Efficient Quantum Secure Direct Communication with Authentication

LIU Wen-Jie(刘文杰)1,2**, CHEN Han-Wu(陈汉武)1, LI Zhi-Qiang(李志强)1, LIU Zhi-Hao (刘志昊)1

1School of Computer Science and Engineering, Southeast University, Nanjing 210096
2School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044

(Received 12 December 2007)

Two protocols of quantum direct communication with authentication [Phys. Rev. A 73 (2006) 042305] were recently indicated to be insecure against the authenticator Trent attacks [Phys. Rev. A 75 (2007) 026301]. We present two efficient protocols by using four Pauli operations, which are secure against inner Trent attacks as well as outer Eve attacks. Finally, we generalize them to multiparty quantum direction communication.

PACS: 03.67.Dd, 03.67.Hk, 03.65.Ud

Since Wiesner\cite{1} and then Bennett et al.\cite{2} found that quantum effects can be used to transmit secret information in an open quantum channel, a remarkable surge of interest in the international scientific and industrial community has propelled quantum cryptography communication into mainstream of computer science and physics. Quantum key distribution (QKD) is the earliest and most mature branch of the mainstream, 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 the eavesdropper. Its ultimate advantage is the unconditional security. Hence, after Bennett and Brassard published the BB84 protocol,\cite{3} a variety of QKD protocols have been proposed, such as E91,\cite{4} B92,\cite{5} and six-state protocol,\cite{6} etc. The security of some QKD protocols was theoretically proven.\cite{7–9}

Recently, a new concept of quantum cryptography communication, quantum secure direct communication (QSDC), was proposed. Different from QKD, the deterministic QSDC protocol is to transmit directly the secret message without generating a random key to encrypt them, so it is more demanding on security. In 2002, Beige et al.\cite{10} presented the pioneering quantum secure direct communication scheme with singlet photon, then Bostrom et al.\cite{11} put forward a ‘ping-pong’ protocol with EPR state.<sup>11</sup> Since then, many other QSDC protocols have been proposed,\cite{12–23} These QSDC protocols can protect against eavesdropping attack called passive attack in cryptography,\cite{24} while they cannot resist other kind of attack, named active attack, such as the impersonation attack, the man-in-the-middle attack etc. To make up these shortcomings, recently Lee, Lim and Yang proposed two QSDC protocols of quantum direct communication with authentication (Lee–Lim–Yang (ZLY) protocols).\cite{25} However, Zhang et al.\cite{26} indicated that these protocols were insecure against the authenticator Trent’s attacks, and put forward two modified protocols by using the operation \(\sigma_x\) instead of the operation \(X\) (Zhang–Liu–Wang (ZLW) protocols).

In this Letter, we improve the ZLY protocols and the ZLW protocols, and propose two novel efficient QSDC protocols with authentication (EQSDCPs). Our modified EQSDCPs have no need to perform the Hadamard operation \(H\). They obtain the twice transition efficiency by utilizing four kinds of Pauli operation \(I, \sigma_x, i\sigma_y, \sigma_z\), and transmit two bits every GHZ state. What is more, these two EQSDCPs show the same security as the ZLY protocols when Trent is honest, and are also secure against ZLW’s Trent attacks when Trent is dishonest.

Let us start by illustrating some notations. We firstly define eight GHZ states as

\[
|P^\pm\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \quad |Q^\pm\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle),
\]

\[
|R^\pm\rangle = \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), \quad |S^\pm\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle),
\]

\[(1)
\]

and four Bell states (EPR pairs) as

\[
|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad (2)
\]

Suppose three parties, Alice, Bob and Trent, share a GHZ triplet \(|\varphi\rangle_{ATB} = |P^+\rangle_{ATB}\), where the subscripts \(A, T\) and \(B\) correspond to Alice, Trent and Bob, respectively. And \(|\varphi\rangle_{ATB}\) can be rewritten as follows:

\[
|\varphi\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} \pm |111\rangle_{ATB})
\]

\[
= \frac{1}{\sqrt{2}}((\phi^+)_{AB}|+\rangle_T + |\phi^−\rangle_{AB}|−\rangle_T), \quad (3)
\]

where \(|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\) and \(|−\rangle = \frac{1}{\sqrt{2}}(|0\rangle − |1\rangle)\).

