Vol 18 No 10, October 2009
1674-1056/2009/18(10)/4105–05

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

An efficient deterministic secure quantum communication scheme based on cluster states and identity authentication*

Liu Wen-Jie(刘文杰)[a)b)†], Chen Han-Wu(陈汉武)[a)], Ma Ting-Huai(马廷淮)[b)], Li Zhi-Qiang(李志强)[a)c)], Liu Zhi-Hao(刘志昊)[a)], and Hu Wen-Bo(胡文博)[a)]

[a)] *School of Computer Science and Engineering, Southeast University, Nanjing* 210096, *China*
[b)] *School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing* 210044, *China*
[c)] *College of Information Engineering, Yangzhou University, Yangzhou* 225009, *China*

(Received 10 November 2008; revised manuscript received 2 December 2008)

A novel efficient deterministic secure quantum communication scheme based on four-qubit cluster states and single-photon identity authentication is proposed. In this scheme, the two authenticated users can transmit two bits of classical information per cluster state, and its efficiency of the quantum communication is 1/3, which is approximately 1.67 times that of the previous protocol presented by Wang *et al* [*Chin. Phys. Lett.* **23** (2006) 2658]. Security analysis shows the present scheme is secure against intercept-resend attack and the impersonator's attack. Furthermore, it is more economic with present-day techniques and easily processed by a one-way quantum computer.

Keywords: deterministic secure quantum communication, cluster state, identity authentication
PACC: 0365, 0367

1. Introduction

By taking advantage of some properties of quantum mechanics, such as no-cloning theorem, uncertainty principle, indistinguishability of nonorthogonal states, etc., quantum cryptography communication can be used to transmit information with unconditional security. Quantum key distribution (QKD) is an important branch of quantum cryptography communication, which provides a novel way for two legitimate parties to share a common secret key over a long distance with negligible leakage of information. Hence, since Bennett and Brassard[1] presented the famous BB84 protocol, a variety of QKD protocols have been proposed.[2−6] And the security of some QKD protocols was theoretically proven.[7,8]

Another branch of quantum cryptography communication is quantum direct communication (QDC), and it is divided into two categories.[9] One is named quantum secure direct communication (QSDC),[10−16] in which the receiver can read the secret message directly, and the two parties of quantum communication exchange classical information only for checking eavesdropping. The other is called deterministic secure quantum communication (DSQC)[17−23] in which the receiver can read out the secret message by exchanging at least an additional classical bit for each qubit, i.e., classical communication is needed besides an eavesdropping check. Although DSQC needs to transmit some additional classical bits, the users do not need to transmit the qubits twice, so the security is more secure in a noise channel and more convenient for quantum error correction. Recently, Lee *et al*[24] proposed two DSQC protocols with authentication, but these protocols are pointed out by Zhang *et al*[25] to be insecure against Trent's attacks. We then put forward two efficient revised protocols which are secure against Trent's attacks.[26] To sum up, these works[10−26] mainly utilize the entanglement resources, such as the EPR pairs, the GHZ states, W states, etc.

The cluster state[27] is a special kind of entanglement state, which has the properties of both the GHZ-class and W-class entangled states. It has a large persistency of entanglement, that is, it is even harder to be destroyed by local operations than GHZ-class state, etc. Furthermore, the cluster state is easily processed by a one-way quantum computer. Wang *et*

*Project supported by the National Natural Science Foundation of China (Grant Nos 60572071 and 60873101), Natural Science Foundation of Jiangsu Province (Grant Nos BM2006504, BK2007104 and BK2008209), and College Natural Science Foundation of Jiangsu Province (Grant No 06KJB520137).
†Corresponding author. E-mail: wenjiel@163.com

al[28] proposed a novel DSQC protocol by using the four-qubit cluster states (WFT06 protocol for short). However, in the WFT06 protocol, each cluster state only carries one bit of secret message. Moreover, the protocol cannot resist the active attacks, such as the impersonator's attack.

