An optimized encoding method for secure key distribution by swapping quantum entanglement and its extension*

Gao Gan(高 干)†

Department of Electrical Engineering, Tongling University, Tongling 244000, *China*

(Received 30 December 2014; revised manuscript received 15 February 2015; published online 20 June 2015)

Song [Song D 2004 *Phys. Rev. A* **69** 034301] first proposed two key distribution schemes with the symmetry feature. We find that, in the schemes, the private channels which Alice and Bob publicly announce the initial Bell state or the measurement result through are not needed in discovering keys, and Song's encoding methods do not arrive at the optimization. Here, an optimized encoding method is given so that the efficiencies of Song's schemes are improved by 7/3 times. Interestingly, this optimized encoding method can be extended to the key distribution scheme composed of generalized Bell states.

Keywords: quantum key distribution, optimized encoding method, entanglement swapping, generalized Bell states

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/24/8/080305

1. Introduction

As we all know, classical cryptography is conditionally secure because it only relies on the difficulty of solving mathematical problems. However, its counterpart, quantum cryptography, whose security is based on the laws of physics, is unconditionally secure. Due to this merit, quantum cryptography has attracted a lot of attention and produced many promising applications. Quantum key distribution (QKD) is one of these promising applications. The first QKD scheme,[1] in which the quantum states from nonorthogonal bases are used, was proposed by Bennett and Brassard in 1984. Customarily, it is called the BB84 scheme. Subsequently, all kinds of QKD schemes[2–20] have been put forward. These existing schemes may be divided into three kinds. One is proposed by using only non-entangled states, another by using only entanglement states, and the third by using both. By making use of the statistics, we find that most of the existing QKD schemes have made use of entanglement states. Obviously, entanglement states play an important role in designing QKD schemes. At present, there are several common methods to produce entanglement states, such as nonlinear crystal and optical pulse,[21] ion trap and ions,[22] and cavity QED and atoms,[23] atomic ensembles,[24] and so on. Entanglement swapping[25] is a nice property of quantum entanglement, and also the method where the entanglement among the particles that do not have a direct interaction is produced. For example, consider two EPR pairs in the state $\Psi_{12}^{-}\Phi_{34}^{+}$ (i.e., qubits 1 and 2 are in the state Ψ^{-}, and qubits 3 and 4 are in the state Φ^{+}). If a Bell measurement on qubits 1 and 3 is performed, they will be entangled to one of the four Bell states, $\Psi^{\pm} = (|01\rangle \pm |10\rangle)/\sqrt{2}$ and $\Phi^{\pm} = (|00\rangle \pm |11\rangle)/\sqrt{2}$. At the same time, qubits 2 and 4 will be also projected onto a corresponding Bell state. The whole system of two EPR pairs evolves as follows:

$$\Psi_{12}^{-} \otimes \Phi_{34}^{+} = \frac{1}{\sqrt{2}}(\Phi_{13}^{-}\Psi_{24}^{+} - \Phi_{13}^{+}\Psi_{24}^{-} + \Psi_{13}^{-}\Phi_{24}^{+} - \Psi_{13}^{+}\Phi_{24}^{-}). \quad (1)$$

After the Bell measurement on qubits 1 and 3 is performed, the whole system will be in $\Phi_{13}^{-}\Psi_{24}^{+}$, $\Phi_{13}^{+}\Psi_{24}^{-}$, $\Psi_{13}^{-}\Phi_{24}^{+}$, and $\Psi_{13}^{+}\Phi_{24}^{-}$ with equal probability of 25% for each. The previous entanglement between qubits 1 and 2, and qubits 3 and 4 are now swapped into the entanglement between qubits 1 and 3, and 2 and 4. If two EPR pairs are not in $\Psi_{12}^{-}\Phi_{34}^{+}$, but other Bell states, similar results can appear. By the way, using the entanglement swapping, some QKD schemes had been proposed. In addition, according to whether two legitimate parties have an equal role, the features of these QKD schemes may be divided into two kinds, the symmetry[12] and the asymmetry.

In 2004, by using the entanglement swapping of two Bell states, Song[4] first proposed two QKD schemes with the symmetry feature. The schemes are interesting, but their efficiencies are not high, because the classical information that two parties announce is too much during forming keys. In fact, the main reasons for low efficiencies of Song's schemes are that the encoding methods are not optimized. In this paper, we will give an optimized encoding method so that the efficiencies of Song's schemes are improved by 7/3 times. Meanwhile, we also research whether this optimized encoding method is fit for the QKD scheme composed of other entanglement states.

*Project supported by the National Natural Science Foundation of China (Grant No. 11205115), the Program for Academic Leader Reserve Candidates in Tongling University (Grant No. 2014tlxyxs30), and the 2014-year Program for Excellent Youth Talents in University of Anhui Province, China.

†Corresponding author. E-mail: gaogan0556@163.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

2. Optimized encoding method for Song's QKD

In this section, we first review Song's two QKD schemes, and then give an optimized encoding method for Song's schemes, in other words, we propose a modified Song's scheme. Meanwhile, we show that the modified scheme and Song's original schemes can stand against the entangle-measure attack. Lastly, we make a comparison for the efficiencies of the modified scheme and Song's original schemes.

2.1. Review of Song's schemes

Let us start with the brief description of Song's scheme I.

