Int J Theor Phys (2010) 49: 1870–1877
DOI 10.1007/s10773-010-0365-7

# Quantum Key Distribution Using a $\chi$-Type State

**Gan Gao**

Received: 16 February 2010 / Accepted: 16 April 2010 / Published online: 30 April 2010


**Abstract** By swapping the entanglement of $\chi$-type state, we propose a quantum key distribution protocol, in which only Alice needs to prepare $\chi$-type states and transmit a particle sequence. Both Alice and Bob need to perform $\chi$-type state measurements.

**Keywords** Quantum key distribution · $\chi$-Type state · Entanglement swapping

## 1 Introduction

Quantum key distribution (QKD) [1–24], combining quantum mechanics and traditional cryptography, allows two remote parties (Alice and Bob) to share a secret key, and the security of the shared key is ensured by virtue of the laws of quantum physics. In 1984, the first key distribution protocol [1] that used quantum states from nonorthogonal bases was proposed by Bennett and Brassard. Customarily, we call it BB84 protocol, in which the quantum entanglement isn't utilized. In 1991, by sharing the quantum entanglement between two participants, Ekert proposed a QKD protocol, that is, the well-known E91 protocol [2]. Subsequently, another QKD protocols that also use the quantum entanglement are put forward [4, 9–18]. Clearly, the quantum entanglement is a kind of very useful and important source in quantum cryptography, and itself has some interesting phenomenons. For example, the quantum entanglement may be swapped, that is, the so-called quantum entanglement swapping. Simply speaking, entanglement swapping can entangle two quantum systems that have never interacted each other before. In terms of this phenomenon, some QKD protocols have been proposed by a group of people [9–18], thereinto, the representational protocols have Cabello protocol [10, 11], Song protocol [16] and so on.

G. Gao (✉)
Department of Electrical Engineering, Tongling University, Tongling 244000, China
e-mail: gaogan0556@163.com

G. Gao
Engineering Technology Research Center of Optoelectronic Technology Appliance (Cultivating Base), Tongling University, AnHui Province, Tongling 244000, China

Recently, in research of the teleportation [25–29] of an arbitrary two-qubit state, Yeo and Chua [30] proposed a four-particle entangled state, say $\chi$-type state, which is a new and genuine four-particle entanglement state. Moreover, they made a detailed comparison between $\chi$-type state and the other four-particle states: GHZ state and W state. Subsequently, Wang and Yang [31] gave a scheme to generate this $\chi$-type state in an ion-trap system, and they still shew that all sixteen states can be discriminated. There are still other schemes that a $\chi$-type state is generated, such as, Wang scheme [32], Wang-Zhang scheme [33], Shen et al. scheme [34]. Thereinto, Wang-Zhang scheme [33] is a simplest experimental one, because only linear optical elements and conventional photon detectors are used in it, which greatly decrease the experimental difficulty. On the other hand, some people are interesting in the application of $\chi$-type state, such as, Xiu et al. [35] use it to put forward a DSQC protocol. In this paper, by employing the $\chi$-type state, we propose a QKD protocol. So to speak, this is another new application of $\chi$-type state. Before describing our QKD protocol, firstly, let us define all sixteen $\chi$-type states as follows:

$$\begin{aligned}\left|\chi^{00}\right\rangle_{abcd} &= \frac{\sqrt{2}}{4}\big(|0000\rangle - |0101\rangle - |0011\rangle \\ &\quad + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle\big)_{abcd} \\ &= \frac{1}{2}\big(|\Psi_1^-\rangle|1+\rangle_{bd} + |\Psi_1^+\rangle|1-\rangle_{bd} + |\Phi_1^-\rangle|0+\rangle_{bd} + |\Phi_1^+\rangle|0-\rangle_{bd}\big) \\ &= \frac{1}{2}\big(-|\Psi_2^-\rangle|+1\rangle_{bd} + |\Psi_2^+\rangle|-1\rangle_{bd} + |\Phi_2^+\rangle|+0\rangle_{bd} + |\Phi_2^-\rangle|-0\rangle_{bd}\big) \qquad (1)\end{aligned}$$

