Commun. Theor. Phys. (Beijing, China) **48** (2007) pp. 79–82

Vol. 48, No. 1, July 15, 2007

Controlled Quantum *N*-Party Simultaneous Direct Communication*

XIA Yun-Jie and MAN Zhong-Xiao

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

(Received July 28, 2006; Revised September 21, 2006)

Abstract *In this paper, we propose a controlled quantum N-party simultaneous direct communication protocol with single-qubit measurements. Many users can simultaneously exchange their secret messages in a set of devices with the control of a supervisor. The eavesdropper's commonly used attacks can be detected through two security checking processes.*

PACS numbers: 03.67.Hk, 03.65.Ud
Key words: direct communication, N-party, simultaneous

Quantum secure communication along a physical channel is doubtlessly one of the most attractive perspectives related to the late developments of quantum physics. In quantum communication, based on physical laws instead of mathematical complexities, correspondence with perfect secrecy could be guaranteed over an insecure channel in Vernam's sense of one-time pad, which is known as quantum cryptography. Quantum cryptography utilizes the original characteristics of quantum mechanics such as superposition and entanglement. Using these properties, information can be secretly shared between users through a quantum channel. Conventionally, the problem reduces to the so-called quantum key distribution (QKD). 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]). Although the methods used in these schemes are different, the basic principle is the same, i.e., the two remote legitimate users (Alice and Bob) establish a shared secret key through the transmission of quantum signals, after that they can use this key to encrypt or decrypt the secret messages.

Recently, a new concept in quantum cryptography, quantum direct communication (QDC) was proposed,[3−15] which permits messages to be communicated directly without first establishing a random key to encrypt them. Boström and Felbinger proposed a so-called Ping-Pong protocol,[4] which allows the encoded bit to be decoded instantaneously in each respective transmission run. After that, Deng *et al.* put forward a two-step QDC protocol by using blocks of EPR pairs.[6] Subsequently, the secure bidirectional (or multidirectional) quantum direct communication (BQDC) idea and theoretical schemes were proposed.[16−20] These BQDC protocols allow two (or many) users simultaneously exchange their different secret messages in a set of communication device. In most of the QDC and BQDC schemes, the joint Bell basis or multi-partite GHZ basis measurement is necessary, hence the realization of the joint-basis measurement is of the key importation for these schemes. However, the realization of the joint-basis measurement is still difficult in experiment. To overcome this obstacle, in this paper, we propose a controlled N-party quantum simultaneous direct communication scheme without using joint-basis measurement. Our scheme can be implemented by only using single-qubit measurements. Consider the following scenario. The administrative personnel of the server, Alice, wishes to control the secret correspondence between N users Bob_1, Bob_2, ..., and Bob_N. This means that if and only if the supervisor Alice gives her permission (that is, Alice is trustworthy and cooperative), can the users obtain the secret messages of his/her 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 secret also to the supervisor Alice. What can they do? The following proposed scheme suits this task.

For convenience, we present firstly a controlled two-party simultaneous QDC scheme, then we generalize it to the controlled N-party case. Suppose one user Bob has a secret message consisting of M bits,

$$\text{Alice's message} = \{i_1, i_2, \ldots, i_M\} \tag{1}$$

with $i_n \in \{0, 1\}$, and his counterpart Charlie has another secret message consisting of N bits,

$$\text{Bob's message} = \{j_1, j_2, \ldots, j_M\} \tag{2}$$

with $j_n \in \{0, 1\}$. Without loss of generality we can set $N = M$. To begin with, the supervisor Alice produces a large enough number of identical three-partite GHZ states, which can be written in two bases as

$$\begin{aligned} |\Phi\rangle_{A,B,C} &= \frac{1}{\sqrt{2}}(|000\rangle_{A,B,C} + |111\rangle_{A,B,C}) \\ &= \frac{1}{2}[|+\rangle_A(|+\rangle_B|+\rangle_C + |-\rangle_B|-\rangle_C) \end{aligned}$$

*The project supported by the Key Program of National Natural Science Foundation of China under Grant No. 10534030

$$+|-\rangle_A(|+\rangle_B|-\rangle_C+|-\rangle_B|+\rangle_C)]\,, \quad (3)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The subscripts A, B, and C stand for three qubits of the three-partite GHZ state while $|0\rangle$ and $|1\rangle$ characterize two degrees of freedom of a qubit. In the scheme, encoding can be represented by a transformation on qubit state rather than by qubit itself. Suppose Bob and Charlie make an agreement that identity operation I encodes binary value 0, while the unitary operation $U = (|0\rangle\langle 1| + |1\rangle\langle 0|)$ encodes 1. Then the three participants proceeds as follows.

