Available online at www.sciencedirect.com

ScienceDirect

Optics Communications 281 (2008) 876–879

OPTICS COMMUNICATIONS

www.elsevier.com/locate/optcom

Quantum key distribution by comparing Bell states

Gan Gao

School of Physics and Material Science, Anhui University, Hefei 230039, China

Received 13 June 2007; received in revised form 7 September 2007; accepted 7 October 2007

Abstract

We propose a quantum key distribution (QKD) scheme based on entanglement swapping. In this scheme, the methods to form secret keys are so interesting. By comparing initial Bell state and outcome of entanglement swapping, the secret keys between Alice and Bob are generated involuntarily.

PACS: 03.67.Dd

Keywords: Bell state comparison; Entanglement swapping; Quantum key distribution

1. Introduction

Entanglement is one of the most intriguing properties of quantum physics and a kind of very useful resource. It is widely used in quantum cryptography, quantum computation, etc. So to speak, it plays a important role in quantum information processing. Several methods to generate the entanglement have been proposed, such as nonlinear crystal and optical pulse [2], ion trap and ions [3], and cavity QED and atoms [4], etc. After the entanglement generation, in order to communicate, the entangled qubits have to be distributed among distant users. In the distributing process, the flying qubits must be used. However, at present, the only feasible flying qubit for long-distance transmission is photons, which will be used in our scheme. In addition, during the distribution process, since the distance becomes long, the entanglement between the qubits will inevitably decrease, which is likely a bad news for those communication schemes that are achieved by using the entanglement. Fortunately, quantum repeater can settle out this problem well [5]. The main theory that quantum repeater adopts is the so-called entanglement swapping, which is a very nice property of entanglement. The entanglement swapping [28–31] can entangle two quantum systems that do not interact with each other. Later on, we will concretely illustrate it with Bell states.

In this letter, by utilizing the entanglement swapping, we propose a quantum key distribution (QKD) scheme. The so-called QKD is a procedure in which two legitimate parties, Alice and Bob, generate a secret key over a long distance in a form that is unintelligible to a third party, Eavesdropper. Since the first key distribution protocol that used four quantum states was proposed by Bennett and Brassard in 1984 (called BB84) [1], a great deal of attention has been paid to this topic. So far, many QKD schemes have been proposed [6–27]. In these works, some schemes [14,15,12,23–25] are proposed based on entanglement swapping. At this stage, we can't help asking what advantages these schemes have in contrast to the un-used entanglement swapping ones? In Refs. [14,15], the answer has been given, that is, only one set of measuring basis is needed. In other words, alternative measurements are not required. Later, the scheme with this property is generalized [33] and simplified [25], and its security was proved in Ref. [24]. In our QKD scheme by using entanglement swapping, we still make use of two sets of measuring basis to check channel security. The advantage to do so is that Eavesdropper will be detected with higher probability.

E-mail address: gaogan0556@163.com

0030-4018/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2007.10.081

(Here, please allow us to show a flashback.) For example, under the intercept-resend attack, if only one set is used in our scheme, the probability that Eavesdropper can't be detected is $\frac{1}{4}$, and if two sets, it is $\frac{3}{4} \times \frac{1}{4} = \frac{3}{16}$. Obviously, it is possible to improve the security by using two sets of measuring basis to check eavesdropping. In our scheme, while transmitting photons, we adopt the ideal of sequence transmission, which has appeared in the previous scheme [19]. In addition, it is worth pointing out that, in this QKD scheme, the method that the secret keys are generated is so interesting, that is Bell state comparison. In other words, by comparing initial Bell state and outcome of entanglement swapping, the secret keys are formed easily. Before introducing this QKD scheme, we first define four Bell state as follows:

$$\psi_{12}^{+} = (|1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2)/\sqrt{2} = (|h\rangle_1|h\rangle_2 - |v\rangle_1|v\rangle_2)/\sqrt{2} \tag{1}$$

$$\psi_{12}^{-} = (|1\rangle_1|0\rangle_2 - |0\rangle_1|1\rangle_2)/\sqrt{2} = (|v\rangle_1|h\rangle_2 - |h\rangle_1|v\rangle_2)/\sqrt{2} \tag{2}$$

