International Journal of Theoretical Physics (2020) 59:562–573
https://doi.org/10.1007/s10773-019-04349-4

Tripartite Layered Quantum Key Distribution Scheme with a Symmetrical Key Structure

Xiao-Hao Zhang[1] · Xing-Yu Yan[2] · Yun-Qian Wang[2] · Li-Hua Gong[2]

Received: 24 September 2019 / Accepted: 19 November 2019 / Published online: 13 January 2020

Abstract
Asymmetric entanglement could provide a crucial layered key structure for quantum cryptography. A new symmetrical tripartite quantum key distribution scheme based on the simplest layered quantum key distribution (L-QKD) model is devised. With an interesting rotational symmetrical key distribution scheme, the proposed tripartite QKD protocol could establish a more integrated key system, which expands the number of conference keys for secure broadcast and distribute layered secret keys among any legitimate participants simultaneously. The proposed scheme is more flexible, robust and efficient to guarantee the fairness among communication parties than the original L-QKD protocol, and our scheme also could be applied to encryption in the butterfly network precisely. Moreover, based on three asymmetric (4, 4, 2) entangled state, a novel symmetric (4, 4, 4) entangled state to implement L-QKD scheme is discussed. Finally, the security of L-QKD scheme is analyzed via information-theoretic proof.

Keywords Asymmetric entangled state · Layered quantum key distribution · Rotational symmetry · Key structure · Quantum cryptography

1 Introduction

Quantum key distribution (QKD) is the most concerned branch of quantum cryptography [1]. The goal of QKD is to allow authenticated parties to create a random and secure key under the quantum no-cloning theorem [2] or the non-classical properties of entanglement [3]. BB84 protocol [4], Ekert protocol [5] and several variations of these original protocols together with their security, have been widely investigated [6–8].

With the advent of QKD, entanglement has become a crucial resource as quantum information carrier frequently. Thus, substantial entangled states have been widely exploited in conventional entanglement-based QKD protocols [9–11] and quantum networks [12–15].

✉ Li-Hua Gong
lhgong@ncu.edu.cn

[1] Department of Computer Science and Technology, Nanchang University, Nanchang 330031, China

[2] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

However, it is known that the dimension of quantum states plays a vital role on actual key rate, the robustness of such protocols against noise [16–18] and capability of tolerating quantum bit error [19]. Therefore, the generalization or preparation of multi-particle entanglement [20] and high-dimensional entanglement, especially high-dimensional multipartite entanglement becomes topical [21–24].

Surprisingly, multipartite high-dimensional quantum states are readily available in experiment [18]. A particular multipartite high-dimensionally entangled quantum state with multiple particles and high dimensions has been demonstrated experimentally [23]. Such a state has an asymmetric entanglement structure, which is not only significant in increasing the efficiency of quantum communication but also interesting for "layered" key structure. Based on this idea, a novel layered quantum key distribution (L-QKD) was proposed [18], where the asymmetric entangled states provide multiple keys between arbitrary agents simultaneously. However, it is noticed that the original layered key structure is powerless to guarantee the fairness among communication parties, since the particular nature of the asymmetric entanglement structure. To raise a more integrated key system, a new symmetrical tripartite quantum key distribution scheme is devised by adopting a rotational symmetrical layered key structure. Furthermore, the communication network via connections among the source party and agents also have been considered.

The paper is structured as follows: the idea behind the L-QKD protocol with the simplest mode is introduced in Sect. 2. Tripartite layered quantum key distribution scheme with rotational symmetrical key structure is presented in Sect. 3. Additionally, in Sect. 4, the strategy to connect the source party with agents is presented, and a simple application scenario is introduced briefly. A novel scheme via symmetric (4, 4, 4) entangled state to implement L-QKD is discussed in Sect. 5. In addition, the security analysis and a brief comparison with the original L-QKD protocol is arrived at in Sect. 6. Finally, a brief conclusion will be drawn in Sect. 7.

2 Ideal Tripartite L-QKD Protocol

The model for tripartite layered quantum distribution is shown in Fig. 1(a). An authorized Source (S) distributes asymmetric entangled states for three agents, i.e., Alice (A), Bob (B) and Charlie (C). These asymmetric entangled states enable two parties to share an additional layer of secure information and build a conference key among all the three parties. Therefore, agents could share keys in two layers, i.e., K_{ABC} and k_{BC}.

The first L-QKD protocol, as well as the first such an asymmetric (3, 3, 2) entangled state $|\Psi_{332}\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |221\rangle)$, was proposed in [14]. The local dimensions for $|\Psi_{332}\rangle$ are 3 for the first two photons and 2 for the third photon. Since the idealized key rate based on $|\Psi_{332}\rangle$ is not perfect in the first L-QKD protocol, recently, Pivoluska M, et al. proposed a simple motivating tripartite asymmetric (4, 4, 2) entangled state [18]. Such an ideal state $|\Psi_{442}\rangle = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)$ guarantees perfect idealized key rate and beautiful key structure, as shown in Fig. 1(b). Firstly, let us introduce the L-QKD protocol with the asymmetric (4, 4, 2) entangled state briefly.

