Quantum direct communication with authentication

Hwayean Lee,[1,3,*] Jongin Lim,[1,†] and HyungJin Yang[1,2,‡]

[1]*Center for Information Security Technologies (CIST) and Graduate School of Information Security (GSIS), Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea*

[2]*Department of Physics, Korea University, Chochiwon, Choongnam, Korea*

[3]*Institut für Experimentalphysik, Universität Wien, Austria*

(Received 6 December 2005; published 7 April 2006)

We propose two quantum direct communication (QDC) protocols with user authentication. Users can identify each other by checking the correlation of Greenberger-Horne-Zeilinger (GHZ) states. Alice can directly send a secret message to Bob without any previously shared secret using the remaining GHZ states after authentication. Our second QDC protocol can be used even though there is no quantum link between Alice and Bob. The security of the transmitted message is guaranteed by properties of entanglement of GHZ states.

DOI: 10.1103/PhysRevA.73.042305 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum cryptography utilizes the original characteristics of quantum mechanics such as superposition and entanglement. Using these properties, information can be secretly shared between users through a quantum channel. The information can be a key or a message. Quantum key distribution (QKD) protocols are used to share a key and quantum direct communication (QDC) protocols are employed to send a message.

Many QKD protocols have been proposed since Bennett and Brassard first proposed a quantum key distribution protocol [1] in 1984. The security of some QKD protocols was theoretically proven in [2–4]. On the other hand, QDC is starting to be researched nowadays. The first QDC protocol was proposed by Beige *et al.* [5] in 2002. It was followed by other QDC protocols [6–10].

The proposed protocols have some shortcomings, however. In most QDC protocols except two protocols proposed by Beige *et al.* [5] and Deng *et al.* [6], the receiver (Bob) must initiate communication in order to receive a secret message from the sender (Alice). For example Bob should generate single photons [7,8] or Bell states [9] or qutrit states [10] and transmit all or some part of them to Alice. In addition, most QDC protocols are vulnerable to the man in the middle attack.

We propose two QDC protocols, which combine user authentication and direct communication. To authenticate users, an authentication method proposed in [11] is introduced. After authentication Alice can send a secret message directly to Bob. This message cannot be leaked to a third party. Moreover, Alice and Bob can communicate without a quantum link between them in our second QDC protocol. We present our QDC protocols in Sec II, analyze the security of them in Sec III, and make conclusions in Sec IV.

II. QUANTUM DIRECT COMMUNICATION PROTOCOLS

Our quantum direct communication protocols are composed of two parts: one is for an authentication process and the other is for a direct communication. A third party, Trent, is introduced to authenticate the users participating in the communication. He is assumed to be more powerful than other users and he supplies the Greenberger-Horne-Zeilinger (GHZ) states [12].

A. Authentication

The user's secret identity sequence and one-way hash function are known to Trent. This information must be kept secret. Suppose Alice's identity sequence is ID_A and her one-way function is h_A. Similarly Bob has an identity sequence ID_B and a one-way hash function h_B. In this paper, the one-way hash function h has the following form:

$$h:\{0,1\}^* \times \{0,1\}^l \rightarrow \{0,1\}^c \qquad (1)$$

where the asterisk, l, and c represent an arbitrary length, the length of a counter, and a fixed number, respectively. The user's authentication key shared with Trent can be calculated as $h_{user}(\mathrm{ID}_{user}, c_{user})$, where c_{user} is the counter of calls on the user's hash function. Authentication keys are used to determine which unitary operations will be performed on GHZ particles heading from Trent to the owner. Users can authenticate each other by checking the correlation of the GHZ states after performing the reverse unitary operations.

