

A pure quantum secret sharing scheme based on GHZ basis measurement and quantum entanglement exchange

Bai Liu(刘白), Jun Zhang(张俊), Shupin Qiu(邱书品), and Mingwu Zhang(张明武)

Citation: Chin. Phys. B, 2025, 34 (**3**): 030304. DOI: 10.1088/1674-1056/ada548
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Improvement and security analysis of multi-ring discrete modulation continuous variable quantum secret sharing scheme

Huan-Yao Jiang(姜欢窈), Min Nie(聂敏), Guang Yang(杨光), Ai-Jing Sun(孙爱晶), Mei-Ling Zhang(张美玲), and Chang-Xing Pei(裴昌幸)
Chin. Phys. B, 2024, 33 (**7**): 070303. DOI: 10.1088/1674-1056/ad3b81

Verifiable quantum secret sharing scheme based on orthogonal product states

Chen-Ming Bai(白晨明), Lu Liu(刘璐), and Sujuan Zhang(张素娟)
Chin. Phys. B, 2024, 33 (**7**): 070302. DOI: 10.1088/1674-1056/ad342a

Cryptanalysis of efficient semi-quantum secret sharing protocol using single particles

Gan Gao(高甘)
Chin. Phys. B, 2024, 33 (**4**): 040301. DOI: 10.1088/1674-1056/ad2bee

An efficient multiparty quantum secret sharing scheme using a single qudit

Wenwen Hu(胡文文), Bangshu Xiong(熊邦书), and Rigui Zhou(周日贵)
Chin. Phys. B, 2023, 32 (**8**): 080303. DOI: 10.1088/1674-1056/aca391

Efficient semi-quantum secret sharing protocol using single particles

Ding Xing(邢丁), Yifei Wang(王艺霏), Zhao Dou(窦钊), Jian Li(李剑),Xiubo Chen(陈秀波), and Lixiang Li(李丽香)
Chin. Phys. B, 2023, 32 (**7**): 070308. DOI: 10.1088/1674-1056/ace159

SPECIAL TOPIC — Quantum communication and quantum network

A pure quantum secret sharing scheme based on GHZ basis measurement and quantum entanglement exchange

Bai Liu(刘白)†, Jun Zhang(张俊), Shupin Qiu(邱书品), and Mingwu Zhang(张明武)

School of Computer Science, Hubei University of Technology, Wuhan 430068, *China*

(Received 28 June 2024; revised manuscript received 21 December 2024; accepted manuscript online 3 January 2025)

At present, most quantum secret sharing (QSS) protocols are more or less designed with the incorporation of classical secret sharing schemes. With the increasing maturity of quantum technology, QSS protocols based on pure quantum mechanics are becoming more important. Classical secret sharing schemes cannot achieve absolute security, and their involvement can compromise the security of QSS protocols. This paper proposes a QSS scheme based on Greenberger–Horn–Zeilinger (GHZ) basis measurement and quantum entanglement exchange. In this protocol, the secret sender stores the secret information using Pauli operations. Participants obtain their shares by measuring the product state sequentially. Finally, participants complete the secret reconstruction through quantum entanglement exchange and other related quantum operations. In addition, the particles held by participants in the protocol do not contain any secret information. Each participant's particles are in a state of maximum entanglement, and no participant can deduce the particle information of other participants through their own particles. At the same time, the protocol is based on pure quantum mechanics and does not involve classical schemes, which avoids the problem of reduced security of the protocol. Security analysis indicates that the protocol is not vulnerable to retransmission interception and collusion attacks. Moreover, it is capable of detecting and terminating the protocol promptly when facing with attacks from dishonest participants.

Keywords: quantum secret sharing, projection measurement, quantum entanglement exchange, threshold

PACS: 03.67.–a, 03.67.Hk, 03.65.ud

DOI: 10.1088/1674-1056/ada548 **CSTR:** 32038.14.CPB.ada548

1. Introduction

1.1. Background

Nowadays, when people engage in important secrecy activities and pay large amounts of money, they tend to divide the secret into multiple parts and distribute them to more parties. The activity of sharing secrets among multiple parties is termed secret sharing (SS), and it has significant applications in areas such as voting,[1] signatures,[2] and identity verification.[3] In 1979, Shamir[4] proposed the first secret sharing protocol based on Lagrange interpolation formula. There are two main forms of common secret sharing schemes: the (n, n) threshold SS protocol and the (t, n) threshold SS protocol. In the (n, n) threshold SS protocol,[5] the secret is divided into n parts and distributed to n participants respectively. The secret can only be recovered when the n participants cooperate with each other, and each participant is crucial to the reconstruction of the secret. In the (t, n) threshold SS protocol,[6] any t $(t \leq n)$ of n participants can recover the secret; that is, the size of each eligible set is at least t. This protocol does not require every participant to participate in the secret reconstruction process, so it is more flexible than the (n, n) threshold SS protocol. But in (t, n) threshold SS protocol, all participants have different influences on the recovery process, and some participants do not even participate in a recovery process. Classical secret sharing schemes usually do not consider the secure transmission between the secret sender and participants, and either leave this problem to other confidentiality protocols, or assume that shares are distributed through a secure classical channel in the secret distribution phase.[7] At the same time, the security of most classical schemes is based on complex mathematical problems related to computation, which reduces the efficiency of the scheme. With the rapid development of quantum information and quantum computing, the field of cryptography has begun to look for ways to combat quantum computer attacks. Using the properties of quantum and the no-cloning theorem, Bennett and Brassard[8] proposed a quantum key distribution (QKD) protocol. The security of QKD was based on the principle of quantum physics, and QKD was proved to be unconditionally secure,[9] which greatly promoted significant progress in cryptography. Subsequently, cryptographers have developed more and more quantum secret sharing (QSS) schemes.

