entropy

IMPACT FACTOR 2.738

Indexed in: PubMed

Article

An Efficient Quantum Secret Sharing Scheme Based on Restricted Threshold Access Structure

Lei Li and Zhi Li

Special Issue
Advances in Information Sciences and Applications

Edited by
Prof. Dr. Jaesung Lee

MDPI

https://doi.org/10.3390/e25020265

entropy

MDPI

Article

An Efficient Quantum Secret Sharing Scheme Based on Restricted Threshold Access Structure

Lei Li * and Zhi Li

School of Mechano-Electronic Engineering, Xidian University, Xi'an 710071, China
* Correspondence: lilei02@xidian.edu.cn

Abstract: Quantum secret sharing is an important branch of quantum cryptography, and secure multi-party quantum key distribution protocols can be constructed using quantum secret sharing. In this paper, we construct a quantum secret sharing scheme built on a constrained (t, n) threshold access structure, where n is the number of participants and t is the threshold number of participants and the distributor. Participants from two different sets perform the corresponding phase shift operations on two particles in the GHZ state passed to them, and then $t-1$ participants with the distributor can recover the key, where the participant recovering the key measures the particles received by himself and finally obtains the key through the collaboration of the distributors. Security analysis shows that this protocol can be resistant to direct measurement attacks, interception retransmission attacks, and entanglement measurement attacks. This protocol is more secure, flexible, and efficient compared with similar existing protocols, which can save more quantum resources.

Keywords: quantum secret sharing; phase shift operation; GHZ state; efficiency

check for updates

Citation: Li, L.; Li, Z. An Efficient Quantum Secret Sharing Scheme Based on a Restricted Threshold Access Structure. *Entropy* **2023**, *25*, 265. https://doi.org/10.3390/e25020265

Academic Editor: Jaesung Lee

Received: 7 December 2022
Revised: 27 January 2023
Accepted: 28 January 2023
Published: 31 January 2023

1. Introduction

Secret sharing is an important branch of information security research, and it provides new ideas for solving key management problems [1,2]. The secret sharing system divides the shared secrets into sub-secrets, which are sent separately to several participants for safekeeping, and it specifies which participants can restore the secrets together and which participants cannot cooperate to obtain the approved secret information. Quantum secret sharing is an important research direction in quantum cryptography, which combines quantum theory and classical secret sharing and belongs to a kind of quantum key distribution in quantum key management [3–6].

Quantum secret sharing means that the distributor divides a classical or quantum message into several copies, and only the participants in the authorized set can recover the secret, while the participants in the non-authorized set cannot recover the secret. The security of the quantum secret sharing scheme is significantly improved in terms of the security of sharing compared to computationally complex classical secrets due to the guarantee of the relevant fundamental principles in quantum exploitation.

The first quantum secret sharing (QSS) scheme was proposed by Hillery [7] in 1999 using the Greenberger–Horne–Zeilinger (GHZ) state. In the same year, Cleve et al. [6] proposed the threshold QSS scheme using the quantum error correction code theory, where the threshold quantum secret sharing scheme means that the distributor divides the secret information into n copies and sends them to n participants separately, and at least t participants cooperate to recover the secret; however, the set of less than t participants cannot recover the secret. Since then, increasingly quantum secret sharing schemes have been proposed [8–14], and some of these schemes are based on quantum physical properties to share classical information, while some schemes are based on quantum mechanics principles to share arbitrary quantum state information.

Many researchers have designed series of different types of schemes based on different quantum principles, such as based on single photons [15–17], product states [18–20], and entangled states [21–25], respectively. Among the above secret sharing schemes, threshold schemes occupy an important position [6,13,26–31]; however, in practical applications, the authorized subset may not consist of any t participants, and there are some occasions in which the permissions of certain participants are restricted, such as confidential data restoration, hierarchical structures, and financial infidelity. Therefore, the (t, n) threshold structure is not suitable for these occasions.

In 2013, Gheorghiu et al. [21] constructed the first quantum secret sharing scheme by local operations and classical communication (LOCC); in 2015, Rahaman et al. [22] gave a QSS model based on LOCC. The above two schemes are built on restricted (t, n) threshold type access structures. This type of access structure does not belong to the general (t, n) threshold structure and can satisfy the use of secret sharing in some special cases. Since this scheme is simple and efficient [22], a number of scholars have constructed many QSS schemes based on this class of restricted access structures on the basis of this property of local distinguishability of quantum states [23–26].

However, all the above schemes utilize the entangled states of n particles, and when the number of participants n is large, n-qudit entangled states are currently difficult to make. Therefore, how to utilize the entangled states of a small number of particles for such restricted threshold structures to accomplish the distribution of multi-party quantum keys is a problem that needs to be solved in the construction of QSS schemes. In this paper, we use phase shift operation based on three-particle entangled states to achieve multi-party quantum key distribution on this kind of restricted access structures, which is an efficient and secure protocol, and at the same time, saves more quantum resources compared with similar protocols.

This paper is organized as follows: In Section 1, we give the phase shift operator and its properties. Then, the detailed procedure of the scheme is given in Section 2. Next, the correctness and security of this scheme is proven in Sections 3 and 4, respectively. The efficiency and other metrics of this protocol are compared with several protocols of the same type in Section 5. Finally, a short conclusion is provided in Section 6.

2. Preliminary Knowledge

This section further studies the properties of unitary operators on the basis of literature [28], providing a theoretical basis for constructing the multi-party quantum key distribution protocol in this paper. Let Z_p be a finite field and p be an odd prime number. The GHZ states used in this paper are $|\mathrm{GHZ}_{000}\rangle$ and $|\mathrm{GHZ}_{100}\rangle$, where

$$|\mathrm{GHZ}_{000}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), |\mathrm{GHZ}_{100}\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle).$$

An angle a shift operation is performed on the relative phase on the j-TH particle of GHZ, denoting by $U_j(a)$, where

$$U_j(a) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\cdot a} \end{pmatrix},$$

where $a \in Z_p, j = 1, 2, 3$.

Lemma 1. *For the $|\mathrm{GHZ}\rangle$ state, we have*

$$\begin{aligned} &U_1(a) \otimes I \otimes I|\mathrm{GHZ}\rangle \\ &= I \otimes U_2(a) \otimes I|\mathrm{GHZ}\rangle \\ &= I \otimes I \otimes U_3(a)|\mathrm{GHZ}\rangle, \end{aligned} \tag{1}$$

where I is a constant operator.

Proof. Prove that the equation holds only for the case $|\mathrm{GHZ}\rangle = |\mathrm{GHZ}_{000}\rangle$. Other cases can be proven similarly.

$$\begin{aligned} U_1(a) \otimes I \otimes I|\mathrm{GHZ}\rangle &= U_1(a) \otimes I \otimes I\left[\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right] \\ &= \frac{1}{\sqrt{2}}[(U_1(a)|0\rangle \otimes |00\rangle + U_1(a)|1\rangle \otimes |11\rangle)] \\ &= \frac{1}{\sqrt{2}}\left[|0\rangle \otimes \Big|00 > +e^{i\cdot a}\Big|1\Big\rangle \otimes |11\rangle\right] \\ &= \frac{1}{\sqrt{2}}\Big(|000\rangle + e^{i\cdot a}|111\rangle\Big). \end{aligned}$$

Similarly, it can be proven that

$$\begin{aligned} I \otimes U_2(a) \otimes I|\mathrm{GHZ}\rangle &= \tfrac{1}{\sqrt{2}}\big(|000\rangle + e^{i\cdot a}|111\rangle\big). \\ I \otimes I \otimes U_3(a)|\mathrm{GHZ}\rangle &= \tfrac{1}{\sqrt{2}}\big(|000\rangle + e^{i\cdot a}|111\rangle\big). \end{aligned}$$

Thus, Lemma 1 holds when $|\mathrm{GHZ}\rangle = |\mathrm{GHZ}_{100}\rangle$. □

Lemma 1 shows the result that a shift of angle a to particle 1 of the GHZ state is equivalent to a shift of angle a to its particle 2 or 3.

