New semi-quantum key agreement protocol based on high-dimensional single-particle states

Huan-Huan Li(李欢欢), Li-Hua Gong(龚黎华), Nan-Run Zhou(周南润)

Citation: Chin. Phys. B . 2020, 29(11): 110304 . **doi:** 10.1088/1674-1056/abaedd
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Coherent attacks on a practical quantum oblivious transfer protocol

Guang-Ping He(何广平)

Chin. Phys. B . 2018, 27(10): 100308 . **doi:** 10.1088/1674-1056/27/10/100308

Two-step quantum secure direct communication scheme with frequency coding

Xue-Liang Zhao(赵学亮), Jun-Lin Li(李俊林), Peng-Hao Niu(牛鹏皓), Hong-Yang Ma(马鸿洋), Dong Ruan(阮东)

Chin. Phys. B . 2017, 26(3): 030302 . **doi:** 10.1088/1674-1056/26/3/030302

Probabilistic direct counterfactual quantum communication

Sheng Zhang(张盛)

Chin. Phys. B . 2017, 26(2): 020304 . **doi:** 10.1088/1674-1056/26/2/020304

Anonymous voting for multi-dimensional CV quantum system

Rong-Hua Shi(施荣华), Yi Xiao(肖伊), Jin-Jing Shi(石金晶), Ying Guo(郭迎), Moon-Ho Lee

Chin. Phys. B . 2016, 25(6): 060301 . **doi:** 10.1088/1674-1056/25/6/060301

Controlled mutual quantum entity authentication using entanglement swapping

Min-Sung Kang, Chang-Ho Hong, Jino Heo, Jong-In Lim, Hyung-Jin Yang

Chin. Phys. B . 2015, 24(9): 090306 . **doi:** 10.1088/1674-1056/24/9/090306

New semi-quantum key agreement protocol based on high-dimensional single-particle states*

Huan-Huan Li(李欢欢), Li-Hua Gong(龚黎华), and Nan-Run Zhou(周南润)†

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, *China*

(Received 14 July 2020; revised manuscript received 5 August 2020; accepted manuscript online 13 August 2020)

A new efficient two-party semi-quantum key agreement protocol is proposed with high-dimensional single-particle states. Different from the previous semi-quantum key agreement protocols based on the two-level quantum system, the propounded protocol makes use of the advantage of the high-dimensional quantum system, which possesses higher efficiency and better robustness against eavesdropping. Besides, the protocol allows the classical participant to encode the secret key with qudit shifting operations without involving any quantum measurement abilities. The designed semi-quantum key agreement protocol could resist both participant attacks and outsider attacks. Meanwhile, the conjoint analysis of security and efficiency provides an appropriate choice for reference on the dimension of single-particle states and the number of decoy states.

Keywords: semi-quantum key agreement protocol, high-dimensional quantum state, quantum cryptography, quantum communication

PACS: 03.67.Dd, 03.67.Hk, 03.67.Ac **DOI:** 10.1088/1674-1056/abaedd

1. Introduction

Quantum cryptography has made tremendous progress in the past few decades, because of the pioneering work of Bennett and Brassard[1] in exploring the applications of quantum mechanics for cryptography. Quantum key agreement (QKA), as an important ingredient of quantum cryptography, has been extensively researched in recent years. QKA protocol allows the legal participants to negotiate a shared secret key fairly in a quantum way. In other words, the final shared secret key is determined by all participants together and cannot be controlled by any non-trivial subset of the participants. In 2004, Zhou *et al.*[2] introduced the first QKA protocol with quantum teleportation. Fairness of QKA protocol then was taken into account to defeat the malicious participants. In 2010, Chong and Hwang[3] investigated a two-party QKA protocol similar to BB84 protocol, which combines unitary operations with the delayed measurement technique. In 2011, Chong *et al.*[4] proposed an enhanced quantum key agreement protocol with Bell states by requiring a participant to verify the received quantum states. However, the above-mentioned QKA protocols only involved two parties and could not be extended to the multi-party situation. Shi and Zhong[5] first devised a multi-party QKA protocol based on Bell measurements and entanglement swapping of Bell states. Unfortunately, Liu *et al.*[6] discovered that this multi-party QKA protocol is susceptible to the participant attacks and investigated a new multiparty QKA protocol with single particles. Subsequently, Sun *et al.*[7] utilized two additional quantum unitary operations to enhance the efficiency based on Liu *et al.*'s protocol. Hereafter, a number of QKA protocols have been put forward based on different quantum entangled states, including Bell state,[8,9] GHZ state,[10,11] cluster state,[12–14] brown state,[15] *etc*. Liu *et al.*[16] first suggested the classification concept of multi-party QKA protocols and propounded the collusive attack scheme for the circle-type multi-party QKA protocols. Wang *et al.*[17] put forward a method to withstand the collusive attack and designed a secure multi-party QKA protocol based on the circle model.