(a) State preparation: Source S distributes $|\Psi_{442}\rangle$ to three agents A, B and C, as shown in Fig. 1(b).

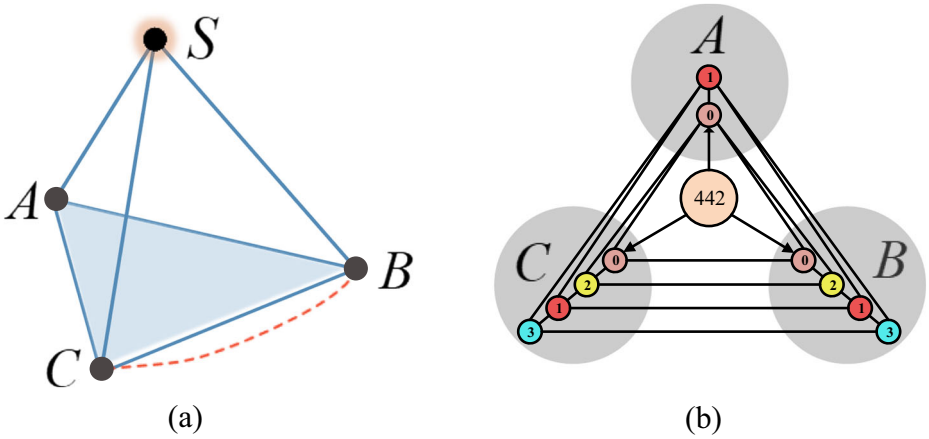

Fig. 1 Tripartite layered quantum key distribution model. **a** In this model, an authorized Source (S) distributes asymmetric entangled states to three agents Alice (A), Bob (B), Charlie (C). Hence, two keys K_{ABC} and k_{BC} could be shared among three agents simultaneously. K_{ABC} (blue area) is a conference key among three agents, while k_{BC} (red dotted line) is a layered secret key only shared between B and C. **b** A novel asymmetric (4, 4, 2) entangled state $|\Psi_{442}\rangle = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)$ shared among three parties. Here the first two photons live in a four-dimensional space, while the third photon lives in a two-dimensional space

$$|\Psi_{442}\rangle_{BCA} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{BCA} \tag{1}$$

where the subscript BCA denotes that the first two particles are assigned to agents B and C, while the third particle is assigned to A.

(b) Measurement: After measuring the state $|\Psi_{442}\rangle_{BCA}$ locally in the computational basis respectively, the outcomes of three agents will exhibit peculiar correlations: the outcomes of B and C (00, 11, 22, and 33) are correlated and independent of the ones of A (0 and 1).

(c) Key generation: Agents B and C could encode bit strings K_{ABC} and k_{BC} according to their outcomes.

$$K_{ABC} = \begin{cases} 1, \text{for outcomes 1 and 3;} \\ 0, \text{for outcomes 0 and 2.} \end{cases}$$

$$k_{BC} = \begin{cases} 1, \text{for outcomes 2 and 3;} \\ 0, \text{for outcomes 0 and 1.} \end{cases}$$

It is known that K_{ABC} is correlated to Alice's measurement outcomes correctly and k_{BC} is independent of Alice's data entirely. On one hand, Alice, Bob and Charlie develop a conference key K_{ABC}, which has interesting secure broadcast applications. On the other hand, Bob and Charlie share a layered secret key k_{BC} that is unknown to Alice.

(d) After parameter estimation and post-processing in raw keys, key strings could be used to encrypt messages among all three agents with one-time pad (OTP). More details can be found in [18].

In the L-QKD protocol, a layered key structure is more efficient in term of the number of quantum channels used. However, it is noticed that the power of the three-party agents to possess key information is unequal. In other words, the original layered key structure is incapable of guaranteeing the fairness among agents. For example, a secret layered key could be built only between Bob and Charlie in the above case, while distributing layered keys between Alice and Bob (Charlie) is not allowed.

To resolve this problem, an improved scheme with rotational symmetrical key structure could be considered.

3 Tripartite L-QKD Scheme with the Rotational Symmetrical Key Structure

To achieve fairness among three agents, first of all, three rounds of asymmetric entangled states are needed, as shown in Fig. 2.

