Int J Theor Phys (2008) 47: 3401–3407
DOI 10.1007/s10773-008-9771-5

Secure Direct Communication Based on Non-Orthogonal Entangled Pairs and Local Measurement

Xiao-jie Yi · Yi-You Nie · Nan-run Zhou · Yi-bing Huang · Zhi-hui Hong

Received: 24 March 2008 / Accepted: 28 May 2008 / Published online: 13 June 2008

Abstract We propose a quantum secure direct communication scheme based on non-orthogonal entangled pairs and local measurement. In this scheme, we use eight non-orthogonal entangled pairs to act as quantum channels. Due to the non-orthogonality of the quantum channels, the present protocol can availably prohibit from all kinds of valid eavesdropping and acquire a secure quantum channel. By local measurement, the sender acquires a secret random sequence. The process of encoding on the random sequence is identical to the one in one-time-pad. So the present protocol is secure. Even for a highly lossy channel, our scheme is also valid. The scheme is feasible with present-day techniques.

Keywords QSDC · Non-orthogonal entangled pairs · Quantum cryptography · Information security

1 Introduce

The combination of quantum mechanics with information theory has produced many interesting and important developments in the field of transmission and processing of information. Quantum key distribution (QKD) is one of the many important applications of quantum mechanics, which provides a secure way to create a private key between two remote parties, the sender, Alice and the receiver, Bob. The non-cloning theorem [1] prohibits a vicious eavesdropper (Eve) from copying perfectly the quantum signal transmitted through a quantum channel, and an eavsdropping event will inevitably disturb the quantum system and leave a track as a result. Alice and Bob can find out Eve by comparing some of the results

X.-j. Yi · Y.-Y. Nie (✉) · Y.-b. Huang · Z.-h. Hong
Coll. of Physics & Communication Electronics, Jiangxi Normal Univ., Nanchang 330027, China
e-mail: nieyiyou@jxnu.edu.cn

Y.-Y. Nie
Key Laboratory of Photoelectron & Telecommunication of Jiangxi Province, Nanchang 330022, China

N.-r. Zhou
Dept. of Electronics Information Engineering, Nanchang Univ., Nanchang 330031, China

chosen randomly and analyzing the error rate. Combined with a private key, secret message can be transmitted securely with one-time-pad algorithm or its modifications [2]. Since Bennett and Brassard proposed the standard BB84 QKD protocol [3] in 1984, QKD has attracted widespread attention and progressed quickly [3–10] over the past two decades.

In recent years, a novel concept, quantum secure direct communication (QSDC) was proposed and actively pursued by some groups [11–31]. Different from quantum key distribution with a goal of generating a common random private key between two parties, QSDC is to transmit the secret message directly without establishing in advance a shared random key to encrypt it. By virtue of the security base of QSDC, they can be attributed to one of the two types. The first one includes the protocols [11–13] similar to BB84 protocol [3]. In these schemes, because quantum states carrying secret message are not orthogonal, the no-cloning theorem prevents any eavesdropper from perfectly copying them and the uncertainty law prohibits any eavesdropper from distinguishing them without disturbing them. The other one includes the protocols [14–31] similar to E91 protocol [4], in which the quantum states carrying secret message are Bell states. Because every particle in Bell states is in a completely mixed state, Eve can't get any useful information from EPR pair only by access to one particle in an EPR pair. Furthermore, any valid attack would disturb the relativity of the two particles in an EPR pair. In this work, we propose an efficient QSDC scheme based on the ideas of the non-orthogonality of entangled pair states and the onetime pad, which is also discussed in [13, 21, 22].

2 The QSDC Scheme

An Einstein-Podolsky-Rosen (EPR) pair is in one of the four Bell states shown as follows

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{HT} = \frac{1}{\sqrt{2}}(|{+}{+}\rangle - |{-}{-}\rangle)_{HT}, \tag{1}$$

$$\left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{HT} = \frac{1}{\sqrt{2}}(|{+}{-}\rangle - |{-}{+}\rangle)_{HT}, \tag{2}$$

$$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{HT} = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)_{HT}, \tag{3}$$

