Multi-layer Quantum Secret Sharing Based on GHZ States

Li-wei Chang[1,2](✉), Yu-qing Zhang[1], Xiao-xiong Tian[1], Yu-hua Qian[2], Zeng-liang Bai[1], and Shi-hui Zheng[3]

[1] School of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China
changliwei002@163.com
[2] Institute of Big Data Science and Industry, Shanxi University, Taiyuan 030006, China
[3] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract. A multi-layer quantum secret sharing protocol based on GHZ states is put forward. In this protocol, Alice wishes to share a secret, carried by the quantum state, with multiple agent nodes in the network. To be specific, the secret is transmitted and shared layer by layer from root Alice to layered agents. Only if all agents at the last layer cooperate together, this secret can be reconstructed accurately. Compared with existing quantum secret sharing protocols, there are two highlights in our proposed protocol. On the one hand, the secret can be distributed to multiple agents only with five-particle GHZ states on account of layered construction. On the other hand, we elaborately design two iterative algorithms under the guidance of computational thinking, Algorithm 1 is helpful to quickly calculate the final collapsed state in each layer, Algorithm 2 is capable of obtaining the specific recovery operation based on the output results of Algorithm 1. Our proposed protocol can be applied to the wireless network in an effort to ensure the security of information delivery.

Keywords: Quantum secret sharing · GHZ states · Multi-player sharing · Iterative algorithms

1 Introduction

Nowadays, with the rapid development of science and technology, human society has stepped into the era of the integration of realistic space and cyberspace. The information superhighway has become the basis of economic development. Thus, how to effectively ensure the security of information is of extreme significance.

Classical cryptography is an important tool to ensure the information security. Unfortunately, quantum algorithms cause them to be broken through in polynomial time. Thereupon, quantum cryptography, which is proven to be unconditionally secure over an insecure channel, has attracted more and more attention from both industry and academia. As a result, so far all kinds of quantum secure communication protocols have been proposed by the researchers such as quantum key distribution (QKD) [1–5],

X. Sun et al. (Eds.): ICAIS 2020, CCIS 1252, pp. 674–685, 2020.
https://doi.org/10.1007/978-981-15-8083-3_60

quantum secure direct communication (QSDC) [6–8], quantum teleportation (QT) [9, 10], remote state preparation (RSP) [11, 12], quantum signature (QS) [13, 14], quantum private query (QPQ) [15, 16], quantum private comparison [17] and so on.

Quantum secret sharing (QSS) is a significant branch of quantum secure communication, which is deemed to be the quantum counterpart of classical secret sharing. In fact, QSS combines quantum mechanics and the kernel idea contained in classical secret sharing to split either a classical secret (bit string) or a quantum state (unknown quantum state) into several shadows, a specific quantity of shadows can reconstruct the secret but every shadow alone cannot. The quantum secret sharing schemes were firstly proposed by Hillery et al. and Karlsson et al. at the same year [18, 19]. Since then, a great many of QSS schemes have been put forward by experts and scholars in both theory and experiment.

In 2008, Deng et al. presented an efficient high-capacity QSS protocol based on the ideas of quantum dense coding [20]. In 2010, Gu et al. proposed two robust three-party QSS protocols to be against both collective-dephasing noise and collective rotation noise with logical Bell states [21]. In 2012, Yang et al. not only summarized how to construct a verifiable quantum (k, n) threshold protocol, but also designed a specific scheme by means of Lagrange Interpolation formula and post-verification mechanisms [22]. In 2013, Hsu et al. put forward a dynamic QSS protocol with the entanglement swapping of EPR pairs to deal with the volatility of agents [23]. In 2015, Rahaman et al. elaborately devised the first QSS scheme by utilizing the local distinguishability of orthogonal multipartite entangled states [24]. In 2017, Wang et al. designed a multi-layer QSS protocol based on GHZ state and generalized Bell-basis measurement [25]. In the same year, Chen et al. came up with a QSS scheme using the Borras-Plastino-Batle (BPB) state, in which the module division and coupling of quantum communication protocols was investigated [26]. In addition, Wang et al. attempted to make use of the local distinguishability of orthogonal Dicke states and multi-qudit entangled states to construct the QSS schemes, respectively [27, 28]. In 2019, a new multi-party QSS model was built by Zhang et al. by analyzing the property of multi-qubit entangled states [29]. In the same year, a novel rational non-hierarchical quantum secret sharing protocol emerged, which is widely applicable [30].

