Quantum Inf Process (2014) 13:649–663
DOI 10.1007/s11128-013-0680-z

Quantum key agreement with EPR pairs and single-particle measurements

Wei Huang · Qiao-Yan Wen · Bin Liu · Fei Gao · Ying Sun

Received: 18 January 2013 / Accepted: 31 October 2013 / Published online: 17 November 2013
© Springer Science+Business Media New York 2013

Abstract In this paper, we present a QKA protocol with the block transmission of EPR pairs. There are several advantages in this protocol. First, this protocol can guarantee both the fairness and security of the shared key. Second, this protocol has a high qubit efficiency since there is no need to consume any quantum state except the ones used for establishing the shared key and detecting eavesdropping. In addition, this protocol uses EPR pairs as the quantum information carriers and further utilizes single-particle measurements as the main operations. Therefore, it is more feasible than the protocols that need to perform Bell measurements. Especially, we also introduce a method for sharing EPR pairs between two participants over collective-dephasing channel and collective-rotation channel, respectively. This method is meaningful since sharing EPR pairs between two participants is an important work in many quantum cryptographic protocols, especially in the protocols over non-ideal channels. By utilizing this method, the QKA protocols, which are based on EPR pairs, can be immune to these kinds of collective noise.

Keywords Quantum key agreement · EPR pairs · Block transmission · Single-particle measurements · Collective noise

W. Huang (✉) · Q.-Y. Wen · B. Liu · F. Gao
State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: huangwei096505@aliyun.com

W. Huang
The State Key Laboratory of Integrated Services Networks, Xidian University, Xian 710071, China

Y. Sun
Beijing Electronic Science and Technology Institute, Beijing 100070, China

1 Introduction

Key distribution (KD) and key agreement (KA) are two similar cryptographic primitives which allow participants to share a common secret key via insecure channel. Different from KD, in which only one participant decides the private key and then distributes it to the other ones, each party in a KA protocol should contribute its part to the shared key. Hence, in a KA protocol, the generated key cannot be determined by any non-trivial subset of the participants. Compared with KD, KA is obviously of higher security requirements. In addition to have the ability of preventing the external attackers from stealing the key as KD protocols, KA protocols should also have the ability of resisting participant attack, i.e., dishonest participant(s) tries to determine the key alone, which is not required in KD.

It is known that the security of most classical cryptosystems (e.g., classical key agreement) must be based on the assumption of computation complexity. However, with the rapid development of quantum algorithms and quantum computer, classical cryptosystems face more and more austere challenges [1,2]. In order to solve this problem, people start to research new cryptographic technology, such as quantum cryptography [3]. Quantum cryptography, whose security is assured by the quantum mechanics principles rather than the assumption of computation complexity, has become a hot spot in cryptography. There are many hot research points in quantum cryptography, such as quantum key distribution (QKD) [4–9], quantum secret direct communication (QSDC) [10–16], deterministic secure quantum communication (DSQC) [17–20], quantum secret sharing (QSS) [21–25], quantum private comparison (QPC) [26–28] and quantum signature(QS) [29–31].

Quantum key agreement (QKA) [32–36] is an important branch of quantum cryptography, which utilizes quantum mechanics to guarantee the security of KD protocols. Different from the security of the classical key agreement which might be susceptible to the strong ability of quantum computation, the security of QKA is simply based on the laws of physics (such as quantum no-cloning theorem and Heisenberg uncertainty principle). Therefore, QKA can resist the threat from an attacker with the ability of quantum computation. In 2004, Zhou et al. [32] presented the first QKA protocol with maximally entangled states. However, Chong et al. [33] pointed out that Zhou et al.'s protocol is susceptible to the participant attack and they also improved it. In 2011, Chong et al. proposed a QKA protocol based on the famous BB84 protocol [4,34]. In 2012, Shi et al. [35] proposed a new QKA protocol based on EPR pairs and entanglement swapping. Recently, Liu et al. [36] presented a multiparty QKA protocol with single particles.

In this paper, we propose a QKA protocol with EPR pairs and single-particle measurements. The EPR pairs in our protocol should be transmitted with the technique of block transmission, which has been proposed firstly by Long et al. [10]. Block transmission is an important method for transmitting quantum states in quantum information processing, which has been utilized in many quantum cryptographic protocols [10–20,28,43]. In block transmission, the quantum information carriers are ordered and transmitted in blocks, and the eavesdropping detection is also completed on the blocks. Our protocol has the following merits. First, this protocol can guarantee both the fairness and security of the shared key. Second, in addition to the EPR pairs utilized to establish the shared key, there is no need to consume any extra pairs except the ones used for detecting eavesdropping. Therefore, the intrinsic efficiency for qubits of this protocol is high. In addition, the proposed protocol makes use of EPR pairs as the information carriers and further utilizes single-particle measurements as the main operations. Hence, our protocol has advantages in implementation over the protocol which utilizes Bell measurements [35]. Considering that all the previous QKA protocols [32–36] have been designed in ideal channel, we further present a method for sharing EPR pairs between two participants over two kinds of collective-noise channels. By utilizing this method, the QKA protocols (both the protocols presented in this paper and in [35]), which are based on EPR pairs, can be executed in these kinds of collective-noise channels.

The rest of this paper is arranged as follows. In Sect. 2, we present our QKA protocol by using EPR pairs and single-particle measurements. In Sect. 3, we prove that the proposed protocol is secure against both outside attacks and participant attacks. In Sect. 4, the method for sharing EPR pairs between two participants over two kinds of collective-noise channels is presented, and finally we give a short conclusion in Sect. 5.