Lemma 2. *For the* $|\mathrm{GHZ}\rangle$ *state, we have*

$$(U_1(a) \otimes I \otimes I)(U_1(b) \otimes I \otimes I)|\mathrm{GHZ}\rangle = U_1(a+b) \otimes I \otimes I|\mathrm{GHZ}\rangle; \tag{2}$$

$$I \otimes (U_2(a) \otimes I)(I \otimes U_2(b) \otimes I)|\mathrm{GHZ}\rangle = I \otimes U_2(a+b) \otimes I|\mathrm{GHZ}\rangle; \tag{3}$$

$$I \otimes I \otimes (U_3(a))(I \otimes I \otimes U_3(b))|\mathrm{GHZ}\rangle = I \otimes I \otimes U_3(a+b)|\mathrm{GHZ}\rangle. \tag{4}$$

Proof. We only prove that the equation holds for the case of $|\mathrm{GHZ}\rangle = |\mathrm{GHZ}_{000}\rangle$; the other cases can be proven similarly. Since

$$(U_1(a) \otimes I \otimes I)(U_1(b) \otimes I \otimes I)|\mathrm{GHZ}\rangle = U_1(a+b) \otimes I \otimes I|\mathrm{GHZ}\rangle$$

$$\begin{aligned} U_1(a+b) \otimes I \otimes I|\mathrm{GHZ}\rangle &= U_1(a+b) \otimes I \otimes I\left[\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right] \\ &= \frac{1}{\sqrt{2}}[U_1(a+b)|0\rangle \otimes |00\rangle + U_1(a+b)|1\rangle \otimes |11\rangle] \\ &= \frac{1}{\sqrt{2}}\left[|0\rangle \otimes |00\rangle + e^{i\cdot(a+b)}|1\rangle \otimes |11\rangle\right]. \\ &= \frac{1}{\sqrt{2}}\left[|000\rangle + e^{i\cdot(a+b)}|111\rangle\right] \end{aligned}$$

and

$$\begin{aligned} &(U_1(a) \otimes I \otimes I)(U_1(b) \otimes I \otimes I)|\mathrm{GHZ}\rangle \\ &= (U_1(a) \otimes I \otimes I)(U_1(b) \otimes I \otimes I)\left[\tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right] \\ &= \tfrac{1}{\sqrt{2}}U_1(a) \otimes I \otimes I\Big)[U_1(b)|0\rangle \otimes |00\rangle + U_1(b)|1\rangle \otimes |11\rangle] \\ &= \tfrac{1}{\sqrt{2}}U_1(a) \otimes I \otimes I\Big)\left[|0\rangle \otimes |00\rangle + e^{i\cdot b}|1\rangle \otimes |11\rangle\right] \\ &= \tfrac{1}{\sqrt{2}}\left[U_1(a)|0\rangle \otimes |00\rangle + e^{i\cdot b}U_1(a)|1\rangle \otimes |11\rangle\right] \\ &= \tfrac{1}{\sqrt{2}}\left[|0\rangle \otimes |00\rangle + e^{i\cdot b}e^{ia}|1\rangle \otimes |11\rangle\right] \\ &= \tfrac{1}{\sqrt{2}}\Big[|000\rangle + e^{i\cdot(a+b)}|111\rangle\Big)\Big] \end{aligned}$$

Therefore, when $|\mathrm{GHZ}\rangle = |\mathrm{GHZ}_{000}\rangle$, $(U_1(a) \otimes I \otimes I)(U_1(b) \otimes I \otimes I)|\mathrm{GHZ}\rangle = U_1(a+b) \otimes I \otimes I|\mathrm{GHZ}\rangle$ holds. It can be proven in the same way that, when $|\mathrm{GHZ}\rangle = |\mathrm{GHZ}_{100}\rangle$, there is $(U_1(a) \otimes I \otimes I)(U_1(b) \otimes I \otimes I)|\mathrm{GHZ}\rangle = U_1(a+b) \otimes I \otimes I|\mathrm{GHZ}\rangle$. □

Lemma 2 shows that the result of performing two consecutive shifts of angles a and b on a particle of the quantum state GHZ is equivalent to performing a shift of angle $a+b$ on this particle. Using Lemma 2, by induction, we have the following result:

Theorem 1. *For the $|\mathrm{GHZ}\rangle$ state, we have,*

$$(U_1(a_1) \otimes I \otimes I) \cdots (U_1(a_l) \otimes I \otimes I)|\mathrm{GHZ}\rangle = U_1(a_1 + \cdots + a_l) \otimes I \otimes I|\mathrm{GHZ}\rangle; \quad (5)$$

$$(I \otimes U_2(a_1) \otimes I) \cdots (I \otimes U_2(a_l) \otimes I)|\mathrm{GHZ}\rangle = I \otimes U_2(a_1 + \cdots + a_l) \otimes I|\mathrm{GHZ}\rangle; \quad (6)$$

$$(I \otimes I \otimes U_3(a_1)) \cdots (I \otimes I \otimes U_3(a_l))|\mathrm{GHZ}\rangle = I \otimes I \otimes U_3(a_1 + \cdots + a_l)|\mathrm{GHZ}\rangle. \quad (7)$$

Theorem 1 shows that the result of performing l successive shifts of angle a_i on a particle of the quantum state $|\mathrm{GHZ}\rangle$ is equivalent to performing a shift of angle $a_1 + a_2 + \cdots + a_l$ on this particle, where $i = 1, 2, \cdots, l$.

Theorem 2. *For the $|\mathrm{GHZ}\rangle$ state, we have,*

$$U_1(a_1) \otimes U_2(a_2) \otimes U_3(a_3)|\mathrm{GHZ}\rangle = U_1(a_1 + a_2 + a_3) \otimes I \otimes I|\mathrm{GHZ}\rangle; \quad (8)$$

$$U_1(a_1) \otimes U_2(a_2) \otimes U_3(a_3)|\mathrm{GHZ}\rangle = I \otimes U_2(a_1 + a_2 + a_3) \otimes I|\mathrm{GHZ}\rangle; \quad (9)$$

$$U_1(a_1) \otimes U_2(a_2) \otimes U_3(a_3)|\mathrm{GHZ}\rangle = I \otimes I \otimes U_3(a_1 + a_2 + a_3)|\mathrm{GHZ}\rangle. \quad (10)$$

Proof. Prove that the equation holds for the case of $|\mathrm{GHZ}\rangle = |\mathrm{GHZ}_{000}\rangle$ only. The other cases can be proven similarly. First, prove that Equation (8) holds. Since

$$\begin{aligned}
&U_1(a_1) \otimes U_1(a_2) \otimes U_3(a_3)|\mathrm{GHZ}\rangle \\
&= (U_1(a_1) \otimes I \otimes I)(I \otimes U_1(a_2) \otimes I)(I \otimes I \otimes U_3(a_3))|\mathrm{GHZ}\rangle \\
&= (U_1(a_1) \otimes I \otimes I)(I \otimes U_1(a_2) \otimes I)\tfrac{1}{\sqrt{2}}(|000\rangle + e^{i \cdot a_3}|111\rangle) \\
&= (U_1(a_1) \otimes I \otimes I)\tfrac{1}{\sqrt{2}}(|000\rangle + e^{i \cdot a_3}e^{i \cdot a_2}|111\rangle) \\
&= \tfrac{1}{\sqrt{2}}\left(|000\rangle + e^{i \cdot (a_3 + a_2)}e^{i \cdot a_1}|111\rangle\right) \\
&= \tfrac{1}{\sqrt{2}}\left(|000\rangle + e^{i \cdot (a_3 + a_2 + a_1)}|111\rangle\right) \\
&= U_1(a_1 + a_2 + a_3) \otimes I \otimes I|\mathrm{GHZ}\rangle.
\end{aligned} \quad (11)$$

Then, $U_1(a_1) \otimes U_2(a_2) \otimes U_3(a_3)|\mathrm{GHZ}\rangle = U_1(a_1 + a_2 + a_3) \otimes I \otimes I|\mathrm{GHZ}\rangle$; therefore, (8) holds.

On the other hand, from Lemma 1, we have

$$\begin{aligned}
&U_1(a_1 + a_2 + a_3) \otimes I \otimes I|\mathrm{GHZ}\rangle \\
&= I \otimes U_2(a_1 + a_2 + a_3) \otimes I|\mathrm{GHZ}\rangle \\
&= I \otimes I \otimes U_3(a_1 + a_2 + a_3)|\mathrm{GHZ}\rangle.
\end{aligned}$$

Combining Equation (11) gives

$$\begin{aligned}
U_1(a_1) \otimes U_2(a_2) \otimes U_3(a_3)|\mathrm{GHZ}\rangle &= I \otimes U_2(a_1 + a_2 + a_3) \otimes I|\mathrm{GHZ}\rangle, \\
U_1(a_1) \otimes U_2(a_2) \otimes U_3(a_3)|\mathrm{GHZ}\rangle &= I \otimes I \otimes U_3(a_1 + a_2 + a_3)|\mathrm{GHZ}\rangle.
\end{aligned}$$

Therefore, Equations (9) and (10) hold.