Here, $|\Psi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle \pm |\phi^-\rangle)$, $|\Phi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle \pm |\psi^-\rangle)$, $|\Psi_2^\pm\rangle = \frac{1}{\sqrt{2}}(|\phi^-\rangle \pm |\psi^-\rangle)$, $|\Phi_2^\pm\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle \pm |\psi^+\rangle)$, $|\psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$, $|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The other fifteen $\chi$-type states can be obtained by the following way:

$$\left|\chi^{ij}\right\rangle_{abcd} = \sigma_a^i \sigma_c^j |\chi^{00}\rangle_{abcd} \quad (i, j = 0, 1, 2, 3) \qquad (2)$$

Here, $\sigma^i$ belongs to one of four Pauli operators: $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $\sigma_y = |1\rangle\langle 0| - |0\rangle\langle 1|$, $\sigma_x = |0\rangle\langle 1| - |1\rangle\langle 0|$. In addition, we still define two sets of measurement basis:

$$PMB_1 = \big\{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\big\} \qquad BMB_1 = \big\{|\Psi_1^+\rangle, |\Psi_1^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle\big\}$$
$$PMB_2 = \big\{|+0\rangle, |-0\rangle, |+1\rangle, |-1\rangle\big\} \qquad BMB_2 = \big\{|\Psi_2^+\rangle, |\Psi_2^-\rangle, |\Phi_2^+\rangle, |\Phi_2^-\rangle\big\}$$

## 2 Our Quantum Key Distribution Protocol

Secret keys will be generated between two legitimate parties, Alice and Bob, and our QKD protocol can be realized in the following steps:

(1) Alice prepares a batch of four-particle entanglement pairs, which each pair is in $|\chi^{00}\rangle_{abcd}$. And then, she arranges these entanglement pairs into one sequence $[P_1^a, P_1^b, P_1^c, P_1^d, P_2^a, P_2^b, P_2^c, P_2^d, \ldots, P_n^a, P_n^b, P_n^c, P_n^d]$. Here, the $a$, $b$, $c$ and $d$ represent four particles in one $\chi$-type state and the subscripts $1, 2, 3, \ldots$ and $n$ indicate the orders of entanglement pairs in the sequence. Alice takes particles $a$, $c$ from each pair to form an ordered sequence $[P_1^a, P_1^c, P_2^a, P_2^c, \ldots, P_n^a, P_n^c]$ (simply say $P_1$ sequence), and the remaining partner particles

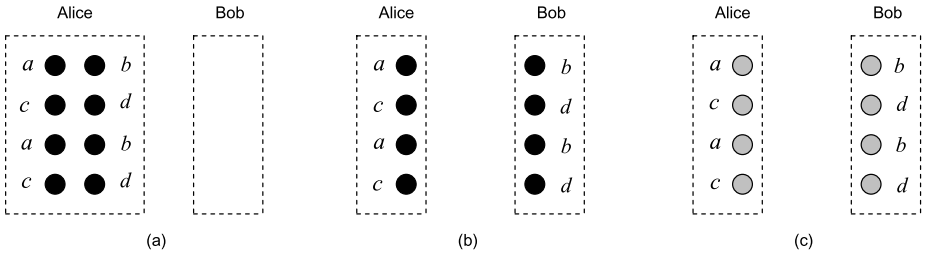


**Fig. 1** Illustrating of quantum key distribution protocol using a $\chi$-type state. Here, the case after dividing groups is shown, that is to say, we take out one group as an example to show the idea of our QKD protocol. The small balls denote the particles. In (**c**), that four balls in each side become gray denotes $\chi$-type state measurement

$b$, $d$ form another sequence $[P_1^b, P_1^d, P_2^b, P_2^d, \ldots, P_n^b, P_n^d]$ (simply say $P_2$ sequence). Alice sends $P_2$ sequence to Bob and retains $P_1$ sequence in her site.

