Vol 17 No 11, November 2008
1674-1056/2008/17(11)/3991-05

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

Construction and application of multi-partner communication network

Xiu Xiao-Ming(修晓明), Dong Li(董 莉), Gao Ya-Jun(高亚军), and Chi Feng(迟 锋)

Department of Physics, Bohai University, Jinzhou 121000, *China*

(Received 17 November 2007; revised manuscript received 9 December 2007)

In this paper, we present a multi-partner communication network protocol. The supervisor prepares numerous Einstein–Podolsky–Rosen (EPR) pairs and auxiliary qubits. He then performs a controlled-NOT(CNOT) gate operation on one qubit of each EPR pair and an auxiliary, which induces the entanglement between the EPR pair and the auxiliary. The supervisor keeps one qubit sequence in his laboratory and sends the others to the outside world. After security approval, the network can be constructed successfully, which can be applied to quantum secret sharing and quantum secure direct communication.

Keywords: quantum information, quantum secret sharing, quantum secure direct communication
PACC: 0365

1. Introduction

Quantum cryptography[1] can make two legitimate partners communicate in privacy, and use quantum mechanics to guarantee the security of communication.

In a quantum key distribution (QKD) scheme, two partners firstly establish a shared secret key through the transmission of classical message and use this key to encrypt (decrypt) the secret message. The first QKD scheme was proposed by Bennett and Brassard in 1984,[2] i.e. BB84 scheme. Since then, many QKD schemes have been presented.[3−7]

Quantum secret sharing (QSS) is a process, in which a sender splits some secret information into several shares and distributes these shares to other partners. And there is an authorized partner, who can obtain the secret information by cooperating with other partners. The first QSS scheme was proposed by Hillery *et al*[8] using three-particle or four-particle Greenberger–Horne–Zeilinger (GHZ) states for sharing classical information. And Karlsson *et al*[9] presented a QSS scheme for quantum information with two-qubit entanglement. Some QSS schemes have been put forward.[10−13]

A secure communication scheme with or without a publicly known key was put forward by Beige *et al*,[14] that is, quantum secure direct communication (QSDC). After that, many topics have focused on QSDC schemes.[15−29] Boström and Felbinger[15] proposed the well-known 'Ping–Pong protocol' that allows the encoded bit to be decoded instantaneously in each respective transmission round. But it is insecure if it is in a lossy quantum channel, as indicated by Wójcik.[16] Also can the ping-pong protocol be attacked without eavesdropping.[17] Later on, Cai and Li modified the ping–pong protocol for transmitting the secret message with a single photon in a mixed state[18] and improved the capacity and security of 'Ping–Pong protocol'.[19] Subsequently, Lü *et al*[20] proposed the modified Cai–Li protocol in a noisy channel. Deng *et al* put forward a two-step QSDC protocol using blocks of Einstein–Podolsky–Rosen (EPR) pairs[21] and a QSDC scheme with a quantum one-time pad using single photons[22] to enhance the security of communication. Some QSDC schemes using teleportation[23−29] were presented, in which no qubit carrying secret message was transmitted. In Ref.[29], Lü *et al* came up with an unconditional secure communication scheme, in which the secret message could be transmitted in a lossy quantum channel.

There are many QKD net schemes,[30−35] in which a partner can communicate with anyone in the net. But in these schemes, a supervisor can steal the secret information without being detected. Deng *et al*[36] proposed two QSDC net schemes using N ordered EPR pairs, in which the authorized partners can communicate with each other securely.

In this paper, a scheme for constructing a multi-partner communication net is proposed. The supervisor mainly answers for the construction of communication net using EPR pairs and auxiliary qubits. If the security is ensured, quantum secret sharing and quantum secure direct communication (QSS–QSDC) can be successfully realized. The scheme needs only to perform single-qubit operations, CNOT gate operations and Bell-basis measurements.

The construction of a multi-partner communication net is proposed in Section 2. As for its application, a QSS–QSDC scheme is put forward in Section 3. And then, the security of the communication net and the QSS–QSDC scheme are discussed in Section 4. Finally, the discussion and conclusion are given in Section 5.