Step 1 Alice prepares an EPR pair of qubits 1 and 2. It is either in Bell basis ($\Psi_{12}^{\pm} = (|01\rangle \pm |10\rangle)_{12}/\sqrt{2}$ and $\Phi_{12}^{\pm} = (|00\rangle \pm |11\rangle)_{12}/\sqrt{2}$), or in rotated basis ($\omega_{12}^{\pm} = (|0+\rangle \pm |1-\rangle)_{12}/\sqrt{2}$ and $\chi_{12}^{\pm} = (|0-\rangle \pm |1+\rangle)_{12}/\sqrt{2}$, here, $|+\rangle = \sqrt{1/4}|0\rangle + \sqrt{3/4}|1\rangle$ and $|-\rangle = \sqrt{3/4}|0\rangle - \sqrt{1/4}|1\rangle$), which is known only to Alice.

Step 2 Bob prepares an EPR pair of qubits 3 and 4. It is either in $\Psi_{34}^{\pm}$ and $\Phi_{34}^{\pm}$, or in $\omega_{34}^{\pm}$ and $\chi_{34}^{\pm}$, which is known only to Bob.

Step 3 Alice sends qubit 2 to Bob, and Bob sends qubit 4 to Alice.

Step 4 Alice and Bob each publicly confirm that the other received the qubits.

Step 5 Alice and Bob also announce which basis is used.

Step 6 If the received qubit was prepared in the rotated basis, Alice (or Bob) rotates back the received qubit into the Bell basis.

Step 7 Alice and Bob perform Bell measurements on 1 and 4, and 2 and 3, respectively.

Step 8 Alice and Bob announce which initial Bell states had been prepared.

Step 9 Knowing the initial Bell states prepared by each other and their own measurement result, they could determine which Bell measurement result the other had got.

Step 10 With the Bell measurement result they got, they share two key bits according to Table 1.

Table 1. "Id", "$+-$", "$\Phi\Psi$", and "Both" denote four combinations of possible entanglement swapping outcomes. "d"$\Rightarrow \{\Phi_{14}^{+}, \Phi_{23}^{+}\}$, $\{\Phi_{14}^{-}, \Phi_{23}^{-}\}$, $\{\Psi_{14}^{+}, \Psi_{23}^{+}\}$, $\{\Psi_{14}^{-}, \Psi_{23}^{-}\}$, and "$+-$" $\Rightarrow$ $\{\Phi_{14}^{+}, \Phi_{23}^{-}\}$, $\{\Phi_{14}^{-}, \Phi_{23}^{+}\}$, $\{\Psi_{14}^{+}, \Psi_{23}^{-}\}$, $\{\Psi_{14}^{-}, \Psi_{23}^{+}\}$, and "$\Phi\Psi$" $\Rightarrow$ $\{\Phi_{14}^{+}, \Psi_{23}^{+}\}$, $\{\Phi_{14}^{-}, \Psi_{23}^{-}\}$, $\{\Psi_{14}^{+}, \Phi_{23}^{+}\}$, $\{\Psi_{14}^{-}, \Phi_{23}^{-}\}$, and "Both" $\Rightarrow$ $\{\Phi_{14}^{+}, \Psi_{23}^{-}\}$, $\{\Phi_{14}^{-}, \Psi_{23}^{+}\}$, $\{\Psi_{14}^{+}, \Phi_{23}^{-}\}$, $\{\Psi_{14}^{-}, \Phi_{23}^{+}\}$.

	Id	$+-$	$\Phi\Psi$	Both
"00"	$\{\Phi_{14}^{+}, \Phi_{23}^{+}\}$	$\{\Psi_{14}^{-}, \Psi_{23}^{+}\}$	$\{\Phi_{14}^{-}, \Psi_{23}^{-}\}$	$\{\Psi_{14}^{+}, \Phi_{23}^{-}\}$
"01"	$\{\Psi_{14}^{-}, \Psi_{23}^{-}\}$	$\{\Phi_{14}^{+}, \Phi_{23}^{-}\}$	$\{\Psi_{14}^{+}, \Phi_{23}^{+}\}$	$\{\Phi_{14}^{-}, \Psi_{23}^{+}\}$
"10"	$\{\Psi_{14}^{+}, \Psi_{23}^{+}\}$	$\{\Phi_{14}^{-}, \Phi_{23}^{+}\}$	$\{\Psi_{14}^{-}, \Phi_{23}^{-}\}$	$\{\Phi_{14}^{+}, \Psi_{23}^{-}\}$
"11"	$\{\Phi_{14}^{-}, \Phi_{23}^{-}\}$	$\{\Psi_{14}^{+}, \Psi_{23}^{-}\}$	$\{\Phi_{14}^{+}, \Psi_{23}^{+}\}$	$\{\Psi_{14}^{-}, \Phi_{23}^{+}\}$

Song's scheme II is similar to scheme I. The only difference exists in the latter three steps.

Step 8′ Alice and Bob announce the result of their measurements.

Step 9′ Knowing the measurement results for both and their own prepared state, Alice and Bob could determine the initial state prepared by each other.

Step 10′ This enables them to share two key bits according to Table 2.

Table 2. "Id", "$+-$", "$\Phi\Psi$", and "Both" denote four combinations of possible prepared states.