Nevertheless, the participants in the aforementioned protocols all possess complete quantum ability implying expensive quantum facilities and resources. It is difficult for each participant to afford the valuable quantum devices. To cope with this problem, the pioneering semi-quantum concept was creatively introduced by Boyer *et al.*[18] Hereafter, the concept could be also absorbed into many related research fields, including quantum key distribution,[19–21] quantum secure direct communication,[22,23] quantum secret sharing,[24] quantum identification,[25] quantum private comparison,[26] and so on. The quantum key agreement protocol also adopts this creative concept to reduce the quantum abilities of participants. Liu *et al.*[27] propounded a semi-quantum key agreement (SQKA) protocol with delegating quantum computation based on the client-server model. Subsequently, Shukla *et al.*[28] presented an SQKA protocol based on orthogonal-state rather than conjugate coding. Yan *et al.*[29] researched two SQKA protocols with Bell states based on the measure-reflect model, where a semi-honest third party is involved to assist two classical participants to generate a final secret key. Zhou *et al.*[30] explored a three-party SQKA protocol with the en-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61871205 and 61561033) and the Major Academic Discipline and Technical Leader of Jiangxi Province, China (Grant No. 20162BCB22011).

†Corresponding author. E-mail: nrzhou@ncu.edu.cn

tanglement properties of four-particle cluster states.

However, the above-mentioned QKA or SQKA protocols only involve the two-level quantum system. Moreover, most of SQKA protocols require the classical parties to perform measurement operation in the classical basis $\{|0\rangle, |1\rangle\}$ and their key agreement efficiency is not high enough. The quantum states in the high-dimensional form are named qudits. The high-dimensional quantum system has been investigated in both theoretical researches and practical applications. For instance, high-dimensional photonic degrees of freedom have been researched in various ways, including transverse spatial state,[31] orbital angular momentum,[32–34] time-bins,[35–37] *etc*. Furthermore, the high-dimensional quantum system could provide a higher information capacity and better robustness against eavesdropping than the two-level quantum system during the communication process.[38–40] Hence, it is worthwhile to explore an SQKA protocol based on these excellent properties of the high-dimensional quantum system.

In this paper, a new efficient two-party SQKA protocol is designed based on d-dimensional single-particle states. Quantum measurement ability is unnecessary for the classical participant in the proposed protocol. The classical participant needs to encode the secret key by performing the qudit shifting operation. Furthermore, the basic operations which include the reflection operation and the permutation operation are required for the classical participant. The security of the proposed SQKA protocol is analyzed for both participant attacks and outsider attacks in the ideal quantum channel. Moreover, the presented protocol provides an appropriate choice to balance the security and the efficiency of QKA or SQKA protocols based on the high-dimensional quantum states.

The rest of this paper is organized as follows. In Section 2, the high-dimensional single-particle states and basic notations are introduced. In Section 3, the detailed description of the proposed two-party SQKA protocol is given. In Section 4, the security of the protocol is discussed. In Section 5, a brief comparison among some typical SQKA protocols and our protocol is performed. Finally, a short conclusion is reached.

2. Preliminaries

To better understand the SQKA protocol based on the high-dimensional situation, some basic concepts and notations are introduced below.

2.1. Mutually unbiased bases and quantum Fourier transform

Similar to the two-dimensional quantum system, the Z-basis for a d-dimensional quantum system could be expressed as

$$B_1 = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}. \tag{1}$$

The X-basis could be also denoted as

$$B_2 = \{|t_1\rangle, |t_2\rangle, \ldots, |t_{d-1}\rangle\}, \tag{2}$$

$$|t_k\rangle = F|k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jk} |j\rangle, \quad k = 0, 1, \ldots, d-1, \tag{3}$$

where the symbol F denotes the discrete quantum Fourier transform[41] described as

$$|k\rangle \xrightarrow{F} \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jk} |j\rangle, \tag{4}$$

where $\omega = e^{2\pi i/d}$. Correspondingly, the symbol F^{-1} represents the quantum inverse Fourier transform expressed as

$$|k\rangle \xrightarrow{F^{-1}} \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-jk} |j\rangle. \tag{5}$$

The two bases B_1 and B_2 constitute the mutually unbiased bases.

2.2. Qudit shifting operation

The qudit shifting operation is defined as

$$U_s = \sum_{j=0}^{d-1} |j \oplus s\rangle \langle j|, \quad s = 0, 1, \ldots, d-1, \tag{6}$$

where the symbol $\oplus$ represents the addition modulo d. It could be deduced that the two single-particle states $|k\rangle$ and $|t_k\rangle$ which are performed the qudit shifting operations will be converted into the states $|k+s\rangle$ and $\omega^{-sk}|t_k\rangle$ respectively according to Theorem 1 in Ref. [42]. In addition, the qudit shifting operations to encode the secret key could be considered as a kind of classical ability.[43]

3. SQKA protocol with high-dimensional single particle states

Suppose that two participants, namely Alice and Bob, prepare their respective random $N\log_2 d$ bits secret key sequences K_A and K_B in advance,

$$K_A = \{k_A^1, k_A^2, \ldots, k_A^N\}, \tag{7}$$

$$K_B = \{k_B^1, k_B^2, \ldots, k_B^N\}, \tag{8}$$

where $k_A^i, k_B^i \in \{0, 1, \ldots, d-1\}$. The two participants intend to negotiate a final secret key K_F, *i.e*.,

$$K_F = K_A \oplus K_B = \{k_A^1 \oplus k_B^1, k_A^2 \oplus k_B^2, \ldots, k_A^N \oplus k_B^N\}. \tag{9}$$

The specific description of the presented two-party SQKA protocol is as follows.

