Controlled Bidirectional Quantum Direct Communication by Using a GHZ State *

MAN Zhong-Xiao(满忠晓)**, XIA Yun-Jie(夏云杰)

College of Physics and Engineering, Qufu Normal University, Qufu 273165

(Received 1 March 2006)

A controlled bidirectional quantum secret direct communication scheme is proposed by using a Greenberger–Horne–Zeilinger (GHZ) state. In the scheme, two users can exchange their secret messages simultaneously with a set of devices under the control of a third party. The security of the scheme is analysed and confirmed.

PACS: 03. 67. Hk, 03. 65. Ud

Based on physical laws instead of mathematical complexities, communication with perfect secrecy could be guaranteed over an insecure channel in Vernam's sense of a one-time pad, which is known as quantum cryptography. Conventionally, the problem reduces to the so-called quantum key distribution (QKD), which is an ingenious application of quantum mechanics. In the QKD scheme, two remote legitimate users (Alice and Bob) establish a shared secret key through the transmission of quantum signals. After the pioneering work of Bennett and Brassard in 1984, i.e. the well-known BB84 protocol,[1] a variety of quantum secret communication protocols have been proposed (for a review see Ref. [2]).

Recently, a new concept in quantum cryptography, quantum secure direct communication (QSDC), was proposed,[3−13,23] which permits messages to be communicated directly without first establishing a random key to encrypt them. Bostroem and Felbinger proposed the so-called ping-pong protocol,[4] which allows the encoded bit to be decoded instantaneously in each respective transmission run. Unfortunately, it was proved that it is not completely secure.[14−16] Deng *et al.*[5] have proposed a two-step quantum direct communication protocol by using an Einstein–Podolsky–Rosen (EPR) pair. Subsequently, the secure bidirectional quantum direct communication (BQDC) idea and theoretical schemes were proposed.[17−20] Nguyen[18] proposed a quantum dialogue scheme that enables both legitimate parties to exchange their secret messages in a direct way. Jin *et al.*[19] proposed a three-party simultaneous QSDC scheme by using the Greenberger–Horne–Zeilinger (GHZ) states. These BQDC protocols allow two legitimate users simultaneously exchange their different secret messages in a set of communication device.

In this Letter, we present a bidirectional quantum secret direct communication protocol with a control by the third party. Consider the following scenario. The administrative personnel of the server, Charlie, wishes to control the secret correspondence between the users. This means that if and only if Charlie gives her permission (that is, Charlie is trustworthy and cooperative), the users can obtain the secret messages of the counterpart. Meanwhile, the communication between the users should be carried out in a secret manner in the sense that the secret contents of the communication should be kept to be secret to the controller. What can they do? The following proposed scheme suits this task.

Before giving our controlled bidirectional quantum direct Communication (CBQDC) protocol, we first introduce the idea of the GHZ state dense coding briefly.[24] Dense coding using three particle entangled states has been proposed by Lee *et al.*[21] The eight GHZ entangled state can be expressed as follows:

$$
\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}),\\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}(|000\rangle_{ABC} - |111\rangle_{ABC}),\\
|\psi_3\rangle &= \frac{1}{\sqrt{2}}(|100\rangle_{ABC} + |011\rangle_{ABC})\\
|\psi_4\rangle &= \frac{1}{\sqrt{2}}(|100\rangle_{ABC} - |011\rangle_{ABC}),\\
|\psi_5\rangle &= \frac{1}{\sqrt{2}}(|010\rangle_{ABC} + |101\rangle_{ABC})\\
|\psi_6\rangle &= \frac{1}{\sqrt{2}}(|010\rangle_{ABC} - |101\rangle_{ABC}),\\
|\psi_7\rangle &= \frac{1}{\sqrt{2}}(|110\rangle_{ABC} + |001\rangle_{ABC}),\\
|\psi_8\rangle &= \frac{1}{\sqrt{2}}(|110\rangle_{ABC} - |001\rangle_{ABC}). \qquad (1)
\end{aligned}
$$

By performing single-particle unitary operations on any two of the three particles, one can change from one GHZ state to another, which will be shown subsequently. The unitary operations are the product of the Pauli and identity matrices: $I, \sigma_x, i\sigma_y, \sigma_z$. Here we assign each unitary operation with two-bit classical information, say, I to (0, 0), σ_z to (0, 1), σ_x to (1, 0), $i\sigma_y$ to (1, 1).

Now let us turn to depict our controlled bidirectional quantum direct communication protocol. Sup-

* Supported by the National Natural Science Foundation of China under Grant Nos 10534030 and 10304022.

