International Journal of Theoretical Physics (2022) 61: 76
https://doi.org/10.1007/s10773-022-05081-2

Multi-Party Quantum Secret Sharing Protocol Based on GHZ States Entanglement Swapping

Yuguang Xu[1] · Zexi Li[2] · Tianhua Liu[2] · Hongfeng Zhu[2]

Received: 10 January 2022 / Accepted: 10 March 2022 / Published online: 18 March 2022

Abstract

In this paper, a multi-party quantum secret sharing protocol based on GHZ states entanglement swapping and measurement is proposed. Firstly, we define the "characteristic", then, using the property that multiple groups of GHZ states swapping any particles to keep the characteristics unchanged, a relationship between the characteristics of measurement results, initial state characteristics and Pauli operator characteristics is given, and the protocol is completed by utilizing this equation. In this scheme, the quantum resources involved are only the n GHZ state particles distributed by *Trent* transmitted in the quantum channel to the participants, and the other classical bit resources are distributed in advance or generated by the participants themselves, which improves the security of resource transmission. Furthermore, all participants only need to make GHZ measurements and contribute their own sub-secrets, and can recover the shared secret through a simple XOR formula. It is proud that the efficiency of the whole scheme (i.e. $1/3n$) has also reached the ideal situation.

Keywords GHZ states · Entanglement swapping · Multi-party quantum secret sharing

✉ Hongfeng Zhu
zhuhongfeng1978@163.com

Yuguang Xu
xuyuggmw@bzmc.edu.cn

Zexi Li
895197771@qq.com

Tianhua Liu
liutianhua@sina.com

[1] Institute of Medical Artificial Intelligence, Binzhou Medical University (Yantai Campus), No. 346 Guanhai Road, Laishan District, Yantai 264003, People's Republic of China

[2] Software College, Shenyang Normal University, No.253, HuangHe Bei Street, HuangGu District, Shenyang 110034, People's Republic of China

1 Introduction

As a branch of cryptography, Shamir [1] and Blakley [2] first proposed the classical secret sharing (CSS) scheme in 1979. CSS is an important technology to ensure the security and availability of confidential information. It has a typical application: the company manager has a secret, and he doesn't want any employees to know his secret completely. Therefore, he divided his secret into many parts and let each employee know only one part. Only with the cooperation of all the staff can his secret be completely restored. The security of CSS depends on the complexity of large prime decomposition, and its research has become mature [3]. However, all CSS schemes assume of computational complexity, that is, security is conditional.

With the development of quantum computers, especially the emergence of quantum algorithms [4], the security of classical cryptography is facing severe challenges. Since Bennett and brassard [5] first introduced quantum cryptography in 1984, classical secret sharing was soon combined with quantum mechanics, and quantum secret sharing (QSS) was born. In 1999, Hillery et al. [6] proposed quantum secret sharing protocol for the first time. As one of the earliest famous branches of quantum cryptography, this protocol has attracted extensive attention. In the scheme, quantum states are used as the coding carrier of secret information, so that all parties share a common secret, which can be restored only by the cooperation of all parties. From the perspective of the types of shared secrets, QSS schemes can be divided into two categories: shared quantum information [7] and shared classical information [8]. The former is mainly realized by quantum operations such as quantum entanglement swapping and quantum teleportation. The latter can show various characteristics in scheme design. The security of these two protocols has been proved in theory. In 2003, Guo et al. [9] proposed a non-entangled QSS protocol, which essentially encodes qubits directly. In 2004, Xiao et al. [10] extended the QSS scheme of Hillery et al. [6] to multiple parties and used the optimal measurement method to improve the efficiency. In 2005, Yan et al. [11] proved that A (t, m) - (s, n) threshold QSS protocol is effective in the absence of channel based on Greenberger-Horne-Zeilinger (GHZ) state.

Semi-quantum secret sharing (SQSS) is also an important research point, which is more in line with the actual application. In 2010, Li et al. [12] proposed SQSS protocol based on two GHZ-like states. In 2012, Wang et al. [13] proposed a SQSS scheme based on two particle entangled states. In 2013, Li et al. [14] proposed a SQSS protocol using the state of tensor product of two particles. In the same year, to improve the efficiency of key generation, Yang and Hwang [15] desynchronized the measurement of the classical party. In 2015, Qin and Dai [16] constructed a proactive QSS scheme. In the same year, Xie et al. [17] proposed a SQSS protocol in which a quantum party can share specific messages with two classical parties. However, Yin and Fu [18] pointed out in 2016 that the SQSS protocol of Xie et al. [17] would suffer intercept-resend attacks from dishonest parties, and put forward corresponding improvement protocols. In 2017, Gao et al. [19] found that Yin and Fu [18] analyzed the intercept-resend attack of dishonest parties incorrectly, and the protocol does not meet the semi-quantum conditions, so they made improvements accordingly. Later, Ye and Ye [20] proposed two circular SQSS protocols based on single particle. The first protocol requires the classical party to have measurement capability, and the second protocol does not.

Up to now, QSS protocol has made great progress, and QSS protocols designed from various angles emerge in endlessly. In 2018, Qin and Tso [21] proposed an efficient QSS scheme based on special multi-dimensional GHZ state. In 2019, Kang et al. [22] proposed a continuous variable QSS scheme by using the Chinese Remainder Theorem. In 2020, Liu et al. [23] proposed a QSS scheme with verifiable function. In the same year, Lai et al. [24] proposed a high-capacity (2,3) threshold QSS scheme based on asymmetric Quantum lossy channel. Subsequently, Sutradhar and Om [25] proposed an effective QSS scheme without trusted participants.