If Alice wants to send a secret message to Bob, she notifies Bob and Trent. On receiving this request, Trent generates N tripartite GHZ states $|\Psi\rangle(=|\Psi_1\rangle\cdots|\Psi_N\rangle)$. For simplicity, the following GHZ state $|\Psi_i\rangle$ is supposed to be prepared:

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB}) \quad (i = 1,2,\ldots,N), \qquad (2)$$

where the subscripts A, T, and B correspond to Alice, Trent, and Bob, respectively. In this paper, we represent the z basis as $\{|0\rangle,|1\rangle\}$ and the x basis as $\{|+\rangle,|-\rangle\}$, where $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$.

[*] Electronic address: hylee@korea.ac.kr; hwayean.lee@univie.ac.at

[†] Electronic address: jilim@korea.ac.kr

[‡] Electronic address: yangh@korea.ac.kr

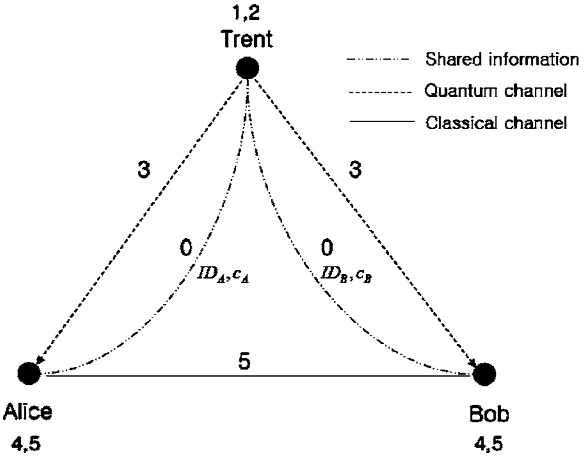

FIG. 1. Procedures of authentication 0 (prerequisite). Alice and Bob register their secret identities and hash functions with Trent. (1) Trent generates GHZ states $|\Psi\rangle = (1/\sqrt{2})(|000\rangle_{ATB} + |111\rangle_{ATB})$. (2) Trent makes unitary operations on $|\Psi\rangle$ with Alice's and Bob's authentication keys. (3) Trent distributes GHZ particles to Alice and Bob. (4) Alice and Bob make reverse unitary operations on their qubits with their authentication keys. (5) Alice and Bob choose a subset of GHZ states, make local measurements in the z basis on them, and compare the results.

Next, Trent encodes Alice's and Bob's particles with their authentication keys $h_A(\mathrm{ID}_A, c_A)$ and $h_B(\mathrm{ID}_B, c_B)$, respectively. For example, if the ith value of $h_A(\mathrm{ID}_A, c_A)$ is 0, then Trent makes an identity operation I to Alice's particle of the ith GHZ state. If it is 1, a Hadamard operation H is applied. If the authentication key does not have enough length to cover all GHZ particles, new authentication keys can be created by increasing the counter until the authentication keys cover all GHZ particles. After making operations on the GHZ particles, Trent distributes the particles to Alice and Bob and keeps the remaining ones for him.

On receiving the qubits, Alice and Bob decode the qubits with unitary transformations which are defined by their respective authentication keys. Next, Alice and Bob select some of the decoded qubits, make von Neumann measurements on them, and compare the results through a public channel. If the error rate is higher than expected, then Alice and Bob abort the protocol. Otherwise they can confirm that their counter parts are legitimate and the channel is secure. Alice and Bob then execute the following message transmission procedures. The authentication process is shown in Fig. 1.

B. Direct communication protocol 1

Alice selects a subset of GHZ states of her remaining set after authentication and keeps it secret. She chooses a random bit string which has no relation to the secret message to transmit to Bob. This random bit string will be used to check the security of the channel. Following this random bit string, Alice performs unitary transformations on the qubits selected for this check process. Before encoding the message and the random bit string on qubits, Alice can encode the secret message with a classical error correction code (ECC) such as the Hamming code, the Reed-Solomon code, or the BCH (Bose-Chaudhuri-Hochquenghem) code, so that Bob will be able to correct errors in the decoded message. For example, if the error rate of the quantum channel is 10% and the length of the codeword is n, then any classical ECC can be used, where the minimum length of the code d is larger than $\lfloor \frac{n}{5} \rfloor + 1$.

