Commun. Theor. Phys. **72** (2020) 025102 (8pp) https://doi.org/10.1088/1572-9494/ab5d01

Two schemes of multiparty quantum direct secret sharing via a six-particle GHZ state*

Xin-Wei Zha, Ruo-Xu Jiang[1] and Min-Rui Wang

School of Science, Xi'an University of Posts and Telecommunications, Xi'an, 710121, China

E-mail: 1149699324@qq.com

Received 26 July 2019, revised 20 September 2019
Accepted for publication 31 October 2019
Published 22 January 2020

Abstract

In this paper, two new efficient multiparty quantum direct secret sharing schemes are proposed via a six-particle GHZ state and Bell measurements. In the first scheme, based on the theory of security cryptanalysis, the secret message of the sender is directly encoded into the transmitted particles, and all the agents can obtain their information by performing bell measurement on the received particles, and then cooperate to recover the information of the sender. In the second scheme, we define a new secret shared coding method by performing local unitary operations on the transmitted particles, then agents perform Bell measurements on their own particles respectively, and feedback the measurement to the dealer. If the agent's results are matched with the previous coding method, the protocol will work out. In addition, the proposed two schemes have the following common advantages: the sender can send all prepared particles to the receiver, and can send an arbitrary key to the receiver, rather than a random secret key; the proposed schemes do not need to insert any detection sets to detect eavesdropping and can resist both existing attacks and spoofing attacks by dishonest agents. The sender need not to retain any photons, so the sender's quantum memory could be omitted here.

Keywords: quantum direct secret sharing, Bell measurement, security cryptanalysis, local unitary operation

1. Introduction

Quantum secret sharing (QSS) is one of the most valuable significant resources in quantum cryptography, which is also considered as an extension for classical message sharing [1–9] presented independently by Sharmir [10] and Blakley [11] in 1979. Then the QSS attracts much attention and develops faster around the world. In 1999, Hillery *et al* [1] firstly utilized the three-photon and four-photon entangled GHZ state to share the private message, which was generalized to the arbitrary multiparty by Xiao *et al* [3], and the other QSS scheme using a two-particle polarization entangled state was presented by Karlsson *et al* [4] subsequently. Up to now, much of the research of QSS studied in the quantum cryptographic conference, quantum communication and quantum networks [12–16] have been reported.

The multiparty QSS protocol based on quantum entanglement swapping and the identification of Bell states was proposed by Zhang *et al* [17] in 2005, where two qubits are generated by each party. As for Dehkordi *et al* [18] and Shi *et al* [19]'s scheme in 2010, (n + 1) bell pairs are prepared by the dealer as quantum resources, meanwhile the remaining agents can get the secret's shadow by performing Bell measurements without generating other entangled states or performing the operation of local unitary. Recently, Song *et al* [20] presented a more practical scheme in quantum secret sharing, which the designed classical message can be shared only with the Bell state and Bell measurement. However, Liu *et al* [21] pointed out that two dishonest agents or an outside attacker may utilize the protocol's flaw to eavesdrop the secret fully. Thus, some constraints exist in those previous QSS schemes, for instance:

A. The security against the collusion attack and outside attack needs to be improved.
B. Some extra checking sets used for prevent eavesdropping are inserted in the sequences of agents that are prepared in protocol.
C. The sequences of photons are requested to preserve by the dealer, so that the dealer could not forget the quantum memory.

* The work is supported by the National Natural Science Foundation of China (Grant No. 10902083).
[1] Author to whom any correspondence should be addressed.

Compared with the previous papers, [22–37] the advantages of ours are as follows: it is different from those schemes preparing (n + 1) EPR pairs, [19, 23, 24] in our schemes, n six-particle GHZ states can be generated to share two or four predetermined classical bits among n agents rather than delivering a random message without any other local unitary operations; any photons need not be preserved by the sender, thus the quantum memory of the sender can be omitted here; proposed schemes do not need to insert any extra detection sets in the photon sequence of agent to detect eavesdropper's existence and can resist both existing attacks and spoofing attacks by the remaining agents' Bell measurement and selecting measuring basis.

The rest of paper is arranged as follows: our two schemes are detailed in sections 2 and 3, respectively. In section 4, we analyse the schemes' security. The efficiency analysis of the two schemes are given in section 5. Finally, a brief discussion and the concluding summary are given in section 6.

2. Scheme 1: multiparty QDSS scheme (two classical bits sharing)

Before describing scheme 1, we first briefly introduce the four kinds of Bell states used to measure particles and four local unitary operations used for encoding:

$$\begin{aligned}
|\phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)\\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle + |{-}{+}\rangle)\\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle - |{-}{-}\rangle)\\
|\phi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle - |{-}{+}\rangle) \qquad (1)
\end{aligned}$$

$$\begin{aligned}
I &= |0\rangle\langle 0| + |1\rangle\langle 1|\\
Z &= |0\rangle\langle 0| - |1\rangle\langle 1|\\
X &= |0\rangle\langle 1| + |1\rangle\langle 0|\\
Y &= |0\rangle\langle 1| - |1\rangle\langle 0| \qquad (2)
\end{aligned}$$

where $|0\rangle$ and $|1\rangle$ are Z-basis, and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are X-basis. It is assumed that the four local unitary operations are encoded as four classical bits respectively:

$$\begin{aligned}
\sigma_{00} &= I \ \ to \ \ '00',\\
\sigma_{01} &= Z \ \ to \ \ '01',\\
\sigma_{10} &= X \ \ to \ \ '10',\\
\sigma_{11} &= Y \ \ to \ \ '11',
\end{aligned}$$

Next, the secret information encoding are added to the Bell state by unitary operations.