Similarly, it follows that, when $|\mathrm{GHZ}\rangle = |\mathrm{GHZ}_{000}\rangle$ holds, then (8), (9), and (10) hold. □

3. The Proposed Protocol

In this section, we propose a multi-party quantum secret sharing protocol based on generalized GHZ states. This QSS protocol is divided into three phases: the initial phase, share distribution phase, and secret reconstruction phase.

3.1. Initialization Phase

Let P be a set containing n participants with $P = \{P_1, P_2, \cdots, P_n\}$. Let $P^{(1)} = \{P_1^{(1)}, \cdots, P_{t_1}^{(1)}\}$ and $P^{(2)} = \left\{P_1^{(2)}, \cdots, P_{t_2}^{(2)}\right\}$ be, respectively, two subsets of P, where $t_i \geq 1$ and satisfies $t_1 + t_2 = t - 1, 3 \leq t \leq n$. The distributor Alice chooses a prime $d(2 < d < 2n)$ and sets a finite field Z_d. Alice then chooses a $(t-1)$-degree polynomial $f(x) = S + a_1x^1 + \cdots + a_{t-1}x^{t-1}$, where S is a secret, $f(x) \in Z_d[x]$, and the symbol '+' is defined as the modulo addition. Let $m = \lceil \log_2 d \rceil$, and then S can be represented as a binary sequence, i.e., $S = (s_1, s_2, \cdots, s_m)$, where $s_i \in \{0, 1\}, i = 1, 2, \cdots, m$. Alice chooses the SHA1 hash function $H(S)$ with key and computes $H(S)$, then shares $H(S)$ with the participants from the set P.

3.2. Share Distribution Phase

In this phase, Alice shares sub-shares among the participants in the set $P^{(1)} \cup P^{(2)}$.

(1) Distribution of classic shares

Alice computes the classical share $f\left(x_r^{(j)}\right)$ and assigns $f\left(x_r^{(j)}\right)$ to the participant $P_r^{(j)}$ via a secure channel (e.g., a quantum direct communication channel), and Alice computes her own share $f(x_0)$ as well as $S_0 = f(x_0)\prod_{1\leq r\leq t_1} \frac{x_r^{(1)}}{\left(x_r^{(1)}-x_0\right)} \prod_{1\leq r\leq t_2} \frac{x_r^{(2)}}{\left(x_r^{(2)}-x_0\right)}$, where $x_1^{(1)}, \cdots, x_{t_1}^{(1)}, x_1^{(2)}, \cdots, x_{t_2}^{(2)}, x_0$ are all not equal to each other.

(2) The preparation of a sequence of quantum states

Alice prepares a sequence of quantum states $\{|\varphi_1\rangle, |\varphi_2\rangle, \cdots, |\varphi_m\rangle\}$ according to the key $S = (s_1, s_2, \cdots, s_m)$ with the following rules:

$$\text{if } s_i = 0, \text{ then } |\varphi_i\rangle = |\mathrm{GHZ}_{100}\rangle;$$
$$\text{if } s_i = 1, \text{ then } |\varphi_i\rangle = |\mathrm{GHZ}_{000}\rangle.$$

Alice then prepares a random sequence of quantum states $\{\phi_1, \quad \phi_2, \cdots, \quad \phi_L\}$ with each $|\varphi_j\rangle$ randomly between $|\mathrm{GHZ}_{000}\rangle$ and $|\mathrm{GHZ}_{100}\rangle$, where $L = m(1+\zeta)(j \in \{1, 2, \cdots, L\})$, and ζ is a factor in determining the size of the test sample.

(3) Distribution of quantum state sequences

Alice lets the first particles in the sequence $\{|\varphi_1\rangle, |\varphi_2\rangle, \cdots, |\varphi_m\rangle\}$ form the sequence G_1, the second particles form the sequence G_2, and the third particles form the sequence G_3. Alice keeps all the particles in the sequence G_1 and does the phase shift operation $U(2\pi - S + S_0)$ on all the particles in the sequence G_1, where

$$U(2\pi - S + S_0) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\cdot(2\pi - S + S_0)} \end{pmatrix}.$$

(4) Alice forms the sequence H_1 with the first particles in the sequence $\{|\phi_1\rangle, |\phi_2\rangle, \cdots, |\phi_m\rangle\}$, the sequence H_2 with the second particle, and the sequence H_3 with the third particles. Alice takes random particles from the sequences G_2 and H_2 and sends them to the participant $P_i^{(1)}(i \in \{1, 2, \cdots, t_1\})$ from the set $P^{(1)}$. Alice takes some particles from the sequences G_3 and H_3 randomly and then sends them to the participant $P_1^{(2)}$ from the set $P^{(2)}$,

Alice records the serial numbers of the particles when they are sent from G_i and H_i $(i = 2, 3)$, and Alice herself keeps all the particles from G_1 and H_1.

The structure of the quantum network between Alice and all participants in this scheme is illustrated in Figure 1.

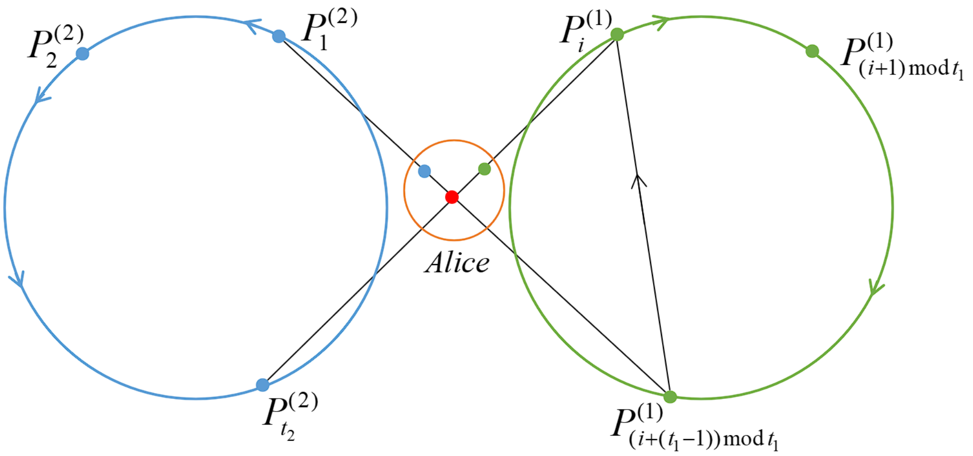


Figure 1. Structure diagram of the quantum network for this scheme.

(5) Secret reconstruction phase

The process of reconstructing the secret by the participant $P_i^{(1)}$ from the set $P^{(1)}$ is given here.

The participant $P_r^{(j)}$ first calculates the shadow $S_r^{(j)}$ of the share.

when $j = 1$,

$$S_r^{(1)} = f\left(x_r^{(1)}\right) \prod_{\substack{1\le i\le t_1\\ i\neq r}} \frac{x_i^{(1)}}{\left(x_i^{(1)} - x_r^{(1)}\right)} \prod_{1\le j\le t_2} \frac{x_j^{(2)}}{\left(x_j^{(2)} - x_r^{(1)}\right)}$$

where $r \in \{1, 2, \cdots, t_1\}$.

When $j = 2$,

$$S_r^{(2)} = f\left(x_r^{(2)}\right) \prod_{1\le i\le t_1} \frac{x_i^{(1)}}{\left(x_i^{(1)} - x_r^{(2)}\right)} \cdot \prod_{\substack{1\le j\le t_2\\ j\neq r}} \frac{x_j^{(2)}}{\left(x_j^{(2)} - x_r^{(2)}\right)}$$

where $r \in \{1, 2, \cdots, t_2\}$.

(6) Transferring particles to $P_i^{(1)}$ and $P_1^{(2)}$

After participants $P_i^{(1)}$ and $P_1^{(2)}$ each receive the particle sequences G_2, H_2 and G_3, H_3, Alice tells $P_i^{(1)}$ and $P_1^{(2)}$ about the positions of these particles in the sequences G_2, H_2 and G_3, H_3, respectively. The participant $P_1^{(2)}$ does a phase shift of $U_3\left(S_1^{(2)}\right)$ for each particle from G_3. Then, participants $P_i^{(1)}$ and $P_1^{(2)}$ send the particle sequences G_2, H_2 and G_3, H_3 to participants $P_{(i+1)\mathrm{mod}t_1}^{(1)}$ and $P_1^{(2)}$ and tells them about the position of each particle in the sequences G_2, H_2 and G_3, H_3, respectively.