(S1) For each prepared three-partite GHZ state Alice keeps qubit A and sends qubits B and C to Bob and Charlie respectively.

(S2) Bob and Charlie confirm Alice that they have received all the B and C qubits, respectively. Then Alice selects at random a sufficiently large subset out of the shared $|\Phi\rangle_{A,B,C}$ states and lets Bob and Charlie know that subset. For each state of the subset Alice measures her qubit A randomly in $ß_z = \{|0\rangle, |1\rangle\}$ or in $ß_x = \{|+\rangle, |-\rangle\}$, then asks Bob and Charlie to measure their corresponding qubits in the same basis as hers. Subsequently, Alice requires Bob and Charlie to publicly reveal the outcome of each their measurement and makes an analysis. Since the GHZ state $|\Phi\rangle_{A,B,C}$ can be written in two basis as shown in Eq. (3), if no eavesdropping exits, 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 the $|0\rangle$ ($|1\rangle$) when they choose $ß_z$ basis, or if Alice obtains $|+\rangle$ ($|-\rangle$), then the measurement results of Bob and Charlie must be the same (opposite) if the operation $ß_x$ has been chosen. Through the comparison among them, in case of the error rate exceeds a predetermined small value, they have to abort the communication. Otherwise they record the order of the residual shared $|\Phi\rangle_{A,B,C}$ states and can use them for the later message transmission process.

(S3) After determining the security of quantum channel, Bob and Charlie encode each B qubit and C qubit of the leftover three-partite GHZ states with one of the two unitary operations I and U, respectively, according to their secret messages defined in Eqs. (1) and (2). After that, Bob and Charlie prepare respectively a large number of single qubits in one of the four randomly chosen states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ that constitute two nonorthogonal bases $ß_z = \{|0\rangle, |1\rangle\}$ and $ß_x = \{|+\rangle, |-\rangle\}$, we call them as checking qubits. Then Bob and Charlie mix their checking qubits with the encoded B qubits and C qubits respectively, and send these mixed qubits to his/her counterpart, i.e., Bob (Charlie) sends the mixed qubits to Charlie (Bob).

(S4) After confirming each other the receipt of the qubits, Bob (Charlie) informs Charlie (Bob) of the position and the preparation basis of the checking qubits. In the same basis as the preparation of Charlie (Bob), Bob (Charlie) measures each checking qubit. Then they make an analysis publicly. If the error rate exceeds a predetermined small value, the whole process must be aborted and resumed from the beginning, otherwise the process goes to next step.

(S5) For each one of the residual three-partite GHZ states $|\Phi\rangle_{A,B,C}$, the three participants measure their particles (i.e., Alice, Bob and Charlie measure qubits A C and B) in the $ß_z$ basis, respectively. If knowing Alice's measurement result on her qubit A for a GHZ state and his own measurement outcome on the corresponding qubit C is the same (opposite) to Alice's result, Bob can deduce Charlie's encoding operation on this qubit is I (U), furthermore the secret bits she encoded is "0" ("1"). Similarly, conditioned on Alice's measurement result on a qubit A and her measurement result on the corresponding qubit B, Charlie can also conclude Bob's encoding operation on this qubit, i.e., Bob's secret message. Hence, one can regard Alice's measurement results on qubit A as the control parameters for Bob and Charlie to simultaneously communicate.

This concludes the description of our controlled two-party simultaneous QDC scheme. We now explicitly analyze the proposed protocol described above. For convenience, we assume Bob's (Charlie's) m-th secret bits is "0" ("1"). After ascertaining the security of the quantum channel, Bob (Charlie) performs the operation I (U) on his (her) particle B (C) of the m-th three-partite GHZ state $|\Phi\rangle_{A,B,C}$. After their encoding operations, the initial GHZ state $|\Phi\rangle_{A,B,C}$ becomes $|\Phi'\rangle_{A,B,C}$, i.e.,

$$|\Phi\rangle_{A,B,C} \to |\Phi'\rangle_{A,B,C} = \frac{1}{\sqrt{2}}(|001\rangle_{A,B,C} + |110\rangle_{A,B,C})\,. \quad (4)$$

If Alice's measurement result on qubit A is $|1\rangle(|0\rangle)$, Bob will obtain the opposite result $|0\rangle(|1\rangle)$ with a measurement on qubit C, and Charlie will get the same result $|1\rangle(|0\rangle)$ with a measurement on qubit B. Hence, if Alice publishes her result, Bob can conclude Charlie's operation on particle C is U, i.e., the secret message is "1", similarly, Charlie can deduce Bob's operation is I and the secret bit is "0".