If a bit of the random bit string or the message is 0, then Alice makes a Hadamard operation H on her GHZ particle. Otherwise, Alice performs a bit-flip operation X and a Hadamard operation H on her qubit. The total state of the system after Alice's operations is represented as follows:

$$\begin{aligned} H_A|\Psi\rangle &= \frac{1}{2}\{|000\rangle_{ATB} + |100\rangle_{ATB} + |011\rangle_{ATB} - |111\rangle_{ATB}\} \\ &= \frac{1}{2}\{(|\phi^+\rangle_{AB} - |\psi^-\rangle_{AB})|-\rangle_T + (|\phi^-\rangle_{AB} + |\psi^+\rangle_{AB})|+\rangle_T\} \end{aligned} \tag{3}$$

when Alice performs an H operation,

$$\begin{aligned} H_A X_A|\Psi\rangle &= \frac{1}{2}\{|000\rangle_{ATB} - |100\rangle_{ATB} + |011\rangle_{ATB} + |111\rangle_{ATB}\} \\ &= \frac{1}{2}\{(|\phi^+\rangle_{AB} + |\psi^-\rangle_{AB})|+\rangle_T + (|\phi^-\rangle_{AB} - |\psi^+\rangle_{AB})|-\rangle_T\} \end{aligned} \tag{4}$$

when Alice performs an HX operation, where we used the following notations for Bell states:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\},$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\{|00\rangle - |11\rangle\},$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\{|01\rangle + |10\rangle\},$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\}. \tag{5}$$

After making all unitary operations, Alice sends the encoded qubits to Bob. Bob makes Bell measurements on pairs of particles consisting of his qubit and Alice's qubit. Trent measures his third qubit in the x basis and publicly announces the measurement outcomes. Bob can then recover Alice's message using Table I. For example, when Bob measures $|\phi^+\rangle$ and Trent reveals $|+\rangle$, Bob can infer that Alice performed an HX operation and the message she sent is 1. After obtaining all messages, Bob notifies Alice of this fact. Alice reveals the position of the check bits and compares the measurement outcomes with Bob's. 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. If the error rate is lower, Bob can extract the secret

TABLE I. The relations of Alice's operation, Bob's measurement, and Trent's announcement in the QDC protocol 1 can be summarized as follows.

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

TABLE II. The relations of Alice's operation, Bob's measurement, and Trent's announcement in the QDC protocol 2 can be summarized as follows.

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

message from the remaining bits. This communication protocol is shown in Fig. 2.

C. Direct communication protocol 2

After the authentication process, there are only two possibilities for Alice to send qubits: one is to Trent and the other is to Bob. The first one is our first QDC protocol and the second is the protocol described in this section. The second QDC protocol is the same as the first protocol except Alice sends her encoded qubits to Trent. There is no need for an additional quantum link between Alice and Bob in this protocol. After making Bell measurements on his and Alice's qubits, Trent reveals the results. 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 (this process done by Bob can even precede Alice's operations). Then the total state of the system is the same as in Eqs. (3) and (4) if the subscripts B and T are interchanged. Using Trent's publication and his measurement outcomes, Bob can infer which operations were performed by Alice as shown in Table II. For example, if 0 is published and $|+\rangle$ is measured, Bob can discover that Alice performed an HX operation and the message is 1.

Alice reveals the positions of her check bits and compares them with Bob's. If the error rate of the check bits is higher than expected, Bob throws away the message. Otherwise, Bob can get the whole secret message by applying the classical ECC code used by Alice. This second communication protocol is shown in Fig. 3.

