Vol 16 No 7, July 2007
1009-1963/2007/16(07)/1838-05

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

An efficient quantum secure direct communication scheme with authentication*

Yang Yu-Guang(杨宇光)[a)b)], Wen Qiao-Yan(温巧燕)[c)], and Zhu Fu-Chen(朱甫臣)[d)]

[a)] *School of Computer Science and Technology, Beijing University of Technology, Beijing* 100022, *China*
[b)] *State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing* 100022, *China*
[c)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[d)] *National Key Laboratory for Modern Communications, Chengdu* 610041, *China*

(Received 28 April 2006; revised manuscript received 16 May 2006)

In this paper an efficient quantum secure direct communication (QSDC) scheme with authentication is presented, which is based on quantum entanglement and polarized single photons. The present protocol uses Einstein–Podolsky–Rosen (EPR) pairs and polarized single photons in batches. A particle of the EPR pairs is retained in the sender's station, and the other is transmitted forth and back between the sender and the receiver, similar to the 'ping–pong' QSDC protocol. According to the shared information beforehand, these two kinds of quantum states are mixed and then transmitted via a quantum channel. The EPR pairs are used to transmit secret messages and the polarized single photons used for authentication and eavesdropping check. Consequently, because of the dual contributions of the polarized single photons, no classical information is needed. The intrinsic efficiency and total efficiency are both 1 in this scheme as almost all of the instances are useful and each EPR pair can be used to carry two bits of information.

Keywords: quantum key distribution, quantum authentication, quantum secure direct communication, non-orthogonal

PACC: 0365

1. Introduction

Quantum key distribution (QKD) provides a novel way for two legitimate parties to establish a common secret key over a long distance. QKD has progressed quickly[1−12] since Bennett and Brassard designed the original QKD protocol.[1]

Recently, a novel branch of quantum communication, quantum secure direct communication (QSDC), was proposed and actively pursued by some groups.[13−26] With QSDC, Bob and Carol can exchange the secret message directly without generating a private key in advance and then encrypting the message, which is different from QKD. In 2002, Beige[26] presented a QSDC protocol in which the message can be read out after the transmission of an additional classical information for each qubit,[13,14] similar to a QKD scheme as each bit of key can represent one bit of secret message with an additional classical information, i.e., retaining or flipping the bit value in the key according to the secret message.[13] The same case takes place in Refs.[17–19]. In 2002, Boström and Felbinger proposed a ping–pong QSDC following some ideas in quantum dense coding[27] with an EPR pair. The authors have claimed that it is secure for generating a private key and quasi-secure for direct communication as it will leak some of the secret message in a noisy channel.[20] Wójcik[28] and Zhang *et al*[29] pointed out that the ping–pong protocol is insecure for direct communication if there are losses in a practical quantum channel. Also, the ping–pong protocol[20] can be attacked without eavesdropping.[30,31] Cai and Li[21] modified the ping–pong protocol for transmitting the secret message directly by replacing the entangled photons with non-orthogonal particles in mixed state, similar to the Bennett 1992 QKD,[4] and inherited its nature of insecurity[14] as it is vulnerable to the opaque attack which is discussed in Ref.[4]. Meanwhile, Deng *et al* put forward a two-step QSDC protocol[13] with EPR pairs transmitted in block and another one based on a sequence of polarized non-orthogonal particles.[14]

*Project supported by the National High Technology Research and Development Program of China (Grant No 2006AA01Z419), the Major Research plan of the National Natural Science Foundation of China (Grant No 90604023), National Laboratory for Moderm Communications Science Foundation of China (Grant No 9140C1101010601) and the Open Foundation of State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences).

Wang *et al* introduced a QSDC protocol with high-dimension quantum superdense coding.[15] The good nature of the QSDC schemes[13−16] with quantum data block is that the parties can perform quantum privacy amplification[32,33] on the unknown states for improving their security in a noisy channel. In Ref.[24], Cai and Li designed a protocol for improving the capacity of the ping–pong QSDC protocol[20] with the same way for eavesdropping check as that in Ref.[13]. However, it is not unconditionally secure as the analysis of eavesdropping check depends on the feature of statistics for which a lot of samples should be chosen randomly and measured. Recently, Lucamarini and Mancini[25] introduced a QSDC protocol for both direct communication and created a private key with some ideas in the Refs.[9, 14]. It is secure for QKD, same as Ref.[9], but it is just quasi-secure for direct communication, similar to the QSDC protocol in Ref.[24].

