ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (376-380), Month: October - December 2015, Available at: www.researchpublish.com

# Controlled Quantum Secure Direct Communication

JIN Yao-yao[1], HU Zhan-ning[2], KONG Ling-hao[3], SUN Zhao-long[4], LIU Qian[5]

School of Electronics and Information Engineering, Tianjin Polytechnic University,300387, Tianjin,China

***Abstract:*** **This paper introduces a new controlled quantum protocol for secure direct communication .We present a controlled three-party communication protocol using Greenberger-Horne-Zeilinger (GHZ)-like state and imperfect Bell-state measurement. In this paper, the receiver can obtain the sender's two-secret bits under the permission of the controller. In order to transmit two bits secret message, entanglement swapping is utilized. Therefore, no qubits carrying the secret messages are transmitted .Also, this protocol is unconditionally secure, if the perfect quantum channel is used. The motivation behind utilizing GHZ-like state as a quantum channel is that if a qubit is lost in the GHZ-like state the other two qubits are still entangled. The proposed protocol improves the efficiency of the previous ones. It is shown that one of these protocols is maximally efficient and that can be modified to an equivalent protocol of quantum secure direct communication (CQSDC). Security and efficiency of the controlled proposed protocols are analyzed and compared.**
***Keywords:*** **controlled quantum secrue direct communication; entanglement swapping; GHZ-like state; quantum cryptography.**

## 1. INTRODUCTION

The goal of cryptography is to ensure that the secret message is intelligible only for the two authorized parties of communication and should not be altered during the transmission[1,2,3].In the proposed protocol ,we assume that Alice trys to transmit her secret messages to Bob under the control of Charlie .Alice produces large enough number of three-particle GHZ-like state .Use of the series of GHZ-like state, so as to carry out secret messages transmission.

## 2. PREPARATION OF QUANTUM CHANNEL

Alice produces 2N GHZ-like state which is denoted as Eq (1):

$$|Q\rangle_{a_i b_i c_i} = \frac{1}{2}(|100\rangle + |010\rangle + |001\rangle + |111\rangle)_{a_i b_i c_i} \qquad (1)$$

where a, b, c represent the three qubits in a tripartite GHZ-like state and $i \in \{1,2,3\ldots 2N\}$ .Alice will be the series of GHZ-like state , witch be arranged as A, B, C .Alice retains A and Send B, C sequence respectively to Bob,Charlie.Alice divided the A sequence into N group, each of the two particles as a group.Such as, $Q(a_1)$ and $Q(a_2)$ are a group,and the like, $Q(a_{2N-1})$ and $Q(a_{2N})$ are a group[4,5].Bob and Charlie confirmed the sequence what they received.Bob and Charlie like Alice to his sequence grouping.Alice randomly selects some of the groups to encoding secret information, which are to ensure that the channel is safe, and the rest of the group as a test particle.

Alice randomly chooses one of two measuring bases, X-basis or Z-basis, to measure her particles .After that, she announces the order of the particles, the measuring basis and the results of her measurement. Bob and Charlie for each of the corresponding particle application and the same measurement group Alice. They compare the results of their measurements. According to Table , measurement results of the users should be correlated, if there is no eavesdropper. If the error rate is more than the threshold, they abort the protocol; otherwise, they execute the next state[6,7].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (376-380), Month: October - December 2015, Available at: www.researchpublish.com

**Table1 Corresponding measurement results**

| Basis | Alice's state | Bob's state | Charlie's state |
|---|---|---|---|
| $\delta_x$ | $\|+\rangle$ | $\|+\rangle$ | $\|+\rangle$ |
| | $\|-\rangle$ | $\|-\rangle$ | $\|-\rangle$ |
| $\delta_z$ | $\|1\rangle$ | $\|0\rangle$ | $\|0\rangle$ |
| | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ |
| | $\|0\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| | $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ |

## 3. THE TRANSFER PROCESS OF THE PROTOCOL

After determining the channel security, Alice to her A sequence of the preservation of encoding. She carries on the unitary operation of each group of the first particles[8], according to the different particles, the particle unitary operation to make a change. The concrete unitary operation is shown in the equation (2):