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{HT} = \frac{1}{\sqrt{2}}(|{+}{-}\rangle + |{-}{+}\rangle)_{HT}, \tag{4}$$

where $|0\rangle$ and $|1\rangle$ are the eigenvectors of the operator σ_z. After a Hadamard (H) operation on the second particle of every Bell state,

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{5}$$

the four Bell states become

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|0{-}\rangle + |1{+}\rangle)_{HT} = \frac{1}{\sqrt{2}}(|{+}0\rangle - |{-}1\rangle)_{HT}, \tag{6}$$

$$\left|\Phi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|0{-}\rangle - |1{+}\rangle)_{HT} = \frac{1}{\sqrt{2}}(|{+}1\rangle - |{-}0\rangle)_{HT}, \tag{7}$$

$$\left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)_{HT} = \frac{1}{\sqrt{2}}(|+0\rangle + |-1\rangle)_{HT}, \tag{8}$$

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|0+\rangle - |1-\rangle)_{HT} = \frac{1}{\sqrt{2}}(|+1\rangle + |-0\rangle)_{HT}, \tag{9}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are the two eigenvectors of the operator σ_x. Now let us describe the scheme in detail as follows:

(1) Alice and Bob agree on in advance that both the $|0\rangle$ and $|+\rangle$ states represent the binary value 0, and both the $|1\rangle$ and $|-\rangle$ states represent the binary value 1, as in the BB84 QKD protocol.

(2) Bob prepares N ordered entangled photon pairs, which are randomly in one of the eight entangled states $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle, |\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$. Bob takes T photon from each entangled pair to form an partner photon sequence $[T_1, T_2, T_3, \ldots, T_N]$ and it is called the T sequence for short. The remaining photons compose the other sequence $[H_1, H_2, H_3, \ldots, H_N]$ or H sequence for short. Then Bob sends the T sequence to Alice.

(3) After receiving the T sequence, Alice randomly chooses a subset of photons from T sequence and then measures them in the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly. Alice tells Bob the position, the measuring basis and the outcome of the measurement for each sampling photon. With the information, Bob measures the corresponding photon in the H sequence in the corresponding measuring basis and compares the measuring results with Alice's. If their results are completely correlated, Bob can decide that Eve is not online and continue to perform next step. Otherwise, they must terminate the communication.

(4) Bob measures the remaining photons of the H sequence in the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly and acquires a random sequence consisted of the states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. At the same time, the entangled pairs which Alice and Bob shared will collapse and the state of Alice's photons will be completely determined. So Alice also gets a random sequence consisted of the states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. However, no one knows his measurement result except Bob and then only Bob knows the state of the photons in the two random sequences.

(5) After Bob's measurement, Alice encodes her secret message in the T sequence. In order to prevent any eavesdropping during the transmission process, Alice randomly chooses some photons in the T sequence and randomly performs one of the two operations $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ or $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ on them as in [13], and then performs a hadamard operation H on the resulted state. Alice keeps the position and the performed operation of the sampling photons secret until the communication is completed. Alice encodes her secret message on the remaining photons in the T sequence with one of the two unitary operators, I and $i\sigma_y$. The operation $i\sigma_y$ can flip the state in both measuring bases,

$$i\sigma_y |0\rangle = -|1\rangle, \qquad i\sigma_y |1\rangle = |0\rangle, \tag{10}$$

$$i\sigma_y |+\rangle = |-\rangle, \qquad i\sigma_y |-\rangle = -|+\rangle. \tag{11}$$

According to the secret message 0 and 1, Alice performs operations I and $i\sigma_y$ on her photon, respectively. Then Alice sends them back to Bob.

(6) After confirming the transmission of the T sequence, Alice tells Bob the position of the sampling photons and the operations on them. Bob measures these sampling photons in a corresponding basis and analyzes their error rate. If the error rate is reasonably low, they will trust this communication, and Bob measures the remaining photons in the corresponding basis and reads out the secret message directly. Otherwise, they must terminate the communication and repeat the process from the beginning.

3 Security Analyses

As usual, Eve is assumed to be limited only by the laws of quantum mechanics. First, we note that in most QSDC protocols based on entangled pairs, because only a kind of Bell state is used to act as the quantum channel, Eve is easy to prepare the same Bell state and takes intercept-resend attack to acquire all information including checking message without being detected [19]. However, this situation can be avoided in our protocol. Quantum channel is randomly in one of the eight entangled states instead of one of the Bell states. Moreover, the two base sets $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ and $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$ are not orthogonal, which can prohibit anyone from distinguishing them perfectly. So our QSDC scheme is secure for any useful intercept-resend attack strategies.