Step 1 Quantum state preparation and distribution

Alice prepares N d-dimensional single-particle states randomly chosen from B_1-basis to construct sequence S_A. Simultaneously, she generates $2N$ decoy states randomly chosen

from the mutually unbiased bases B_1 and B_2 and randomly inserts them into sequence S_A to constitute a new sequence S_A^*. Subsequently, Alice distributes sequence S_A^* to Bob. To detect whether the invisible photons and the illegitimate multiphoton signals are inserted by Eve in the transmitted sequences, Alice and Bob need to install quantum wavelength filters and photon number splitters before all related quantum devices.

Step 2 Eavesdropping detection

After Bob confirms that he has received sequence S_A^*, Alice and Bob start the first eavesdropping check. Alice first publishes the location information of decoy states through the classical authenticated channel. Then, Bob randomly chooses to reflect half of the decoy states in sequence S_A^*. After Alice confirms that she has received these single-particle states, Bob announces the corresponding location information of these decoy states via the classical authenticated channel. Subsequently, Alice measures these single-particle states with the information published by Bob and obtains the corresponding measurement results. To check whether Eve performs attacks on the transmitted particles or not, Alice and Bob need to calculate the error rate by comparing the measurement results with the initial states of the decoy particles. If the error rate is below the preset threshold, the next step will be executed. Otherwise, the protocol will be terminated.

Step 3 Encoding operation

Bob could obtain a new sequence S_B after sending those decoy states involved in the first round of eavesdropping detection. He could perform the qudit shifting operations to encode his secret key K_B. Since Alice discloses the position information of the rest of decoy states in sequence S_B via the classical authenticated channel in step 2, Bob only implements the encoding operations on those single-particle states which do not include the remaining decoy states in sequence S_B to obtain a new sequence S_B^*. If k_B^i is equal to s, Bob performs the qudit shifting operation U_s on the i-th particle in sequence S_B. Besides, he selects a permutation operator $\prod_{2N}^{B}$ to rearrange sequence S_B^* to acquire a new sequence $S_B^{*\prime}$. Subsequently, Bob sends sequence $S_B^{*\prime}$ to Alice. Similarly, two participants implement the second round of eavesdropping check after Alice confirms the receipt of sequence $S_B^{*\prime}$. If the transmission channel is insecure, the protocol will be aborted. Otherwise, they will proceed to the next step.

Step 4 Generation of the final secret key

Alice first declares the secret key sequence K_A with the classical authenticated channel. Subsequently, she discards the decoy particles and performs B_1-basis measurements on sequence $S_B^{*\prime}$. The measurement results of sequence $S_B^{*\prime}$ are encoded as the corresponding sequence M_B. The corresponding encoding rule is shown in Table 1. Then Bob announces the random permutation operator $\prod_N^B$ about the remaining single-particle states. From Alice's perspective, she could obtain Bob's secret key by comparing the initial states of the prepared particles with the corresponding measurement results. Hence, the final secret key K_F is shared between Alice and Bob.

Table 1. Encoding rule.

Measurement result	Encoding result
$\|0\rangle$	0
$\|1\rangle$	1
⋮	⋮
$\|d-1\rangle$	$d-1$

4. Security analysis

When the security of the proposed two-party SQKA protocol is analyzed, outsider attacks and participant attacks should be taken into account in general.

4.1. Outsider attacks

The confidentiality of the final shared secret key K_F is insusceptible to the disclosure of Alice's raw secret key K_A. Even if Eve acquires sequence K_A, she is unable to acquire the final shared secret key. Since the corresponding qudit shifting operations are unknown to her, she could not obtain Bob's secret key K_B. Thus, Eve has to implement some attack strategies to extract information about these operations as much as possible. When the particles are transmitted between Alice and Bob in the ideal quantum channel, some common attack strategies may be adopted, including the intercept-resend attack, the measure-resend attack, the entangle-measure attack, and the Trojan horse attacks.

4.1.1. Intercept-resend attack

The intercept-resend attack means that Eve intercepts the transmitted sequences sent by Alice and prepares the corresponding fake sequences to Bob. The presented protocol prepares enough d-dimensional single-particle states which are chosen randomly from the two kinds of mutually unbiased bases. Meanwhile, the decoy states are randomly inserted in each transmitted qudit sequence. Thus, Eve does not know the locations and the measurement bases of the decoy states in sequences S_A^* and $S_B^{*\prime}$. Besides, she does not perform any measurement operations on the intercepted particles before each eavesdropping check. Eve could only guess the states of particles to prepare the corresponding fake sequences. It could be deduced that the probability of detected eavesdropping for the intercept-resend attack could be calculated as

$$P = 1 - [P(C)P(S|C) + P(M)P(S|M)]^q, \tag{10}$$

where $P(C)$, $P(M)$, $P(S|C)$, $P(S|M)$ and q denote the probability of choosing the correct measurement basis, the probability of choosing the mismatched measurement basis, the two corresponding conditional probabilities of passing eavesdropping detection, and the number of decoy particles during each

eavesdropping detection stage, respectively. Since Eve does not know any information about the measurement basis, she could only guess the correct basis or the mismatched measurement basis of each decoy particle prepared by Alice with the same probability of 0.5. Similarly, the two corresponding conditional probabilities of passing eavesdropping detection are equivalent and equal to d^{-1} since no measurement operations should be executed. Eve could pass the eavesdropping detection with the probability of d^{-1} for each decoy particle which is inserted into the transmitted qudit sequence. Therefore, the intercept-resend attack will be detected with the probability of $1-d^{-q}$. When the number of decoy particles is large enough, the intercept-resend attack will inevitably be detected. Therefore, Eve could not successfully perform the intercept-resend attack to obtain the shared secret key without being detected.