Based on the theorem that the entanglement swapping characteristics of GHZ state particles are invariant, an anonymously verifiable multi-party quantum secret sharing scheme is proposed, in which the shared secret is classical information. The protocol conforms to the basic principle of secret sharing. Any participant less than n cannot recover the secret alone. All participants must cooperate and take their share before they can get the secret. Moreover, the proposed scheme also meets the high standard of efficiency and security requirements, and can complete the purpose of the experiment with less quantum resources.

The rest of the work is arranged as follows: Section 2 gives some preliminary preparations, mainly several theorems quoted and deduced. Section 3 describes in detail the specific process of how to share classical information with the help of quantum methods. Sections 4 provides the security analysis of the protocol and sections 5 analyzes the efficiency. Finally, a summary is given in section 6.

2 Preliminaries

2.1 GHZ State and Pauli Operation

There are eight three-particle entangled GHZ states, written as follows:

$$\begin{array}{ll}
|\varPsi_{000}\rangle = \frac{1}{\sqrt{2}}\Big(|100\rangle + |011\rangle\Big), & |\varPsi_{001}\rangle = \frac{1}{\sqrt{2}}\Big(|100\rangle - |011\rangle\Big) \\
|\varPsi_{010}\rangle = \frac{1}{\sqrt{2}}\Big(|111\rangle + |000\rangle\Big), & |\varPsi_{011}\rangle = \frac{1}{\sqrt{2}}\Big(|111\rangle - |000\rangle\Big) \\
|\varPsi_{100}\rangle = \frac{1}{\sqrt{2}}\Big(|101\rangle + |010\rangle\Big), & |\varPsi_{101}\rangle = \frac{1}{\sqrt{2}}\Big(|101\rangle - |010\rangle\Big) \\
|\varPsi_{110}\rangle = \frac{1}{\sqrt{2}}\Big(|110\rangle + |001\rangle\Big), & |\varPsi_{111}\rangle = \frac{1}{\sqrt{2}}\Big(|110\rangle - |001\rangle\Big)
\end{array}$$

Furthermore, any GHZ state $|\Psi_{ijk}\rangle$ can be rewritten as the following general formula:

$$\left|\Psi_{ijk}\right\rangle = \frac{1}{\sqrt{2}}\left(|1jt\rangle + (-1)^k \left|0\bar{j}\,\bar{t}\right\rangle\right)$$

where $i, j, k, t \in (0,\ 1)$, $t = i \oplus j$ and $\bar{j} = j \oplus 1$, $\bar{t} = t \oplus 1$ (i.e., a bar over a bit value indicates its logical negation). In this paper, ⊕ represents XOR operation, and the classical bit string ijk is regarded as the characteristic of GHZ state $|\Psi_{ijk}\rangle$.

Next, we introduce four basic Pauli operators, as follows:

$$\begin{array}{c}
U_{000} = I = |0\rangle\langle 0| + |1\rangle\langle 1|, U_{001} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \\
U_{110} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, U_{111} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|
\end{array}$$

Similarly, the subscript $k_1k_2k_3$ is regarded as the characteristic of the Pauli operator $U_{k_1}\ k_2\ k_3$, where k_1, k_2, $k_3 \in (0,\ 1)$.

Here, the state change of |0⟩ or |1⟩ after being operated by each Pauli operator is given:

$$I|0\rangle = |0\rangle, I|1\rangle = |1\rangle\sigma_z|0\rangle = |0\rangle, \sigma_z|1\rangle = -|1\rangle$$
$$\sigma_x|0\rangle = |1\rangle, I|1\rangle = |0\rangle\sigma_y|0\rangle = -|1\rangle, \sigma_z|1\rangle = |0\rangle$$

2.2 Entanglement Swapping Theorem

Theorem 1. [26] For *n* GHZ states {(1, 2, 3), (4, 5, 6), …, (3*n*-2, 3*n*-1, 3*n*)}, after entanglement swapping as Fig. 1, the possible measurement results and the initial states always meet the following equation:

$$M_{1,2,3n}\oplus M_{4,5,3}\oplus\ldots\oplus M_{3n-2,3n-1,3n-3} = B_{1,2,3}\oplus B_{4,5,6}\oplus\ldots\oplus B_{3n-2,3n-1,3n} \tag{1}$$

where B_{ijk} and M_{rst} denote the characteristics of the initial states of the particles *i*, *j* and *k*, and the possible measurement results of the particles *r*, *s* and *t*, respectively. This formula applies when only one set of particles is exchanged.

Theorem 2. [26] For *n* GHZ states {(1, 2, 3), (4, 5, 6), …, (3*n*-2, 3*n*-1, 3*n*)}, after entanglement swapping as Fig. 2, the possible measurement results and the initial states always meet the following equation:

$$M_{1,3n-1,3n}\oplus M_{4,2,3}\oplus\ldots\oplus M_{3n-2,3n-4,3n-3} = B_{1,2,3}\oplus B_{4,5,6}\oplus\ldots\oplus B_{3n-2,3n-1,3n} \tag{2}$$

where B_{ijk} and M_{rst} denote the characteristics of the initial states of the particles *i*, *j* and *k*, and the possible measurement results of the particles *r*, *s* and *t*, respectively. This formula applies when two sets of particles are exchanged.