	Id	$+-$	$\Phi\Psi$	Both
"00"	$\{\Phi_{12}^{+}, \Phi_{34}^{+}\}$	$\{\Psi_{12}^{-}, \Psi_{34}^{+}\}$	$\{\Phi_{12}^{-}, \Psi_{34}^{-}\}$	$\{\Psi_{12}^{+}, \Phi_{34}^{-}\}$
"01"	$\{\Psi_{12}^{-}, \Psi_{34}^{-}\}$	$\{\Phi_{12}^{+}, \Phi_{34}^{-}\}$	$\{\Psi_{12}^{+}, \Phi_{34}^{+}\}$	$\{\Phi_{12}^{-}, \Psi_{34}^{+}\}$
"10"	$\{\Psi_{12}^{+}, \Psi_{34}^{+}\}$	$\{\Phi_{12}^{-}, \Phi_{34}^{+}\}$	$\{\Psi_{12}^{-}, \Phi_{34}^{-}\}$	$\{\Phi_{12}^{+}, \Psi_{34}^{-}\}$
"11"	$\{\Phi_{12}^{-}, \Phi_{34}^{-}\}$	$\{\Psi_{12}^{+}, \Psi_{34}^{-}\}$	$\{\Phi_{12}^{+}, \Psi_{34}^{+}\}$	$\{\Psi_{12}^{-}, \Phi_{34}^{+}\}$

2.2. Optimized encoding method

From the above tables, we see that combinations of the measurement results and ones of the initial Bell states are used to discover secret keys in Song's scheme I and scheme II, respectively. Obviously, Alice and Bob have to announce their own initial Bell states or their own measurement results of the Bell state in order to form secret keys. By the way, their announcements are finished through a classical channel, moreover, there are a total of three times that classical channels are used in Song's schemes. It is used for the first time when Alice and Bob confirm that the transmitted qubits are received and announce which basis is used, and for the second time when announcing the initial Bell states or the measurement results, and for the third time when taking out a sample to check eavesdropping. Hereinto, the quantity of the transmitted information in the second time is the most. In general, classical channels are used as little as possible when designing a quantum communication scheme, which can achieve two advantages, one is to save a communication source, and the other is to debase the threat that the schemes are attacked. Next, by greatly reducing classical channels in Song's schemes, we propose a modified scheme, in which a novel encoding method is given. The modified scheme is simply described as follows. The former seven steps are the same as that in Song's schemes. The eighth step of the modified scheme may be written as: **Step 8** Now Alice and Bob know their own measurement results and initial Bell states. According to Table 3, they can share two key bits.

Now, let us give an explanation for Table 3. Please see the first lattice. Alice's or Bob's initial Bell states and the possible entanglement swapping results are one of (Φ^{+}, Φ^{+}), (Φ^{-}, Φ^{-}), (Ψ^{+}, Ψ^{+}), and (Ψ^{-}, Ψ^{-}). There are sixteen combinations, which correspond to the classical bits, "00". In the second lattice, they are one of (Φ^{+}, Φ^{-}), (Φ^{-}, Φ^{+}), (Ψ^{+}, Ψ^{-}), and (Ψ^{-}, Ψ^{+}). There are also sixteen combinations, which correspond to the classical bits, "01". For the remaining lattices in Table 3, the analysis is similar.

Table 3. In the bracket (•), the subscripts 12 and 14 states are Alice's initial Bell states and her entanglement swapping results (measurement results), respectively, and the subscripts 34 and 23 states are Bob's initial Bell states and his entanglement swapping results (measurement results), respectively. The bracket [•] denotes one possible entanglement swapping case.

