^{\frac{-2\pi ijk}{2}}|X_k\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} \mathrm{e}^{-\pi ijk}|X_k\rangle. \tag{2}$$

Since $|\langle|Z_j|X_k\rangle| = \frac{1}{\sqrt{2}}$ for $j, k \in \{0, 1\}$, by definition of the mutually unbiased bases [35], the X-basis and Z-basis are mutually unbiased. Moreover, we introduce generalized GHZ states, namely two maximally entangled states $|\phi_0\rangle$ and $|\phi_1\rangle$, in the n-particle Hilbert space, as shown in the following:

$$|\phi_0\rangle_{1\ldots n} = \frac{1}{\sqrt{2}}(|00\ldots0\rangle_{1,2,\ldots,n} + |11\ldots1\rangle_{1,2,\ldots,n}), \tag{3}$$

and

$$|\phi_1\rangle_{1\ldots n} = \frac{1}{\sqrt{2}}(|00\ldots0\rangle_{1,2,\ldots,n} - |11\ldots1\rangle_{1,2,\ldots,n}), \tag{4}$$

where $n \geq 2$. Note that the states are Einstein–Podolsky–Rosen (EPR) pairs when $n = 2$ and they are GHZ states when $n \geq 3$.

According to Eqs. (1) and (2), n-qudit generalized GHZ state can be represented by mutually unbiased bases (X-basis and Z-basis) as follows:

$$\begin{aligned}
|\phi_0\rangle_{1\ldots n} &= \frac{1}{\sqrt{2}}\left(|00\cdots0\rangle_{1,2,\ldots,n} + |11\cdots1\rangle_{1,2,\ldots,n}\right) \\
&= \frac{1}{\sqrt{2}}\sum_{j=0}^{1}|Z_j\rangle_1|Z_j\rangle_2\cdots|Z_j\rangle_n \\
&= \frac{1}{\sqrt{2}}\sum_{j=0}^{1}\left\{\left(\frac{1}{\sqrt{2}}\sum_{k_1=0}^{1}\mathrm{e}^{-\pi ijk_1}|X_{k_1}\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{k_2=0}^{1}\mathrm{e}^{-\pi ijk_2}|X_{k_2}\rangle\right)\right. \\
&\quad \left.\cdots\left(\frac{1}{\sqrt{2}}\sum_{k_n=0}^{1}\mathrm{e}^{-\pi ijk_n}|X_{k_n}\rangle\right)\right\} \\
&= 2^{\frac{-(n+1)}{2}}\sum_{k_1,k_2,\ldots,k_n=0}^{1}\left(\sum_{j=0}^{1}\mathrm{e}^{-\pi ij[(k_1+k_2+\cdots+k_n)(\mathrm{mod}2)]}|X_{k_1}\rangle|X_{k_2}\rangle\cdots|X_{k_n}\rangle\right) \\
&= 2^{\frac{-(n-1)}{2}}\sum_{\substack{k_1,k_2,\ldots,k_n=0 \\ k_1+k_2+\cdots+k_n=0(\mathrm{mod}2)}}^{1}|X_{k_1}\rangle|X_{k_2}\rangle\cdots|X_{k_n}\rangle,
\end{aligned} \tag{5}$$

$$
\begin{aligned}
|\phi_1\rangle_{1\ldots n} &= \frac{1}{\sqrt{2}}\left(|00\cdots0\rangle_{1,2,\ldots,n} - |11\cdots1\rangle_{1,2,\ldots,n}\right) \\
&= \frac{1}{\sqrt{2}}\left(|Z_0\rangle_1|Z_0\rangle_2\cdots|Z_0\rangle_n - |Z_1\rangle_1|Z_1\rangle_2\cdots|Z_1\rangle_n\right) \\
&= 2^{\frac{-(n+1)}{2}}\left[\left(\sum_{\substack{k_1,k_2,\ldots,k_n=0\\ k_1+k_2+\cdots+k_n=0(\mathrm{mod}2)}}^{1}|X_{k_1}\rangle|X_{k_2}\rangle\cdots|X_{k_n}\rangle\right.\right. \\
&\quad \left. + \sum_{\substack{k_1,k_2,\ldots,k_n=0\\ k_1+k_2+\cdots+k_n=1(\mathrm{mod}2)}}^{1}|X_{k_1}\rangle|X_{k_2}\rangle\cdots|X_{k_n}\rangle\right) \\
&\quad - \left(\sum_{\substack{k_1,k_2,\ldots,k_n=0\\ k_1+k_2+\cdots+k_n=0(\mathrm{mod}2)}}^{1}|X_{k_1}\rangle|X_{k_2}\rangle\cdots|X_{k_n}\rangle\right. \\
&\quad \left.\left. + \sum_{\substack{k_1,k_2,\ldots,k_n=0\\ k_1+k_2+\cdots+k_n=1(\mathrm{mod}2)}}^{1}\mathrm{e}^{-\pi i}|X_{k_1}\rangle|X_{k_2}\rangle\cdots|X_{k_n}\rangle\right)\right] \\
&= 2^{\frac{-(n-1)}{2}}\sum_{\substack{k_1,k_2,\ldots,k_n=0\\ k_1+k_2+\cdots+k_n=1(\mathrm{mod}2)}}^{1}|X_{k_1}\rangle|X_{k_2}\rangle\cdots|X_{k_n}\rangle. \qquad (6)
\end{aligned}
$$

Here, if each particle in $|\phi_0\rangle_{1\ldots n}$ ($|\phi_1\rangle_{1\ldots n}$) is measured in the X-basis, we can get the measurement results $X_{k_1}, X_{k_2}, \ldots, X_{k_n}$, where $k_i (i \in \{1, 2, \ldots, n\})$ is the i-th particle in $|\phi_0\rangle_{1\ldots n}$ ($|\phi_1\rangle_{1\ldots n}$) and X_{k_i} will be $|X_0\rangle$ or $|X_1\rangle$. If $|X_0\rangle$ represents the classical bit "0" and $|X_1\rangle$ represents the classical bit "1", then the measurement results satisfy $X_{k_1} \oplus X_{k_2} \oplus \cdots \oplus X_{k_n} = 0$ for $|\phi_0\rangle$ and $X_{k_1} \oplus X_{k_2} \oplus \cdots \oplus X_{k_n} = 1$ for $|\phi_1\rangle$, where $\oplus$ is the bitwise exclusive-OR. Equations (5) and (6) will be used later as a coding function in the proposed DQDSS.

3 The proposed DQDSS scheme

In this section, we will introduce a new DQDSS scheme under the four-party scenario and extend it to an $(n+1)$-party case. Then, we will demonstrate how to add a new agent and revoke a current agent from our scheme. Furthermore, the property of periodical updates will be pointed out at the end of this section.