Next, we would like to discuss the security of the scheme. To gain useful secret bits, Eve must attack the quantum channel during the qubit transmission process. In our scheme, Eve has two chances to attack the sending B and C qubits, however, there are also two security checking processes to detect the attacks.

We first consider Eve's attacks when Alice sends B and C qubits to Bob and Charlie. As one can see, any attacks that cut off the entanglement of qubits A, B, and C can be detected with the first security checking procedure, since Alice, Bob, and Charlie collaborate to select randomly a sufficiently large subset from the shared GHZ states to detect eavesdropping by using the randomly chosen measurement basis. If there are no attacks, the measurement

result of Alice, Bob and Charlie should have deterministic correlation according to Eq. (3). Hence, Eve's commonly used types of attack that disturb the correlation among the users, such as the intercept-and-resend attack and the denial-of-service(Dos) attack, can be detected during this security checking process. Alternatively, Eve may steal some information by entangling her ancilla (prepared, say, in the state $|\chi\rangle_E$) with a qubit B (C) (assumed to be in the state $|i\rangle_m$ with $i \in \{0,1\}$) before the qubit reaches Bob (Charlie): $|\chi\rangle_E \otimes |i\rangle_m \to \alpha|\chi_i\rangle_E|i\rangle_m + \beta|\chi_{i\oplus 1}\rangle_E|i\oplus 1\rangle_m$, where $|\alpha|^2 + |\beta|^2 = 1$ and $\langle\chi_i|\chi_{i\oplus 1}\rangle = 0$. Then she resends this qubit to the legitimate receiver. However, with a probability of $|\beta|^2$ she is detected if the security check by Alice, Bob and Charlie is performed on this state.

Next, we consider Eve's attacks when Bob and Charlie exchange their qubits. During this transmission process, Bob and Charlie mix the detecting single qubits prepared in randomly chosen basis with the encoding ones and transmit them together. Here, conditioned on our scheme, the effective eavesdropping method is measurement-resend. Since Eve cannot distinguish the detecting qubits from the message ones, to gain useful information, she must measure every qubit in ß$_z$ basis and resends them to the legitimate receivers. However, the error rate introduced to detecting qubits suffices for Bob and Charlie to detect this type attack. We point out that though Eve can get a series of measurement results $\{|0\rangle, |1\rangle\}$ by the measurements on the sending qubits in the basis ß$_z$ and also know which are the detecting particles later, she cannot conclude the encoding operations of Bob and Charlie (i.e., the secret messages) since the security checking is implemented before Alice publishes the measurement result of qubit A. Without Alice's publishing "control parameters", Eve's measurement results are meaningless. Therefore, in our scheme, the secret messages exchanged between Bob and Charlie will not in any case be leaked to Eve.

Now let us generalize the controlled two-party simultaneous QDC scheme to the controlled N-party case. Alice severs still as the controller, while Bob$_1$, Bob$_2$, ..., and Bob$_N$ are N legitimate users who want to correspond with each other directly. Without loss of generality, we assume Bob$_1$ wants to transmit his secret messages to Bob$_2$, Bob$_i$ to Bob$_{i+1}$, and Bob$_N$ to Bob$_1$. To begin with, the controller Alice produces a large enough number of identical $(N+1)$-partite GHZ states in the form

$$|\Psi\rangle_{A,1,2,\ldots,N} = \frac{1}{\sqrt{2}}(|00\ldots0\rangle_{A,1,2,\ldots,N} + |11\ldots1\rangle_{A,1,2,\ldots,N}) . \quad (5)$$

The users agree on that identity operation I encodes binary value 0, while the unitary operation $U = (|0\rangle\langle 1| + |1\rangle\langle 0|)$ encodes 1. Then the controlled N-party BQDC scheme can be achieved as follows.

(G1) For each prepared $N+1$-partite GHZ state Alice keeps qubit A and sends qubits 1, 2, ..., N to Bob$_1$, Bob$_2$, ..., Bob$_N$, respectively.

(G2) All the receivers confirm Alice that they have received the sending qubits. Then Alice selects at random a sufficiently large subset out of the shared $(N+1)$-partite states and lets all the Bobs know that subset. For each state of the subset Alice measures her qubit A randomly in ß$_z = \{|0\rangle, |1\rangle\}$ or in ß$_x = \{|+\rangle, |-\rangle\}$, then asks every Bob to measure their corresponding qubits in the same basis as hers. Alice's (Bobs') measurement outcome in ß$_z$ basis can be represented as $A^z(B_i^z)$=$\{0,1\}$ corresponding to finding $\{|0\rangle, |1\rangle\}$ and that in ß$_x$ is $A^x(B_i^x)$=$\{1,-1\}$ corresponding to finding $\{|+\rangle, |-\rangle\}$. Alice requires every Bob to publicly reveal the outcomes of their measurements and makes an analysis. For the measurements in ß$_z$, if $A^z = (B_i^z)$, they consider the quantum channel is secure, otherwise she realizes a possible attack of an Eavesdropper Eve in the quantum channel. As for measurements in ß$_x$, if $A^x = \prod_{i=1}^{N}(B_i^x)$, it is all-right, otherwise there is Eve in the line. Through the comparison among them, if the error rate exceeds the threshold, they have to abort the communication. Otherwise they record the order of the remaining shared states and can use them for the later message transmission process.