2 The proposed QKA protocol based on EPR pair block and single-particle measurements

In this section, we introduce our QKA protocol, in which two participants, say Alice and Bob, can share a common secret key with EPR pair block and single-particle measurements. The steps of this protocol can be described as follows (see also Fig. 1).

(1) Alice prepares n EPR pairs in state

$$\begin{aligned} |\phi^+\rangle_{A_iB_i} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_iB_i} \\ &= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)_{A_iB_i}, \end{aligned} \tag{1}$$

where $i = 1, 2, \ldots, n$. $|0\rangle$ and $|1\rangle$ are the up and down eigenstates of σ_z, $|+\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{2}(|0\rangle - |1\rangle)$ are the up and down eigenstates of σ_x. Then she divides these particles into two sequences: $[A_1, A_2, \ldots, A_n]$ (denoted as S_A) and $[B_1, B_2, \ldots, B_n]$ (denoted as S_B).

(2) For checking eavesdropping, Alice generates m decoy particles, which are randomly in one of the four states: $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. Then she randomly inserts them into the sequence S_B and sends the new sequence (denoted as S'_B) to Bob.

(3) After confirming that Bob has received the sequence S'_B, Alice announces the positions and the initial states of the decoy particles. Then for each of the decoy particles, Bob measures it in the corresponding basis and compares the measurement outcome with its initial state to check eavesdropping. If there exists no error, Alice and Bob continue to the next step; otherwise, they abort this protocol and restart from step (1).

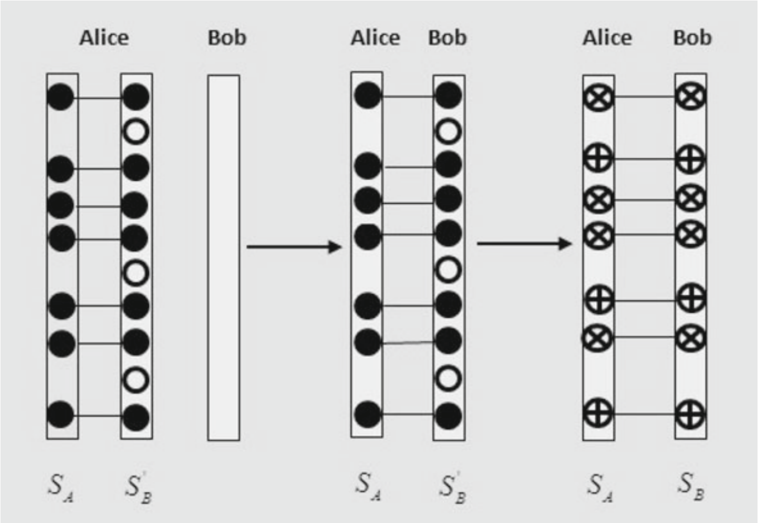

Fig. 1 Illustration of the proposed QKA protocol with EPR pairs. Alice prepares a sequence of ordered EPR pairs in $|\phi^+\rangle$ and divides them into two partner–particle sequences. She first sends the sequence, which is inserted with decoy particles, to Bob. If the transmission of S_B is secure, they measure the particles of their sharing EPR pairs in σ_x-basis or σ_z-basis according to Bob's announced binary string. Here, $\oplus$ and $\otimes$ means measuring the particle in σ_x-basis and σ_z-basis, respectively

(4) Bob announces a binary string (denoted as C) of length n. If the i-th bit in C is 0 (1), i.e., $C_i = 0$ (1), Alice and Bob measure A_i and B_i in basis $\sigma_z = \{|0\rangle, |1\rangle\}$ ($\sigma_x = \{|+\rangle, |-\rangle\}$), respectively. And if the measurement result is $|0\rangle$ or $|+\rangle$ ($|1\rangle$ or $|-\rangle$), they get the key bit 0 (1).

By utilizing the above protocol, two participants (Alice and Bob) can share a common secret key. In this protocol, the secret key shared between Alice and Bob can neither be eavesdropped by outside eavesdroppers nor be determined by one of the two participants alone. That is to say, this protocol can resist not only outside attacks but also participant attacks.

3 Security analysis

In this section, we prove the security of the proposed protocol. First, we consider the outside attacks, then we take into consideration of the participant attacks.

3.1 Outside attack

The process of detecting eavesdropping done by the two participants (Alice and Bob) in this protocol is essentially equivalent to that in the BB84 QKD protocol [4], which has been proved to be unconditionally secure. That is, the decoy particles, which are randomly inserted into S_B, are generated by randomly choosing from one of the two mutually unbiased bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. After Bob obtains the information of the positions and states of the decoy particles, he measures them with the same bases as those chosen by Alice for preparing them. For any outside eavesdropper, the bases used by Bob are random even though they are finally announced publicly as no eavesdropper has the access to the particles in S'_B after Bob receives them. Just like the situation in the BB84 protocol [4], if an outside attacker eavesdrops in the process of this protocol, his/her eavesdropping actions will inevitably disturb part of the decoy particles and be found by the two participants.

3.2 Participant attack

We first consider the situation that Bob is a dishonest participant who wants to determine the secret key alone. After the eavesdropping check in step (3), the states in Alice's hand (i.e., $A_i, i = 1, 2, 3, \ldots, n$), as well as the states in Bob's hand (i.e., $B_i, i = 1, 2, 3, \ldots, n$), are maximally mixed states. Whatever basis Bob chooses in step (4), Alice's measurement outcomes are random. Even though Bob measures the states in his hand first and then decides which bases to announce, he cannot deterministically control the final key. We take the state $|\phi^+\rangle_{A_k B_k}$, for example, suppose Bob wants the k-th bit in the key to be 1, without loss of generality, we suppose that he measures his particle B_k in σ_z-basis, the measurement outcome will randomly be $|0\rangle$ or $|1\rangle$. If the outcome is $|1\rangle$ (i.e., the key bit is 1), Bob can announce that C_k is 0 and he successfully controls this bit. If the outcome is $|0\rangle$, then Bob can only announce that C_k is 1. However, when Alice measures A_k in σ_x-basis, Alice's measurement result will randomly be $|+\rangle$ or $|-\rangle$, which means Alice's key bit will randomly be 0 or 1. That is to say, the k-th bit in the key generated by Alice and Bob will be different with a probability of 25 %. Therefore, the key in Alice's hand will not be identical with the one in Bob's hand with a probability of 1–(3/4)^n provided Bob adopts such attack, especially this probability will be exponentially close to 1 with the increase of n.