It is easy to discover that each of aforementioned QSS schemes is deem to be a representative of one kind of QSS. Aiming at the fact that it is difficult to prepare multi-particle entangled states, based on layered structure, we put forward a multi-layer QSS protocol with five-particle GHZ states which can be created in laboratory. In our scheme, the secret, carried by one quantum state, is distributed to the multiple agent nodes in the network layer by layer from root to layered agents. Only if all agents at the last layer cooperate together, the secret can be reconstructed.

The structure of this paper is organized as follows. In Sect. 2, we come up with a multi-layer quantum secret sharing protocol by means of five-particle GHZ states. In Sect. 3, we design two iterative algorithms under the guidance of computational thinking. One is to calculate the multi-qubit entangled states carrying the secret in the last layer, while the other is to compute the recovery operations performed by the designated agent in the last layer. Finally, this paper ends up with a discussion in Sect. 4.

2 Multi-layer Quantum Secret Sharing Protocols

In this section, we design a multi-layer QSS protocol with five-particle GHZ states by using Bell-basis measurement. We take into account that the agent's number in each layer is a geometric sequence with common ratio 4. The workflow of this QSS protocol can be depicted as follows.

2.1 The Secret Sharing Process of the First Layer

Suppose that there are five participants, one sender Alice and four agents $\mathrm{Bob_i}(i = 1, \cdots, 4)$ in the first layer. Alice holds a secret carried by the one-qubit quantum state and wants to distribute this secret to the agents $\mathrm{Bob_i}(i = 1, \cdots, 4)$. The one-qubit state corresponding to this secret can be written as.

$$|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are complex numbers, which satisfy the normalization condition $\alpha^2 + \beta^2 = 1$.

For sharing the one-qubit state with four agents, Alice first prepares a five-particle GHZ state, as shown in the Fig. 1(a), which can be expressed in

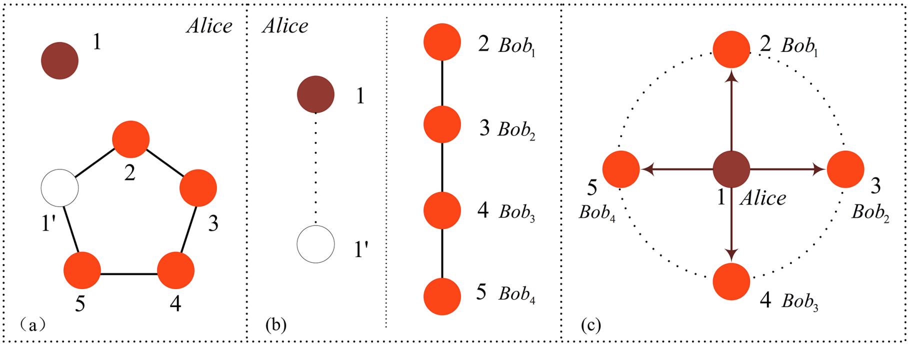

Fig. 1. The secret sharing process of the first layer

$$|\psi\rangle_{1'2345} = \frac{1}{\sqrt{2}}(|00000\rangle + |11111\rangle) \tag{2}$$

This five-particle GHZ state can be created in laboratory conditions. To set up the quantum channel, Alice sends the particle 2 to $\mathrm{Bob_1}$, the particle 3 to $\mathrm{Bob_2}$, the particle 4 to $\mathrm{Bob_3}$ and the particle 5 to $\mathrm{Bob_4}$. Therefore, the state of the whole six-particle system can be described as

$$\begin{aligned}|\psi\rangle_1 \otimes |\psi\rangle_{1'2345} = &\frac{1}{\sqrt{2}}(\alpha|000000\rangle + \alpha|011111\rangle + \beta|100000\rangle \\ &+ \beta|111111\rangle)\end{aligned} \tag{3}$$

In order to transfer the secret to four agents, Alice performs a Bell-basis measurement on the particles 1 and 2 as depicted in the Fig. 1(b). This measurement basis is made up of four Bell states

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\ |\varphi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$$
$$|\varphi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),\ |\varphi_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \quad (4)$$

As a result, the state of the whole quantum system, which is composed of six particles, can be rewritten as

$$\begin{aligned}|\psi\rangle_{11'2345} =& \frac{1}{\sqrt{2}}[|\varphi_1\rangle_{11'}(\alpha|0000\rangle + \beta|1111\rangle)_{2345} \\ &+ |\varphi_2\rangle_{11'}(\alpha|0000\rangle - \beta|1111\rangle)_{2345} \\ &+ |\varphi_3\rangle_{11'}(\alpha|1111\rangle + \beta|0000\rangle)_{2345} \\ &+ |\varphi_4\rangle_{11'}(\alpha|1111\rangle - \beta|0000\rangle)_{2345}]\end{aligned} \quad (5)$$

It is obvious that the whole system will collapse to a term of Eq. (5) with the probability of 1/4, after Alice implements the Bell-basis measurement.