(G3) After determining the security of quantum channel, all Bobs encode their qubits of the leftover $(N+1)$-partite GHZ states with one of the two unitary operations I and U, respectively, according to their secret messages. Then every Bob will send the encoded qubits to his counterpart who wants to contact, i.e., Bob$_1$ to Bob$_2$, ..., Bob$_i$ to Bob$_{i+1}$, ..., and Bob$_N$ to Bob$_1$. To detect the eavesdropping during this transmission process, they can adopt the detecting method described in the step (S3) of the controlled two-party BQDC scheme, i.e., they mix their checking qubits with the encoded ones, and send the mixed qubits to their counterparts.

(G4) After confirming each other the receipt of the qubits, every Bob informs his counterpart of the position and the preparation basis of the checking qubits. Then they make an analysis publicly after measuring each checking qubit in the same basis as the preparation. If the error rate exceeds a predetermined small value, the whole process must be aborted and resumed from the beginning, otherwise the process goes to next step.

(G5) For each one of the $(N+1)$-partite GHZ states $|\Psi\rangle_{A,1,2\ldots,N}$, all the participants measure their qubits in the ß$_z$ basis, respectively. If knowing Alice's measurement result on her qubit A for each state $|\Psi\rangle_{A,1,2\ldots,N}$, every Bob can deduce his counterpart's encoding operation is I (U), furthermore the secret bits is "0" ("1"), when his measurement outcome is same (opposite) to Alice's. So the

controlled N-party simultaneous QDC has been successfully completed. The security analysis is similar to the controlled two-party simultaneous QDC scheme, we do not repeat it again.

In conclusion, we have proposed a controlled N-party simultaneous QDC scheme by using three-partite GHZ states and also generalize it to controlled N-party BQDC scheme by using $N+1$-partite GHZ states. Instead of using joint-basis measurement, the proposed schemes utilize only single qubit measurement, hence it is more easy to realize in experiment. Any attacks can be detected efficiently with two security checking processes.

References

[1] C.H. Bennett and G. Brassard, in: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings*, Bangalore, India, IEEE, New York (1984) p. 175.

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

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

[4] Kim Bostrom and Timo Felbinger, Phys. Rev. Lett. **89** (2002) 187902.

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

[6] F.G. Deng and G.L. Long, Phys. Rev. A **69** (2004) 052319.

[7] Q.Y. Cai and B.W. Li, Chin. Phys. Lett. **21** (2004) 601.

[8] F.L. Yan and Z. Zhang, Euro. Phys. J. B **41** (2004) 75.

[9] T. Gao, F.L. Yan, and Z.W. Wang, Nuove Cimento Della Societa Italiana Di Fisica B **119** (2004) 313.

[10] Z.X. Man, *et al.*, Chin. Phys. Lett. **22** (2005) 18.

[11] T. Gao, F.L. Yan, and Z.X. Wang, Zeitschrift fur Naturforschung A **59** (2004) 597.

[12] J. Wang, C. Zhang, and C.J. Tang, arXiv:quant-ph/0602166 and quant-ph/0511092.

[13] C. Wang, F.G. Deng, Y.S. Li, X.S. Liu, and G.L. Long, Phys. Rev. A **71** (2005) 044305.

[14] A.D. Zhu, Y. Xia, Q.B. Fan, and S. Zhang, Phys. Rev. A **73** (2006) 022338.

[15] P. Xue, C. Han, X.M. Lin, and G.C. Guo, Phys. Rev. A **69** (2004) 052318.

[16] Z.J. Zhang and Z.X. Man, arxiv: quant-ph/0403215.

[17] B.A. Nguyen, Phys. Lett. A **328** (2004) 6.

[18] T. Gao, F.L. Yan, and Z.X. Wang, J. Phys. A **38** (2005) 5761.

[19] X.R. Jin, X. Ji, Y.Q. Zhang, *et al.*, Phys. Lett. A **354** (2006) 67.

[20] Y. Xia, C.B. Fu, S. Zhang, *et al.*, J. Korean Phys. Soc. **48** (2006) 24.