Now we consider the situation that Alice is a dishonest participant who wants to determine the secret key alone. Whatever state Bob receives, the measurement outcome of a state cannot be the same in the two mutually unbiased bases. If Alice sends fake states to Bob in order to determine the final key, she would face the same dilemmas as Bob who adopts the above attack, i.e., she cannot determine the key accurately but probably makes the protocol failed. Obviously, Alice's attack strategy is similar to Bob's and is more powerful, so here we only analyze Alice's attack in detail.

Without loss of generality, we take one key bit for example. Suppose Alice wants the key bit to be 0. She prepares the following two-qubit system $|\varphi\rangle_{AB}$ and sends the subsystem B to Bob, where

$$|\varphi\rangle_{AB} = \sum_{i=1}^{2} \lambda_i |a_i\rangle_A |b_i\rangle_B. \tag{2}$$

The right of Eq. (2) is in the form of Schmidt decomposition. The reduced density matrix of system B is

$$\rho_B = |\lambda_1|^2 |b_1\rangle\langle b_1| + |\lambda_2|^2 |b_2\rangle\langle b_2|. \tag{3}$$

When Bob chooses the σ_z-basis, the probability of measurement outcome to be 0 is

$$P_0 = \mathtt{Tr}(|\lambda_1|^2|b_1\rangle\langle b_1||0\rangle\langle 0| + |\lambda_2|^2|b_2\rangle\langle b_2||0\rangle\langle 0|). \tag{4}$$

When Bob chooses the σ_x-basis, the probability of measurement outcome to be 0 is

$$P_+ = \mathtt{Tr}(|\lambda_1|^2|b_1\rangle\langle b_1||+\rangle\langle +| + |\lambda_2|^2|b_2\rangle\langle b_2||+\rangle\langle +|). \tag{5}$$

Suppose $|b_i\rangle = \mu_i|0\rangle + \nu_i|1\rangle$, where $|\mu_i|^2 + |\nu_i|^2 = 1, i = 1, 2$. Since $\langle b_2|b_1\rangle = 0$, then

$$\mu_1\mu_2^* + \nu_1\nu_2^* = 0. \tag{6}$$

Hence, the probability that Alice succeed to cheat is

$$\begin{aligned}P &= \frac{1}{2}(P_0 + P_+)\\ &= \frac{1}{2}\mathtt{Tr}[(|\lambda_1|^2|b_1\rangle\langle b_1| + |\lambda_2|^2|b_2\rangle\langle b_2|)(|0\rangle\langle 0| + |+\rangle\langle +|)]\\ &= \frac{1}{4}[|\lambda_1|^2(2|\mu_1|^2 + \mu_1\nu_1^* + \mu_1^*\nu_1)\\ &\quad +|\lambda_2|^2(2|\mu_2|^2 + \mu_2\nu_2^* + \mu_2^*\nu_2) + 1].\end{aligned} \tag{7}$$

Without loss of generality, we suppose $|\lambda_1| = \cos\alpha, |\lambda_2| = \sin\alpha$ and $\mu_j = e^{\beta_j i}\cos\theta_j, \nu_j = \sin\theta_j$, where $j = 1, 2$. Then

$$\begin{aligned}P = \frac{1}{4}[&\cos^2\alpha(2\cos^2\theta_1 + 2\cos\beta_1\cos\theta_1\sin\theta_1)\\ &+ \sin^2\alpha(2\cos^2\theta_2 + 2\cos\beta_2\cos\theta_2\sin\theta_2) + 1].\end{aligned} \tag{8}$$

According to Eq. (6),

$$\cos\theta_1\cos\theta_2 e^{i(\beta_1-\beta_2)} + \sin\theta_1\sin\theta_2 = 0 \tag{9}$$

Based on Eq. (9), β_1 and β_2 must meet the condition: $\beta_1 - \beta_2 = k\pi, k \in Z$. The further discussion about the parameters β_1, β_2, $\sin\theta_1$ and $\sin\theta_2$ is: (a) when $\beta_1 - \beta_2 = 2k\pi$, $\cos\theta_1\cos\theta_2 + \sin\theta_1\sin\theta_2 = \cos(\theta_1 - \theta_2) = 0$, i.e., $\theta_1 - \theta_2 = k\pi + \frac{\pi}{2}, k \in Z$; (b) when $\beta_1 - \beta_2 = 2k\pi + \pi$, $\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 = \cos(\theta_1 + \theta_2) = 0$, i.e., $\theta_1 + \theta_2 = k\pi + \frac{\pi}{2}, k \in Z$. According to Eq. (8) and the above discussion, we have

$$\begin{aligned}P &\leq \frac{1}{4}(2\cos^2\alpha\cos^2\theta_1 + 2\sin^2\alpha\sin^2\theta_1 + 2\cos\theta_1\sin\theta_1 + 1)\\ &= \frac{\cos 2\alpha\cos 2\theta_1 + \sin 2\theta_1 + 2}{4}\\ &\leq \frac{\sqrt{1+\cos^2 2\alpha} + 2}{4}\\ &\leq \frac{\sqrt{2}+2}{4}\\ &\approx 0.85.\end{aligned} \tag{10}$$

That is to say, by utilizing the optimal strategy, Alice can successfully control one bit of the key with the probability of 0.85. Therefore, Alice can successfully determine an n-bit key with a probability of $(0.85)^n$, which will be exponentially close to 0 with the increase of n.