1.2. Related work

Up to now, QSS protocols have made significant progress, and schemes designed from various angles emerge in an endless stream. Since then scholars have proposed many more perfect QSS protocols; they are roughly classified as based

†Corresponding author. E-mail: liubai@hbut.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

on single qubit,[10,11] Bell state[12,13] and Greenberger–Horn–Zeilinger (GHZ) state.[14] In 1999, Hillery *et al.*[15] proposed the QSS protocol using GHZ quantum state for the first time. The protocol does not take into account the impact of dishonest participants. To detect external attackers and dishonest internal parties, some verifiable QSS protocols have been proposed.[16,17] These papers mainly verify the identity of the participant and the accuracy of the message sent. In the identity authentication scheme, the receiver proves whether the sender is a legitimate participant by authentication method before establishing communication channel, so as to avoid the situation that external attackers impersonate the participant. Since additional identity authentication for participants will waste resources, in 2020 Kartick Sutradhar *et al.*[18] proposed a QSS scheme that does not rely on a trusted party. A variety of QSS schemes have also been proposed based on quantum Fourier transform (QFT). For example, in 2013, Yang *et al.*[19] designed an (n, n) threshold QSS using Pauli operators and QFT. In 2016, Qin *et al.*[20] proposed a verifiable (t, n) threshold QSS scheme based on D-dimensional Bell states. In this scheme, the secret sender distributes shares to participants through quantum-secure direct communication. During the secret reconstruction phase, the secret sender creates a Bell state in a d-dimensional Hilbert space, and the players execute Pauli operations on the Bell state to retrieve the secret. Then, Hu *et al.*[21] proposed an efficient QSS scheme utilizing high-dimensional single qubits. In 2017, Song *et al.*[22] proposed a d-dimensional (t, n) threshold QSS based on Shamir's SS[4] and Lagrange interpolation formula, but the scheme was infeasible due to the limitation of participant shares. In 2020, Mashhadi[23] pointed out the problems existing in the protocol proposed by Song *et al.*[22] and gave an improvement scheme. In 2019, Samaneh Mashhadi[24] proposed a general QSS based on QFT. In this paper, called the monotone span program (MSP), access structure and QFT are integrated. The scheme has the advantages of both classical and QSS schemes. In its secret distribution phase, it uses quantum state sharing instead of a classical public key protocol to resist the attack of quantum computer. In the secret reconstruction phase, quantum computing methods such as QFT and d-dimensional Pauli operations are used, so that a participant does not know the shares of other participants. Most of the advantages of QFT-based QSS models are the use of D-dimensional quantum states instead of two-dimensional quantum states to increase the practicability of the scheme. In 2022, Xu *et al.*[25] proposed a multi-party QSS protocol based on GHZ state particle entanglement exchange and GHZ basis measurement. Firstly, the "characteristic" of the GHZ state was defined, and then multiple groups of GHZ states were used to exchange arbitrary particles without changing the "characteristic". The relationship between the "characteristic" of the measurement result, the "characteristic" of the initial state and the "characteristic" of the Pauli operator is proved, and then the protocol is completed by combining the classical scheme.

Most of the schemes mentioned above combine classical protocols with quantum protocols. In today's advancing quantum technology, the incorporation of classical schemes renders the entire protocol vulnerable to quantum attacks.

1.3. Contribution

Classical secret sharing occupies an important proportion of the QSS schemes mentioned above and some existing QSS schemes, which weakens the anti-jamming ability of QSS because the classical secret sharing scheme cannot achieve unconditional security. In this paper, we propose a three-party QSS protocol where the secret sender generates a product state related to the GHZ state and stores the classical secret. Then, the particles in the product state are sent to each participant according to the requirements, and the participant recovers the original product state through measurement and quantum entanglement exchange to complete the secret transmission. The particles transmitted in this protocol do not carry any information. At the same time, this paper uses GHZ states as quantum resources, and uses pure quantum mechanics as the theoretical basis, without the fusion of classical schemes, so as to avoid the problem of reduced security of the protocol. So if a perfect quantum channel is used, the protocol is secure. This paper specifically shows a (3,3)-threshold QSS, which can be extended to (n, n)-threshold QSS.

1.4. Organization

The rest of this paper is organized as follows. In Section 2 we give the preliminaries needed for this paper. In Section 3, we propose a concrete (3, 3)-threshold QSS scheme. In Section 4, we analyze the security of the protocol. In Section 5, we compare and analyze this protocol with some previous protocols. In Section 6, we summarize the paper and draw conclusions.

2. Preliminaries

2.1. GHZ State

The three-particle GHZ state has widespread applications in quantum communication. In 1989, Greenberger and others studied a class of maximally entangled states involving three or more particles (GHZ states). There are eight three-particle entangled GHZ states, written as follows:

$$|\psi_{000}\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \quad |\psi_{001}\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle),$$

$$|\psi_{010}\rangle = \frac{1}{\sqrt{2}}(|111\rangle + |000\rangle), \quad |\psi_{011}\rangle = \frac{1}{\sqrt{2}}(|111\rangle - |000\rangle),$$

$$|\psi_{100}\rangle = \frac{1}{\sqrt{2}}(|101\rangle + |010\rangle), \quad |\psi_{101}\rangle = \frac{1}{\sqrt{2}}(|101\rangle - |010\rangle),$$

$$|\psi_{110}\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle),\ |\psi_{111}\rangle = \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle). \tag{1}$$

The characteristics of a three-particle GHZ entangled state are as follows: measuring the state of the first particle does not determine the states of the other two particles; it only reveals whether the other two particles are in the same state. When further determining the state of the second particle, the state of the third particle can be accurately inferred without measurement.