Theorem 3. If we perform any Pauli operator $U_{k_1}\ k_2\ k_3$ on any particle in any GHZ state $|\Psi_{ijk}\rangle_{123}$, the characteristic B'_{123} of transformed particles 1, 2 and 3 always satisfies the following equation:

$$B'_{123} = k_1k_2k_3\oplus B_{123} \tag{3}$$

Proof. Suppose we apply any Pauli operator $U_{k_1}\ k_2\ k_3$ to the first particle of GHZ state $|\Psi_{ijk}\rangle_{123}$, we will get,

$$U_{k_1k_2k_3}\left|\Psi_{ijk}\right\rangle_{123} = U_{k_1k_2k_3}\frac{1}{\sqrt{2}}\left(|1jt\rangle + (-1)^k\left|0\bar{j}\,\bar{t}\right\rangle\right)_{123}$$

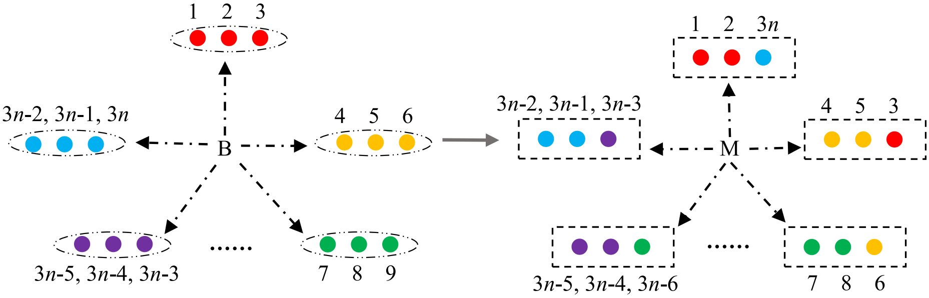

Fig. 1 Entanglement swapping of a group of particles in *n* GHZ states

When $k_1 = k_2 = 0$, there will be:

$$U_{k_1k_2k_3}\left|\Psi_{ijk}\right\rangle_{123} = \frac{1}{\sqrt{2}}\left((-1)^{k_3}|1jt\rangle + (-1)^{k}\left|0\bar{j}\,\bar{t}\right\rangle\right)_{123}$$
$$= \frac{1}{\sqrt{2}}\left((-1)^{k_3}\left(|1jt\rangle + (-1)^{k\oplus k_3}\left|0\bar{j}\,\bar{t}\right\rangle\right)\right)_{123} = (-1)^{k_3}\left|\Psi_{ij(k\oplus k_3)}\right\rangle_{123}$$

So $B'_{123} = ij(k\oplus k_3) = k_1\ k_2\ k_3\oplus ijk$, that is, $B'_{123} = k_1\ k_2\ k_3\oplus B_{123}$.When $k_1 = k_2 = 1$, there will be:

$$U_{k_1k_2k_3}\left|\Psi_{ijk}\right\rangle_{123} = \frac{1}{\sqrt{2}}\left(|0jt\rangle + (-1)^{k}(-1)^{k_3}\left|1\bar{j}\,\bar{t}\right\rangle\right)_{123}$$
$$= \frac{1}{\sqrt{2}}\left(|0jt\rangle + (-1)^{k\oplus k_3}\left|1\bar{j}\,\bar{t}\right\rangle\right)_{123} = \left|\Psi_{\bar{i}\,\bar{j}(k\oplus k_3)}\right\rangle_{123}$$

So $B'_{123} = \bar{i}\,\bar{j}(k\oplus k_3) = (i\oplus 1)\ (j\oplus 1)\ (k\oplus k_3) = k_1\ k_2\ k_3\oplus ijk$, that is, $B'_{123} = k_1\ k_2\ k_3\oplus B_{123}$.

After verification, the result of applying any Pauli operator $U_{k_1}\ k_2\ k_3$ to the second or third particle is the same as the above conclusion, which will not be repeated here. Therefore, we can conclude that no matter which Pauli operator is executed on which particle, it satisfies Eq. (3).

Theorem 4. For n GHZ states {(1, 2, 3), (4, 5, 6), …, (3n-2, 3n-1, 3n)}, If we perform Pauli operator $U_{k_{3i-2}}\ k_{3i-1}\ k_{3i}$ on any particle of the i-th GHZ state (3i,3i + 1,3i + 2) or (3i-2,3i-1,3i), the measurement results after entanglement swapping (as shown in Fig. 3) have the following relationship with the initial state:

$$\oplus_{i=1}^{n}M_{3i,3i+1,3i+2} = \oplus_{i=1}^{n}M_{3i-1,3i,3i+1} = \left\{\oplus_{i=1}^{n}B_{3i-2,3i-1,3i}\right\}\oplus\left\{\oplus_{i=1}^{n}k_{3i-2}k_{3i-1}k_{3i}\right\} \quad (4)$$

Where $M_{3i,\ 3i\ +\ 1,\ 3i\ +\ 2}$ and $M_{3i\ -\ 1,\ 3i,\ 3i\ +\ 1}$ represents the characteristics of particles (3i,3i + 1,3i + 2) and (3i-1,3i,3i + 1) measurement results, respectively, $B_{3i\ -\ 2,\ 3i\ -\ 1,\ 3i}$ is the characteristics of the initial state particle (3i-2,3i-1,3i), and $k_{3i\ -\ 2}k_{3i\ -\ 1}k_{3i}$ denotes the characteristics of Pauli operator $U_{k_{3i-2}}\ k_{3i-1}\ k_{3i}$.