Formally, the authorized Source S produces three asymmetric (4, 4, 2) entangled states, then agents A, B and C share $|\Psi_{442}\rangle$ states as shown in Fig. 2(a)-(c).

$$|\Psi_{442}\rangle_{BCA} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{BCA} \tag{2}$$

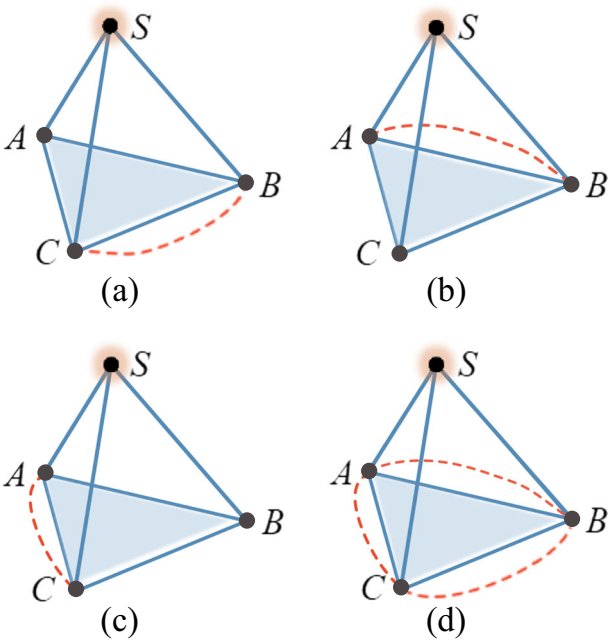

Fig. 2 Tripartite layered key distribution with rotational symmetrical structure. Here, after three rounds distribution shown in (**a-c**), all three parties could share three conference keys $\{K_{ABC}^{R_1}, K_{ABC}^{R_2}, K_{ABC}^{R_3}\}$, at the same time, any two of parties could build a secure channel shared only among themselves equally shown in (**d**)

$$|\Psi_{442}\rangle_{ABC} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{ABC} \tag{3}$$

$$|\Psi_{442}\rangle_{ACB} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{ACB} \tag{4}$$

After processing the necessary L-QKD steps mentioned in Sect. 2, ideally, conference keys could be shared among three agents three times, and bipartite keys between any pairs of agents could be built simultaneously, as shown in Fig. 2(d). Thus, the key system for three agents is obtained, as listed in Table 1.

Therefore, the unfairness among three parties is overcome by using the rotational symmetrical key structure, where any two parties could build a layered secure channel to share bipartite keys only among themselves equally.

4 An Implementation Strategy for Connecting the Source Party with Agents

As is known, it is necessary to connect central source router with agents for building communication network. Therefore, to improve the integrity of system structure, the strategy connecting the source party with agents is presented in our scheme.

Apart from building a layered key structure in three agents as shown in Sect. II, similarly, the layered key structure among source party and agents is constructed, as shown in Fig. 3.

Note that the authorized Source S prepares six-round asymmetric (4, 4, 2) entangled states, and the entangled states are distributed as follows:

$$|\Psi_{442}\rangle_{BCA} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{BCA} \tag{5}$$

$$|\Psi_{442}\rangle_{ABC} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{ABC} \tag{6}$$

$$|\Psi_{442}\rangle_{ACB} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{ACB} \tag{7}$$

Table 1 Layered key system for three agents

Agent	Key
Alice	$\{K_{ABC}^{R_1}, K_{ABC}^{R_2}, K_{ABC}^{R_3}, k_{AB}, k_{AC}\}$
Bob	$\{K_{ABC}^{R_1}, K_{ABC}^{R_2}, K_{ABC}^{R_3}, k_{AB}, k_{BC}\}$
Charlie	$\{K_{ABC}^{R_1}, K_{ABC}^{R_2}, K_{ABC}^{R_3}, k_{AC}, k_{BC}\}$

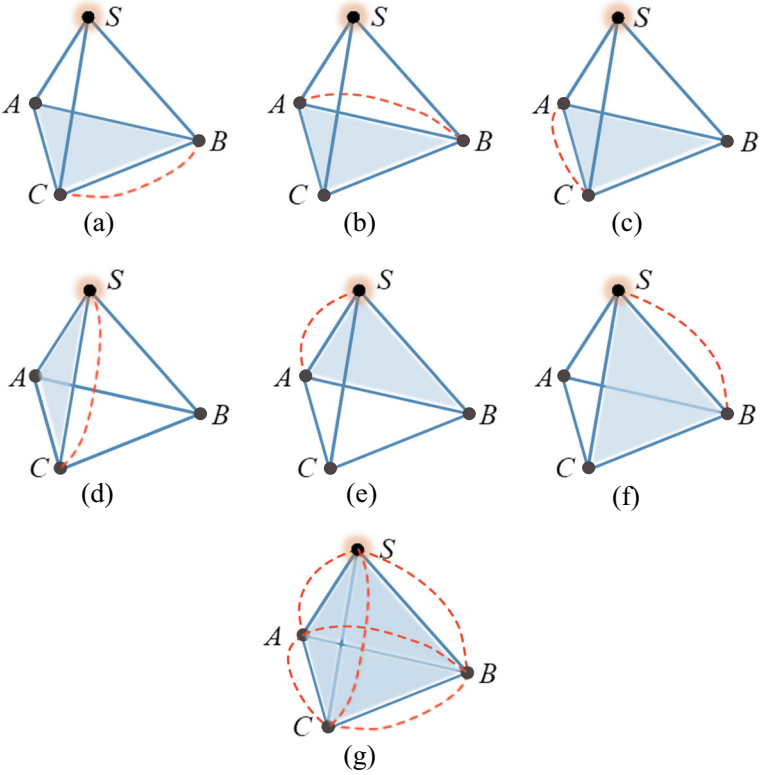

Fig. 3 An improved symmetrical tripartite layered key distribution. The final scheme (g) consists of six-level layered key structures (**a**-**f**)

$$|\Psi_{442}\rangle_{SCA} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{SCA} \tag{8}$$

$$|\Psi_{442}\rangle_{SAB} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{SAB} \tag{9}$$

$$|\Psi_{442}\rangle_{SBC} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{SBC} \tag{10}$$

Likewise, after necessary L-QKD steps performed, a greater key system could be obtained, as shown in Table 2.