$$\phi_{12}^{+} = (|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)/\sqrt{2} = (|h\rangle_1|h\rangle_2 + |v\rangle_1|v\rangle_2)/\sqrt{2} \tag{3}$$

$$\phi_{12}^{-} = (|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2)/\sqrt{2} = (|h\rangle_1|v\rangle_2 + |v\rangle_1|h\rangle_2)/\sqrt{2} \tag{4}$$

where $\mid 0\rangle$ and $\mid 1\rangle$ are the up and down eigenstates of $\sigma_z, \mid h\rangle = (\mid 0\rangle + \mid 1\rangle)/\sqrt{2}$ and $\mid v\rangle = (\mid 0\rangle - \mid 1\rangle)/\sqrt{2}$ are the up and down eigenstates of σ_x. The subscripts 1 and 2 denote the two correlated photons in an Einstein–Podolsky–Rose (EPR) pair. Let U_1, U_2, U_3, and U_4 act on one photon of EPR pair in Bell state. We can see that $U_1\psi_{12}^{-} = \psi_{12}^{-}, U_2\psi_{12}^{-} = \psi_{12}^{+}, U_3\psi_{12}^{-} = \phi_{12}^{+}$, and $U_4\psi_{12}^{-} = \phi_{12}^{-}$. Suppose two distant parties, Alice and Bob, share ψ_{12}^{-} and ϕ_{34}^{+}. Where Alice has photons 1 and 3, and Bob has photons 2 and 4. The state of the whole system shows as follows:

$$\psi_{12}^{-} \otimes \phi_{34}^{+} = \frac{1}{2}(-\phi_{13}^{+}\psi_{24}^{-} + \phi_{13}^{-}\psi_{24}^{+} - \psi_{13}^{+}\phi_{24}^{-} + \psi_{13}^{-}\phi_{24}^{+}) \tag{5}$$

If a Bell state measurement on photons 1 and 3 is carried out, the whole system state collapses to $(\phi_{13}^{-}, \psi_{24}^{+}), (\phi_{13}^{+}, \psi_{24}^{-}), (\psi_{13}^{-}, \phi_{24}^{+})$ and $(\psi_{13}^{+}, \phi_{24}^{-})$ with equal probability of 25% for each. The previous entanglement between photons 1 and 2,and photons 3 and 4 are now swapped into the entanglement between photons 1 and 3, and 2 and 4. If Alice and Bob share other Bell states, similar results can appear. The corresponding relations between the two prepared Bell states (TPBSs) and the two possible output Bell states (TPOBSs) after entanglement swapping are summarized in Table 1.

2. Scheme

Let's describe this QKD scheme. We only consider the ideal condition: there is no noise and losses in the quantum channel. There are two legitimate parties, Alice and Bob. Secret keys are generated between them. The concrete steps are as follows:

(1) Alice prepares an ordered EPR pairs, and each EPR pair may be in arbitrary Bell state. And then, she takes one photon from each EPR pair to form an ordered photon sequence, say S_{h}. The remaining EPR partner photons form another photon sequence, say S_{t}. Alice sends the S_{t} to Bob and retains the S_{h} in her site. Here, it is worth emphasizing that none, but Alice herself, knows the states of her prepared EPR pairs.

(2) After confirming that the S_{t} has been received by Bob, Alice starts to check whether the photon sequences is transmitted securely, that is to check eavesdropping. The checking procedure is: Bob randomly chooses some photons in the S_{t} and publicly tells Alice the positions of chosen photons through the classical channel. And he chooses randomly one of two sets of measuring basis, say, $\{\mid 0\rangle, \mid 1\rangle\}$ and $\{\mid h\rangle, \mid v\rangle\}$ to measure the chosen photons. And then, Bob tells Alice which measuring basis he has chosen for each photon and his outcomes of measurements. Next, Alice uses the same measuring basis as Bob to measure the corresponding photons in the S_{h}. From the above expressions for Bell states, their outcomes of measurements are correlated if no eavesdropping exists. Therefore, Alice can analyze the error rate of the S_{t} transmission by comparing outcomes of measurements. If the error rate goes beyond the threshold, the process is aborted. Otherwise, the process continues to the next step.