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$U_1 = \delta_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$U_2 = i\delta_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

$$U_3 = \delta_z = |0\rangle\langle 0| - |1\rangle\langle 1| \qquad (2)$$

If Alice wants to send "00", she performs $U_0$ operation on each group of first particles. As shown in equation (3):

$$\begin{aligned}|Q_{00}\rangle &= (U_0 \otimes I^{\otimes 5})(|Q\rangle_{a_1b_1c_1} \otimes |Q\rangle_{a_2b_2c_2}) \\ &= \frac{1}{4}[(|1100\rangle + |1001\rangle + |0110\rangle + |0111\rangle)_{a_1a_2b_1b_2}|00\rangle_{c_1c_2} + (|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{a_1a_2b_1b_2}|11\rangle_{c_1c_2} \\ &\quad + (|1000\rangle + |1101\rangle + |0010\rangle + |0111\rangle)_{a_1a_2b_1b_2}|01\rangle_{c_1c_2} + (|0100\rangle + |0001\rangle + |1110\rangle + |1011\rangle)_{a_1a_2b_1b_2}|10\rangle_{c_1c_2}] \qquad (3) \\ &= \frac{1}{2\sqrt{2}}[(|\phi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2})|\phi^+\rangle_{c_2c_2} - (|\phi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\phi^-\rangle_{c_1c_2} \\ &\quad + (|\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2})|\psi^+\rangle_{c_1c_2} - (|\psi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\psi^-\rangle_{c_1c_2}]\end{aligned}$$

Charlie perform Hadamard operation on his two particles in a group. The Hadamard matrix is defined in Eq(4):

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|) \qquad (4)$$

$|Q_{00}\rangle$ perform Hadamard operation to $|Q'_{00}\rangle$, As shown in equation (5):

$$\begin{aligned}|Q'_{00}\rangle &= \frac{1}{4}[(|\phi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\phi^-\rangle_{c_1c_2} \\ &\quad + (|\phi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} - |\psi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} - |\phi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\psi^+\rangle_{c_1c_2} \\ &\quad + (|\phi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2})|\psi^-\rangle_{c_1c_2} \\ &\quad + (-|\phi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} - |\psi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2})|\phi^+\rangle_{c_1c_2}]\end{aligned}$$

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (376-380), Month: October - December 2015, Available at: www.researchpublish.com

(5)

If Alice wants to send "01", she performs $U_1$ operation on each group of first particles. As shown in equation (6):

$$
\begin{aligned}
|Q_{01}\rangle &= (U_1 \otimes I^{\otimes 5})(|Q\rangle_{a_1b_1c_1} \otimes |Q\rangle_{a_2b_2c_2}) \\
&= \frac{1}{4}[(|0100\rangle + |0001\rangle + |1110\rangle + |0111\rangle)_{a_1a_2b_1b_2}|00\rangle_{c_1c_2} + (|0010\rangle + |0111\rangle + |1000\rangle + |1101\rangle)_{a_1a_2b_1b_2}|11\rangle_{c_1c_2} \\
&\quad + (|1000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{a_1a_2b_1b_2}|01\rangle_{c_1c_2} + (|0110\rangle + |0011\rangle + |1100\rangle + |1001\rangle)_{a_1a_2b_1b_2}|10\rangle_{c_1c_2}] \\
&= \frac{1}{2\sqrt{2}}[(|\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2})|\phi^+\rangle_{c_2c_2} + (|\psi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\phi^-\rangle_{c_1c_2} \\
&\quad + (|\phi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2})|\psi^+\rangle_{c_1c_2} - (|\phi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\psi^-\rangle_{c_1c_2}]
\end{aligned}
\tag{6}
$$

$|Q_{01}\rangle$ perform Hadamard operation to $|Q'_{01}\rangle$, As shown in equation (7):

$$
\begin{aligned}
|Q'_{01}\rangle = \frac{1}{4}[&(|\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} - |\phi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} - |\psi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\phi^-\rangle_{c_1c_2} \\
&+ (|\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} - |\phi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} - |\psi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\psi^+\rangle_{a_1a_2} \\
&+ (-|\phi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} - |\psi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\psi^-\rangle_{c_1c_2} \\
&+ (|\phi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\phi^+\rangle_{c_1c_2}]
\end{aligned}
\tag{7}
$$