2.2. Pauli operation

Here, we introduce four types of Pauli operations

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|,\ Z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$
$$X = |0\rangle\langle 1| + |1\rangle\langle 0|,\ Y = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{2}$$

Each Pauli operator can induce the following transformations on quantum states $|0\rangle$ or $|1\rangle$, thereby enabling conversions between different GHZ states:

$$I|0\rangle = |0\rangle,\ I|1\rangle = |1\rangle,\ Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle,$$
$$X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle,\ Y|0\rangle = -|1\rangle,\ Y|1\rangle = |0\rangle. \tag{3}$$

3. The proposed protocol

3.1. Protocol design

Dealer D uses Pauli operations I, Z, Y, and X to correspond to the classical message it wants to deliver. We consider that the participants in this scheme are P_1, P_2, and P_3. Dealer D randomly selects one of the eight GHZ states to create a product state $|\phi\rangle$, without losing the general assumption, the choice is $|\psi_{000}\rangle$. The requirement that at least one participant be honest in our protocol, assuming that P_1 is honest, has several real-life applications. For instance, in a business setting, there are two types of employees: managers (P_1) and regular employees (P_2, P_3). The boss (D) intends to communicate confidential information to all employees (P_1, P_2, P_3). The manager is an employee whom the boss trusts, and the boss selects a trustworthy individual to serve as the manager to oversee the enterprise.

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{123} \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{456} \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{789}. \tag{4}$$

With all three participants, D assigns particles to the corresponding users via a quantum channel, and the security of this quantum channel can be ensured by incorporating decoy particles. Assume that P_1 gets qubits 1, 5 and 6, P_2 gets qubits 2, 3 and 9, P_3 gets qubits 4, 7 and 8. This allocation can be any other combination provided each party has a share of the other entangled particle. D will announce in advance that he will only perform Pauli operations on the first particle. The Pauli operation performed by dealer D corresponds to the classical message it intends to deliver. The correspondence is as follows:

$$I_1 = \text{`00'},\ X_1 = \text{`01'},\ Y_1 = \text{`11'},\ Z_1 = \text{`10'}, \tag{5}$$

where the operator Z_1 means that the operator Z is acting on qubit 1, The protocol simultaneously transmits 2-bit classical messages, while 4-bit classical messages are transmitted twice. For instance, the dealer wants to share $s = 9 = 1001$, The dealer will perform two distinct Pauli operations on its product state $-(ZX)_1$.

3.2. Secret distribution

The overall steps of the secret distribution stage are shown in Fig. 1. The dealer creates a quantum system $|\phi'\rangle$ where P_1 obtains share $|\psi_{001}\rangle_{156}$ by performing GHZ-based measurements on particles (1, 5, 6), while the entire quantum system collapses into $|a\rangle$. P_2 obtains its share $|\psi_{100}\rangle_{239}$ by performing GHZ-based measurements on particles (2, 3, 9) in $|a\rangle$. P_3 obtains share $|\psi_{011}\rangle_{478}$ by performing GHZ-based measurements on the remaining three particles (4, 7, 8). At this point, the share allocation phase of the entire scheme has been completed. The specific implementation process consists of the following nine steps:

(i) The dealer D decides to alter the particles of P_1(1,5,6). It also decides to operate the X gate on particle 1, thereby resulting in the state as follows:

$$|\phi'\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123} \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{456} \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{789}. \tag{6}$$

(ii) P_1 decides to measure his share of the entangled particles in the GHZ basis $|\psi_{000}\rangle$, $|\psi_{001}\rangle$, $|\psi_{010}\rangle$, $|\psi_{011}\rangle$, $|\psi_{100}\rangle$, $|\psi_{101}\rangle$, $|\psi_{110}\rangle$, $|\psi_{111}\rangle$. The quantum measurement operators involved in the measurements are as follows:

$$\langle\psi_{000}|_{156} = \frac{1}{\sqrt{2}}(\langle 100| + \langle 011|),$$
$$\langle\psi_{001}|_{156} = \frac{1}{\sqrt{2}}(\langle 100| - \langle 011|),$$
$$\langle\psi_{010}|_{156} = \frac{1}{\sqrt{2}}(\langle 111| + \langle 000|),$$
$$\langle\psi_{011}|_{156} = \frac{1}{\sqrt{2}}(\langle 111| - \langle 000|),$$
$$\langle\psi_{100}|_{156} = \frac{1}{\sqrt{2}}(\langle 101| + \langle 010|),$$
$$\langle\psi_{101}|_{156} = \frac{1}{\sqrt{2}}(\langle 101| - \langle 010|),$$
$$\langle\psi_{110}|_{156} = \frac{1}{\sqrt{2}}(\langle 110| + \langle 001|),$$

$$\langle\psi_{111}|_{156} = \frac{1}{\sqrt{2}}(\langle 110| - \langle 001|). \tag{7}$$

(iii) Without loss of generality, if P_1 is measured as $\langle\psi_{001}|_{156}$, then the entire quantum system will collapse to

$$\begin{aligned}
&\langle\psi_{001}|_{156}|\phi'\rangle \\
&= \frac{1}{\sqrt{2}}(\langle 100| - \langle 011|)_{156} \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123} \\
&\otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{456} \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{789} \\
&= \frac{1}{8}(|\psi_{111}\rangle|\psi_{110}\rangle + |\psi_{110}\rangle|\psi_{111}\rangle \\
&+ |\psi_{011}\rangle|\psi_{100}\rangle + |\psi_{010}\rangle|\psi_{101}\rangle)_{239478}.
\end{aligned} \tag{8}$$

(iv) We refer to the collapsed state following the measurement of P_1 as the $|a\rangle$ state. When P_2 and P_3 measure their respective shares, only the three sets of results in the $|a\rangle$ state are possible.

(v) Since P_1 has access to the seven other GHZ basis projective measurement operators, the possible outcomes of these projective measurements collapse the system into three possible cases as shown in Table 1.

Table 1. The correspondence between P_1 measurements and the collapse state of the system.