Conference keys for any tripartite have been shared, as well as layered secret keys for any bipartite. Thus key system grows more extensive and more integrated, which could enrich our symmetrical L-QKD scheme more flexible and more robust. Furthermore, this layered key system with central source could implement a quantum communication network. As an ideal application, our scheme will be discussed in the butterfly network [25–27] briefly.

Table 2 The greater layered key system involving the source party

Party	Key
Alice	$\{K_{ABC}^{R_1}, K_{ABC}^{R_2}, K_{ABC}^{R_3}, k_{AB}, k_{AC}, K_{SAC}, K_{SAB}, k_{SA}\}$
Bob	$\{K_{ABC}^{R_1}, K_{ABC}^{R_2}, K_{ABC}^{R_3}, k_{AB}, k_{BC}, K_{SAB}, K_{SBC}, k_{SB}\}$
Charlie	$\{K_{ABC}^{R_1}, K_{ABC}^{R_2}, K_{ABC}^{R_3}, k_{AC}, k_{BC}, K_{SAC}, K_{SBC}, k_{SC}\}$
Source	$\{K_{SAC}, K_{SAB}, K_{SBC}, k_{SA}, k_{SB}, k_{SC}\}$

Suppose Alice wants to send bits a and b to both Bob and Charlie. The classical case can be shown in Fig. 4(a). To ensure the security of bits a and b, an alternative encryption structure with asymmetric entangled states could be designed, as shown in Fig. 4(b).

Firstly, the Source produces two asymmetric (4, 4, 2) entangled states for AC and AB, respectively, i.e., $|\Psi_{442}\rangle_{ACS} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{ACS}$ and $|\Psi_{442}\rangle_{ABS} = \frac{1}{2}(|000\rangle + |111\rangle + |220\rangle + |331\rangle)_{ABS}$. As mentioned, the conference key K_{ACS} could be shared among Alice, Charlie and Source, so could K_{ABS}. Furthermore, the layered secret keys k_{AB} and k_{AC} could be distributed simultaneously. Hence, Alice possesses $\{K_{ACS}, K_{ABS}, k_{AB}, k_{AC}\}$, Bob and Charlie hold $\{K_{ABS}, k_{AB}\}$ and $\{K_{ACS}, k_{AC}\}$, respectively.

Encryption: Alice encrypts bits a and b via bitwise XOR operation with her keys, i.e., $a \oplus k_{AC}$, $(a \oplus b) \oplus K_{ACS}$, $b \oplus k_{AB}$ and $(a \oplus b) \oplus K_{ABS}$. Then Alice transmits the encrypted messages $a \oplus k_{AC}$ and $(a \oplus b) \oplus K_{ACS}$ to Charlie, while sends messages $b \oplus k_{AB}$ and $(a \oplus b) \oplus K_{ABS}$ to Bob.

Decryption: After receiving encoded messages, Charlie and Bob decrypt the bits with their keys respectively. i.e., Charlie computes $k_{AC} \oplus (a \oplus k_{AC})$ and $K_{ACS} \oplus ((a \oplus b) \oplus K_{ACS})$, while Bob operates $k_{AB} \oplus (b \oplus k_{AB})$ and $K_{ABS} \oplus ((a \oplus b) \oplus K_{ABS})$.

Therefore Charlie obtains bits a and $a \oplus b$, while Bob obtains bits b and $a \oplus b$. Performing simple XOR operation on their outcomes, i.e., $a \oplus (a \oplus b) \rightarrow b$ and $b \oplus (a \oplus b) \rightarrow a$, both Bob and Charlie could receive bits a and b finally.

It is known that the security is guaranteed by the layered key structure and one-time pad encryption algorithm, even if the source is under the control of eavesdropper, only the result of $a \oplus b$ could be leaked.

