Chapter 14
Quantum Secure Direct Communication Protocol Based on Four-Qubit Cluster State

Xianzhong Li, Guotian He, Mingxin Gu and Pengfei Dai

Abstract In order to improve the reliability and security of quantum direct communication, this paper proposed a new quantum secure direct communication protocol based on the entanglement properties of cluster state and EPR entangled pairs. This protocol takes four-quit cluster state as the information carrier, using unitary transformation, through quantum information states to do the Bell-based measurements to interpret the secret messages. The cluster state is better than W state of entanglement properties, has a higher efficiency of the communication, and is more comfortable to use for information carrier.

Keywords Quantum cryptography · Cluster state · Quantum secure direct communication protocol · Bell basis measurement

14.1 Introduction

Quantum communication has been a rapidly developing area of research in the past 20 years, and is a new interdisciplinary study which unifies the quantum–mechanical theory, and computer science. After the BB84 [1] and B92 [2] protocol, a lot of quantum key distribution protocols were proposed.

Compared with QKD [3–5], QSDC [6–8] can delivery secret messages directly without prior agreement key. It is not necessay to encrypt the message, and thus improve the efficiency of communication. According to the information carrier, the

X. Li (✉) · G. He · M. Gu · P. Dai
Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences
College of Computer and Information Science, Chongqing Normal University,
Chongqing 400110, China
e-mail: 493402719@qq.com

Z. Zhong (ed.), *Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012*, Lecture Notes in Electrical Engineering 219,
DOI: 10.1007/978-1-4471-4853-1_14,

QSDC [9] protocol can be divided into two kinds: one based on the single photon system and the other based on the entanglement system. Now, the majority of QSDC take entangled state as the information carrier. In 2006, Lee Hayman et al. proposed two kinds of self- certified QSDC protocols [10], which first confirms the correspondent's legal identity and then carries on the communication.

This article takes a four-quit cluster state as information carrier and completes QSDC with the help of classical channel. The plan chosen is cluster state rather than entangled state, as the cluster state interrelatedness and entanglement stubbornness is biggest, increases communication efficiency, and in addition, before the formal coding communication, the introduction of the test photon is once again determined to improve the safety performance of the communication protocol security.

14.2 Prerequisite Knowledge

$\{|0\rangle, |1\rangle\}$, is a standard orthogonal basis, called Z-based, now let$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$,$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which is called X–based. Four Bell states can be expressed as:

$$\begin{aligned} |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \end{aligned} \tag{14.1}$$

Record the four-quit cluster state as follows:

$$|\psi\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle) \tag{14.2}$$

14.3 Protocol Description

The protocol's purpose is Alice sends secret message 0 or 1 to Bob by the quantum channel security. It is not necessary to take into account the identity of the parties.

14.3.1 Interceptive Examination Stage

The sender Alice prepares orderly 2n four-quit cluster states$|\psi\rangle_{1234}$, then stochastically carries out the unitary transformation U_I or U_X where, $U_I = I \otimes I \otimes I \otimes I$, $U_X = \sigma_X \otimes \sigma_X \otimes \sigma_X \otimes \sigma_X$.

After completing the operation, Alice randomly chooses n-States in the cluster state as a checking sequence, and records its location, then hold the unitary transformation stochastically I or H.

Alice gets the checked sequence's particles 1, 2, to compose sequence for QA, and 3, 4, for QB, where:

$$Q_A = \{P_1(1) \otimes P_1(2), \ldots, P_n(1) \otimes P_n(2)\} \tag{14.3}$$

$$Q_B = \{P_1(3) \otimes P_1(4), \ldots, P_n(3) \otimes P_n(4)\} \tag{14.4}$$

And then sends QB to Bob, after which Bob will select randomly X -based or Z -based to measure the sequence, and tells the results to Alice. After Alice receives, informs Bob, Bob then tells Alice about the selected measure base. Alice measures the particles in his own hand with the measure base of Bob's, and compares the results with Bob. According to Eq. (14.2), combines with entanglement properties [12] of the four-quit cluster state, analyses of error rates. If the error rate is higher than the pre-set value, then give up the communication protocol and restart from the first step.

