Eur. Phys. J. B **41**, 75–78 (2004)
DOI: 10.1140/epjb/e2004-00296-4

THE EUROPEAN PHYSICAL JOURNAL B

A scheme for secure direct communication using EPR pairs and teleportation

F.L. Yan[1,2,a] and X.Q. Zhang[2]

[1] CCAST (World Laboratory), P.O. Box 8730, Beijing 100080, P.R. China
[2] Department of Physics, Hebei Normal University, Shijiazhuang 050016, P.R. China

Received 17 March 2004
Published online 30 September 2004 –

Abstract. A novel scheme for secure direct communication between Alice and Bob is proposed, where there is no need for establishing a shared secret key. The communication is based on Einstein-Podolsky-Rosen (EPR) pairs and teleportation between Alice and Bob. After insuring the security of the quantum channel (EPR pairs), Bob encodes the secret message directly on a sequence of particle states and transmits them to Alice by teleportation. In this scheme teleportation transmits Bob's message without revealing any information to a potential eavesdropper. Alice can read out the encoded messages directly by the measurement on her qubits. Because there is not a transmission of the qubit which carries the secret message between Alice and Bob, it is completely secure for direct secret communication if perfect quantum channel is used.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication

1 Introduction

Cryptography is an art to transmit information so that it is unintelligible and therefore useless to those who are not meant to have access to it. Cryptography schemes are only completely secure when the two communicating parties, Alice and Bob, establish a shared secret key before the transmission of a message. This means they first should create a secret key which is composed of a random bit sequence, not known to anyone else, and of the same length as the message.

As a matter of fact, it is difficult to establish securely a secret key composed of a random bit sequence through a classical channel. Fortunately, by using quantum mechanics principle people can make distribution of secret key.

Since Bennett and Brassard proposed the standard BB84 quantum key distribution (QKD) protocol [1] in 1984, QKD has been developed quickly. Up to now, there have already been a lot of theoretical QKD schemes, for instance in references [1–18]

Recently Beige et al. [19] proposed a quantum secure direct communication (QSDC) scheme, where the message is deterministically sent through the quantum channel, but can only be deduced after a final transmission of classical information. Following Beige's scheme, Boström and Felbinger presented a Ping-Pong QSDC scheme [20]. However Wójcik showed that it is insecure if it is operated in a noisy quantum channel [21]. More recently Deng et al [22] put forward a two-step quantum direct communication protocol using Einstein-Podolsky-Rosen (EPR) pair block. It was shown that it is provably secure. Unfortunately, in all these secure direct communication schemes it is necessary to send the qubits carrying secret messages in a public channel. Therefore, Eve can attack the qubits in transmission.

In this paper we present a scheme for secure direct communication between Alice and Bob, where there is no need for establishing a shared secret key. The scheme is based on EPR pairs and teleportation [23]. Because there is not a transmission of the qubit which carries the secret message between Alice and Bob in a public channel, it is completely secure for direct secret communication if perfect quantum channel is used.

The new protocol can be divided into two steps, one is to prepare EPR pairs (quantum channel), the other is to transmit messages using teleportation.

2 Preparing EPR pairs

Suppose that Alice and Bob share a set of entangled pairs of qubits in one of the Bell's states

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B), \quad (1)$$

[a] *Present address:* Department of Physics, Hebei Normal University, Shijiazhuang 050016, P.R. China
e-mail: gaoting@heinfo.net

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB}) = \frac{1}{\sqrt{2}}(|+\rangle_A|-\rangle_B + |-\rangle_A|+\rangle_B), \quad (2)$$

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}) = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B - |-\rangle_A|-\rangle_B), \quad (3)$$

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}) = \frac{1}{\sqrt{2}}(|-\rangle_A|+\rangle_B - |+\rangle_A|-\rangle_B), \quad (4)$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (5)$$

There are many different ways to obtain these states. For example, Alice could prepare the pairs and then send half of each to Bob. Or a third party could prepare the pairs and then send half of each to Alice and Bob. To test the purity of EPR pairs, Alice and Bob can select a random subset of EPR pairs, and test to see if they violate Bell's inequality [2]. Passing the test certifies that they continue to hold sufficiently pure, entangled quantum states. However, if tampering has occurred, Alice and Bob discard these EPR pairs, and new EPR pairs should be constructed again. Without loss of generality we suppose that all EPR pairs used in our scheme are the Bell state $|\Phi^+\rangle_{AB}$.