---

*Supported by the National Natural Science Foundation of China under Grant No 60572071, the Natural Science Foundation of Jiangsu Province under Grant Nos BM2006504 and BK2007104, and the College Natural Science Foundation of Jiangsu Province under Grant No 06KJB520137.

**Email: wenjie@163.com

© 2008 Chinese Physical Society and IOP Publishing Ltd
Our EQSDCPs are composed of two parts: one is the authentication process, and the other is the direct communication process with dense coding. There are three parties, Alice and Bob are the two legitimate users of the communication, and Trent is the third party who will be used to authenticate the two users. And Trent is assumed to be more powerful than the other two parties and supplies the GHZ states.

The purpose of the authentication process is to let the three participants safely share GHZ states. Similar to Ref. [25], we suppose that Trent is a trusted third party, and he shares a secret identity number IDuser and a one-way hash function h with the legitimate users. Here the hash function is

$$h : \{0, 1\}^l \times \{0, 1\}^m \rightarrow \{0, 1\}^n, \quad (4)$$

where l, m and n denote the length of the identity number, the length of a counter, and the length of authentication key, respectively. Thus the user’s authentication key can be expressed as $AK_{user} = h(ID_{user}, c_{user})$, where $c_{user}$ is the counter of calls on the hash function. When the user want to continue next authentication process, he can obtain a new authentication key by only adding the counter number, and does not change his ID. In the authentication process, Trent performs authentication with Alice by using Alice’s authentication key $AK_A = h(ID_A, c_A)$, and with Bob by using Bob’s authentication key $AK_B = h(ID_B, c_B)$. The brief procedure is as follows:

1. Prerequisite. Alice and Bob register their secret identities and hash functions with Trent.
2. Trent generates a GHZ triplets sequence $|\psi\rangle = \{|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_N\rangle\}$, suppose

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{AB}, |111\rangle_{AB}), \quad (i = 1, 2, \cdots, N). \quad (5)$$

3. Trent makes unitary operations on $|\psi_i\rangle$ with Alice’s and Bob’s authentication keys $AK_A$ and $AK_B$. For example, if the $i$th value of $AK_A$ is 0, then Trent makes an identity operation $I$ on Alice’s particle (the first particle) of the $i$th GHZ state. If it is 1, a Hadamard operation $H$ is applied.
4. Trent distributes the first particle, the third particle of every GHZ triple to Alice and Bob, respectively, and keeps remaining particles for him.
5. Alice and Bob make reverse operations of step (3) on their qubits with their authentication keys $AK_A$ and $AK_B$, respectively.
6. Alice and Bob choose a subset of GHZ states for checking eavesdropper. If the error rate is higher than expected, then Alice and Bob resume the process. Otherwise, they can confirm that their counter parts are legitimate and the channel is secure, so they can continue the next phase, quantum direct communication process.

After the above-mentioned authentication process, the GHZ states are safely shared among the three parties, and two EQSDCPs will be put forward to transmit the secret message. We depict our EQSDCP 1 first.

In EQSDCP 1, the scenario is that Alice wants to send secret message to distant Bob, and there is a quantum channel between Alice and Bob. To achieve this task, Alice encodes the secret message on her particles and directly transmits them to Bob as follows:

1. Alice selects randomly some particles of the remaining GHZ states after authentication, and performs on them randomly one of the four operations $I, \sigma_x, i\sigma_y, \sigma_z$. The number of such particles is not big as long as it can provide an analysis of the error rate. Only Alice knows the positions of these sampling particles and she keeps them secret.
2. Alice encodes the secret message with an error correction code (ECC), such as the Hamming code, the Reed–Solomon code, the CSS (Calderbank–Shor–Steane) code, or BCH (Bose–Chaudhuri–Hochquenghem) code, so that Bob can correct errors after transmission.
3. Alice encodes the ECC-encoded message on the remaining particles after step (2) by performing the four unitary operations. According to our dense coding strategy, two bits correspond to a unitary operation: the bits 00 corresponds to the operation $I$, 01 to $\sigma_x$, 10 to $i\sigma_y$, and 11 to $\sigma_z$.