3.1 The proposed DQDSS scheme using the mutually unbiased bases measurement

We first consider four-party DQDSS scheme. Suppose Alice is the dealer who wants to send a secret key S to three agents: Bob, Charlie and David. S can be recovered if and only if they cooperate. Now, let us give the detail steps in the following:

1. Alice randomly generates N three-particle GHZ entangled states, and each one is in the state $|\phi_0\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Then, she imposes secret messages by performing local unitary operations on the third particle of $|\phi_0\rangle_{123}$. If the two local unitary operations we use are $U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $U_1 = |0\rangle\langle 0| - |1\rangle\langle 1|$, then we have

$$I \otimes I \otimes U_0|\phi_0\rangle_{123} = |\phi_0\rangle_{123}, \quad I \otimes I \otimes U_1|\phi_0\rangle_{123} = |\phi_1\rangle_{123}. \tag{7}$$

   Each of the above two local unitary operations corresponds two encodings of the secret messages, respectively, i.e., U_0 to '0' and U_1 to '1'.
2. Alice takes all of the first qubits, second qubits and third qubits from each GHZ state to form three sequences S_1, S_2 and S_3, respectively. Then, she prepares three checking sets of decoy photons arbitrarily chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then randomly inserts these decoy photons into S_1 (S_2, S_3) to form S_1^* (S_2^*, S_3^*). Alice keeps a record of the insertion positions and initial states of the decoy particles and delivers S_1^*, S_2^*, S_3^* to Bob, Charlie and David, respectively.
3. After Bob, Charlie and David receive the sequences, Alice publicly announces the positions of the decoy particles and asks them to measure these particles in the Z-basis or X-basis. Bob, Charlie and David measure the decoy particles according to Alice's announcements and tell Alice their measurement results. Alice can compute the error rate through comparing the measurement results to the initial states. If the error rate is higher than the threshold determined by the channel noise, Alice cancels this protocol and restarts; otherwise, they continue to the next step.
4. After confirming that the channels are secure, Bob, Charlie and David perform X basis measurements on S_1, S_2 and S_3, respectively. They can obtain their shadows $K_1 = \{k_{11}, k_{12}, \ldots, k_{1N}\}$, $K_2 = \{k_{21}, k_{22}, \ldots, k_{2N}\}$ and $K_3 = \{k_{31}, k_{32}, \ldots, k_{3N}\}$,respectively, where $k_{ji} = 0 (1 \leq j \leq 3, 1 \leq i \leq N)$ if the measurement of the i-th particle is $|+\rangle$ and $k_{ji} = 1$ if the measurement of the i-th particle is $|-\rangle$.
5. According to Eqs. (5)–(7), we can see that $S = (j_1, j_2, \ldots, j_l, \ldots, j_N) = K_1 \oplus K_2 \oplus K_3$, where $1 \leq l \leq N$, j_l denotes the subscript of local unitary operation, which Alice acted on the third particle in Step (1) for the l-th $|\phi_0\rangle_{123}$, $j_l \in \{0, 1\}$.

Remark 1 Based on $|\phi_0\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\phi_1\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, the three-party DQDSS scheme can be constructed similarly.

It is easy to expand this DQDSS protocol to an $(n + 1)$-party DQDSS with a boss, Alice, and n agents, $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n$. Alice prepares N n-particle GHZ states in $|\phi_0\rangle_{1\ldots n} = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$. She imposes secret messages by performing

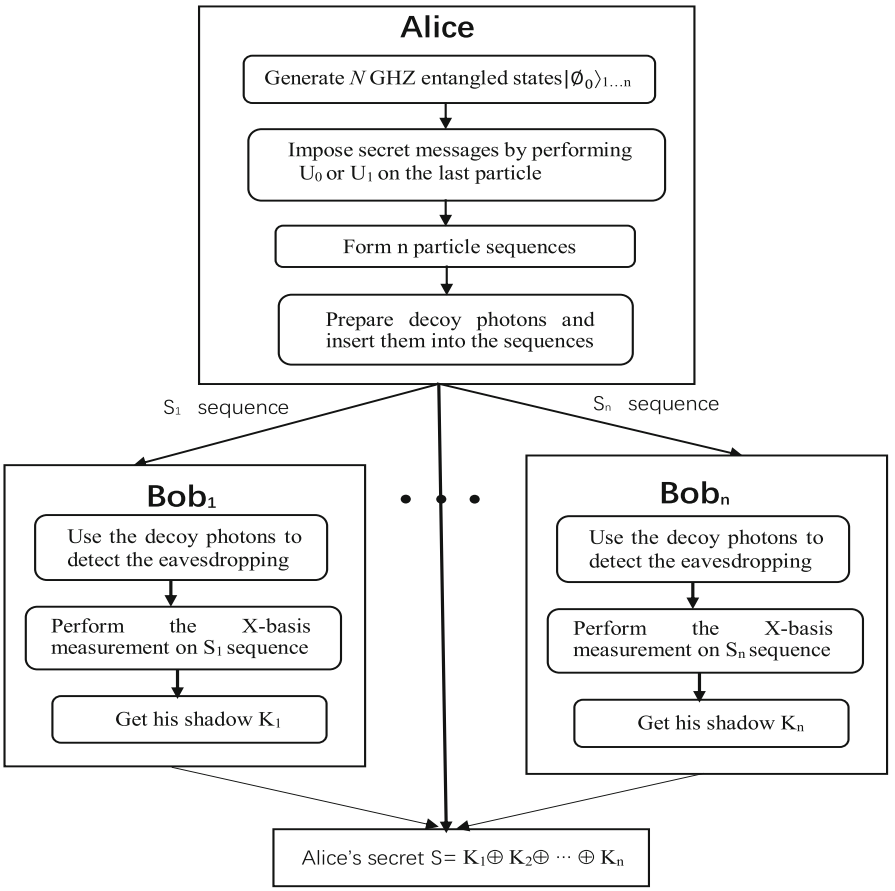

Fig. 1 Detail steps of our DQDSS scheme

local unitary operations $\{U_0, U_1\}$ on the n-th particle of $|\phi_0\rangle_{1\ldots n}$. Then, she divides these n-qubit GHZ states into n ordered sequences, $S_1, S_2, \ldots, S_n$. After that, Alice delivers these sequences to $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n$, respectively. In order to avoid eavesdropping attacks, decoy photons are used to protect each quantum transmission as described in Step (2). After the eavesdropping checks, all parties perform the X basis measurements on their particles to obtain the measurement results $K_1, K_2, \ldots, K_n$. Finally, when all agents $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n$ cooperate, they can recover Alice's secret $S = (j_1, j_2, \ldots, j_l, \ldots, j_N) = K_1 \oplus K_2 \oplus \cdots \oplus K_n$, where $1 \leq l \leq N$, j_l denotes the subscript of local unitary operation, which Alice acted on the n-th particle in Step (1) for l-th $|\phi_0\rangle_{1\ldots n}$, $j_l \in \{0, 1\}$. The basic idea of this $(n+1)$-party DQDSS is shown in Fig. 1.