3 Secure direct communication using teleportation

After insuring the security of the quantum channel (EPR pairs), we begin secure direct communication. Suppose that Bob has a particle sequence and he wishes to communicate information to Alice. First Bob makes his particle sequence in the states, composed of $|+\rangle$ and $|-\rangle$, according to the message sequence. For example if the message to be transmitted is 01001, then the sequence of particle states should be in the state $|+\rangle|-\rangle|+\rangle|+\rangle|-\rangle$, i.e. $|+\rangle$ and $|-\rangle$ correspond to 0 and 1 respectively. Remarkably quantum entanglement of EPR pairs can serve as a channel for transmission of messages encoded in the sequence of particle states. This is the process so called quantum teleportation [23] which we now describe. We will use subscripts A and B for the systems which comprise $|\Phi^+\rangle_{AB}$ and the subscript C for Bob's particles with messages. The systems B and C are thus in Bob's possession and A is in Alice's possession. In components we write the qubit state carrying message

$$|\Psi\rangle_C = \frac{1}{\sqrt{2}}(|0\rangle_C + b|1\rangle_C), \quad (6)$$

where $b = 1$ and $b = -1$ correspond to $|+\rangle$ and $|-\rangle$ respectively. The overall state of the systems ABC is

$$\begin{aligned} &|\Phi^+\rangle_{AB}|\Psi\rangle_C \\ &= \frac{1}{2}(|00\rangle_{AB} + |11\rangle_{AB})(|0\rangle_C + b|1\rangle_C) \\ &= \frac{1}{2\sqrt{2}}\{(|0\rangle_A + b|1\rangle_A)|\Phi^+\rangle_{BC} + (|0\rangle_A - b|1\rangle_A)|\Phi^-\rangle_{BC} \\ &\quad + (b|0\rangle_A + |1\rangle_A)|\Psi^+\rangle_{BC} + (b|0\rangle_A - |1\rangle_A)|\Psi^-\rangle_{BC})\}. \end{aligned} \quad (7)$$

Bob performs a Bell measurement on his two particles BC, then each outcome will occur randomly with equal probability $\frac{1}{4}$. Hence after this measurement, the resulting state of Alice's particle will be respectively

$$\frac{1}{\sqrt{2}}(|0\rangle_A + b|1\rangle_A) = U_{00}|\Psi\rangle_A, \quad (8)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_A - b|1\rangle_A) = U_{01}|\Psi\rangle_A, \quad (9)$$

$$\frac{1}{\sqrt{2}}(b|0\rangle_A + |1\rangle_A) = U_{10}|\Psi\rangle_A, \quad (10)$$

$$\frac{1}{\sqrt{2}}(b|0\rangle_A - |1\rangle_A) = U_{11}|\Psi\rangle_A, \quad (11)$$

where U_{ij} are

$$U_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, U_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad U_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, U_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (12)$$

Evidently, in each case the state of Alice's particle is related to $|\Psi\rangle_C$ by a fixed unitary transformation U_{ij} independent of the identity of $|\Psi\rangle$. Bob sends his actual Bell measurement outcome to Alice in a public channel then Alice will be able to apply the corresponding inverse transformation U_{ij}^{-1} to her particle, restoring it to state $|\Psi\rangle_A$. After that Alice measures the basis $\{|+\rangle, |-\rangle\}$ and reads out the messages that Bob wants to transmit to her.