Table 1. Corresponding relationship between the measurement outcomes of Bob_2–Bob_4 and the unitary operations performed by Bob_1

Bob_2's SM results	Bob_3's SM results	Bob_4's SM results	Bob_1's operations
$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	I_2
$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	σ_2^z
$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	σ_2^z
$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	I_2
$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	σ_2^z
$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	I_2
$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	I_2
$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	σ_2^z

That is to say, as shown in the Fig. 1(c), the secret carried by the particle 1 is transferred to the quantum system composed of four particles 2, 3, 4 and 5. As a result, this secret is shared by four agents Bob_1, Bob_2, Bob_3 and Bob_4 through one time distribution. Only if these four agents collaborate with each other, they can recover the secret.

If Alice decides that the protocol only works in the first layer, she will announce her measurement results and designate one agent to recover the secret at random. Assume she empowers Bob_1 to recover the secret, Bob_2, Bob_3 and Bob_4 should carry out a single-qubit measurement in the basis $|X^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$ on their own particles respectively and publish their measurement outcomes to Bob_1 via a classical channel. According to the measurement outcomes from both Alice and Bob_2–Bob_4, Bob_1 can recover the original secret by applying a suitable unitary transformation on his particle 2. As illuminated in Table 1, when Alice's measurement result is $|\varphi_1\rangle$, Bob_1 should carry out the corresponding unitary transformations.

If Alice wishes to make more agents share this secret, she does not publish her measurement results and not designate any agent to reconstruct it. Bob_1, Bob_2, Bob_3 and Bob_4 will continue to distribute this secret to the second layer. Obviously, these four agents are not able to recover the secret accurately, because they are ignorant of Alice's measurement results.

2.2 The Secret Sharing Process of the Second Layer

After the first distribution, the entangled state, carrying the secret, shared among Bob_1, Bob_2, Bob_3 and Bob_4 can be written as Eq. (5). The target is to share this secret among sixteen agents $\mathrm{Charlie}_i (i = 1, \cdots, 16)$ in the second layer.

As shown in the Fig. 2(a), Bob_1–Bob_4 should prepare a five-particle GHZ state respectively,

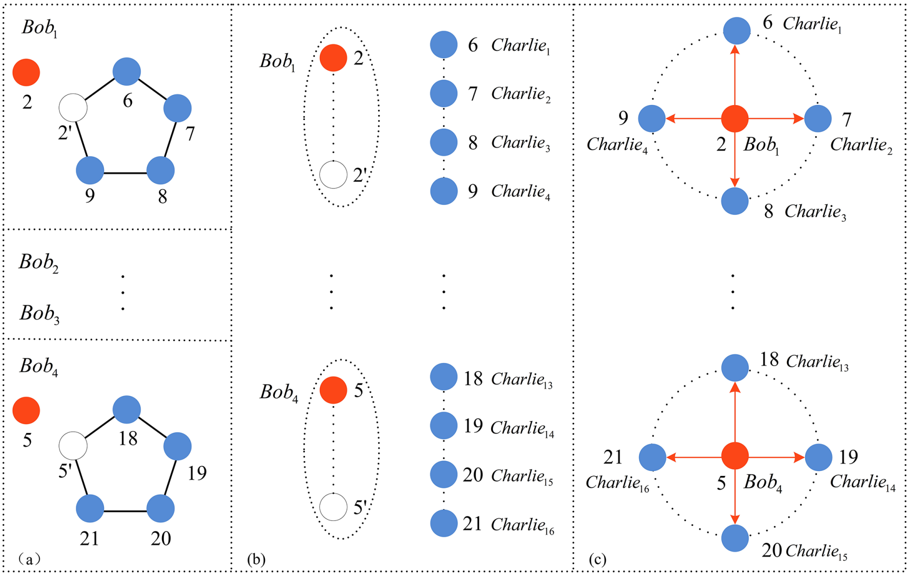

Fig. 2. The secret sharing process of the second layer

$$|\psi\rangle_{2'6789} = \frac{1}{\sqrt{2}}(|00000\rangle+|11111\rangle)_{2'6789}$$