4.1.2. Measure-resend attack

Similar to the security analysis on the intercept-resend attack, Eve also does not know the relevant information about the decoy states in sequences S_{A}^{*} and $S_{\mathrm{B}}^{*\prime}$. The difference between these two attack strategies is that Eve could perform measurement operations to obtain some measurement results in the measure-resend attack. If Eve selects the mismatched measurement basis to measure a decoy particle, the eavesdropping action is undetected with the probability of d^{-1}. If Eve chooses the correct measurement basis, she will pass the eavesdropping check. The probability of passing the eavesdropping check is $\frac{1}{2}\left(1+d^{-1}\right)$ when a decoy particle is inserted into the transmitted qudit sequence. Thus, the eavesdropping detection could find this kind of attack with the probability of $1-[(d+1/2d)]^{q}$ according to Eq. (10).

The relationship among the detection probability, the dimension of single-particle states, and the number of decoy states is shown in Fig. 1. When the dimension of single-particle decoy states remains unchanged, the probability of detecting eavesdropping quickly approximates to 1 with the increasing number of decoy states. While for the fixed number of decoy particles, the probability of detecting eavesdropping approaches 1 at a relatively slow speed as the dimension of decoy states increases. Once one could choose the number of decoy states and the dimension of single-particle states appropriately, it is obvious that the propounded SQKA protocol could resist the measure-resend attack well. If q is large enough, it is manifest that the probability of the detected measure-resend attack will approximate to 1. Nevertheless, the efficiency of the protocol will inevitably decrease as the number of decoy state particles increases. For the high-dimensional single-particle states, it could furnish better robustness of a quantum communication system against eavesdropping than that of the two-dimensional single-particle states. It is not necessary to insert a great amount of decoy states to ensure the security of the protocol, since one can balance between the security and the complexity in preparation of the high-dimensional single-particle states. For instance, the probability of detecting eavesdropping approaches 1 when q and d are equal to 30 and 4, respectively.

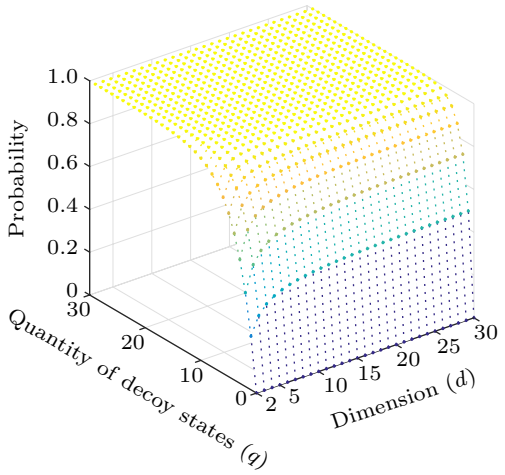

Fig. 1. Probability of detected eavesdropping.

4.1.3. Entangle-measure attack

If Eve desires to execute the entangle-measure attack, she needs to implement the entanglement operations U on the prepared ancillary particles in state $|E\rangle$ and the target particles transmitted between Alice and Bob. Since the proposed protocol is a two-way communication protocol, Eve performs the entanglement operations U_{T} and U_{R} on those particles of back and forth transmission between Alice and Bob, respectively. Besides, she conducts suitable measurements on the ancillary particles to deduce the related information about the shared secret key when the protocol is completed. At different phases of the protocol, she could intercept and perform the entanglement operations on two types of particles which belong to the two mutually unbiased bases, including B_1-basis and B_2-basis. Nevertheless, since Eve is unaware of the position information of the decoy photons, she will implement the same entanglement operations on all transmitted particles before each eavesdropping detection stage. For the proposed protocol, the entangle-measure attack could be analyzed from the following process.

In Step 1, after executing the entanglement operation U_{T} on the particles sent from Alice to Bob, Eve resends the particles to Bob immediately. The relationship between those d-dimensional single-particle states from the two mutually unbiased bases and the ancillary particles is

$$U_{\mathrm{T}}|k\rangle|E\rangle = \sum_{j=0}^{d-1}\lambda_{kj}|j\rangle\left|e_{kj}\right\rangle, \tag{11}$$

$$\begin{aligned} U_{\mathrm{T}}|t_k\rangle|E\rangle &= U_{\mathrm{T}}\left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{jk}|j\rangle\right)|E\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{jk}U_{\mathrm{T}}|j\rangle|E\rangle, \end{aligned} \tag{12}$$

where $k \in \{0,1,\ldots,d-1\}$ and $|e_{kj}\rangle$ is a pure state uniquely determined by U_{T} and the coefficients satisfy the conditions such that $\sum_{j=0}^{d-1} |\lambda_{kj}|^2 = 1$. According to the inverse quantum Fourier transform as shown in Eq. (5), equation (12) could be equivalently rewritten as

$$\begin{aligned} U_{\mathrm{T}}|t_k\rangle|E\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{jk}\sum_{r=0}^{d-1}\lambda_{jr}\left(\frac{1}{\sqrt{d}}\sum_{m=0}^{d-1}\omega^{-mr}|t_m\rangle\right)|e_{jr}\rangle \\ &= \frac{1}{d}\sum_{j=0}^{d-1}\sum_{r=0}^{d-1}\sum_{m=0}^{d-1}\omega^{jk-mr}\lambda_{jr}|t_m\rangle|e_{jr}\rangle. \end{aligned} \tag{13}$$