(2) After it is confirmed that Bob have received the $P_2$ sequence, Alice and Bob check whether it is attacked during the transmission. In the $P_2$ sequence, Alice randomly selects some particles $b$, $d$ and asks Bob to randomly use the basis $PMB_1$ or $PMB_2$ to measure them. Moreover, she still requires Bob to tell her his measurement outcomes. And then, Alice uses the suitable basis to measure the corresponding particles $a$, $c$ of one entanglement pair in the $P_1$ sequence. Incidentally, if Bob's measuring basis is $PMB_1$, Alice should select $BMB_1$; if Bob's is $PMB_2$, Alice selects $BMB_2$. According to the ahead $\chi$-type state expressions, that is, (1), their measurement outcomes are correlated if there is no eavesdropping in the quantum channel. By comparing measurement outcomes, Alice can analyze the error rate of $P_2$ sequence transmission. If the error rate goes beyond the threshold, the process is aborted. Otherwise, the process goes on.

(3) Alice and Bob divide these four-particle entanglement pairs (except for the entanglement pairs used to check eavesdropping) into plenty of groups. There are two pairs in each group. For clarity, let us take one group as an example, as shown in (a) of Fig. 1. The next task is to generate secret keys between two parties. According to the ahead content, Alice now holds particles $a$, $c$, $a$, $c$ and Bob holds particles $b$, $d$, $b$, $d$. Alice performs $\chi$-type state measurement on particles $a$, $c$, $a$, $c$, and Bob performs $\chi$-type state measurement on particles $b$, $d$, $b$, $d$. Obviously, the entanglement swapping of $\chi$-type state occurs, and the state of the whole system evolves as follows:

$$
\begin{aligned}
|\chi^{00}\rangle_{abcd}|\chi^{00}\rangle_{abcd} = \frac{1}{4}\big(&|\chi^{00}\rangle_{acac}|\chi^{00}\rangle_{bdbd} + |\chi^{10}\rangle_{acac}|\chi^{10}\rangle_{bdbd} + |\chi^{03}\rangle_{acac}|\chi^{03}\rangle_{bdbd} \\
&+ |\chi^{13}\rangle_{acac}|\chi^{13}\rangle_{bdbd} + |\chi^{21}\rangle_{acac}|\chi^{21}\rangle_{bdbd} + |\chi^{31}\rangle_{acac}|\chi^{31}\rangle_{bdbd} \\
&+ |\chi^{22}\rangle_{acac}|\chi^{22}\rangle_{bdbd} + |\chi^{01}\rangle_{acac}|\chi^{12}\rangle_{bdbd} + |\chi^{32}\rangle_{acac}|\chi^{32}\rangle_{bdbd} \\
&+ |\chi^{12}\rangle_{acac}|\chi^{01}\rangle_{bdbd} + |\chi^{11}\rangle_{acac}|\chi^{02}\rangle_{bdbd} + |\chi^{02}\rangle_{acac}|\chi^{11}\rangle_{bdbd} \\
&+ |\chi^{20}\rangle_{acac}|\chi^{33}\rangle_{bdbd} + |\chi^{23}\rangle_{acac}|\chi^{30}\rangle_{bdbd} + |\chi^{30}\rangle_{acac}|\chi^{23}\rangle_{bdbd} \\
&+ |\chi^{33}\rangle_{acac}|\chi^{20}\rangle_{bdbd}\big)
\end{aligned}
\tag{3}
$$

It is evident that Alice's measurement outcome can be deduced by Bob according to his measurement outcome, similarly, Bob's can also be deduced by Alice according to hers. In advance, they have a agreement that $|\chi^{00}\rangle, |\chi^{01}\rangle, |\chi^{02}\rangle, \ldots, |\chi^{33}\rangle$ are encoded into

0000, 0001, 0010, ..., 1111, respectively. So secret keys are generated between Alice and Bob successfully.

So far, we use the $\chi$-type states to successfully put forward a QKD protocol, in which only Alice needs to prepare the $\chi$-type states and transmit the particle sequence, and both Alice and Bob need to perform $\chi$-type state measurements.