In order to make up these leaks, we propose a revised efficient and secure DSQC scheme with the same four-qubit cluster states by introducing four unitary operations (I, σ_x, $\mathrm{i}\sigma_y$ and σ_z) and the single-photon authentication. The rest of this paper is organized as follows: In Section 2, the details of the efficient DSQC protocol will be given. In Section 3, the security and efficiency will be analyzed, and finally conclusion remarks will be drawn in Section 4.

2. The DSQC scheme with cluster states

Suppose there are two legitimate anticipators, Alice and Bob. Alice is the sender, who attempts to send $2N$ bits classical message to Bob. In this scheme, we use four-qubit cluster states as message carriers and single-photon sequence for checking eavesdropping.

In order to prepare the single-photon sequence, similar to the BB84 protocol,[1] we use two measurement bases (MBs), the Z basis $\{|0\rangle, |1\rangle\}$ and the X basis $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. We suppose the $|0\rangle$ and $|+\rangle$ states represent the binary value 0, the $|1\rangle$ and $|-\rangle$ states represent the binary value 1, B represents the basis sequence and V represents the binary value sequence. So, 0 in B represents the Z basis, 1 in B represents the X basis, then 0 in the Z basis represents the $|0\rangle$ state, 0 in the X basis represents the $|+\rangle$ state. For example, if B=11011001 and V=10101010, then the non-orthogonal states are $|-\rangle\,|+\rangle\,|1\rangle\,|+\rangle\,|-\rangle\,|0\rangle\,|1\rangle\,|+\rangle$.

Using the similar method in Ref.[28], we depict the specific steps of our scheme as follows:

(S1) **Preparing the seed key** Alice and Bob share a binary seed key SK in advance, and then extend SK to EK with the length enough to check eavesdropping in the following communication process by using an extension function G:

$$G:\ \{0,\ 1\}^d \to \{0,\ 1\}^k, \tag{1}$$

where the superscripts d, k represent the lengths of SK and EK, respectively. The selection of G should make EK satisfy the randomness condition, that is, the number of 0, 1 should appear with the probability of 1/2.

(S2) **Generating authentication keys** Alice and Bob divide EK into EK_A, EK_B equally. EK_A and EK_B, named the authentication keys, will be used for authenticating the identity of Alice and Bob respectively. And EK_A (EK_B) is subdivided into EK_{A1}, EK_{A2} (EK_{B1}, EK_{B2}) equally. Then EK_{A1} (EK_{B1}) represents the information of the basis sequence B, and EK_{A2} (EK_{B2}) represents the information of the binary value sequence V. Note that, if Alice wants to send a message to Bob, Alice will use her authentication key EK_A in order that Bob can authenticate Alice's identity. On the contrary, Bob's identity key EK_B will be utilized when Bob transmits a message to Alice.

(S3) **Preparing a quartet sequence** Alice prepares a sequence of N ordered quartets. Each quartet is randomly in one of the two states $|\varphi\rangle$

$$|\varphi\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{a_1a_2b_1b_2}, \tag{2}$$

and $|\varphi'\rangle$,

$$|\varphi'\rangle = \frac{1}{2}(|1001\rangle + |1010\rangle + |0101\rangle - |0110\rangle)_{a_1a_2b_1b_2}, \tag{3}$$

where the subscripts a_1, a_2, b_1 and b_2 represent the four particles of the cluster state. Note that $|\varphi'\rangle$ can be generated by utilizing some unitary operations on $|\varphi\rangle$. We call the sequence as the sequence P, and it can be rewritten as $\{P_1(a_1, a_2), P_1(b_1, b_2), P_2(a_1, a_2), P_2(b_1, b_2), \ldots, P_N(a_1, a_2), P_N(b_1, b_2)\}$, here the subscripts 1, 2, ..., N indicate the order of each quartet particle in the sequence P, respectively.