(3) Alice and Bob divide these EPR pairs (except for the sample EPR pairs) into some groups. There are two EPR pairs in each group. Suppose two EPR pairs in one group are in ψ_{12}^{-} and ϕ_{34}^{+}, respectively. According to the above content, Alice now holds the pho-

Table 1
The subscripts 12 and 34 states are Alice's and Bob's states prepared, respectively; the subscripts 13 and 24 states are Alice's and Bob's outcomes of entanglement swapping, respectively

TPBSs				TPOBSs			
$(\phi_{12}^{+}, \phi_{34}^{+})$	$[(\phi_{12}^{-}, \phi_{34}^{-})$	$(\psi_{12}^{+}, \psi_{34}^{+})$	$(\psi_{12}^{-}, \psi_{34}^{-})]$	$(\phi_{13}^{+}, \phi_{24}^{+})$	$(\phi_{13}^{-}, \phi_{24}^{-})$	$(\psi_{13}^{+}, \psi_{24}^{+})$	$(\psi_{13}^{-}, \psi_{24}^{-})$
$(\phi_{12}^{-}, \phi_{34}^{+})$	$[(\phi_{12}^{+}, \phi_{34}^{-})$	$(\psi_{12}^{-}, \psi_{34}^{+})$	$(\psi_{12}^{+}, \psi_{34}^{-})]$	$(\phi_{13}^{+}, \phi_{24}^{-})$	$(\phi_{13}^{-}, \phi_{24}^{+})$	$(\psi_{13}^{+}, \psi_{24}^{-})$	$(\psi_{13}^{-}, \psi_{24}^{+})$
$(\psi_{12}^{+}, \phi_{34}^{+})$	$[(\psi_{12}^{-}, \phi_{34}^{-})$	$(\phi_{12}^{+}, \psi_{34}^{+})$	$(\phi_{12}^{-}, \psi_{34}^{-})]$	$(\phi_{13}^{+}, \psi_{24}^{+})$	$(\phi_{13}^{-}, \psi_{24}^{-})$	$(\psi_{13}^{+}, \phi_{24}^{+})$	$(\psi_{13}^{-}, \phi_{24}^{-})$
$(\psi_{12}^{-}, \phi_{34}^{+})$	$[(\psi_{12}^{+}, \phi_{34}^{-})$	$(\phi_{12}^{-}, \psi_{34}^{+})$	$(\phi_{12}^{+}, \psi_{34}^{-})]$	$(\phi_{13}^{+}, \psi_{24}^{-})$	$(\phi_{13}^{-}, \psi_{24}^{+})$	$(\psi_{13}^{+}, \phi_{24}^{-})$	$(\psi_{13}^{-}, \phi_{24}^{+})$

Table 2
For convenience, Alice's preparing Bell state combination, Alice's un-published state, Alice's measurement outcome, Alice's comparison outcome, Alice's published state, Bob's measurement outcome and Bob's comparison outcome are abbreviated by APBSC, AUS, AMO, ACO, APS, BMO and BCO, respectively