## 3 Security of Quantum Key Distribution Protocol

As we all know, the security problem is the most basic problem in quantum communication. If a protocol isn't secure, even if its configuration is rather graceful, it is meaningless. Obviously, the security is important for quantum communication protocols. In what follows, we start to discuss the security of the above QKD protocol. For eavesdropping some useful messages, the eavesdropper has to attack the $P_2$ sequence during its transmission. In general, the attack methods that she used to employ are as follows:

(i) *The intercept-resend attack*. During the transmission of particles $b$, $d$ between Alice and Bob, the eavesdropper intercepts them. In addition, the eavesdropper prepares another $\chi$-type state, $|\chi^{00}\rangle_{a'b'c'd'}$ in advance, and sends particles $b'$ and $d'$, instead of $b$ and $d$, to Bob. So, the particles that Bob really measures are not $b$ and $d$, but $b'$ and $d'$ in the security-check. Of course, both Alice and Bob don't know this. When Bob announces his measurement outcome (assuming that his measurement outcome is $|0-\rangle$) via a classical channel, the eavesdropper also obtains this information and chooses $PMB_1$ to measure particles $b$ and $d$. Since the system state randomly collapses, the probability that the measurement outcome on particles $b$ and $d$ is similar to that on particles $b'$ and $d'$ is 25%. So the eavesdropper will introduce some errors if eavesdropping. Obviously, the replacing trick of the eavesdropper will be detected with a bigger probability while Alice and Bob use two sets of measuring basis to check the channel security.

(ii) *The entangle-measure attack*. The eavesdropper intercepts particles $b$ and $d$ while they are traveling between Alice and Bob. Afterwards, she performs unitary operation on the intercepted particles, that is particles $b$ and $d$, and the auxiliary particle $e$ that she prepares in advance. By observing the auxiliary particles, the eavesdropper wants to get some useful messages. In what follows, we will analysis whether her eavesdropping is feasible. In terms of the ahead content, we know that the eavesdropper has access to only two particles of four-particle entanglement pair, that is, particles $b$ and $d$. For the eavesdropper, particles $b$ and $d$ are in the mix state, and its density matrix is $\rho = \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$ (particles $a$ and $c$ are traced out). Suppose that the eavesdropper's auxiliary particle $e$ is prepared in $|\varepsilon\rangle$. And her general operation may be written as follows:

$$
\begin{aligned}
U_E\colon\ |00\rangle_{bd}|\varepsilon\rangle &\to |00\rangle_{bd}|\varepsilon_1\rangle + |01\rangle_{bd}|\varepsilon_1'\rangle + |10\rangle_{bd}|\varepsilon_1''\rangle + |11\rangle_{bd}|\varepsilon_1'''\rangle \\
|01\rangle_{bd}|\varepsilon\rangle &\to |00\rangle_{bd}|\varepsilon_2\rangle + |01\rangle_{bd}|\varepsilon_2'\rangle + |10\rangle_{bd}|\varepsilon_2''\rangle + |11\rangle_{bd}|\varepsilon_2'''\rangle \\
|10\rangle_{bd}|\varepsilon\rangle &\to |00\rangle_{bd}|\varepsilon_3\rangle + |01\rangle_{bd}|\varepsilon_3'\rangle + |10\rangle_{bd}|\varepsilon_3''\rangle + |11\rangle_{bd}|\varepsilon_3'''\rangle \\
|11\rangle_{bd}|\varepsilon\rangle &\to |00\rangle_{bd}|\varepsilon_4\rangle + |01\rangle_{bd}|\varepsilon_4'\rangle + |10\rangle_{bd}|\varepsilon_4''\rangle + |11\rangle_{bd}|\varepsilon_4'''\rangle \qquad (4)
\end{aligned}
$$

