Comment on "Quantum direct communication with authentication"

Zhan-jun Zhang,[1,2,*] Jun Liu,[2] Dong Wang,[2] and Shou-hua Shi[2]
[1]*Department of Physics and Center for Quantum Information Science, National Cheng Kung University, Tainan 70101, Taiwan*
[2]*Key Laboratory of Optoelectronic Information Acquisition & Manipulation of Ministry of Education of China, School of Physics & Material Science, Anhui University, Hefei 230039, China*
(Received 19 April 2006; published 23 February 2007)

Two protocols of quantum direct communication with authentication [Phys. Rev. A **73**, 042305 (2006)] were recently proposed by Lee, Lim, and Yang. In this paper we will show that in the two protocols the authenticator Trent should be prevented from knowing the secret message. The first protocol can be eavesdropped on by Trent using the intercept-measure-resend attack, while the second protocol can be eavesdropped on by Trent using a simple single-qubit measurement. To fix these leaks, we revise the original versions of the protocols by using the Pauli Z operation σ_z instead of the original bit-flip operation X. As a consequence, the attacks we present can be prevented and accordingly the protocol securities are improved.

DOI: 10.1103/PhysRevA.75.026301 PACS number(s): 03.67.Dd

Quantum key distribution (QKD) is one of the most interesting topics in quantum-information processing, which provides a novel way for two legitimate parties to share a common secret key over a long distance with negligible leakage of information to an eavesdropper Eve. Its ultimate advantage is the unconditional security. Hence, after Bennett and Brassard's pioneering work published in 1984 [1], much attention has been focused on this topic and a variety of quantum-communication protocols [1–13,17,18] have been proposed. In these works, various properties of quantum mechanics, such as the no-cloning theorem, uncertainty principle, entanglement, indistinguishability of nonorthogonal states, nonlocality, and so on, are used to accomplish QKD tasks. Different from QKD, the deterministic quantum secure direct communication (QSDC) protocol is to transmit directly the secret message without first generating a QKD to encrypt them. Hence it is very useful and usually desired, especially if there is some urgency. However, a deterministic secure direct communication protocol is more demanding on security. Therefore, only recently a few deterministic secure direct communication protocols have been proposed [3–12] and some of them are essentially insecure [13–15,19,20]. Recently, using the Greenberger-Horne-Zeilinger (GHZ) states [16] Lee, Lim, and Yang proposed two QSDC protocols of quantum direct communication with authentication [12]. Based on some security analysis they claimed that their two protocols are secure. However, in this paper we will show that in the two protocols the authenticator Trent should be prevented from knowing the secret message. The first protocol can be eavesdropped on by Trent using the intercept-measure-resend attack, while the second protocol can be eavesdropped on by Trent using single-qubit measurement. We will fix these leaks by modifying the original versions of the protocols using the Pauli Z operation σ_z instead of the original bit-flip operation X so that the attacks we present can be prevented and accordingly the protocol securities are improved.

There are three parties in either of the Lee-Lim-Yang protocols. Alice and Bob are the two legitimate users of the communication. Trent is the third party who is introduced to authenticate the two users participating in the communication. He is assumed to be more powerful than the other two parties and supplies the GHZ states each in the form of $|\Psi\rangle=(|000\rangle+|111\rangle)/\sqrt{2}$. The protocols are composed of two parts: one is for an authentication process and the other for a direct communication. The authentication process is the same for both Lee-Lim-Yang protocols. After the authentication, there are two possibilities for Alice to send qubits: one is to Bob and the other is to Trent. The former case corresponds to the Lee-Lim-Yang protocol 1 and the latter case to the protocol 2. This is a difference between the two protocols. Incidentally, there is an unphysical mistake about the responses in the text of Ref. [12].

The purpose of the authentication process in the Lee-Lim-Yang protocols is to let the three participants safely share GHZ states. To achieve this goal, it is assumed that Trent should share in *a priori* secret authentication keys K_{ta} and K_{tb} with Alice and Bob, respectively. The lengths of the authentication keys K_{ta} and K_{tb} are larger than the length of the bit string of the secret message which will be communicated from Alice to Bob. According to the one-time pad cryptography, when the private key length is equal to the secret message length, the secret message can be securely communicated to remote places after encryption. If Trent is not assumed to be prevented from knowing the secret message, then in this case the secret message can be transferred in the following very simple classical way instead of using the Lee-Lim-Yang QSDC protocols, i.e., Alice can securely send the secret message to Trent by using their secret authentication key K_{ta} and then Trent can securely send the secret message to Bob by using their secret authentication key K_{tb}. Hence, in the Lee-Lim-Yang protocols Trent should be prevented from knowing the secret message though he is introduced to authenticate the communication.