Let us analyze a four-party QDSS scheme firstly: suppose that a 2N bit class encrypted message M is delivered to the other three agents (Bob, Charlie and David) by the dealer Alice, meanwhile the contents of this encrypted message can only be known if all agents cooperate together. The specific scheme is implemented as follows:

(1) Alice first prepares a six-particle GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000000\rangle + |111111\rangle)_{123456}$, then a special local unitary operation is performed on the sixth particle.
(2) Assume that particles (1, 2) belong to Bob, particles (3, 4) are in the possession of Charlie, and David owns particles (5, 6).
(3) After the secure quantum channel is set up, all agents perform Bell measurement on their particles, and the corresponding relationship between their measurement results can be depicted as follows:

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(I\otimes I\otimes I\otimes I\otimes \sigma_{00})\\
&\quad (|000000\rangle + |111111\rangle)_{123456}\\
&= \frac{1}{2}(|\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_1\rangle_{56} + |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_2\rangle_{56}\\
&\quad + |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_2\rangle_{56} + |\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_1\rangle_{56}) \qquad (3)
\end{aligned}$$

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{\sqrt{2}}(I\otimes I\otimes I\otimes I\otimes \sigma_{01})\\
&\quad (|000000\rangle + |111111\rangle)_{123456}\\
&= \left[\frac{1}{\sqrt{2}}(|000000\rangle - |111111\rangle)\right]_{123456}\\
&= \frac{1}{2}(|\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_2\rangle_{56} + |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_1\rangle_{56}\\
&\quad + |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_1\rangle_{56} + |\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_2\rangle_{56}) \qquad (4)
\end{aligned}$$

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{2}}(I\otimes I\otimes I\otimes I\otimes \sigma_{10})\\
&\quad (|000000\rangle + |111111\rangle)_{123456}\\
&= \left[\frac{1}{\sqrt{2}}(|000001\rangle + |111110\rangle)\right]_{123456}\\
&= \frac{1}{2}(|\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_3\rangle_{56} + |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_4\rangle_{56}\\
&\quad + |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_4\rangle_{56} + |\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_3\rangle_{56}) \qquad (5)
\end{aligned}$$

$$\begin{aligned}
|\psi_4\rangle &= \frac{1}{\sqrt{2}}(I\otimes I\otimes I\otimes I\otimes \sigma_{11})\\
&\quad (|000000\rangle + |111111\rangle)_{123456}\\
&= \left[\frac{1}{\sqrt{2}}(-|000001\rangle + |111110\rangle)\right]_{123456}\\
&= \frac{1}{2}(-|\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_4\rangle_{56} - |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_3\rangle_{56}\\
&\quad - |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_3\rangle_{56} - |\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_4\rangle_{56}) \qquad (6)
\end{aligned}$$

At this point, the participants encode the quantum state as follows:

$$\begin{aligned}
|\phi_1\rangle \ \ as \ \ '00',\\
|\phi_2\rangle \ \ as \ \ '01',\\
|\phi_3\rangle \ \ as \ \ '10',\\
|\phi_4\rangle \ \ as \ \ '11',
\end{aligned}$$

From the above four expressions (from equation (3) to equation (6)), it is not hard to find that the local unitary local operations encoded as the classical bits can be deduced from the Bell state measurement results of participants, which