Here, all $|\varepsilon_i\rangle$, $|\varepsilon_i'\rangle$, $|\varepsilon_i''\rangle$, $|\varepsilon_i'''\rangle$ ($i \in \{1, 2, 3, 4\}$) are auxilia states and they are decided by $U_E$. After the eavesdropper performs her operation, the auxiliary particle $e$ and particles $a$, $b$, $c$

and $d$ are entangled together, and the whole system will be:

$$\begin{aligned}|\xi\rangle = \frac{1}{2}\big[&|\phi^+\rangle\big(|00\rangle_{bd}|\varepsilon_1\rangle + |01\rangle_{bd}|\varepsilon_1'\rangle + |10\rangle_{bd}|\varepsilon_1''\rangle + |11\rangle_{bd}|\varepsilon_1'''\rangle\big)\\ &- |\psi^-\rangle\big(|00\rangle_{bd}|\varepsilon_2\rangle + |11\rangle_{bd}|\varepsilon_2'''\rangle\big)\\ &+ |\psi^+\rangle\big(|00\rangle_{bd}|\varepsilon_3\rangle + |01\rangle_{bd}|\varepsilon_2'\rangle + |10\rangle_{bd}|\varepsilon_2''\rangle + |01\rangle_{bd}|\varepsilon_3'\rangle + |10\rangle_{bd}|\varepsilon_3''\rangle + |11\rangle_{bd}|\varepsilon_3'''\rangle\big)\\ &- |\phi^-\rangle\big(|00\rangle_{bd}|\varepsilon_4\rangle + |01\rangle_{bd}|\varepsilon_4'\rangle + |10\rangle_{bd}|\varepsilon_4''\rangle + |11\rangle_{bd}|\varepsilon_4'''\rangle\big)\big] \end{aligned} \tag{5}$$

In terms of Step (2), we may see that the two sets of measuring basis are randomly selected by Bob in checking eavesdropping. If Bob select $PMB_2$ to measure particles $b$, $d$ and Alice uses $BMB_2$ to measure particles $a$, $c$, (5) should be turned into as follows:

$$|\xi\rangle = \frac{1}{2}\big(|\Psi_2^+\rangle|\varrho_2\rangle - |\Psi_2^-\rangle|\varrho_1\rangle + |\Phi_2^+\rangle|\varrho_3\rangle + |\Phi_2^-\rangle|\varrho_4\rangle\big)_{acbde} \tag{6}$$

Here,

$$\begin{aligned}|\varrho_1\rangle = \frac{1}{\sqrt{2}}\big(&|00\rangle|\varepsilon_4\rangle + |01\rangle|\varepsilon_4'\rangle + |10\rangle|\varepsilon_4''\rangle + |11\rangle|\varepsilon_4'''\rangle - |00\rangle|\varepsilon_2\rangle - |01\rangle|\varepsilon_2'\rangle\\ &- |10\rangle|\varepsilon_2''\rangle - |11\rangle|\varepsilon_2'''\rangle\big)_{bde}\\ |\varrho_2\rangle = \frac{1}{\sqrt{2}}\big(&-|00\rangle|\varepsilon_4\rangle - |01\rangle|\varepsilon_4'\rangle - |10\rangle|\varepsilon_4''\rangle - |11\rangle|\varepsilon_4'''\rangle - |00\rangle|\varepsilon_2\rangle - |01\rangle|\varepsilon_2'\rangle\\ &- |10\rangle|\varepsilon_2''\rangle - |11\rangle|\varepsilon_2'''\rangle\big)_{bde}\\ |\varrho_3\rangle = \frac{1}{\sqrt{2}}\big(&|00\rangle|\varepsilon_1\rangle + |01\rangle|\varepsilon_1'\rangle + |10\rangle|\varepsilon_1''\rangle + |11\rangle|\varepsilon_1'''\rangle + |00\rangle|\varepsilon_3\rangle + |01\rangle|\varepsilon_3'\rangle\\ &+ |10\rangle|\varepsilon_3''\rangle + |11\rangle|\varepsilon_3'''\rangle\big)_{bde}\\ |\varrho_4\rangle = \frac{1}{\sqrt{2}}\big(&|00\rangle|\varepsilon_1\rangle + |01\rangle|\varepsilon_1'\rangle + |10\rangle|\varepsilon_1''\rangle + |11\rangle|\varepsilon_1'''\rangle - |00\rangle|\varepsilon_3\rangle - |01\rangle|\varepsilon_3'\rangle\\ &- |10\rangle|\varepsilon_3''\rangle - |11\rangle|\varepsilon_3'''\rangle\big)_{bde}\end{aligned}$$