III. SECURITY ANALYSIS

The security of our protocol results from the properties of the entanglement of GHZ states. We first analyze the process

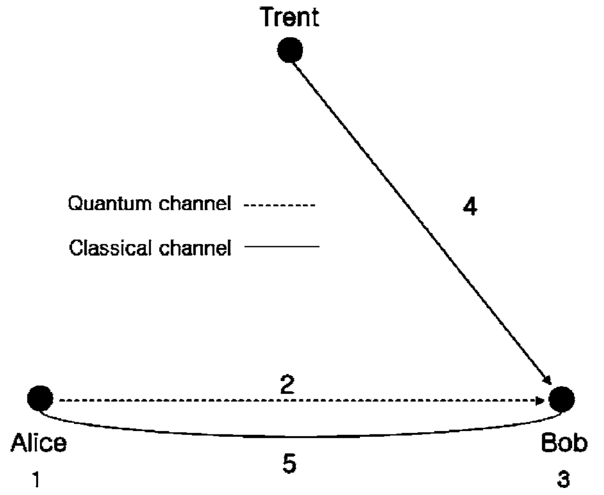

FIG. 2. Procedures of the first direct communication protocol (GHZ states were distributed as depicted in Fig. 1). (1) Alice chooses a subset of GHZ states and a random bit string. Alice performs unitary transformations both on the qubits selected for the check process following this random bit string and on the remaining qubits following the secret message. For example if the bit is 0, she makes a Hadamard operation H; otherwise a bit-flip operation and a Hadamard operation, HX. (2) Alice sends the qubits to Bob. (3) Bob makes Bell measurements on pairs of particles consisting of his qubit and Alice's qubit. (4) Trent makes von Neumann measurements on his GHZ particles and reveals the results. (5) Alice and Bob compare the check bits.

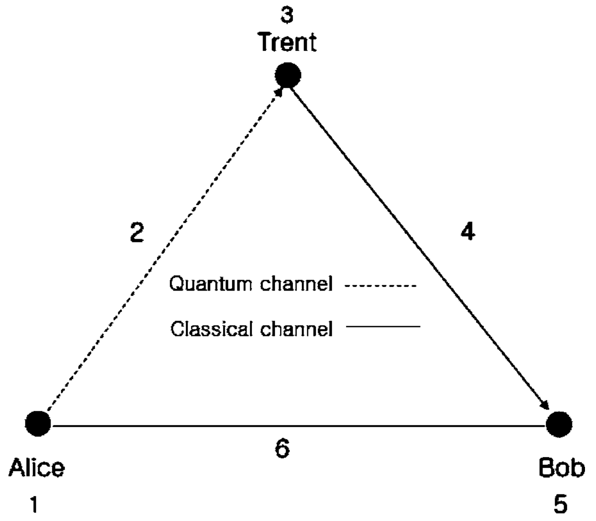

FIG. 3. Procedures of the second direct communication protocol (GHZ states were distributed as depicted in Fig. 1). (1) Alice chooses the position of check bits and a random bit string. Alice performs unitary transformations on the qubits selected for the check process following this random bit string and on the remaining qubits following the secret message. For example if the bit is 0, she makes a Hadamard operation H; otherwise a bit-flip operation and a Hadamard operation, HX. (2) Alice sends the encoded qubits to Trent. (3) Trent makes Bell measurements on pairs of particles consisting of his qubit and Alice's qubit. (4) Trent reveals the measurement outcomes. (5) Bob makes von Neumann measurements on his GHZ particles. (6) Alice and Bob compare the check bits.

of authentication. If Trent is honest as we supposed, he will generate tripartite GHZ states, encrypt them with the right authentication keys, and then distribute them to the designated users. Only the legitimate users can decrypt the qubits to recover the original GHZ states. This procedure can be written in the following form of a sequence of local unitary operations. The initial state

$$|\Psi_i\rangle_1 = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB}), \tag{6}$$

