A random quantum key distribution by using Bell states

Chong Li,* He-Shan Song, Ling Zhou
Department of Physics, Dalian University of Technology,
Dalian 116024, PR China

Chun-Feng Wu
Department of Physics, Faculty of Science,
National University of Singapore, 119260, Singapore

December 28, 2021

Abstract
We proposed a new scheme for quantum key distribution based on entanglement swapping. By this protocol Alice can securely share a random quantum key with Bob, without transporting any particle.

1 Introduction
The main goals of cryptography are securely supplying a key to two parties and detecting eavesdroppers. These goals cannot be achieved classically, but they can be overcome by quantum cryptography. Since BB84 protocol [1], the first quantum cryptography scheme, was published, various quantum encryption schemes have been proposed, such as the EPR scheme [2][3], the 4 + 2 protocol [4], the six-state protocol [5], the Goldenberg /Vaidman scheme [6], Koashi/Imoto scheme [7], and the recent protocol [8] and so on. But most of protocol need transport particles.

In this paper, we present a new method in which the communicators use entanglement swapping [9] to distribute the quantum cryptographic random key and use the correlations of entanglement swapping results to detect the eavesdropper. There are two merits than the previous protocol in our scheme, 1. if the communicators shared enough known entangled pairs before the key distribution, sender (Alice) need not send any particle to receiver (Bob). 2. The efficiency can approach 4 bit secret communication per 2 entangled pairs (in BB84 protocol, it is only 1 bit per pair particle).

* lichong@student.dlut.edu.cn
2 protocol

Entanglement swapping has been proposed by Zukowski et al.\[9\] for two entangled pairs in one of the Bell states. Entanglement swapping works as follows. Consider two pairs of entangled particles 1,2,3 and 4, prepared in Bell states respectively $|\phi^+\rangle_{12}$ and $|\psi^-\rangle_{34}$. If a Bell operator measurement is performed on particle 2 and particles 3, then we have

$$|\psi\rangle_{1234} = |\phi^+\rangle_{23} \otimes |\psi^-\rangle_{14} = \frac{1}{2} \left( |\phi^+\rangle_{23} |\phi^-\rangle_{14} + |\phi^-\rangle_{23} |\phi^-\rangle_{14} + |\phi^-\rangle_{23} |\phi^+\rangle_{14} + |\phi^+\rangle_{23} |\phi^+\rangle_{14} \right).$$

From above equation, we found the four possible results $|\phi^+\rangle_{23}$, $|\phi^-\rangle_{23}$, $|\psi^+\rangle_{23}$, and $|\psi^-\rangle_{23}$ have the same probability to occur. In fact, the outcome of each measurement is purely random. Suppose that the result $|\phi^+\rangle_{23}$ is obtained, consequently the state of the pair 1 and 4 after the measurement is $|\psi^-\rangle_{14}$. Therefore, the state of 1 and 4 become entangled although they have never interacted.

Recently entanglement swapping has been used in quantum key distribution\[10\]. Although there are 3 entangled pairs in protocol\[10\], yet Alice must send particles to Bob. Here we propose a quantum key distribution scheme without particles transported. The proposed protocol for quantum key distribution is illustrated in Fig. 1 and it is described as follows. The parties, Alice and Bob, initially share $2^n$ EPR pairs in known entangled states $|\eta\rangle_{AB}$, $|\eta\rangle_{AB}$ is one of the four Bell states. Alice and Bob divide all entangled pairs into $n$ ordered groups, every group include 2 entangled pairs. Alice and Bob agree beforehand that $|\phi^+\rangle,|\psi^+\rangle,|\psi^-\rangle,|\phi^-\rangle$ are encoded as 00, 01, 10, 11 respectively. They can perform the series operations as following. (Alice own particle 1 and particle 3, the particle 2 and particle 4 belong to Bob.)

1. Alice made a Bell operator measurement on particle 1 and particle 3.

For example, we can assumed initially the state of particle 1 and particle 2 is $|\phi^+\rangle_{12}$, and the state of particle 3 and particle 4 is $|\psi^+\rangle_{34}$, where

$$|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}} \left( |00\rangle_{12} + |11\rangle_{12} \right) \quad \text{and} \quad |\psi^+\rangle_{34} = \frac{1}{\sqrt{2}} \left( |01\rangle_{34} + |10\rangle_{34} \right).$$

Alice perform Bell operator measurement on particle 1 and particle 3, and record the measurement.