The previous QSDC schemes are presented under the condition that the parties of communication are legitimate. However, in practical conditions, it is possible that an impersonator exists. In this paper, based on the ideas from the QSDC with entanglement,[13] ping–pong protocol,[20] the QSDC[14,21,34] with non-orthogonal particles and quantum dense coding,[27] an efficient QSDC scheme with authentication is presented, which is based on quantum entanglement and non-orthogonal particles. The present protocol uses EPR pairs and non-orthogonal particles in batches. According to the shared information beforehand, these two kinds of quantum states are mixed and then transmitted via a quantum channel. A particle of EPR pairs is retained in the sender's station, and the other is transmitted to and forth between the sender and the receiver, similar to 'ping–pong' QSDC protocol. The EPR pairs are used to transmit secret messages and the non-orthogonal particles used for authentication and eavesdropping check. Consequently, because of the dual contributions of non-orthogonal particles, no classical information is needed. And the intrinsic efficiency and total efficiency are both 1 in this scheme as almost all of the instances are useful and each EPR pair can be used to carry two bits of information.

2. The QSDC scheme

An EPR pair is in one of the four Bell states shown as follows:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\rm A}|1\rangle_{\rm B} - |1\rangle_{\rm A}|0\rangle_{\rm B}), \tag{1}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\rm A}|1\rangle_{\rm B} + |1\rangle_{\rm A}|0\rangle_{\rm B}), \tag{2}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\rm A}|0\rangle_{\rm B} - |1\rangle_{\rm A}|1\rangle_{\rm B}), \tag{3}$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\rm A}|0\rangle_{\rm B} + |1\rangle_{\rm A}|1\rangle_{\rm B}). \tag{4}$$

Here $|0\rangle$ and $|1\rangle$ are the up and down eigenstate of σ_z, the photon polarization operator. If we measure the state of a non-orthogonal particle, the Bell-state will collapse and the state of the other particle will be completely determined if we know the measurement result of the first photon. For example, if we measure the state of photon A in the Bell state $|\psi^-\rangle$ and obtain $|0\rangle$, then the state of photon B will collapse to quantum state $|1\rangle$. Four unitary operations $\{U_0, U_1, U_2, U_3\}$ can transform the state $|\psi^-\rangle$ into $|\psi^-\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, $|\phi^+\rangle$, respectively:

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{5}$$

$$U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{6}$$

$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \tag{7}$$

$$U_3 = {\rm i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \tag{8}$$

where I is 2×2 identity matrix. $\sigma_i (i = x, y, z)$ is Pauli matrix, that is

$$I \otimes U_0|\psi^\pm\rangle = |\psi^\pm\rangle, \quad I \otimes U_0|\phi^\pm\rangle = |\phi^\pm\rangle, \tag{9}$$

$$I \otimes U_1|\psi^\pm\rangle = |\psi^\mp\rangle, \quad I \otimes U_1|\phi^\pm\rangle = -|\phi^\mp\rangle, \tag{10}$$

$$I \otimes U_2|\psi^\pm\rangle = |\phi^\pm\rangle, \quad I \otimes U_2|\phi^\pm\rangle = |\psi^\pm\rangle, \tag{11}$$

$$I \otimes U_3|\psi^\pm\rangle = -|\phi^\mp\rangle, \quad I \otimes U_3|\phi^\pm\rangle = |\psi^\mp\rangle. \tag{12}$$

Similar to the BB84 QKD protocol,[1] Alice and Bob use two measuring bases (MBs), namely the rectilinear basis, i.e. $\{|H\rangle = |0\rangle, |V\rangle = |1\rangle\}$ and the diagonal basis, i.e.

$$\{|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|d\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\},$$

where $|H\rangle$ and $|V\rangle$ are the horizontal and vertical polarization states respectively. As in the BB84 QKD protocol, the $|0\rangle$ and $|u\rangle$ states represent the binary value 0, and the $|1\rangle$ and $|d\rangle$ states represent binary

value 1. For simplicity we call them as the $\oplus$ basis and $\otimes$ basis respectively. B represents basis and V represents value. 0 in B represents $\oplus$ basis and 1 represents $\otimes$ basis. 0 in $\oplus$ basis represents $|0\rangle$ state and 1 represents $|1\rangle$ state. 0 in $\otimes$ basis represents $|u\rangle$ state and 1 represents $|d\rangle$ state. For example, $B = 01100101$, $V = 10110100$, then these non-orthogonal states are $|1\rangle|u\rangle|d\rangle|1\rangle|0\rangle|d\rangle|0\rangle|u\rangle$ respectively.