the state after Trent's transformation

$$\begin{aligned}|\Psi_i\rangle_2 = \{[1 - h_A(\mathrm{ID}_A, c_A)]I + [h_A(\mathrm{ID}_A, c_A)]H\}_A \\ \otimes \{[1 - h_B(\mathrm{ID}_B, c_B)]I + [h_B(\mathrm{ID}_B, c_B)]H\}_B|\Psi_i\rangle_1,\end{aligned} \tag{7}$$

and finally the state after Alice's and Bob's local operations

$$\begin{aligned}|\Psi_i\rangle_3 = \{[1 - h_A(\mathrm{ID}_A, c_A)]I + [h_A(\mathrm{ID}_A c_A)]H\}_A \\ \otimes \{[1 - h_B(\mathrm{ID}_B, c_B)]I + [h_B(\mathrm{ID}_B, c_B)]H\}_B|\Psi_i\rangle_2 = |\Psi_i\rangle_1,\end{aligned} \tag{8}$$

where $|\Psi_i\rangle$ is the state of the ith GHZ particle and the subscripts 1, 2, and 3 represent the three steps of authentication. Of course, this is only the case if there is no attacker Eve.

If Eve intercepts the qubits heading to Alice or Bob and impersonates the sender, then Eve can be detected with probability 1/4 per check bit in the authentication process. If Eve uses her probe for a coherent attack, she then causes an error per check bit with a probability 1/4, as in the Bennett-Brassard 1984 protocol when she uses the original bases used by Alice and Bob. In both cases, it is because Eve did not know the authentication key and she cannot decrypt the encoded qubits. For example, if the authentication key bit is 0, Eve does not make an error in the qubit. Otherwise, an error occurs with probability 1/2. If Eve prepares the $|0\rangle$ state and entangles it with Alice's qubit, then the final state of the system composed of GHZ states and Eve's qubit after decoding by Alice and Bob is as follows:

$$\begin{aligned}|\Psi'\rangle_{ATBE} &= U_{AE}|\Psi\rangle_{ATB} \otimes |0\rangle_E \\ &= \frac{1}{2}\{|000\rangle_{ATB}|+\rangle_E + |100\rangle_{ATB}|-\rangle_E + |011\rangle_{ATB}|-\rangle_E \\ &\quad + |111\rangle_{ATB}|+\rangle_E\}.\end{aligned} \tag{9}$$

This is for a specific attack where $U_{AE}|0\rangle_A|0\rangle_E \rightarrow |0\rangle_A|0\rangle_E$ and $U_{AE}|1\rangle_A|0\rangle_E \rightarrow |1\rangle_A|1\rangle_E$. Eve can be detected with higher probability than 1/2 per check bit in this case. Hence, if $m(\ll N)$ GHZ states are checked in the authentication process, Alice and Bob can confirm that the entangled states are distributed to the legitimate users with probability $1-(\frac{3}{4})^m$. We expect more advanced attacks to be detected when m is increased.

After the authentication process, only Alice's qubits are transmitted. Eve may make operations on these qubits in our QDC protocols. In both protocols, Eve must not disclose herself during the authentication process to obtain any information of the secret message. Suppose Eve uses the following unitary operation U_{AE} on the pair of Alice's and her qubit $|E\rangle$:

$$U_{AE}|0E\rangle_{AE} = \alpha|0\rangle_A|e_{00}\rangle_E + \beta|1\rangle_A|e_{01}\rangle_E, \tag{10}$$

$$U_{AE}|1E\rangle_{AE} = \beta'|0\rangle_A|e_{10}\rangle_E + \alpha'|1\rangle_A|e_{11}\rangle_E, \tag{11}$$

where $|\alpha|^2+|\beta|^2=1$, $|\alpha'|^2+|\beta'|^2=1$, and $\alpha\beta^* + \alpha'^*\beta' = 0$.

Then the total state of the protocol is changed as follows.