P_1's measurement outcome	Collapsed state
$\|\psi_{000}\rangle$	$\frac{1}{8}(\|\psi_{110}\rangle\|\psi_{110}\rangle + \|\psi_{111}\rangle\|\psi_{111}\rangle + \|\psi_{010}\rangle\|\psi_{100}\rangle + \|\psi_{011}\rangle\|\psi_{101}\rangle)_{239478}$
$\|\psi_{010}\rangle$	$\frac{1}{8}(\|\psi_{110}\rangle\|\psi_{100}\rangle - \|\psi_{111}\rangle\|\psi_{101}\rangle + \|\psi_{010}\rangle\|\psi_{110}\rangle - \|\psi_{011}\rangle\|\psi_{111}\rangle)_{239478}$
$\|\psi_{011}\rangle$	$\frac{1}{8}(\|\psi_{111}\rangle\|\psi_{100}\rangle - \|\psi_{110}\rangle\|\psi_{101}\rangle + \|\psi_{011}\rangle\|\psi_{110}\rangle - \|\psi_{010}\rangle\|\psi_{111}\rangle)_{239478}$

(vi) The secret sender D can perform three other operations (I, iY, Z), and for each operation, P_1 each measurement and the corresponding collapse states are calculated in a similar way as when X is operated.

(vii) The secret sender D discloses the initial product state it has prepared and announces that it will perform the Pauli operation on the first particle.

(viii) P_1 announces the results of its GHZ-based measurements performed on particles (1,5,6).

(ix) Participants P_2 and P_3 perform GHZ-based measurements on particles (2,3,9) and (4,7,8), respectively, to obtain their respective shares.

After the completion of share allocation, the entanglement form of particles in the entire system also changes. In Fig. 2, we illustrate the process of changing the entanglement form of the quantum system with each measurement performed. The circles with colors and numbers in the figure represent particles in the system, and the particles encircled by black lines indicate that they are entangled. In the subsequent section, we will elaborate on the process of refactoring secrets.

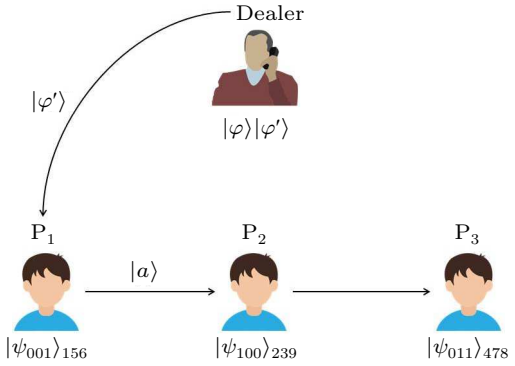


Fig. 1. The process of the particle distribution phase.

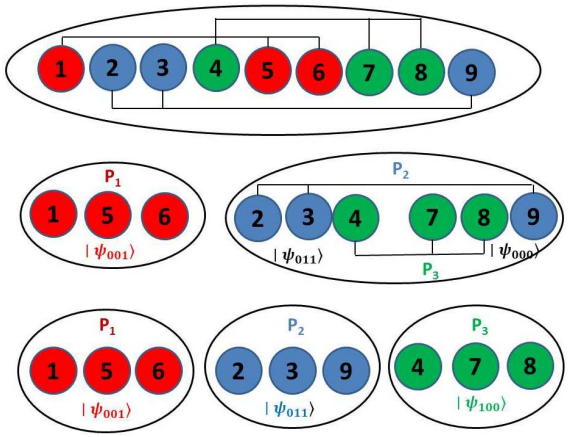


Fig. 2. The secret distribution of phase particles in each participant's mutual state.

3.3. Secret reconstruction

The steps of the secret reconstruction are illustrated in Fig. 3. P_2 and P_3 exchange measurement results. P_3 (P_2) acquires quantum state $|C\rangle$ through a series of operations, then derives product state $|E\rangle$ based on the measurement result $|\psi_{001}\rangle_{156}$ announced by P_1. Finally, P_3 (P_2) compares it with the product state $|\phi\rangle$ announced by the dealer to deduce the Pauli operation executed by the dealer. P_2 and P_3 play symmetrical roles in the scheme. The following are the detailed steps of the secret reconstruction process.

(i) The following information is available at the beginning of the reconstruction process. (a) The product state $|\phi\rangle$ was originally created by dealer D. (b) The qubit where the dealer performs the Pauli operation is assumed to be the first qubit. (c) Measurement results $|\psi_{001}\rangle_{156}$ of the participant P_1.

(ii) Participants P_2 and P_3 announce their measurements as $|\psi_{100}\rangle_{239}$ and $|\psi_{011}\rangle_{478}$. Then, the combined state becomes

$$|b\rangle = |\psi_{100}\rangle_{239}|\psi_{011}\rangle_{478}$$

$$
\begin{aligned}
&= \frac{1}{4}[(|111\rangle - |000\rangle)_{239}(|101\rangle + |010\rangle)_{478}] \\
&= \frac{1}{4}[(|111011\rangle + |110101\rangle - |001010\rangle - |000100\rangle)_{234789}] \\
&= \frac{1}{16}\big[(|\psi_{010}\rangle + |\psi_{011}\rangle)_{234}(|\psi_{000}\rangle - |\psi_{001}\rangle)_{789} \\
&\quad +(|\psi_{110}\rangle + |\psi_{111}\rangle)_{234}(|\psi_{101}\rangle + |\psi_{100}\rangle)_{789} \\
&\quad -(|\psi_{110}\rangle - |\psi_{111}\rangle)_{234}(|\psi_{100}\rangle - |\psi_{101}\rangle)_{789} \\
&\quad -(|\psi_{010}\rangle - |\psi_{011}\rangle)_{234}(|\psi_{000}\rangle + |\psi_{001}\rangle)_{789}\big] \\
&= \frac{1}{8}\big[2|\psi_{011}\rangle_{234}|\psi_{000}\rangle_{789} - 2|\psi_{010}\rangle_{234}|\psi_{001}\rangle_{789} \\
&\quad +2|\psi_{111}\rangle_{234}|\psi_{100}\rangle_{789} - 2|\psi_{110}\rangle_{234}|\psi_{101}\rangle_{789}\big]. \qquad (9)
\end{aligned}
$$