Second, according to Stinespring dilation theorem, a unitary operator on a larger Hilbert space can realize Eve's eavesdropping attack. Suppose Eve adds ancillary photon in the state $|E\rangle$ and performs a unitary operation $\hat{E}$ on both systems to entangle her photon to the traveling photon. When the state of the traveling photons is in one of the states $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$, Eve's effect on the system is described as follows

$$\hat{E}\,|0,E\rangle = \hat{E}\,|0\rangle_T\,|E\rangle = \alpha\,|0\rangle_T\,|\varepsilon_{00}\rangle + \beta\,|1\rangle_T\,|\varepsilon_{01}\rangle = \alpha\,|0,\varepsilon_{00}\rangle + \beta\,|1,\varepsilon_{01}\rangle\,, \tag{12}$$

$$\hat{E}\,|1,E\rangle = \hat{E}\,|1\rangle_T\,|E\rangle = \beta'\,|0\rangle_T\,|\varepsilon_{10}\rangle + \alpha'\,|1\rangle_T\,|\varepsilon_{11}\rangle = \beta'\,|0,\varepsilon_{10}\rangle + \alpha'\,|1,\varepsilon_{11}\rangle\,. \tag{13}$$

Since the operator $\hat{E}$ must be unitary, we have

$$\begin{aligned} |\alpha|^2 + |\beta'|^2 &= 1,\\ |\alpha'|^2 + |\beta|^2 &= 1,\\ \alpha\beta^* + \alpha'^*\beta' &= 0. \end{aligned} \tag{14}$$

At this point, Eve's attack will lead to an error rate $e = |\beta|^2 = |\beta'|^2 = 1 - |\alpha|^2 = 1 - |\alpha'|^2$. When the state of the traveling photons is in one of the states $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$, Eve's effect on the system is described as follows

$$\begin{aligned} \hat{E}\,|+,E\rangle &= \frac{1}{\sqrt{2}}[\alpha\,|0,\varepsilon_{00}\rangle + \beta\,|1,\varepsilon_{01}\rangle + \beta'\,|1,\varepsilon_{10}\rangle + \alpha'\,|0,\varepsilon_{11}\rangle]\\ &= \frac{1}{\sqrt{2}}\left[|+\rangle\left[\frac{1}{\sqrt{2}}(\alpha\,|\varepsilon_{00}\rangle + \beta\,|\varepsilon_{01}\rangle + \beta'\,|\varepsilon_{10}\rangle + \alpha'\,|\varepsilon_{11}\rangle)\right]\right.\\ &\quad \left. + |-\rangle\left[\frac{1}{\sqrt{2}}(\alpha\,|\varepsilon_{00}\rangle - \beta\,|\varepsilon_{01}\rangle + \beta'\,|\varepsilon_{10}\rangle - \alpha'\,|\varepsilon_{11}\rangle)\right]\right]\\ &= \frac{1}{\sqrt{2}}(|+\rangle\,|\varepsilon_{++}\rangle + |-\rangle\,|\varepsilon_{+-}\rangle\,, \end{aligned} \tag{15}$$

$$\begin{aligned} \hat{E}\,|-,E\rangle &= \frac{1}{\sqrt{2}}[\alpha\,|0,\varepsilon_{00}\rangle + \beta\,|1,\varepsilon_{01}\rangle - \beta'\,|1,\varepsilon_{10}\rangle - \alpha'\,|0,\varepsilon_{11}\rangle]\\ &= \frac{1}{\sqrt{2}}\left[|+\rangle\left[\frac{1}{\sqrt{2}}(\alpha\,|\varepsilon_{00}\rangle + \beta\,|\varepsilon_{01}\rangle - \beta'\,|\varepsilon_{10}\rangle - \alpha'\,|\varepsilon_{11}\rangle)\right]\right.\\ &\quad \left. + |-\rangle\left[\frac{1}{\sqrt{2}}(\alpha\,|\varepsilon_{00}\rangle - \beta\,|\varepsilon_{01}\rangle - \beta'\,|\varepsilon_{10}\rangle + \alpha'\,|\varepsilon_{11}\rangle)\right]\right]\\ &= \frac{1}{\sqrt{2}}(|+\rangle\,|\varepsilon_{-+}\rangle + |-\rangle\,|\varepsilon_{--}\rangle\,. \end{aligned} \tag{16}$$