(S4) **Encoding message on cluster states** Alice performs one of the four unitary operations $\{I, \sigma_x, \mathrm{i}\sigma_y, \sigma_z\}$ on the particle b_2 of each quartet in the sequence P,

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\ \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\ \mathrm{i}\sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0|, \\ \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|; \end{aligned} \tag{4}$$

then two-bit classical information corresponds to an operation as follows: "00" $\to I_4$, "01" $\to \sigma_{x4}$, "10" $\to \mathrm{i}\sigma_{y4}$, "11" $\to \sigma_{z4}$. And the state $|\varphi\rangle$ or $|\varphi'\rangle$ will be

transformed into

$$\begin{aligned}|\varphi_1\rangle &= I_4\,|\varphi\rangle \\ &= \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{a_1a_2b_1b_2} \\ &= \frac{1}{\sqrt{2}}(|00\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |11\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2}),\end{aligned} \tag{5}$$

$$\begin{aligned}|\varphi_1'\rangle &= I_4\,|\varphi'\rangle \\ &= \frac{1}{2}(|1001\rangle + |1010\rangle + |0101\rangle - |0110\rangle)_{a_1a_2b_1b_2} \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |10\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}),\end{aligned} \tag{6}$$

$$\begin{aligned}|\varphi_2\rangle &= \sigma_{x4}\,|\varphi\rangle \\ &= \frac{1}{2}(|0001\rangle + |0010\rangle + |1101\rangle - |1110\rangle)_{a_1a_2b_1b_2} \\ &= \frac{1}{\sqrt{2}}(|00\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |11\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}),\end{aligned} \tag{7}$$

$$\begin{aligned}|\varphi_2'\rangle &= \sigma_{x4}\,|\varphi'\rangle \\ &= \frac{1}{2}(|1000\rangle + |1011\rangle + |0100\rangle - |0111\rangle)_{a_1a_2b_1b_2} \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |10\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2}),\end{aligned} \tag{8}$$

$$\begin{aligned}|\varphi_3\rangle &= \mathrm{i}\,\sigma_{y4}\,|\varphi\rangle \\ &= \frac{1}{2}(-|0001\rangle + |0010\rangle - |1101\rangle - |1110\rangle)_{a_1a_2b_1b_2} \\ &= -\frac{1}{\sqrt{2}}(|00\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2} + |11\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}),\end{aligned} \tag{9}$$

$$\begin{aligned}|\varphi_3'\rangle &= \mathrm{i}\,\sigma_{y4}\,|\varphi'\rangle \\ &= \frac{1}{2}(|1000\rangle - |1011\rangle + |0100\rangle + |0111\rangle)_{a_1a_2b_1b_2} \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2} + |10\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2}),\end{aligned} \tag{10}$$

$$\begin{aligned}|\varphi_4\rangle &= \sigma_{z4}\,|\varphi\rangle \\ &= \frac{1}{2}(|0000\rangle - |0011\rangle + |1100\rangle + |1111\rangle)_{a_1a_2b_1b_2} \\ &= \frac{1}{\sqrt{2}}(|00\rangle_{a_1a_2}|\phi^-\rangle_{b_1b_2} + |11\rangle_{a_1a_2}|\phi^+\rangle_{b_1b_2}),\end{aligned} \tag{11}$$

$$\begin{aligned}|\varphi_4'\rangle &= \sigma_{z4}\,|\varphi'\rangle \\ &= \frac{1}{2}(-|1001\rangle + |1010\rangle - |0101\rangle - |0110\rangle)_{a_1a_2b_1b_2} \\ &= -\frac{1}{\sqrt{2}}(|01\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2} + |10\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}),\end{aligned} \tag{12}$$

where $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ are the four Bell states,

$$\begin{aligned}|\phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).\end{aligned} \tag{13}$$

(S5) **Dividing particles in *P* sequence** Alice takes the particles a_1 and a_2 from each quartet in the sequence P to form an ordered particle pair sequence $\{P_1(a_1, a_2), P_2(a_1, a_2), \ldots, P_N(a_1, a_2)\}$, named the PA sequence. The remaining partner particle pairs $\{P_1(b_1, b_2), P_2(b_1, b_2), \ldots, P_N(b_1, b_2)\}$ is called the PB sequence.