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad i\sigma_y = |0\rangle\langle -1| + |1\rangle\langle 0|. \quad (6)$$

Then the GHZ states are transformed into different forms as follows. (a) If the bits are 00, then

$$I_A|\varphi\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})$$

$$= \frac{1}{\sqrt{2}}(|\varphi^+\rangle_{AB} + \varphi^-\rangle_{AB})_T. \quad (7)$$

(b) If the bits are 01, then

$$\sigma_x A|\varphi\rangle = \frac{1}{\sqrt{2}}(|100\rangle_{ATB} + |011\rangle_{ATB})$$

$$= \frac{1}{\sqrt{2}}(|\psi^+\rangle_{AB} + |\psi^-\rangle_{AB})_T. \quad (8)$$

(c) If the bits are 10, then

$$i\sigma_y A|\varphi\rangle = \frac{1}{\sqrt{2}}(|011\rangle_{ATB} - |100\rangle_{ATB})$$

$$= \frac{1}{\sqrt{2}}(|\varphi^+\rangle_{AB} - |\varphi^-\rangle_{AB})_T. \quad (9)$$

(d) If the bits are 11, then

$$\sigma_z A|\varphi\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} - |111\rangle_{ATB})$$

$$= \frac{1}{\sqrt{2}}(|\varphi^+\rangle_{AB} - |\varphi^-\rangle_{AB})_T. \quad (10)$$

(4) After finishing all unitary operations, Alice sends all the qubits to Bob.
these decoded bits consist of the sampling particles’ announcement measurement operation

publication is necessary for us to prove that the EQSDCPs are parallel to the ZLY protocols when Trent is honest. Thus, proof was given in Ref. [25]. Our EQSDCPs are similar to Eve’s attacks when Trent is honest, and the security message.

(8) Alice tells Bob the position of the sampling pairs and the type of unitary operations on them. Then Bob check the sampling pairs that Alice had chosen, and he will obtain an estimate of error rate in the transmission.

(9) If the error rate is reasonably low, Alice and Bob can trust the process. Then Bob gets rid of the sample particles, and gets secret bits encoded with the corresponding ECC code. Otherwise, Alice and Bob abandon the transmission.

(10) Bob does error correction on the remaining bits, and finally gets the secret message from Alice.

In this message transmission process, even if Eve exists, but she at most get one particle from a GHZ state, and could not distinguish which operation Alice had performed, so she could not obtain any secret message.

Table 1. Corresponding relations of Alice’s operation, Bob’s measurement and Trent’s publication in EQSDCP 1.

| Trent’s announcement | Bob’s measurement | Alice’s operation |
|----------------------|------------------|------------------|
| $|+\rangle_T$        | $|0\rangle_B$    | $I(00)$          |
| $|+\rangle_T$        | $|\psi^+\rangle_{AB}$ | $\sigma_x(11)$ |
| $|+\rangle_T$        | $|\psi^-\rangle_{AB}$ | $\sigma_x(10)$ |
| $|+\rangle_T$        | $|\sigma_x\rangle_{AB}$ | $\sigma_x(11)$ |
| $|+\rangle_T$        | $|\sigma_y\rangle_{AB}$ | $I(00)$          |
| $|+\rangle_T$        | $|\sigma_z\rangle_{AB}$ | $\sigma_x(11)$ |

In EQSDCP 2, the scenario is that Alice wants to send secret message to distant Bob, but there is not any quantum channel between Alice and Bob. To achieve this task, Alice encodes the message on her particles and transmits them to Trent, instead of Bob. Thus Trent is acting as the message transfer centre.

The detailed procedure is similar to EQSDCP 1, except that Alice transmits her particles to Trent in step (4), Bob makes $x$ basis measurement in step (5), and Trent performs Bell measurement in step (6). Finally, Bob can infer the secret message according to Trent’s measurement and his measurement (see Table 2).

As we know, ZLY protocols are secure against Eve’s attacks when Trent is honest, and the security proof was given in Ref. [25]. Our EQSDCPs are similar to the ZLY protocols when Trent is honest. Thus, it is necessary for us to prove that the EQSDCPs are secure against ZLY’s Trent attacks when Trent is dishonest.