Proof. From **Theorems 1** and **2**, we can get,

$$M_{1,2,3n}\oplus M_{4,5,3}\oplus\ldots\oplus M_{3n-2,3n-1,3n-3}$$
$$= M_{1,3n-1,3n}\oplus M_{4,2,3}\oplus\ldots\oplus M_{3n-2,3n-4,3n-3}$$
$$= B'_{1,2,3}\oplus B'_{4,5,6}\oplus\ldots\oplus B'_{3n-2,3n-1,3n}$$

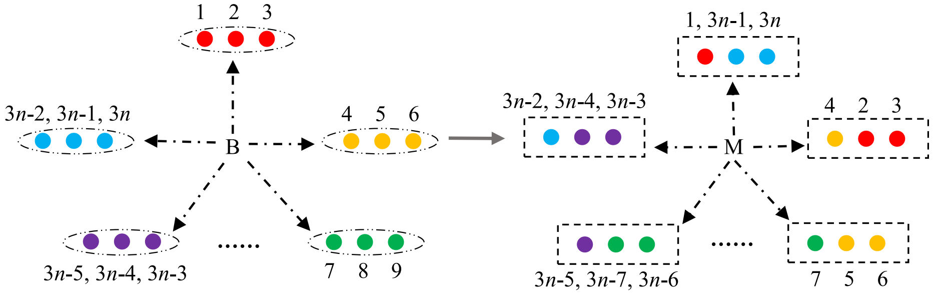

Fig. 2 Entanglement swapping of two groups of particles in n GHZ states

In addition, by **Theorem 3**, there are the following equations,

$$B^{'}_{3i-2,3i-1,3i} = k_{3i-2}k_{3i-1}k_{3i} \oplus B_{3i-2,3i-1,3i}$$

Therefore, $\oplus_{i=1}^{n} M_{3i,3i+1,3i+2} = \oplus_{i=1}^{n} M_{3i-1,3i,3i+1} = \left\{\oplus_{i=1}^{n} B_{3i-2,3i-1,3i}\right\} \oplus \left\{\oplus_{i=1}^{n} k_{3i-2}\ k_{3i-1}\ k_{3i}\right\}$ is established.

The black solid line represents the entanglement between the initial three particles, and both GM and red dotted box represent GHZ measurement.

3 The Proposed Protocol

Suppose *Trent* has a secret S to be shared among n participants: $p_1, p_2, \ldots, p_n$. For convenience, we only consider the case where the shared secret is 3-bit. In addition, we assume that *Trent* verified the identity of the participant p_i for $i = 1, 2, \ldots, n$ in advance and distributed a 3-bit subkey K_i face-to-face for each authenticated p_i. Then, *Trent* computed the XOR result of all subkeys, that is, $K = \oplus_{i=1}^{n} K_i$.

Next, we will introduce the protocol in detail.

Step 1. *Trent* prepared n GHZ states, in which each GHZ state was randomly in one of eight states, and then disrupted the particles of all GHZ states. Currently, there are $3n$ particles in disorder. Next, for $i = 1, 2, \ldots, n$, *Trent* randomly selects three particles and sends them to p_i through the quantum channel. That is, each participant has three particles in the disordered n GHZ states at random.

Step 2. Each participant p_i ($i = 1, 2, \ldots, n$) randomly prepares a 3-bit sub-secret S_i as its private secret and computes $Q_i = S_i \oplus K_i$. It should be noted here that when the first two bits of Q_i are different, p_i needs to replace them with the same two bits, i.e. 00 or 11. Furthermore, p_i applies the Pauli operator U_{Q_i} on any one of the three received particles, and then performs GHZ measurement on the three particles.

Step 3. All participants p_1, p_2, …, p_n publish their measurement results $M_{p_1}, M_{p_2}, \ldots, M_{p_n}$, where M_{p_i} represents the characteristics of the measurement results of participant p_i.

Step 4. We specify $M = \oplus_{i=1}^{n} M_{p_i}$, $B = \oplus_{i=1}^{n} B_i$, where B_i denotes the characteristics of the i-th initial GHZ state after the Pauli operator is executed. Next, *Trent* computes $T = M \oplus B \oplus S \oplus K$ and declares the value of T.

Step 5. When n participants $p_1, p_2, \ldots, p_n$ need to obtain *Trent*'s secret S, first, all of them need to contribute their private secret S_i. Through **Theorem 4**, we can infer that the characteristics of n GHZ measurement results, the characteristics of the initial GHZ state after the application of n Pauli operator and the characteristics of n Pauli operator meet the following relations:

$$\left\{\oplus_{i=1}^{n} M_{p_i}\right\} = \left\{\oplus_{i=1}^{n} B_i\right\} \oplus \left\{\oplus_{i=1}^{n} Q_i\right\}$$

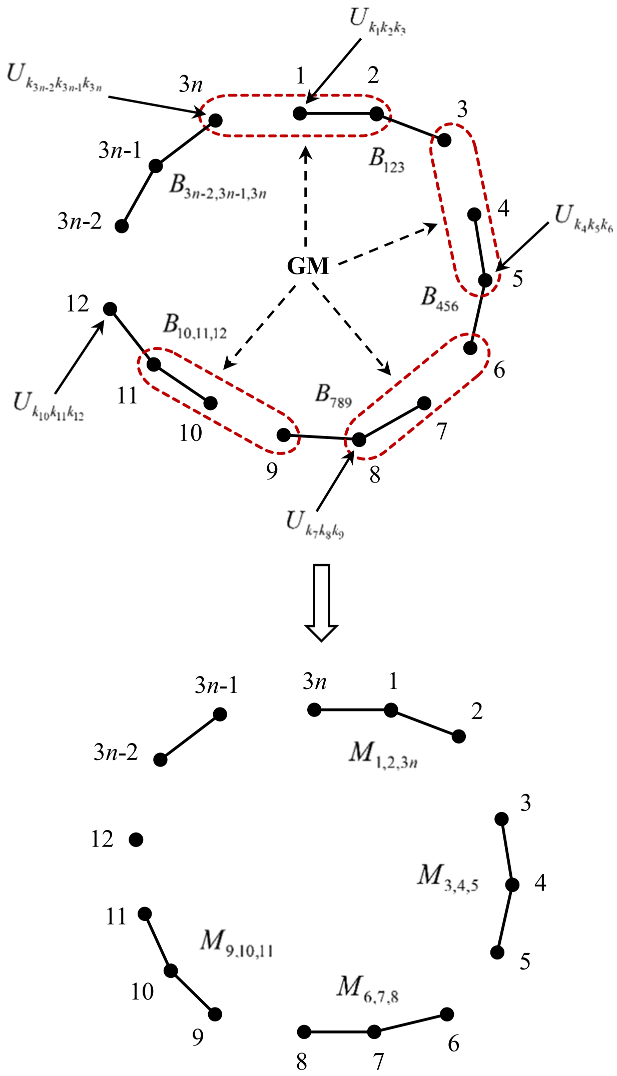

Fig. 3 Entanglement swapping of *n* GHZ state particles after applying *n* Pauli operators