Remark 2 The eavesdropping check can be executed in another way. Alice prepares $N + \sigma$ generalized GHZ states, where each of the σ GHZ states used to check the security is randomly in either $|\phi_0\rangle_{1\ldots n}$ or $|\phi_1\rangle_{1\ldots n}$, and each of the N GHZ states is in the same state $|\phi_0\rangle_{1\ldots n}$. After agents receive the sequences, Alice announces the

positions and the measurement basis from one of the mutually unbiased bases for the sample particles in each of the GHZ states without inserting any checking sets. If the corresponding measurement basis is the Z-basis, all agents should obtain the same results; otherwise, the measurement results should satisfy $\sum_{j=1}^{n} k_{ji_l} = 0(\mathrm{mod}2)$ for $|\phi_0\rangle$ and $\sum_{j=1}^{n} k_{ji_l} = 1(\mathrm{mod}2)$ for $|\phi_1\rangle$, where $k_{ji_l} = 0(1 \leq j \leq n, 1 \leq i_l \leq N, 1 \leq l \leq \sigma)$ if the measurement of the i_l-th particle is $|+\rangle$ and $k_{ji_l} = 1$ if the measurement of the i_l-th particle is $|-\rangle$.

3.2 Add a new agent

Suppose that a new agent, say Frieda, wants to join the four-party DQDSS before the distributed quanta are measured. With the help of one of the old members, Alice and Frieda execute the following steps:

1. One of the old members, suppose Bob, prepares a checking set of decoy photons arbitrarily chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then randomly inserts these decoy photons into his sequence S_1 to form $S_1^{\clubsuit}$. Bob keeps a record of the insertion positions and initial states of the decoy particles, and delivers $S_1^{\clubsuit}$ to Alice.
2. After Alice receives the sequence $S_1^{\clubsuit}$, Bob publicly announces the positions of the decoy particles and the corresponding measurement basis. Alice measures the decoy particles according to Bob's announcements and tell Bob her measurement result. Bob can compute the error rate through comparing the measurement results to the initial states. If the error rate is higher than the threshold determined by the channel noise, Bob will ask Alice to cancel this process of adding a new agent; otherwise, they continue to the next step.
3. After confirming that the channel is secure, Alice prepares a sequence of N single photons S_4 in $|0\rangle$ and performs the CNOT operations between S_1 and S_F, where each particle in S_1 is as the control qubit and the single photon $|0\rangle$ in S_F as the target qubit, and then the 3-particle GHZ state $|\phi_0\rangle_{123}$ and $|\phi_1\rangle_{123}$ will convert to a 4-particle GHZ state $|\phi_0\rangle_{123F} = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ and $|\phi_1\rangle_{123F} = \frac{1}{\sqrt{2}}(|0000\rangle - |1111\rangle)$, respectively. After that, Alice randomly inserts decoy photons arbitrarily chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ into the sequence S_1 and S_F to form $S_1^{*'}$ and S_F^*. Finally, Alice delivers $S_1^{*'}$ and S_F^* to Bob and Frieda, respectively.
4. After Bob and Frieda receive the sequence $S_1^{*'}$ and S_F^* sent from Alice, they perform the eavesdropping check to confirm the security of S_1 and S_F (similar to Step (3) in Sect. 3.1). Then, Bob, Charlie, David and Frieda perform X basis measurements on S_1, S_2, S_3 and S_F, respectively. They can obtain their shadows $K_1 = \{k_{11}, k_{12}, \ldots, k_{1N}\}$, $K_2 = \{k_{21}, k_{22}, \ldots, k_{2N}\}$, $K_3 = \{k_{31}, k_{32}, \ldots, k_{3N}\}$, and $K_4 = \{k_{41}, k_{42}, \ldots, k_{4N}\}$, respectively, where $k_{ji} = 0(1 \leq j \leq 4, 1 \leq i \leq N)$ if the measurement of the i-th particle is $|+\rangle$ and $k_{ji} = 1$ if the measurement of the i-th particle is $|-\rangle$.
5. According to Eqs. (5)–(7), we can see that $S = (j_1, j_2, \ldots, j_l, \ldots, j_N) = K_1 \oplus K_2 \oplus K_3 \oplus K_4$, where $1 \leq l \leq N$, j_l denotes the subscript of local unitary operation which Alice acted on the third particle in Step (1) in Sect. 3.1 for l-th $|\phi_0\rangle_{123}$, $j_l \in \{0, 1\}$.

3.3 Revoke an agent

Suppose that Alice wants to revoke an agent, say David, before the distributed quanta are measured in our four-party DQDSS scheme. Alice and David will perform the following steps:

1. Upon the request from Alice, David randomly inserts enough decoy photons into his sequence S_3 to form S_3' and sends S_3' back to Alice.
2. After Alice receives the sequence S_3' sent from David, David and Alice perform the eavesdropping check to confirm the security of S_3 [similar to Step (3) in Sect. 3.1].
3. To check the correctness of the sequence S_3, Alice randomly selects enough check positions in S_3 and then announces these positions to Bob and Charlie. After that, Bob and Charlie take out the corresponding check photons in S_1 and S_2 to form S_{C1} and S_{C2} and then randomly insert enough decoy photons into their sequences, respectively. The new sequences are denoted as S_{C1}^* and S_{C2}^*, which are delivered to Alice through quantum channel.
4. After the eavesdropping check [similar to Step (3) in Sect. 3.1], Alice receives S_{C1} and S_{C2} from Bob and Charlie. Then she performs the X-basis measurements on S_{C1}, S_{C2} and S_{C3} to check the correctness of S_3 from David.
5. After verifying the correctness of S_3 successfully, she prepares two-particle generalized GHZ entangled states for the checking positions. According to Remark 1, Alice makes Bob and Charlie obtain the components of their secret shadows in checking positions of S_1 and S_2, denoted as K_{C1} and K_{C2}, respectively, which form partial components of the secret from Alice. Then Alice, Bob and Charlie perform X-basis measurements on the remaining qubits in S_3, S_1 and S_2 to obtain the measurement results K_{R3}, K_{R1} and K_{R2}, and Alice announces K_{R3}. Finally, Bob and Charlie can recover the remaining components of the secret by computing $K_{R1} \oplus K_{R2} \oplus K_{R3}$.

3.4 Updating

Suppose that there is an $(n+1)$-party DQDSS with a boss, Alice, and n agents, $\text{Bob}_1, \text{Bob}_2 \ldots, \text{Bob}_n$. They can use the following steps to update their shadows.

1. In the first updating period, Bob_1 randomly generates N generalized GHZ entangled states and each one is in the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$. He divides these n-qubit generalized GHZ states into n ordered sequences, $S_{U1}, S_{U2}, \ldots, S_{Un}$. Then Bob_1 keeps the sequence S_{U1} himself and sends the sequence S_{U2} to Bob_2. This process is similar to the Steps (2), (3) in Sect. 3.1.
2. Bob_2 measures his particles in S_{U2} using the X-basis and gets the binary number $U_2 = (u_{21}, u_{22}, \ldots, u_{2N})$. This process is similar to Step (4) in Sect. 3.1. Then Bob_2 computes $K_2' = K_2 \oplus U_2$ and updates his shadow.
3. Similarly, Bob_1 sends the sequence S_{U3} to Bob_3. Bob_3 measures his particles in S_{U3} using the X-basis and updates his shadow K_3. This process is continued until Bob_n.
4. Bob_1 measures his particles in S_{U1} using the X-basis and updates his shadow K_1.