$$|\psi\rangle_{3'10111213} = \frac{1}{\sqrt{2}}(|00000\rangle+|11111\rangle)_{3'10111213}$$

$$|\psi\rangle_{4'14151617} = \frac{1}{\sqrt{2}}(|00000\rangle + |11111\rangle)_{4'14151617}$$
$$|\psi\rangle_{5'18192021} = \frac{1}{\sqrt{2}}(|00000\rangle + |11111\rangle)_{5'18192021} \tag{6}$$

For simplicity, the numbers 6, 7, 8, 9 are written as 6–9, the numbers 10, 11, 12, 13 are written as 10–13, the numbers 14, 15, 16, 17 are written as 14–17, and the numbers 18, 19, 20, 21 are written as 18–21.

Bob_1 respectively sends the particles 6–9 to $Charlie_1$–$Charlie_4$ with the help of decoy photons, Bob_2 respectively sends the particles 10–13 to $Charlie_5$–$Charlie_8$ with the help of decoy photons, Bob_3 respectively sends the particles 14–17 to $Charlie_9$–$Charlie_{12}$ with the help of decoy photons, and Bob_4 respectively sends the particles 18–21 to $Charlie_{13}$–$Charlie_{16}$ with the help of decoy photons.

Suppose Alice's measurement result is $|\varphi_2\rangle$, the state of the whole quantum system, which is composed of twenty-four particles, can be described as

$$\begin{aligned}
|\psi\rangle &= |\psi\rangle_{2345} \otimes |\psi\rangle_{2'6-9} \otimes |\psi\rangle_{3'10-13} \otimes |\psi\rangle_{4'14-17} \otimes |\psi\rangle_{5'18-21} \\
&= \frac{1}{4}(\alpha|0000\rangle - \beta|1111\rangle)_{2345} \otimes (|00000\rangle + |11111\rangle)_{2'6-9} \\
&\quad \otimes (|00000\rangle + |11111\rangle)_{3'10-13} \otimes (|00000\rangle + |11111\rangle)_{4'14-17} \\
&\quad \otimes (|00000\rangle + |11111\rangle)_{5'18-21}
\end{aligned} \tag{7}$$

After Bob_1 completes his measurement work, the state of the whole quantum system will collapse into

$$\begin{aligned}
|\psi\rangle = &\frac{1}{4\sqrt{2}}[|\varphi_1\rangle_{22'}(\alpha|0000000\rangle - \beta|1111111\rangle)_{3-9} \\
&+ |\varphi_2\rangle_{22'}(\alpha|0000000\rangle + \beta|1111111\rangle)_{3-9} \\
&+ |\varphi_3\rangle_{22'}(-\beta|1111000\rangle + \alpha|0000111\rangle)_{3-9} \\
&+ |\varphi_4\rangle_{22'}(\beta|1111000\rangle + \alpha|0000111\rangle)_{3-9}] \\
&\otimes (|00000\rangle + |11111\rangle)_{3'10-13} \otimes (|00000\rangle + |11111\rangle)_{4'14-17} \\
&\otimes (|00000\rangle + |11111\rangle)_{5'18-21}
\end{aligned} \tag{8}$$

Assume Bob_1's measurement result is $|\varphi_1\rangle$, after Bob_2 implements a Bell-basis measurement on particles 3 and $3'$, the state of the whole quantum system can be written as

$$\begin{aligned}
|\psi\rangle = &\frac{1}{8}[|\varphi_1\rangle_{33'}(\alpha|0000000000\rangle - \beta|1111111111\rangle)_{4-13} \\
&+ |\varphi_2\rangle_{33'}(\alpha|0000000000\rangle + \beta|1111111111\rangle)_{4-13} \\
&+ |\varphi_3\rangle_{33'}(-\beta|1111110000\rangle + \alpha|0000001111\rangle)_{4-13} \\
&+ |\varphi_4\rangle_{33'}(\beta|1111110000\rangle + \alpha|0000001111\rangle)_{4-13}] \\
&\otimes (|00000\rangle + |11111\rangle)_{4'14-17} \otimes (|00000\rangle + |11111\rangle)_{5'18-21}
\end{aligned} \tag{9}$$