Consequently, we can get the shared secret *S*:

$$\begin{aligned} S &= T\oplus M\oplus B\oplus K = T\oplus\left\{\oplus_{i=1}^{n} Q_i\right\}\oplus K \\ &= T\oplus\left\{\oplus_{i=1}^{n}(S_i\oplus K_i)\right\}\oplus K = T\oplus\left\{\oplus_{i=1}^{n} S_i\right\} \end{aligned} \tag{5}$$

Example. Suppose there are three users: p_1, p_2 and p_3. Each user has three particles distributed by *Trent*, as shown in Fig. 4, p_1, p_2 and p_3 hold particles (1, 4, 9), (3, 7, 6) and (2, 5, 8), respectively. The Pauli operators U_{Q_1}, U_{Q_2} and U_{Q_3} of the three users are applied to particles 4, 7 and 2 respectively.

The black solid line represents the entanglement between the initial three particles, and the red dotted box denotes the GHZ measurement.

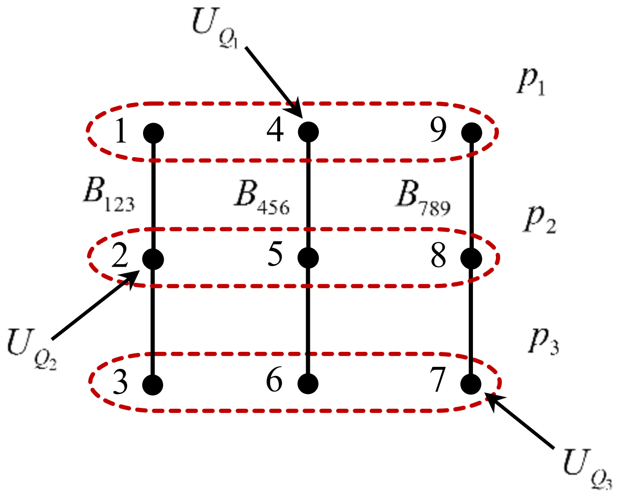

Fig. 4 Distribute three GHZ state particles to three participants

From **Theorem 3**, we can obtain the following equations:

$$B_{123}^{'} = Q_3 \oplus B_{123} = (S_3 \oplus K_3) \oplus B_{123}$$

$$B_{456}^{'} = Q_1 \oplus B_{456} = (S_1 \oplus K_1) \oplus B_{456}$$

$$B_{789}^{'} = Q_2 \oplus B_{789} = (S_2 \oplus K_2) \oplus B_{789}$$

Besides, by **Theorems 1 and 2**, we can get,

$$\begin{gathered} M_{p_1} \oplus M_{p_2} \oplus M_{p_3} = B_{456}^{'} \oplus B_{789}^{'} \oplus B_{123}^{'} \\ = \{(S_1 \oplus K_1) \oplus B_{456}\} \oplus \{(S_2 \oplus K_2) \oplus B_{789}\} \oplus \{(S_3 \oplus K_3) \oplus B_{123}\} \\ = \{S_1 \oplus S_2 \oplus S_3\} \oplus \{K_1 \oplus K_2 \oplus K_3\} \oplus \{B_{123} \oplus B_{456} \oplus B_{789}\} \\ = \{\oplus_{i=1}^{3} S_i\} \oplus \{\oplus_{i=1}^{3} K_i\} \oplus \{\oplus_{i}^{3} B_{3i-2,3i-1,3i}\} \end{gathered} \tag{6}$$

From **Eq. (6)**, we get,

$$\begin{gathered} \{\oplus_{i=1}^{3} S_i\} \oplus T = \{\oplus_{i=1}^{3} S_i\} \oplus S \oplus K \oplus M \oplus B \\ = \{\oplus_{i=1}^{3} S_i\} \oplus S \oplus K \oplus \{\oplus_{i=1}^{3} S_i\} \oplus \{\oplus_{i=1}^{3} K_i\} = S \end{gathered}$$

As can be seen, only authenticated participants with a subkey (i.e. K_i) can recover the secret through **Eq. (5)**. But the protocol needs to ensure that the subkey is not disclosed, that is, it can realize anonymous authentication through different K_i of each participant.

4 Security Analysis

This section analyzes the security of the proposed protocol. We discuss two aspects: external attacks and participant attacks. For external attack, we mainly consider interception-measure attack and entangle-measure attack. The following is a detailed analysis.

4.1 External Attack

(1) Intercept-Measure Attack

Firstly, the external attacker can perform intercept-measure attacks. We assume that the external attacker *Eve* can intercept three particles assigned to any participant, then he directly measures the three particles in GHZ basis, and finally sends them back to the participant. If the attacker *Eve* successfully implements this attack, he will obtain the measurement state of the three particles distributed to the participant p_i. Furthermore, since the characteristic M_{p_i} of the measurement results of the participants is public, *Eve* can easily infer Q_i. However, $Q_i = S_i \oplus K_i$, where S_i is randomly selected by the user p_i, and K_i is p_i's absolutely secure private key. Therefore, even though *Eve* can obtain Q_i, he still cannot obtain any relevant information about S_i or K_i. That is, *Eve* cannot get any private information about K and $\left\{\oplus_{i=1}^{n} S_i\right\}$. Without relevant information about K and $\left\{\oplus_{i=1}^{n} S_i\right\}$, it is obvious that *Eve* cannot know the secret S shared by *Trent* to the participants, because $T = S \oplus K \oplus M \oplus B$ and $S = \left\{\oplus_{i=1}^{n} S_i\right\} \oplus T$. Therefore, this attack is completely infeasible for the proposed quantum secret sharing protocol.