In this section, the security of the proposed QKA protocol is analyzed in detail. It is shown that the outside eavesdropper cannot get any information of the generated key. In addition, neither of the two participants can determine the generated key alone.

4 Fault-tolerant QKA protocols with EPR pair block over two collective-noise channels

To share a common key by the proposed QKA protocol, the two participants should first share a sequence of EPR pairs in $|\phi^+\rangle$. In addition, in another QKA protocol [35] which is also based on the property of EPR pairs, the participants should also first share a sequence of EPR pairs which are randomly in one of the four states: $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle\}$, where

$$\begin{aligned}|\phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),\\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).\end{aligned} \tag{11}$$

As described in both the two protocols, to share an EPR pair between two participants in theory, one participant can first prepare the EPR pair and then directly send one particle of the pair to the other one.

However, in practical situation, the qubits transmitted in quantum channel often interact with the environment uncontrollably and noises are then introduced in the transmission unexpectedly. The noise will not only decrease the fidelity of the transmitting qubits, but also provide the eavesdropper a chance to disguise the disturbance caused by her eavesdropping actions during the transmission. To combat with the decoherence of quantum qubits caused by the channel noise, some good methods, such as entanglement purification [37], single-photon error rejection [38] and decoherence-free subspace (DFS) [39–44], have been proposed. For the schemes based on the ideal of DFS, there is an important precondition named the collective-noise assumption [39,40]. That is, if several qubits transmit through the noisy channel simultaneously or they are spatially close to each other, the alterations caused by the noise on each of the qubits are identical.

In the collective-noise channel, two participants can no longer share the EPR pairs between each other simply as described in both our protocol and the one in [35]. In the following part, we will introduce an method for sharing all the four kinds of EPR pairs over collective-dephasing noise channel and collective-rotation noise channel, respectively, inspired by the ideals in [43,44]. This method is very useful since sharing EPR pairs between two participants is an important work in many quantum protocols, especially in the protocols over non-ideal channels. By utilizing this method, both our protocol and the one in [35] can be immune to these two kinds of collective noise.

Herein, we first describe the distribution processes of the EPR pair $|\psi^+\rangle$ over the two kinds of collective-noise channels. Obviously, if two participants could successfully share the EPR pair $|\psi^+\rangle$ over the collective-noise channels, they can also easily share the other three kinds of EPR pairs ($|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^-\rangle$). Concretely, if the two users want to share the EPR pairs $|\phi^+\rangle$ ($|\phi^-\rangle$, $|\psi^-\rangle$) between each other, they first share $|\psi^+\rangle$ and then they can transform $|\psi^+\rangle$ to $|\phi^+\rangle$ ($|\phi^-\rangle$, $|\psi^-\rangle$) by performing the unitary operation U_x (U_y, U_z) on the first qubit of their EPR pair $|\psi^+\rangle$, where

$$U_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad U_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \quad U_z = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{12}$$

The distribution processes of the state $|\psi^+\rangle$ over the two collective-noise channels can be described, respectively, as follows.

4.1 Distribution process of EPR pairs over collective-dephasing channel

The transformation effects of the collective-dephasing noise are illustrated as

$$U_{dp}|0\rangle = |0\rangle, \qquad U_{dp}|1\rangle = e^{i\phi}|1\rangle, \tag{13}$$

where ϕ is the noise parameter which fluctuates with time. In general, a logical qubit encoded into two physical qubits with antiparallel parity is immune to this kind of noise since these two logical qubits acquire the same global phase factor $e^{i\phi}$.

$$|0\rangle_L \equiv |0\rangle|1\rangle, \qquad |1\rangle_L \equiv |1\rangle|0\rangle. \tag{14}$$

Here, $|0\rangle_L$ and $|1\rangle_L$ are sufficient to encode one bit of information over collective-dephasing channel. Specifically, an input state of a single qubit can be generally expressed as $|\vartheta\rangle = a|0\rangle + b|1\rangle$. By appending an auxiliary qubit in state $|1\rangle$ via the circuits shown in Fig. 2, it will be encoded into the state as

$$|\vartheta\rangle_L = a|0\rangle_L + b|1\rangle_L = a|01\rangle + b|10\rangle. \tag{15}$$

Obviously, the decoding circuits can be constructed by the same operations in the reverse order. In both the encoding circuits and decoding circuits, time proceeds from left to right.

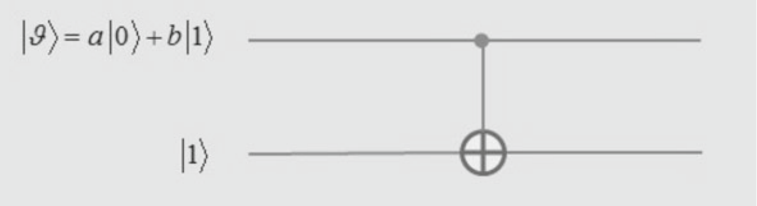

Fig. 2 The encoding circuit for preventing collective-dephasing noise

To communicate securely, at least two non-orthogonal measuring bases are needed. One of the bases is $\{|0\rangle_L, |1\rangle_L\}$, the other one can be chosen as $\{|+\rangle_L, |-\rangle_L\}$, where

$$\begin{aligned} |+\rangle_L &= \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L) = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle), \\ |-\rangle_L &= \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L) = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle). \end{aligned} \tag{16}$$

It can be easily verified that $\{|0\rangle_L, |1\rangle_L\}$ and $\{|+\rangle_L, |-\rangle_L\}$ form two mutually unbiased bases. The steps of the method for sharing the EPR pairs $|\psi^+\rangle$ between two authorized users (Alice and Bob) over collective-dephasing channel can be described as follows.