5. Once the above steps are completed, the first updating period is over. When the second updating period starts, Bob_2 does the similar operations as Bob_1. The other updating can be performed periodically in the similar way.

Theorem 1 *After the updating of shadows, the secret S satisfied* $S = K_1' \oplus K_2' \oplus \cdots K_n'$, *where* K_i' *is the new shadow of the agent* Bob_i, $i \in \{1, 2, \ldots, n\}$.

Proof Assume that $K_1, K_2, \ldots, K_n$ are the old shadows of $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n$. After the first updating period, their shadows will become as follows

$$K_1' = K_1 \oplus U_1, K_2' = K_2 \oplus U_2, \ldots, K_n' = K_n \oplus U_n.$$

According to the updating process and the property of the generalized GHZ state, we can get that $U_1 = U_2 \oplus U_3 \oplus \cdots \oplus U_n$. So

$$\begin{aligned} K_1' \oplus K_2' \oplus \cdots K_n' &= (K_1 \oplus U_1) \oplus (K_2 \oplus U_2) \oplus \cdots \oplus (K_n \oplus U_n) \\ &= (K_1 \oplus U_2 \oplus U_3 \oplus \cdots \oplus U_n) \oplus (K_2 \oplus U_2) \oplus \cdots \oplus (K_n \oplus U_n) \\ &= K_1 \oplus K_2 \oplus \cdots \oplus K_n = S. \end{aligned} \tag{8}$$

The above suffices to show that the secret is changeless after the first updating period. Since the other updating periods are similar to the first one, we can know that the secret is unchanged after the updating and that the Theorem is proved. □

Example In order to specify the updating process more clearly, we will give an example as follows. We assume that the dealer Alice wants to share a 2-bit '01' secret S among three agents Bob, Charlie and David. Without loss of generality, we assume that $K_1 = 01$, $K_2 = 10$ and $K_3 = 10$ after executing the five steps in Sect. 3.1. We can know that Bob, Charlie and David can recover the secret S by computing $K_1 \oplus K_2 \oplus K_3$. In an updating period, Bob_1 generates two GHZ entangled states $|\phi_{01}'\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|\phi_{02}'\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, and then uses the first particles of $|\phi_{01}'\rangle$ and $|\phi_{02}'\rangle$ to compose the sequence S_{U1}, the second particles to compose the sequence S_{U2} and the third particles to compose the sequence S_{U3}, Then he keeps the sequence S_{U1} himself and S_{U2}, S_{U3} to Charlie and David, respectively. After that, all of them perform the X-basis measurement on S_{U1}, S_{U2} and S_{U3} to get U_1, U_2, and U_3, respectively. We assume $U_1 = 11$, $U_2 = 01$, and $U_3 = 10$. finally, they can update their shadows through computing $K_1' = K_1 \oplus U_1 = 01 \oplus 11 = 10$, $K_2' = K_2 \oplus U_2 = 10 \oplus 01 = 11$ and $K_3' = K_3 \oplus U_3 = 10 \oplus 10 = 00$. We can see that the secret S is not changed after the updating.

4 Analysis of the proposed scheme

4.1 Security analysis

Now we will prove that the present scheme is secure. As mentioned in [30], if a QSS scheme is secure for a dishonest agent, then it is secure for any outside eavesdropper,

because he knows partial information legally and can tell a lie at the stage of eavesdropping detection to try to avoid introducing errors. Thus, our main goal for the security of the proposed DQDSS scheme is to prevent dishonest agents from deception. In the following, for the two approaches employed to check eavesdropping, we will analyze the intercept-and-attack, entangle-and-measure attack, collusion attack, Trojan horse attack, the honest check of added or revoked agents and the security under a noisy quantum channel, against the proposed scheme.

4.1.1 The security of the scheme against the intercept-and-resend attack

Suppose that there are dishonest agents who can intercept the particle sequences sent by Alice and resend other forged particles prepared by themselves in hope to pass the eavesdropping. Therefore, they can obtain the initial particle sequences S_i $(i = 1, 2, 3)$ and then they intend to get the information of Alice. But according to the two ways for eavesdropping check, Alice inserts randomly k samples in each transmitted sequences, requires the agents to measure them later, and checks their measurement results. In fact, if the dishonest agent starts an intercept-resend attack, he cannot know the position, basis and value of each decoy particle. Since each decoy particle is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, the successful probability is less than $\left(\frac{1}{4}\right)^k$, where k is the number of the decoy particles in each sequences transmitted to other agents.

4.1.2 The security of the scheme against the entangle-and-measure attack

Here we consider a more complicated eavesdropping attack by a dishonest agent who is able to prepare an ancilla and entangle the ancilla to gain information about the secret without the help of other agents.

In this kind of attack, for the first way of checking eavesdroppings, since the dishonest agent does not know the positions and states of the decoy photons in the intercepted sequences, the dishonest agent then prepares some ancillas $E = (|E_1\rangle, |E_2\rangle, \ldots)$, entangles these ancillas with the intercepted sequences using a unitary operation U_E, and measures the ancillary particles to steal secret information. The effect of the unitary operation U_E performed on the decoy particle is shown as follows.

$$U_E|0\rangle|E_i\rangle = \alpha|0\rangle|\varepsilon_0\rangle + \beta|1\rangle|\varepsilon_1\rangle, \tag{9}$$

$$U_E|1\rangle|E_i\rangle = \eta|0\rangle|\varepsilon_0'\rangle + \gamma|1\rangle|\varepsilon_1'\rangle, \tag{10}$$

$$\begin{aligned} U_E|+\rangle|E_i\rangle &= \frac{1}{\sqrt{2}}\left(\alpha|0\rangle|\varepsilon_0\rangle + \beta|1\rangle|\varepsilon_1\rangle + \eta|0\rangle|\varepsilon_0'\rangle + \gamma|1\rangle|\varepsilon_1'\rangle\right) \\ &= \frac{1}{2}[|+\rangle(\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle + \eta|\varepsilon_0'\rangle + \gamma|\varepsilon_1'\rangle) \\ &\quad + |-\rangle(\alpha|\varepsilon_0\rangle - \beta|\varepsilon_1\rangle + \eta|\varepsilon_0'\rangle - \gamma|\varepsilon_1'\rangle)], \end{aligned} \tag{11}$$

$$U_E|-\rangle|E_i\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle|\varepsilon_0\rangle + \beta|1\rangle|\varepsilon_1\rangle - \eta|0\rangle|\varepsilon_0'\rangle - \gamma|1\rangle|\varepsilon_1'\rangle)$$

$$= \frac{1}{2}[|+\rangle(\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle - \eta|\varepsilon_0'\rangle - \gamma|\varepsilon_1'\rangle) + |-\rangle(\alpha|\varepsilon_0\rangle - \beta|\varepsilon_1\rangle - \eta|\varepsilon_0'\rangle + \gamma|\varepsilon_1'\rangle)], \tag{12}$$

where $U_E\hat{U_E} = \hat{U_E}U_E = I$; $|\alpha^2| + |\beta^2| = |\eta^2| + |\gamma^2| = 1$; $|E_i\rangle$ is the initial state of Bob's ancilla and $\{|\varepsilon_0\rangle, |\varepsilon_1\rangle, |\varepsilon_0'\rangle, |\varepsilon_1'\rangle\}$ are the pure ancilla's states determined uniquely by the unitary operation U_E, i.e.,

$$\alpha^2 \langle\varepsilon_0|\varepsilon_0\rangle + \beta^2 \langle\varepsilon_1|\varepsilon_1\rangle = 1, \quad \eta^2 \langle\varepsilon_0'|\varepsilon_0'\rangle + \gamma^2 \langle\varepsilon_1'|\varepsilon_1'\rangle = 1,$$
$$\alpha\beta \langle\varepsilon_1|\varepsilon_0\rangle + \eta\gamma \langle\varepsilon_1'|\varepsilon_0'\rangle = 1, \quad \alpha\beta \langle\varepsilon_0'|\varepsilon_0'\rangle + \eta\gamma \langle\varepsilon_1'|\varepsilon_1'\rangle = 1.$$