(2) Entangle-Measure Attack

External attackers can also perform more complex attacks, namely entangle-measure attacks. Suppose that the external attacker *Eve* intercepts the particles assigned to the participants and prepares ancillary particles for each intercepted particle. *Eve* first entangles the ancillary particles with the intercepted particles through the local unitary operator, and finally extracts some useful information by measuring the ancillary particles. For example, as shown in Fig. 5, the attacker *Eve* intercepts six particles 1, 2, 3, 4, 5, 6 transmitted through the quantum channel, where (1, 2, 3) and (4, 5, 6) are two pairs of entangled GHZ state particles, and executes *CNOT* gate operators for particle pairs $(1,a_1)$, $(2,a_2)$, $(3,a_3)$, $(4,a_4)$, $(5,a_5)$ and $(6,a_6)$, where a_1, a_2, a_3, a_4, a_5 and a_6 are six ancillary particles prepared by *Eve* for the target particles.

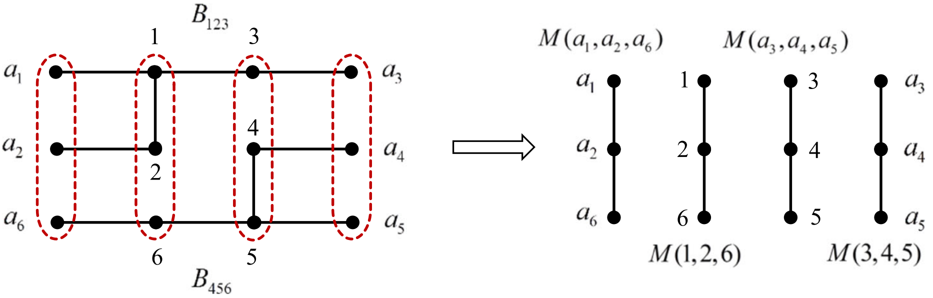

Fig. 5 The entangle-measure attack

Finally, *Eve* sends the intercepted particles back to the corresponding participants. Here, for simplicity, we omit the Pauli operators and assume that the corresponding participants directly perform GHZ-basis measurements on particles (1,2,6) and (3,4,5), respectively. Without losing generality, we assume that the initial states of GHZ state particles (1, 2, 3) and (4, 5, 6) are $|\Psi_{000}\rangle_{123} = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)\ _{123}$, $|\Psi_{010}\rangle_{456} = \frac{1}{\sqrt{2}}(|111\rangle + |000\rangle)\ _{456}$, and the initial states of all ancillary particles are $|0\rangle$.

Next, we start to execute the *CNOT* gate operators, and then we can get:

$$\begin{aligned}
&CNOT[1,a_1]CNOT[2,a_2]CNOT[3,a_3]\Big(|\Psi_{000}\rangle_{123}\otimes|0\rangle_{a_1}\otimes|0\rangle_{a_2}\otimes|0\rangle_{a_3}\Big)\\
&= CNOT[1,a_1]CNOT[2,a_2]CNOT[3,a_3]\left(\frac{1}{\sqrt{2}}\Big(|100\rangle + |011\rangle\Big)_{123}\otimes|0\rangle_{a_1}\otimes|0\rangle_{a_2}\otimes|0\rangle_{a_3}\right)\\
&= \frac{1}{\sqrt{2}}\Big(|100100\rangle + |011011\rangle\Big)_{123a_1a_2a_3}\\
&CNOT[4,a_4]CNOT[5,a_5]CNOT[6,a_6]\Big(|\Psi_{010}\rangle_{456}\otimes|0\rangle_{a_4}\otimes|0\rangle_{a_5}\otimes|0\rangle_{a_6}\Big)\\
&= CNOT[4,a_4]CNOT[5,a_5]CNOT[6,a_6]\left(\frac{1}{\sqrt{2}}\Big(|111\rangle + |000\rangle\Big)_{456}\otimes|0\rangle_{a_4}\otimes|0\rangle_{a_5}\otimes|0\rangle_{a_6}\right)\\
&= \frac{1}{\sqrt{2}}\Big(|111111\rangle + |000000\rangle\Big)_{456a_4a_5a_6}
\end{aligned}$$

Due to the randomness of the measurement, if the measurement results of particles (1, 2, 6) and (3, 4, 5) are $|\Psi_{100}\rangle_{126} = \frac{1}{\sqrt{2}}(|101\rangle + |010\rangle)\ _{126}$ and $|\Psi_{110}\rangle_{345} = \frac{1}{\sqrt{2}}(|110\rangle + |001\rangle)\ _{345}$, the following results will be obtained:

$$\begin{aligned}
&\langle\Psi_{100}\Big|_{123}\otimes\langle\Psi_{110}\Big|_{345}\otimes\frac{1}{\sqrt{2}}\Big(|100100\rangle + |011011\rangle\Big)_{123a_1a_2a_3}\otimes\frac{1}{\sqrt{2}}\Big(|111111\rangle + |000000\rangle\Big)_{456a_4a_5a_6}\\
&= \frac{1}{\sqrt{2}}\Big(\langle 101| + \langle 010|\Big)_{126}\otimes\frac{1}{\sqrt{2}}\Big(\langle 110| + \langle 001|\Big)_{345}\otimes\frac{1}{\sqrt{2}}\Big(|100100\rangle + |011011\rangle\Big)_{123a_1a_2a_3}\\
&\otimes\frac{1}{\sqrt{2}}\Big(|111111\rangle + |000000\rangle\Big)_{456a_4a_5a_6} = \frac{1}{4}\Big(|100111\rangle + |011000\rangle\Big)_{a_1a_2a_3a_4a_5a_6}
\end{aligned}$$