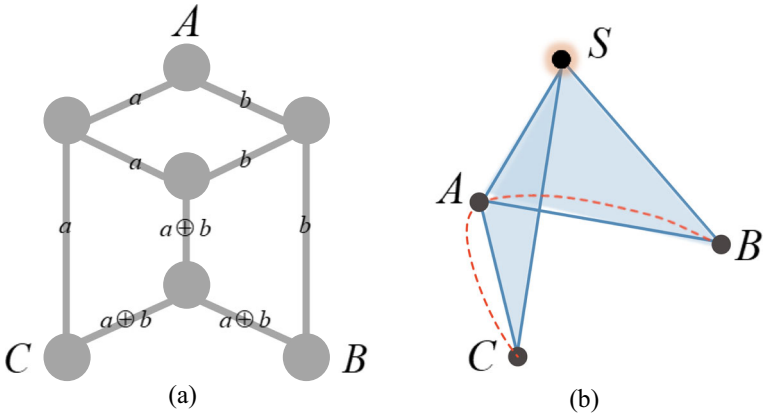

Fig. 4 The butterfly network. In the classical case, Alice wants to send bits a and b to both Bob and Charlie by employing the linear network code given by the transmitted symbols written onto the channels ($\oplus$ means XOR) [6]. **a** Classical linear network. **b** An encryption structure with asymmetric entangled states

5 A Symmetric L-QKD Scheme Via Symmetric (4, 4, 4) Entangled State

Apart from the above, another scheme to achieve fairness among three agents is discussed below. Based on three asymmetric (4, 4, 2) entangled state$|\Psi_{442}\rangle$, a novel symmetric (4, 4, 4) entangled state $|\Psi_{444}\rangle$ is considered for our protocol.

$$\begin{aligned}|\Psi_{444}\rangle_{ABC} &= \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle + |220\rangle + |331\rangle + |202\rangle + |313\rangle + |022\rangle + |133\rangle)_{ABC} \\ &= \frac{1}{2\sqrt{2}}\Big[|0\rangle_A\otimes(|00\rangle + |22\rangle)_{BC} + |1\rangle_A\otimes(|11\rangle + |33\rangle)_{BC} + \\ &\qquad |2\rangle_A\otimes(|20\rangle + |02\rangle)_{BC} + |3\rangle_A\otimes(|31\rangle + |13\rangle)_{BC}\Big] \\ &= \frac{1}{2\sqrt{2}}\Big[|0\rangle_B\otimes(|00\rangle + |22\rangle)_{AC} + |1\rangle_B\otimes(|11\rangle + |33\rangle)_{AC} + \\ &\qquad |2\rangle_B\otimes(|20\rangle + |02\rangle)_{AC} + |3\rangle_B\otimes(|31\rangle + |13\rangle)_{AC}\Big] \\ &= \frac{1}{2\sqrt{2}}\Big[|0\rangle_C\otimes(|00\rangle + |22\rangle)_{AB} + |1\rangle_C\otimes(|11\rangle + |33\rangle)_{AB} + \\ &\qquad |2\rangle_C\otimes(|20\rangle + |02\rangle)_{AB} + |3\rangle_C\otimes(|31\rangle + |13\rangle)_{AB}\Big]\end{aligned} \tag{11}$$

It is noted any individual agent could distribute the layered keys to others by the partially entangled states $|0\rangle_{A/B/C}\otimes(|00\rangle+|22\rangle)_{BC/AC/AB}$ and $|1\rangle_{A/B/C}\otimes(|11\rangle+|33\rangle)_{BC/AC/AB}$, which is equal to the asymmetric (4, 4, 2) entangled state. Besides, the rest of entangled states $|2\rangle_{A/B/C}\otimes(|20\rangle+|02\rangle)_{BC/AC/AB}$ and $|3\rangle_{A/B/C}\otimes(|31\rangle+|13\rangle)_{BC/AC/AB}$ also could be of benefit to build conference keys. The implementation of the scheme is described briefly below.

Similarly, three agents A, B and C share N three symmetric (4, 4, 4) entangled states $|\Psi_{444}\rangle_{ABC}^{\otimes N}$. After performing measurements on the states in order, each of the eight possible combinations 000, 111, 220, 331, 202, 313, 022, 133 is distributed uniformly. Then three agents label the N outcomes with 0, 1, 2 and 3 individually.

Suppose they intend to achieve L-QKD scheme shown in Fig. 2(a), i.e., A, B and C share K_{ABC} while B and C share k_{BC} secretly. In this case, firstly agent A only announces the labeled number of outcomes 0 and 1 publicly, then B and C picks up corresponding labeled particles from A's announcement, according to the correlation of $|\Psi_{444}\rangle$ and the key generation in Sect. 2, three agents could implement the L-QKD scheme. Furthermore, the remaining unselected particles, could also be applied to generate conference key string K_{ABC}.

$$K_{ABC} = \begin{cases} 1, \text{for outcomes 1 and 3;} \\ 0, \text{for outcomes 0 and 2.} \end{cases}$$

where K_{ABC} is correlated to agent's measurement outcomes correctly. Similarly, after parameter estimation and post-processing in raw keys, key strings could be used to encrypt messages among all three agents with one-time pad (OTP). Moreover, it is easy to achieve fairness among three agents, for example, if agents desire to implement the scheme shown in Fig. 2(c), only few steps need to be changed, where B firstly announces the labeled number of outcomes 0 and 1 in his hand publicly, then A and C select the same marked particles to build the layered key structure.