(7) Transferring particles to $P_{(i+1)\mathrm{mod}t_1}^{(1)}$ and $P_2^{(2)}$

The participants $P_{(i+1)\mathrm{mod}t_1}^{(1)}$ and $P_2^{(2)}$ do a phase shift of $U_2(S_{(i+1)\mathrm{mod}t_1}^{(1)})$ and $U_3(S_2^{(2)})$ for each particle in G_2 and G_3, respectively. Then, they send the particle sequences G_2, H_2 and G_3, H_3 to participant $P_{(i+2)\mathrm{mod}t_1}^{(1)}$ and participant $P_3^{(2)}$, respectively, and tell them about the position of each particle in the sequences G_2, H_2 and G_3, H_3.

(8) Transferring particles to $P_{(i+t_1-1)\mathrm{mod}t_1}^{(1)}$ and $P_{t_2}^{(2)}$

Follow the above steps and so on, until $P_{(i+t_1-1)\mathrm{mod}t_1}^{(1)}$ and $P_{t_2}^{(2)}$ receive the particle sequences G_2, H_2 and G_3, H_3 from $P_{(i+t_1-2)\mathrm{mod}t_1}^{(1)}$ and $P_{t_2-1}^{(2)}$, respectively, $P_{(i+t_1-1)\mathrm{mod}t_1}^{(1)}$ and

$P^{(2)}_{t_2}$ do phase shift each of the particles in G_2 and G_3 by $U_2(S^{(1)}_{(i+t_1-1)\mathrm{mod}t_1})$ and $U_3(S^{(2)}_{t_2})$, respectively. Then, $P^{(1)}_{(i+t_1-1)\mathrm{mod}t_1}$ sends the particle sequence G_2, H_2 back to $P^{(1)}_i$. At the same time, $P^{(2)}_{t_2}$ also sends the particle sequence G_3, H_3 back to $P^{(1)}_i$ and tells $P^{(1)}_i$ the position of each particle from the particle sequence G_2, H_2 and G_3, H_3. Finally, participant $P^{(1)}_i$ does a phase shift of $U_2(S^{(1)}_i)$ for each of the particles from the sequence G_2.

3.3. Detecting Eavesdropping

Alice uses the measurement base $B_x = \{|x\rangle, |-x\rangle\}$ to measure the particles in the sequence H_1. Then, $P^{(1)}_i$ measures the corresponding particles in the sequences H_2 and H_3 using either the measurement base $B_x = \{|x\rangle, |-x\rangle\}$ or $B_y = \{|y\rangle, |-y\rangle\}$. Where the measurement bases $|+x\rangle, |-x\rangle$ and $|+y\rangle, |-y\rangle$ are represented by the base vector $|0\rangle, |1\rangle$ as

$$\begin{aligned}|+x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\\ |+y\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |-y\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).\end{aligned}$$

For $|\mathrm{GHZ}_{000}\rangle$ and $|\mathrm{GHZ}_{100}\rangle$, when Alice and $P^{(1)}_i$ measure with the above bases, the following four combinations of measurement bases with associated properties occur.

(1) If both sides measure $|\mathrm{GHZ}_{000}\rangle$ with B_x, B_x, B_x-bases, then

$$\begin{aligned}|\mathrm{GHZ}_{000}\rangle = \frac{1}{2}(&|+x\rangle|+x\rangle|+x\rangle + |+x\rangle|-x\rangle|-x\rangle\\ &+|-x\rangle|-x\rangle|+x\rangle + |-x\rangle|+x\rangle|-x\rangle).\end{aligned}$$

(2) If both sides measure $|\mathrm{GHZ}_{000}\rangle$ with B_x, B_y, B_y-bases, then

$$\begin{aligned}|\mathrm{GHZ}_{000}\rangle = \frac{1}{2}(&|+x\rangle|+y\rangle|-y\rangle + |-x\rangle|-y\rangle|+y\rangle\\ &+|-x\rangle|+y\rangle|+y\rangle + |+x\rangle|-y\rangle|-y\rangle).\end{aligned}$$

(3) If both sides measure $|\mathrm{GHZ}_{100}\rangle$ with B_x, B_x, B_x-bases, then

$$\begin{aligned}|\mathrm{GHZ}_{100}\rangle = \frac{1}{2}(&|+x\rangle|+x\rangle|-x\rangle + |+x\rangle|-x\rangle|+x\rangle\\ &+|-x\rangle|-x\rangle|-x\rangle + |-x\rangle|+x\rangle|+x\rangle).\end{aligned}$$

(4) If both sides measure $|\mathrm{GHZ}_{100}\rangle$ with B_x, B_y, B_y-bases, then

$$\begin{aligned}|\mathrm{GHZ}_{100}\rangle = \frac{1}{2}(&|+x\rangle|+y\rangle|+y\rangle + |+x\rangle|-y\rangle|-y\rangle\\ &+|-x\rangle|+y\rangle|-y\rangle + |-x\rangle|-y\rangle|+y\rangle).\end{aligned}$$

From the above results, it is clear that, when Alice measures the particles from the sequence H_1 with basis B_x, $P^{(1)}_i$ measures the corresponding particles, which he holds using the basis B_x or B_y, then the measurements are correlated; see Table 1.

When these measurements are completed, Alice asks $P^{(1)}_i$ to tell her the results of their measurements; however, Alice will not open her measurement base. Then, Alice statistically determines the error rate from Table 1. If the error rate is above a certain threshold, this communication is abandoned. Otherwise, this protocol continues.

Table 1. Correlation of two-sided measurements of $|GHZ_{000}\rangle$ and $|GHZ_{100}\rangle$.

	Measurements of $P_i^{(1)}$			
Alice	$\|\mathbf{GHZ_{000}}\rangle$		$\|\mathbf{GHZ_{100}}\rangle$	
$\|+x\rangle$	$\|+x\rangle$	$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$
$\|+x\rangle$	$\|-x\rangle$	$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$
$\|+x\rangle$	$\|+y\rangle$	$\|-y\rangle$	$\|+y\rangle$	$\|+y\rangle$
$\|+x\rangle$	$\|-y\rangle$	$\|+y\rangle$	$\|-y\rangle$	$\|-y\rangle$
$\|-x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|+x\rangle$
$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|-x\rangle$
$\|-x\rangle$	$\|+y\rangle$	$\|+y\rangle$	$\|+y\rangle$	$\|-y\rangle$
$\|-x\rangle$	$\|-y\rangle$	$\|-y\rangle$	$\|-y\rangle$	$\|+y\rangle$

3.4. Measuring Information Particles

When Alice and $P_i^{(1)}$ confirms that the channel is secure, Alice measures her particle sequence G_1, and $P_i^{(1)}$ measures her particle sequence G_2 and G_3.

(1) First, $P_i^{(1)}$ secretly selects the random sequence $K_1^{(1,i)} = \left(k_1^{(1,1,i)}, k_2^{(1,1,i)}, \cdots, k_m^{(1,1,i)}\right)$ consisting of 0 and 1 and uses the following rules to measure the particles from sequence G_2 and G_3 from their own hand, and the rules for the measuring base are as follows:

When the j-th bit of $K_1^{(1,i)}$ is equal to 0, it selects the B_x base.
When the j-th bit of $K_1^{(1,i)}$ is equal to 1, it selects the B_y base.

(2) $P_i^{(1)}$ uses the same base to measure the particles from sequences G_2 and G_3 and records these results. These measurements are converted into binary numbers—that is, $|+x\rangle$ and $|+y\rangle$ correspond to 1, while $|-x\rangle$ and $|-y\rangle$ correspond to 0, which in turn constitute two subkeys of $P_i^{(1)}$ and are recorded as $K_2^{(1,i)}$ and $K_3^{(1,i)}$, respectively.