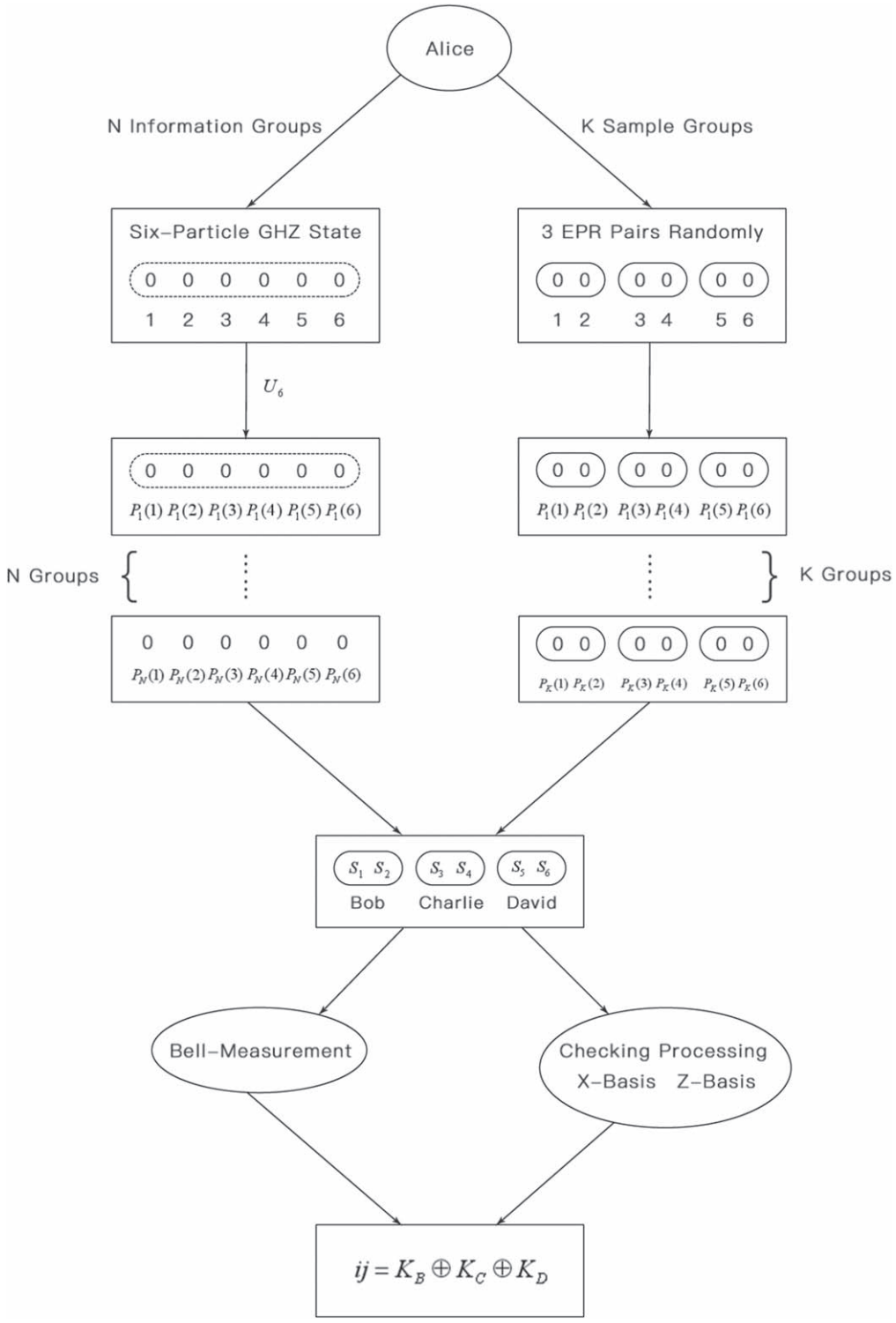

Figure 1. The flow chart of scheme 1 includes the distribution of particles sequences and corresponding unitary operation U_6.

satisfies the following formula:

$$ij = S_{12} \oplus S_{34} \oplus S_{56} \tag{7}$$

where ij belongs to {00, 01, 10, 11}, representing the subscript of the local unitary operation acting on the sixth particle, meanwhile S_{uv} represents the coding of Bell measurement results on particles u and v respectively. For instance, in $|\psi_3\rangle$, the corresponding local unitary operation acting on the sixth particle is σ_{10} and all Bell measurement results satisfy $S_{12} \oplus S_{34} \oplus S_{56}$. By taking the advantage of this character, we can build a set of classical secret information system that can be shared among all the participants.

Next, we will give the detail of the four-party (2 bits) QDSS scheme and figure 1 shows the basic idea of scheme 1.

(1) Firstly, dealer Alice prepares N groups of six-particle GHZ state and K groups EPR pairs, where there is only one six-particle GHZ state in each N (information) group.