It is noted that since only half outcomes of N entangled states $|\Psi_{444}\rangle$ could contribute to L-QKD scheme, the implementation results of a three symmetric (4, 4, 4) entangled states in the idealized key rates are $R_{K_{ABC}} = 1$ and $R_{k_{AB}/k_{BC}/k_{AC}} = 1/2$.

6 Security Analysis and Comparison

As stated above, the proposed symmetrical tripartite quantum key distribution scheme is based on the L-QKD model (see Fig. 1). Therefore, the primary issue is the security of the L-QKD protocol, wherein the asymmetric (4, 4, 2) entangled state $|\Psi_{442}\rangle_{i,j,u}$, $i, j, u \in \{A, B, C\}$, is a crucial process.

It is known that $|\Psi_{442}\rangle_{i,j,u}$ guarantees the key strings $K_{i,j,u}$ and $k_{i,j}$ independently, i.e., $I(K_{i,j,u}; k_{i,j}) = 0$, and the idealized key rate of the L-QKD protocol could achieve 100%, which is better than the conventional EPR- and GHZ- QKD protocols. Here, by employing the composable security definition in [6], we principally discuss the security of the key under the most general eavesdropping attack, i.e., coherent attack [28].

Suppose that the agents i, j and u share N asymmetric (4, 4, 2) entangled states. The eavesdropper E is given to hold a purification of the global state. After performing respective computational measurement of three agents, the total quantum state is expressed by the density operator,

$$\rho^{N}_{K_i k_i, K_j k_j, K_u, E} = \sum_{M_i, M_j, M_u} P_{K_i k_i, K_j k_j, K_u, E}(M_i, M_j, M_u) |M_i\rangle\langle M_i| \otimes |M_j\rangle\langle M_j| \otimes |M_u\rangle\langle M_u| \otimes \rho_E^{M_i, M_j, M_u} \tag{12}$$

where the strings of measurement outcomes M_i, M_j and M_u of agents i, j and u, which occur with probability $P_{K_i k_i, K_j k_j, K_u, E}(M_i, M_j, M_u)$, are stored in key systems $K_i k_i$, $K_j k_j$ and K_u, respectively.

Similar to the classical post-processing in the bipartite scheme, in the error correction step, agent u pre-processes the random key string K_u according to the channel $V \leftarrow K_u$ and sends classical error correction information W (W is same as three agents) to i and j, who calculate their individual guesses V_i and V_j for V from K_i, K_j and W. Moreover, in the privacy amplification step, agent u randomly chooses hash function h, computes his key $S_u = h(V)$ and announces the description of h, then i and j also perform $S_i = h(V_i)$ and $S_j = h(V_j)$. Therefore, the total quantum state could be described as $\rho_{S_i S_j S_u E^{\varepsilon}}$. As is known from [6], the key system (S_i, S_j, S_u) is called ε-secure, if it is ε-close to the ideal state, i.e., $\mathrm{tr}\left|\rho_{S_i S_j S_u E^{\varepsilon}} - \rho_{SSS} \otimes \rho_{E^{\varepsilon}}\right| \leq 2\varepsilon$.

According to [29], the length $\varsigma^{(N)}_{K_{i,j,u}}$ of the conference key $K_{i,j,u}$ generated from N asymmetric (4, 4, 2) entangled states will then be denoted as

$$\zeta^{(N)}_{K_{i,j,u}} = \sup_{V \leftarrow K_u} \left[S_2^{\varepsilon}(VE) - S_0^{\varepsilon}(E) - \max_{i,j} H_0^{\varepsilon}(V|K_{i,j}) \right] \tag{13}$$

where $V \leftarrow K_u$ denotes a bitwise preprocessing channel on raw key bit K_u of agent u, $S_{\alpha}^{\varepsilon}(\rho)$ is a smooth Rényi entropy, and the last term $\max_{i,j} H_0^{\varepsilon}(V|K_{i,j})$ denotes the maximal leakage to eavesdropper in the error correction step.

Without considering parameter estimation step, for the limit $N \to \infty$, the secret fraction $r^{\infty}_{K_{i,j,u}}$ is given by

$$r^{\infty}_{K_{i,j,u}} = \lim_{N\to\infty} \zeta^{(N)}_{K_{i,j,u}}/N = \sup_{V\leftarrow K_u} \inf_{\sigma_{i,j,u}\in\Gamma} \left[S(V|E) - \max_{i,j} H\left(V|K_{i,j}\right) \right] \tag{14}$$

where $S(V|E)$ is the conditional Von-Neumann entropy of the key variable, E denotes the system state of eavesdropper, $H(V|K_{i,j})$ is the conditional Shannon entropy, which denotes agents i and j's guess of K_u, and Γ is the set of all density matrices $\sigma_{i,j,u}$ of all agents, which are consistent with the parameter estimation.