14.3.2 Formal Communication Stage

14.3.2.1 Code Part

Alice takes the left n four-quit cluster states as code sequence. Now the n states that Alice held are: $U_I|\psi\rangle_{1234}$ or$U_X|\psi\rangle_{1234}$=$|\psi'\rangle_{1234}$.

Before coding, Alice has left 3 and 4 particles composed sequence SB, particles 1 and 2 for SA. Where:

$$S_A = \{P_1(1) \otimes P_1(2), \ldots, P_n(1) \otimes P_n(2)\} \tag{14.5}$$

$$S_A = \{P_1(3) \otimes P_1(4), \ldots, P_n(3) \otimes P_n(4)\} \tag{14.6}$$

At the same time, Alice prepares n test photons, which are chosen randomly from$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and installed in S_B and then composed the sequence Sc, and record the location of the test photon and the corresponding state. Alice sends Sc to Bob; when Bob receives, he informs Alice. Alice then announces the location and state of the test photon. Bob selects Z-based to measure the test photon, and compared with the results Alice announces, then Bob analyzes the error rate. If the error rate is lower than expected, notify Alice to encode the SA.

The coding rules are as follows:

If Alicee wants to send a secret message its bit is 0, to perform a $\sigma_0 = I$ transformation on particle 2.

If Alice wants to send a secret message its bit is 1, to perform a $\sigma_1 = \sigma_Z$ transformation on particle 2.

Table 14.1 Coding details

Coding cluster state send information content	The coding on particle 1	The coding on particle 2	After the coding
0	I	I	$\sigma_0 \otimes \sigma_0 \otimes \sigma_0 \otimes \sigma_0 \|\psi\rangle_{1234}$
0	σ_Z	I	$\sigma_Z \otimes \sigma_0 \otimes \sigma_0 \otimes \sigma_0 \|\psi\rangle_{1234}$
1	I	σ_X	$\sigma_0 \otimes \sigma_X \otimes \sigma_0 \otimes \sigma_0 \|\psi\rangle_{1234}$
1	σ_Z	σ_X	$\sigma_Z \otimes \sigma_X \otimes \sigma_0 \otimes \sigma_0 \|\psi\rangle_{1234}$

Note: At the same time Alice performs a random transformation $\sigma_0 = I$ or $\sigma_1 = \sigma_Z$ on particles 1. Its purpose is, in theory, the Bell-based measurement results released by the decode stage equally probability to appear $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ and $|\beta_{11}\rangle$. Which can prevent the eavesdropper on the measurement results from the public get sends information; the coding on the particle 2 has no effect with the coding on secret messages.

Assume that Alice has the n state is: $U_I|\psi\rangle_{1234}=|\psi\rangle_{1234}$.

The coding details are shown in Table 14.1.

14.3.2.2 Decoding Parts

After Alice's coding, then Alice and Bob simultaneously joint Bell-based [11] measurement, Alice sends the measurement results through the classical channel to Bob. Bob deciphers the secret message and decodes control rules as shown in Table 14.2. Decode control rules are shown in Table 14.2:

Similarly assuming that Alice has the n states is $U_X|\psi\rangle_{1234}=|\psi'\rangle_{1234}$.

The coding scheme is shown in Table 14.1.

Decode control rules is the same as in Table 14 2.

Hypothesis by four particle W states as information carrier, after the coding and decoding, decode rule table is as shown in Table 14.3.

In theory, the cluster state is better than W state of entanglement properties and more comfortable to use for information carrier. Through Tables 2 and table 3 to be known, the cluster state as information carrier combination measurement results have eight kinds, and W state a dozen states, redundancy combination more. Obviously with the cluster state as information carrier have a higher efficiency of the communication.

Table 14.2 Decode control rules

Alice	$\|\beta_{00}\rangle$	$\|\beta_{01}\rangle$	$\|\beta_{10}\rangle$	$\|\beta_{11}\rangle$
$\|\beta_{00}\rangle$	0	×	0	×
$\|\beta_{01}\rangle$	1	×	1	×
$\|\beta_{10}\rangle$	0	×	0	×
$\|\beta_{11}\rangle$	1	×	1	×