The details of the present QSDC are as follows:

(1) Alice and Bob agree on that these four unitary operations correspond to 00, 01, 10, 11, respectively.

(2) Alice and Bob share a seed key S in advance, and then extend S to S' with a length enough to check eavesdropping in the quantum line by using an extension function G. The selection of G should make the obtained S' satisfy the randomness condition, for example, the number of 0 and 1 is equal.

(3) Alice and Bob divide S' into S'_1 and S'_2 equally. S'_1 and S'_2 are used for the authentication of the identity of Alice and Bob respectively. $S'_1(S'_2)$ is subdivided into S'_{11}, S'_{12}, S'_{13} (S'_{21}, S'_{22}, S'_{23}) equally. $S'_{11}(S'_{21})$ represents the information of basis B, and $S'_{12}(S'_{22})$ represents the information of value V. $S'_{13}(S'_{23})$ is used to designate the positions of the inserted non-orthogonal particles. According to S'_{11} and S'_{12}, Alice prepares the non-orthogonal particles in batch and inserts them into the positions designated by S'_{13}. Then in the other positions the entangled particles are in randomly one of the four states in Eqs.(1)–(4). Alice transmits in order all the particles to Bob. The remaining particles of all the EPR pairs are retained in Alice's station.

(4) To verify the identity of Alice and check eavesdropping. According to S'_1, Bob makes the corresponding measurement on the non-orthogonal particles in the corresponding positions in the batch. If the difference between the outcomes of measurement and S'_{12} is tolerable, then it shows that Alice is authentic. And they continue to step (5); otherwise, Alice is fake or eavesdropper exists. Bob terminates the communication.

(5) According to the secret message he wants to transmit to Alice, Bob makes the corresponding unitary operation on the entangled particles in the other positions. Based on the values of S'_{21} and S'_{22}, Bob also prepares a non-orthogonal particle sequence and inserts them into the entangled particle sequence based on the value of S'_{23}. And then Bob sends the entangled particles and the newly prepared particles back to Alice.

(6) To verify the identity of Bob and check eavesdropping. According to S'_2, Alice makes the corresponding measurement on the non-orthogonal particles in the corresponding positions in the batch. If the difference between the outcomes of measurement and S'_{22} is tolerable, then it shows that Bob is authentic. And they continue to step (7); otherwise, Bob is fake or eavesdropper exists. Alice terminates the communication.

(7) Alice makes Bell measurement on the received entangled particles and the retained entangled particles, obtains the secret message of Bob. And then Alice and Bob continue to correct the errors in the secret message by using error correction method. This procedure is exactly the same as that in QKD.

As discussed above, Alice and Bob can ensure the security of the quantum channel before the secret message is transmitted. The impersonator or Eve will be found out if she eavesdrops the quantum line. It is of interest that Eve cannot read out the information encoded in the EPR pairs even if she captures one of the EPR pair, because no one can read the information from one particle of an EPR pair alone. In this way, no secret message will be leaked to Eve. It is secure. Moreover, the capacity is high in this protocol, because each of EPR pair carries two bits of classical information.