(iii) Since the participant knows that the (7,8,9) particle has never been tampered with, the state of the qubit (7,8,9) should be $|\psi_{000}\rangle_{789}$ which corresponds only to $|\psi_{011}\rangle_{234}$ in Eq. (11) above. Therefore, the current state of their qubits is

$$|C\rangle = |\psi_{011}\rangle_{234}|\psi_{000}\rangle_{789}. \qquad (10)$$

(iv) Next, using P_1's measurement result information $|\psi_{001}\rangle_{156}$, they write the system as follows:

$$
\begin{aligned}
|X\rangle &= [(111) - (000)]_{234}[(100) - (011)]_{156} \\
&= (111100 - 111011 - 000100 + 000011)_{234156} \\
&= (111100 - 011111 - 100000 + 000011)_{123456} \\
&= (|\psi_{010}\rangle + |\psi_{011}\rangle)_{123}(|\psi_{000}\rangle + |\psi_{001}\rangle)_{456} \\
&\quad -(|\psi_{000}\rangle - |\psi_{001}\rangle)_{123}(|\psi_{010}\rangle + |\psi_{011}\rangle)_{456} \\
&\quad -(|\psi_{000}\rangle + |\psi_{001}\rangle)_{123}(|\psi_{010}\rangle - |\psi_{011}\rangle)_{456} \\
&\quad +(|\psi_{010}\rangle - |\psi_{011}\rangle)_{123}(|\psi_{000}\rangle|\psi_{001}\rangle)_{456} \\
&= 2\big(|\psi_{010}\rangle_{123}|\psi_{000}\rangle_{456} + |\psi_{011}\rangle_{123}|\psi_{001}\rangle_{456} \\
&\quad -|\psi_{000}\rangle_{123}|\psi_{010}\rangle_{456} + |\psi_{001}\rangle_{123}|\psi_{011}\rangle_{456}\big). \qquad (11)
\end{aligned}
$$

(v) D transforms the first qubit and announces this information, P_2 and P_3 receive this information so they know that the entangled state of the (4,5,6) particle is not affected; that is, the entangled state of the (4,5,6) particle is $|\psi_{000}\rangle_{456}$, according to Eq. (11), it can be inferred that the entangled state of the (1,2,3) particle is $|\psi_{010}\rangle_{123}$, and the complete product state recovered by the final participant is as follows:

$$|E\rangle = |\psi_{010}\rangle_{123}|\psi_{000}\rangle_{456}|\psi_{000}\rangle_{789}. \qquad (12)$$

The product states reconstructed by the participants are compared with the product states originally created by dealer D; i.e., Eq. (4) is compared with Eq. (12).

$$X_1|\psi_{000}\rangle = |\psi_{010}\rangle. \qquad (13)$$

The participants speculated that D executed X on the first particle. According to Eq. (5) published by D, the recipient successfully decrypted the classical secret '01' transmitted by D.

The above describes the execution process of a (3,3) protocol. When the number of participants increases by one, the secret sender only needs to add an additional GHZ state to the initially prepared system state. For four participants, the secret sender prepares the system state multiplied by four GHZ states and assigns particles to the groups (1,5,6), (4,8,9), (7,11), and (10,2,3) respectively. These particles are sent to the four participants, who then perform GHZ measurements. The calculation principle for the collapse case of the quantum state and the secret reconstruction process is similar to that of the (3,3) protocol, except that the multiplication of the GHZ state is performed one additional time during the secret recovery process. Similarly, when there are n GHZ states in the prepared system state for n participants, the measurement results of the n users are multiplied when recovering the secret.

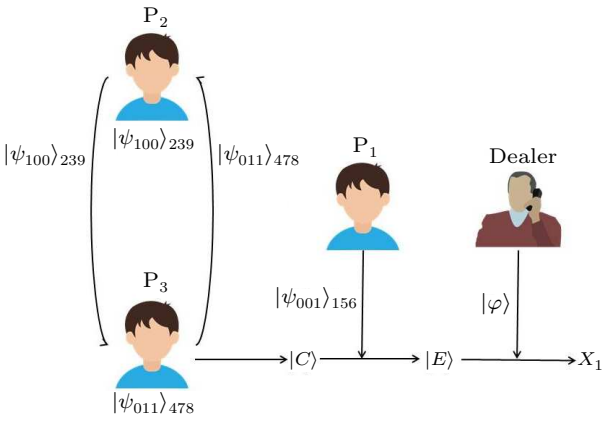


Fig. 3. The process of secret reconstruction phase.

4. Example

(i) Suppose D creates the following product state from GHZ states:

$$
\begin{aligned}
|\phi\rangle &= \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{123} \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{456} \\
&\quad \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{789}. \qquad (14)
\end{aligned}
$$

(ii) D operates an X gate on qubit 1 to obtain

$$
\begin{aligned}
|\phi'\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123} \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{456} \\
&\quad \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{789} \qquad (15)
\end{aligned}
$$

and shares the qubits with the three participants.

(iii) P_1 measures $\langle\psi_{001}|_{156}$, which causes the system to enter specific states

$$
\begin{aligned}
&\big(|\psi_{111}\rangle|\psi_{110}\rangle + |\psi_{110}\rangle|\psi_{111}\rangle \\
&+|\psi_{011}\rangle|\psi_{100}\rangle + |\psi_{010}\rangle|\psi_{101}\rangle\big)_{239478}. \qquad (16)
\end{aligned}
$$

(iv) P_2 and P_3 announce their measurements as $|\psi_{100}\rangle_{239}$ and $|\psi_{011}\rangle_{478}$. The combined state is

$$\big(|\psi_{011}\rangle_{234}|\psi_{000}\rangle_{789} - |\psi_{010}\rangle_{234}|\psi_{001}\rangle_{789}$$

$$+|\psi_{111}\rangle_{234}|\psi_{100}\rangle_{789}-|\psi_{110}\rangle_{234}|\psi_{101}\rangle_{789}\big). \quad (17)$$

(v) Participants P_2 and P_3 receive the initial state created by D, as described in Eq. (14). By eliminating the redundant terms in Eq. (17), the resulting state is as follows:

$$|\psi_{011}\rangle_{234}|\psi_{000}\rangle_{789}. \quad (18)$$

(vi) P_1 announces his quantum state $|\psi_{001}\rangle_{156}$, which, when combined with Eq. (18), yields the following state:

$$\big(|\psi_{010}\rangle_{123}|\psi_{000}\rangle_{456}+|\psi_{011}\rangle_{123}|\psi_{001}\rangle_{456} -|\psi_{000}\rangle_{123}|\psi_{010}\rangle_{456}+|\psi_{001}\rangle_{123}|\psi_{011}\rangle_{456}\big). \quad (19)$$

(vii) D announces his initial state, namely, equality (14), and notes that he changes the first qubit. Based on this information, we retain only the first term $|\psi_{010}\rangle_{123}|\psi_{000}\rangle_{456}$ of equality (19).