Assume that the GHZ states are safely shared among the three parties after the authentication process. Let us now briefly review the second part of the Lee-Lim-Yang protocol 1.

(a) Alice selects a subset of GHZ states of her remaining set after authentication and keeps it secret.

*Electronic address: zjzhang@ahu.edu.cn

 ©2007 The American Physical Society

(b) Alice chooses a random bit string which has no correlation with the secret message to transmit to Bob. This bit string will be used to check the security of the quantum channel.

(c) Following this random bit string, Alice performs unitary operations on the qubits selected for this check process. The unitary operations are defined as follows: the bit 0 corresponds to H and the bit 1 to HX, where H is the Hadamard operation and X is the bit-flip operation. The GHZ states after Alice's operations are transformed into

$$\begin{aligned} H_A|\Psi\rangle &= H_A(|000\rangle_{ATB} + |111\rangle_{ATB})/\sqrt{2} \\ &= \frac{1}{2}\{|000\rangle_{ATB} + |100\rangle_{ATB} + |011\rangle_{ATB} - |111\rangle_{ATB}\} \\ &= \frac{1}{2}\{(|\phi^+\rangle_{AB} - |\psi^-\rangle_{AB})|-\rangle_T + (|\phi^-\rangle_{AB} + |\psi^+\rangle_{AB})|+\rangle_T\}, \end{aligned} \tag{1}$$

$$\begin{aligned} H_A X_A|\Psi\rangle &= H_A(|100\rangle_{ATB} + |011\rangle_{ATB})/\sqrt{2} \\ &= \frac{1}{2}\{|000\rangle_{ATB} - |100\rangle_{ATB} + |011\rangle_{ATB} + |111\rangle_{ATB}\} \\ &= \frac{1}{2}\{(|\phi^-\rangle_{AB} - |\psi^+\rangle_{AB})|-\rangle_T + (|\phi^+\rangle_{AB} \\ &\quad + |\psi^-\rangle_{AB})|+\rangle_T\}, \end{aligned} \tag{2}$$

where $|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

(d) Alice encodes the secret message with a classical error correction code on the remaining GHZ states in terms of the unitary operation definition in (c).

(e) After making all unitary operations, Alice sends the encoded qubits to Bob.

(f) Bob makes Bell measurements on pairs of particles consisting of his qubit and Alice's qubit.

(g) Trent measures his third qubit in the x basis $\{|+\rangle,|-\rangle\}$ and publishes the measurement outcomes.

(h) Using Trent's publication and his Bell-state measurement outcomes, Bob infers all Alice's secret bits consisting of both the random bits and the secret message.

(i) Bob lets Alice reveal the check bits' positions and values.

(j) Bob can know whether the quantum channel is disturbed according to the error rate. If the error rate is higher than expected, it is concluded that there is an eavesdropper in the communication but fortunately the secret message is not leaked out. If the error rate is lower, Bob can extract the secret message (see Table I in Ref. [12]).

As we showed before, the authenticator Trent should be prevented from knowing the secret message. Otherwise, the communication can be realized in a very simple classical way. Although the Lee-Lim-Yang protocol 1 is claimed to be secure (that is, the secret message cannot be leaked out), the insider Trent can eavesdrop on the secret message by using the intercept-measure-resend attack. This can be seen as follows. When Alice sends her encoded qubits to Bob, Trent intercepts the qubits and performs the H operation on each qubit. In this case, all the states are transformed into

$$H_A H_A|\Psi\rangle = (|000\rangle_{ATB} + |111\rangle_{ATB})/\sqrt{2}, \tag{3}$$

$$H_A H_A X_A|\Psi\rangle = (|100\rangle_{ATB} + |011\rangle_{ATB})/\sqrt{2}. \tag{4}$$

After the unitary operations, Trent measures Alice's qubit and his qubit in the z basis $\{|0\rangle,|1\rangle\}$. If the two outcomes are the same, then Trent can conclude that Alice has performed a H operation corresponding to the bit 0. Otherwise, Alice has performed a HX operation corresponding to the bit 1. In this case, Trent has already got Alice's whole bit string including both the random bit string and the secret message. In the following what he needs to do is to remove the random bits. Fortunately, in the step (i), Alice will publish which qubits are used as check qubits. This means that Trent can completely know the secret message using this intercept-measure-resend attack.