Assume Bob_2's measurement result is $|\varphi_1\rangle$, after Bob_3 carries out a Bell-basis measurement on particles 4 and $4'$, the state of the whole quantum system can be expressed as

$$
\begin{aligned}
|\psi\rangle = & \frac{1}{8\sqrt{2}}[|\varphi_1\rangle_{44'}(\alpha|0000000000000\rangle - \beta|1111111111111\rangle)_{5-17} \\
& + |\varphi_2\rangle_{44'}(\alpha|0000000000000\rangle + \beta|1111111111111\rangle)_{5-17} \\
& + |\varphi_3\rangle_{44'}(-\beta|1111111110000\rangle + \alpha|0000000001111\rangle)_{5-17} \\
& + |\varphi_4\rangle_{44'}(\beta|1111111110000\rangle + \alpha|0000000001111\rangle)_{5-17}] \\
& \otimes (|00000\rangle + |11111\rangle)_{5'18-21}
\end{aligned} \tag{10}
$$

Assume Bob$_3$'s measurement result is $|\varphi_1\rangle$, after Bob$_4$ executes a Bell-basis measurement on particles 5 and 5$'$, the state of the whole quantum system can be depicted as

$$
\begin{aligned}
|\psi\rangle = & \frac{1}{16}[|\varphi_1\rangle_{55'}(\alpha|0000000000000000 - \beta|1111111111111111\rangle)_{6-21} \\
& + |\varphi_2\rangle_{55'}(\alpha|0000000000000000\rangle + \beta|1111111111111111\rangle)_{6-21} \\
& + |\varphi_3\rangle_{55'}(-\beta|1111111111110000\rangle + \alpha|0000000000001111\rangle)_{6-21} \\
& + |\varphi_4\rangle_{55'}(\beta|1111111111110000\rangle + \alpha|0000000000001111\rangle)_{6-21}
\end{aligned} \tag{11}
$$

If Alice empowers Charlie$_1$ to recover the secret, she will announce her measurement results. Charlie$_i$$(i = 2, \cdots, 16)$ should respectively carry out a single-qubit measurement in the basis $|X^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ on their own particles and publish their measurement outcomes to Charlie$_1$ via classical channels. In the light of the measurement outcomes from Charlie$_i$$(i = 2, \cdots, 16)$, Charlie$_1$ can recover the original secret by applying a corresponding unitary transformation on his particle 6.

If Alice wishes to make more agents share this secret, she does not publish her measurement results and not designate any agent to reconstruct it. Charlie$_i$$(i = 2, \cdots, 16)$ will continue to distribute the secret to the third layer. To be apparent, Charlie$_i$ cannot recover the secret accurately, since they are unaware of Alice's measurement results.

2.3 The Secret Sharing of Higher Layer

As shown in Fig. 3, we can achieve the secret sharing of higher layer in the same way described in Subsect. 2.2. Take the third layer as an example, Charlie$_i$ needs to prepare one five-particle maximally entangled GHZ states, sends four particles to four agents in the fourth layer with the help of decoy photons, leaves one particle in her own hand, and performs a Bell-basis measurements on two particles in her own hands. Finally, the secret can be shared with 4^3 agents in the third layer. Repeat this work again and again, we are able to realize that the number of each layer of agents is a geometric sequence with common ratio 4. With the increase of layer number, the secret can be shared with more and more agents. It is worth noting that no matter how many agents the secret is shared with, our proposed protocol only needs five-particle GHZ states.

3 Iterative Algorithms

In this section, we make every endeavor to look for an appropriate manner to clearly exhibit the whole evolution process of multi-layer quantum secret sharing protocols. The