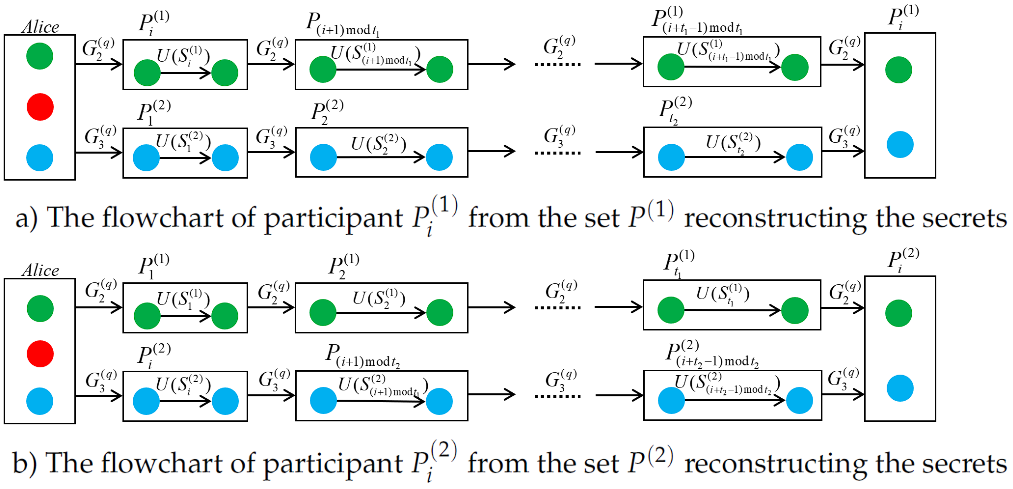
(3) Alice measures the corresponding particle using the base B_x from the sequence G_1 and encodes these results as a bit string $K_A^{(1,i)}$. The encoding rule is that it is recorded as 1 when the measurement result is $|+x\rangle$ and 0 when the measurement result is $|-x\rangle$. Alice then sends $E_{f\left(x_i^{(1)}\right)}\left(K_A^{(1,i)}\right)$ secretly to $P_i^{(1)}$. $P_i^{(1)}$ receives $E_{f\left(x_i^{(1)}\right)}\left(K_A^{(1,i)}\right)$ and decrypts it using $f(x_i^{(1)})$ to obtain $K_A^{(1,i)}$.

3.5. Reconstruction and Detection of Keys

$P_i^{(1)}$ computes $K_1^{(1,i)} \oplus K_2^{(1,i)} \oplus K_3^{(1,i)} \oplus K_A^{(1,i)}$, and verifies whether $H(K_1^{(1,i)} \oplus K_2^{(1,i)} \oplus K_3^{(1,i)} \oplus K_A^{(1,i)}) = H(S)$ holds. If this equation holds, $P_i^{(1)}$ retains S as the shared key. Otherwise, he judges that some of the participants had offered a false share in the secret recovery process and can therefore abandon this round.

Next, we present the process in which participant $P_i^{(1)} (i \in \{1, 2, \cdots, t_1\})$ from the set $P^{(1)}$ gives their shares to all participants. For the ease of presentation, we arranged the order in which the participants from the set $P^{(2)}$ pass the particles with the natural order of their numbers.

Figure 2a shows the transferring process of the information particle in the q-th GHZ state where the GHZ state consists of a green ball $G_1^{(q)}$, red ball $G_2^{(q)}$, and blue ball $G_3^{(q)}$, $q \in \{1, 2, \cdots, m\}$. First, Alice does the $U(2\pi - S + S_0)$ phase operation to particle $G_1^{(q)}$. Then, Figure 2a gives the process in which participant $P_i^{(1)}$ from the set $P^{(1)}$ shares the sub-shares of all participants, and Figure 2b gives the process in which participant $P_i^{(2)}$ from the set $P^{(2)}$ shares the sub-shares of all participants.



a) The flowchart of participant $P_i^{(1)}$ from the set $P^{(1)}$ reconstructing the secrets

b) The flowchart of participant $P_i^{(2)}$ from the set $P^{(2)}$ reconstructing the secrets

Figure 2. The process of the information particles transferring.

The process participant $P_i^{(2)}(i \in \{1,2,\cdots,t_2\})$ from the set $P^{(2)}$ shares the sub-shares for all participants, which is similar to the above process.

4. Performance Analysis

4.1. Correctness

Theorem 3. *When Alice and $t-1$ participants from two sets $P^{(1)}$ and $P^{(2)}$ perform a phase shift operation on the particles in the GHZ quantum state sequence $\{|\varphi_1\rangle, |\varphi_2\rangle, \cdots, |\varphi_m\rangle\}$, then Alice and $P_i^{(1)}$ $(i \in \{1,2,\cdots,t_1\})$ complete the corresponding measurement. $P_i^{(1)}$ will finally obtain the distributed key sequence S.*

Proof. First, if Alice and $P_i^{(1)}$ confirm that the channel is secure, the quantum state $|\varphi_j\rangle$ will become $U_1(2\pi - S + S_0) \otimes I \otimes I|\varphi_j\rangle$ when Alice has performed the phase shift operation $j \in \{1,2,\cdots,m\}$. In the recovery phase, according to Theorems 1 and 2, after $t-1$ participants have performed a phase shift operation, the quantum state $U_1(2\pi - S + S_0) \otimes I \otimes I|\varphi_j\rangle$ will become

$$I \otimes U_2\left[(2\pi - S + S_0) + \left(\sum_{r=1}^{t_1} S_r^{(1)} + \sum_{r=1}^{t_2} S_r^{(2)}\right)\right] \otimes I|\varphi_i\rangle = I \otimes U_2(2\pi) \otimes I|\varphi_j\rangle = |\varphi_j\rangle.$$

Here, it is easy to see from Lagrange's formula that $S = S_0 + \sum_{r=1}^{t_1} S_r^{(1)} + \sum_{r=1}^{t_2} S_r^{(2)}$. Thus, $P_i^{(1)}$ will recover the sequence of quantum states $\{|\varphi_1\rangle, |\varphi_2\rangle, \cdots, |\varphi_m\rangle\}$.

Next, we will prove that, when Alice and $P_i^{(1)}$ confirmed that the channel is security, $P_i^{(1)}$ will obtain the following equation according to this protocol, i.e.,

$$S = K_1^{(1,i)} \oplus K_2^{(1,i)} \oplus K_3^{(1,i)} \oplus K_A^{(1,i)}. \tag{12}$$

Here, $S = (s_1, s_2, \cdots, s_m)$, $s_i \in \{0,1\}, i = 1,2,\cdots,m$.

Let

$$M = \begin{pmatrix} S \\ K_A^{(1,i)} \\ K_1^{(1,i)} \\ K_2^{(1,i)} \\ K_3^{(1,i)} \end{pmatrix},$$

where M is a $5 \times m$ matrix. Let us first analyze the value of the j-th column of this matrix M. □

Case (1) When the j-th portion of S is 0, i.e., the j-th entangled state of S is encoded as $|\mathrm{GHZ}_{100}\rangle$. In this case, there are two ways that $K_1^{(1,i)}$ can be evaluated.

(1.1) The j-th element of $K_1^{(1,i)}$ takes the value 1. This means that $P_i^{(1)}$ measures the particles in the corresponding G_2 and G_3 with the B_y-base, and then the j-th column of $(K_2^{(1,i)}, K_3^{(1,i)})$ will take the following two cases.

$$\text{(i)}\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix};\text{(ii)}\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}.$$

In case (i), the j-th element of $K_1^{(1,i)}$ is 1; and in case (ii), the j-th element of $K_1^{(1,i)}$ is 0. From the above analysis, it follows that the j-th column of M is the following four cases.

$$\begin{aligned}&\begin{pmatrix}0&1&1&1&1\end{pmatrix}^T,\begin{pmatrix}0&1&1&0&0\end{pmatrix}^T,\\&\begin{pmatrix}0&0&1&1&0\end{pmatrix}^T,\begin{pmatrix}0&0&1&0&1\end{pmatrix}^T.\end{aligned}\tag{13}$$

(1.2) The j-th element of $K_1^{(1,i)}$ takes the value 0. This means that $P_i^{(1)}$ measures the corresponding particles in G_2 and G_3 with the B_x base, and the j-th column element of $(K_2^{(1,i)}, K_3^{(1,i)})$ will take the following two cases.

$$\text{(i)}\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix};\text{(ii)}\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix}.$$

In case (i), the j-th element of $K_1^{(1,i)}$ is 1; and in case (ii), the j-th element of $K_1^{(1,i)}$ is 0. From the above analysis, it is clear that the j-th column element of M is in the following four cases.

$$\begin{aligned}&\begin{pmatrix}0&1&0&1&0\end{pmatrix}^T,\begin{pmatrix}0&1&0&0&1\end{pmatrix}^T,\\&\begin{pmatrix}0&0&0&1&1\end{pmatrix}^T,\begin{pmatrix}0&0&0&0&0\end{pmatrix}^T.\end{aligned}\tag{14}$$

Case (2) When the j-th portion of S is 1, i.e., the j-th entangled state that S is encoded as $|\mathrm{GHZ}_{000}\rangle$, in this case, there are two ways that $K_1^{(1,i)}$ can be evaluated.