** Email: manzhongxiao@163.com

©2006 Chinese Physical Society and IOP Publishing Ltd

pose that the users, say, Alice and Bob, want to communicate with each other simultaneously under the control of the controller Charlie. Firstly Charlie prepares an order of N three-particle GHZ states. Each of the three-particle states is in the form

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}). \quad (2)$$

We denote the order-N three-particle qubits with $\{[P_1(A), P_1(B), P_1(C)], [P_2(A), P_2(B), P_2(C)], \cdots, [P_N(A), P_N(B), P_N(C)]\}$, where the subscript indicates the order of each three-particle in the sequence; and A, B, C represents the three particles of each state, respectively. Then the scheme proceeds as follows.

(S1) Charlie takes one particle from each state to form an ordered partner photon sequence $[P_1(A), P_2(A), \cdots, P_N(A)]$, called sequence A. The remaining partner photons compose sequence B, $[P_1(B), P_2(B), \cdots, P_N(B)]$ and sequence C, $[P_1(C), P_2(C), \cdots, P_N(C)]$. Then she sends sequences A and B to Alice and Bob respectively, and keeps sequence C at her own site.

(S2) Alice and Bob confirm Charlie that they have received sequence A and B, respectively. To check if there is eavesdropping in the line, the three participants can carry out the following security checking process, which we call the first security checking. First, Alice (any one of the two parties Alice and Bob: we say Alice) selects randomly a sufficiently large subset from sequence A and make either σ_z or σ_x measurement on them. Then she announces the positions of these particles and the kind of measurement she has made. With this information, Bob and Charlie make the same measurement as Alice on the corresponding particles in sequences B and C, respectively. Then the controller Charlie publishes her measurement outcome firstly. Since the GHZ state they prepared is $|\psi_1\rangle$, which can be written in two bases as follows:

$$\begin{aligned}|\psi_1\rangle =& \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}) \\ =& \frac{1}{2}[|+\rangle_A(|++\rangle_{BC} + |--\rangle_{BC}) + |-\rangle_A \\ & \cdot(|+-\rangle_{BC} + |-+\rangle_{BC})], \end{aligned} \quad (3)$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. If no eavesdropping exists, their outcomes must be correlated: i.e., if Alice gets $|0\rangle$ ($|1\rangle$), then the measurement outcomes of Bob and Charlie must also be $|0\rangle$ ($|1\rangle$) when they choose their measurements along the z direction, or if Alice obtains $|+\rangle$ ($|-\rangle$), then the measurement results of Bob and Charlie must be the same (opposite) if the operation σ_x has been chosen. Through the comparison between them, if the error rate exceeds the threshold, they have to abort the communication. Otherwise they continue to execute the next step.

(S3) Based on the secret messages they want to send to the counterpart, Alice and Bob perform the unitary operations on the remaining particle, respectively. For the secure communication, Alice and Bob should prepare a sufficient number of single particles, which we call the checking particles, in one of the four quantum states that constitute two bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then Alice and Bob mix these checking particles with sequences A and B, respectively, and send them together to Charlie sequentially.

(S4) After receiving Charlie's confirmation of receiving their particles, Alice and Bob tell Charlie the position and the preparation bases of the checking particles. Then Charlie measures the checking particles in those bases and compares the outcome with Alice and Bob publicly. If the error rate exceeds the threshold, they have to abort the communication. Under the condition of safe channel, they go to the next step.

(S5) Charlie performs the GHZ basis measurement on particles in sequence A, B, and C. The measurement outcomes suffice Alice and Bob to extract the secret messages of the counterpart as shown in Table 1, thus these parameters hold by Charlie can control the communication of Alice and Bob. If Charlie wants to let Alice and Bob communicate, she can announce these measurement information publicly.

Table 1. Corresponding relations between Bob's and Alice's unitary operations and Charlie's GHZ basis measurement results on the three particles. Bob's (Alice's) unitary operations are listed in the first row (column).

	I	σ_z	σ_x	$i\sigma_y$
I	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_5\rangle$	$\|\psi_6\rangle$
σ_z	$\|\psi_2\rangle$	$\|\psi_1\rangle$	$\|\psi_6\rangle$	$\|\psi_5\rangle$
σ_x	$\|\psi_3\rangle$	$\|\psi_4\rangle$	$\|\psi_7\rangle$	$\|\psi_8\rangle$
$i\sigma_y$	$\|\psi_4\rangle$	$\|\psi_3\rangle$	$\|\psi_8\rangle$	$\|\psi_7\rangle$

This concludes the description of our controlled bidirectional quantum direct communication (CBQDC) scheme. We now explicitly analyse the proposed protocol described above. Suppose Alice encodes two bits classical information 01 on the ith particle of sequence A, i.e. $P_i(A)$, by performing the unitary operation σ_z, while Bob encodes 11 in the corresponding particle $P_i(B)$ by an unitary operation $i\sigma_y$. It can be verified that with Alice and Bob's operations, the initial three-particle GHZ state $|\psi_1\rangle$ has been transformed into the state $|\psi_3\rangle$. Therefore, when Charlie makes a GHZ basis measurement and publishes this measurement result, Alice can deduce Bob's operation $i\sigma_y$, i.e. the secret messages 01, since she herself has performed an operation σ_z on one of the three particles (Table 1). Similarly, Bob can also conclude Alice's operation and the secret messages she

wants to send.