APBSC	AUS	AMO	ACO	APS	BMO	BCO
$(\psi_{12}^-, \phi_{34}^+)$	ψ_{12}^-	ϕ_{13}^+	$\psi^- \leftrightarrow U_4\phi^+$	ϕ_{34}^+	ψ_{24}^-	$\phi^+ \leftrightarrow U_4\psi^-$
$(\psi_{12}^-, \phi_{34}^+)$	ψ_{12}^-	ϕ_{13}^-	$\psi^- \leftrightarrow U_3\phi^-$	ϕ_{34}^+	ψ_{24}^+	$\phi^+ \leftrightarrow U_3\psi^+$
$(\psi_{12}^-, \phi_{34}^+)$	ψ_{12}^-	ψ_{13}^+	$\psi^- \leftrightarrow U_2\psi^+$	ϕ_{34}^+	ϕ_{24}^-	$\phi^+ \leftrightarrow U_2\phi^-$
$(\psi_{12}^-, \phi_{34}^+)$	ψ_{12}^-	ψ_{13}^-	$\psi^- \leftrightarrow U_1\psi^-$	ϕ_{34}^+	ϕ_{24}^+	$\phi^+ \leftrightarrow U_1\phi^+$
$(\psi_{12}^-, \phi_{34}^+)$	ϕ_{34}^+	ϕ_{13}^+	$\phi^+ \leftrightarrow U_1\phi^+$	ψ_{12}^-	ψ_{24}^-	$\psi^- \leftrightarrow U_1\psi^-$
$(\psi_{12}^-, \phi_{34}^+)$	ϕ_{34}^+	ϕ_{13}^-	$\phi^+ \leftrightarrow U_2\phi^-$	ψ_{12}^-	ψ_{24}^+	$\psi^- \leftrightarrow U_2\psi^+$
$(\psi_{12}^-, \phi_{34}^+)$	ϕ_{34}^+	ψ_{13}^+	$\phi^+ \leftrightarrow U_3\psi^+$	ψ_{12}^-	ϕ_{24}^-	$\psi^- \leftrightarrow U_3\phi^-$
$(\psi_{12}^-, \phi_{34}^+)$	ϕ_{34}^+	ψ_{13}^-	$\phi^+ \leftrightarrow U_4\psi^-$	ψ_{12}^-	ϕ_{24}^+	$\psi^- \leftrightarrow U_3\phi^+$

tons 1 and 3, and Bob holds the photons 2 and 4. Alice performs Bell state measurement on the photons 1 and 3, and Bob performs Bell state measurement on the photons 2 and 4. After the two parties both finish Bell state measurements, Alice randomly publishes one of two Bell states: ψ_{12}^- and ϕ_{34}^+. Suppose the published state is ϕ_{34}^+, and Alice's and Bob's measurement outcomes is ϕ_{13}^+ and ψ_{24}^-, respectively. There is a following law:Alice's un-published state ψ_{12}^- and her measurement outcome ϕ_{13}^+.

$$\psi^- \leftrightarrow U_4\phi^+ \tag{6}$$

The published state ϕ_{34}^+ and Bob's measurement outcome ψ_{24}^-

$$\phi^+ \leftrightarrow U_4\psi^- \tag{7}$$

Note that we have omitted state's subscripts 12, 13, 34 and 24 in order to find the law clearly and easily. And the following are also omitted. In order to save the space, we do not list out the other cases with the above form. All cases are summarized in Table 2.

From the Table 2, we can see that, regardless of which state is published by Alice and no matter what swapping outcomes are, the comparison outcomes between published (un-published) state and measurement outcome on both sides are entirely identical. Taking advantage of the law, the two parties, Alice and Bob, can define and establish the secret keys entirely. For example, U_1, U_2, U_3, and U_4 are encoded into 00, 01, 10, and 11, respectively. There are sixteen Bell state combinations (see Table 1). If the Bell state combination that Alice prepares is not $(\psi_{12}^-, \phi_{34}^+)$, but other combinations, the law can't be altered either. According to the law, the secret keys can be established successfully and easily between Alice and Bob. After finishing entanglement swapping, Alice's published state will decide what the key is, that is, the different published state leads to the different key. Thus, during the final course of generating key, Alice possesses the initiative with some degree.

Next, let us make a comparison with the protocol [25] and see the advantages of our protocol. First, we calculate the efficiencies of two protocols. Let's employ Cabellos definition of QKD efficiency: $\eta = \frac{b_s}{q_t+b_t}$, where, η 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 protocol, it is obvious that b_s and q_t both equal to 2 bits; as Alice must publish one of four Bell states each time, b_t should also equal to 2 bits, so the total efficiency $\eta = \frac{2}{2+2} = 50\%$ (except for the classical information exchanged during checking eavesdropping and dividing groups). It should be relatively higher and is equivalent to the efficiency in Refs. [6,12], is > the ones in Refs. [1,8]. To get back to our comparative goal, the total efficiency in the protocol [25] is only 33% (In the protocol [25], b_s and q_t both equals to 2 bits, b_t is 4 bits). Obviously, our protocol is more efficient. Thinking about the reason that the efficiency of the protocol [25] is lower than ours, we can see that the methods to form the secret keys in two protocols are different and the quantities of classical information exchanged are not equal, though two protocols are both realized by entanglement swapping. With respect to the security of our protocol, what we want to say is that its security proof is the same as that in Ref. [8]. So our protocol is secure.