2. Alice calculated out the state of particle 2 and particle 4.
Suppose that Alice’s Bell operator measurement is $|\psi^+\rangle_{1A}$, she can obtain Bob’s Bell operator measured result $|\phi^+\rangle_{2B}$ by the following equation,

$$|\Phi\rangle_{1234} = \frac{1}{2} \left\{ |\phi^+\rangle_{1A} |\psi^+\rangle_{2B} + |\phi^-\rangle_{1A} |\psi^-\rangle_{2B} + |\psi^+\rangle_{1A} |\phi^+\rangle_{2B} + |\psi^-\rangle_{1A} |\phi^-\rangle_{2B} \right\}.$$

Alice decode the Bell operator measured results, she get 10 and 00.

3. Alice told Bob she had made Bell operator measurement on her particles, but did not told him the measured result by classical channel.

4. Bob performed a Bell operator measurement on particle 2 and particle 4 and calculated Alice’s Bell operator measurement result.

After he captured Alice’s classical information, Bob make Bell operator measurement on particle 2 and 4. He get the measured result $|\phi^+\rangle_{2B}$, and he obtain Alice’s Bell operator measurement $|\psi^+\rangle_{1A}$ from the eq.(2). So Bob can gain the bits 10 and 00.

they perform above progree repeatedly,

5. Bob chose some results and sent them to Alice, then Alice compared Bob’s results with her corresponding results, she can find if there is eavesdropper.

The important point is that the efficiency of the quantum key distribution has been improved in this protocol. From above operations, We know that Alice shared 4 bits with Bob by two entangled pairs. This way largely improves the efficiency of the distribution for cryptographic key. The efficiency can reach 1 bit per particle, it is higher than the previous protocol, for example, in BB84 protocol it is 1 bit per pair, and in B92 protocol it is 1 bit per two pairs.

3 Security

How secure is this protocol? Now we discuss the security of our protocol against three type of attacks.

Type I. General eavesdropping

Suppose that Eve, the eavesdropper, can get secretly the classical information of Alice and Bob and know all the states of the quantum channel. If Alice and Bob do not publish their’s Bell operator measured result, eavesdropper (Eve) can not get the information from the known entangled channels. For example, both the quantum channels are the same Bell states $|\phi^+\rangle_{12}$ and $|\phi^+\rangle_{34}$. By the entanglement swapping calculation, we know the state of these entangled particles is

$$|\Phi\rangle_{1234} = \frac{1}{2} \left\{ |\phi^+\rangle_{1A} |\phi^+\rangle_{2B} + |\phi^-\rangle_{1A} |\phi^-\rangle_{2B} + |\psi^+\rangle_{1A} |\phi^+\rangle_{2B} + |\psi^-\rangle_{1A} |\phi^-\rangle_{2B} \right\}.$$

Eve have many entangled pairs in state $|\phi^+\rangle_{EE}$, she performed Bell operator measurement on her particles 1/, 2/, 3/ and 4/.
only 1 measurement on particles 1 and 3, is only 1, and is not detected by Alice or Bob, is only \((\frac{1}{4})^n\). When n is large enough, this probability is 0 approximately.

Type II. Share the quantum channel.
If the Eve were smart enough, she made the state \(|\phi^+\rangle_{ABE} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} |0\rangle_E + |11\rangle_{AB} |1\rangle_E)\) instead of \(|\phi^+\rangle_{AB}^\prime\), when Alice made a Bell operator measurement on particle 1 and particle 3, the state became

\[
|\Psi\rangle_{123456}^{ABE} = |\phi^+\rangle_{123456}^{ABE} \otimes |\phi^+\rangle_{ABE}^{123456}
\]

\[
= \frac{1}{2\sqrt{2}} \left( |\phi^+\rangle_{13}^{AA} \left( |\phi^+\rangle_{24}^{BB} |\phi^+\rangle_{EE} + |\phi^-\rangle_{24}^{BB} |\phi^-\rangle_{EE} \right) + |\phi^-\rangle_{13}^{AA} \left( |\phi^+\rangle_{24}^{BB} |\phi^-\rangle_{EE} + |\phi^-\rangle_{24}^{BB} |\phi^+\rangle_{EE} \right) + |\psi^+\rangle_{13}^{AA} \left( |\psi^+\rangle_{24}^{BB} |\psi^+\rangle_{EE} + |\psi^-\rangle_{24}^{BB} |\psi^-\rangle_{EE} \right) + |\psi^-\rangle_{13}^{AA} \left( |\psi^+\rangle_{24}^{BB} |\psi^-\rangle_{EE} + |\psi^-\rangle_{24}^{BB} |\psi^+\rangle_{EE} \right) \right).
\]

Compare eq.[3] with eq.[5], we found if there is an eavesdropper, there is only \(\frac{1}{2}\) probability that the two results are same. Bob can send some results randomly to Alice; then Alice will be sure that there is an eavesdropper if she finds different results—they would then abandon this key. That is, Eve cannot gain any information about the key.