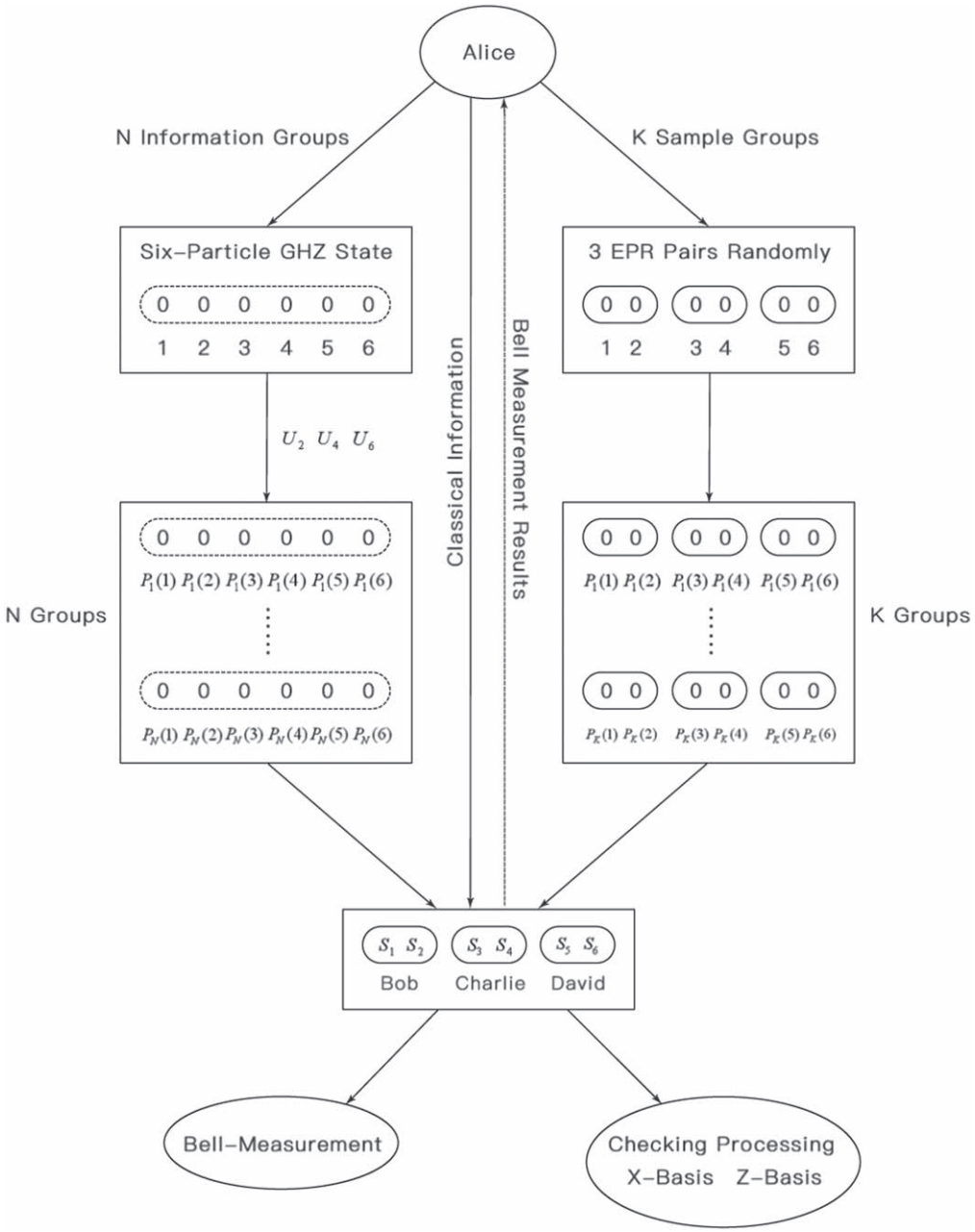

Figure 2. The flow chart of scheme 2 includes the distribution of particles sequences and corresponding unitary operations U_2, U_4, U_6.

As for rest K (sample) groups, which are used to check the scheme's security and each k group contains three pairs of four Bell states at random $\{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle\}$.

(2) Secondly, dealer Alice records the locations of K sample groups. Then the local unitary operations are used to encode the secret coding on the sixth particle of the six-particle GHZ state. Last, Alice then divides all the prepared particles into six sequences.

$$S_1 = [P_1(1), P_2(1),\ldots, P_{N+K}(1)],$$
$$S_2 = [P_1(2), P_2(2),\ldots, P_{N+K}(2)]$$
$$S_3 = [P_1(3), P_2(3),\ldots, P_{N+K}(3)],$$
$$S_4 = [P_1(4), P_2(4),\ldots, P_{N+K}(4)]$$
$$S_5 = [P_1(5), P_2(5),\ldots, P_{N+K}(5)],$$
$$S_6 = [P_1(6), P_2(6),\ldots, P_{N+K}(6)]$$

As for $P_i(j)$, i represents the groups from one to N + K; j stands for the particles' sequence.

(3) Thirdly, dealer Alice sends the sequence $\{S1, S2\}$ to Bob, sequence $\{S3, S4\}$ to Charlie, and sequence $\{S5, S6\}$ is sent to David.

(4) After confirming that Bob, Charlie and David have received their own particle sequences, Alice begins to perform the process of eavesdropping checking. First, she randomly announced the position of the sample group and the measurement basis chosen from the Z or X basis. Based on these information, by using the the corresponding measurement basis, each agent measures the sample particles on the corresponding measurement basis and tells the dealer (Alice) their measurement results subsequently. Finally, Alice can deduce the

communication's error rate according to original state and measurement results of the particles in the sample group. If the value is lower than the threshold, the protocol continues. Otherwise, the protocol will be abandoned.

(5) Agents Bob, Charlie and David perform Bell measurements on their own particles respectively for the remaining N information groups, and the measurement results stand for part of their secret: K_B, K_C, K_D. It is not difficult to find that agents Bob, Charlie and David can cooperate to reconstruct the information of dealer (Alice)$ij = K_B \oplus K_C \oplus K_D$.

Attention: symbol '$\oplus$' represents exclusive-OR value.

3. Scheme 2: a newly proposed multiparty QDSS scheme (four classical bits sharing)

The dealer (Alice) prepares a six-particle GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000000\rangle + |111111\rangle)_{123456}$ firstly, where particles (1, 2) belong to Bob, particles (3, 4) are in the possession of Charlie, and David owns particles (5, 6). Then the unitary operations (shown in (2)) are performed on the second, fourth and sixth particles of the GHZ state respectively, (64 changes totally), which are listed as follows:

$$
\begin{array}{cccc}
I_2I_4I_6, & Y_2I_4I_6, & X_2I_4I_6, & Z_2I_4I_6,\\
I_2I_4Z_6, & Y_2I_4Z_6, & X_2I_4Z_6, & Z_2I_4Z_6,\\
I_2I_4X_6, & Y_2I_4X_6, & X_2I_4X_6, & Z_2I_4X_6,\\
I_2I_4Y_6, & Y_2I_4Y_6, & X_2I_4Y_6, & Z_2I_4Y_6,\\
I_2Z_4I_6, & Y_2Z_4I_6, & X_2Z_4I_6, & Z_2Z_4I_6,\\
I_2Z_4Z_6, & Y_2Z_4Z_6, & X_2Z_4Z_6, & Z_2Z_4Z_6,\\
I_2Z_4X_6, & Y_2Z_4X_6, & X_2Z_4X_6, & Z_2Z_4X_6,\\
I_2Z_4Y_6, & Y_2Z_4Y_6, & X_2Z_4Y_6, & Z_2Z_4Y_6,\\
I_2X_4I_6, & Y_2X_4I_6, & X_2X_4I_6, & Z_2X_4I_6,\\
I_2X_4Z_6, & Y_2X_4Z_6, & X_2X_4Z_6, & Z_2X_4Z_6,\\
I_2X_4X_6, & Y_2X_4X_6, & X_2X_4X_6, & Z_2X_4X_6,\\
I_2X_4Y_6, & Y_2X_4Y_6, & X_2X_4Y_6, & Z_2X_4Y_6,\\
I_2Y_4I_6, & Y_2Y_4I_6, & X_2Y_4I_6, & Z_2Y_4I_6,\\
I_2Y_4Z_6, & Y_2Y_4Z_6, & X_2Y_4Z_6, & Z_2Y_4Z_6,\\
I_2Y_4X_6, & Y_2Y_4X_6, & X_2Y_4X_6, & Z_2Y_4X_6,\\
I_2Y_4Y_6, & Y_2Y_4Y_6, & X_2Y_4Y_6, & Z_2Y_4Y_6,
\end{array}
$$