(viii) The final products reported by the participants are as follows:

$$(|\psi_{010}\rangle_{123}|\psi_{000}\rangle_{456}|\psi_{000}\rangle_{789}). \quad (20)$$

By comparing with Eq. (14), we can conclude that the Pauli operation performed by D is X.

The entire process completes the reconstruction of the secret by employing a strategy in which participants introduce quantum bits and discard redundant items.

5. Security analysis

Security analysis is a crucial criterion for assessing the feasibility and security of a quantum scheme.[26] To test our protocol against this benchmark, we simulate the secret sender, the participation of all parties, and the eavesdropping behavior of an external attacker to demonstrate the security of the protocol.

Theorem 1 The quantum state of each participant is the maximally entangled state.

Proof The security of the scheme is determined by many aspects, the most important of which is the lack of knowledge of each participant about his or her own subsystem.[27] To determine the information accessible to each participant through the particles in their hands, one can analyze the density matrix of their subsystems. We refer to the proof procedure outlined in Ref. [26] to complete our proof, and the detailed steps of the proof are as follows.

Denote the density matrix of P_1 as M_{P_1}. Since the cases of assigning particles to P_1, P_2, and P_3 in the protocol are similar, the method for computing the density matrices of other users is equivalent to that of P_1. The density matrix M_{All} of the whole system is denoted as

$$\begin{aligned} M_{ALL} &= |\phi'\rangle\langle\phi'| \\ &= \frac{1}{8}\big[(|0\rangle_1|0\rangle_2|0\rangle_3+|1\rangle_1|1\rangle_2|1\rangle_3) \\ &\quad\times(|1\rangle_1|0\rangle_2|0\rangle_3+|0\rangle_1|1\rangle_2|1\rangle_3) \\ &\quad\times(|1\rangle_1|0\rangle_2|0\rangle_3+|0\rangle_1|1\rangle_2|1\rangle_3) \\ &\quad\times(\langle 0|_1\langle 0|_2\langle 0|_3+\langle 1|_1\langle 1|_2\langle 1|_3) \\ &\quad\times(\langle 1|_1\langle 0|_2\langle 0|_3+\langle 0|_1\langle 1|_2\langle 1|_3) \\ &\quad\times(\langle 1|_1\langle 0|_2\langle 0|_3+\langle 0|_1\langle 1|_2\langle 1|_3)\big]. \end{aligned} \quad (21)$$

The density matrix of the subsystems of P_1 is calculated as follows:

$$M_{156}=\sum_a \mathrm{Tr}_{234789}|a\rangle M_{ALL}\langle a|. \quad (22)$$

By the basic formula $\mathrm{Tr}(|\phi\rangle A\langle\phi|)=\langle\phi|A|\phi\rangle$, equality (17) can be transformed into the following form:

$$M_{156}=\mathrm{Tr}_{234789}=\sum_a |a\rangle M_{ALL}\langle a|. \quad (23)$$

Here $|a\rangle = |001100\rangle$, $|001100\rangle$, $|001100\rangle$, $|001100\rangle$, $|001100\rangle$, $|001100\rangle$, $|001100\rangle$, $|001100\rangle$, so we get

$$\begin{aligned} M_{156} &= 1/4(|0\rangle\langle 0|+|1\rangle\langle 0|+|0\rangle\langle 1|+|1\rangle\langle 1|+) \\ &= 1/4(\mathbb{I}\otimes\mathbb{I}). \end{aligned} \quad (24)$$

Since $\mathrm{Tr}(M_{156})=1$, $\mathrm{Tr}(M_{156}^2)=1/4<1$ the particle state of P_1 is the maximally entangled state. This determines that the measurements of P_1 may be $|100\rangle$, $|011\rangle$, $|111\rangle$, $|000\rangle$, with a probability of $1/4$ in each case. Even if P_1 is measured not on an ordinary computational basis but on a GHZ basis, it may measure these quantum states: $|\psi_{000}\rangle$, $|\psi_{001}\rangle$, $|\psi_{010}\rangle$, $|\psi_{011}\rangle$, each quantum state with a probability of $1/4$. For example, the probability of measuring $|\psi_{001}\rangle$

$$\begin{aligned} &P(|\psi_{001}\rangle) \\ &= 1/4\langle\psi_{001}|\left[\left(\frac{|\psi_{001}\rangle+|\psi_{000}\rangle}{\sqrt{2}}\right)\left(\frac{\langle\psi_{001}|+\langle\psi_{000}|}{\sqrt{2}}\right)\right. \\ &\quad+\left(\frac{|\psi_{011}\rangle-|\psi_{010}\rangle}{\sqrt{2}}\right)\left(\frac{\langle\psi_{011}|-\langle\psi_{010}|}{\sqrt{2}}\right) \\ &\quad+\left(\frac{|\psi_{011}\rangle+|\psi_{010}\rangle}{\sqrt{2}}\right)\left(\frac{\langle\psi_{011}|+\langle\psi_{010}|}{\sqrt{2}}\right) \\ &\quad+\left.\left(\frac{|\psi_{001}\rangle-|\psi_{000}\rangle}{\sqrt{2}}\right)\left(\frac{\langle\psi_{001}|-\langle\psi_{000}|}{\sqrt{2}}\right)\right]|\psi_{001}\rangle \\ &= \frac{1}{4}. \end{aligned} \quad (25)$$

Each participant's particles are in a maximally entangled state, which ensures that no participant can use their particles to obtain information about other entangled particles before the protocol starts.