(S6) **Inserting the checking single photons and transmitting the PB sequence** According to EK_{A1} (one part of Alice's authentication key EK_A), Alice prepares the non-orthogonal single photons in batch, namely the S batch, and inserts randomly them into the PB sequence. These single photons will be used to check eavesdropping and authenticate Alice's identity. Finally, Alice sends the PB sequence to Bob and keeps the PA sequence in her hand.

(S7) **Verifying Alice's identity and checking eavesdropping** After confirming Bob has received the PB sequence, Alice announces publicly the positions of the S batch, and then Bob can easily distinguish the S batch from the PB sequence. According to EK_{A1}, Bob makes the corresponding Z-basis or X-basis measurement on the particles of the S batch. Having compared his measurement results with EK_{A2} (the other part of Alice's authentication key EK_A), Bob can estimate the error rate. If the error rate exceeds the threshold, they abort the scheme and repeat the quantum communication from the beginning. Otherwise, they continue to the next step.

(S8) **Extracting message from the *PB* sequence** Alice performs Z-basis measurements on her particles a_1 and a_2 in the PA sequence, respectively, and Bob performs Bell measurements on the partner particle pairs (b_1 and b_2) in the PB sequence.

Table 1. Relations of Bob's measurement (listed in the top row), Alice's publication (listed in the left column), and the encoding operations (i.e. the message) in our DSQC scheme.

	$\|\phi^+\rangle_{b_1b_2}$	$\|\phi^-\rangle_{b_1b_2}$	$\|\psi^+\rangle_{b_1b_2}$	$\|\psi^-\rangle_{b_1b_2}$
$\|00\rangle_{a_1a_2}$	I_4 (00)	$\sigma_{z4}(11)$	$\sigma_{x4}(01)$	$\mathrm{i}\,\sigma_{y4}(10)$
$\|11\rangle_{a_1a_2}$	$\sigma_{z4}(11)$	I_4 (00)	$\mathrm{i}\,\sigma_{y4}(10)$	$\sigma_{x4}(01)$
$\|01\rangle_{a_1a_2}$	$\mathrm{i}\,\sigma_{y4}(10)$	$\sigma_{x4}(01)$	$\sigma_{z4}(11)$	I_4 (00)
$\|10\rangle_{a_1a_2}$	$\sigma_{x4}(01)$	$\mathrm{i}\,\sigma_{y4}(10)$	I_4 (00)	$\sigma_{z4}(11)$

Alice then publishes her measurement results of the particles a_1 and a_2. Thus Bob can obtain Alice's secret message by comparing his measurement results with Alice's corresponding publication results according to Table 1.

3. Security and efficiency analysis

3.1. Security analysis

Let us discuss the security for the present scheme. The most possible attack is the intercept-resend attack. Moreover, suppose that Eve knows that Bob measures his particles in the Bell basis. In this kind of attack, Eve intercepts the particles in the PB sequence, makes Bell measurements on them, and then resends the two-particle sequence to Bob. Suppose Eve's measurement result is $|\phi^+\rangle$, then the possible operation is I, σ_x, $\mathrm{i}\sigma_y$ or σ_z with probability 1/4, which is shown in Table 1. So, there is $-4\times\frac{1}{4}\log_2\frac{1}{4}=2$ bits message per cluster state unknown to Eve, and the message we want to send is just 2 bits, that is to say, Eve cannot get any information about the message. Furthermore, Eve will soon be found by the single-photon checking procedure in step (S7). Because the single-photon particles are prepared by two nonorthogonal bases: the Z basis $\{|0\rangle, |1\rangle\}$ and the X basis $\{|+\rangle, |-\rangle\}$, so the process of checking eavesdropping is essentially identical to that in the BB84 protocol.[1] As we all know, some works[5,6] have proven the BB84 QKD protocol is unconditionally secure. Therefore, the checking process is secure and Eve will be found if he disturbs the quantum channel. In a word, Eve will be detected, besides, she obtains no information about the message before she is found.