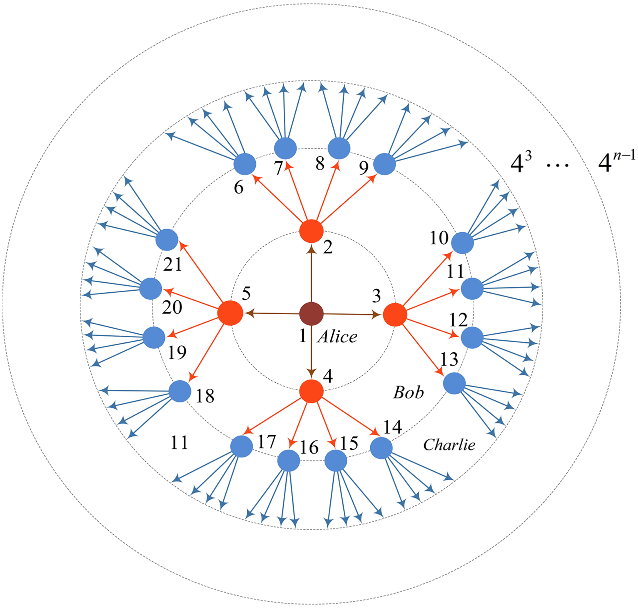

Fig. 3. The secret sharing process of higher layer

core work is how to calculate the collapsed states and recovery operations quickly and accurately. In view of the fact, we design two iterative algorithms to quickly calculate the collapsed states as well as recovery operations. Algorithm 1 is helpful to quickly calculate the final collapsed states in each layer, while Algorithm 2 is capable of obtaining the specific recovery operation performed by the designated agent in the last layer.

3.1 Algorithm 1

Algorithm 1 Calculate the final collapsed states carrying the secret in every layer

Input: The total numbers of layers m, all the measurement results $|\varphi'_{i,j}\rangle (1 \le i \le m, 1 \le j \le 4^{i-1} m)$ and the collapsed state $|\psi_{1,1}\rangle$ of the first layer

Output: Multi-qubit entangled states carrying the secret in the mth layer $|\psi\rangle$

Initiate $|\psi\rangle$

Generate a reference Table 2 in accordance with Eq.(5)

for $i = 2$ to m **do**

$|\psi_{i,j-1}\rangle = |\psi_{i-1,4^{i-2}}\rangle$

for $j = 1$ to 4^{i-1} **do**

Denote α and it's symbol as α' as well as β and it's symbol as β', where α and β are the coefficients of the collapsed state $|\psi_{i,j-1}\rangle$

Compare the first qubit of the collapsed state $|\psi_{i,j-1}\rangle$ with the j th one of GHZ $= |0\rangle^{\otimes 4^{i-1}} + |1\rangle^{\otimes 4^{i-1}}$ from left to right

if They are equal **then**

$|\psi_{i,j-1}\rangle = \alpha' |\underbrace{\qquad\qquad}_{4^{i-1}+3j-4}\underbrace{\quad}_{4}\rangle + \beta' |\underbrace{\qquad\qquad}_{4^{i-1}+3j-4}\underbrace{\quad}_{4}\rangle$

Fill the last $4^{i-1} + 3j - 4$ bits of $|\psi_{i,j-1}\rangle$ into the first $4^{i-1} + 3j - 4$ ones of $|\psi_{i,j}\rangle$

Query the reference Table 2 according to the current measurement result $|\varphi'_{i,j}\rangle$, find out the corresponding collapsed state and fill this collapsed state into the last four qubits of $|\psi_{i,j}\rangle$

else

$|\psi_{i,j-1}\rangle = \beta' |\underbrace{\qquad\qquad}_{4^{i-1}+3j-4}\underbrace{\quad}_{4}\rangle + \alpha' |\underbrace{\qquad\qquad}_{4^{i-1}+3j-4}\underbrace{\quad}_{4}\rangle$

Fill the last $4^{i-1} + 3j - 4$ bits of $|\psi_{i,j-1}\rangle$ into the first $4^{i-1} + 3j - 4$ ones of $|\psi_{i,j}\rangle$

Query the reference Table 2 according to the current measurement result $|\varphi_{i,j}\rangle$, find out the corresponding collapsed state and fill this collapsed state into the last two qubits of $|\psi_{i,j}\rangle$

end if

end for

Return $|\psi_{i,j}\rangle$ to $|\psi\rangle$

end for

Before describing this algorithm, we needs to do some preparation work. To be specific, we must create a reference table called Table 2 in accordance with Eq. (5), which plays an important role during calculation. Table 2 presents the corresponding relationship between measurement results and collapsed states in the first layer, it will be called to calculate the collapsed states in next layers. Table 2 is described as follows.