Obviously, the effect of Bob's eavesdropping will introduce an error rate for every decoy photon in the stage of the honest check.

$$P_0 = \alpha^2 \langle\varepsilon_0|\varepsilon_0\rangle = 1 - \beta^2 \langle\varepsilon_1|\varepsilon_1\rangle, \tag{13}$$
$$P_1 = \eta^2 \langle\varepsilon_0'|\varepsilon_0'\rangle = 1 - \gamma^2 \langle\varepsilon_1'|\varepsilon_1'\rangle, \tag{14}$$
$$P_+ = \frac{1}{2}\left(1 + \alpha\eta \langle\varepsilon_0|\varepsilon_0'\rangle + \beta\gamma \langle\varepsilon_1|\varepsilon_1'\rangle + \alpha\gamma \langle\varepsilon_0|\varepsilon_1'\rangle + \beta\eta \langle\varepsilon_1|\varepsilon_0'\rangle\right), \tag{15}$$
$$P_- = \frac{1}{2}\left(1 - \alpha\eta \langle\varepsilon_0|\varepsilon_0'\rangle - \beta\gamma \langle\varepsilon_1|\varepsilon_1'\rangle + \alpha\gamma \langle\varepsilon_0|\varepsilon_1'\rangle + \beta\eta \langle\varepsilon_1|\varepsilon_0'\rangle\right). \tag{16}$$

If Bob wants to achieve the eavesdropping without being detected in the stage of the honest check, the rates P_0, P_1, P_+, P_- have to equal to 1. Therefore, the following equations must be satisfied:

$$\beta^2 \langle\varepsilon_1|\varepsilon_1\rangle = \eta^2 \langle\varepsilon_0'|\varepsilon_0'\rangle = 0, \alpha^2 \langle\varepsilon_0|\varepsilon_0\rangle = \gamma^2 \langle\varepsilon_1'|\varepsilon_1'\rangle = 1,$$
$$\alpha\gamma \langle\varepsilon_0|\varepsilon_1'\rangle = 1. \tag{17}$$

Equation (17) implies that $\alpha|\varepsilon_0\rangle = \gamma|\varepsilon_1'\rangle$. Obviously, Bob cannot distinguish $\alpha|\varepsilon_0\rangle$ from $\gamma|\varepsilon_1'\rangle$ and cannot obtain useful information from the ancillary particles. So the entangle-and-measure attack is unsuccessful.

From another point of view, we will analyze that our scheme can resist an entangle-and-measure attack from the dishonest agent considered in Remark 2 (i.e., without inserting any checking sets to detect eavesdropping). The dishonest agent prepares ancillas $E = \{|\varepsilon_0\rangle, |\varepsilon_1\rangle\}$ and entangles these ancillas with $|\phi_0\rangle$ and $|\phi_1\rangle$ by performing a unitary operation U hoping that he can pass the eavesdropping check among honest agents and derive useful information about the honest agents'shadow. However, taking $|\phi_0\rangle$ as an example, the effect of the dishonest agent's operation on the generalized GHZ states will produce the following results:

$$\hat{U}|\phi_0\rangle|E\rangle = |\phi_0'\rangle = \sum_{j=0}^{1} a_j |Z_j\rangle_1 |Z_j\rangle_2 \cdots |Z_j\rangle_n \otimes |\varepsilon_j\rangle, \tag{18}$$

where the coefficients a_j satisfy $\sum_{j=0}^{1} a_j^* a_j = 1$.

According to Remark 2, if no eavesdropping exists, all agents' measurement outcomes should be the same with Z-basis. So we have

$$|\phi_0'\rangle = \sum_{j=0}^{1} |j\rangle|j\rangle\cdots|j\rangle \otimes |\varepsilon_j\rangle. \tag{19}$$

Furthermore, $|\phi_0'\rangle$ can be represented by X-basis as follows:

$$\begin{aligned}|\phi_0'\rangle &= 2^{-n/2}\sum_{j=0}^{1}\sum_{k_1,k_2,\ldots,k_n=0}^{1} a_j e^{-\pi i j(k_1+k_2+\cdots+k_n)}|X_{k_1}\rangle|X_{k2}\rangle\cdots|X_{k_n}\rangle\otimes|\varepsilon_j\rangle \\ &= 2^{-n/2}\sum_{k_1,k_2,\ldots,k_n=0}^{1}\left\{|X_{k_1}\rangle|X_{k2}\rangle\cdots|X_{k_n}\rangle\otimes\sum_{j=0}^{1} a_j e^{-\pi i j(k_1+k_2+\cdots+k_n)}|\varepsilon_j\rangle\right\}.\end{aligned} \tag{20}$$

In order to avoid the eavesdropping check, the dishonest agent has to set

$$2^{-n/2}\sum_{\substack{k_1,k_2,\ldots,k_n=0\\ k_1+k_2+\cdots+k_n=1(\mathrm{mod}2)}}^{1}\left\{|X_{k_1}\rangle|X_{k2}\rangle\cdots|X_{k_n}\rangle\otimes\sum_{j=0}^{1} a_j e^{-\pi i j(k_1+k_2+\cdots+k_n)}|\varepsilon_j\rangle\right\} = 0. \tag{21}$$

Then

$$2^{-n/2}\sum_{\substack{k_1,k_2,\ldots,k_n=0\\ k_1+k_2+\cdots+k_n=1(\mathrm{mod}2)}}^{1}\{|X_{k_1}\rangle|X_{k2}\rangle\cdots|X_{k_n}\rangle\otimes(a_0|\varepsilon_0\rangle - a_1|\varepsilon\rangle\} = 0. \tag{22}$$

That is

$$a_0|\varepsilon_0\rangle - a_1|\varepsilon\rangle = 0, \quad a_0|\varepsilon_0\rangle = a_1|\varepsilon\rangle. \tag{23}$$

In terms of Eq. (23) and $\sum_{j=0}^{1} a_j^* a_j = 1$, Eq. (19) can be written as

$$|\phi_0'\rangle = \left(\frac{1}{\sqrt{2}}\sum_{j=0}^{1}|j\rangle|j\rangle\cdots|j\rangle\right)\otimes|\varepsilon_0\rangle = |\phi_0\rangle\otimes|\varepsilon_0\rangle. \tag{24}$$

It can be seen that $|\phi_0'\rangle$ is a product of a GHZ state and the ancilla. The density operator of the ancilla is $\rho_E = tr_{|\phi_0'\rangle}(|\phi_0'\rangle|\varepsilon_0\rangle\langle\varepsilon_0|\langle\phi_0'|) = |\varepsilon_0\rangle\langle\varepsilon_0|tr_{|\phi_0'\rangle}(|\phi_0'\rangle\langle\varepsilon_0|) = |\varepsilon_0\rangle\langle\varepsilon_0|$. Thus, von Neumann entropy $S(\rho_E) = 0$, which implies that the dishonest agent will gain no information about the secret from Alice by observing the ancilla.