Similarly, Eve also implements the entanglement operation U_{R} on the particles transmitted from Bob to Alice. Note that Bob executes his encoding operation U_{s} before sending sequence $S_{\mathrm{B}}^{*\prime}$. The relationship between those d-dimensional single-particle states and the ancillary particles is expressed as

$$\begin{aligned} U_{\mathrm{R}}U_{\mathrm{s}}U_{\mathrm{T}}|k\rangle|E\rangle &= U_{\mathrm{R}}\left(\sum_{j=0}^{d-1}\lambda_{kj}|j\oplus s\rangle|e_{kj}\rangle\right) \\ &= \sum_{j=0}^{d-1}\mu_{kj}U_{\mathrm{s}}|j\rangle|\varepsilon_{kj}\rangle, \end{aligned} \tag{14}$$

$$U_{\mathrm{R}}U_{\mathrm{s}}U_{\mathrm{T}}|t_k\rangle|E\rangle = U_{\mathrm{R}}U_{\mathrm{s}}U_{\mathrm{T}}\left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{jk}|j\rangle\right)|E\rangle. \tag{15}$$

According to Eqs. (11)–(13) and the above-mentioned related properties of qudit shifting operations in Section 2, equation (15) can be rewritten as

$$\begin{aligned} &U_{\mathrm{R}}U_{\mathrm{s}}U_{\mathrm{T}}|t_k\rangle|E\rangle \\ &= \frac{1}{d}\sum_{j=0}^{d-1}\sum_{r=0}^{d-1}\sum_{m=0}^{d-1}\omega^{jk-mr}\lambda_{jr}U_{\mathrm{R}}U_{\mathrm{s}}|t_m\rangle|e_{jr}\rangle \\ &= \frac{1}{d}\sum_{j=0}^{d-1}\sum_{r=0}^{d-1}\sum_{m=0}^{d-1}\omega^{jk-mr-sm}\lambda_{jr}U_{\mathrm{R}}|t_m\rangle|e_{jr}\rangle \\ &= \frac{1}{d}\left[|t_0\rangle\left(\sum_{j,r=0}^{d-1}\mu_{jr}\omega^{jk}|\varepsilon_{jr}\rangle\right)\right. \\ &\quad + |t_1\rangle\left(\sum_{j,r=0}^{d-1}\mu_{jr}\omega^{jk-(r+s)}|\varepsilon_{jr}\rangle\right) \\ &\quad + |t_2\rangle\left(\sum_{j,r=0}^{d-1}\mu_{jr}\omega^{jk-2(r+s)}|\varepsilon_{jr}\rangle\right)+\cdots \\ &\quad \left.+ |t_{d-1}\rangle\left(\sum_{j,r=0}^{d-1}\mu_{jr}\omega^{jk-(d-1)(r+s)}|\varepsilon_{jr}\rangle\right)\right]. \end{aligned} \tag{16}$$

If Eve attempts to pass the eavesdropping detection stages in Steps 2 and 3, the states of these particles belonging to B_1-basis should remain unchanged after Eve implements the entanglement operations U_{T} and U_{R}. Thus equation (14) should satisfy the conditions such that $\mu_{kj} = 0$ if $j \neq k$ and $j \in \{0,1,\ldots,d-1\}$; otherwise, $\mu_{kk} \neq 0$. That is to say, equations (14) and (16) can be equivalently simplified as

$$\begin{aligned} U_{\mathrm{R}}U_{\mathrm{s}}U_{\mathrm{T}}|k\rangle|E\rangle &= U_{\mathrm{R}}\left(\sum_{j=0}^{d-1}\lambda_{kj}|j\oplus s\rangle|e_{kj}\rangle\right) \\ &= \mu_{kk}U_{\mathrm{s}}|k\rangle|\varepsilon_{kk}\rangle, \end{aligned} \tag{17}$$

$$U_{\mathrm{R}}U_{\mathrm{s}}U_{\mathrm{T}}|t_k\rangle|E\rangle = \frac{1}{d}\sum_{j=0}^{d-1}\sum_{m=0}^{d-1}\omega^{j(k-m)-ms}\mu_{jj}|t_m\rangle|\varepsilon_{jj}\rangle, \tag{18}$$

where $\sum_{j=0}^{d-1}|\mu_{jj}|^2 = 1$ and s denotes the corresponding secret key value for Bob's qudit shifting operations. Likewise, those single-particle states belonging to B_2-basis also should remain unchanged. Hence, if $m \neq k$ and $m \in \{0,1,\ldots,d-1\}$, equation (18) should satisfy the condition

$$\sum_{j=0}^{d-1}\omega^{j(k-m)-ms}\mu_{jj}|\varepsilon_{jj}\rangle = 0. \tag{19}$$