In terms of the ahead (1), in order that any error isn't introduced into, the following conditions must be satisfied:

$$\begin{aligned}&\langle -1|\varrho_1\rangle = \langle +0|\varrho_1\rangle = \langle +0|\varrho_1\rangle = 0 \qquad \langle +1|\varrho_2\rangle = \langle +0|\varrho_2\rangle = \langle -0|\varrho_2\rangle = 0\\ &\langle +1|\varrho_3\rangle = \langle -1|\varrho_3\rangle = \langle -0|\varrho_3\rangle = 0 \qquad \langle +1|\varrho_4\rangle = \langle -1|\varrho_4\rangle = \langle +0|\varrho_4\rangle = 0\end{aligned} \tag{7}$$

So, we may get the following results:

$$\begin{aligned}&|\varepsilon_1\rangle = |\varepsilon_3''\rangle \quad |\varepsilon_2'\rangle = |\varepsilon_4'''\rangle \quad |\varepsilon_1''\rangle = |\varepsilon_3\rangle \quad |\varepsilon_2'''\rangle = |\varepsilon_4'\rangle\\ &|\varepsilon_1'\rangle = |\varepsilon_1'''\rangle = |\varepsilon_3'\rangle = |\varepsilon_3'''\rangle = \mathbf{0} \quad |\varepsilon_2\rangle = |\varepsilon_2''\rangle = |\varepsilon_4\rangle = |\varepsilon_4''\rangle = \mathbf{0}\end{aligned} \tag{8}$$

Here, $\mathbf{0}$ denotes a null vector.

When another set of measuring basis is chosen, that is, Bob chooses $PMB_1$ to measure particles $b$, $d$ and Alice uses $BMB_1$ to measure particles $a$, $c$, (5) may be turned into as

follows:

$$|\xi\rangle = \frac{1}{2}\left(|\Psi_1^-\rangle|\sigma_1\rangle + |\Psi_1^+\rangle|\sigma_2\rangle + |\Phi_1^+\rangle|\sigma_3\rangle + |\Phi_1^-\rangle|\sigma_4\rangle\right)_{acbde} \tag{9}$$

Here,

$$\begin{aligned}
|\sigma_1\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle|\varepsilon_3\rangle + |01\rangle|\varepsilon_3'\rangle + |10\rangle|\varepsilon_3''\rangle + |11\rangle|\varepsilon_3'''\rangle + |00\rangle|\varepsilon_4\rangle + |01\rangle|\varepsilon_4'\rangle \right.\\
&\quad \left. + |10\rangle|\varepsilon_4''\rangle + |11\rangle|\varepsilon_4'''\rangle\right)_{bde}\\
|\sigma_2\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle|\varepsilon_3\rangle + |01\rangle|\varepsilon_3'\rangle + |10\rangle|\varepsilon_3''\rangle + |11\rangle|\varepsilon_3'''\rangle - |00\rangle|\varepsilon_4\rangle - |01\rangle|\varepsilon_4'\rangle \right.\\
&\quad \left. - |10\rangle|\varepsilon_4''\rangle - |11\rangle|\varepsilon_4'''\rangle\right)_{bde}\\
|\sigma_3\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle|\varepsilon_1\rangle + |01\rangle|\varepsilon_1'\rangle + |10\rangle|\varepsilon_1''\rangle + |11\rangle|\varepsilon_1'''\rangle - |00\rangle|\varepsilon_2\rangle - |01\rangle|\varepsilon_2'\rangle \right.\\
&\quad \left. - |10\rangle|\varepsilon_2''\rangle - |11\rangle|\varepsilon_2'''\rangle\right)_{bde}\\
|\sigma_4\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle|\varepsilon_1\rangle + |01\rangle|\varepsilon_1'\rangle + |10\rangle|\varepsilon_1''\rangle + |11\rangle|\varepsilon_1'''\rangle + |00\rangle|\varepsilon_2\rangle + |01\rangle|\varepsilon_2'\rangle \right.\\
&\quad \left. + |10\rangle|\varepsilon_2''\rangle + |11\rangle|\varepsilon_2'''\rangle\right)_{bde}
\end{aligned}$$