Type III. Replace the quantum channel.
If Eve shared the entangled pairs \(|\phi^+\rangle_{i/j}^{AB} \) with Alice instead of Bob, and Eve shared entangled pairs \(|\phi^+\rangle_{i/j}^{i/j} \) with Bob, before the key supply, both Alice and Bob would be unaware of this. Then the process of key distribution become

\[
|\Phi\rangle_{1234}^{ABE} = \frac{1}{2} \left( |\phi^+\rangle_{13}^{AA} |\phi^+\rangle_{24}^{EE} + |\phi^-\rangle_{13}^{AA} |\phi^-\rangle_{24}^{EE} + |\psi^+\rangle_{13}^{AA} |\psi^+\rangle_{24}^{EE} + |\psi^-\rangle_{13}^{AA} |\psi^-\rangle_{24}^{EE} \right).
\]

The four Bell operator measurements in eq.[3] and [4] are equally likely, each occurring with probability \(\frac{1}{4}\). The probability, Eve’s Bell operator measurements on particles 1’ and 3’ is same as Alice’s Bell operator measurements on particles 1 and 3, is only \(\frac{1}{4}\) That is to say, the probability, Eve eavesdrop 4n bits and is not detected by Alice or Bob, is only \((\frac{1}{4})^n\). When n is large enough, this probability is 0 approximately.

\[
|\Phi\rangle_{1234}^{ABE} = \frac{1}{2} \left( |\phi^+\rangle_{13}^{AA} |\phi^+\rangle_{24}^{EE} + |\phi^-\rangle_{13}^{AA} |\phi^-\rangle_{24}^{EE} + |\psi^+\rangle_{13}^{AA} |\psi^+\rangle_{24}^{EE} + |\psi^-\rangle_{13}^{AA} |\psi^-\rangle_{24}^{EE} \right).
\]
and

$$\left| \Phi^{'} \right>_{EEBB}^{1/2/3/4} = \frac{1}{2} \left\{ \left| \phi^{+} \right>_{EE}^{1/3} \left| \phi^{+} \right>_{BB}^{2/4} + \left| \phi^{-} \right>_{EE}^{1/3} \left| \phi^{-} \right>_{BB}^{2/4} + \left| \psi^{+} \right>_{EE}^{1/3} \left| \psi^{+} \right>_{BB}^{2/4} + \left| \psi^{-} \right>_{EE}^{1/3} \left| \psi^{-} \right>_{BB}^{2/4} \right\}.$$  \( (7) \)

From Eq.(6) and Eq.(7), we know that, the probability, which Bell operator measurement of particle 1 and 3 is same as particle 1’ and 3’, is only $$\frac{1}{4}$$, when Bob send some his measurement results to Alice, Alice can find if there is eavesdropper. So we can say this protocol is secure.

4 Conclusion

We have given an effective quantum key distribution protocol, if the two legitimate parties shared much enough entangled pairs before the random key distribution, then there is no particle to be transported. The efficiency can approach 1 bit secret communication per particle.

References

[1] C.H.Bennett, G.Brassard, in proc IEEE int conf on Computers System,and Signal Processing, Bangalore (IEEE, New York, 1984)P175
[2] A.K.Ekert, Phys.Rev.Lett 67 (1991)661
[3] C. H. Bennett, G. Brassard and N. D. Mermin, Phys. Rev. Lett.68 (1992) 557. C.H.Bennett, Phys.Rev.Lett.68 (1992)3121
[4] B. Huttner, N. Imoto, N. Gisin and T. Mor, Phys. Rev. A 51 (1995) 1863.
[5] D. Bruß, Phys. Rev. Lett. 81 (1998) 3018.
[6] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. 75 (1995) 1239
[7] M. Koashi and N. Imoto, Phys. Rev. Lett. 79 (1997) 2383.
[8] G. L. Long and X.S. Liu, quant-ph/0012056
[9] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert,Phys. Rev. Lett 71, 4287 (1993).
[10] A.Cabello,Phys. Rev. A 61 (2000) 052312
[11] C.Li,H.S.Song and Y.X.Luo,Phys. Lett. A 297 (2002) 121
Fig. 1 Random quantum key distribution protocol