It is easy to access the length $\zeta^{(N)}_{k_{i,j}}$ of the layer secret key $k_{i,j}$ and the secret fraction $r^{\infty}_{k_{i,j}}$ between i and j, which are given by

$$\zeta^{(N)}_{k_{i,j}} = \sup_{U\leftarrow k_i} \left[S^{\varepsilon}_2(UE) - S^{\varepsilon}_0(E) - \max H^{\varepsilon}_0\left(U|k_j\right) \right] \tag{15}$$

$$r^{\infty}_{k_{i,j}} = \sup_{U\leftarrow k_i} \inf_{\sigma_{i,j}\in\Lambda} \left[S(U|E) - \max H\left(U|k_j\right) \right] \tag{16}$$

Likewise, $U \leftarrow k_i$ denotes a bitwise preprocessing channel on agent i's raw key bit k_i, $H(U|k_j)$ denotes agents j's guess of k_i, and Λ is the set of all density matrices $\sigma_{i,j}$ of agents i and j.

Finally, the conference secret key rate and the layer secret key rate are $R = r^{\infty}_{K_{i,j,u}}/t_{\text{rep}}$ and $R = r^{\infty}_{k_{i,j}}/t_{\text{rep}}$, respectively. Note that t_{rep} is the repetition time when one round protocol takes, generally we assume that $t_{\text{rep}} = 1$.

Additionally, to immune to the intercept-and-resend attack, extra techniques such as decoy state technique [30–34] could be used. In a practical implementation of the proposed scheme, the participants can also use of the methods given in [35, 36] to avoid the Trojan horse attack and in-visible-photon attack. The necessary post-processing, such as the parameter estimation results, error correction and privacy amplification, is inevitably involved.

With respect to the original L-QKD protocol, our rotational symmetrical L-QKD scheme has a more integrated key system, where one could perform authentication to resist dishonest participant attacks via the secure bipartite channel (i.e., k_{SA}, k_{SB}, k_{SC}, k_{AB}, k_{AC}, k_{BC}). Besides, our scheme enhances the capacity of the original layered key system by consuming more high-dimensional entangled states.

Herein, a brief comparison for the proposed protocols with the original L-QKD protocol is described.

For the rotational symmetrical L-QKD scheme in Sect. 3, a more integrated key system in a three-party case is established. Different from the original case, it exploits three rounds entanglement distribution to expand the type of keys from 2 (K_{iju}, k_{ij}) to 4 (K_{iju}, k_{ij}, k_{iu}, k_{ju}), and all idealized key rates are 100% similarly. More importantly, this scheme is immune to the participant attack via the fairness key structure among three parties.

Moreover, for the symmetric L-QKD scheme in Sect. 5, the layered key structure could be accomplished by half outcomes by utilizing symmetric (4, 4, 4) entangled states. Compared with the original protocol, the fairness among three agents could be achieved. The idealized key rates are $R_{K_{iju}} = 1$, $R_{k_{ij}/k_{iu}/k_{ju}} = 1/2$. It should be pointed out that the tripartite layered key distribution with rotational symmetrical structure is an application of the original L-QKD protocol, but it enhances the quality of the final key system.

7 Conclusion

A new symmetrical quantum key distribution scheme for three parties based on layered key structure is proposed. To raise a more integrated key system and guarantee the fairness among communication parties, an interesting rotational symmetrical key structure is generalized. Moreover, the strategy to implement a quantum communication network via the layered key system with a central source is presented, which could be employed to encrypt information in the butterfly network correctly. Furthermore, according to the three asymmetric (4, 4, 2) entangled states, a novel symmetric (4, 4, 4) entangled state is discussed for our L-QKD scheme. It is easy to achieve fairness among three agents via a different method. Finally, the security of our scheme via information-theoretic proof is analyzed.

In summary, our scheme expands the number of conference keys for secure broadcast and distributes the bipartite keys for any two participants. Such high dimension entangled states could be used for many cryptographic tasks. Furthermore, the idea of layered key structure could be extended to other quantum information fields, such as semi-quantum key agreement [37], quantum group authentication [38], quantum-information splitting [39], continuous-variable quantum key distribution [39], quantum networks communication, and so forth.

Acknowledgements The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that help improve the quality of this manuscript. This work is supported by the National Natural Science Foundation of China (Grant Nos. 61871205 and 61561033), the China Scholarship Council (Grant No. 201606825042), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011), and the Natural Science Foundation of Jiangxi Province (Grant No. 20171BAB202002).