If Alice wants to send "01"or"11", she will be performs $U_2$ or $U_3$ operation on each group of first particles respectively.As shown in equation (8), (9) :

$$
\begin{aligned}
|Q'_{10}\rangle = \frac{1}{4}[&(|\psi^-\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} - |\phi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} - |\psi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\phi^-\rangle_{c_1c_2} \\
&+ (|\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\psi^+\rangle_{a_1a_2} \\
&+ (-|\psi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} - |\phi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\psi^-\rangle_{c_1c_2} \\
&+ (|\psi^+\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2})|\phi^+\rangle_{c_1c_2}]
\end{aligned}
\tag{8}
$$

$$
\begin{aligned}
|Q'_{11}\rangle = \frac{1}{4}[&(|\psi^-\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |\psi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2})|\phi^-\rangle_{c_1c_2} \\
&+ (|\psi^-\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} - |\phi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} - |\psi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2})|\psi^+\rangle_{a_1a_2} \\
&+ (|\psi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |\phi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2})|\psi^-\rangle_{c_1c_2} \\
&+ (-|\psi^+\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} - |\phi^+\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |\phi^-\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |\psi^-\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2})|\phi^+\rangle_{c_1c_2}]
\end{aligned}
\tag{9}
$$

After performinng Hadamard operation, Charlie performs the Bell based measurement.If the measurement result is $|\phi^-\rangle$ or $|\psi^+\rangle$, Charlie sends to Bob "0". Otherwise,Charlie sends to Bob "1".Thus Charlie can simplify the control, the operation is more simple[9].

According to each Bell state to carry the classic two bit information:One is Parity bit, $|\phi\rangle$ odd parity bit, $|\psi\rangle$ even parity bit;Other is Phase bit,0 express +.1 express -.As shown in equation (10):

$|\phi^+\rangle \rightarrow$ (00) $|\phi^-\rangle \rightarrow$ (01)

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (376-380), Month: October - December 2015, Available at: www.researchpublish.com

$|\psi^+\rangle \rightarrow$ （10） $|\psi^-\rangle \rightarrow$ （11） （10)

So, Alice performes the Bell based measurement on her result. If the measurement result is $|\phi^+\rangle$ ,Alice sends to Bob "00". If the measurement result is $|\psi^+\rangle$ ,, Alice sends to Bob "01". If the measurement result is $|\phi^-\rangle$ , Alice sends to Bob "10". If the measurement result is $|\psi^+\rangle$ ,, Alice sends to Bob "11".

## 4. BOB DECODING PROCESS

If Bob receives "00" or "01", it is considered "0";If Bob receives "10" or "11", it is considered "1"";Bob apply exclusive-or gate of a classical bit with Charlie's information. After that, Bob also performs Bell based measurements, and the results obtained are carried out by unitary operation.(If after the operation of exclusive-or gate "0", measurements of Bob will be perform I operation;If after the operation of exclusive-or gate "1", measurements of Bob will be perform $\delta_x$ operation.) Bob compares the results obtained with the results of the Alice, and then gets the secret information to be sent by Alice[10,11].

Because of the conversion between four Bell States: $I:|\phi^\pm\rangle \leftrightarrow |\phi^\pm\rangle, |\psi^\pm\rangle \leftrightarrow |\psi^\pm\rangle$ , $\delta_x:|\phi^+\rangle \leftrightarrow |\psi^+\rangle, |\phi^-\rangle \leftrightarrow |\psi^-\rangle$ , $\delta_z:|\phi^+\rangle \leftrightarrow |\phi^-\rangle, |\psi^+\rangle \leftrightarrow |\psi^-\rangle$ , $i\delta_y:|\phi^+\rangle \leftrightarrow |\psi^-\rangle, |\phi^-\rangle \leftrightarrow |\psi^+\rangle$ .