The quantum teleportation has two notable features. First, teleportation can achieve perfect transmission of delicate information across a noisy environment assuming that classical information is robust and easy to protect against noise (as it is). Also the entanglement of EPR pair is independent of the spatial location of Alice relative to Bob so that Bob can transfer the information without even knowing Alice's location – he needs only to broadcast his Bell measurement outcome. In the process of teleportation, Alice is left with a perfect instance of $|\Psi\rangle$ and the Bell measurement outcome, which is transmitted in a public channel, is random. So in our scheme teleportation transmits Bob's message without revealing any information to a potential eavesdropper if the quantum channel is perfect EPR pairs (perfect quantum channel).

4 Security of the scheme

The security of this protocol only depends on the perfect quantum channel (pure EPR pairs). Thus as long as

the quantum channel is perfect, our scheme is secure and confidential. By using the schemes testing the security of quantum channel in references [2,13,22], we can obtain a perfect quantum channel. So our scheme for direct communication using EPR pairs and teleportation is absolutely reliable, deterministic and secure.

We should point out that it is necessary to test the security of quantum channel, since a potential eavesdropper may obtain information as following:

(1) Eve can use the entanglement pair to obtain information. Suppose that Eve has a particle pair in the state $|\Phi^+\rangle_{DE}$. When Eve obtains particle B in preparing EPR pair, she performs a Bell measurement on the particles BD. Then the particles AE will be in one of the entanglement states $\{|\Phi^+\rangle_{AE}, |\Phi^-\rangle_{AE}, |\Psi^+\rangle_{AE}, |\Psi^-\rangle_{AE}\}$. The entanglement state will be determined by the measurement outcome according to the following equation

$$|\Phi^+\rangle_{AB}|\Phi^+\rangle_{DE} = \frac{1}{2}(|\Phi^+\rangle_{BD}|\Phi^+\rangle_{AE} + |\Phi^-\rangle_{BD}|\Phi^-\rangle_{AE} + |\Psi^+\rangle_{BD}|\Psi^+\rangle_{AE} + |\Psi^-\rangle_{BD}\rangle|\Psi^-\rangle_{AE}). \quad (13)$$

Suppose after the measurement the state of particles BD collapses to the state $|\Phi^-\rangle_{BD}$, thus the particles AE must be in the state $|\Phi^-\rangle_{AE}$. Then Eve will transmit the particle B to Bob. Both Alice and Bob do not know that there is a potential eavesdropper listening to their conversation if they do not test the quantum channel. Bob will proceed as usual. Therefore a part of messages might be leaked to Eve.

However by testing quantum channel we can find Eve and avoid the information being leaked. In fact after the Bell measurement performed by Eve, particles AE are in an entangled state

$$|\Phi^-\rangle_{AE} = \frac{1}{\sqrt{2}}(|+\rangle_A|-\rangle_E + |-\rangle_A|+\rangle_E), \quad (14)$$

and particles BD are also in an entangled state

$$|\Phi^-\rangle_{BD} = \frac{1}{\sqrt{2}}(|+\rangle_B|-\rangle_D + |-\rangle_B|+\rangle_D), \quad (15)$$

but there is not any correlation between A and B. So when Alice and Bob perform the measurement in the basis $\{|+\rangle, |-\rangle\}$ independently, the result will be random without any correlation. If it is the case we can assert that an eavesdropper exists and the EPR pairs should be discarded.

(2) Eve can obtain information by coupled EPR pair with her probe in preparing EPR pair. We can test whether the quantum channel is perfect or not in this case by the following strategy. We select a random subset of EPR pairs. Alice and Bob perform a measurement in basis $\{|0\rangle, |1\rangle\}$ or basis $\{|+\rangle, |-\rangle\}$ randomly. If the measurement outcomes are completely correlation in the same basis of Alice and Bob, then the quantum channel is completely perfect or secure, because EPR pair state is the simultaneous eigenstate of the operators $\sigma_x^A\sigma_x^B$ and $\sigma_z^A\sigma_z^B$ with the same eigenvalue 1. Here σ_x and σ_z are Pauli operators. However if the measurement outcomes of Alice and Bob are not correlation completely in the same basis chosen by Alice and Bob, there might be a potential Eve, who have coupled EPR pair with her probe. Here we omit the proof and give an example of this case only. Let Alice's particle A, Bob's particle B and Eve's particle F be in the following entangled state

$$|\Phi^+\rangle_{ABF} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABF} = \frac{1}{2}[|+\rangle_A(|+\rangle_B|+\rangle_F + |-\rangle_B|-\rangle_F) + |-\rangle_A(|+\rangle_B|-\rangle_F + |-\rangle_B|+\rangle_F)]. \quad (16)$$