Conversely, if gaining information about the secret, the dishonest agent will invariably introduce errors.

4.1.3 The security of the scheme against the collusion attack

Furthermore, there may be two or more dishonest agents, and they can collude to perform an attack (i.e., the collusion attack). For example, suppose that Bob is honest and other two agents, Charlie and David, are dishonest, that is, Charlie and David try to collude to perform an attack to obtain the shared secret without the help of Bob. However, since the dealer in the proposed DQDSS scheme distributes all photons to the agents without preserving anything, $k_1 \oplus k_2 \oplus k_3$ is not known to two agents Charlie and David, i.e., they do not obtain any information about secret. That is, our DQDSS protocol is still secure against the collusion attack by two or more dishonest agents (as long as there is an honest agent).

4.1.4 Security for Trojan horse attack

According to [30], if the particles used in the QSS are the photons, then the proposed protocol may be insecure against the two kinds of Trojan horse attacks: the delay photon attack and the invisible photon attack. In order to prevent delay photon attack, the agents have to introduce a special quantum device that filters out the spy photons whose wavelength is close to the legitimate one. Furthermore, each agent will have to take a portion of the received photons as sample signals and splits each particle by a photon number splitter (PNS). Then they measure the two signals with the base $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly. If there is an unreasonably high rate of multiphoton signal, then the existence of a Trojan horse attack is detected. 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 filtered out.

4.1.5 Security of adding or deleting participants

In the proposed scheme, the agents can be added or deleted and the shared secret need not be changed. When adding agents, the boss, Alice, generates a GHZ state in the Z-basis and sends the particles to agents, and then each agent measures his particle in the X-basis and gets his shadows. Besides, the property of GHZ state can ensure the confidentiality of our scheme, and any agents cannot know the states of the new agents' particles. So the old agents cannot know the states of the new agents' particles and cannot get the new agents' shadows. In the revocation process, Alice asks a revoked agent to send his/her qubits back to her. Then, she randomly chooses enough check positions to perform the X-basis measurements and request the other agents to deliver the X-basis measurement results in the corresponding check positions by quantum signals, respectively. According to these measurement results, Alice can check the correctness of the revoked agent's qubits. If the check result is positive, the shadows of removed agents will be useless. Otherwise, Alice asks other agents to abort the process and starts a new one.

4.1.6 Security under a noisy channel

In the above-mentioned analysis, we assume that the quantum channel is ideal. That is, the quantum channel is noiseless. However, in practice, due to the fluctuation of the birefringence of the optical fiber, the quantum channel is imperfect (i.e., photons tend to suffer from noises in the quantum channel). In the following, we analyze the security of the proposed scheme in the noisy quantum channel.

Eve intercepts the photons transmitted from Alice to Bob (Charlie, David), performs intercept-and-resend attack or entangle-and-measure attack, and then sends theses intercepted photons to Bob through an ideal channel established by herself. Eve may attempt to hide her attack in the noise on the quantum channel. Suppose that the quantum bit error rate (QBER) caused by the channel noise τ is approximately between 2 and 8.9% [36–39]. It is clear that the attack will not be detected if the eavesdropper detection rate of our protocols is smaller than τ. However, the eavesdropper detection rate of our protocol is 25%, which is obviously larger than τ. Hence, even in a noisy channel the present protocol works securely also.

4.2 Efficiency analysis

In this section, we compare the qubit efficiency of several existing DQSS schemes [25,26,29,30] with our scheme. According to [40], a method $\eta_q = \frac{q_u}{q_t}$ has been used to evaluate the qubit efficiency, where q_u denotes the useful qubits (i.e., the qubits used for creating the master key and the shadow keys), q_t denotes the total number of transmitted qubits (except the number of decoy photons). Thus, except a few particles which used to check the security of quantum channel, all of the above schemes can achieve a maximum value of 100%.

Another qubit efficiency η of a quantum protocol is defined as $\eta_E = \frac{q_s}{q_g}$, where q_s denotes the bit length of the dealer's master key, and q_g is the total number of generated particles. This definition underlines each photon's contribution in average to the shared key in the scheme. Suppose that the decoy photons account for fifty percent of every quantum channel to each agent. We consider the n-party QSS scenario, i.e., $n-1$ agents share $2N$ or N bits of classical secret from the dealer.

In Jia et al.'s scheme [26], to share N bits of classical secret, Alice must prepare nN star-like cluster states (i.e., $(2n-1)N$ qubits), and each cluster state can be used to share N-bit classical secret. Since half of star-like cluster states are used for eavesdropping check, the qubit efficiency of Jia et al.'s scheme is $\frac{1}{4n-2}$ (i.e., $\frac{N}{2(n-1)N} \times \frac{1}{2} = \frac{1}{4n-2}$). In Hsu et al.'s scheme [25], since $2nN$ EPR pairs have been prepared by the dealer for secret sharing and $2nN$ EPR pairs are used for eavesdropping check, the qubit efficiency of our scheme can be expressed as $\frac{1}{2n}$ (i.e., $\frac{2N}{2nN} \times \frac{1}{2} = \frac{1}{2n}$). Liao et al.'s scheme [29] and Qin et al.'s scheme [30] require the dealer generate N n-particle GHZ states and N $n-1$ decoy photons to share N-bit classical secret. Hence, the qubit efficiency of Liao et al.'s scheme is $\frac{1}{2n-1}$ (i.e., $\frac{N}{nN+(n-1)N} = \frac{1}{2n-1}$). For the proposed DQSS scheme, since N $(n-1)$-particle generalized GHZ states have been prepared by the dealer for secret sharing and $(n-1)N$ decoy photons are used for eavesdropping check, the qubit efficiency of our scheme can be expressed as $\frac{1}{2n-2}$

Table 1 Comparisons among the schemes in [25,26,29,30] and our scheme

Issue/scheme	[26]	[25]	[29]	[30]	Our scheme
Quantum state	Star-like cluster	Bell state	GHZ state	GHZ state	Generalized GHZ state
Qubit efficiency (n-party DQSS)	$\frac{1}{4n-2}$	$\frac{1}{2n}$	$\frac{1}{2n-1}$	$\frac{1}{2n-1}$	$\frac{1}{2n-2}$
Qubit efficiency (3-party DQSS)	10%	16.67%	20%	20%	25%
Qubit generation for agents	No	Yes	No	No	No
Prepare qubits for adding an agent	Linear cluster state	Two Bell states	Single photon	4-Particle GHZ state	Single photon
	(3 Qubits)	(4 Qubits)	(1 Qubit)	(4 Qubits)	(1 Qubit)
The scheme is a multiparty DQDSS	No	No	No	No	Yes
The dealer need not retain photons	No	No	No	No	Yes
Features	Only dynamic	Only dynamic	Only dynamic	Only dynamic	Dynamic and updated periodically

(i.e., $\frac{N}{(n-1)N} \times \frac{1}{2} = \frac{1}{2n-2}$). Table 1 shows the efficiency and performance comparison of the proposed protocol with the previous ones. It can be seen that the efficiency of the proposed protocol is higher than these four important multiparty DQSS schemes and that the performance advantage of our scheme is clear.