As long as Eve would attack the traveling photons, her action must result in an error rate of $1/2$. Moreover, even if Alice and Bob didn't find out Eve's eavesdropping in the checking process, due to the non-orthogonality between the state sets $\{|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle\}$ and $\{|\varepsilon_{++}\rangle, |\varepsilon_{+-}\rangle, |\varepsilon_{-+}\rangle, |\varepsilon_{--}\rangle\}$, Eve can't get any useful information from her ancillary photons. On average, Eve's action will introduce an error rate of $(1+2e)/4$, for every ancillary photon, and Alice have a probability of $(1+2e)/4$ to obtain a wrong result.

Third, the Trojan horse attack strategy [6, 32] gets no useful information. Suppose an attacker has lurked a Trojan horse U in Alice or Bob's apparatus in advance, which can identify the quantum states $|0\rangle$ and $|1\rangle$, the entangled states influenced by the Trojan horse are given as

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0^{\parallel}1^{\perp}\right\rangle \pm \left|1^{\perp}0^{\parallel}\right\rangle\right)_{HT}, \tag{17}$$

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0^{\parallel}0^{\parallel}\right\rangle \pm \left|1^{\perp}1^{\perp}\right\rangle\right)_{HT}. \tag{18}$$

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0^{\parallel}-^{?}\right\rangle \pm \left|1^{\perp}+^{?}\right\rangle\right)_{HT}, \tag{19}$$

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0^{\parallel}+^{?}\right\rangle \pm \left|1^{\perp}-^{?}\right\rangle\right)_{HT}. \tag{20}$$

Equations (17)–(20) indicates that if the qubits are in quantum state $|0\rangle$ or $|1\rangle$, then the Trojan horse feedbacks information $\parallel$ or $\perp$, respectively. However, if the qubits are in quantum state $|+\rangle$ or $|-\rangle$, there are no determined feedback information, which is represented by the notion ? in (19)–(20). That is to say, a Trojan horse cannot distinguish non-orthogonal states as quantum mechanics implies. Therefore, Trojan horse attack strategy is invalid in practice.

We note that the process of encoding secret message in our scheme is completely identical to that in [13]. In [13], it is claimed that: *First we notice that the encoding of secret messages in the second phase (doves returning phase) is identical to the process in a one-time pad encryption where the text is encrypted with a random key as the state of the photon in the B batch is completely random. In a one-time pad encryption, it is completely safe and no secret messages can be leaked even if the cipher text is intercepted by the eavesdropper. Here the quantum-one-time pad QSDC protocol is even more secure than the classical one-time pad in the sense that an eavesdropper cannot even intercept the whole cipher text as the photons' measuring basis is chosen randomly.* Therefore, our proposed scheme is completely secure.

4 Discussion and Summary

Our present protocol is secure in ideal lossless channels from the above analysis. However, in a practical quantum channel, the channels are noisy and lossy in reality, which will threaten the security of quantum communication. In a weak noisy channel, an eavesdropper attack action will increase either the error rate or a loss of signal, so a higher error rate or a loss of signal may indicate an eavesdropping event. Even if in a high noisy channel, because the entangled pair is randomly in one of the eight states $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle, |\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$ and the two base sets $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ and $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$ are non-orthogonal, Eve's any valid attack can be detected. In the meantime, in order to check eavesdropping, we introduce a Hadamard

transform H in step (5). It is known that

$$\begin{aligned} H|0\rangle &= |+\rangle, \qquad H|1\rangle = |-\rangle, \\ H|+\rangle &= |0\rangle, \qquad H|-\rangle = |1\rangle. \end{aligned} \tag{21}$$

So an eavesdropper's attack will introduce additional error rate. Compared with the other similar protocols [11–13, 21–27, 31], the implementation of the present protocol is the same as them; moreover, due to the use the eight non-orthogonal entangled pairs to act as quantum channels, the present protocol can more effectively repel all kinds of the valid intercept-resent attacks and entangle-measure attacks, which is the advantage of the present protocol. In addition, in our scheme Alice need not make Bell measurement on the two photons, but she only needs to make a local measurement. Therefore, our proposed scheme is easier to realize in experiment. However, to transmit a two-bit message, in the present protocol two entangled photon pair have to be consumed while in [22] only a entangled pair is consumed. This is a disadvantage of the present protocol.