Note The " ×" says it will not appear this kind of measuring combination results

Table 14.3 Decode rule

Alice	$\|\beta_{00}\rangle$	$\|\beta_{01}\rangle$	$\|\beta_{10}\rangle$	$\|\beta_{11}\rangle$
$\|\beta_{00}\rangle$	1	0	1	×
$\|\beta_{01}\rangle$	0	1	0	×
$\|\beta_{10}\rangle$	1	0	1	×
$\|\beta_{11}\rangle$	0	1	0	×

Note The " ×" says it will not appear this kind of measuring combination results

14.4 The Protocol Security Analysis

The security of the protocol is to establish the security on the basis of the QA, QB sequence and SA, SC sequence transmitted. The communicating parties use the X-based or Z-based measurements to detect eavesdropping; this method is the same as BBM92 protocol. The protocol BBM92 has proved to be unconditionally secure. This paper's protocol security and protocol BBM92 are equivalent from the perspective of information theory. We can be more straightforward; Eve cannot escape the detection of the communicating parties. Assuming Eve does not take any eavesdropping measures, Alice according to the news of the secret message bit value 0 or 1 does transform respectively. In this, assuming that Alice sends secret message 0 or 1 probability is 1/2. Because the encoding and decoding part in the communication process does not require any auxiliary classical information, Eve does not get any useful classical information. So, Eve guesses the probability of Alice sends a secret message can only be 1/2, thus you can get Alice and Eve's mutual information:

$$I(A,E) = H(A) - H(A|E) = 1 - \frac{1}{2}H\left(\frac{1}{2}\right) - \frac{1}{2}H\left(\frac{1}{2}\right) = 0 \tag{14.7}$$

Where, H is the Shannon entropy. Similarly, $I(B,E) = 0$ So Eve can easily be detected.

Next, analyze the safety of the strongest attacks. Suppose the eavesdropper Eve sends to each particle placed as detector in the quantum channel. When Alice coding is complete, Eve is ready to steal the secret message that Alice sends to Bob. We may assume that the initial state of the detector is $|0\rangle_e$, the state after the interaction of the detector with the Four-Quit Cluster State $|\psi\rangle_{1234}$, the whole system density operator is $\rho_{1234e} = U|\psi\rangle|00\rangle\langle 00|\langle\psi|U^{\dagger}$, for which the U is an execution unitary transformation of Eve. Eve in the placement of the detectors, at the same time, the cluster state will disturbance that is $U \neq I$ For a single particle and detector interaction, according to Schmidt decomposition theorem [13, 14] available:

$$U(|0\rangle \otimes |0\rangle_e) = |0\rangle|a_{00}\rangle_e + |1\rangle|a_{01}\rangle_e \tag{14.8}$$

$$U(|1\rangle \otimes |0\rangle_e) = |0\rangle|a_{10}\rangle_e + |1\rangle|a_{11}\rangle_e \tag{14.9}$$

$$U(|+\rangle \otimes |0\rangle_e) = |+\rangle|b_{00}\rangle_e + |-\rangle|b_{01}\rangle_e \tag{14.10}$$

$$U(|-\rangle \otimes |0\rangle_e) = |+\rangle|b_{10}\rangle_e + |-\rangle|b_{11}\rangle_e \tag{14.11}$$

where, $\langle a_{00}|a_{01}\rangle = 0$, $\langle a_{10}|a_{11}\rangle = 0$, $\langle b_{00}|b_{01}\rangle = 0$, $\langle b_{10}|b_{11}\rangle = 0$.

For a single particle and detector interaction, according to Schmidt decomposition theorem available:

(1). When subscript 0 and 1 swap inner product in a variety of $|a_{ij}\rangle$and $|b_{ij}\rangle$ remain unchanged, $i, j \in \{0, 1\}$

(2). When subscript a and b swap, inner product in a variety of $|a_{ij}\rangle$ and $|b_{ij}\rangle$ remain unchanged,$i, j \in \{0, 1\}$

Available by the symmetry conditions (1):

$$\langle a_{00}|a_{00}\rangle = \langle a_{11}|a_{11}\rangle \quad \langle a_{01}|a_{01}\rangle = \langle a_{10}|a_{10}\rangle$$

$$\langle b_{00}|b_{00}\rangle = \langle b_{11}|b_{11}\rangle \quad \langle b_{01}|b_{01}\rangle = \langle b_{10}|b_{10}\rangle \tag{14.12}$$