Theorem 2 If P_1 dishonestly publishes its measurements, the protocol will be broken. The protocol requires P_1 to be a trusted secret reconstructor, which is crucial for the complete

reconstruction of the secret. However, P_1 may also be dishonest and not share its measurement results with other participants. Here is an example of P_1 dishonesty: D creates the product state $|A\rangle = |\psi_{000}\rangle_{123}|\psi_{000}\rangle_{456}|\psi_{000}\rangle_{789}$. It wants to pass the secret '10', so it performs the X-gate operation on the first particle of $|A\rangle$, without loss of generality, let measurements of P_1 are $|\psi_{001}\rangle_{156}$, and those of P_2 and P_3 are $|\psi_{100}\rangle_{239}$ and $|\psi_{011}\rangle_{478}$, respectively. P_2 and P_3 cooperate with each other to obtain the quantum state $|B\rangle = |\psi_{011}\rangle_{234}|\psi_{000}\rangle_{789}$. Then, based on the error measurement result $|\psi_{000}\rangle_{156}$ published by P_1, the final quantum state deduced by the participants is

$$|B\rangle = |\psi_{011}\rangle_{123}|\psi_{000}\rangle_{456}|\psi_{000}\rangle_{789} \Rightarrow \mathbb{Y}_1 \Rightarrow \text{'11'}. \quad (26)$$

However, the correct product state would be

$$|B\rangle = |\psi_{010}\rangle_{123}|\psi_{000}\rangle_{456}|\psi_{000}\rangle_{789} \Rightarrow \mathbb{X}_1 \Rightarrow \text{'10'}. \quad (27)$$

Therefore, we infer that honest disclosure by P_1 of his measurement results is a necessary condition for the reconstruction of the correct classical secret.

Theorem 3 If either P_1 or P_2 is dishonest, the protocol will be compromised.

Proof Suppose P_2 has not published its actual measurements, and although P_3 knows P_1's published measurements for particles (1,5,6), they cannot infer the correct state of particles (2,3,4), so they cannot further reconstruct the secret. P_2 and P_3 play the same role in the protocol, so the protocol is also broken when P_3 is dishonest.

Theorem 4 The protocol can resist eavesdropper Eve's forgery attack.

Proof Suppose there is a malicious eavesdropper, Eve, who tries to break the protocol. If she somehow obtains one of the qubits created by D, let us say the 7th qubit, and performs an X-gate operation on it without anyone knowing, the modified product state is

$$\begin{aligned}|\phi\rangle_{\mathrm{m}} = & \frac{1}{\sqrt{2}}(|100\rangle+|011\rangle)_{123}\frac{1}{\sqrt{2}}(|100\rangle+|011\rangle)_{456} \\ & \times\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{789}. \end{aligned} \quad (28)$$

The measurement of P_1 might as well be $|\psi_{001}\rangle_{156}$, and this product state collapses to $|\psi_{111}\rangle_{234}|\psi_{010}\rangle_{789}$. Since P_1 measures particles (1,5,6), the state of particles (7,8,9) will not change. Therefore, D finds that the state of particles (7,8,9) in the product state it creates is tampered with by $|\psi_{010}\rangle_{789}$ using $|\psi_{000}\rangle_{789}$. At this time, D announces that the product state it creates is $|\phi\rangle_{\mathrm{m}}$ (in Eq. (24)), and the quantum of its operation is 1. Participants can still obtain the correct classical secret through the information announced by D. When D discovers that the product state it creates has been tampered with by Eve, it will announce the correct product states so that the whole scheme is not affected by the forgery particle attack.

6. Efficiency analysis

In this section, we will discuss the transmission efficiency of the protocol. According to Ref. [27], the transmission efficiency of the scheme can be calculated using the following equation:

$$\eta = \frac{b_{\mathrm{s}}}{q_{\mathrm{t}}+b_{\mathrm{t}}}. \quad (29)$$

In the equation above, b_{s} denotes the length of the secret being transmitted, q_{t} signifies the total consumption of quantum resources, and b_{t} represents the total number of classical bits utilized. In our scheme, the length of the secret transmitted by the sender D, is 2 bits, which means $b_{\mathrm{s}} = 2$. The secret sender D must prepare n GHZ states at the beginning of the protocol, resulting in a total requirement of $3n$ quantum resources, so $q_{\mathrm{t}} = 3n$. Notably, this scheme does not require the use of decoy particles to verify the security of the transmission channel, which reduces the consumption of quantum resources. It is a purely quantum scheme, with no integration of classical methods or consumption of classical resources; hence, $b_{\mathrm{t}} = 0$. Consequently, we can conclude that the efficiency of this scheme is represented by $\eta = 2/(3n)$.

7. Comparative analysis

In this section, we present a comparative analysis of the proposed scheme with several QSS schemes.

(i) In Ref. [28], an efficient QSS scheme based on the new structure and single qubit is proposed. In this scheme, each participant randomly prepares a certain number of single qubits, which are selected randomly from 0, 1, +, −. Then, each participant sends the prepared bit string to the secret sender D. D performs operation I or operation Y on the received qubit string according to the classical message it wants to transmit, where operations I and Y represent the '0' and '1' of the classical message, respectively. D sends the operated bit string to the corresponding participant, and each participant compares the received qubit string with the one they prepared to recover the corresponding Pauli operation. Each participant contributes the recovered classical bit, and the complete classical bit string can be recovered.