2. The construction of multi-partner communication net

In order to construct a multi-partner communication net, the following procedures should be performed.

(P1) The supervisor (say, Alice) introduces N EPR pairs numbered (A_l, B_l), $(l = 1, 2, \ldots, N)$ in the state denoted as

$$|\Phi^{\pm}\rangle_{A_l,B_l} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),$$
$$|\Psi^{\pm}\rangle_{A_l,B_l} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (1)$$

(P2) And she prepares auxiliary qubits $C_{l,j}$, $(l = 1, 2, \ldots, N;\ j = 1, 2, \ldots, M)$ in an initial state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

(P3) Alice sends qubit pairs $(C_{l,1}, A_l)$, $(C_{l,2}, A_l)$, …, $(C_{l,M}, A_l)$ through CNOT gates, that is, the former one in the each qubit pair is used as the control qubit and the latter one as the target qubit. In the CNOT gate, when the state of the control qubit is $|1\rangle$, the state of the target qubit $|1\rangle(|0\rangle)$ is changed into $|0\rangle(|1\rangle)$. And the state of target qubit cannot be changed when the state of the control qubit is $|0\rangle$.

(P4) Alice transmits the qubit sequences $(B_l, C_{l,1}, C_{l,2}, \ldots, C_{l,j}, \ldots, C_{l,M})$ to $M + 1$ partners (Bob, Charlie and David *et al*), respectively. The entangled state of the qubits for a same index (l) can be denoted as

$$|\xi_{l,M+2}\rangle_{A_l,B_l,C_{l,j}}$$
$$= \frac{1}{\sqrt{2}}(|i_{l,\mathrm{arb}}\rangle|\xi_{l,M+1}\rangle \pm |\bar{i}_{l,\mathrm{arb}}\rangle|\xi'_{l,M+1}\rangle), \quad (2)$$

where $|i_{l,\mathrm{arb}}\rangle$ denotes the state of arbitrary qubit in the multi-qubit entangled state. And $i_{l,\mathrm{arb}} = i_{l,1}, i_{l,2}, \ldots, i_{l,M+2} \in \{0, 1\}$, and $\bar{i}_{l,\mathrm{arb}} = \bar{i}_{l,1}, \bar{i}_{l,2}, \ldots, \bar{i}_{l,M+2}$ are the counterparts of the binary numbers $i_{l,1}, i_{l,2}, \ldots, i_{l,M+2}$, respectively. The state $|\xi_{l,M}\rangle\,(M \geq 2)$ is the $M-$ qubit maximally entangled state and conforms to the following condition:

$$\langle\xi_{l,M}|\xi'_{l,M}\rangle = 0,$$
$$|\xi_{l,M}\rangle = \frac{1}{\sqrt{2}}(|i_{l,\mathrm{arb}}\rangle|\xi_{l,M-1}\rangle \pm |\bar{i}_{l,\mathrm{arb}}\rangle|\xi'_{l,M-1}\rangle),$$
$$|\xi_{l,2}\rangle = \frac{1}{\sqrt{2}}(|i_{l,1}\rangle|i_{l,2}\rangle \pm |\bar{i}_{l,1}\rangle|\bar{i}_{l,2}\rangle),$$
$$|\xi'_{l,2}\rangle = \frac{1}{\sqrt{2}}(|\bar{i}_{l,1}\rangle|i_{l,2}\rangle \pm |i_{l,1}\rangle|\bar{i}_{l,2}\rangle). \quad (3)$$

(P5) Alice selects randomly a sufficiently large subset as a checking group to test the security of communication net. She asks the other partners to perform the measurement on the checking group by using one of two measurement bases $\{|0\rangle, |1\rangle\}$ or $\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$.

(P6) The other partners perform measurements along the same basis on the same numbered qubits according to Alice's requirement, and then transmit the measurement outcomes to Alice.