Available by the symmetry conditions (2)

$$\langle a_{00}|a_{00}\rangle = \langle b_{00}|b_{00}\rangle \quad \langle a_{01}|a_{01}\rangle = \langle b_{01}|b_{01}\rangle \tag{14.13}$$

According to the above two equations, make:

$$F = \langle a_{00}|a_{00}\rangle = \langle a_{11}|a_{11}\rangle = \langle b_{00}|b_{00}\rangle = \langle b_{11}|b_{11}\rangle > 0 \tag{14.14}$$

$$D = \langle a_{01}|a_{01}\rangle = \langle a_{10}|a_{10}\rangle = \langle b_{01}|b_{01}\rangle = \langle b_{10}|b_{10}\rangle > 0 \tag{14.15}$$

On both sides of (14.14) and (14.15) equations of their respective take inner product we can get:

$$F + D = 1 \tag{14.16}$$

Let$|a_{ii}\rangle = \sqrt{F}|\hat{a}_{ii}\rangle, |b_{ii}\rangle = \sqrt{F}|\hat{b}_{ii}\rangle, |a_{ij}\rangle = \sqrt{D}|\hat{a}_{ij}\rangle, |b_{ij}\rangle = \sqrt{D}|\hat{b}_{ij}\rangle, i, j \in \{0, 1\}$, where, $\langle \hat{a}_{ii}|\hat{a}_{ii}\rangle = \langle \hat{b}_{ii}|\hat{b}_{ii}\rangle = \langle \hat{a}_{ij}|\hat{a}_{ij}\rangle = \langle \hat{b}_{ij}|\hat{b}_{ij}\rangle = 1$.

Equations (14.16)–((14.19) can be expressed as:

$$U(|0\rangle \otimes |0\rangle_e) = \sqrt{F}|0\rangle|\hat{a}_{00}\rangle_e + \sqrt{D}|1\rangle|\hat{a}_{01}\rangle_e \tag{14.17}$$

$$U(|1\rangle \otimes |0\rangle_e) = \sqrt{F}|1\rangle|\hat{a}_{11}\rangle_e + \sqrt{D}|0\rangle|\hat{a}_{10}\rangle_e \tag{14.18}$$

$$U(|+\rangle \otimes |0\rangle_e) = \sqrt{F}|+\rangle|\hat{b}_{00}\rangle_e + \sqrt{D}|-\rangle|\hat{b}_{01}\rangle_e \tag{14.19}$$

$$U(|-\rangle \otimes |0\rangle_e) = \sqrt{F}|-\rangle|\hat{b}_{11}\rangle_e + \sqrt{D}|+\rangle|\hat{b}_{01}\rangle_e \tag{14.20}$$

Among them, F is fidelity and D is the bit error ratio. Alice sends check sequence that the state is: $IU_I|\psi\rangle_{1234}$ Eve sends to each particle placing a detector in the quantum channel, and then the entire quantum channel system by Z-based can be expressed as:

So, when Alice and Bob choose Z-based measuring the check sequence, the error ratio is 2FD. Similarly, Alice sends another check sequence and chooses Z-based measurement; the error ratio is also 2FD.

In conclusion, Alice on the analysis of four-quit cluster State entanglement properties, Eve inevitably disturbance cluster State. Being tapped test, in theory, 2FD > 0, Alice can detect the existence of Eve. In addition, in the formal communication stage, introduce the test photons, its secrecy by quantum No-Cloning Theorem and quantum uncertainty principle guarantee. Therefore, there will also be found Eve eavesdropping, ensure the confidentiality of further communication.