1) By utilizing the encoding circuits in Fig. 2, Alice first prepares a sequence of quantum entangled states in

$$\begin{aligned} |\Theta_{dp}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle_L + |1\rangle|0\rangle_L)_{AB} \\ &= \frac{1}{\sqrt{2}}(|0\rangle|10\rangle + |1\rangle|01\rangle)_{AB_1B_2}. \end{aligned} \tag{17}$$

Then Alice divides these quantum states into two sequences, which are denoted as T_A and T_B. T_A is consisted of all the qubits A in these entangled states and T_B is made up of the logical qubits B, which is composed of B_1 and B_2.

2) Alice generates m decoy states, which are randomly in one of the four states: $|0\rangle_L$, $|1\rangle_L$, $|+\rangle_L$ and $|-\rangle_L$. Then she randomly inserts them into the sequence T_B to form a new sequence T'_B. After that, Alice sends Bob the sequence T'_B and preserves the sequence T_A.

3) After Bob confirms the reception of T'_B, Alice announces the positions and the initial states of all the m decoy states. Then for each one of the decoy states, Bob measures it in $\sigma_z \otimes \sigma_z$-basis ($\sigma_x \otimes \sigma_x$-basis) if its initial state is $|0\rangle_L$ or $|1\rangle_L$ ($|+\rangle_L$ or $|-\rangle_L$). With the measurement outcomes of the m decoy states, Bob checks eavesdropping according to Table 1. If there exists no eavesdropping, they utilize the remaining states to share the EPR pairs $|\psi^+\rangle$ as described in the next step. Otherwise, they abort the states and restart from the begging.

4) For each of the remaining states $|\Theta_{dp}\rangle_{AB}$, Bob performs a controlled-NOT operation $\mathrm{CNOT}_{B_1B_2}$ on particles B_1 and B_2 by using particle B_1 as the controller and

Table 1 The possible measurement outcomes which will be obtained by measuring the four states, $|0\rangle_L$, $|1\rangle_L$, $|+\rangle_L$ and $|-\rangle_L$, in the bases $\sigma_z \otimes \sigma_z$ and $\sigma_x \otimes \sigma_x$, respectively

State	$\sigma_z \otimes \sigma_z$-basis	$\sigma_x \otimes \sigma_x$-basis
$\lvert 0\rangle_L$	$\lvert 01\rangle$	$\lvert ++\rangle, \lvert --\rangle, \lvert -+\rangle, \lvert -+\rangle$
$\lvert 1\rangle_L$	$\lvert 10\rangle$	$\lvert ++\rangle, \lvert --\rangle, \lvert -+\rangle, \lvert -+\rangle$
$\lvert +\rangle_L$	$\lvert 01\rangle, \lvert 10\rangle$	$\lvert ++\rangle, \lvert --\rangle$
$\lvert -\rangle_L$	$\lvert 01\rangle, \lvert 10\rangle$	$\lvert -+\rangle, \lvert -+\rangle$

B_2 as the target. Then the state of the quantum system will be converted from $|\Theta_{dp}\rangle_{AB}$ into

$$
\begin{aligned}
|\Xi_{dp}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|11\rangle + |1\rangle|01\rangle)_{AB_1B_2} \\
&= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB_1} \otimes |1\rangle_{B_2}.
\end{aligned} \tag{18}
$$

Till now, Alice and Bob have securely share a sequence of EPR pairs $|\psi^+\rangle_{AB_1} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB_1}$ over collective-dephasing channel. Of course, if the EPR pair that they want share is $|\phi^+\rangle$ ($|\phi^-\rangle$, $|\psi^-\rangle$), they can simply perform the unitary operation U_x (U_y, U_z) on the first qubit of each their shared EPR pairs $|\phi^+\rangle$.

4.2 Distribution process of EPR pair block over collective-rotation channel

The transformation effects of the collective-rotation noise are illustrated as

$$
\begin{aligned}
U_r|0\rangle &= \cos\theta|0\rangle + \sin\theta|1\rangle, \\
U_r|1\rangle &= -\sin\theta|0\rangle + \cos\theta|1\rangle.
\end{aligned} \tag{19}
$$

The parameter θ are the noise parameter which fluctuates with time. It is known that the two EPR pairs, $|\Phi^+\rangle$ and $|\Psi^-\rangle$, are invariant under the collective-rotation noise. Therefore, we can choose the logical qubits as

$$
\begin{aligned}
|0_r\rangle \equiv |\Phi^+\rangle &= \frac{1}{2}(|++\rangle + |--\rangle), \\
|1_r\rangle \equiv |\Psi^-\rangle &= \frac{1}{2}(|-+\rangle - |+-\rangle).
\end{aligned} \tag{20}
$$

Here, $|0_r\rangle$ and $|1_r\rangle$ are sufficient to encode one bit of information over collective-rotation channel. Concretely, an input state of a single qubit can be generally expressed as $|\vartheta\rangle = a|0\rangle + b|1\rangle$. By appending an auxiliary qubit in state $|0\rangle$ via the circuits given in Fig. 3, it is encoded into the following state:

$$
|\vartheta_r\rangle = a|0_r\rangle + b|1_r\rangle = a|\Phi^+\rangle + b|\psi^-\rangle. \tag{21}
$$

Apparently, the decoding circuits can be constructed by the same operations in the reverse order. In both the encoding circuits and decoding circuits, time proceeds from left to right.