"00"	$[(\Phi_{12}^{+},\Phi_{14}^{+}),(\Phi_{34}^{+},\Phi_{23}^{+})]$	$[(\Phi_{12}^{-},\Phi_{14}^{-}),(\Phi_{34}^{-},\Phi_{23}^{-})]$	$[(\Psi_{12}^{+},\Psi_{14}^{+}),(\Psi_{34}^{+},\Psi_{23}^{+})]$	$[(\Psi_{12}^{-},\Psi_{14}^{-}),(\Psi_{34}^{-},\Psi_{23}^{-})]$
	$[(\Phi_{12}^{-},\Phi_{14}^{-}),(\Phi_{34}^{+},\Phi_{23}^{+})]$	$[(\Phi_{12}^{+},\Phi_{14}^{+}),(\Phi_{34}^{-},\Phi_{23}^{-})]$	$[(\Psi_{12}^{-},\Psi_{14}^{-}),(\Psi_{34}^{+},\Psi_{23}^{+})]$	$[(\Psi_{12}^{+},\Psi_{14}^{+}),(\Psi_{34}^{-},\Psi_{23}^{-})]$
	$[(\Psi_{12}^{+},\Psi_{14}^{+}),(\Phi_{34}^{+},\Phi_{23}^{+})]$	$[(\Psi_{12}^{-},\Psi_{14}^{-}),(\Phi_{34}^{-},\Phi_{23}^{-})]$	$[(\Phi_{12}^{+},\Phi_{14}^{+}),(\Psi_{34}^{+},\Psi_{23}^{+})]$	$[(\Phi_{12}^{-},\Phi_{14}^{-}),(\Psi_{34}^{-},\Psi_{23}^{-})]$
	$[(\Psi_{12}^{-},\Psi_{14}^{-}),(\Phi_{34}^{+},\Phi_{23}^{+})]$	$[(\Psi_{12}^{+},\Psi_{14}^{+}),(\Phi_{34}^{-},\Phi_{23}^{-})]$	$[(\Phi_{12}^{-},\Phi_{14}^{-}),(\Psi_{34}^{+},\Psi_{23}^{+})]$	$[(\Phi_{12}^{+},\Phi_{14}^{+}),(\Psi_{34}^{-},\Psi_{23}^{-})]$
"01"	$[(\Phi_{12}^{+},\Phi_{14}^{-}),(\Phi_{34}^{+},\Phi_{23}^{-})]$	$[(\Phi_{12}^{-},\Phi_{14}^{+}),(\Phi_{34}^{-},\Phi_{23}^{+})]$	$[(\Psi_{12}^{+},\Psi_{14}^{-}),(\Psi_{34}^{+},\Psi_{23}^{-})]$	$[(\Psi_{12}^{-},\Psi_{14}^{+}),(\Psi_{34}^{-},\Psi_{23}^{+})]$
	$[(\Phi_{12}^{-},\Phi_{14}^{+}),(\Phi_{34}^{+},\Phi_{23}^{-})]$	$[(\Phi_{12}^{+},\Phi_{14}^{-}),(\Phi_{34}^{-},\Phi_{23}^{+})]$	$[(\Psi_{12}^{-},\Psi_{14}^{+}),(\Psi_{34}^{+},\Psi_{23}^{-})]$	$[(\Psi_{12}^{+},\Psi_{14}^{-}),(\Psi_{34}^{-},\Psi_{23}^{+})]$
	$[(\Psi_{12}^{+},\Psi_{14}^{-}),(\Phi_{34}^{+},\Phi_{23}^{-})]$	$[(\Psi_{12}^{-},\Psi_{14}^{+}),(\Phi_{34}^{-},\Phi_{23}^{+})]$	$[(\Phi_{12}^{+},\Phi_{14}^{-}),(\Psi_{34}^{+},\Psi_{23}^{-})]$	$[(\Phi_{12}^{-},\Phi_{14}^{+}),(\Psi_{34}^{-},\Psi_{23}^{+})]$
	$[(\Psi_{12}^{-},\Psi_{14}^{+}),(\Phi_{34}^{+},\Phi_{23}^{-})]$	$[(\Psi_{12}^{+},\Psi_{14}^{-}),(\Phi_{34}^{-},\Phi_{23}^{+})]$	$[(\Phi_{12}^{-},\Phi_{14}^{+}),(\Psi_{34}^{+},\Psi_{23}^{-})]$	$[(\Phi_{12}^{+},\Phi_{14}^{-}),(\Psi_{34}^{-},\Psi_{23}^{+})]$
"10"	$[(\Phi_{12}^{+},\Psi_{14}^{+}),(\Phi_{34}^{+},\Psi_{23}^{+})]$	$[(\Phi_{12}^{-},\Psi_{14}^{-}),(\Phi_{34}^{-},\Psi_{23}^{-})]$	$[(\Psi_{12}^{+},\Phi_{14}^{+}),(\Psi_{34}^{+},\Phi_{23}^{+})]$	$[(\Psi_{12}^{-},\Phi_{14}^{-}),(\Psi_{34}^{-},\Phi_{23}^{-})]$
	$[(\Phi_{12}^{-},\Psi_{14}^{-}),(\Phi_{34}^{+},\Psi_{23}^{+})]$	$[(\Phi_{12}^{+},\Psi_{14}^{+}),(\Phi_{34}^{-},\Psi_{23}^{-})]$	$[(\Psi_{12}^{-},\Phi_{14}^{-}),(\Psi_{34}^{+},\Phi_{23}^{+})]$	$[(\Psi_{12}^{+},\Phi_{14}^{+}),(\Psi_{34}^{-},\Phi_{23}^{-})]$
	$[(\Psi_{12}^{+},\Phi_{14}^{+}),(\Phi_{34}^{+},\Psi_{23}^{+})]$	$[(\Psi_{12}^{-},\Phi_{14}^{-}),(\Phi_{34}^{-},\Psi_{23}^{-})]$	$[(\Phi_{12}^{+},\Psi_{14}^{+}),(\Psi_{34}^{+},\Phi_{23}^{+})]$	$[(\Phi_{12}^{-},\Psi_{14}^{-}),(\Psi_{34}^{-},\Phi_{23}^{-})]$
	$[(\Psi_{12}^{-},\Phi_{14}^{-}),(\Phi_{34}^{+},\Psi_{23}^{+})]$	$[(\Psi_{12}^{+},\Phi_{14}^{+}),(\Phi_{34}^{-},\Psi_{23}^{-})]$	$[(\Phi_{12}^{-},\Psi_{14}^{-}),(\Psi_{34}^{+},\Phi_{23}^{+})]$	$[(\Phi_{12}^{+},\Psi_{14}^{+}),(\Psi_{34}^{-},\Phi_{23}^{-})]$
"11"	$[(\Phi_{12}^{+},\Psi_{14}^{-}),(\Phi_{34}^{+},\Psi_{23}^{-})]$	$[(\Phi_{12}^{-},\Psi_{14}^{+}),(\Phi_{34}^{-},\Psi_{23}^{+})]$	$[(\Psi_{12}^{+},\Phi_{14}^{-}),(\Psi_{34}^{+},\Phi_{23}^{-})]$	$[(\Psi_{12}^{-},\Phi_{14}^{+}),(\Psi_{34}^{-},\Phi_{23}^{+})]$
	$[(\Phi_{12}^{-},\Psi_{14}^{+}),(\Phi_{34}^{+},\Psi_{23}^{-})]$	$[(\Phi_{12}^{+},\Psi_{14}^{-}),(\Phi_{34}^{-},\Psi_{23}^{+})]$	$[(\Psi_{12}^{-},\Phi_{14}^{+}),(\Psi_{34}^{+},\Phi_{23}^{-})]$	$[(\Psi_{12}^{+},\Phi_{14}^{-}),(\Psi_{34}^{-},\Phi_{23}^{+})]$
	$[(\Psi_{12}^{+},\Phi_{14}^{-}),(\Phi_{34}^{+},\Psi_{23}^{-})]$	$[(\Psi_{12}^{-},\Phi_{14}^{+}),(\Phi_{34}^{-},\Psi_{23}^{+})]$	$[(\Phi_{12}^{+},\Psi_{14}^{-}),(\Psi_{34}^{+},\Phi_{23}^{-})]$	$[(\Phi_{12}^{-},\Psi_{14}^{+}),(\Psi_{34}^{-},\Phi_{23}^{+})]$
	$[(\Psi_{12}^{-},\Phi_{14}^{+}),(\Phi_{34}^{+},\Psi_{23}^{-})]$	$[(\Psi_{12}^{+},\Phi_{14}^{-}),(\Phi_{34}^{-},\Psi_{23}^{+})]$	$[(\Phi_{12}^{-},\Psi_{14}^{+}),(\Psi_{34}^{+},\Phi_{23}^{-})]$	$[(\Phi_{12}^{+},\Psi_{14}^{-}),(\Psi_{34}^{-},\Phi_{23}^{+})]$