Next, we analyse the security of the scheme. In the present scheme, one of the entangled particles is always kept in the sender's site, which is just like the BBM92 QKD protocol.[22] As the secret information is encoded in the whole entangled state, Eve cannot obtain useful information if she just obtains a part of the entangled state. As one can see, in the scheme, there are two eavesdropping checking processes that can be considered. After Charlie sends the particle sequences A and B to Alice and Bob, respectively, the first checking process is implemented. Firstly, we consider the 'intercept-and-resend' attack, i.e. Eve intercepts all of the travelling particles and send the fake particles of her prepared GHZ state to the receivers. When Alice announces the information of the position and the measurement basis of the sampling particles, Eve then measures the corresponding fake particles in the publishing basis. However, this attack actually cut off the entanglement between Charlie and Alice, and between Charlie and Bob. Hence, when they make the measurements in the randomly chosen bases and compare the measurement outcomes, this attack can be detected. Alternatively, Eve can let a system of her probe entangle with the travelling particles seeking to acquire partial information when the particles travel back. However, this strategy would introduce the error rate which can be detected by the error analysis in the first security checking. After the encoding operation, the particles be send back to Charlie. In this transmission run, Eve can make the denial-of-service attack.[14] However, in the scheme, we have the second checking process. The users mix the encoding particles with checking particles which was prepared randomly in two bases and send them to Charlie together. Since Eve cannot distinguish the checking particles from the particle block, this attack can be detected by the measurement and comparison of the checking particles. Since the present QSDC scheme includes a control of the third party, besides considering the eavesdropping of a outsider Eve we should consider the dishonesty of the controller. In the first security checking process, we let Alice (or Bob) rather than Charlie select the checking subset and decide the measurement bases. After measuring the particles of the checking subset, we let Charlie publish the measurement results firstly. Therefore, with the correlation of the three particles of the three-partite GHZ state, both eavesdroppings of insider and outsider Eve can be detected.

The proposed scheme has several advantages compared to the schemes proposed previously. Firstly, in our scheme, two legitimate parties can simultaneously exchange their secret messages with a set of devices, which is more efficient and economic. Secondly, compared to the two-particle Bell state, a three-particle GHZ state can be encoded with four bits of classical information each time with two encoding unitary operations performed on two qubits, which is a characteristic signature of the superdense coding. Lastly, the sender transmits a block of the particle each round; hence once the channel is detected safely, the residual ones can be used as the information carrier.

In conclusion, we have proposed a quantum protocol for two legitimate parties to simultaneously exchange their secret messages with the control of a third party. Though the controller holds the necessary information for the users to communicate, he/she cannot obtain the useful secret messages. On the other hand, without the controlled parameters, the users cannot realize the communication anyway. The security of the protocol is also discussed.

References

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) (New York: IEEE) p 175
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[3] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357
[4] Bostrom K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[5] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[6] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[7] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[8] Yan F L and Zhang X 2004 *Eur. Phys. J.* B **41** 75
[9] Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A **38** 5761
[10] Zhang Z J et al 2004 *Phys. Lett.* A **333** 46
Man Z X et al 2005 *Chin. Phys. Lett.* **22** 18
[11] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys. Lett.* **22** 2473
[12] Wang J, Zhang C and Tang C J arXiv:quant-ph/0602166 and quant-ph/0511092
[13] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305
[14] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[15] Wojcik A 2003 *Phys. Rev. Lett.* **90** 157901
[16] Zhang Z J et al 2004 *Phys. Lett.* A **333** 46
Zhang Z J et al 2005 *Phys. Lett.* A **341** 385
[17] Zhang Z J and Man Z X arxiv: quant-ph/0403215
[18] Nguyen B A 2004 *Phys. Lett.* A **328** 6
[19] Jin X R, Ji X, Zhang Y Q and Zhang S et al *Phys. Lett.* A (in press)
[20] Yan X, Fu C B, Zhang S et al 2006 *J. Korean Phys. Soc.* **48** 24
[21] Lee H J, Ahn D and Hwang S W 2004 *Phys. Rev.* A **66** 024304
[22] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[23] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
[24] Chen J L and Kuang L M 2004 *Chin. Phys. Lett.* **21** 12