4.3 Security and efficiency model based on quantum information theory

In this section, we analyze the security of the present scheme by quantum information theory. Then we establish a mathematical model about the efficiency and security and perform simulation analyses with different parameters using MATLAB.

Because each photon is in the maximal mixed state, any measurement performed on the system of photo by Eve cannot distinguish quantum states. If Eve intervene, the particles will be entangled into Eve's ancilla and it knows that the GHZ state $|\xi\rangle$ becomes a mixed state ρ. According to [41], the information that the agent Bob can gain from ρ is bounded by the Holevo quantity $\chi(\rho)$ [42]. Let I_{Eve} denote the information Eve can obtain, then $I_{\text{Eve}} \leq \chi(\rho)$. (Obviously, Eve cannot gain more information about Bob's measurement result than Bob.) From

$$\chi(\rho) = S(\rho) - \sum_i p_i S(\rho_i), \tag{25}$$

we know $S(\rho)$ is the upper bound of $\chi(\rho)$. According to [43], $F(|\xi\rangle, \rho)^2 = \langle\xi|\rho|\xi\rangle = 1-r$, where $F(|\xi\rangle, \rho)$ is the fidelity [44] of the state $|\xi\rangle$ and $\rho, 0 \leq r \leq 1$. Therefore,the

entropy of ρ is bounded above by the entropy of a diagonal density matrix $\rho_{\max}$ with diagonal entries $1-r, 3/r, 3/r, 3/r$. The entropy of $\rho_{\max}$ is

$$S(\rho_{\max}) = -(1-r)\log_2(1-r) - r\log_2\frac{r}{3}. \tag{26}$$

From Eqs. (25) and (26), we can obtain

$$I_{\text{Eve}} \leq -(1-r)\log_2(1-r) - r\log_2\frac{r}{3}. \tag{27}$$

Let ω denote the probability of Eve introducing an error. When Alice detects eavesdropping, only $|\xi\rangle$ is the correct result, whereas any other Bell state will be regarded as an error. Since $F(|\xi\rangle, \rho)^2 = 1-r$, the detection probability $\omega = r$. From Eq. (27), we get

$$I_{\text{Eve}} \leq -(1-\omega)\log_2(1-\omega) - \omega\log_2\frac{\omega}{3}. \tag{28}$$

By the efficiency definition η_q in Sect. 4.2, we can get

$$\eta = \frac{6n - p\cdot 6n}{6n}. \tag{29}$$

where n is the number of generalized GHZ states prepared by Alice and p is the proportion of eavesdropping particles. Besides, let f denote the probability of Eve being found, and then we have

$$f = 1-(1-\omega)^{6pn}. \tag{30}$$

From Eqs. (28)–(30), we can obtain the following model equations about the efficiency and security of the proposed scheme:

$$\begin{cases} I_{\text{Eve}} \leq -(1-\omega)\log_2(1-\omega) - \omega\log_2\frac{\omega}{3} \\ \eta = \frac{6n-p\cdot 6n}{6n} \\ f = 1-(1-\omega)^{6pn} \end{cases} \tag{31}$$

Let $n = 1$ for convenience. We perform simulation analyses with different parameters using MATLAB. The results of the simulation analyses are shown in Figs. 2 and 3.

It can be seen from Fig. 2 that if Eve gain more information, the probability of Eve being found will increase. Besides, Eve has to face a higher risk of being detected along with the proportion of eavesdropping particles increasing. The relation indicates that when $\omega = 0$, i.e., Eve introduces no error to the key, she will obtain no information, which is in agreement with the above result. When $\omega > 0$, i.e., Eve can gain some of Bob's information, but she has to face a nonzero risk $\omega = r$ of being detected. When $I_{\text{Eve}} = 2$, Eve has the chance to eavesdrop on all of Bob's information, which

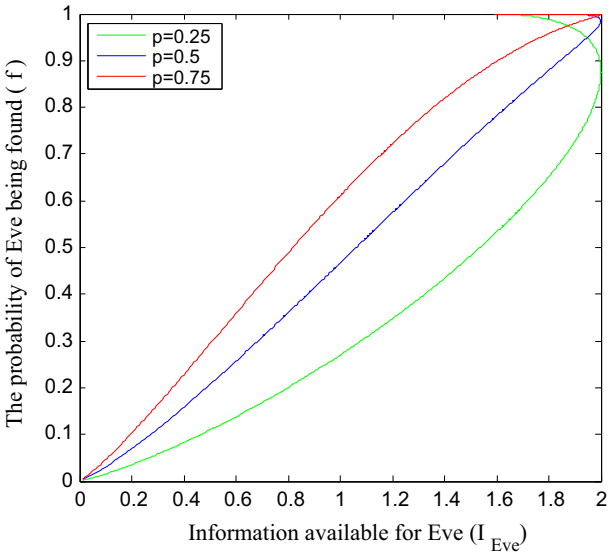

Fig. 2 Relationship among I_{Eve}, p and f

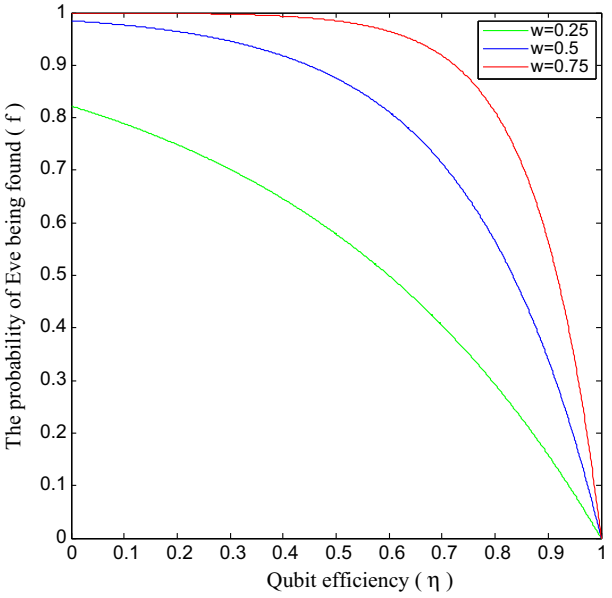

Fig. 3 Relationship among η, ω and f

indicates that the detection probability is no less than r per state for eavesdropping detection in this case.

Figure 3 shows the relationship among η, ω and f. On the one hand, the probability of Eve being found decreases along with the efficiency increasing; on the other hand, the probability of Eve introducing an error will impact efficiency and security as well.