(P7) According to all the partners' measurement outcomes including hers, Alice analyses the security of communication net. If the original EPR state is $|\Phi^{+}\rangle$, the number of measurement outcomes $|1\rangle$ should be even. If the original EPR state is $|\Psi^{+}\rangle$, the number of measurement outcomes $|1\rangle$ should be odd. The measurement outcomes of all the partners should be the same when $\{|+\rangle, |-\rangle\}$ is adopted as the measurement basis.

If the error rate is reasonably low, the secure communication net is constructed successfully with the rest of qubits. Otherwise, she constructs a communication net again.

3. The QSS–QSDC scheme

If the security of communication net is ensured, a QSS–QSDC scheme can be realized in it. The supervisor can provide partners with quantum channels to complete different goals. Anyone in the net can share the secret message with the other partners, that is, quantum secret sharing. Two authorized partners can directly communicate in privacy, i.e. quantum secure

direct communication. For simplicity, the communication net is taken into consideration, which is comprised of the EPR pairs in the state $|\Phi^+\rangle$ ($|\Psi^+\rangle$) and auxiliary qubit with the initial state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The following steps are adopted to realize QSS–QSDC scheme.

(Q1) The sender (for example, Bob) prepares the state according to the content of a secret message

$$|\psi\rangle_{1,2,\ldots,N} = \prod_{l=1}^{N} \frac{1}{\sqrt{2}}(|0\rangle + b_l|1\rangle)_l, \tag{4}$$

where b_l equals 1(–1) according to the secret message 0(1). The whole system state can be denoted as

$$\begin{aligned} |\Psi\rangle &= |\psi\rangle_{1,2,\ldots,N} \otimes |\xi_{l,M+2}\rangle_{A_l,B_l,C_{l,j}} \\ &= \prod_{l=1}^{N} \frac{1}{2\sqrt{2}}[|\Phi^+\rangle_{l,A_l}(|\xi_{l,M+1}\rangle + b_l|\xi'_{l,M+1}\rangle) \\ &\quad +|\Phi^-\rangle_{l,A_l}(|\xi_{l,M+1}\rangle - b_l|\xi'_{l,M+1}\rangle) \\ &\quad +|\Psi^+\rangle_{l,A_l}(|\xi'_{l,M+1}\rangle + b_l|\xi_{l,M+1}\rangle) \\ &\quad +|\Psi^-\rangle_{l,A_l}(|\xi'_{l,M+1}\rangle - b_l|\xi_{l,M+1}\rangle)]. \end{aligned} \tag{5}$$

(Q2) Bob performs Bell-basis measurements on qubit pairs (l, A_l). At this time, the secret message can be distributed uniformly on $(M+1)N$ qubits and is shared by the rest of partners in the net. Anyone (e.g. Charlie) can obtain the secret message with the help of the other partners (the supervisor and the controllers).

(Q3) The controllers perform computational basis $\{|0\rangle, |1\rangle\}$ measurements on the qubits obtained by them, and inform Charlie of the measurement outcomes.

(Q4) After receiving the measurement outcomes, Charlie asks Alice to tell him which EPR pairs are adopted to construct the communication net. If the original EPR state is $|\Phi^+\rangle$, Alice transmits 0 to Charlie. If the original EPR state is $|\Psi^+\rangle$, she transmits 1.

(Q5) In order to recover the state containing the secret message on the qubits in his place, Charlie should perform the unitary transformations on them according to the classical information from Alice and the controllers. The possible unitary transformations that should be performed by Charlie are given in Table 1, where the unitary transformations $I = |1\rangle\langle 1| + |0\rangle\langle 0|$ is the two-dimensional identity and $X = |1\rangle\langle 0| + |0\rangle\langle 1|$, $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

(Q6) Charlie can obtain the secret message after performing the measurements along the basis of $\left\{\frac{1}{\sqrt{2}}|0\rangle + |1\rangle, \frac{1}{\sqrt{2}}|0\rangle - |1\rangle\right\}$.