3. Security analysis

The QSDC protocol is secure, the reasons are as follows:

(1) The protocol uses two quantum channels. One is from Alice to Bob, the other from Bob to Alice. Before Bob makes the unitary operation, security of the quantum channel from Alice to Bob must be ensured. The procedure of eavesdropping check in the quantum channel from Alice to Bob is similar to BB84 protocol. The difference between the present QSDC protocol and BB84 protocol is that the non-orthogonal particles used in the present QSDC protocol is stored in batch, while the non-orthogonal particles are measured one by one in the BB84 protocol. The security of BB84 QKD is assured by means of the fact that Alice and Bob choose randomly sufficient instances for checking eavesdropping. The process of the QSDC scheme before Bob encodes his message by using the unitary operation is in fact identical to the variant of BB84 QKD process. The BB84 QKD has been proven to be unconditionally secure by several groups.[35] The

BB84 QKD protocol is secure even when the channel is noisy. In this way, the process for establishing a secure quantum channel in this QSDC scheme is proven to be unconditionally secure by this observation.

(2) The shared information S is only known by Alice and Bob. If Eve does not know S, it is impossible for her to insert the non-orthogonal particles into the correct positions. If Eve impersonates Alice, she can only transmit entangled particles. So her probability of successful impersonation is less than $(1/2)^n$ (if the length of the non-orthogonal particles designated by S'_{13} is n). The larger n is, the smaller the probability is.

(3) The properties of physics such as Heisenberg uncertainty principle and quantum no-cloning theorem ensure that the quantum information can not be eavesdropped without detection by legitimate parties. Eve has only one chance to measure these particles. According to Heisenberg uncertainty principle and quantum no-cloning principle, she cannot distinguish the non-orthogonal states and the entangled states. And her measurement inevitably introduces errors.

(4) No classical information is transmitted during the process of communication.

(5) The shared information S is used only once. After each successful communication, Alice and Bob change the seed key.

(6) The authentication and security of direct communication are done concurrently which prevents Eve to do a man-in-the-middle attack.

(7) Similar to Refs.[13,14], the essential difference between this protocol and the ping–pong protocol[20] and its variant[21] is that the security of the quantum channel is analysed first in a batch after batch manner and the encoding of the message is done only after the confirmation of the security of the quantum channel, while in the ping–pong protocol the security check and the encoding of messages are done concurrently. Since the security of the channel is assured first in this QSDC protocol, Eve can get nothing even though she monitors the rest of the process of communication.

One difference between the present QSDC and that in Ref.[14] is that the encoded particles are entangled particles, while in Ref.[14] the encoded particles are non-orthogonal particles. This does not reduce its security. Furthermore, its capacity of the QSDC is twice than that in Ref.[14].

In a practical channel, the robustness of two-way quantum communication protocols against Trojan horse attack is discussed in Ref.[36].

4. Conclusions

An efficient QSDC scheme with authentication is presented, which is based on quantum entanglement and non-orthogonal particles. According to the shared information beforehand, these two kinds of quantum states are mixed and then transmitted via a quantum channel. The EPR pairs are used to transmit secret messages and the non-orthogonal particles used for authentication and eavesdropping check. Consequently, because of the dual contributions of non-orthogonal particles, no classical information is needed. The intrinsic efficiency and total efficiency are both 1 in this scheme as almost all of the instances are useful and each EPR pair can be used to carry two bits of information.

Compared with the QSDC in Refs.[13,14], the present scheme has its shortcoming. That is, it uses two kinds of particles, so two kinds of devices have to be used to prepare the entangled particles and non-orthogonal particle.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984) pp175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[5] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[6] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[7] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
[8] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315
[9] Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311
[10] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **9** 3995 (in Chinese)
[11] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **12** 5544 (in Chinese)
[12] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **12** 5549 (in Chinese)
[13] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[14] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[15] Wang C, Deng F G and Long G L 2005 *Phys. Rev.* A **71** 044305

[16] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[17] Yan F L and Zhang X 2004 *Euro. Phys. J.* B **41** 75
[18] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[19] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
[20] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[21] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[22] Nguyen B A 2004 *Phys. Lett.* A **328** 6
[23] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 22
[24] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301
[25] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[26] Beige A 2002 *Acta Phys. Pol.* A **101** 357
[27] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **68** 3121
[28] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[29] Zhang Z J, Man Z X and Li Y 2005 *Phys. Lett.* A **341** 385
[30] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[31] Zhang Z J, Man Z X and Li Y 2004 *Int. J. Quantum Inform.* **2** 521
[32] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[33] Deng F G and Long G L 2004 quant-ph/0408102
[34] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[35] Mayers D 1998 quant-ph/9802025
Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 411
[36] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2005 quant-ph/0508168