After Trent's attack, he sends Alice's qubits to Bob. One can easily find that for Alice and Bob the error rate will obviously be higher than expected. Unfortunately, about the Lee-Lim-Yang protocol 1 the authors wrote: "If the error rate is higher than expected, Alice and Bob conclude there was an eavesdropper in the communication. In this case, the transferred message contains errors, but fortunately Eve cannot obtain any of the content" (see the last few sentences Ref. [12], p. 2). This means that Alice and Bob only know that the channel is disturbed and still believe that the secret message has not leaked out.

To fix this leak, we think the original version of the Lee-Lim-Yang protocol 1 can be modified by using the Pauli Z operation σ_z instead of the original bit-flip operation X. In this case, the total states after Alice's operations are represented as follows:

$$\begin{aligned} H_A|\Psi\rangle &= H_A(|000\rangle_{ATB} + |111\rangle_{ATB})/\sqrt{2} \\ &= \frac{1}{2}\{|000\rangle_{ATB} + |100\rangle_{ATB} + |011\rangle_{ATB} - |111\rangle_{ATB}\} \\ &= \frac{1}{2}\{(|\phi^+\rangle_{AB} - |\psi^-\rangle_{AB})|-\rangle_T + (|\phi^-\rangle_{AB} + |\psi^+\rangle_{AB})|+\rangle_T\}, \end{aligned} \tag{5}$$

$$\begin{aligned} H_A\sigma_{zA}|\Psi\rangle &= H_A(|000\rangle_{ATB} - |111\rangle_{ATB})/\sqrt{2} \\ &= \frac{1}{2}\{|000\rangle_{ATB} + |100\rangle_{ATB} - |011\rangle_{ATB} + |111\rangle_{ATB}\} \\ &= \frac{1}{2}\{(|\phi^-\rangle_{AB} + |\psi^+\rangle_{AB})|-\rangle_T \\ &\quad + (|\phi^+\rangle_{AB} - |\psi^-\rangle_{AB})|+\rangle_T\}. \end{aligned} \tag{6}$$

After this modification, if Trent intercepts Alice's encoded qubits and performs H operations, then the total states are transformed into

TABLE I. Relations of Alice's operation, Bob's measurement, and Trent's announcement in the revised Lee-Lim-Yang protocol 1.

Trent's announcement	Bob's measurement	Alice's operation
$\|+\rangle_T$	$\|\phi^+\rangle_{AB}$ or $\|\psi^-\rangle_{AB}$	$H\sigma_z$ (1)
$\|+\rangle_T$	$\|\phi^-\rangle_{AB}$ or $\|\psi^+\rangle_{AB}$	H (0)
$\|-\rangle_T$	$\|\phi^+\rangle_{AB}$ or $\|\psi^-\rangle_{AB}$	H (0)
$\|-\rangle_T$	$\|\phi^-\rangle_{AB}$ or $\|\psi^+\rangle_{AB}$	$H\sigma_z$ (1)

TABLE II. Relations of Alice's operation, Bob's measurement, and Trent's announcement in the revised Lee-Lim-Yang protocol 2.

Trent's announcement	Bob's measurement	Alice's operation
0 ($\|\phi^+\rangle_{AT}$ or $\|\psi^-\rangle_{AT}$)	$\|+\rangle_B$	$H\sigma_z$ (1)
0 ($\|\phi^+\rangle_{AT}$ or $\|\psi^-\rangle_{AT}$)	$\|-\rangle_B$	H (0)
1 ($\|\phi^-\rangle_{AT}$ or $\|\psi^+\rangle_{AT}$)	$\|+\rangle_B$	H (0)
1 ($\|\phi^-\rangle_{AT}$ or $\|\psi^+\rangle_{AT}$)	$\|-\rangle_B$	$H\sigma_z$ (1)

$$H_A H_A|\Psi\rangle = (|000\rangle_{ATB} + |111\rangle_{ATB})/\sqrt{2}, \tag{7}$$

$$H_A H_A \sigma_{zA}|\Psi\rangle = (|000\rangle_{ATB} - |111\rangle_{ATB})/\sqrt{2}. \tag{8}$$

If he measures, respectively, his qubit and Alice's qubit in the z basis, the outcomes will always be the same. In this case, he cannot know for each of Alice's qubits which unitary operation has been performed. This means that Trent cannot know Alice's secret message. However, one can easily find that the revised protocol works successfully as for as Alice and Bob's communication is concerned. See Table I for a brief summary.