(2.1) The j-th element of $K_1^{(1,i)}$ takes the value 1. This means that $P_i^{(1)}$ measures the particles in the corresponding G_2 and G_3 with the B_y-base, and then the j-th column of $(K_2^{(1,i)}, K_3^{(1,i)})$ takes the following two cases.

$$\text{(i)}\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix};\text{(ii)}\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix}.$$

In case (i), the j-th element of $K_1^{(1,i)}$ is 1; and in case (ii), the j-th element of $K_1^{(1,i)}$ is 0. From the above analysis, it follows that the j-th column of M is the following four cases.

$$\begin{aligned}&\begin{pmatrix}1&1&1&1&0\end{pmatrix}^T,\begin{pmatrix}1&1&1&0&1\end{pmatrix}^T,\\&\begin{pmatrix}1&0&1&1&1\end{pmatrix}^T,\begin{pmatrix}1&0&1&0&0\end{pmatrix}^T.\end{aligned}\tag{15}$$

(2.2) The j-th element of $K_1^{(1,i)}$ takes the value 0. This means that $P_i^{(1)}$ measures the particles in the corresponding G_2 and G_3 with the B_x base, and the j-th column element of $(K_2^{(1,i)}, K_3^{(1,i)})$ is either

$$\text{(i)}\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix};\text{(ii)}\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}.$$

In case (i), the j-th element of $K_1^{(1,i)}$ is 1; and in case (ii), the j-th element of $K_1^{(1,i)}$ is 0.

From the above analysis, it is clear that the j-th column of M is in the following four cases.

$$\begin{array}{c}\begin{pmatrix}1 & 1 & 0 & 1 & 1\end{pmatrix}^T, \begin{pmatrix}1 & 1 & 0 & 0 & 0\end{pmatrix}^T, \\ \begin{pmatrix}1 & 0 & 0 & 1 & 0\end{pmatrix}^T, \begin{pmatrix}1 & 0 & 0 & 0 & 1\end{pmatrix}^T.\end{array} \tag{16}$$

Equations (13)–(16) give all the values of the j-th row element of the matrix M, which shows that the first column of M is exactly the sum of the remaining four rows; thus, we have proven that $S = K_A^{(1,i)} \oplus K_1^{(1,i)} \oplus K_2^{(1,i)} \oplus K_3^{(1,i)}$. Therefore, $P_i^{(1)}(i \in \{1, 2, \cdots, t_1\})$ will finally obtain the key S distributed by Alice.

Using these steps of $P_i^{(1)}$, reconstructing the key in Theorem 3, participant $P_i^{(2)}(i \in \{1, 2, \cdots, i-1, i+1, \cdots, t_2\})$ can also obtain the distributed key S in the same way.

4.2. Security Analysis of the Protocol

The security of the protocol relies on the decoy particle sequences randomly inserted during the transmission of quantum information. In this protocol, Alice sends randomly selected particles from sequences G_2 and H_2 to participant $P_i^{(1)}$ from the set $P^{(1)}$ and randomly selected particles from sequences G_3 and H_3 to participant $P_1^{(2)}$ from the set $P^{(2)}$. Then, when these information particles are transmitted according to Figure 2a, the decoy particles are also interspersed with the information particle sequence until $P_i^{(1)}$ receives the particles from sequence G_2 and G_3, and the particles in sequence H_2 and H_3. $P_i^{(1)}$ will detect this round of communication by detecting particles from the decoy state sequences H_2 and H_3.

If the measurement is above a certain threshold, it indicates that there is the presence of an external eavesdropper, Eve. This means that any attack from an external eavesdropper will be detected with a certain probability during the eavesdropping inspection phase. That is to say, this protocol can prevent eavesdropping from external attackers, thus, achieving the security of the scheme. In essence, this prevents eavesdropping by external attackers. The types of attacks that the protocol can resist are further discussed below based on certain properties.

4.2.1. Direct Measurement by the Attacker

If the eavesdropper Eve attacks the two particles in the GHZ state by measuring the two transmitting particles, which are distributed to participants from the set $P^{(1)}$ and $P^{(2)}$, respectively. However, Eve cannot measure both particles at the same time, she can only measure one of them.

Assuming that the i-th initial GHZ state is $|\varphi_i\rangle = \left[\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right]$, then, after Alice performs the phase shift operation $U_1(2\pi - S + S_0)$ on the first particle in the quantum state $|\varphi_i\rangle$, the participants perform the phase shift operation on $|\varphi_i\rangle$ in turn.

After Alice has operated on the quantum state $|\varphi_i\rangle$, suppose that $l_1(l_1 \in \{1, 2, \cdots, t_1\})$ participants from the set $P^{(1)}$ have performed l_1 operations and $l_2(l_2 \in \{1, 2, \cdots, t_2\})$ participants from the set $P^{(2)}$ have performed l_2 operations. Using Theorems 1 and 2, it follows that the quantum state $|\varphi_i\rangle$ then becomes

$$|\varphi_i'\rangle = \frac{1}{\sqrt{2}}(|000\rangle + e^{i\cdot\alpha}|111\rangle), \tag{17}$$

where $\alpha = (2\pi - S + S_0) + \sum_{r=1}^{l_1} S_{(i+r) \bmod t_1}^{(1)} + \sum_{r=1}^{l_2} S_{r \bmod t_2}^{(2)}$.

From Equation (6), the probability of each particle in the GHZ state existing in state $|0\rangle$ or $|1\rangle$ is

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}e^{i\cdot\alpha}\right|^2 = \frac{1}{2}.$$

Furthermore, since $l_i (i = 1, 2)$ was arbitrary, it was impossible for Eve to obtain any useful information by measuring the GHZ particles that had been passed on.

4.2.2. Interception–Relaunch Attack

Eve may have intercepted the particles in the participants' hands and sent her own counterfeit particles to the participants. In this case, Eve cannot obtain any information about the key. This is because it is known from this protocol construction process that the entire key is obtained through the post-processing phase after the transferring the particle sequences $G^{(2)}$ and $G^{(3)}$ from the GHZ sequence $\{|\varphi_1\rangle, |\varphi_2\rangle, \dots, |\varphi_m\rangle\}$, during which the original quantum sequence $\{|\varphi_1\rangle, |\varphi_2\rangle, \dots, |\varphi_m\rangle\}$ requires the phase shifting operations of each participant, and these unitary matrices are known only by each participant.

Even if Eve tries to intercept the last round of particles, we suppose that the $P_i^{(1)} (i \in \{1, 2, \cdots, t_1\})$ can reconstruct the key. Specifically, if Eve had managed to intercept particles from $P^{(1)}_{(i+t_1-1)mod t_1}$ to $P_i^{(1)}$ or $P_{t_2}^{(2)}$ to $P_i^{(1)}$, it would also have been impossible for Eve to have obtained particles from the original quantum state sequence $\{|\varphi_1\rangle, |\varphi_2\rangle, \dots, |\varphi_m\rangle\}$, since the original quantum state sequence $\{|\varphi_1\rangle, |\varphi_2\rangle, \dots, |\varphi_m\rangle\}$ could only be restored after $P_i^{(1)}$ had received the returned particles and performed a phase shift operation. As a result, Eve could not obtain any information about the key.

4.2.3. Entanglement Measurement Attack

Eve tries to launch an entanglement attack when the participants from the sets $P^{(1)}$ and $P^{(2)}$ each transport particles. Let us set that, when the participant $P_i^{(1)} (i \in \{1, 2, \cdots, t_1\})$ from the set $P^{(1)}$ passes $G_2^{(u)}$ particles of $|\varphi_u\rangle$-state to $P^{(1)}_{i+1(\text{mod} t_1)}$, Eve launches an entanglement attack, and the auxiliary qubit is $|E_{init}\rangle$, while the entanglement bit and the auxiliary qubit form a hybrid quantum state,

$$\left|\Psi_{AP_i^{(1)}P_j^{(2)}E}\right\rangle = |\varphi_u\rangle \otimes |E_{\text{init}}\rangle,$$

where $A, P_i^{(1)}, P_j^{(2)}, E$ denote the holders of four particles from the entangled state $\left|\Psi_{AP_i^{(1)}P_j^{(2)}E}\right\rangle$ Alice, $P_i^{(1)}, P_j^{(2)}$ and Eve, respectively, where $i \in \{1, 2, \cdots, t_1\}, j \in \{1, 2, \cdots, t_2\}$.