Similarly, in terms of (1), in order that no error is introduced into, the following conditions must be satisfied:

$$\begin{aligned}
&\langle 1-|\sigma_1\rangle = \langle 0+|\sigma_1\rangle = \langle 0-|\sigma_1\rangle = 0 \qquad \langle 1+|\sigma_3\rangle = \langle 1-|\sigma_3\rangle = \langle 0-|\sigma_3\rangle = 0\\
&\langle 1+|\sigma_2\rangle = \langle 0+|\sigma_2\rangle = \langle 0-|\sigma_2\rangle = 0 \qquad \langle 1+|\sigma_4\rangle = \langle 1-|\sigma_4\rangle = \langle 0+|\sigma_4\rangle = 0
\end{aligned} \tag{10}$$

So, we may get the following results:

$$\begin{aligned}
&|\varepsilon_1\rangle = |\varepsilon_2''\rangle \quad |\varepsilon_3''\rangle = |\varepsilon_4'''\rangle \quad |\varepsilon_1'\rangle = |\varepsilon_2\rangle, |\varepsilon_3'''\rangle = |\varepsilon_4''\rangle\\
&|\varepsilon_3\rangle = |\varepsilon_3'\rangle = |\varepsilon_4\rangle = |\varepsilon_4'\rangle = \mathbf{0} \quad |\varepsilon_1''\rangle = |\varepsilon_1'''\rangle = |\varepsilon_2''\rangle = |\varepsilon_2'''\rangle = \mathbf{0}
\end{aligned} \tag{11}$$

Here, the $\mathbf{0}$ also denotes a null vector. In terms of (9) and (10), we find that (5) must be changed into as follows:

$$|\xi\rangle = |\varepsilon_1\rangle_e\left|\chi^{00}\right\rangle_{abcd} \tag{12}$$

It may be seen that $|\xi\rangle$ is a product of the ancilla and a four-particle $|\chi^{00}\rangle_{abcd}$ state. That is to say, there is not any entanglement between particles $a$, $b$, $c$, $d$ particle $e$. The eavesdropper can't obtain any information about secret keys by observing the ancilla in the case that no error is introduced into. So, this kind of entangle-measure attack is invalid. All in all, in terms of the above analysis, the security of our QKD protocol can be assured.

Next, we compare our QKD protocol with Song's protocol [16] so that the advantage of our protocol may be shown. Firstly, we calculate the efficiencies of the two QKD protocols. Let's employ Cabello's definition [36] of QKD efficiency: $\eta = \frac{b_s}{q_t + b_t}$, where, $\eta$ denotes the efficiency, $b_s$ is the expected secret bits received by Bob. $q_t$ and $b_t$ are the qubit used and the classical bits exchanged between Alice and Bob, respectively. In our QKD protocol, it is

evident that, $b_s$ and $q_t$, both equal to 4 bits; since Alice and Bob needn't publish any message after they make the $\chi$-type state measurement, $b_t$ equals to 0 bit, so the total efficiency of our QKD protocol $\eta = \frac{4}{4} = 100\%$ (except for the classical messages exchanged during checking eavesdropping and dividing groups). However, as each party needs to publish 2 bits classical messages in Song's protocol [16] after making Bell state measurement, the efficiency of Song's protocol is only 33%, that is, it isn't very high. Obviously, our QKD protocol has higher efficiency than Song's QKD protocol [16].

## 4 Discussion and Conclusion

In summary, an efficient QKD protocol using a $\chi$-type state has been proposed successfully. Secret keys can be generated over secure quantum channel between Alice and Bob in this protocol. In the security-check, two sets of measuring basis are employed. In addition, we may see that both Alice and Bob need to perform $\chi$-type state measurement in this protocol. Here, it is worth stressing that they don't make $\chi$-type state measurements until Alice and Bob ascertain that there is no eavesdropping in their quantum channel, in other words, after they finishes the security check, the eavesdropping isn't detected. We confess that the present QKD protocol is similar to that in the paper [17], and the difference between the two protocols is only that the present protocol uses $\chi$-type states and Bell states are employed in the paper [17]. In addition, we still confess that the present QKD protocol has not the symmetry trait, that is, Alice's and Bob's roles in it are not equal. Another QKD protocol that has the symmetry trait has been finished and will be published elsewhere.