Obviously, the state of possible measurement results of ancillary particles (1, 2, 6) and (3, 4, 5) are $\Big\{|\Psi_{100}\rangle_{a_1}\ a_2\ a_6\ , |\Psi_{000}\rangle_{a_3}\ a_4\ a_5\}$ or $\Big\{|\Psi_{101}\rangle_{a_1}\ a_2\ a_6\ , |\Psi_{001}\rangle_{a_3}\ a_4\ a_5\}$. This means that the attacker *Eve* can infer the XOR result of the measurement results of n participants, i.e. $\oplus_{i=1}^{n} M_{p_i}$, by measuring ancillary particles on the GHZ basis. However, $\oplus_{i=1}^{n} M_{p_i}$ is originally public, so *Eve* does not obtain substantive information. In fact, he still can't get K and $\oplus_{i=1}^{n} S_i$, so he never learns about the shared secret S. According to the above, our quantum secret sharing protocol can resist the entangle-measure attack.

The black solid line represents the entanglement relationship, and the red dotted box denotes GHZ measurement.

4.2 Participant Attack

We assume that there are any dishonest participants with n-1 or less than n-1 who want to recover secret S through illegal conspiracy. However, all quantum resources used and all subkeys distributed are privately generated by *Trent*, and each sub-secret S_i is randomly selected by each participant. Obviously, any dishonest participant with n-1 or less than n-1 cannot obtain the values of K and $\oplus_{i=1}^{n} S_i$, that is, they cannot obtain secret S by collusion. Therefore, our protocol can resist participant attack.

4.3 Others

In addition, the initial subkey K_i distributed by *Trent* in advance can ensure the authenticity of GHZ state particles distributed by *Trent*, because only *Trent* knows the value of K (i.e. $\oplus_{i=1}^{n} K_i$). Of course, *Trent* can also assign a group of particles to each participant instead of three particles, so that *Trent* and participants can select some particles to jointly check the security of quantum channels [27]. Moreover, we can also use decoy photon detection technology [28] to check eavesdropping on quantum channels. Besides, participants can privately exchange particles before executing Pauli operators, to avoid distributing known GHZ states to designated participants. Consequently, the attacker *Eve* (even *Trent*) cannot infer the private operator executed by the participant only from its public measurement results.

Our QSS protocol has the following advantages:

(1) Particles are randomly distributed, and each participant does not know whose particles are entangled with the particles he holds.
(2) Anonymous authentication can be provided.
(3) All subkeys K_i and sub-secrets S_i do not need to be transmitted through any classical or quantum channel.
(4) The operator performed by each participant is completely independent of its sub-secret or subkey. That is, no attacker or eavesdropper can obtain any private information about single subkey or single sub-secret.
(5) The attacker cannot obtain any private information about K and $\oplus_{i=1}^{n} S_i$, and he has no information about the shared secret S. Hence, the proposed secret sharing protocol is unconditionally secure.

5 Efficiency Analysis

Now let us discuss the efficiency of our protocol. According to [29], some efficiency factors can be defined as the following formula, which can be used to obtain the efficiency of quantum communication protocols.

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

Where b_s is the bit length of the shared secret, and q_t is the total number of quantum resources utilized, and b_t represents the number of classical bits used in the protocol. In this scheme, the length of secret S to be shared by *Trent* is 3-bit, so b_s is 3; The quantum resources utilized in the protocol are only n GHZ state particles distributed by *Trent* at the beginning, so q_t is $3n$; Before the start of the protocol, *Trent* distributed a 3-bit subkey K_i to each participant, after the start of the protocol, each participant randomly generated a 3-bit sub-secret S_i, so b_t is $6n$. It can be concluded that the efficiency of our protocol is $\eta = \frac{b_s}{q_t + b_t} = \frac{1}{3n}$.

In Table 1, we also show comparisons with several similar typical protocols in many aspects.

Table 1 Comparison among related protocols

The protocols	Ref. [30]	Ref. [31]	Ref. [32]	Our protocol
Quantum Resources	Bell states	Bell states	Bell states	GHZ states
Shared Secret	Random	Determinate	Determinate	Determinate
Quantum Operators	–	Pauli operators	Pauli operators	Pauli operators
Quantum Measurement	Bell-basis measurements	Bell-basis measurements	Bell-basis measurements	GHZ-basis measurements
Qubit Efficiency	Close to 100%	$1/2n-2$	$1/3n$	$1/3n$
Between Operators and $S_i$orK_i	–	Dependent	Independent	Independent
Transport Order	Ordered	Ordered	Random	Random
Authentication	No	No	Yes	Yes

6 Conclusion

Firstly, we quote the theorem that the entanglement swapping characteristics of GHZ state are invariant. Through the existing theorems, we deduce two new theorems: one is the relationship between the characteristics of initial GHZ state, the characteristics of initial state after executing Pauli operator and the characteristics of Pauli operator; The other is the relationship among the characteristics after swapping measurement, initial state characteristics and Pauli operator characteristics. By the transformation relationship between equations and the nature of XOR operation, all honest participants obtain the final shared secret. This scheme has many advantages, such as particle randomness, anonymous authentication, unconditional security and so on. The security analysis and efficiency analysis show that it cannot only resist most attacks and ensure that the shared secret is not leaked, but also has ideal efficiency. Therefore, under the existing quantum technology conditions, our multi-party quantum secret sharing protocol is completely feasible. In the future, we will combine our derived formulas with machine learning, such as quantum neural structure search, quantum intelligent program synthesis and other fields.