Finally, three agents perform Bell measurement on their own particles respectively. By comparing the Bell measurement results of 64 kinds of unitary transformations, it is not tough to find that 48 kinds of the Bell measurement results are the same. Therefore, the corresponding local unitary operation and Bell measurement results of the remaining 16 kinds of six-particle GHZ state are shown as follows:

$$
\begin{aligned}
\varphi_1 : Z_2Z_4I_6 \quad & \frac{1}{2}(|\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_1\rangle_{56} + |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_2\rangle_{56}\\
& + |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_2\rangle_{56} + |\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_1\rangle_{56})\\
\varphi_2 : Z_2Z_4Z_6 \quad & \frac{1}{2}(|\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_2\rangle_{56} + |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_1\rangle_{56}\\
& + |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_1\rangle_{56} + |\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_2\rangle_{56}\\
\varphi_3 : Z_2Z_4X_6 \quad & \frac{1}{2}(|\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_3\rangle_{56} + |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_4\rangle_{56}\\
& + |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_4\rangle_{56} + |\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_3\rangle_{56}\\
\varphi_4 : Z_2Z_4Y_6 \quad & \frac{1}{2}(-|\phi_2\rangle_{12}|\phi_2\rangle_{34}|\phi_4\rangle_{56} - |\phi_2\rangle_{12}|\phi_1\rangle_{34}|\phi_3\rangle_{56}\\
& - |\phi_1\rangle_{12}|\phi_2\rangle_{34}|\phi_3\rangle_{56} - |\phi_1\rangle_{12}|\phi_1\rangle_{34}|\phi_4\rangle_{56}\\
\varphi_5 : Z_2X_4I_6 \quad & \frac{1}{2}(|\phi_2\rangle_{12}|\phi_3\rangle_{34}|\phi_1\rangle_{56} + |\phi_2\rangle_{12}|\phi_4\rangle_{34}|\phi_2\rangle_{56}\\
& + |\phi_1\rangle_{12}|\phi_3\rangle_{34}|\phi_2\rangle_{56} + |\phi_1\rangle_{12}|\phi_4\rangle_{34}|\phi_1\rangle_{56}\\
\varphi_6 : Z_2X_4Z_6 \quad & \frac{1}{2}(|\phi_2\rangle_{12}|\phi_3\rangle_{34}|\phi_2\rangle_{56} + |\phi_2\rangle_{12}|\phi_4\rangle_{34}|\phi_1\rangle_{56}\\
& + |\phi_1\rangle_{12}|\phi_3\rangle_{34}|\phi_1\rangle_{56} + |\phi_1\rangle_{12}|\phi_4\rangle_{34}|\phi_2\rangle_{56}\\
\varphi_7 : Z_2X_4X_6 \quad & \frac{1}{2}(|\phi_2\rangle_{12}|\phi_3\rangle_{34}|\phi_3\rangle_{56} + |\phi_2\rangle_{12}|\phi_4\rangle_{34}|\phi_4\rangle_{56}\\
& + |\phi_1\rangle_{12}|\phi_3\rangle_{34}|\phi_4\rangle_{56} + |\phi_1\rangle_{12}|\phi_4\rangle_{34}|\phi_3\rangle_{56}\\
\varphi_8 : Z_2X_4Y_6 \quad & \frac{1}{2}(-|\phi_2\rangle_{12}|\phi_3\rangle_{34}|\phi_4\rangle_{56} - |\phi_2\rangle_{12}|\phi_4\rangle_{34}|\phi_3\rangle_{56}\\
& - |\phi_1\rangle_{12}|\phi_3\rangle_{34}|\phi_3\rangle_{56} - |\phi_1\rangle_{12}|\phi_4\rangle_{34}|\phi_4\rangle_{56}\\
\varphi_9 : X_2Z_4I_6 \quad & \frac{1}{2}(|\phi_3\rangle_{12}|\phi_2\rangle_{34}|\phi_1\rangle_{56} + |\phi_3\rangle_{12}|\phi_1\rangle_{34}|\phi_2\rangle_{56}\\
& + |\phi_4\rangle_{12}|\phi_2\rangle_{34}|\phi_2\rangle_{56} + |\phi_4\rangle_{12}|\phi_1\rangle_{34}|\phi_1\rangle_{56}\\
\varphi_{10} : X_2Z_4Z_6 \quad & \frac{1}{2}(|\phi_3\rangle_{12}|\phi_2\rangle_{34}|\phi_2\rangle_{56} + |\phi_3\rangle_{12}|\phi_1\rangle_{34}|\phi_1\rangle_{56}\\
& + |\phi_4\rangle_{12}|\phi_2\rangle_{34}|\phi_1\rangle_{56} + |\phi_4\rangle_{12}|\phi_1\rangle_{34}|\phi_2\rangle_{56}\\
\varphi_{11} : X_2Z_4X_6 \quad & \frac{1}{2}(|\phi_3\rangle_{12}|\phi_2\rangle_{34}|\phi_3\rangle_{56} + |\phi_3\rangle_{12}|\phi_1\rangle_{34}|\phi_4\rangle_{56}\\
& + |\phi_4\rangle_{12}|\phi_2\rangle_{34}|\phi_4\rangle_{56} + |\phi_4\rangle_{12}|\phi_1\rangle_{34}|\phi_3\rangle_{56}\\
\varphi_{12} : X_2Z_4Y_6 \quad & \frac{1}{2}(-|\phi_3\rangle_{12}|\phi_2\rangle_{34}|\phi_4\rangle_{56} - |\phi_3\rangle_{12}|\phi_1\rangle_{34}|\phi_3\rangle_{56}\\
& - |\phi_4\rangle_{12}|\phi_2\rangle_{34}|\phi_3\rangle_{56} - |\phi_4\rangle_{12}|\phi_1\rangle_{34}|\phi_4\rangle_{56}\\
\varphi_{13} : X_2X_4I_6 \quad & \frac{1}{2}(|\phi_3\rangle_{12}|\phi_3\rangle_{34}|\phi_1\rangle_{56} + |\phi_3\rangle_{12}|\phi_4\rangle_4|\phi_2\rangle_{56}\\
& + |\phi_4\rangle_{12}|\phi_3\rangle_{34}|\phi_2\rangle_{56} + |\phi_4\rangle_{12}|\phi_4\rangle_{34}|\phi_1\rangle_{56}\\
\varphi_{14} : X_2X_4Z_6 \quad & \frac{1}{2}(|\phi_3\rangle_{12}|\phi_3\rangle_{34}|\phi_2\rangle_{56} + |\phi_3\rangle_{12}|\phi_4\rangle_{34}|\phi_1\rangle_{56}\\
& + |\phi_4\rangle_{12}|\phi_3\rangle_{34}|\phi_1\rangle_{56} + |\phi_4\rangle_{12}|\phi_4\rangle_{34}|\phi_2\rangle_{56}\\
\varphi_{15} : X_2X_4X_6 \quad & \frac{1}{2}(|\phi_3\rangle_{12}|\phi_3\rangle_{34}|\phi_3\rangle_{56} + |\phi_3\rangle_{12}|\phi_4\rangle_{34}|\phi_4\rangle_{56}\\
& + |\phi_4\rangle_{12}|\phi_3\rangle_{34}|\phi_4\rangle_{56} + |\phi_4\rangle_{12}|\phi_4\rangle_{34}|\phi_3\rangle_{56}\\
\varphi_{16} : X_2X_4Y_6 \quad & \frac{1}{2}(-|\phi_3\rangle_{12}|\phi_3\rangle_{34}|\phi_4\rangle_{56} - |\phi_3\rangle_{12}|\phi_4\rangle_{34}|\phi_3\rangle_{56}\\
& - |\phi_4\rangle_{12}|\phi_3\rangle_{34}|\phi_3\rangle_{56} - |\phi_4\rangle_{12}|\phi_4\rangle_{34}|\phi_4\rangle_{56}
\end{aligned}
$$