The condition can be equivalent to

$$\sum_{j=0}^{d-1}\omega^{j(k-m)}\mu_{jj}|\varepsilon_{jj}\rangle = 0, \tag{20}$$

where $m \neq k$, $\omega = \mathrm{e}^{2\pi\mathrm{i}/d}$ and $\sum_{j=0}^{d-1}\omega^{j(k-m)} = 0$. It could be deduced that those ancillary particles entangled with the single-particle states transmitted between Alice and Bob should satisfy the following condition:

$$\mu_{00}|\varepsilon_{00}\rangle = \mu_{11}|\varepsilon_{11}\rangle = \cdots = \mu_{d-1,d-1}|\varepsilon_{d-1,d-1}\rangle. \tag{21}$$

It is observed that the final states of auxiliary particles in $|E\rangle$ are independent of the transmitted single-particle states. Thus, Eve cannot derive useful information about the measurement results of sequences S_{A}^{*} and $S_{\mathrm{B}}^{*\prime}$ by measuring her ancillary particles. Even if two participants publish sequence K_{A} and the permutation operator $\prod_N^{\mathrm{B}}$, it is obvious that Eve does not know the information about the final shared secret keys. On the contrary, if the entanglement operations do not meet the above condition as shown in Eq. (21), the entangle-measure attack will disturb the single-particle states and leave some traces that could be detected. In conclusion, if Eve tries to implement the entangle-measure attack, it is either being detected or unable for Eve to obtain secret key information. Therefore, the protocol can resist the entangle-measure attack.

4.1.4. Trojan horse attacks

Since the proposed semi-quantum key agreement protocol is a two-way communication protocol, it is susceptible to Trojan horse attacks, including the invisible photon attack, the delayed photon attack, and so on. The invisible photon attack means that Eve could produce the fake single particles whose wavelengths are close to the legitimate ones and insert these fake particles into the transmitted sequence. Besides, Eve could also prepare the multiphoton signals to replace the

original single-photon ones to perform the delayed photon attack. It is difficult for common detectors to distinguish between these fake photons or delayed photons and legitimate ones. Bob will inevitably perform the same operation on those illegitimate photons. After Bob performing the encoding operation and sending sequence $S_B^{*\prime}$ to Alice, Eve could intercept the sequence and separate the fake photons and the delayed photons. Then, Eve resends the remaining legitimate particles to Alice without any interference. In this way, she could obtain the information about Bob's secret key with the corresponding measurements. Hence, Alice and Bob must equip quantum wavelength filters and photon number splitters to resist the two kinds of Trojan horse attacks.[44–46]

4.2. Participant attacks

It is important for quantum key agreement protocols to satisfy the fairness condition, which guarantees each participant to make the same contribution for the shared secret key. Since the participants could possess more information than outsider eavesdroppers, this kind of attack is stronger than the outside attack on QKA protocols. Hence, the attacks of malicious participants need to be taken into consideration. The so-called participant attacks mean that the malicious participants in the QKA protocol attempt to control the final agreement key independently without being detected. The presented protocol is a two-party protocol, so the two situations need to be considered for two malicious participants.

Assume that Alice is a malicious participant and she attempts to control the final shared secret key independently without being detected. In this case, she needs to crack the secret key of Bob before sending her secret key information. Nevertheless, before publishing the permutation operator $\prod_N^B$ to Alice, Bob receives Alice's secret key K_A. Therefore, the malicious participant Alice could not successfully perform the participant attack. If Bob is a malicious participant, it is similar to the case of malicious participant Alice. Only after Bob sends sequence $S_B^{*\prime}$ containing the information of his secret key sequence K_B to Alice, could he acquire the raw secret key sequence K_A. It could be deduced that Bob cannot control the final shared key independently either. Hence, the proposed protocol could resist malicious participant attacks.

5. Comparison

To compare with other SQKA protocols based on the two-dimensional quantum states, the efficiency of the proposed SQKA protocol based on d-dimensional quantum states could be calculated similarly to the qubit efficiency.[47] Furthermore, since one qudit could carry $\log_2 d$ bits of classical secret key information, the final shared secret key needs to be converted into binary bits to calculate the efficiency. The efficiency of the presented protocol could be calculated as $\eta = c/(q_d + b)$, where c, b, and q_d denote the numbers of shared classical secret key bits, classical bits exchanged except for eavesdropping check, and d-dimensional quantum single-particle states, respectively. Throughout the implementation of the protocol, Alice requires to prepare $3N$ high-dimensional single-particle states (including $2N$ decoy states) and publishes her sequence K_A ($N\log_2 d$ bits) containing secret key information in all. Furthermore, Bob also needs to declare his permutation operator $\prod_N^B$ (N bits). Therefore, the efficiency of our protocol is $\log_2 d/(4+\log_2 d)$, where d denotes the dimension of single-particle states and is greater than 2 for the high-dimensional case.