However, the security of the protocol is not guaranteed against Eve's forgery attack. Suppose D wants to transmit the classical bit '0', and it performs operation I on the received bit $|0\rangle$. At this time, the quantum bit after the operation is still $|0\rangle$, and a malicious eavesdropper Eve tries to sabotage the correct transmission of the protocol, it uses some means to obtain the quantum bit $|0\rangle$ in the hand of D, and performs the X-gate operation on it without anyone's knowledge, so that $|0\rangle$ becomes $|1\rangle$. When the participant receives quantum bit $|1\rangle$, by comparing it with its corresponding quantum bit, the classical bit '1' is recovered, which leads to the secret recovery error.

Table 2. Comparison with other protocols

Protocols	[28]	[25]	[24]	[22]	[20]	Our
Basic scheme	single qubit + Pauli gate	GHZ state particle exchange law + "characteristics"	QFT + MSP + access structure	QFT + CNOT gate	Bell state + Lagrange polynomial	quantum entanglement swapping
Secret reconstruction	Y	Y	Y	N	Y	Y
Entanglement operation	N	Y	N	N	Y	Y
System dimension	2	2	d	d	d	2
Use of classic secret sharing	Y	Y	Y	Y	Y	N
Quantum measurement	single qubit	GHZ based	single qubit	N	N	GHZ based
Qubit efficiency (n-party QSS)	$2/(n^2+2n)$	$1/(3n)$	$n/[\log_2 d]^n$	$2/n^2$	$1/(3n)$	$2/(3n)$

(ii) In Ref. [25], a multi-party QSS scheme based on GHZ state quantum entanglement exchange is proposed. Firstly, the concept of 'characteristics' is defined in the scheme. The relationship among the characteristics of the measurement result, the characteristics of the initial state, and the characteristics of the Pauli operator are established. However, the specific implementation process of the protocol follows a classical sharing scheme, so its security is primarily reliant on the classical scheme and is minimally influenced by the quantum aspect of sharing. Once eavesdroppers or dishonest participants gain access to the classical scheme, they can illicitly obtain secrets without needing to make qubit measurements.

(iii) In Ref. [24], a universal secret-sharing scheme based on the quantum Fourier transform (QFT) is proposed. This scheme combines the QFT and Monotone Span programs. It also utilizes a universal access structure to create a hybrid scheme that incorporates the benefits of both classical and quantum secret sharing. Although this hybrid scheme has the advantages of both, the existence of the classical scheme will inevitably weaken its security. The classical scheme falls short in achieving unconditional security, making it less secure compared to the pure QSS scheme.

In Table 2, we present a comparative analysis of our scheme with several typical schemes in various aspects.

8. Conclusion

In the era of rapid development of quantum technology, QSS schemes based on pure quantum mechanics have greater advantages in combating quantum attacks. Using the measurement collapse principle of GHZ states, this paper proposes a QSS scheme based on pure quantum (n,n) threshold. In this scheme, the dealer creates a product state and performs Pauli operations on the product state to store classical information. Participants obtain their shares by measuring the product state in turn. There is no integration of classical frameworks and the utilization of classical tools at each stage of the scheme.

The security analysis indicates that the scheme is not vulnerable to intercept retransmission attacks and collusion attacks. It is capable of detecting and terminating the protocol promptly when dealing with dishonest participants. It can also resist quantum attacks in a pure quantum environment.

Acknowledgments

Project supported by the National Natural Science Foundation of China (Grant No. 62002105) and the Key Research and Development Program of Hubei, China (Grant No. 2021BEA163).

References

[1] Liu B X, Jiang D H, Liang X Q and Zhang Y H 2021 *International Journal of Theoretical Physics* **60** 1339
[2] Zhang T, Xin X, Jiang B, Li C and Li F 2024 *Optical and Quantum Electronics* **56** 131
[3] Gheorghiu A, Kapourniotis T and Kashefi E 2019 *Theory of Computing Systems* **63** 715
[4] Shamir A 1979 *Communications of the ACM* **22** 612
[5] Wan S, Qi L, Yang G, Lu Y, Yan X and Li L 2020 *Multimedia Tools and Applications* **79** 2789
[6] Tan L, Lu Y, Yan X, Liu L and Li L 2019 *IEEE Access* **7** 59278
[7] Zhang J and Zhang F 2015 *Future Generation Computer Systems* **52** 109
[8] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7
[9] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[10] Giorgi L G 2005 *Phys. Rev. A* **71** 064303
[11] Gao G 2024 *Chin. Phys. B* **33** 40301
[12] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev. A* **59** 162
[13] Chou Y H, Chen C Y, Fan R K, Chao H C and Lin F J 2012 *IET Information Security* **6** 84
[14] Basak N, Das N, Paul G, Nandi K and Patel N 2023 *Quantum Inform. Proc.* **22** 393
[15] Hillery M 1999 *Phys. Rev. A* **59** 1829
[16] Yan C, Li Z, Liu L and Lu D 2022 *Quantum Inform. Proc.* **21** 24
[17] Lu C, Miao F, Hou J, Huang W and Xiong Y 2020 *Quantum Inform. Proc.* **19** 101
[18] Sutradhar K and Om H 2020 *QQuantum Inform. Proc.* **19** 73
[19] Yang W, Huang L, Shi R and He L 2013 *Quantum Inform. Proc.* **12** 2465
[20] Qin H and Dai Y 2016 *Information Processing Letters* **116** 351
[21] Hu W, Xiong B and Zhou R 2023 *Chin. Phys. B* **32** 080303
[22] Song X L, Liu Y B, Deng H Y and Xiao Y G 2017 *Scientific Reports* **7** 6366
[23] Mashhadi S 2022 *Journal of Applied Security Research* **17** 123
[24] Mashhadi, Samaneh 2019 *Quantum Inform. Proc.* **18** 114
[25] Xu Y, Li Z, Liu T and Zhu H 2022 *International Journal of Theoretical Physics* **61** 76
[26] Musanna F and Kumar S 2020 *Quantum Inform. Proc.* **19** 348
[27] Musanna, Farhan and Kumar, Sanjeev 2022 *International Journal of Theoretical Physics* **61** 255
[28] Kuo S Y, Tseng K C, Yang C C and Chou Y H 2023 *EPJ Quantum Technology* **10** 29