**Acknowledgements** I thank my parents for their encouragements. This work is supported by the Natural Science Foundation of Anhui Province under Grant No. KJ2010B236.

## References

1. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings, p. 175, Bangalore, India. IEEE, New York (1984)
2. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
3. Bennett, C.H.: Phys. Rev. Lett. **68**, 3121 (1992)
4. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
5. Bennett, C.H., Wiesner, S.J.: Phys. Rev. Lett. **69**, 2881 (1992)
6. Huttner, B., Imoto, N., Gisin, N., et al.: Phys. Rev. A **51**, 1863 (1995)
7. Goldenberg, L., Vaidman, L.: Phys. Rev. Lett. **75**, 1239 (1995)
8. Bruß, D.: Phys. Rev. Lett. **81**, 3018 (1998)
9. Koashi, M., Imoto, N.: Phys. Rev. Lett. **79**, 2383 (1997)
10. Cabello, A.: Phys. Rev. A **61**, 052312 (2000)
11. Cabello, A.: Phys. Rev. A **64**, 024301 (2001)
12. Cabello, A.: arXiv:quant-ph/0009025
13. Zhang, Y.S., Li, C.F., Guo, G.C.: Phys. Rev. A **63**, 036301 (2001)
14. Li, C., Song, H.S., Zhou, L.: J. Opt. B: Quantum Semiclass. Opt. **5**, 155 (2003)
15. Lee, J., Lee, S., Kim, J., et al.: Phys. Rev. A **70**, 032305 (2004)
16. Song, D.: Phys. Rev. A **69**, 034301 (2004)
17. Gao, G.: Opt. Commun. **281**, 876 (2008)
18. Zhao, Z., Yang, T., Chen, Z.B., Du, J., Pan, J.W.: arXiv:quant-ph/0211098
19. Long, G.L., Liu, X.X.: Phys. Rev. A **65**, 032302 (2002)
20. Deng, F.G., Long, G.L.: Phys. Rev. A **68**, 042315 (2003)
21. Gao, G.: Commun. Theor. Phys. **51**, 820 (2009)
22. Wang, X.B.: Phys. Rev. A **71**, 052328 (2005)
23. Guo, Y., Lee, M., Zeng, G.H.: Opt. Commun. **281**, 3938 (2008)

24. Eusebi, A., Mancini, S.: Quantum Inf. Comput. **9**, 950 (2009)
25. Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Phys. Rev. Lett. **70**, 1895 (1993)
26. Deng, F.G., Li, C.Y., Li, Y.S., Zhou, H.Y., Wang, Y.: Phys. Rev. A **72**, 022338 (2005)
27. Wang, Y.H., Yu, C.S., Song, H.S.: Chin. Phys. Lett. **23**, 3143 (2006)
28. Yeo, Y.: Phys. Rev. A **74**, 052305 (2006)
29. Yan, F.L., Ding, H.W.: Chin. Phys. Lett. **23**, 17 (2006)
30. Yeo, Y., Chua, W.K.: Phys. Rev. Lett. **96**, 060502 (2006)
31. Wang, X.W., Yang, G.J.: Phys. Rev. A **78**, 024301 (2008)
32. Wang, X.W.: Opt. Commun. **282**, 1052 (2009)
33. Wang, H.F., Zhang, S.: Phys. Rev. A **79**, 042336 (2009)
34. Shen, H.W., Wang, H.F., Ji, X., Zhang, S.: Chin. Phys. **18**, 3706 (2009)
35. Xiu, X.M., Dong, L., Gao, Y.J., Chi, F.: Commun. Theor. Phys. **52**, 60 (2009)
36. Cabello, A.: Phys. Rev. Lett. **85**, 5635 (2000)