Table 1. The unitary transformations (U.Ts.) that should be performed by Charlie according to Alice's Bell-basis measurement outcomes (B.M.Os.), the rest of partners' computational basis measurement outcomes (C.M.Os.) and the original EPR states that are to be used to construct a communication net, where the sign 'E' denotes the number of measurement outcomes $|1\rangle$ being even, 'O' the number being odd, '0' the state $|\Phi^+\rangle$ that is used to construct the communication net, and '1' the state $|\Psi^+\rangle$.

B.M.Os.	C.M.Os.	EPR state	U.Ts.
$\|\Phi^+\rangle_{l,A_l}$	E	0	I
$\|\Phi^+\rangle_{l,A_l}$	O	0	X
$\|\Phi^-\rangle_{l,A_l}$	E	0	Z
$\|\Phi^-\rangle_{l,A_l}$	O	0	XZ
$\|\Psi^+\rangle_{l,A_l}$	E	0	X
$\|\Psi^+\rangle_{l,A_l}$	O	0	I
$\|\Psi^-\rangle_{l,A_l}$	E	0	XZ
$\|\Psi^-\rangle_{l,A_l}$	O	0	Z
$\|\Phi^+\rangle_{l,A_l}$	E	1	X
$\|\Phi^+\rangle_{l,A_l}$	O	1	I
$\|\Phi^-\rangle_{l,A_l}$	E	1	XZ
$\|\Phi^-\rangle_{l,A_l}$	O	1	Z
$\|\Psi^+\rangle_{l,A_l}$	E	1	I
$\|\Psi^+\rangle_{l,A_l}$	O	1	X
$\|\Psi^-\rangle_{l,A_l}$	E	1	Z
$\|\Psi^-\rangle_{l,A_l}$	O	1	XZ

In the above scheme, any of the partners in the net may obtain the secret message if the rest of partners cooperate with each other. None of them can obtain the secret message without the cooperation with the others.

With a little modification, the above QSS scheme can be changed into the QSDC scheme. Suppose that Bob and Charlie communicate between them under the agreement with the other partners, that is, the sender (Bob) and the recipient (Charlie) in the QSS become two authorized communicators in the QSDC.

In order to communicate securely between them, Bob and Charlie should test the security of quantum channel. They ask the others to perform the computational basis $\{|0\rangle, |1\rangle\}$ measurements on their qubits.

After receiving all the measurement outcomes, Bob and Charlie select randomly qubit subset as the testing group, which is enough for testing the security of quantum channel, and the rest of qubits as the coding group.

And then, Bob and Charlie perform local measurements on the testing group along z-axis or x-axis

randomly and analyse the security of quantum channel according to the measurement outcomes. If the error rate is low enough, they can communicate with each other in privacy. Otherwise, they abandon this communication.

After the above security test, the rest of processes are similar to those of the above QSS scheme.

4. The security of this communication net and QSS–QSDC scheme

The crucial issue of quantum communication is its security and privacy.

Suppose that an eavesdropper (say, Eve) who is outside the communication net wants to steal the secret message. She can intercept the qubits that are transmitted to the other partners by the supervisor, and resend her prepared qubits to them to imitate the qubits she intercepted previously. Whereas, Eve's actions are doomed to increase the error rate of measurement outcomes and can be detected efficiently by Alice.

The security test of multi-partner communication net can be realized only under the cooperation of all the partners when the losses of quantum channel are taken into consideration.[37] An opaque attack can be performed by the dishonest partner to eavesdrop the message obtained by other partner freely. For preventing this attack, we need to ensure the high transmission efficiency in the scheme. That is, the process of qubit transmission is important in the whole scheme.

The security test of quantum channel is necessary for realizing quantum secure direct communication between the two authorized partners. If the dishonest partner obtains all the classical information in transmission, they can deduce the quantum channel between the two communicators. But the information cannot make them obtain the secret message because the teleportation[38] is used to transmit the secret message. Moreover, they do not know which qubits are selected as the checking group by the two communicators. Once the dishonest partners want to steal the secret message or disturb communication, their actions would increase the error rate and can be found by the two communicators in the security test of quantum channel.