Therefore, we define (φ_1, φ_2 . . . φ_{15}, φ_{16}) respectively, representing the shared classical bit (0000, 0001. . . 1110, 1111), as shown in the following:

$$\begin{aligned}
\varphi_1 &: Z_2Z_4I_6 \quad 0000\\
\varphi_2 &: Z_2Z_4Z_6 \quad 0001\\
\varphi_3 &: Z_2Z_4X_6 \quad 0010\\
\varphi_4 &: Z_2Z_4Y_6 \quad 0011\\
\varphi_5 &: Z_2X_4I_6 \quad 0100\\
\varphi_6 &: Z_2X_4Z_6 \quad 0101\\
\varphi_7 &: Z_2X_4X_6 \quad 0110\\
\varphi_8 &: Z_2X_4Y_6 \quad 0111\\
\varphi_9 &: X_2Z_4I_6 \quad 1000\\
\varphi_{10} &: X_2Z_4Z_6 \quad 1001\\
\varphi_{11} &: X_2Z_4X_6 \quad 1010\\
\varphi_{12} &: X_2Z_4Y_6 \quad 1011\\
\varphi_{13} &: X_2X_4I_6 \quad 1100\\
\varphi_{14} &: X_2X_4Z_6 \quad 1101\\
\varphi_{15} &: X_2X_4X_6 \quad 1110\\
\varphi_{16} &: X_2X_4Y_6 \quad 1111
\end{aligned}$$

If dealer (Alice) wants to share a 4N bits classic encrypted message M to the remaining agents, Bob, Charlie and David only under the cooperation of all agents can we know the content of this secret message. For example, Alice first prepares a six-particle GHZ state. Suppose that the dealer (Alice) wants to share the classical information (0011), so we need Alice to perform operation Z^2 on particle 2, Z^4 on particle 4, Y^6 on particle 6. Later, three agents perform Bell measurement on their own particles and inform the dealer (Alice) of their measurement results. In order to prevent agents from executing internal attack and external attack, Alice compares all agents' Bell measurement results with the local unitary operation and Bell measurement results of 16 kinds of six-particle GHZ states defined above. If the two measurement results are the same, Alice can inform the agents of the secret information she wants to share (i.e. we call this encoding method tabulation).