2.3. Comparison of QKD schemes' efficiencies

Clearly, the modified scheme is much simpler than Song's schemes. First, its steps are fewer, only eight. Secondly, the requirements that the measurement results or the initial Bell states are announced do not exist, which makes this modified scheme have a high efficiency. In the following, let us calculate its efficiency by employing Cabello's efficiency definition[26]

$$\eta = \frac{b_{\rm s}}{q_{\rm t}+b_{\rm t}}. \tag{2}$$

Here, η denotes the efficiency; $b_{\rm s}$ is the expected secret bits received, while $q_{\rm t}$ and $b_{\rm t}$ are the qubit used and the classical bits exchanged between Alice and Bob, respectively. Obviously, in the modified scheme, $b_{\rm s}$ equals 2 bits, and $q_{\rm t}$ and $b_{\rm t}$ equal 2 and 1 bits, respectively. So the efficiency of the modified scheme η equals $2/3$. However, the efficiency of Song's scheme η only equals $2/7$ since its $b_{\rm t}$ equals 5 bits. As a matter of fact, the main reason that the efficiency of the modified scheme is higher than Song's is that, the encoding method in the former is more ingenious than those in the latter. By the way, in essence, our encoding method is slightly similar to that in Ref. [9].

2.4. QKD schemes stand against entangle-measure attack

Notice that the modified scheme as well as Song's schemes need a process to check eavesdropping. Also by taking out a sample and announcing both the correlated measurement results and the initial states, they can judge whether eavesdropping exists. In addition, we see that, in Ref. [4], Song only listed the intercept-resend attack in order to demonstrate that the process is efficient. Obviously, this is not enough. In what follows, we will show that the process is also efficient for standing against the entangle-measure attack.

In advance, an eavesdropper (Eve) prepares an auxiliary qubit that is in $|\varepsilon\rangle$. When qubit 2 is traveling from Alice to Bob, Eve intercepts it, and then performs a unitary operation $U_{\rm E}$ on it and the auxiliary qubit. Without loss of generality, the system state of qubits 1, 2, and the auxiliary qubit can be written as:

$$\begin{aligned} U_{\rm E}|\psi\rangle_{12}|\varepsilon\rangle \;=\; & |00\rangle_{12}|\varepsilon_{00}\rangle + |01\rangle_{12}|\varepsilon_{01}\rangle + |10\rangle_{12}|\varepsilon_{10}\rangle \\ & + |11\rangle_{12}|\varepsilon_{11}\rangle. \end{aligned} \tag{3}$$

Here, $\psi \in \{\Psi^{\pm}, \Phi^{\pm}\}$. For qubit 4, what Eve does is the same as that for qubit 2. So the system state of qubits 3, 4, and the auxiliary qubit can be written as:

$$\begin{aligned} U_{\rm E}|\psi\rangle_{34}|\varepsilon\rangle \;=\; & |00\rangle_{34}|\varepsilon_{00}\rangle + |01\rangle_{34}|\varepsilon_{01}\rangle + |10\rangle_{34}|\varepsilon_{10}\rangle \\ & + |11\rangle_{34}|\varepsilon_{11}\rangle. \end{aligned} \tag{4}$$

In the modified scheme (and Song's schemes), since each EPR pair prepared by Alice and Bob is in Bell basis or rotated basis and there is a process to switch the basis before measuring, this indirectly denotes that two sets of bases are used in checking eavesdropping. When Alice and Bob choose the Bell basis as the measurement basis, in order to avoid introducing error, the following equation must be satisfied

$$|\varepsilon_{01}\rangle = |\varepsilon_{10}\rangle = \mathbf{0}, \tag{5}$$

where $\mathbf{0}$ denotes a null vector. That is, the system states are:

$$U_{\rm E}|\psi\rangle_{12}|\varepsilon\rangle = |00\rangle_{12}|\varepsilon_{00}\rangle + |11\rangle_{12}|\varepsilon_{11}\rangle, \tag{6}$$

$$U_{\rm E}|\psi\rangle_{34}|\varepsilon\rangle = |00\rangle_{34}|\varepsilon_{00}\rangle + |11\rangle_{34}|\varepsilon_{11}\rangle. \tag{7}$$