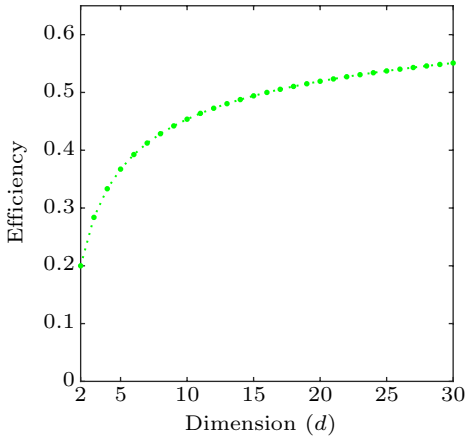

Fig. 2. Relationship between efficiency and dimension.

Since the efficiency η is a monotonically increasing function of d, it is obviously greater than 20% for the proposed protocol based on high-dimensional single-particle states, as shown in Fig. 2. It could be observed that the efficiency will slowly approximate to 100% as the dimension of single-particle states increases. For example, even if d is equal to a million,[31] the efficiency of the proposed protocol just reaches 83%. Moreover, the preparation and measurement of high-dimensional single-particle states will become more difficult with the increase of dimension. However, the efficiency approaches 50% at a relatively high speed when the dimension of decoy states ranges from 2 to 16. Assuming the dimension of single-particle states is 4, the efficiency of the proposed protocol could reach 33%. Under the condition of ensuring the efficiency and the security of the protocol, it is important to select the appropriate size of the dimension and the number of decoy state particles to achieve a proper balance. If the number of decoy states is fixed at 30, it is evident that the efficiency will enhance rapidly with the increasing proportion of the encoded single-particle states in all transmitted particles. As mentioned above in the security analysis on the measure-resend attack, the proposed semi-quantum key agreement protocol could obtain acceptable efficiency and high-level security when q and d are equal to 30 and 4, respectively.

The brief comparison results among several representative QKA or SQKA protocols and the presented protocol are

shown in Table 2. The comparison mainly focuses on three aspects, including quantum resources and channel, the necessary abilities of the classical participant and quantum participant, and the efficiency. Since the quantum ability is required for all participants of the QKA protocol based on single photons,[3] there is no classical participant in the protocol. It could be observed that the propounded protocol demands weaker quantum ability and possesses higher efficiency in comparison with the QKA protocol based on single photons. It is necessary for the classical participants in the SQKA protocols based on Bell states not only to prepare and measure the qubits in the classical basis $\{|0\rangle, |1\rangle\}$ but also to perform permutation operations and reflect qubits without disturbance.[28,29] Different from these SQKA protocols based on Bell states, the classical party of the designed protocol doesn't need the preparation and measurement abilities of single-particle states. Comparing with the SQKA protocol based on cluster states,[30] the proposed protocol just needs simpler quantum operations and quantum resources involving single photons rather than the entangled photons. Furthermore, the presented semi-quantum key agreement protocol requires fewer quantum channels compared with the two SQKA protocols based on Bell states and cluster states, respectively.[29,30] In conclusion, the proposed two-party semi-quantum key agreement protocol possesses higher efficiency and requires relatively fewer quantum resources or weaker quantum ability among several representative QKA and SQKA protocols.

Table 2. Comparisons of some typical protocols and our protocol.

	QR	QC	QPNQO	CPNO	Efficiency/%
Ref. [3]	single photon	1	SPUO + SPM	None	16.67
Ref. [28]	Bell state	2	SPUO + BM	CBM + PO + RO + PP	9.09
Ref. [29]	Bell state	4	SPM + BM	CBM + PO + RO	6.7
Ref. [30]	cluster state	4	SPM + BM + FPOM	CBM + RO + PP	2.08
Ours	single photon	3	SPM	QSO + PO + RO	$\frac{100\log_2 d}{4+\log_2 d}$

QR (quantum resource), QC (quantum channel), BM (Bell measurement), PP (particles preparation), QPNQO (quantum participant necessary quantum operation), SPM (single-particle measurement), CPNO (classical participant necessary operation), SPUO (single-particle unitary operation), FPOM (four-particle orthogonal measurement), CBM (classical basis measurement), PO (permutation operation), RO (reflection operation), and QSO (qudit shifting operation).