Let us now briefly review the second part of the Lee-Lim-Yang protocol 2. The second protocol is the same as the first except Alice sends her encoded qubits to Trent. After making Bell measurements on his and Alice's qubits, Trent reveals the result. If the Bell measurement outcome is $|\phi^+\rangle$ or $|\psi^-\rangle$, then Trent publicly announces 0. Otherwise he notifies 1. Bob measures his particles in the x basis. Then the total state of the system is the same as in Eqs. (1) and (2) if the subscripts B and T are interchanged. Using Trent's publication and his measurement outcomes, Bob can infer Alice's secret message. Finally, Alice reveals the positions and values of her check bits and compares them with Bob's. If the error rate is higher than expected, Bob throws away the message. Otherwise, Bob can get the secret message (see Table II in Ref. [12]).

Similarly, in the protocol 2 Trent can eavesdrop on the secret message by using single-qubit measurement, i.e., he performs a H operation on each qubit he received from Alice and then measures, respectively, Alice's qubit and his qubit in the z basis to extract the secret message. After Trent's attack, he randomly publishes some Bell measurement outcomes to Bob. In this case, Trent can get the secret message but Alice and Bob know only that the channel is disturbed and still believe that the secret message is not leaked out.

To fix this leak, the original version of Lee-Lim-Yang protocol 2 can also be modified by using the Pauli Z operation σ_z instead of the original bit-flip operation X. The transformation of the whole states and the specific analysis are the same as the statements above if the subscripts B and T are interchanged. For simplicity, here we do not repeat any more. See Table II for a brief summary.

To summarize, in this paper we have shown that the Lee-Lim-Yang protocols can be eavesdropped on by the authenticator Trent using some specific attacks, and we have revised the original versions of the protocols by using the Pauli Z operation σ_z instead of the original bit-flip operation X, so that the attacks we present can be prevented and accordingly the protocol securities are improved.

Z.Z. thanks Dr. Hwayean Lee for her reading of the original manuscript and her affirmation of our improvement on her work. This work is supported by the National Natural Science Foundation of China under Grants No. 60677001 and No. 10304022, the Science Technology Fund of Anhui Province for Outstanding Youth under Grant No. 06042087, the general fund of the Educational Committee of Anhui Province under Grant No. 2006KJ260B, and the key fund of the Ministry of Education of China under Grant No. 206063.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984* (IEEE, New York, 1984), p. 175.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).
[4] K. Bostroem and F. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[5] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[6] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[7] B. A. Nguyen, Phys. Lett. A **328**, 6 (2004).
[8] Z. J. Zhang, Z. X. Man, and Y. Li, Int. J. Quantum Inf. **2**, 521 (2004).
[9] Z. J. Zhang, Z. X. Man, and Y. Li, Chin. Phys. Lett. **22**, 18 (2005).
[10] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
[11] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Phys. Rev. A **71**, 044305 (2005).
[12] Hwayean Lee Jongin Lim, and HyungJin Yang, Phys. Rev. A **73**, 042305 (2006).
[13] Z. X. Man, Z. J. Zhang, and Y. Li, Chin. Phys. Lett. **22**, 22 (2005).
[14] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Lett. A **333**, 46 (2004).
[15] Z. J. Zhang, e-print quant-ph/0604035.

[16] D. M. Greenberger, M. A. Horne, A. Shimony, and Z. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[17] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Rev. A **71**, 044301 (2005).
[18] Z. J. Zhang and Z. X. Man, Phys. Rev. A **72**, 022303 (2005).
[19] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Lett. A **341**, 385 (2005).
[20] A. Wojcik, Phys. Rev. Lett. **90**, 157901 (2003).