Between the final the results of Bob and the measurement results of Alice have a certain conversion relationship .When the conversion relationship is I, the Bob gets a secret message to "00"..When the conversion relationship is $\delta_x$ , the Bob gets a secret message to "01"..When the conversion relationship is $\delta_z$ , the Bob gets a secret message to "10"..When the conversion relationship is $i\delta_y$ , the Bob gets a secret message to "11".If Alice wants to send "00",we will accord to the equation (5) is obtained in Table Ⅱ .

**Table Ⅱ . Alice wants to send "00",Bob's operation and the secret message.**

| Alice's Result | Charlie's Result | Classical Iformation $A\rightarrow B$ $C\rightarrow B$ | Bob's Result | Bob's the final the results | Secret message |
|---|---|---|---|---|---|
| $\|\phi^+\rangle$ | $\|\phi^-\rangle$ , $\|\psi^+\rangle$ | 00 0 | $\|\phi^+\rangle$ | $\|\phi^+\rangle$ | 00 |
| $\|\phi^+\rangle$ | $\|\phi^+\rangle$ , $\|\psi^-\rangle$ | 00 1 | $\|\psi^+\rangle$ | $\|\phi^+\rangle$ | |
| $\|\psi^+\rangle$ | $\|\phi^-\rangle$ , $\|\psi^+\rangle$ | 01 0 | $\|\psi^+\rangle$ | $\|\psi^+\rangle$ | |
| $\|\psi^+\rangle$ | $\|\phi^+\rangle$ , $\|\psi^-\rangle$ | 01 1 | $\|\phi^+\rangle$ | $\|\psi^+\rangle$ | |
| $\|\phi^-\rangle$ | $\|\phi^-\rangle$ , $\|\psi^+\rangle$ | 10 0 | $\|\psi^-\rangle$ | $\|\phi^-\rangle$ | |
| $\|\phi^-\rangle$ | $\|\phi^+\rangle$ , $\|\psi^-\rangle$ | 10 1 | $\|\phi^-\rangle$ | $\|\phi^-\rangle$ | |
| $\|\psi^-\rangle$ | $\|\phi^-\rangle$ , $\|\psi^+\rangle$ | 11 0 | $\|\phi^-\rangle$ | $\|\psi^-\rangle$ | |
| $\|\psi^-\rangle$ | $\|\phi^+\rangle$ , $\|\psi^-\rangle$ | 11 1 | $\|\psi^-\rangle$ | $\|\psi^-\rangle$ | |

## 5. CONCLUSION

In this scheme, the users share the class GHZ state. Alice let her particles perform the definition of unitary operations, and encoding her two bit secret message. In addition, the controler Charlie let his particle to perform Hadamard operation. After that, Charlie and Alice were measured using Bell, and the measurement results were informed to the receiver. Then, Bob found the secret message by measuring the particle. The efficiency of this protocol is significantly improved compared with the prior agreement.

## REFERENCES

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

[2] .A. Beige, B. G. Engler, C. Kurtsiefer, H. Weinfurter, Acta Phys. Pol. A 101 (2002) 357.

[3] Z. X. Man, Y. J. Xia, Nguyen, J. Phys. B: At. Mol. Opt. phys. 39 (2006) 3855.

[4] T. Gao, F. Yan, Chin. Phys. Soc. 14 (2005) 893.

[5] L. Dong, X. M. Xiu, Y. J. Gao, Y. P. Ren, H. W. Liu, Opt. Commun. 284 (2011) 905.

[6] . A. Banerjee, A. Pathak, Phys. Lett. A 376 (2012) 2944.

[7] J. Wang, Q. Zhang, C. J. Tang, Commun. Theor. Phys. 47 (2007).

[8] F. L. Yan, X. Q. Zhang, Euro. Phys. J. B 41 (2004) 75.

[9] Y. Xia, C. B. Fu, F. Y. Li, S. Zhang, J. Korean Phys. Soc.47 (2005) 753.

[10] Z. X. Man, Y. J. Xia, Nguyen, J. Phys. B: At. Mol. Opt. phys. 39 (2006) 3855.