6. Conclusion

Based on the properties of high-dimensional single-particle states, an efficient two-party semi-quantum key agreement protocol is introduced. The decoy state method guarantees the security of the particle transmission. The security analysis shows that the presented quantum key agreement protocol possesses good performance in resisting both outsider attacks and participant attacks. Furthermore, the classical basis measurement ability of the classical party is unnecessary for the proposed semi-quantum key agreement protocol. Since the high-dimensional single-particle states have the large information capacity and the high sensibility to different types of attacks, if one selects the appropriate size of the dimension and the number of decoy state particles, the proposed protocol could obtain acceptable efficiency and enough security. The designed semi-quantum key agreement protocol enhances the efficiency and reduces the consumption of quantum resources. Meanwhile, the difficulty in preparing high-dimensional single-particle states increases gradually with the increase of dimension. Nevertheless, the ability to prepare high-dimensional single-particle states is just required for the quantum participant rather than the classical one for the propounded protocol. Therefore, the proposed protocol is feasible with the development of the related quantum facilities and techniques.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, December 10–12, 1984, Bangalore, India, p. 175
[2] Zhou N, Zeng G and Xiong J 2004 *Electron. Lett.* **40** 1149
[3] Chong S K and Hwang T 2010 *Opt. Commun.* **283** 11923
[4] Chong S K, Tsai C W and Hwang T 2011 *Int. J. Theor. Phys.* **50** 1793
[5] Shi R H and Zhong H 2013 *Quantum Inf. Process.* **12** 921
[6] Liu B, Gao F, Huang W and Wen Q Y 2013 *Quantum Inf. Process.* **12** 1797
[7] Sun Z, Zhang C, Wang B, Li Q and Long D 2013 *Quantum Inf. Process.* **12** 3411
[8] Shukla C, Alam N and Pathak A 2014 *Quantum Inf. Process.* **13** 2391
[9] Huang W, Wen Q Y, Liu B, Gao F and Sun Y 2014 *Quantum Inf. Process.* **12** 649
[10] Xu G B, Wen Q Y, Gao F and Qin S J 2014 *Quantum Inf. Process.* **13** 2587
[11] He Y F and Ma W P 2016 *Quantum Inf. Process.* **14** 1650007
[12] Shen D S, Ma W P and Wang L L 2014 *Quantum Inf. Process.* **13** 2313
[13] Yang Y G, Li B R, Kang S Y, Chen X B, Zhou Y H and Shi W M 2019 *Quantum Inf. Process.* **18** 77
[14] Liu H N, Liang X Q, Jiang D H, Xu G B and Zheng W M 2013 *Quantum Inf. Process.* **18** 242
[15] Cai T, Jiang M and Cao G 2018 *Quantum Inf. Process.* **17** 103
[16] Liu B, Xiao D, Jia H Y and Liu R Z 2016 *Quantum Inf. Process.* **15** 2113
[17] Wang P, Sun Z W and Sun X Q 2017 *Quantum Inf. Process.* **16** 170
[18] Boyer M, Kenigsberg D and Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[19] Guo Y, Su Y, Zhou J, Zhang L and Huang D 2019 *Chin. Phys. B* **28** 010305

[20] Zhou N R, Zhu K N and Zou X F 2019 *Ann. Phys.* **531** 1800520
[21] He R S, Jiang M S, Wang Y, Gan Y H, Zhou C and Bao W S 2019 *Chin. Phys. B* **28** 040303
[22] Yang L, Ma H Y, Zheng C, Ding X L, Gao J C and Long G L 2017 *Acta Phys. Sin.* **66** 230303 (in Chinese)
[23] Luo Y P and Hwang T 2018 *Quantum Inf. Process.* **15** 947
[24] Xiang Y, Liu J, Bai M Q, Yang X and Mo Z W 2019 *Int. J. Theor. Phys.* **58** 2883
[25] Zhou N R, Zhu K N, Bi W and Gong L H 2019 *Quantum Inf. Process.* **18** 197
[26] Jiang L Z 2020 *Quantum Inf. Process.* **19** 180
[27] Liu W J, Chen Z Y, Ji S, Wang H B and Zhang J 2017 *Int. J. Theor. Phys.* **56** 3164
[28] Shukla C, Thapliyal K and Pathak A 2017 *Quantum Inf. Process.* **16** 295
[29] Yan L L, Zhang S B, Chang Y, Sheng Z W and Sun Y H 2019 *Quantum Inf. Process.* **58** 3852
[30] Zhou N R, Zhu K N and Wang Y Q 2020 *Int. J. Theor. Phys.* **59** 663
[31] Shi Z, Mirhosseini M, Margiewicz J, Malik M, Rivera F, Zhu Z and Boyd R W 2013 *Optica* **12** 3411
[32] Molina-Terriza G, Vaziri A, Rehacek J, Hradil Z and Zeilinger A 2004 *Phys. Rev. A* **92** 167903
[33] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lutkenhaus N and Forbes A 2013 *Phys. Rev. A* **88** 032305
[34] De Oliveira M, Nape I, Pinnell J, TabeBordbar N and Forbes A 2020 *Phys. Rev. A* **101** 042303
[35] Nunn J, Wright L J, Soller C, Zhang L, Walmsley I A and Smith B J 2013 *Opt. Express* **21** 15959
[36] Tang G Z, Sun S H, Chen H, Li C Y and Liang L M 2016 *Chin. Phys. Lett.* **33** 120301
[37] Niu M Y, Xu F, Shapiro J H and Furrer F 2016 *Phys. Rev. A* **94** 052323
[38] Wang J, Yang J Y, Fazal I M, Ahmed N, Yan Y, Huang H and Willner A E 2012 *Nat. Photon.* **6** 488
[39] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[40] Bradler K, Mirhosseini M, Fickler R, Broadbent A and Boyd R 2016 *New J. Phys.* **18** 073030
[41] Yan X Y, Zhou N R, Gong L H, Wang Y Q and Wen X J 2013 *Quantum Inf. Process.* **18** 271
[42] Ye C Q and Ye T Y 2019 *Int. J. Theor. Phys.* **58** 1282
[43] Nie Y Y, Li Y H and Wang Z S 2013 *Quantum Inf. Process.* **12** 437
[44] Cai Q Y 2006 *Phys. Lett. A* **351** 23
[45] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev. A* **74** 054302
[46] Yang Y G, Sun S J and Zhao Q Q 2015 *Quantum Inf. Process.* **14** 681
[47] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635