In summary, based on non-orthogonal entangled pairs and local measurement, a new quantum secure direct communication scheme is proposed. In this scheme, quantum channel is randomly in one of the eight non-orthogonal entangled pairs, in order to ensure the security of the channel. By local measurement, Alice gets a random sequence that only Bob knows. The secret message encoded on the random sequence is transmitted securely.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 10647133 and No. 10404010); the Natural Science Foundation of Jiangxi Province, China; the Research Foundation of the Education Department of Jiangxi Province.

References

1. Wootters, W.K., Zurek, W.H.: Nature **299**, 802 (1982)
2. Zhou, N., Liu, Y., Zeng, G., Xiong, J., Zhu, F.: Physica A **375**, 693 (2007)
3. Bennett, C.H., Brassard, G.: In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179. IEEE Press, New York (1984)
4. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
5. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
6. Gisin, N., Ribordy, G., Tattle, W., Zbinden, H.: Rev. Mod. Phys. **74**, 145 (2002)
7. Long, G.L., Liu, X.S.: Phys. Rev. A **65**, 032302 (2002)
8. Deng, F.G., Long, G.L.: Phys. Rev. A **68**, 042315 (2003)
9. Deng, F.G., Long, G.L.: Phys. Rev. A **70**, 012311 (2004)
10. Zhang, Y.S., Li, C.F., Guo, G.C.: Phys. Rev. A **64**, 024302 (2001)
11. Lucamarimi, M., Mancini, S.: Phys. Rev. Lett. **94**, 140501 (2005)
12. Cai, Q.Y., Li, B.W.: Chin. Phys. Lett. **21**, 601 (2004)
13. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
14. W'ojcik, A.: Phys. Rev. Lett. **90**, 157901 (2003)
15. Zhang, Z.J., Man, Z.X., Li, Y.: Phys. Lett. A **333**, 46 (2004)
16. Cai, Q.Y.: Phys. Rev. Lett. **91**, 109801 (2003)
17. Zhang, Z.J., Man, Z.X., Li, Y.: Int. J. Quantum Inf. **2**, 521 (2004)
18. Zhang, Z.J., Li, Y., Man, Z.X.: Phys. Lett. A **341**, 385 (2005)
19. Zhu, A.D., Xia, Y., Fan, Q.B., Zhang, S.: Phys. Rev. A **73**, 022338 (2006)
20. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: Acta Phys. Pol. A **101**, 57 (2002)
21. Bostrom, K., Felbinger, T.: Phys. Rev. Lett. **89**, 187902 (2002)
22. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
23. Yan, F.L., Zhang, X.Q.: Eur. Phys. J. B **41**, 75 (2004)
24. Gao, T., Yan, F.L., Wang, Z.X.: Nuovo Cim. B **119**, 313 (2004)
25. Gao, T., Yan, F.L., Wang, Z.X.: J. Phys. A **38**, 5761 (2005)
26. Wang, C., Deng, F.G., Long, G.L.: Opt. Commun. **253**, 15 (2005)

27. Wang, C., et al.: Phys. Rev. A **71**, 044305 (2005)
28. Lee, H., Lim, J., Yang, H.J.: Phys. Rev. A **73**, 04230 (2006)
29. Zhang, Z.J., Liu, J., Wang, D., Shi, S.H.: Phys. Rev. A **75**, 026301 (2007)
30. Man, Z.X., Zhang, Z.J., Li, Y.: Chin. Phys. Lett. **22**, 18 (2005)
31. Cai, Q.Y., Li, B.W.: Phys. Rev. A **69**, 054301 (2004)
32. Zhou, N.R., Zeng, G.H., Nie, Y.Y., Xiong, J., Zhu, F.C.: Physica A **362**, 305 (2006)