(1) The states after Alice performed a unitary operation are

$$\begin{aligned}|\Psi_1\rangle_{ATBE} &= U_A|\Psi\rangle_{ATB} \otimes |E\rangle_E \\ &= \frac{1}{2}(|000\rangle_{ATB} \mp |100\rangle_{ATB} + |011\rangle_{ATB} \pm |111\rangle_{ATB}) \\ &\quad \otimes |E\rangle_E.\end{aligned} \tag{12}$$

(2) The states after Eve made a unitary operation on her qubit and Alice's qubit heading to Bob or Trent are

$$\begin{aligned}|\Psi_2\rangle_{ATBE} = U_{AE}|\Psi_1\rangle_{ATBE} &= \frac{1}{2}\{|000\rangle_{ATB}(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle)_E + |100\rangle_{ATB}(\beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E + |011\rangle_{ATB}(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle)_E \\ &\quad + |111\rangle_{ATB}(\beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E\} \\ &= \frac{1}{2\sqrt{2}}[\phi^+_{AB}\{|+\rangle_T(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle + \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E + |-\rangle_T(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle - \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E\} \\ &\quad + \phi^-_{AB}\{|+\rangle_T(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle - \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E + |-\rangle_T(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle + \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E\} \\ &\quad + \psi^+_{AB}\{|+\rangle_T(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle + \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E - |-\rangle_T(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle - \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E\} \\ &\quad + \psi^-_{AB}\{|+\rangle_T(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle - \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E - |-\rangle_T(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle + \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E\}].\end{aligned} \tag{13}$$

As shown in the above equations, Eve introduces errors in the check bits with the probability of $1/2$ regardless of the order of measurement by Bob, Trent, and Eve. Moreover, Eve cannot get any information from this attack since Eve cannot distinguish whether Alice performed an H or HX operation. For example, suppose Alice performs an $H(0)$ operation, Bob measures $|\psi^+\rangle$, and Eve measures $|e_{00}\rangle$. Then Trent will reveal $|+\rangle$ or $|-\rangle$ with equal probability. If Trent reveals $|+\rangle$ then Bob can revoke the correct information. Otherwise, Bob can find an error. Hence if the length of the check sequence is long enough, Alice and Bob can detect the existence of Eve in the transmission of the message.

IV. CONCLUSIONS

In this paper, we propose two authenticated quantum direct communication protocols. To prevent man-in-the-middle attacks we do not need any preshared seed but Trent. Trent supplies GHZ states to Alice and Bob and he helps to recover the secret message by announcing his measurement outcomes publicly.

Alice and Bob can choose one of our two QDC protocols depending on the existence of a quantum link between them. In both cases, Alice can send a secret message directly to Bob without any leakage of the message. If eavesdropping occurs in the communication, the secret message will be broken and Alice and Bob can find out the existence of an eavesdropper by using the check bits. Though the message was broken, Eve cannot get any information from it because of the properties of entanglement of GHZ states.

We expect our protocol can be implemented in practice for quantum networks in spite of the weakness of the assumption of a trusted third party Trent. In particular, the second QDC protocol may be very useful for a restricted environment where there is no quantum link between Alice and Bob.

ACKNOWLEDGMENTS

We thank Marek Zukowski, Andreas Poppe, Hannes Hübel, and Anton Zeilinger for useful discussions and comments. This work was supported by the Korea Research Foundation funded by the Korean Government (MOEHRD) (Grant No. KRF-2005-213-D00090).

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[3] D. Mayers, e-print quant-ph/9802025.

[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[5] A. Beige, B. G. Englert, Ch. Kurstsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).

[6] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu, Phys. Rev. A **68**, 042317 (2003).

[7] Fu-Guo Deng and Gui Lu Long, Phys. Rev. A **69**, 052319 (2004).

[8] Marco Lucamarini and Stefano Mancini, Phys. Rev. Lett. **94**, 140501 (2005).

[9] Kim Bostroem and Timo Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[10] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long, Phys. Rev. A **71**, 044305 (2005).

[11] H. Lee, S. Lee, D. Lee, J. Lim, and H. Yang, e-print quant-ph/0510144.

[12] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).