Now, let us give the detailed steps of method tabulation (four-party of 4-bit QDSS scheme) in the following (figure 2 shows the schematic diagram of QDSS for four parties in scheme 2):

(1) First, dealer Alice generates N groups of six-particle GHZ state and K groups EPR pairs, which there is only one six-particle GHZ state in each N group, and for the remaining K sample groups, each group contains 3 EPR pairs randomly of 4 Bell states, which are used to check information security.
(2) Dealer Alice records the locations of k sample groups. For the remaining N information groups, the encoding of the secret is imposed on the second, fourth and sixth particles of the six-particle GHZ state by the corresponding local unitary operations. Alice then divides these particles into six sequences (the same as step two in scheme 1):

$$\begin{aligned}
S_1 &= [P_1(1), P_2(1), \ldots, P_{N+K}(1)],\\
S_2 &= [P_1(2), P_2(2), \ldots, P_{N+K}(2)]\\
S_3 &= [P_1(3), P_2(3), \ldots, P_{N+K}(3)],\\
S_4 &= [P_1(4), P_2(4), \ldots, P_{N+K}(4)]\\
S_5 &= [P_1(5), P_2(5), \ldots, P_{N+K}(5)],\\
S_6 &= [P_1(6), P_2(6), \ldots, P_{N+K}(6)]
\end{aligned}$$

(3) Dealer Alice delivers the sequence (S_1, S_2) to Bob, sequence (S_3, S_4) to Charlie, and sequence (S_5, S_6) to David.
(4) After all agents receive their own particle sequences, Alice executes the process of eavesdropping detection.
   a. She randomly announces the location of the K sample group and the corresponding measurement basis (Z-basis or X-basis).
   b. Each agent measures the sample particles on the matched measurement basis and tells the dealer (Alice) their measurement results.
   c. Alice can deduce the error rate, based on the measurement results and the particles' original state in the sample group. Similarly to step (4) in scheme 1, if the value is lower than the threshold, the protocol continues. Otherwise, the protocol will be abandoned.
(5) To prevent the secret message from being leaked, agents Bob, Charlie and David respectively measure their particles of the remaining N information groups and inform the dealer (Alice) of their corresponding measurement results. Alice compares the agents' measurement results with local unitary operation and 16 kinds of Bell measurement result of six-particle GHZ states defined above. If the two measurement results are the same, Alice can inform each agent of the classical information that she wants to share.

4. Security analysis

We will demonstrate the security of both scenarios in this section. As we know, no quantum qubits carrying secret messages are transmitted in the quantum channel in the proposed two schemes. Thus, only during the preparation phase that an attacker, Eve, may launch an attack. Therefore, we can guarantee that the two schemes we proposed are absolutely safe, as long as we are sure that the quantum channel and all agents are safe. In other words, the above schemes can be guaranteed to be unconditionally safe if dishonest agents can be prevented from making false statements. In the following statement, these attacks will be analyzed: collusion attack and intercept-and-resend attack.

4.1. Security analysis of collusion attack

Without loss of generality, two or more dishonest agents may conspire to eavesdrop the secret information. Among the

Table 1. The analysis of several schemes' qubit efficiency.

Parameter/Scheme	[18]	[17]	Scheme 1	Scheme 2
Classical bits of information in a four-party	6	6	6	12
Total qubits used in a four-party	30	36	24	24
Qubits efficiency in a four-party	20%	16. 67%	25%	50%

above schemes, suppose that both Charlie and David are dishonest agents. Meanwhile, they try to deliver an attack to steal the secret information shared by Alice without Bob's help. In our presented schemes, however, dealer (Alice) distributes all her prepared particles to the remaining agents, which means Alice is not required to keep any photons. Hence, the information ($ij = K_B + K_C + K_D$) is unknown to agents Charlie and David in scheme 1. In scheme 2, the dealer (Alice) needs to compare the defined encoding scheme with agents' Bell measurement result, from which we can conclude that our QDSS schemes are absolutely safe for two or more dishonest agents.

4.2. Security analysis of intercept-and-resend attack

Suppose some dishonest agents exist who can intercept the dealer's (Alice) particle sequences and resend the forged particles generated by themselves in order to perform eavesdropping processing. So, the original sequences of particles can be obtained by them (i.e. they may steal the information of Alice). However, based on step (1) of our proposed two schemes, Alice has randomly inserted k sample groups information in each delivered sequence which then requires agents to measure and check the results of measurement. Actually, once the dishonest agent performs an intercept-and-resend attack, he will not be able to obtain the position, corresponding measurement basis of each decoy photon. In addition, since the measurement basis is selected to measure the sample group randomly by each agent, the successful rate is lower than the value $\left(\frac{1}{4}\right)^K$, where K stands for the amount of sample particles in each sequence delivered to the rest of the agents.