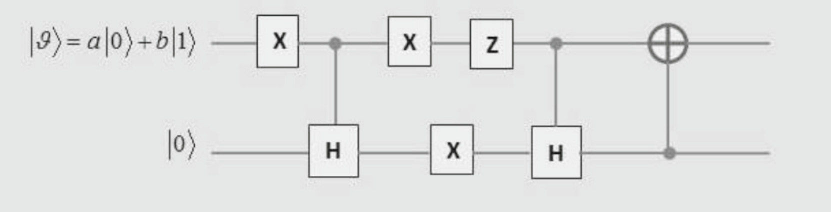

Fig. 3 The encoding circuit for preventing collective-rotation

For secure communication, at least two non-orthogonal bases are required. One of the bases can be $\{|0\rangle_r, |1\rangle_r\}$, and the other one can be chosen as $\{|+\rangle_r, |-\rangle_r\}$, where

$$
\begin{aligned}
|+_r\rangle &= \frac{1}{\sqrt{2}}(|0_r\rangle + |1_r\rangle) = \frac{1}{\sqrt{2}}(|0+\rangle - |1-\rangle),\\
|-_r\rangle &= \frac{1}{\sqrt{2}}(|0_r\rangle - |1_r\rangle) = \frac{1}{\sqrt{2}}(|0-\rangle + |1+\rangle).
\end{aligned} \tag{22}
$$

It can be easily proved that $|\langle_r{+}|0_r\rangle|^2 = |\langle_r{+}|1_r\rangle|^2 = |\langle_r{-}|0_r\rangle|^2 = |\langle_r{-}|1_r\rangle|^2 = \frac{1}{2}$, which indicates that $\{|0_r\rangle, |1_r\rangle\}$ and $\{|+_r\rangle, |-_r\rangle\}$ form two mutually unbiased bases. The steps of the method for sharing the EPR pairs $|\psi^+\rangle$ between two participants (Alice and Bob) over collective-rotation channel can be described as follows.

a) By utilizing the encoding circuits in Fig. 3, Alice first prepares a sequence of quantum entangled states in

$$
\begin{aligned}
|\Theta_r\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|0_r\rangle - |1\rangle|1_r\rangle)_{AB}\\
&= \frac{1}{2}(|0\rangle(|00\rangle + |11\rangle) - |1\rangle(|01\rangle - |10\rangle))_{AB_1B_2}\\
&= \frac{1}{\sqrt{2}}(|sts\rangle + |tst\rangle)_{AB_1B_2},
\end{aligned} \tag{23}
$$

where $|s\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|t\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ are the up and down eigenstates of σ_y. Alice divides these quantum states into two sequences, T_A and T_B. T_A is consisted of all the qubits A in these entangled states and T_B is made up of the logical qubits B, which is consisted of two physical qubits B_1 and B_2.

b) Alice generates m decoy states which are randomly in one of the four states: $|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle$. Then she randomly inserts them into the sequence T_B to form a new sequence T_B'. Afterwards, Alice sends Bob the sequence T_B' and preserves the sequence T_A.

c) After Bob confirms the reception of T_B', Alice announces the positions and the initial states of all the m decoy states. Then for each one of the decoy states, Bob measures it in $\sigma_x \otimes \sigma_x$-basis ($\sigma_z \otimes \sigma_x$-basis) if its initial state is $|0_r\rangle$ or $|1_r\rangle$ ($|+_r\rangle$ or $|-_r\rangle$). With the measurement outcomes of the m decoy states, Bob checks eavesdropping according to Table 2. If there exists no eavesdropping, they make

Table 2 The possible measurement outcomes which will be obtained by measuring the four states, $|0_r\rangle$, $|1_r\rangle$, $|+_r\rangle$ and $|-_r\rangle$, in the bases $\sigma_x \otimes \sigma_x$ and $\sigma_z \otimes \sigma_x$, respectively

State	$\sigma_x \otimes \sigma_x$-basis	$\sigma_z \otimes \sigma_x$-basis
$\|0_r\rangle$	$\|++\rangle, \|--\rangle$	$\|0+\rangle, \|1-\rangle, \|0-\rangle, \|1+\rangle$
$\|1_r\rangle$	$\|-+\rangle, \|-+\rangle,$	$\|0+\rangle, \|1-\rangle, \|0-\rangle, \|1+\rangle$
$\|+_r\rangle$	$\|++\rangle, \|--\rangle, \|-+\rangle, \|-+\rangle$	$\|0+\rangle, \|1-\rangle$
$\|-_r\rangle$	$\|++\rangle, \|--\rangle, \|-+\rangle, \|-+\rangle$	$\|0-\rangle, \|1+\rangle$

use of the remaining states to share the EPR pairs $|\psi^+\rangle$ as described in the following steps. Otherwise, they abort the states and restart from the begging.

d) Alice and Bob cooperate to perform the operations $S \otimes S \otimes S$ and $H \otimes H \otimes H$ on their shared entangled state $|\Theta_r\rangle_{AB}$, respectively. Here S is phase gate and H is Hadamard gate, where

$$\begin{aligned} H &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|), \\ S &= |0\rangle\langle 0| + i|1\rangle\langle 1|. \end{aligned} \tag{24}$$

After these operations, the state of the shared quantum system will be transformed from $|\Theta_r\rangle_{AB}$ into

$$|\Gamma_r\rangle_{AB} = \frac{1}{\sqrt{2}}(|1\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle)_{AB_1B_2}. \tag{25}$$

e) For each of the states $|\Gamma_r\rangle_{AB}$, Bob performs a controlled-NOT operation $\text{CNOT}_{B_1B_2}$ on particles B_1 and B_2 by using particle B_1 as the controller and B_2 as the target. Then the state of the quantum system will be converted from $|\Gamma_r\rangle_{AB}$ into

$$\begin{aligned} |\Delta_r\rangle_{AB} &= \frac{1}{\sqrt{2}}(|1\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|1\rangle)_{AB_1B_2} \\ &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB_1} \otimes |1\rangle_{B_2}. \end{aligned} \tag{26}$$

Till now, Alice and Bob have securely share a sequence of EPR pairs $|\psi^+\rangle_{AB_1} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB_1}$. Of course, if the EPR pair that they want share is $|\phi^+\rangle$ ($|\phi^-\rangle$, $|\psi^-\rangle$), they can simply perform the unitary operation U_x (U_y, U_z) on the first qubit of each their shared EPR pairs $|\phi^+\rangle$.