3.2 Algorithm 2

In the last layer, the secret from Alice must be carried by the multi-particle entangled states. The function of Algorithm 2 is able to help the researchers to effectively acquire

Table 2. Corresponding relationship between Alice's measurement results and the collapsed states in Bob_1–Bob_4's hands in the first layer

Alice's GM results $\lvert\varphi'_{1,1}\rangle$	The collapsed states $\lvert\psi_{1,1}\rangle$ in Bob_1–Bob_4's hands
$\lvert\varphi_1\rangle$	$\alpha\lvert 0000\rangle + \beta\lvert 1111\rangle$
$\lvert\varphi_2\rangle$	$\alpha\lvert 0000\rangle - \beta\lvert 1111\rangle$
$\lvert\varphi_3\rangle$	$\alpha\lvert 0000\rangle - \beta\lvert 1111\rangle$
$\lvert\varphi_4\rangle$	$\alpha\lvert 0000\rangle + \beta\lvert 1111\rangle$

the recovery operations. For simplicity, in the following algorithm we assume Alice empowers the first agent in the last layer to recover the secret.

Algorithm 2 Calculate the recovery operations

Input: The multi-qubit entangled states carrying the secret $\lvert\psi_{m,4^{m-1}}\rangle$ and the single particle measurement results $SM_i(i = 2, \cdots, 4^m)$ from the $4^m - 1$ agents in the mth layer

Output: The operations performed by the designated agent who is responsible for recovering the secret

1: Initiate the operation OP

2: Record the positions of all the 1 in the term with the coefficients α and β of $\lvert\psi_{m,2^{m-1}}\rangle$, respectively

3: Count the number C_α and C_β of the measurement outcome $\lvert -\rangle$ corresponding to the position of 1 in the term with the coefficients α and β

4: Generate the final collapsed state $(-1)^{C_\alpha}\alpha\lvert\bar{0}\rangle + (-1)^{C_\beta}\beta\lvert\bar{1}\rangle$, $\bar{0}$ and $\bar{1}$ correspond the state of the qubit in the first agent in the last layer

5: Obtain the recovery operation OP

4 Conclusion

This paper puts forward a multi-layer QSS protocol based on five-particle GHZ stats by adopting the layered construction. The number of each layer of agents is a geometric sequence with common ratio 4. There exist two bright spots in this paper. The first bright spot is that sharing the quantum secret in multi-party agents only needs GHZ states with less particles which can be easily prepared in the laboratory. The second bright spot is that we design two iterative algorithms for quickly calculating the collapsed states and recovery operations. The ideas of these two algorithms can make a variety of entangled states to be utilized to design multi-layer QSS protocols and wireless communication protocols.

Acknowledgements. The work was supported by the National Natural Science Foundation of China (Grant No. 61672332), Natural Science Foundation of Shanxi Province in China (Grant No. 201801D221159), Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi, China (Grant Nos. 2019L0470 and 2019L0479), the Key R&D program (international science and technology cooperation project) of Shanxi Province, China (No. 201903D421003).