References

1. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002)
2. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature. **299**, 802 (1982)
3. Coffman, V., Kundu, J., Wootters, W.K.: Distributed entanglement. Phys. Rev. A. **61**, 052306 (2000)
4. Bennett, C. H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers. Systems and Signal Processing. Bangalore, India, 175–179 (1984)
5. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991)
6. Epping, M., Kampermann, H., Bruß, D.: Multi-partite entanglement can speed up quantum key distribution in networks. New J. Phys. **19**, 093012 (2017)
7. Scarani, V., Bechmann, P.H., Cerf, N.J.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301 (2009)
8. Mayers, D.: Unconditional security in quantum cryptography. J. ACM. **48**, 351 (2001)
9. Greenberger, D.M., Horne, M.A., Shimony, A., Zeilinger, A.: Bell's theorem without inequalities. Am. J. Phys. **58**, 1131 (1990)
10. Schön, C., Solano, E., Verstraete, F.: Sequential generation of entangled multiqubit states. Phys. Rev. Lett. **95**, 110503 (2005)
11. Huang, P., Huang, J., Zhang, Zeng, G.H.: Quantum key distribution using basis encoding of Gaussian-modulated coherent states. Phys. Rev. A. **97**, 042311 (2018)
12. Acín, A., Cirac, J.I., Lewenstein, M.: Entanglement percolation in quantum networks. Nat. Phys. **3**, 256 (2007)
13. Luo, M.X.: Computationally efficient nonlinear bell inequalities for quantum networks. Phys. Rev. Lett. **120**, 140402 (2018)
14. Yang, Y., Yang, J., Zhou, Y., Shi, W., Chen, X.: Quantum network communication: a discrete-time quantum-walk approach. Science China Inf. Sci. **61**, 042501 (2018)

15. Leung, D., Oppenheim, J., Winter, A.: Quantum network communication—the butterfly and beyond. IEEE Trans. Inf. Theory. **56**, 3478 (2010)
16. Bechmann, P.H., Tittel, W.: Quantum cryptography using larger alphabets. Phys. Rev. A. **61**, 062308 (2000)
17. Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Security of quantum key distribution using *d*-level systems. Phys. Rev. Lett. **88**, 127902 (2002)
18. Pivoluska, M., Huber, M., Malik, M.: Layered quantum key distribution. Phys. Rev. A. **97**, 032312 (2018)
19. Wang, X.B.: Quantum key distribution with two-qubit quantum codes. Phys. Rev. Lett. **92**, 077902 (2004)
20. Xiu, X.M., Li, Q.Y., Lin, Y.F., Dong, H.K., Dong, L., Gao, Y.J.: Preparation of four-photon polarization-entangled decoherence-free states employing weak cross-Kerr nonlinearities. Phys. Rev. A. **94**, 042321 (2016)
21. Erhard, M., Malik, M., Krenn, M., Zeilinger, A.: Experimental GHZ entanglement beyond qubits. arXiv. 1708, 03881 (2017)
22. Hiesmayr, B.C., De Dood, M.J.A., Löffler, W.: Observation of four-photon orbital angular momentum entanglement. Phys. Rev. Lett. **116**, 073601 (2016)
23. Malik, M., Erhard, M., Huber, M.: Multi-photon entanglement in high dimensions. Nat. Photonics. **10**, 248 (2016)
24. Huber, M., de Vicente, J.I.: Structure of multidimensional entanglement in multipartite systems. Phys. Rev. Lett. **110**, 030501 (2013)
25. Ahlswede, R., Cai, N., Li, S.Y., Yeung, R.W.: Network information flow. IEEE Trans. Inf. Theory. **46**, 1204 (2000)
26. Epping, M., Kampermann, H., Bruss, D.: Robust entanglement distribution via quantum network coding. New J. Phys. **18**, 103052 (2016)
27. Li, D., Gao, F., Qin, S., Wen, Q.: Perfect quantum multiple-unicast network coding protocol. Quantum Inf. Process. **17**, 13 (2018)
28. Bechmann-Pasquinucci, H., Gisin, N.: Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. Phys. Rev. A. **59**, 4238 (1999)
29. Renner, R., Gisin, N., Kraus, B.: Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A. **72**, 012332 (2005)
30. Li, C.Y., Zhou, H.Y., Wang, Y.: Secure quantum key distribution network with bell states and local unitary operations. Chin. Phys. Lett. **22**, 1049 (2005)
31. Lo, H.K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)
32. Lucamarini, M., Patel, K.A., Dynes, J.F.: Efficient decoy-state quantum key distribution with quantified security. Opt. Express. **21**, 24550 (2013)
33. Xiu, X.M., Dong, L., Gao, Y.J.: Secure four-site distribution and quantum communication of $\chi-$ type entangled states. Opt. Commun. **284**, 2065–2069 (2011)
34. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A. **74**, 054302 (2006)
35. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A. **351**, 23–25 (2006)
36. Zhou, N.R., Zhu, K.N., Zou, X.F.: Multi-party semi-quantum key distribution protocol with four-particle cluster state. Ann. Phys. **531**, 1970031 (2019)
37. Liao, L., Peng, X., Shi, J., Guo, Y.: Graph state-based quantum group authentication scheme. J. Phys. Soc. Jpn. **86**, 024403 (2017)
38. Wang, X.W., Xia, L.X., Wang, Z.Y., Zhang, D.Y.: Hierarchical quantum-information splitting. Opt. Commun. **283**, 1196–1199 (2010)
39. Chai, G., Cao, Z.W., Liu, W.Q., Wang, S.Y., Huang, P., Zeng, G.H.: Parameter estimation of atmospheric continuous-variable quantum key distribution. Phys. Rev. A. **99**, 032326 (2019)