4.3 Security analysis of the distribution processes of EPR pair block over the two collective-noise channels

The above distribution processes of EPR pairs are secure since the eavesdropping detecting processes done by the two participants in step 3) and step *c*) are essentially equivalent to that in the BB84 QKD protocol [4].

Now, we take the distribution process over collective-dephasing channel, for example. The decoy states that used in the eavesdropping detection in Sect. 4.1 are generated by randomly choosing from one of the two mutually unbiased bases $\{|0\rangle_L, |1\rangle_L\}$ and $\{|+\rangle_L, |-\rangle_L\}$ and are randomly inserted into T_B. For each of the decoy states, after Bob obtains the information of its position and initial state, he measures it in $\sigma_z \otimes \sigma_z$-basis ($\sigma_x \otimes \sigma_x$-basis) if its initial state is $|0\rangle_L$ or $|1\rangle_L$ ($|+\rangle_L$ or $|-\rangle_L$).

For any eavesdropper, the bases used by Bob are random since the decoy states are generated by randomly using one of the two bases $\{|0\rangle_L, |1\rangle_L\}$ and $\{|+\rangle_L, |-\rangle_L\}$. Although the information of the bases is finally announced in public, once Bob receives them, no eavesdropper has the access to the states in T'_B. Same as that in the BB84 protocol which has been proved to be unconditionally secure, any eavesdropping action will inevitably disturb part of the decoy states and be noticed by the two participants if an eavesdropper eavesdrops in the distribution process of the EPR pairs.

As for the distribution process over collective-rotation channel, it is also secure since the eavesdropping detecting process in Sect. 4.2, in essence, is also the same as that in the BB84 QKD protocol. Thus, we omit the redundant description here.

5 Discussion and conclusions

The proposed protocol utilizes EPR pairs as the information carriers, and further utilizes single-particle measurements as the main operations. In practice, EPR pairs have been experimentally generated by many research groups [45–49], and the single-particle measurements have also been a mature technology which has been widely used in quantum information processing. Therefore, our protocol is more feasible than the protocol which need to perform Bell measurements [35]. In addition, in order to transmit the ordered particle block (i.e., S'_B) to Bob, the sender Alice can make use of the similar circuits composed of optical delays and switches in [11,12] to adjust the particles in S'_B. Moreover, our protocol is presented with EPR pairs, if the qubits of the EPR pairs are transmitted in a noisy channel, it seems that the entanglement may be threaten over a long distance. In this situation, the quantum–repeater technique [50,51], which contains the entanglement purification and teleportation, can be utilized to keep the reliability of the shared entanglement.

In conclusion, we first present an efficient and feasible QKA protocol with blocks of EPR pairs and single-particle measurements in this paper. Then we proved this protocol to be secure against both the outside attacks and participant attack. In addition to this protocol, a useful method for sharing EPR pairs between two participants over collective-dephasing channel/collective-rotation channel is introduced. This method is very useful since sharing EPR pairs between two participants is an important work in many quantum cryptographic protocols, especially in the protocols over non-ideal channels. By utilizing this method, both our proposed protocol and the one in [35] can be immune to these two kinds of collective noise. What is more, the implementation of the both the proposed QKA protocol and the method for sharing EPR pairs only needs to utilize EPR pairs and single-particle measurements. Therefore, our protocols is feasible with the present techniques.

Acknowledgments This work is supported by NSFC (Grant Nos. 61272057, 61170270, 61100203, 61003286, 61121061, 61103210), NCET (Grant No. NCET-10-0260), SRFDP (Grant No. 2009000 5110010), Beijing Natural Science Foundation (Grant Nos. 4112040, 4122054), the Fundamental Research Funds for the Central Universities (Grant No. 2011YB01) and BUPT Excellent Ph.D. Students Foundation (Grant No. CX201217, CX201334).