3. Conclusion

In summary, we have proposed an efficient QKD protocol and the secret keys can be established securely over a secure quantum channel between two parties. By the way, in the practical implementations, our protocol needs to pursue Bell states analysis for photon pairs. However, no scheme is known that allows the measurement of a complete set of Bell states [32]. With the development of new optical elements, our QKD schemes might become feasible in the future.

Acknowledgement

The author thanks Prof. Zhang Zhan-Jun for his encouragement and helpful discussion.

References

[1] C.H. Bennett, G. Brassard, in: Proceedings of the IEEE international conference on computers systems and signal processings, Bangalore, India, IEEE, New York, 1984, p. 175.

[2] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. 75 (1995) 4337.
[3] Q.A. Turchette, C.S. Wood, et al., Phys. Rev. Lett. 81 (1998) 3631.
[4] S.B. Zheng, G.C. Guo, Phys. Rev. Lett. 85 (2000) 2392.
[5] H.-J. Briegel, W. Duer, J.I. Cirac, P. Zoller, Phys. Rev. Lett. 81 (1998) 5932.
[6] A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
[7] C.H. Bennett, Phys. Rev. Lett. 68 (1992) 3121.
[8] C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. 68 (1992) 557.
[9] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881.
[10] B. Huttner, N. Imoto, N. Gisin, et al., Phys. Rev. A 51 (1995) 1863.
[11] L. Goldenberg, L. Vaidman, Phys. Rev. Lett. 75 (1995) 1239.
[12] M. Koashi, N. Imoto, Phys. Rev. Lett. 79 (1997) 2383.
[13] D. Bru ß, Phys. Rev. Lett. 81 (1998) 3018.
[14] A. Cabello, Phys. Rev. A 61 (2000) 052312;
A. Cabello, Phys. Rev. A 64 (2001) 024301.
[15] Y.S. Zhang, C.F. Li, G.C. Guo, Phys. Rev. A 63 (2001) 036301.
[16] A. Cabello, Phys. Rev. Lett. 85 (2000) 5635.
[17] H.-k. Lo, H.F. Chan, M. Ardehali, e-print quant-ph/0011056.
[18] G.P. Guo, C.F. Li, B.S. Shi, G.C. Guo, Phys. Rev. A 64 (2001) 042301.
[19] G.L. Long, X.X. Liu, Phys. Rev. A 65 (2002) 032302.
[20] P. Xue, C.F. Li, G.C. Guo, Phys. Rev. A 65 (2002) 022317.
[21] N. Gisin, G. Ribordy, W. Tittel, et al., Rev. Mod. Phys. 74 (2002) 145.
[22] Z. Zhao, T. Yang, Z.B. Chen, J. Du, J.W. Pan, quant-ph/0211098.
[23] C. Li, H.S. Song, L. Zhou, J. Opt. B: Quantum Semiclass. Opt. 5 (2003) 155.
[24] J. Lee, S. Lee, J. Kim, et al., Phys. Rev. A 70 (2004) 032305.
[25] D. Song, Phys. Rev. A 69 (2004) 034301.
[26] X.B. Wang, Phys. Rev. A 71 (2005) 052328.
[27] G.L. Giorgi, Phys. Rev. A 71 (2005) 064303.
[28] M. Zukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, Phys. Rev. Lett. 71 (1993) 4287.
[29] S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A 57 (1998) 822.
[30] L. Hardy, D. Song, Phys. Rev. A 62 (2000) 052315.
[31] J.W. Pan, M. Daniell, S. Gasparoni, G. Weihs, A. Zeilinger, Phys. Rev. Lett. 86 (2001) 4435.
[32] S. Scheel, N. Lutkenhaus, New J. Phys. 6 (2004) 51.
[33] A. Cabello, quant-ph/0009025.