On the other hand, when Alice and Bob choose a rotated basis as the measurement basis, the following constraint can be similarly deduced

$$|\varepsilon_{00}\rangle = |\varepsilon_{11}\rangle. \tag{8}$$

Thus, $U_{\rm E}|\psi\rangle|\varepsilon\rangle = |\psi\rangle \otimes |\varepsilon\rangle$, that is, $U_{\rm E}|\psi\rangle|\varepsilon\rangle$ is a product of a Bell state and a single qubit. This implies that Eve cannot gain any useful information from observing the auxiliary qubit. In other words, if Eve wants to eavesdrop secret keys by using this attack, his action must introduce errors. Therefore, the processes to check eavesdropping in the modified scheme and Song's schemes are also efficient for standing against the entangle-measure attack.

3. Extension of optimized encoding method

Next, we will investigate whether the encoding method may be extended to QKD schemes composed of other entanglement states. Along the qubit number, we find that the encoding method cannot be used to the QKD scheme composed of any three-qubit entanglement state. However, in four-qubit entanglement states, it seems that it also adapts to the QKD scheme composed of G states.[27] In the following, we will concretely demonstrate this.

(I) Alice prepares qubits 1, 2, 3, 4 either in the generalized Bell basis $\{|g_1\rangle, |g_2\rangle, ..., |g_{16}\rangle\}$ (here, $|g_n\rangle = U^i U^j |g_1\rangle$, $|g_1\rangle = (|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)/2$, $n = 1, ..., 16$ and $U^i, U^j \in \{I, \sigma_x, \sigma_y, \sigma_z\}$), or in the rotated basis $\{|\rho_1\rangle, |\rho_2\rangle, ..., |\rho_{16}\rangle\}$ (here, $\langle\rho_n|\rho_m\rangle = \delta_{nm}$, $\sum_{n=1}^{16} = |\rho_n\rangle\langle\rho_n| = I$, $|\rho_n\rangle = U_r|g_n\rangle$ and $0 < \langle\rho_n|g_n\rangle < 1$), which is known only to Alice.

(II) Bob also prepares qubits 5, 6, 7, 8 either in the generalized Bell basis, or in the rotated basis, which is known only to Bob.

(III) Alice sends qubits 3, 4 to Bob, and Bob sends qubits 5, 6 to Alice.

(IV) Alice and Bob publicly confirm that the two qubits of the other side have been received by each other.

(V) Alice and Bob also announce which bases are used in preparing the four-qubit entangled state.

(VI) If the received qubits were prepared in the rotated basis, Alice (or Bob) rotates back them into the generalized Bell basis.

(VII) They perform generalized Bell basis measurements on qubits 1, 2, 5, 6, and qubits 3, 4, 7, 8, respectively. Obviously, there is an entanglement swapping process. Suppose that Alice's qubits 1, 2, 3, 4 and Bob's qubits 5, 6, 7, 8 are in $|g_{10}\rangle$ and $|g_1\rangle$, respectively, and the whole system evolves as follows:

$$\begin{aligned}
&|g_{10}\rangle_{1234} \otimes |g_1\rangle_{5678} \\
=\ &\frac{1}{4}(-|g_1\rangle_{1256}|g_{10}\rangle_{3478} + |g_2\rangle_{1256}|g_9\rangle_{3478} \\
&- |g_3\rangle_{1256}|g_{12}\rangle_{3478} + |g_4\rangle_{1256}|g_{11}\rangle_{3478} - |g_5\rangle_{1256}|g_{14}\rangle_{3478} \\
&+ |g_6\rangle_{1256}|g_{13}\rangle_{3478} - |g_7\rangle_{1256}|g_{16}\rangle_{3478} + |g_8\rangle_{1256}|g_{15}\rangle_{3478} \\
&- |g_9\rangle_{1256}|g_2\rangle_{3478} + |g_{10}\rangle_{1256}|g_1\rangle_{3478} - |g_{11}\rangle_{1256}|g_4\rangle_{3478} \\
&+ |g_{12}\rangle_{1256}|g_3\rangle_{3478} - |g_{13}\rangle_{1256}|g_6\rangle_{3478} + |g_{14}\rangle_{1256}|g_5\rangle_{3478} \\
&- |g_{15}\rangle_{1256}|g_8\rangle_{3478} + |g_{16}\rangle_{1256}|g_7\rangle_{3478}).
\end{aligned} \tag{9}$$

(VIII) Since Alice and Bob know their own measurement result and their own initial generalized Bell state, according to Table 4, they can share four key bits.