If Alice and Bob perform a measurement in the basis $\{|+\rangle, |-\rangle\}$, Bob will obtain $|+\rangle_B$ and $|-\rangle_B$ in the same probability $\frac{1}{2}$ whether Alice's measurement outcome is $|+\rangle_A$ or $|-\rangle_A$. This means Alice's outcomes are not correlation with that of Bob's. If this case happens, evidently there is a potential eavesdropper. We should abandon the quantum channel.

As a matter of fact, in any case, as long as an eavesdropper exists, we can find her and insure the security of quantum channel to realize secure direct communication.

5 Summary

We give a scheme for secure direct communication. There is no need for establishing a shared secret key in this protocol. The communication is based on EPR pairs and teleportation between Alice and Bob. After insuring the security of the quantum channel (EPR pairs), Bob encodes the secret message directly on a sequence of particle states and transmits them to Alice by teleportation. Evidently teleportation transmits Bob's message without revealing any information to a potential eavesdropper. Alice can read out the encoded messages directly by the measurement on her qubits. Because there is not a transmission of the qubit which carries the secret message between Alice and Bob, it is completely secure for direct secret communication if perfect quantum channel is used.

In the schemes [19,20,22], the qubits carrying secret messages must be sent in a public channel. So, Eve can make interruption of communication by intercepting these particles with secret messages in the transmitting channel, although she can not obtain any information. However, in our scheme information was transmitted using teleportation, the communication can not be intercepted. Therefore our new protocol has high capacity to defend signal against interference.

Teleportation has been realized in the experiments [24–26], therefore our protocol for secure direct communication will be realized by experiment easily.

This work was supported by Hebei Natural Science Foundation under Grant No. A2004000141.

References

1. C.H. Bennett, G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179
2. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
3. C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
4. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)
5. C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992)
6. L. Goldenberg, L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995)
7. B. Huttner, N. Imoto, N. Gisin, T. Mor, Phys. Rev. A **51**, 1863 (1995)
8. M. Koashi, N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997)
9. D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998)
10. W.Y. Hwang, I.G. Koh, Y.D. Han, Phys. Lett. A **244**, 489 (1998)
11. A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000)
12. A. Cabello, Phys. Rev. A **61**, 052312 (2000)
13. G.L. Long, X.S. Liu, Phys. Rev. A **65**, 032302 (2002)
14. B.S. Shi, Y.K. Jiang, G.C. Guo, Appl. Phys. B **70**, 415 (2000)
15. P. Xue, C.F. Li, G.C. Guo, Phys. Rev. A **65**, 022317 (2002)
16. F.G. Deng et al., Chin. Phys. Lett. **19**, 893 (2002)
17. S.J.D. Phoenix, S.M. Barnett, P.D. Townsend, K.J. Blow, J. Modern Optics **42**, 1155 (1995)
18. H.-K. Lo, H.F. Chan, M. Ardehali, `arXiv:quant-ph/0011056`
19. A. Beige et al., Acta Phys. Pol. A **101**, 357 (2002)
20. K. Boström, T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002)
21. A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003)
22. F.G. Deng, G.L. Long, X.S. Liu, Phys. Rev. A **68**, 042317 (2003)
23. C.H. Bennett et al., Phys. Rev. Lett. **70**, 1895 (1993)
24. D. Bouwmeester et al., Nature **390**, 575 (1997)
25. D. Boschi et al., Phys. Rev. Lett. **80**, 1121 (1998)
26. M.A. Nielsen et al., Nature **396**, 52 (1998)