Acknowledgements This work was supported by the National Natural Science Foundation of China: Research on Precision PCR Instrument Model and Its Application in Genetic Engineering (Grant No. 62172330), and the Basic Scientific Research Project of Liaoning Provincial Department of Education (Grant No. LJC202007).

References

1. Shamir, A.: How to share a secret. *Commun*. ACM. **22**, 612–613 (1979)
2. Blakley, G.R.: Safeguarding cryptographic keys[C]. *In: 1979 International Workshop on Managing Requirements Knowledge* (MARK), pp. 313–318. IEEE (1979)
3. R. Bitar, E.R. Salim, IEEE Trans. Inf. Theor.64, 933 (2018)
4. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. P*roceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134
5. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing, pp. 175–179. *Proc. IEEE Int. Conf. Computers, Systems and Signal Processin*g (1984)
6. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A. **59**(3), 1829–1834 (1999)
7. Lai, H., Pieprzyk, J., Luo, M.X., et. al.: High-capacity (2,3) threshold quantum secret sharing based on asymmetric quantum lossy channels. *Quantum Inf. Process*.19(5), 1–13 (2020)

8. Chen, X.B., Dou, Z., Xu, G., et al.: A kind of universal quantum secret sharing protocol. Sci. Rep.7, 39845 (2017)
9. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Rev. A. **310**(4), 247–251 (2003)
10. Xiao, L., Long, G.L., Deng, F.G., et al.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A. **69**(5), 052307 (2004)
11. Yan, F.L., Gao, T.: Quantum secret sharing between multiparty and multiparty without entanglement. Phys. Rev. A. **72**(1), 012304 (2005)
12. Li, Q., Chan, W.H., Long, D.Y.: Semi-quantum secret sharing using entangled states. Phys. Rev. A. **82**(2), 022303 (2010)
13. Wang, J., Zhang, S., Zhang, Q., et al.: Semi-quantum secret sharing using two-particle entangled state. Int. J. Quantum Inf. **10**(5), 1250050 (2012)
14. Li, L.Z., Qiu, D.W., Mateus, P.: Quantum secret sharing with classical bobs. J. Phys. A Math. Theor. **46**(4), 045304 (2013)
15. Yang, C.W., Hwang, T.: Efficient key construction on semi-quantum secret sharing protocols. Int. J. Quantum Inf. **11**(5), 1350052 (2013)
16. Qin, H.W., Dai, Y.W.: Proactive quantum secret sharing. Quantum Inf. Process. **14**, 4237–4244 (2015)
17. Xie, C., Li, L.Z., Qiu, D.W.: A novel semi-quantum secret sharing scheme of specific bits. Int. J. Theor. Phys. **54**(10), 3819–3824 (2015)
18. Yin, A., Fu, F.: Eavesdropping on semi-quantum secret sharing scheme of specific bits. Int. J. Theor. Phys. **55**(9), 4027–4035 (2016)
19. Gao, X., Zhang, S.B., Chang, Y.: Cryptanalysis and improvement of the semi-quantum secret sharing protocol. Int. J. Theor. Phys. **56**(8), 2512–2520 (2017)
20. Ye, C.Q., Ye, T.Y.: Circular semi-quantum secret sharing using single particles. Commun. Theor. Phys. **70**(6), 661–671 (2018)
21. Qin, H.W., Tso, R.L.: Efficient quantum secret sharing based on special multi-dimensional GHZ state. *Opt. Quant. Electron*.50, 167 (2018)
22. Kang, Y., Liao, Q., Geng, J., Guo, Y.: Continuous variable quantum secret sharing with Chinese remainder theorem. Int. J. Theor. Phys.58, 3 9 8 6–3997 (2019)
23. Liu, L.J., Li, Z.H., Han, Z.W., Zhi, D.L.: A quantum secret sharing scheme with verifiable function. *Eur. Phys. J. D*.74, 154 (2020)
24. Lai, H., Pieprzyk, J., Luo, M.X., Zhan, C., Pan, L., Orgun, M.A.: High-capacity (2,3) threshold quantum secret sharing based on asymmetric quantum lossy channels. Quantum Inf. Process.19, 157 (2020)
25. Sutradhar, K., Om, H.: Efficient quantum secret sharing without a trusted player. Quantum Inf. Process.19, 73 (2020)
26. Wang, C., Li, Z., Zhu, H.: Flexible for multiple equations about GHZ states and a prototype case. Int. J. Theor. Phys. **60**, 3868–3884 (2021)
27. Z. Zhang, Z. Man, “Multiparty quantum secret sharing of classical message based on entanglement swapping”, *Phys. Rev. A*, vol.72, no.2, 022303, 2005
28. R.H. Shi, “Quantum private computation of cardinality of set intersection and union”, *European Physical Journal D*, vol.72, no.12, pp.221, 2018
29. Ye Tian-Yu, Jiang Li-Zhen. Improvement of Controlled Bidirectional Quantum Direct Communication Using a GHZ State[J]. Chin. Phys. Lett., 2013, 30(4), 30
30. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Multiparty quantum secret sharing with bell states and bell measurements. Opt. Commun. **283**(11), 2476–2480 (2010)
31. Song, Y., Li, Y., Wang, W.: Multiparty quantum direct secret sharing of classical information with bell states and bell measurements. Int. J. Theor. Phys. **57**(5), 1559–1571 (2018)
32. Shi, R.H.: Useful equations about bell states and their applications to quantum secret sharing. IEEE Commun. Lett. **24**(2), 386–390 (2020)