In each lattice of Table 4, the 16×16 entanglement swapping cases correspond to a four-bit key. Here, the so-called "entanglement swapping case" may be explained as follows. For example, $[(|g_1\rangle_{1234}, |g_1\rangle_{1256}), (|g_1\rangle_{5678}, |g_1\rangle_{3478})]$ belongs to one entanglement swapping case. In it, $|g_1\rangle_{1234}$ and $|g_1\rangle_{5678}$ are initially prepared with G states, and $|g_1\rangle_{1256}$ and $|g_1\rangle_{3478}$ are one possible measurement result after swapping the entanglement of the G states. In addition, since the number 16×16 is too big, here only four indicative cases are listed and others are replaced with suspension points. For clarity, we need further to point out the information that suspension points contain. Let us take the second lattice as an example to explain this. From $[(|g_3\rangle_{1234}, |g_1\rangle_{1256}), (|g_3\rangle_{5678}, |g_1\rangle_{3478})]$ to $[(|g_3\rangle_{1234}, |g_1\rangle_{1256}), (|g_{14}\rangle_{5678}, |g_{16}\rangle_{3478})]$, the array rule of the row is as follows. The contents in all first parentheses, that is, $(|g_3\rangle_{1234}, |g_1\rangle_{1256})$ remain the same, but the ones in all the second parentheses are different. The set of the second states in all the second parentheses is $\{|g_1\rangle_{3478}, |g_2\rangle_{3478}, ..., |g_{16}\rangle_{3478}\}$, and that of the first states is $\{I\sigma_z|g_1\rangle_{3478}, I\sigma_z|g_2\rangle_{3478}, ..., I\sigma_z|g_{16}\rangle_{3478}\}$. Obviously, the set of the first states can be produced based on the set of the second states. From $[(|g_3\rangle_{1234}, |g_1\rangle_{1256}), (|g_3\rangle_{5678}, |g_1\rangle_{3478})]$ to $[(|g_{14}\rangle_{1234}, |g_{16}\rangle_{1256}), (|g_3\rangle_{5678}, |g_1\rangle_{3478})]$, the array rule of the column is similar to that of the row, and the only difference is that the contents in all the second parentheses remain the same and the ones in all the first parentheses will regularly change. For other lattices of Table 4, the array rules are similar.

As in Song's schemes, for detecting eavesdropping, also Alice and Bob need to take out a sample from the above raw keys in this QKD scheme composed of G states. By the way, the sample is not big as long as it can provide an analysis of the error rate. Then, they publicly announce the measurement results and the initial generalized Bell states about the sample, so that Alice and Bob can judge whether the quantum channel between them is attacked. If the channel is safe, getting rid of the sample, they will establish the final mature keys. In fact, the manners to check eavesdropping in Song's QKD schemes and two proposed schemes are essentially the same as that in the BBM92 scheme,[2] that is, two sets of no-orthonormal quantum states (measuring basis) are employed.

In the end, there are two questions that arise. (i) In Step 7, we see that Alice and Bob perform generalized Bell basis measurements on qubits 1, 2, 5, 6, and qubits 3, 4, 7, 8, respectively. In fact, if Bob sends not qubits 5, 6, but qubits 7, 8, to Alice in Step 3, that is, they perform generalized Bell basis measurements on qubits 1, 2, 7, 8, and qubits 3, 4, 5, 6,

Table 4. The subscripts 1234 and 1256 states are Alice's preparing states and her measurement results, respectively, and the subscripts 5678 and 3478 states are Bob's preparing states and his measurement results, respectively. The content in the bracket shows one possible entanglement swapping case.

"0000"	$[(\|g_1\rangle_{1234},\|g_1\rangle_{1256}),(\|g_1\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_1\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{16}\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_{16}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_1\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{16}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{16}\rangle_{5678},\|g_{16}\rangle_{3478})]$
"0001"	$[(\|g_3\rangle_{1234},\|g_1\rangle_{1256}),(\|g_3\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_3\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{14}\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_{14}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_3\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{14}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{14}\rangle_{5678},\|g_{16}\rangle_{3478})]$
"0010"	$[(\|g_5\rangle_{1234},\|g_1\rangle_{1256}),(\|g_5\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{12}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{12}\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_{12}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_5\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{12}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{12}\rangle_{5678},\|g_{16}\rangle_{3478})]$
"0100"	$[(\|g_2\rangle_{1234},\|g_1\rangle_{1256}),(\|g_2\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_2\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{15}\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_{15}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_2\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{15}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{15}\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1000"	$[(\|g_9\rangle_{1234},\|g_1\rangle_{1256}),(\|g_9\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_9\rangle_{1234},\|g_1\rangle_{1256}),(\|g_8\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_8\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_9\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_8\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_8\rangle_{5678},\|g_{16}\rangle_{3478})]$
"0011"	$[(\|g_7\rangle_{1234},\|g_1\rangle_{1256}),(\|g_7\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_7\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{10}\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_{10}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_7\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{10}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{10}\rangle_{5678},\|g_{16}\rangle_{3478})]$
"0110"	$[(\|g_6\rangle_{1234},\|g_1\rangle_{1256}),(\|g_6\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_6\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{11}\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_{11}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_6\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{11}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{11}\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1100"	$[(\|g_{10}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{10}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{10}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_7\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_7\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{10}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_7\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_7\rangle_{5678},\|g_{16}\rangle_{3478})]$
"0101"	$[(\|g_4\rangle_{1234},\|g_1\rangle_{1256}),(\|g_4\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_4\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{13}\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_{13}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_4\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{13}\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{13}\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1001"	$[(\|g_{11}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{11}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{11}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_6\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_6\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{11}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_6\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_6\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1010"	$[(\|g_{13}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{13}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{13}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_4\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_4\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{13}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_4\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_4\rangle_{5678},\|g_{16}\rangle_{3478})]$
"0111"	$[(\|g_8\rangle_{1234},\|g_1\rangle_{1256}),(\|g_8\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_8\rangle_{1234},\|g_1\rangle_{1256}),(\|g_9\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_9\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_8\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_9\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_9\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1011"	$[(\|g_{15}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{15}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{15}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_2\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_2\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{15}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_2\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_2\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1101"	$[(\|g_{12}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{12}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{12}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_5\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_5\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{12}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_5\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_5\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1110"	$[(\|g_{14}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{14}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{14}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_3\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_3\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{14}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_3\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_3\rangle_{5678},\|g_{16}\rangle_{3478})]$
"1111"	$[(\|g_{16}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_{16}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_{16}\rangle_{1234},\|g_1\rangle_{1256}),(\|g_1\rangle_{5678},\|g_{16}\rangle_{3478})]$
	...	...	...
	$[(\|g_1\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_{16}\rangle_{5678},\|g_1\rangle_{3478})]$	...	$[(\|g_1\rangle_{1234},\|g_{16}\rangle_{1256}),(\|g_1\rangle_{5678},\|g_{16}\rangle_{3478})]$