To sum up, by means of simulation analyses with different parameters, if the eavesdropping introduces no errors into the proposed scheme, Eve will gain no information about the key by observing the ancilla, which is exactly consistent with the previous security analysis.

5 Conclusion

In this paper, we proposed a practical and efficient dynamic quantum direct secret sharing scheme using mutually unbiased measurements results for generalized GHZ states. The dealer can share a determinate secret among agents by performing unitary operations. Agents only perform single-photon measurements to get their shadows, and even the dealer cannot know their shadows. Our scheme is not only dynamic, but can make agents update their shadows periodically without changing the secret, which makes it more convenient in a practical application than other schemes. Our newly proposed protocol can stand against participant attacks, provide a higher efficiency in transmission, and reduce the complexity of implementation.

Acknowledgements The authors would like to thank the anonymous referees for their very valuable comments that enhance the quality of this paper. This work was supported by the National Natural Science Foundation of China (61602291, 61671280, 11671244) and China Postdoctoral Science Foundation (2018M633456).

References

1. Smith, A.: Multi-party quantum computation. Arxiv Cornell University Library (2001)
2. Liu, B., Xiao, D., Huang, W., et al.: Quantum private comparison employing single-photon interference. Quantum Inf. Process. **16**, 180 (2017)
3. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**, 373–384 (2011)
4. Sharma, R.D., Thapliyal, K., Pathak, A.: Quantum sealed-bid auction using a modified scheme for multiparty circular quantum key agreement. Quantum Inf. Process. **16**, 169 (2017)
5. Gao, F., Liu, B., Huang, W., et al.: Postprocessing of the oblivious key in quantum private query. IEEE J. Sel. Top. Quantum Electron. **21**, 98–108 (2014)
6. Huang, W., Wen, Q.Y., Liu, B., et al.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China-Phys. Mech. Astron. **56**, 1670–1678 (2013)
7. Zhang, L., Sun, H.W., Zhang, K.J., et al.: An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption. Quantum Inf. Process. **16**, 70 (2017)
8. Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**, 042312 (2001)
9. Hillery, M., Buzek, V., Berthiaunie, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1840 (1999)
10. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 052307 (2004)
11. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)

12. Lu, H., et al.: Secret sharing of a quantum state. Phys. Rev. Lett. **117**, 030501 (2016)
13. Gao, X., Zhang, S., Chang, Y.: Cryptanalysis and improvement of the semi-quantum secret sharing protocol. Int. J. Theor. Phys. **56**, 2512–2520 (2017)
14. Matsumoto, R.: Unitary reconstruction of secret for stabilizer-based quantum secret sharing. Quantum Inf. Process. **16**, 202 (2017)
15. Bai, C.M., Li, Z.H., et al.: Quantum secret sharing using the d-dimensional GHZ state. Quantum Inf. Process. **16**, 59 (2017)
16. Qin, H.W., Zhu, X.H., Dai, Y.W.: A proactive quantum secret sharing scheme based on GHZ state. Mod. Phys. Lett. B **29**, 550165 (2015)
17. Yu, K.F., et al.: Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. Quantum Inf. Process. **16**, 194 (2017)
18. Fiedler, L., Naaijkens, P., Osborne, T.J.: Jones index, secret sharing and total quantum dimension. New J. Phys. **19**, 023039 (2017)
19. Kogias, I., Xiang, Y., He, Q., et al.: Unconditional security of entanglement-based continuous-variable quantum secret sharing. Phys. Rev. A **95**, 012315 (2017)
20. Wang, J., Li, L., Peng, H., et al.: Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. Phys. Rev. A **95**, 022320 (2017)
21. Chen, X.B., Dou, Z., Xu, G., et al.: A kind of universal quantum secret sharing protocol. Sci. Rep. **7**, 39845 (2017)
22. Xu, T.T., Li, Z.H., et al.: A new improving quantum secret sharing scheme. Int. J. Theor. Phys. **56**, 1–10 (2017)
23. Ahmadi, M., Wu, Y.D., Sanders, B.C.: Relativistic (2, 3)-threshold quantum secret sharing. Phys. Rev. D Part. Fields **96**, 065018 (2017)
24. Abulkasim, H., Hamad, S., et al.: Quantum secret sharing with identity authentication based on Bell states. Int. J. Quantum Inf. **15**, 1750023 (2017)
25. Hsu, J.L., Chong, S.K., Hwang, T., Tsai, C.W.: Dynamic quantum secret sharing. Quantum Inf. Process. **12**, 331–344 (2013)
26. Jia, H.Y., Wen, Q.Y., Gao, F., et al.: Dynamic quantum secret sharing. Phys. Lett. A **376**, 1035–1041 (2012)
27. 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)
28. Wang, T.Y., Li, Y.P.: Cryptanalysis of dynamic quantum secret sharing. Quantum Inf. Process. **12**, 1991–1997 (2013)
29. Liao, C.H., Yang, C.W., Hwang, T.: Dynamic quantum secret sharing protocol based on GHZ state. Quantum Inf. Process. **13**, 1907–1916 (2014)
30. Qin, H., Dai, Y.: Dynamic quantum secret sharing by using d-dimensional GHZ state. Quantum Inf. Process. **16**, 64 (2017)
31. Shi, R.H., Mu, Y., Zhong, H., et al.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
32. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**, 10064–10070 (2007)
33. Huang, W., Wen, Q.Y., Liu, B., et al.: Quantum anonymous ranking. Phys. Rev. A **89**, 87–90 (2014)
34. Dolev, S., Pitowsky, I., Tamir, B.A.: Quantum secret ballot. Computer Science (2006)
35. Pittenge, A.O., Rubin, M.H.: Mutually unbiased bases, generalized spin matrices and separability. Linear Algebra Appl. **390**, 255–278 (2004)
36. Jennewein, T., Simon, C., Weihs, G., et al.: Quantum cryptography with entangled photons. Phys. Rev. Lett. **84**, 4729 (2000)
37. Beveratos, A., Brouri, R., Gacoin, T., et al.: Single photon quantum cryptography. Phys. Rev. Lett. **89**, 187901 (2002)
38. Hughes, R.J., Nordholt, J.E., Derkacs, D., et al.: Practical free-space quantum key distribution over 10 km in daylight, and at night. New J. Phys. **4**, 3283–3286 (2002)
39. Gobby, C., Yuan, Z.L., Shields, A.J.: Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. **84**, 3762–3764 (2004)
40. Shi, R.H., Huang, L.S., Yang, W., et al.: Multiparty quantum secret sharing with Bell states and Bell. Opt. Commun. **283**, 2476–2480 (2010)
41. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Quantum key distribution without alternative measurements and rotations. Phys. Rev. A **349**, 53–58 (2006)

42. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
43. Cai, Q.Y., Li, B.W.: Improving the capacity of the Boström–Felbinger protocol. Phys. Rev. A **69**, 521–524 (2004)
44. Barnum, H., Caves, C.M., Fuchs, C.A., et al.: Noncommuting mixed states cannot be broadcast. Phys. Rev. Lett. **76**, 2818–2821 (1996)