Another potential attack is the impersonator's attack, which is a typical active attack. Suppose that Eve impersonates Bob, receives all particles from Alice, and tries to acquire the message without being detected. As described in our protocol, EK_A is regarded as Alice's identity key, and it is only known between Alice and Bob in advance. Hence, he will soon be detected when Bob checks eavesdropping and authenticates Alice's identity, because Eve does not have any information about EK_A, and cannot prepare the right non-orthogonal single-photon particles which were prepared according to EK_{A1}. If Eve prepares randomly single-photon particles to Bob, then her probability of successful impersonation is less than $(1/2)^l$ (l is the length of the S batch). The larger the l is, the smaller the probability is. So, we can say, our scheme is immune to the impersonator's attack.

3.2. Efficiency analysis

In 2006, Li *et al*[23] presented a useful efficiency coefficient to describe the utilization rate of the quantum resource: $\eta = m_u/(q_t + b_t)$ (m_u is the numbers of messages transmitted, q_t is the number of total qubits used and b_t is the numbers of the classical bits exchanged). Since the legitimate users need two bits of classical information and a four-qubit cluster state to communicate two bits of secret message, that is, m_u= 2, q_t= 4 and b_t= 2, our scheme's efficiency is $\eta_{\mathrm{our}} = 2/(4+2) = 1/3$. While in the WFT06 protocol, the users utilize one bit of classical information and a four-qubit cluster state to communicate one bit of secret message, that is, $m_u = 1$, $q_t = 4$ and $b_t = 1$, so $\eta_{\mathrm{WFT06}} = 1/(4+1) = 1/5$. Obviously, $\eta_{\mathrm{our}} \approx 1.67\eta_{\mathrm{WFT06}}$, that is to say, our scheme is more efficient than the WFT06 protocol. In the present scheme, we use single photons instead of the high-cost cluster states for checking eavesdropping. So, our scheme is more economic with the present-day technique. Alternatively, we use the cluster state as carriers, it is easily processed by a one-way quantum computer.[28]

4. Conclusions

In this paper, we have presented an efficient DSQC scheme based on the four-qubit cluster states and single-photon identity authentication. The two legitimate users exploit the four local unitary operations $\{I, \sigma_x, \mathrm{i}\sigma_y, \sigma_z\}$ to encode their secret messages, and then decode them by using the Bell measurements and the Z-basis measurements with help of classical information exchanging. The security is analyzed to be secure against the intercept-resend attack and the impersonator's attack. Moreover, this scheme has the advantage of high capacity as each cluster state can carry two bits of information, twice that of the WFT06 protocol, and its efficiency coefficient $\eta_{\mathrm{our}} = 1/3$, which is approximately 1.67 times that of the WFT06 protocol.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing,* Bangalore, India (New York: IEEE) pp175–179

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[4] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018

[5] Yang Y G and Wen Q Y 2007 *Chin. Phys.* **16** 2215

[6] Yang Y G, Wen Q Y and Zhu F C 2007 *Chin. Phys.* **16** 910

[7] Lo H K and Chau H F 1999 *Science* **283** 2050

[8] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[9] Long G L, Deng F G, Wang C, Li X, Wen K and Wang W 2007 *Front. Phys.* **2** 251

[10] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

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

[12] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15

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

[14] Man Z X and Xia Y J 2007 *Chin. Phys.* **16** 1197

[15] Yang Y G, Wen Q Y and Zhu F C 2007 *Chin. Phys.* **16** 1838

[16] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149

[17] Yan F L and Zhang X 2004 *Euro. Phys. J.* B **41** 75

[18] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18

[19] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento* B **119** 313

[20] Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A: *Math. Gen.* **38** 5761

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

[22] Cao H J and Song H S 2006 *Chin. Phys. Lett.* **23** 290

[23] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P and Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354

[24] Lee H, Lim J, and Yang H, 2006 *Phys. Rev.* A **73** 042305

[25] Zhang Z J, Liu J, Wang D and Shi S 2007 *Phys. Rev.* A **75** 026301

[26] Liu W J, Chen H W, Li Z Q and Liu Z H 2008 *Chin. Phys. Lett.* **25** 2354

[27] Raussendorf R and Briegel H J 2001 *Phys. Rev. Lett.* **86** 5188

[28] Wang G Y, Fang X M and Tan X H, 2006 *Chin. Phys. Lett.* **23** 2658