Optics Communications 284 (2011) 905–908

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Controlled three-party communication using GHZ-like state and imperfect Bell-state measurement

Li Dong [a], Xiao-Ming Xiu [a,*], Ya-Jun Gao [a], Yuan-Peng Ren [b], Hui-Wei Liu [c]

[a] Department of Physics, Bohai University, Jinzhou 121013 P. R. China
[b] College of Applied Technology, Bohai University, Jinzhou 121013 P. R. China
[c] College of Information Science and Engineering, Bohai University, Jinzhou 121000 PR China

ARTICLE INFO

Article history:
Received 30 July 2010
Received in revised form 15 September 2010
Accepted 30 September 2010

Keywords:
Quantum communication
Quantum cryptography
GHZ-like state
Bell-state measurement

ABSTRACT

We present a controlled three-party communication protocol using Greenberger-Horne-Zeilinger (GHZ)-like state and imperfect Bell-state measurement. Using the idea of controlled quantum teleportation, it can realize the secret information transmission between the legitimate participants under the control of the controller. It needs no unitary operation to recover the original state for the receiver, and it saves half of communication cost publicized by the sender. The order rearrangement of particles and data block transmission ensure the security of communication. With imperfect Bell-state measurement, it is tolerant of some noise effects and is feasible by using the present optical technique.

1. Introduction

Quantum cryptography [1] is one of the most striking developments in quantum communication, which enables legitimate participants to communicate in private using the principle of quantum mechanics. Among many of its applications, quantum key distribution [2–8] is a mature process that legitimate participants are able to transmit secret information based on the shared secret key. Particularly, quantum secure direct communication [9–15] and deterministic secure quantum communication [16–27] permit the participants to transmit secret information without establishing a key beforehand.

In some communication protocols, it is necessary to send the particles carrying secret information in a public channel. An eavesdropper has a chance to attack the particles in transmission. However, using quantum teleportation [28] which transmits the state of a quantum system from some place to other place without transmitting the system itself, no particle carrying secret information is transmitted, so it can avoid the attacks on the transmitted particles.

In practical situation of communication, the transmission of information should be supervised. Only with the help of a controller, a sender and a receiver can communicate successfully. Many controlled quantum communication protocols are proposed [29–35] where the communicators are incapable of the communication without the controller's agreement and cooperation.

Bell-state measurement is a crucial step in quantum teleportation. Bouwmeester et al. [36] proposed a method to identify two of four Bell states in their experiment of quantum teleportation. Lütkenhaus et al. [37] showed that no experimental setup using only linear elements can implement perfectly a Bell-state analyzer. It is limited to a 50% overall success rate without using auxiliary photons [38]. Houwelingen et al. [39] presented a linear Bell-state analyzer without auxiliary photons. It can distinguish three of the four Bell states for polarization qubits or time-bin qubits using today's technology, but this happens only half of the time on average. Using imperfect Bell-state measurement, Xiu et al. [40] proposed an information transmission protocol, where Bouwmeester's method to analyze Bell state works well.

In this paper, based on Bell-state analyzer of Bouwmeester et al., we propose a controlled quantum communication protocol using GHZ-like state. There is no particle with secret information to be transmitted and the eavesdropper has no access to the encoded particle. Two participants can communicate under the control of the controller. Using imperfect Bell-state measurement, it is tolerant of some noise effects. Moreover, it can be realized by using today's optical technique and consumes lesser resources than the communication protocols using general quantum teleportation. Even further, in the protocol, the particles as quantum channel are transmitted in the mode of data block [8] and order rearrangement [25–27], which ensures the security of the communication.

* Corresponding author.
E-mail address: xiuxiaomingdl@126.com (X.-M. Xiu).

0030-4018/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2010.09.089

2. Controlled three-party communication using GHZ-like state and imperfect Bell-state measurement

The controlled three-party communication using GHZ-like state and imperfect Bell-state measurement can be achieved with the following steps.

(1) The controller (Charlie) prepares ordered GHZ-like states $|\phi\rangle_{A_iB_iC_i}$ which can be denoted as

$$|\phi\rangle_{A_iB_iC_i} = \frac{1}{2}(|000\rangle + |110\rangle + |011\rangle + |101\rangle)_{A_iB_iC_i}, \quad (1)$$

which can be also obtained by the following method. Charlie introduces an EPR pair $|\Phi^+\rangle_{B_iC_i} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{B_iC_i}$ and an auxiliary particle with $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_{A_i}$. Then, he sends particles (A_i,C_i) or particles (A_i,B_i) through a *CNOT* gate (the particle A_i is used as the controller, the particle B_i(C_i) is the target), which can be expressed as $CNOT = [(|0\rangle\langle 0| + |1\rangle\langle 1|)|0\rangle\langle 0| + (|0\rangle\langle 1| + |1\rangle\langle 0|)|1\rangle\langle 1|]$.

(2) Charlie remains *C*-sequence (particle C_i) and transmits *A*-sequence (particles A_i) and *B*-sequence (particles B_i) to the sender (Alice) and the receiver (Bob) by the data block mode. For insuring the control role, before he distributes the particles, Charlie changes their order.

(3) Alice and Bob confirm Charlie that they receive all the particles through classical channel.