The attacker applies a quantum operation to $\left|\Psi_{AP_i^{(1)}P_j^{(2)}E}\right\rangle$ by a unitary transformation $U(\varepsilon)$ to obtain

$$\begin{aligned} U(\varepsilon)\left|\Psi_{AP_i^{(1)}P_j^{(2)}E}\right\rangle &= U(\varepsilon)(|\varphi_u\rangle \otimes |E_{\text{init}}\rangle) \\ &= U(\varepsilon)\left[\frac{1}{\sqrt{2}}\left(\left|0_A 0_{P_i} 0_{P_j}\right\rangle + \left|1_A 1_{p_i^{(1)}} 1_{P_j^{(2)}}\right\rangle\right) \otimes |E_{\text{init}}\rangle\right]. \end{aligned}$$

Since $|E_{\text{init}}\rangle$ is a qubit $|0_E\rangle$ or $|1_E\rangle$, let us say that $|E_{\text{init}}\rangle = |0_E\rangle$, and let the $U(\varepsilon)$ act on the particles held by $P_i^{(1)}$ and Eve. Then, we have

$$\begin{aligned} U(\varepsilon)\left|\Psi_{AP_i^{(1)}P_j^{(2)}E}\right\rangle &= U(\varepsilon)\left(\left|\Phi^+\right\rangle \otimes |0_E\rangle\right) \\ &= U(\varepsilon)\left[\frac{1}{\sqrt{2}}\left(\left|0_A 0_{P_i^{(1)}} 0_{P_j^{(2)}}\right\rangle + \left|1_A 1_{P_i^{(1)}} 1_{P_j^{(2)}}\right\rangle\right) \otimes |0_E\rangle\right] \\ &= U(\varepsilon)\left[\frac{1}{\sqrt{2}}\left(\left|0_A 0_{P_1^{(1)}} 0_{P_j^{(2)}} 0_E\right\rangle + \left|1_A 1_{P_i^{(1)}} 1_{P_j^{(2)}} 0_E\right\rangle\right)\right]. \end{aligned}$$

According to the Schmidt decomposition of the quantum state, let

$$\begin{aligned}U(\varepsilon)\left|0_{P_i^{(1)}}0_E\right\rangle &= \left|0_{P_i^{(1)}}\right\rangle \otimes E_1 + \left|1_{P_1^{(1)}}\right\rangle \otimes E_2,\\ U(\varepsilon)\left|1_{P_i^{(l)}}0_E\right\rangle &= \left|0_{P_i^{(1)}}\right\rangle \otimes \tilde{E}_1 + \left|1_{P_i^{(1)}}\right\rangle \otimes \tilde{E}_2.\end{aligned}$$

and then

$$\begin{aligned}U(\varepsilon)\left|\Psi_{AP_i^{(1)}P_j^{(2)}E}\right\rangle &= U(\varepsilon)\left[\frac{1}{\sqrt{2}}\left(\left|0_A0_{P_i^{(1)}}0_{P_j^{(2)}}0_E\right\rangle + \left|1_A1_{P_i^{(1)}}1_{p_j^{(2)}}1_E\right\rangle\right)\right]\\ &= \left|0_A0_{P_t^{(1)}}0_{P_j^{(2)}}\right\rangle \otimes |E_1\rangle + \left|0_A0_{P_t^{(1)}}1_{P_j^{(2)}}\right\rangle \otimes |E_2\rangle\\ &+\left|1_A1_{p_t^{(1)}}0_{P_j^{(2)}}\right\rangle \otimes |\tilde{E}_1\rangle + \left|1_A1_{p_t^{(1)}}1_{P_j^{(2)}}\right\rangle \otimes |\tilde{E}_2\rangle.\end{aligned} \tag{18}$$

where $|E_1\rangle \perp |E_2\rangle, \left|\tilde{E}_1\right\rangle \perp \left|\tilde{E}_2\right\rangle$, and $\left\langle E_1 \mid \tilde{E}_2\right\rangle + \left\langle E_2 \mid \tilde{E}_1\right\rangle = 0$.

From Equation (12) and the key generation process of this protocol, it is clear that Eve cannot obtain any information about the key from $U(\varepsilon)\left|\Psi_{AP_i^{(1)}P_j^{(2)}E}\right\rangle$.

5. Comparisons

We analyzed and compared the proposed QSS protocol with several similar existing QSS protocols—namely, RP2015 [22], YGWQZW2015 [26], BLWLL2018 [16], and LYZ2021 [25], based on four parameters, including the universality of the scheme, communication costs, computational costs, and the efficiency of the scheme as shown in Table 2. First, the similarity of these schemes is that their access structure is a kind of special threshold structure.

Universality is shown in Table 2, which includes the theoretical basis of these schemes' dependency, the adaptive access structure, the trajectory of information particles, the number of participants who ultimately calculate the key, and the key validation. Communication costs are based on the transmitted particles, i.e., information particles and decoy particles. The cost is calculated according to the following three parameters: the unitary operation, the measurement operation, and the hash function. Finally, we give the efficiency of each scheme.

Table 2. Comparisons among several kinds of multi-party QKA protocols.

	RP2015 [22]	**YGWQZW2015 [26]**	**BLWLL2018 [16]**	**LYZ2021 [25]**	**Our Scheme**
Number of participants reconstruction key	2	2	k	1	1
Information particle trajectories	Tree form	Tree form	Tree form	Single circle	Double circle
Information quantum states	GHZ state (with t particles)	GHZ state (with t particles)	GHZ state (with t particles)	Generalised Bell state (with two particles)	GHZ state (with three particles)
The dimension of information quantum states	2	k	k	k	2
Detection of quantum states	GHZ state (with t particles)	Single photon	GHZ state (with t particles)	Single photon	Three dimensions GHZ state
Number of measurements	$t(m+L)$	$t(m+L)$	$t(m+L)$	$t(2m+l)$	$3(m+L)$
Number of unitary operations	0	0	0	$t+1$	$t+1$
Hash function	N	N	N	Y	Y
Information efficiency	$\frac{m}{t(m+L)}$	$\frac{m}{t(m+L)}$	$\frac{m}{t(m+L)}$	$\frac{m}{t(2m+l)}$	$\frac{m}{3(m+L)}$

Information Efficiency η [32] is defined as $\eta = \frac{c}{q}$, in which c represents the number of classical bits shared and q represents the total number of qubits transmitted within a quantum channel. According to this efficiency formula, the information efficiency of a protocol sharing m classical information can be expressed as $\eta = \frac{m}{n_1 m + n_2 v}$, where n_1 represents the number of particles contained in each quantum state when m bits of classical information are converted to m quantum state information. n_2 represents the number of particles contained in each quantum state in which the eavesdropping is detected. Furthermore, v represents the number of quantum states in which the eavesdropping is detected. Let $v = L$ when the detected particles are entangled, and let $v = l$ when the detected particles are single photons.

For the sake of parameter uniformity, the communication and computational costs required to recover the key once for t participants in each scenario are calculated in Table 1. The following is an analysis and comparison among RP2015 [22], YGWQZW2015 [26], BLWLL2018 [16], LYZ2021 [25], and our proposal.

(1) RP2015 Protocol The RP2015 protocol distribution model is a tree structure, i.e., the distributor distributes t information particles from the GHZ state to t participants, all from the two-dimensional Hilbert space. m GHZ states are used to share m bits of classical information, while L GHZ states are applied to detect eavesdropping . Thus, the information efficiency of both schemes is $\frac{m}{t(m+L)}$. The access structure of the participants in this distribution model is a restricted threshold structure, which is also a fully bipartite graph structure.

(2) YGWQZW2015 Protocol The distribution YGWQZW2015 model is a tree structure, i.e., the distributor distributes t information particles from the GHZ state to t participants, unlike in the BLWLL2018 protocol [16] where these particles are all from the K-dimensional Hilbert space. m GHZ states are used to share m bits of classical information, while L GHZ states are applied to detect eavesdropping. Therefore, the information efficiency of this scheme is $\frac{m}{t(m+L)}$. The access structure of the participants in this allocation model belongs to the fully bipartite graph.