The dishonest partners can introduce the auxiliary qubits and make them entangle into the communication net, but the action can also be detected by any message authentication method in the QSS and the two security tests in the QSDC.

If the communication net is perfect and all partners are honest, the security test of quantum channel is not necessary, and the eavesdropper outside the net can be detected in the communication net security test.

There exist the Trojan horse attacks[1] in the process of direct quantum communication, which can be divided into three types,[39−42] i.e. the general Trojan horse attack, the delay-photon Trojan horse attack, and the invisible photon attack. These technical problems can be solved by the technical measures. For example, a photon number splitter can prevent the multi-photon signal, wavelength filter can make light at an appropriate wavelength enter, time window should be open during shorter time and reduce the intensity of light.

So the security of the communication net and QSS–QSDC scheme can be guaranteed by the principle of quantum mechanics and technical measures.

5. Discussion and conclusion

In the scheme, we present a scheme for constructing a communication net. The supervisor can increase or decrease the number of the partners in the net according to actual demands by increasing or decreasing the number of auxiliary qubits.

As its application, a QSS–QSDC scheme is proposed. The successful realization of quantum secret sharing depends on the secure communication net and all partners' honesty. A sender shares the secret information with the others, and an authorized recipient can obtain the content of secret information under the control of the others. The completion of quantum secure direct communication depends on the two security tests. Two partners can communicate under the cooperation with the other partners.

The scheme needs only single-qubit operations, CNOT gate operations and Bell-basis measurements, which could be implemented in the near future, for the required technology is rapidly developed currently.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Bennett C H and Brassard G 1984 in: *Proc. IEEE International Conference on Computer, Systems and Signal Processing* Bangalore India (New York: IEEE) p175

[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[5] Bruβ D 1998 *Phys. Rev. Lett.* **81** 3018

[6] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[7] Acín A, Gisin N and Masanes L 2006 *Phys. Rev. Lett.* **97** 120405

[8] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[9] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162.

[10] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1084

[11] Chen P, Deng F G and Long G L 2006 *Chin. Phys.* **15** 2228

[12] Liu W T, Liang L M, Li C Z and Yuan J M 2006 *Chin. Phys. Lett.* **23** 3148

[13] Zhang Y Q, Jin X R and Zhang S 2006 *Chin. Phys.* **15** 2252

[14] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta. Phys. Pol.* A **101** 357

[15] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[16] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

[17] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801

[18] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601

[19] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301

[20] Lü H, Yan X D and Zhang X Z 2004 *Chin. Phys. Lett.* **21** 2340

[21] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[22] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[23] Yan F L and Zhang X Q 2004 *Eur. Phys. J.* B **41** 75

[24] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 0893

[25] Gao T, Yan F L and Wang Z X 2005 *Int. J. Mod. Phys.* C **16** 1293

[26] Cao H J and Song H S 2006 *Phys. Scr.* **74** 572

[27] Man Z X and Xia Y J 2006 *Chin. Phys. Lett.* **23** 1973

[28] Cai Q Y and Lü H 2007 *Chin. Phys. Lett.* **24** 1154

[29] Lü H, Chen A X and Yan X D 2007 *Chin. Phys.* **16** 2862

[30] Townsend P D 1997 *Nature* **385** 47

[31] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651

[32] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317

[33] Deng F G, Liu X S, Ma Y J, Li X and Long G L 2002 *Chin. Phys. Lett.* **19** 893

[34] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049

[35] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y and Deng F G 2006 *Chin. Phys. Lett.* **23** 1080

[36] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359

[37] Deng F G, Li X H and Zhou Y Y 2007 arXiv: quant-ph/0705.0279

[38] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895

[39] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[40] Cai Q Y 2006 *Phys. Lett.* A **351** 23

[41] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2005 arXiv: quant-ph/0508168v1

[42] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2005 arXiv: quant-ph/0507063v2