References

1. Huang, W., et al.: Authenticated quantum key distribution with collective detection using single photons. Int. J. Theor. Phys. **55**(10), 4238–4256 (2016). https://doi.org/10.1007/s10773-016-3049-0
2. Zhu, J., Zhang, C., Wang, Q.: Biased decoy-state reference-frame-independent quantum key distribution. Eur. Phys. J. D **71**(12), 1–6 (2017). https://doi.org/10.1140/epjd/e2017-80219-2
3. Zhu, K.-N., Zhou, N.-R., Wang, Y.-Q., Wen, X.-J.: Semi-quantum key distribution protocols with GHZ states. Int. J. Theor. Phys. **57**(12), 3621–3631 (2018). https://doi.org/10.1007/s10773-018-3875-3
4. Zhou, N.R., Zhu, K.N., Zou, X.F.: Multi-party semi-quantum key distribution protocol with four-particle cluster states. Ann. Phys. **531**(8), 1800520 (2019)
5. Xiao, H., Zhang, J., Huang, W., et al.: An efficient quantum key distribution protocol with dense coding on single photons. Comput. Mater. Contin. **61**(2), 759–775 (2019)
6. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
7. Cao, Z., Li, Y., Peng, J., Chai, G., Zhao, G.: Controlled quantum secure direct communication protocol based on Huffman compression coding. Int. J. Theor. Phys. **57**(12), 3632–3642 (2018). https://doi.org/10.1007/s10773-018-3876-2
8. Zheng, X.-y., Long, Y.-x.: Controlled quantum secure direct communication with authentication protocol based on five-particle cluster state and classical XOR operation. Quantum Inf. Process. **18**(5), 1–12 (2019). https://doi.org/10.1007/s11128-019-2239-0
9. Li, Y.H., Li, X.L., Nie, L.P., et al.: Quantum teleportation of three and four-qubit state using multi-qubit cluster states. Int. J. Theor. Phys. **55**(3), 1820–1823 (2016). https://doi.org/10.1007/s10773-015-2821-x
10. Sisodia, M., Verma, V., Thapliyal, K., Pathak, A.: Teleportation of a qubit using entangled non-orthogonal states: a comparative study. Quantum Inf. Process. **16**(3), 1–23 (2017). https://doi.org/10.1007/s11128-017-1526-x
11. Chang, L.W., Zheng, S.H., Gu, L.Z., et al.: Joint remote preparation of an arbitrary five-qubit Brown state via non-maximally entangled channels. Chin. Phys. B **23**(9), 090307 (2014)
12. Chang, L.-W., Zheng, S.-H., Gu, L.-Z., Jin, L., Yang, Y.-X.: Multiparty-controlled joint remote preparation of an arbitrary four-qubit cluster-type state via two different entangled quantum channels. Int. J. Theor. Phys. **54**(8), 2864–2880 (2015). https://doi.org/10.1007/s10773-015-2522-5
13. Jiang, D.-H., Xu, Y.-L., Xu, G.-B.: Arbitrary quantum signature based on local indistinguishability of orthogonal product states. Int. J. Theor. Phys. **58**(3), 1036–1045 (2019). https://doi.org/10.1007/s10773-018-03995-4
14. Chen, F.-L., Liu, W.-F., Chen, S.-G., Wang, Z.-H.: Public-key quantum digital signature scheme with one-time pad private-key. Quantum Inf. Process. **17**(1), 1–14 (2017). https://doi.org/10.1007/s11128-017-1778-5
15. Wei, C.Y., Wang, T.Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A **93**(4), 042318 (2016)
16. Gao, F., Qin, S., Huang, W., Wen, Q.: Quantum private query: a new kind of practical quantum cryptographic protocol. Sci. China Phys. Mech. Astron. **62**(7), 1–12 (2019). https://doi.org/10.1007/s11433-018-9324-6
17. Yan, L., Chang, Y., Zhang, S., et al.: Measure-resend semi-quantum private comparison scheme using GHZ class states. Comput. Mater. Contin. **61**(2), 877–887 (2019)
18. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)

19. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**(1), 162 (1999)
20. Deng, F.G., Li, X.H., Zhou, H.Y.: Efficient high-capacity quantum secret sharing with two-photon entanglement. Phys. Lett. A **372**(12), 1957–1962 (2008)
21. Gu, B., Mu, L., Ding, L., et al.: Fault tolerant three-party quantum secret sharing against collective noise. Opt. Commun. **283**(15), 3099–3103 (2010)
22. Yang, Y.G., Jia, X., Wang, H.Y., et al.: Verifiable quantum (k, n)-threshold secret sharing. Quantum Inf. Process. **11**(6), 1619–1625 (2012). https://doi.org/10.1007/s11128-011-0323-1
23. Hsu, J.L., Chong, S.K., Hwang, T., et al.: Dynamic quantum secret sharing. Quantum Inf. Process. **12**(1), 331–344 (2013). https://doi.org/10.1007/s11128-012-0380-0
24. Rahaman, R., Parker, M.G.: Quantum scheme for secret sharing based on local distinguishability. Phys. Rev. A **91**(2), 022330 (2015)
25. Wang, X.J., An, L.X., Yu, X.T., et al.: Multilayer quantum secret sharing based on GHZ state and generalized Bell basis measurement in multiparty agents. Phys. Lett. A **381**(38), 3282–3288 (2017)
26. Chen, X.B., Dou, Z., Xu, G., et al.: A kind of universal quantum secret sharing protocol. Sci. Rep. **7**, 39845 (2017)
27. Wang, J., Li, L., Peng, H., et al.: Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. Phys. Rev. A **95**(2), 022320 (2017)
28. Wang, J.T., Xu, G., Chen, X.B., et al.: Local distinguishability of Dicke states in quantum secret sharing. Phys. Lett. A **381**(11), 998–1002 (2017)
29. Zhang, K., Zhang, X., Jia, H., et al.: A new n-party quantum secret sharing model based on multiparty entangled states. Quantum Inf. Process. **18**(3), 81 (2019). https://doi.org/10.1007/s11128-019-2201-1
30. Dou, Z., Xu, G., Chen, X.B., et al.: Rational non-hierarchical quantum state sharing protocol. Comput. Mater. Contin. **58**(2), 335–347 (2019)