(3) BLWLL2018 Protocol This distribution model of the BLWLL2018 scheme is also a tree structure, i.e., the distributor distributes t information particles from the GHZ state to t participants, all of which come from the k-dimensional Hilbert space. m GHZ states are used to share m bits of classical information, while L GHZ states are applied to detect eavesdropping. Therefore, the information efficiency of this scheme is $\frac{m}{t(m+L)}$. Unlike the YGWQZW2015 protocol, the access structure of the participants in this distribution model is a restricted threshold structure and also a fully bipartite graph structure.

(4) LYZ2021 Protocol The LYZ2021 distribution model of the LYZ2021 scheme is a one circle structure, where the distributor distributes a particle of information from a generalized Bell state to one of the participants, and the particle is then passed through t participants in turn, where the two particles in the Bell state are from the k-dimensional Hilbert space. m-generalised Bell states are used to share m-bit classical information, while l X-bases and Z-bases are applied to detect eavesdropping. Thus, the information efficiency of the scheme is $\frac{m}{t(m+l)}$.

(5) Our Protocol This distribution model of our scheme is a bicyclic structure, i.e., the distributor distributes two information particles from the GHZ state to t participants according to the requirements of a fully bipartite graph structure, where the three particles from the GHZ state are from a three-dimensional Hilbert space. m GHZ states are used to share m-bit classical information, while L GHZ states are applied to detect eavesdropping. Thus, the information efficiency of both schemes is $\frac{m}{3(m+L)}$.

In the protocol proposed, the quantum states corresponding to the information particles and the detection particles are three-dimensional GHZ states, and are only detected between Alice and $P_i^{(1)}$ (or $P_j^{(2)}$), where $(m+L)$ three-dimensional GHZ states are used as information quantum states and detection quantum states, m-dimensional bits of classical information are obtained, and the efficiency of the scheme is $\frac{m}{3(m+L)}$. It can be seen that the scheme in this paper significantly saves quantum resources and is significantly more efficient than the above schemes.

6. Conclusions

In this paper, we proposed an efficient quantum secret sharing scheme for restricted gated access structures. The three-dimensional GHZ state of this scheme was used for the key transfer and the detection of the decoy state particles, and the distributor did not need to send the particles that she holds to the key reconstruction during the detection of the decoy state particles and the reconstruction of the key. This protocol is more practical, secure, and quantum resource efficient compared with similar processes.

Author Contributions: L.L. and Z.L. contributed the idea. L.L. performed the calculations, made formal reasoning and wrote the main manuscript. Z.L. improved the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China OF FUNDER grant number 12201484.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. How to share a secret. *Commun. Acm.* **1979**, *22*, 612–613. [CrossRef]
2. Blakley, G. Safeguarding cryptographic keys. In Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK), New York, NY, USA, 4–7 June 1979; Volume 48, pp. 313–317.
3. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–19 December 1984; pp. 175–179.
4. Goldenberg, L.; Vaidman, L. Quantum cryptography based on orthogonal states. *Phys. Rev. Lett.* **1995**, *75*, 1239. [CrossRef] [PubMed]
5. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
6. Cleve, R.; Gottesman, D.; Lo, H. How to share a quantum secret. *Phys. Rev. Lett.* **1999**, *83*, 648–651. [CrossRef]
7. Hillery, M.; Buzek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [CrossRef]
8. Guo, G.P.; Guo, G.C. Quantum secret sharing without entanglement. *Phys. Rev. A* **2003**, *310*, 247–251. [CrossRef]
9. Hsu, L. Quantum secret-sharing protocol based on Grover's algorithm. *Phys. Rev. A* **2003**, *68*, 022306. [CrossRef]
10. Zhang, Z.; Li, Y.; Man, Z. Multiparty quantum secret sharing. *Phys. Rev. A* **2005**, *71*, 044301. [CrossRef]
11. Bai, C.M.; Li, Z.H.; Li, Y.M. Improving fidelity of quantum secret sharing in noisy environments. *Eur. Phys. J. D* **2018**, *72*, 126. [CrossRef]
12. Zhang, K.; Zhang, X.; Jia, H.; Zhang, L. A new n-party quantum secret sharing model based on multiparty entangled states. *Quantum Inf. Process.* **2019**, *18*, 81. [CrossRef]
13. Sutradhar, K.; Om, H. Efficient quantum secret sharing without a trusted player. *Quantum Inf. Process.* **2020**, *19*, 73. [CrossRef]
14. Chou, Y.H.; Zeng, G.J.; Chen, X.Y.; Kuo, S.Y. Multiparty weighted threshold quantum secret sharing based on the Chinese remainder theorem to share quantum information. *Sci. Rep.* **2021**, *11*, 6093. [CrossRef]
15. Tavakoli, A.; Herbauts, I.; Zukowski, M.; Bourennane, M. Secret sharing with a single d-level quantum system. *Phys. Rev. A* **2015**, *92*, 030302(R). [CrossRef]
16. Bai, C.M.; Li, Z.H.; Wang, J.T.; Liu, C.J.; Li, Y.M. Restricted (k, n)-threshold quantum secret sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. *Quantum Inf. Process.* **2018**, *17*, 312 [CrossRef]
17. Liu, L.J.; Li, Z.H.; Han, Z.W.; Zhi, D.L. A quantum secret sharing scheme with veriable function. *Eur. Phys. J. D* **2020**, *74*, 154. [CrossRef]
18. Hsu, L.Y. Quantum Secret Sharing Using Product Statesm. *Phys. Rev. A* **2005**, *71*, 159. [CrossRef]
19. Yang, Y.G.; Wen, Q.Y.; Zhu, F.C. An Efficient Quantum Secret Sharing Protocol with Orthogonal Product States. *Sci. China Ser. G* **2007**, *50*, 331–338. [CrossRef]
20. Xu, J.; Chen, H.W.; Liu, W.J.; Liu, Z.H. An Efficient Quantum Secret Sharing Scheme Based on Orthogonal Product States. In Proceedings of the IEEE Congress on Evolutionary Computation, Barcelona, Spain, 18–23 July 2010; pp. 1–4.

21. Gheorghiu, V.; Sanders, B.C. Accessing quantum secrets via local operations and classical communication. *Phys. Rev. A* **2013**, *88*, 022340. [CrossRef]
22. Rahaman, R.; Parker, M.G. Quantum secret sharing based on local distinguishability. *Phys. Rev. A* **2015**, *91*, 022330. [CrossRef]
23. Wang, J.; Li, L.; Peng, H.; Yang, Y. Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. *Phys. Rev. A* **2017**, *95*, 022320. [CrossRef]
24. Li, M.S.; Shi, F.; Wang, Y.L. Local discrimination of generalized Bell states via commutativity. *Phys. Rev. A* **2022**, *105*, 032455. [CrossRef]
25. Li, F.L.; Yan, J.Y.; Zhu, S.X. General quantum secret sharing scheme based on two-Qudit. *Quantum Inf. Process.* **2021**, *20*, 328. [CrossRef]
26. Yang, Y.H.; Gao, F.; Wu, X.; Qin, S.; Zuo, H.; Wen, Q. Quantum secret sharing via local operations and classical communication. *Sci. Rep.* **2015**, *5*, 16967. [CrossRef] [PubMed]
27. Qin, H.; Zhu, X.; Dai, Y. (t, n) threshold quantum secret sharing using the phase shift operation. *Quantum Inf. Process.* **2015**, *14*, 2997–3004. [CrossRef]
28. Nielsen, M.A.; Chuang, I. *Quantum Computation and Quantum Information*; Cambridge University: Cambridge, UK, 2002.
29. Song, X.; Liu, Y.; Deng, H.; Xiao, Y. (t, n) threshold d-level quantum secret sharing. *Sci. Rep.* **2017**, *7*, 6366. [CrossRef]
30. Lu, C.; Miao, F.; Meng, K.; Yu, Y. Threshold quantum secret sharing based on single qubit. *Quantum Inf. Process.* **2018**, *17*, 64. [CrossRef]
31. Yan, C.H.; Li, Z.H.; Liu, L.; Lu, D.J. Cheating identifiable (k, n) threshold quantum secret sharing scheme. *Quantum Inf. Process.* **2022**, *21*, 8. [CrossRef]
32. Cabello, A. Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* **2000**, *85*, 5635–5638. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.