5. Efficiency analysis

We compare the qubit efficiency of several schemes with us in this part. Generally, there are two main methods to define the qubit efficiency. One is $\eta = \frac{q_u}{q_t + q_b}$ [38], another is $\eta = \frac{q_u}{q_t}$ [39], where q_u stands for the total classical bits of information transmitted;q_t on behalf of total number of particles prepared by dealer Alice;q_b denotes the number of classical bits announced. As for $\eta = \frac{q_u}{q_t + q_b}$, it is not tough to prove that not only our schemes but most of previous presented will reach 100%. Therefore, we choose the equation $\eta = \frac{q_u}{q_t}$ to define our schemes' qubit efficiency, which emphasizes the average contribution of each photon of the shared key. It is assumed to be that there are one third decoy particles in the whole quantum channel system for each agent (i.e. $N = 3K$).

In scheme 1, for four-party secret sharing, i.e. 3 agents existing, suppose that a 6-bit classical encrypted message is delivered to the remaining three agents and the dealer Alice generates three groups of six-particle GHZ state and three EPR pairs, so the qubit efficiency of scheme 1 for four parties is $\frac{3 \times 2}{3 \times 6 + 6}$; The qubit efficiency of scheme 2 can be expressed as $\frac{3 \times 4}{3 \times 6 + 6}$ in the same way. Meanwhile, table 1 presents, in a more direct fashion, that our qubit efficiency is higher than the others.

6. Conclusion and summary

In this article, we propose two efficient and practical quantum direct secret sharing schemes, which the dealer (Alice) can share a certain secret information through the local unitary operations among agents. And then, Bell measurements are performed by the rest of the agents to obtain the corresponding shadows, which is unknown to the dealer (Alice). In addition, neither of the two proposed schemes in this paper need to insert a set of detection devices into the particle sequence of the agents to detect eavesdropping, which also proves that they are more convenient than other schemes in practical applications. Finally, the schemes we proposed can not only resist the participants' attack but also provide higher efficiency of transmission and reduce the complexity in practical applications.

References

[1] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[2] Nie Y Y, Li Y H and Liu J C 2011 *Int. J. Theor. Phys.* **50** 2526
[3] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[4] Xiao L, Long G L, Pan F G and Pan J W 2004 *Phys. Rev.* A **69** 052307
[5] Lance A M, Symul T and Bowen W P 2004 *Phys. Rev. Lett.* **92** 177903
[6] Qin H W, Zhu X H and Dai Y W 2015 *Quantum Inf. Proc.* **14** 2997
[7] Deng F G, Zhou H Y and Long G L 2006 *J. Phys. A Math. Gen.* **39** 14089
[8] Chen J H, Lee K C and Hwang T 1999 *Int. J. Mod. Phys.* C **20** 1531
[9] Lin J and Hwang T 2011 *Opt. Commun.* **284** 1468
[10] Shamir A 1979 *Commun. ACM* **22** 612
[11] Blakley G R 1979 *Proceedings of AFIPS National Computer Conference* 48 *(New York)* 313
[12] Zhang F, Wang D, Liu K and Liu C 2016 *Int. J. Theor. Phys.* **55** 595
[13] Verma V and Prakash H 2016 *Int. J. Theor. Phys.* **55** 2061
[14] Tian J H, Zhang J Z and Li Y P 2016 *Int. J. Theor. Phys.* **55** 2303
[15] Binayak S C and Arpan D 2016 *Int. J. Theor. Phys.* **55** 3393
[16] Wootton J R and Loss D 2018 *Phys. Rev.* A **97** 052313
[17] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303

[18] Dehkordi M H and Fattahi E 2012 *Sci. China Phys. Mech. Astron.* **55** 1828
[19] Shi R H *et al* 2010 *Opt. Commun.* **283** 2476
[20] Song Y, Li Y and Wang W 2018 *Int. J. Theor. Phys.* **57** 1559
[21] Liu X F 2019 *Int. J. Theor. Phys.* **58** 713
[22] Wang S H, Chong S K and Hwang T 2010 *Opt. Commun.* **283** 4405
[23] Wang T Y, Wen Q Y and Zhu F C 2011 *Opt. Commun.* **284** 1711
[24] Wang W H *et al* 2013 *Int. J. Theor. Phys.* **52** 2099
[25] Lin J and Hwang T 2011 *Opt. Commun.* **284** 1468
[26] Hao L, Li J L and Long G L 2010 *Sci. China Phys.* **53** 491
[27] Hou K, Li Y B and Shi S H 2010 *Opt. Commun.* **283** 1961
[28] Gottesman D 2000 *Phys. Rev.* A **61** 042311
[29] Chau H F 2002 *Phys. Rev.* A **66** 060302
[30] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
[31] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301
[32] Hsu L Y and Li C M 2005 *Phys. Rev.* A **71** 022321
[33] Zhang Z J, Yang J, Man Z X and Li Y 2005 *Eur. Phys. J.* D **33** 133
[34] Zhang Z J 2006 *Opt. Commun.* **261** 199
[35] Han L F, Liu Y M, Liu J and Zhang Z J 2008 *Opt. Commun.* **281** 2690
[36] Xiao L, Wang C, Zhang W, Huang H D, Peng J D and Long G L 2008 *Phys. Rev.* A **77** 042315
[37] Sun Y, Wen Q Y, Gao F, Chen X B and Zhu F C 2009 *Opt. Commun.* **282** 3647
[38] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[39] Hsieh C R, Tasi C W and Hwang T 2010 *Commun. Theor. Phys.* **54** 1019