Table 2. Corresponding relations of Alice’s operation, Bob’s measurement and Trent’s announcement in EQSDCP 2.

| Trent’s announcement | Bob’s measurement | Alice’s operation |
|----------------------|------------------|------------------|
| $|\phi^+\rangle_T$   | $|+\rangle_B$    | $I(00)$          |
| $|\phi^+\rangle_T$   | $|\psi^+\rangle_{AB}$ | $\sigma_x(01)$ |
| $|\phi^+\rangle_T$   | $|\psi^-\rangle_{AB}$ | $\sigma_x(01)$ |
| $|\phi^+\rangle_T$   | $|\psi^+\rangle_{AB}$ | $I(00)$          |
| $|\phi^+\rangle_T$   | $|\sigma_x\rangle_{AB}$ | $\sigma_x(01)$ |
| $|\phi^+\rangle_T$   | $|\sigma_y\rangle_{AB}$ | $I(00)$          |

Let us start with the first ZLY’s Trent attack to the first protocol, which is an intercept-resent attack. The procedure can be depicted as follows. First, Trent intercepts the qubits that Alice attempts to transmit to Bob, and performs the $H$ operation on each qubit. Then Trent measures Alice’s and his qubit in the $z$ basis $\{0\}, \{1\}$ separately. If the two outcomes are the same, Trent can deduce that Alice had performed an $H$ operation corresponding to the bit 0. Otherwise, Alice has performed an $HX$ operation corresponding to the bit 1. Hence, Trent will obtain Alice’s whole bits string including both the random bits string and the secret message. Finally Trent removes the random bits according to Alice’s publication in step (8), and completely know the secret message.

According to this attack strategy, Trent intercepts Alice’s particle, and respectively performs his qubit and Alice’s qubit in the same basis $\{0\}, \{1\}$ respectively. If the outcomes are the same, the possible operation is $I_A$ or $\sigma_x A$ (see Eqs. (7) and (10)). If the outcomes are different, the possible operation is $\sigma_x A$ or $\sigma_y A$ (see Eqs. (8) and (9)).

Even if Trent performs the $H$ operation before singlet measurement, and the states are transformed into

$$H_A\sigma_x A|\varphi\rangle = \frac{1}{\sqrt{2}} H_A(|000\rangle_{ATB} + |111\rangle_{ATB})$$

$$= \frac{1}{2}(|000\rangle_{ATB} + |100\rangle_{ATB}$$

$$+ |011\rangle_{ATB} - |111\rangle_{ATB}),$$

(11)

$$H_A\sigma_s A|\varphi\rangle = \frac{1}{\sqrt{2}} H_A(|100\rangle_{ATB} + |011\rangle_{ATB})$$

$$= \frac{1}{2}(|000\rangle_{ATB} - |100\rangle_{ATB}$$

$$+ |011\rangle_{ATB} + |111\rangle_{ATB}),$$

(12)

$$H_A\sigma_z A|\psi\rangle = \frac{1}{\sqrt{2}} H_A(|011\rangle_{ATB} - |100\rangle_{ATB})$$

$$= \frac{1}{2}(|011\rangle_{ATB} + |111\rangle_{ATB}$$

$$- |000\rangle_{ATB} + |100\rangle_{ATB}),$$

(13)

$$H_A\sigma_z A|\psi\rangle = \frac{1}{\sqrt{2}} H_A(|000\rangle_{ATB} - |111\rangle_{ATB})$$
As shown above, Trent is still unable to differentiate which operation has been performed by comparing the outcomes of Alice’s and Trent’s measurement. This means Trent cannot infer Alice’s secret message, so our revised EQSDCP is secure against ZLW’s Trent attack.

The second ZLW’s Trent attack to the protocol 2 can be described as follows. Trent performs an $H$ operation on each qubit he received from Alice, and then respectively measures his qubit and Alice’s qubit in the $z$ basis to extract the secret message. According to Eqs. (7)–(10) and Eqs. (11)–(13), Trent cannot obtain the secret message whether the $H$ operation is performed or not. In short, our second EQSDCP is secure against ZLW’s Trent attack too.