(4) Bob selects randomly a sufficiently large subset in each transmitted block as checking group $\{A_c,B_c,C_c\}$, which can be used to check whether there is eavesdropping in transmission line or not. He randomly chooses one of two sets of orthogonal basis $\{|0\rangle,|1\rangle\}, \left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ to measure his particles in the checking group. And then, Bob publicizes which particles he selected and which basis measurement he performed.

(5) Charlie publicizes the right order of the particles chosen by Bob so that Alice can correctly perform the measurement on the particles in the checking group. Alice and Charlie measure the corresponding particles in checking group under the same orthogonal basis as what chosen by Bob. The state $|\phi\rangle_{A_cB_cC_c}$ can also be described as

$$\begin{aligned}|\phi\rangle_{A_cB_cC_c} &= \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)_{A_cB_cC_c} \\ &= \frac{1}{\sqrt{2}}[(|00\rangle + |11\rangle)|0\rangle + (|01\rangle + |10\rangle)|1\rangle]_{A_cB_cC_c}.\end{aligned} \quad (2)$$

(6) After that, they compare the measurement outcomes publicly. If there is no eavesdropping, the measurement outcomes should correspond with Eq. (2) in perfect transmission path. In the imperfect channel, Alice and Bob will evaluate first the adverse effect. If the detection probability in security check is below the limit they evaluated beforehand, Alice and Bob consider that there is no eavesdropping and transmit secret information using the other particles in the transmitted blocks. Or else, they abandon this block and check other blocks.

(7) If the security of quantum channel is ensured, Alice and Bob communicate under the control of Charlie. If he permits their communication, Charlie performs measurements along the measurement bases $\{|0\rangle,|1\rangle\}$ on his particles, and publicizes the right order of transmitted particles and his measurement outcomes.

(8) After they receive the information from Charlie, Alice and Bob learn of the explicit states shared by them. Following the idea of teleportation, Alice prepares the encoded particle, *E*-sequence (particles E_i), in the states correspond to the secret information bits ($|0\rangle \rightarrow$ '0' and $|1\rangle \rightarrow$ '1').

(9) Alice performs Bell-state measurements on particles (E_i,A_i). After measurements, their states collapse to anyone of the following states,

$$|\Phi^{\pm}\rangle_{E_iA_i} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{E_iA_i}, |\Psi^{\pm}\rangle_{E_iA_i} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{E_iA_i}. \quad (3)$$

Alice needs not distinguish all Bell states, but ascertain that it is in either $|\Psi^{\pm}\rangle_{E_i,Ai}$ state or $|\Phi^{\pm}\rangle_{E_i,Ai}$ state which can be realized perfectly [36]. Subsequently, she publicizes the information concerning Charlie's and her measurement outcomes. The measurement outcomes $|\Phi^{\pm}\rangle$ ($|\Psi^{\pm}\rangle$) and Alice's publicized information have the correlation denoted as Table 1.

(10) After receiving the information, Bob performs the measurements on his particles using the bases of $\{|0\rangle,|1\rangle\}$, and registers the recorded information '0' ('1') corresponds to his measurement outcomes $|0\rangle$ ($|1\rangle$). Based on Alice's publicized information and his measurement outcomes, Bob extracts the secret information according to the addition of binary system. If Alice's publicized information is '0', Bob's recorded information is unchanged, but if it is '1', the corresponding bit should be reversed ('0' → '1', and '1' → '0').

So far the process of controlled quantum communication completes.

3. The security and feasibility of the present protocol

In perfect quantum channel of GHZ state, the security of the communication protocol has been proved [41]. Moreover, based on the method of quantum data block transmission and particle order rearrangement, the present protocol is secure. An eavesdropper outside of the three participants is incapable of obtaining the secret information.

As a receiver, Bob wants to obtain Alice's secret information without the control of any one. So he attempts to bypass Charlie by taking the following strategies to attain his objective.

Bob prepares the product state of single particles as auxiliary particles b_i. After Charlie sends all the particles out, Bob intercepts all the particles and entangles his auxiliary particles b_i by CNOT operations with the intercepted particles as control particles. His action can be represented by $\sum_i |A_i\rangle|B_i\rangle|C_i\rangle|b_i\rangle \rightarrow \sum_i |A_i\rangle|B_i\rangle|C_i\rangle|b_i \oplus A_i \oplus B_i\rangle$ under the computational basis. It can be deduced that the state of Bob's auxiliary particles b_i is identical to the state of particle C_i according to Eq. (2). Therefore, when he measures his auxiliary particles b_i along computational basis, Bob will obtain the same measurement outcomes as Charlie's. More important, Bob's entanglement and measurement will not introduce any error in the security check. In this way, the control role of Charlie is removed unknowingly, and Bob can deduce Alice's secret information no matter whether Charlie would like to help him.

However, in the present protocol, Bob fails to achieve the right order of the particles if Charlie does not publicize it. So Bob's evil purpose is unable to realize.

Table 1
Based on Charlie's computational basis ($\{|0\rangle,|1\rangle\}$) measurement outcomes (C. M. Os.) and her Bell-state measurement outcomes (A. M. Os.), Alice informs Bob of the publicized information (A. P. I.).

C.M.Os.	A.M.Os.	A.P.I.
0	$\|\Phi^{\pm}\rangle$	0
0	$\|\Psi^{\pm}\rangle$	1
1	$\|\Phi^{\pm}\rangle$	1
1	$\|\Psi^{\pm}\rangle$	0