respectively, the optimized encoding method can also work. At the moment, we cannot help asking that if Alice sends qubits 2, 4 to Bob, and Bob sends qubits 6, 8 to Alice, can it still work? (ii) Except four-qubit G states, can the optimized encoding method adapt to the QKD schemes composed of other four-qubit entangled states, like, four-qubit GHZ states,[28] four-qubit W states,[29] four-qubit cluster states,[30,31] four-qubit χ states,[32,33] etc.? In addition, with the further increase of the qubit number, can the optimized encoding method adapt to the QKD scheme composed of N-qubit ($N > 4$) entangled states? In our opinion, these questions are interesting and can be studied in the future.

4. Summary

In summary, we have proposed an optimized encoding method for Song's QKD schemes, which makes the efficiencies of the schemes improve trebly. The proposed optimized encoding method is not only interesting, but also saves plenty of classical sources for the QKD schemes with the symmetry feature. In other words, our optimized encoding method is economical if it is practically applied. Moreover, we discuss whether the optimized encoding method has more theoretical application. As a result, it is detected that it also adapts to the QKD scheme composed of four-qubit G states. We will continue further research on its application after this work. Finally, let us compare our optimized encoding method with Song's encoding methods[4] from a security aspect. Obviously, ours is safer than Song's scheme because an eavesdropper needs to guess one result from 4 possible cases if using Song's method, but one result from 64 possible cases if using ours.

Acknowldgment

I thank my parents for their encouragements.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings*, Bangalore, India (IEEE, New York, 1984) p. 175
[2] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[3] Deng F G and Long G L 2003 *Phys. Rev. A* **68** 042315
[4] Song D 2004 *Phys. Rev. A* **69** 034301
[5] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[6] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[7] He G Q and Zeng G H 2006 *Chin. Phys.* **15** 1284
[8] Chen P, Li Y S, Deng F G and Long G L 2007 *Commun. Theor. Phys.* **47** 49
[9] Gao G 2009 *Commun. Theor. Phys.* **51** 820
[10] Gao G 2008 *Opt. Commun.* **281** 876
[11] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **78** 022321
[12] Wang C, Xiao L, Wang W, Zhang G and Long G L 2009 *J. Opt. Soc. Am. B* **26** 2072
[13] Zhang X Z, Gong W G, Tan Y G, Ren Z Z and Guo X T 2009 *Chin. Phys. B* **18** 2143
[14] Shen Y, Peng X, Yang J and Guo H 2011 *Phys. Rev. A* **83** 052304
[15] Yang J, Xu B, Peng X and Guo H 2012 *Phys. Rev. A* **85** 052302
[16] Fung C F, Ma X, Chau H F and Cai Q 2012 *Phys. Rev. A* **85** 032308
[17] Deng F G, Liu X S, Ma Y J, Xiao L and Long G L 2002 *Chin. Phys. Lett.* **19** 893
[18] Huang P, He G, Fang J and Zeng G 2013 *Phys. Rev. A* **87** 012317
[19] Zhou Y Y, Zhou X J, Tian P G and Wang Y J 2013 *Chin. Phys. B* **22** 010305
[20] Li H W, Yin Z Q, Chen W, Wu S, Guo G C and Han Z F 2014 *Phys. Rev. A* **89** 032302
[21] Kwiat P G, Mattle K, Weinfurter H and Zeilinger A 1995 *Phys. Rev. Lett.* **75** 4337
[22] Turchette Q A, Wood C S, King B E, *et al.* 1998 *Phys. Rev. Lett.* **81** 3631
[23] Zheng S B and Guo G C 2000 *Phys. Rev. Lett.* **85** 2392
[24] Duan L M 2002 *Phys. Rev. Lett.* **88** 170402
[25] Zukowski M *et al.* 1993 *Phys. Rev. Lett.* **71** 4287
[26] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[27] Rigolin G 2005 *Phys. Rev. A* **71** 032303
[28] Greenberger D M, Horne M A and Zeilinger A 1989 in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by Kafatos M (Dordrecht: Kluwer Academic) pp. 69–72
[29] Zeilinger A, Horne M A and Greenberger D M 1992 in *Proceedings of Squeezed States and Quantum Uncertainty*, edited by Han D, Kim Y S, and Zachary W W, NASA Conference Publication No. 3135 (NASA, Washington, DC, 1992), pp. 73–81
[30] Briegel H J and Raussendorf R 2001 *Phys. Rev. Lett.* **86** 910
[31] Wen J J, Yeon K H, Wang H F and Zhang S 2014 *Chin. Phys. B* **23** 040301
[32] Yeo Y and Chua W K 2006 *Phys. Rev. Lett.* **96** 060502
[33] Wang H F and Zhang S 2009 *Phys. Rev. A* **79** 042336