$$\begin{aligned}
|\psi\rangle_{1234E} = \frac{1}{2}\Big[& |0000\rangle\left(F|\hat{a}_{00}\rangle_{e3}|\hat{a}_{00}\rangle_{e4} + D|\hat{a}_{10}\rangle_{e3}|\hat{a}_{10}\rangle_{e4}\right) + \\
& |0001\rangle\sqrt{FD}\left(|\hat{a}_{00}\rangle_{e3}|\hat{a}_{01}\rangle_{e4} + |\hat{a}_{10}\rangle_{e3}|\hat{a}_{11}\rangle_{e4}\right) + \\
& 0010\rangle\sqrt{FD}\left(|\hat{a}_{01}\rangle_{e3}|\hat{a}_{00}\rangle_{e4} + |\hat{a}_{11}\rangle_{e3}|\hat{a}_{10}\rangle_{e4}\right) + \\
& |0011\rangle\left(F|\hat{a}_{11}\rangle_{e3}|\hat{a}_{11}\rangle_{e4} + D|\hat{a}_{01}\rangle_{e3}|\hat{a}_{01}\rangle_{e4}\right) + \\
& 1100\rangle\left(F|\hat{a}_{00}\rangle_{e3}|\hat{a}_{00}\rangle_{e4} - D|\hat{a}_{10}\rangle_{e3}|\hat{a}_{10}\rangle_{e4}\right) + \\
& |1101\rangle\sqrt{FD}\left(|\hat{a}_{00}\rangle_{e3}|\hat{a}_{01}\rangle_{e4} - |\hat{a}_{10}\rangle_{e3}|\hat{a}_{11}\rangle_{e4}\right) + \\
& 1110\rangle\sqrt{FD}\left(|\hat{a}_{01}\rangle_{e3}|\hat{a}_{00}\rangle_{e4} - |\hat{a}_{11}\rangle_{e3}|\hat{a}_{10}\rangle_{e4}\right) + \\
& |1111\rangle\left(F|\hat{a}_{11}\rangle_{e3}|\hat{a}_{11}\rangle_{e4} - D|\hat{a}_{01}\rangle_{e3}|\hat{a}_{01}\rangle_{e4}\right)
\end{aligned} \tag{14.21}$$

14.5 Conclusion

Through the above analysis of the security protocol, in the ideal channel, the protocol for non-coherent attack is safe. In the actual conditions, the safety of the protocol depends on the actual noise level of the channel. The advantages of the protocol are:

1. Inserted into the test photons in the communication phase, strengthen the communication of safety performance.
2. Ensure the security of quantum channel conditions, the cluster state as an information carrier, maximum entanglement, the highest correlation.

Along with the continuous quantum communication understanding and thorough research, more schemes will be out; I believe the actual quantum communication will be widely applied in the near future.

References

1. Bennett CH, Brassard G (1984) In: Proceedings of IEEE international conference on computers, systems and signal processing vol 16/4. Bangalore, pp 175–179
2. Bennett CH, Brassard G, Mermin ND (1992) Quantum cryptography without bell's theorem.Phys Rev Lett 68(11):557–559
3. Bennett CH (1992) Quantum cryptography Using any two nonorthogonal states[J]. Phys Rev Lett 68(9):3121–3126
4. Bennett CH, Wiesner SJ (1992) Communication via one and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett 68(8):3111–3116
5. Gisin N, Ribordy G, Tittel W, Zbinden H (2002) Quantum cryptography. Rev Mod Phys 74 145, and the references therein 13(5):831–837
6. Deng FG, Long GL, Liu XS (2003) Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A68, 042317 14(9):123–138
7. Deng FG, Long GL (2004) Secure direct communication with a quantm one-time-pad. Phys Rev A69 052319 7(5):342–348
8. Cao WF, Yang YG, Wen QY (2010) Quantum secure direct communication with cluster states. Sci China Phys Mech Astron 53:1271–1275
9. Zhang XL, Zhang YX, Wei H (2009) Quantum secure direct communication with Greenberger-Horne-Zeilinger- type state (GHZ state) over noisy channels. Chin Phys B18:435–439
10. Lee HJ, Ahn D, Hwang SW (2004) Quantum ditect communication with authentication. Phys Rev 66(15):24–34
11. Li XH, Li CY, Deng FG, Zhou P, Liang YJ, Zhou HY (2007) Quantum secure direct communication with quantum encryption b ased on pure entangled states. Chin Phys 16:2149–2153
12. Cirac JI, Gisin N (1997) Coherent eavesdropping strategies for the four state quantum cryptography protocol. Physics Letters A 229(1):1–7
13. Nielsen MA, Chuang IL (2000) Quantum computation and quantum information, vol 62/5. Press of the University of Cambridge, Cambridge, pp 28–31
14. Gao T, Yan FL, Wang ZX (2005) Deterministic secure direct communication using GHZ states and swapping quantum entanglement. J Phys A Math Gen 22(10):2473–2476