References

1. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mexico, pp. 124–234 (1994)
2. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of 28th Annual ACM Symposium on Theory of Computing, New York, pp. 212–219 (1996)
3. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145–95 (2002)
4. Bennett, C.H., Brassard, G.: Public-key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179 (1984)
5. Deng, F.G., Long, G.L.: Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys. Rev. A **70**, 012311 (2004)
6. Liu, B., Gao, F., Wen, Q.Y.: Single-photon multiparty quantum cryptographic protocols with collective detection. IEEE J. Quant. Electron. **47**, 1389–1390 (2011)
7. Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys. Rev. A **68**, 042315 (2003)
8. Tan, Y.G., Cai, Q.Y.: Practical decoy state quantum key distribution with finite resource. Eur. Phys. J. D **56**, 449–455 (2010)
9. Song, S.Y., Wang, C.: Recent development in quantum communication. Chin. Sci. Bull. **57**, 4694–4700 (1999)
10. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
11. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
12. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
13. Long, G.L., Deng, F.G., Wang, C., Li, X.H., et al.: Quantum secure direct communication and deterministic secure quantum communication. Front. Phys. China **2**, 251 (2007)
14. Wang, C., Deng, F.G., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**, 044305 (2005)
15. Huang, W., Zuo, H.J., Li, Y.B.: Cryptanalysis and improvement of a multi-user quantum communication network using type entangled states. Int. J. Theor. Phys. **52**, 1354–1361 (2013)
16. Lin, S., Wen, Q.Y., Zhu, F.C.: Quantum secure direct communication with χ-type entangled states. Phys. Rev. A **78**, 064304 (2008)
17. Li, X.H., Deng, F.G., Li, C.Y., Liang, Y.J., Zhou, P., Zhou, H.Y.: Deterministic secure quantum communication without maximally entangled states. J. Koeran Phys. Soc. **49**, 1354 (2006)
18. Yuan, H., Song, J., Zhou, J., Zhang, G., Wei, X.F.: High-capacity deterministic secure four-qubit W state protocol for quantum communication based on order rearrangement of particle pairs. Quantum Inf. Process. **50**, 2403–2409 (2011)
19. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Chen, H.: Deterministic secure quantum communication with collective detection using single photons. Int. J. Theor. Phys. **51**, 2787–2797 (2012)
20. Gu, B., Pei, S.X., Song, B., Zhong, K.: Deterministic secure quantum communication over a collective-noise channel. Sci. China Ser. G **52**, 1913–1918 (2009)
21. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum secret sharing schemes. Phys. Rev. A **69**, 052307 (2004)
22. Hao, L., Wang, C., Long, G.L.: Quantum secret sharing protocol with four state Grover algorithm and its proof-of-principle experimental demonstration. Opt. Commun. **284**, 3639–3642 (2011)

23. Tsai, C.W., Hwang, T.: Multi-party quantum secret sharing based on two special entangled states. Sci. China Phys. Mech. Astron. **55**, 460–464 (2012)
24. Massoud, H.D., Elham, F.: A novel and efficient multiparty quantum secret sharing scheme using entangled states. Sci. China Phys. Mech. Astron. **55**, 1828–1831 (2012)
25. Adhikari, S., Chakrabarty, I., Agrawal, P.: Probabilistic secret sharing theory through noisy channel. Quantum Inf. Comput. **12**, 253–270 (2012)
26. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. **42**, 055305 (2009)
27. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545–549 (2011)
28. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China Phys. Mech. Astron. **56**, 1670–1678 (2013)
29. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**, 042312 (2002)
30. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A **84**, 022344 (2011)
31. Su, Q., Huang, Z., Wen, Q.Y., Li, W.M.: Quantum blind signature based on two-state vector formalism. Opt. Commun. **283**, 4408 (2010)
32. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149 (2004)
33. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on "Quantum Key Agreement Protocol with Maximally Entangled States". Int. J. Theor. Phys. **50**, 1793–1802 (2011)
34. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192–1195 (2010)
35. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**, 921–932 (2012)
36. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement protocol with single particles. Quantum Inf. Process. **12**, 1797–1805 (2012)
37. Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A., Wootters, W.K.: Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett. **76**, 722 (1996)
38. Li, X.H., Deng, F.G., Zhou, H.Y.: Faithful qubit transmission against collective noise without ancillary qubits. Appl. Phys. Lett. **91**, 144101 (2007)
39. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
40. Zanardi, P., Rasetti, M.: Noiseless quantum codes. Phys. Rev. Lett. **79**, 3306 (1997)
41. Huang, W., Guo, F.Z., Huang, Z., Wen, Q.Y., Zhu, F.C.: Three-particle QKD protocol against a collective noise. Opt. Commun. **284**, 536–540 (2011)
42. Skotiniotis, M., Duer, W., Kraus, B.: Efficient quantum communication under collective noise. Quantum Inf. Comput. **12**, 290–323 (2013)
43. Huang, W., Wen, Q.Y., Jia, H.Y., Qin, S.J., Gao, F.: Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin. Phys. B **21**, 100308 (2012)
44. Li, X.H., Zhao, B.K., Sheng, Y.B., Deng, F.G., Zhou, H.Y.: Fault tolerant quantum key distribution based on quantum dense coding with collective noise. Int. J. Quantum Inform. **7**, 1479 (2009)
45. Shih, Y.: Entangled biphoton source-property and preparation. Rep. Prog. Phys. **66**, 1009–1044 (2003)
46. Sweke, R., Sinayskiy, I., Petruccione, F.: Dissipative preparation of generalized Bell states. J. Phys. B At. Mol. Opt. Phys. **46**, 104004 (2013)
47. Brida, G., Chekhova, M., Genovese, M., Krivitsky, L.: Generation of different Bell states within the spontaneous parametric down-conversion phase-matching bandwidth. Phys. Rev. A **76**, 053807 (2007)
48. Agnew, M., Salvail, J.Z., Leach, J., Boyd, R.W.: Generation of orbital angular momentum bell states and their verification via accessible nonlinear witnesses. Phys. Rev. Lett. **111**, 030402 (2013)
49. Wang, T.J., Lu, Y., Long, G.L.: Generation and complete analysis of the hyperentangled Bell state for photons assisted by quantum-dot spins in optical microcavities. J. Phys. B At. Mol. Opt. Phys. **86**, 042337 (2012)
50. Chen, Z.W., Zhao, B., Chen, Y.A., Schmiedmayer, J., Pan, J.W.: Fault-tolerant quantum repeater with atomic ensembles and linear optics. Phys. Rev. A **76**, 022329 (2007)
51. Sheng, Y.B., Zhou, L., Long, G.L.: Hybrid entanglement purification for quantum repeaters. Phys. Rev. A **88**, 022302 (2013)