Table 3. Relations of Alice’s operation, Bob’s operation, Trent’s publication, and Charlie’s measurement in the first EQSDCP.

| Trent’s publication | Charlie’s operation | Alice’s operation | Bob’s operation |
|---------------------|---------------------|------------------|----------------|
| $I_T$               | $I^+_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $S^+_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $P^+_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $P^-_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $S^-_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $S^+_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $Q^+_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $Q^-_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $R^+_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $R^-_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $Q^+_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $Q^-_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $R^+_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $R^-_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $Q^+_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $Q^-_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |
| $z_A$               | $R^+_A B C$         | $I_A(00)$        | $I_B(0)$       |
| $z_A$               | $R^-_A B C$         | $\sigma_{z_A}(11)$ | $I_B(0)$       |

In addition, our protocols can be generalized to multiparty quantum direction communication. A simple example is the three-party efficient QSDC protocols (3EQSDCPs) by using four particles GHZ state. Suppose that the four-particle GHZ is

$$|\varphi\rangle_4 = \frac{1}{\sqrt{2}}(|0000\rangle_{ABC} + |1111\rangle_{ABC})$$

$$= \frac{1}{\sqrt{2}}(|P^+_A B C|+\rangle_T + |P^-_A B C|-\rangle_T).$$

(15)

The scenario is that two spatially separated parties Alice and Bob want to send messages to distant Charlie. First, Trent distributes three particles of four-particle GHZ state to Alice, Bob and Charlie separately by utilizing the authentication process. Similarly, we can design two 3EQSDCPs. In the first 3EQSDCP, Alice encodes her message with $I_A(00)$, $\sigma_{z_A}(01)$, $\sigma_{z_A}(10)$, $\sigma_{z_A}(11)$, Bob encodes his message with $I_B(0)$, $\sigma_{z_B}(1)$, then Alice and Bob simultaneously send their particles to Charlie. After Charlie’s GHZ measurement and Trent’s $x$ measurement, Charlie will obtain the secret messages from Alice and Bob according to Table 3.

In the second 3EQSDCP, Alice and Bob simultaneously transmit their particles to Trent respectively after message encoding, and Charlie can extract the secret messages from Alice and Bob, respectively (see Table 4).

Table 4. Relations of Alice’s operation, Bob’s operation, Trent’s announcement, and Charlie’s measurement in the second 3EQSDCP.

| Trent’s announcement | Charlie’s operation | Alice’s operation | Bob’s operation |
|---------------------|---------------------|------------------|----------------|
| $|P^+_A B C\rangle$ | $|+\rangle_C$ | $I_A(00)$ | $I_B(0)$ |
| $|P^-_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(11)$ | $I_B(0)$ |
| $|S^+_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(01)$ | $I_B(0)$ |
| $|S^-_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(10)$ | $I_B(0)$ |
| $|P^+_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(11)$ | $I_B(0)$ |
| $|P^-_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(01)$ | $I_B(0)$ |
| $|S^+_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(10)$ | $I_B(0)$ |
| $|S^-_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(01)$ | $I_B(0)$ |
| $|R^+_A B C\rangle$ | $|+\rangle_C$ | $I_A(00)$ | $I_B(0)$ |
| $|R^-_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(11)$ | $I_B(0)$ |
| $|R^+_A B C\rangle$ | $|+\rangle_C$ | $I_A(00)$ | $I_B(0)$ |
| $|R^-_A B C\rangle$ | $|+\rangle_C$ | $\sigma_{z_A}(11)$ | $I_B(0)$ |

In summary, we have presented two revised efficient protocols, which are more efficient than Ref. [25] and secure against ZLW’s Trent attacks. Finally, we generalize them to multiparty quantum secure direction communication.

References

[1] Wiesner S 1983 *Signet News* **15** 78
[2] Bennett C H, Brassard G, Breidhart S and Wiesner S 1982 Advances in Cryptology: Proceedings of Crypto ’82 26
[3] Bennett C H and Brassard G 1984 in *Proc. IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE) pp 175–179
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[6] Bruk D 1998 *Phys. Rev. Lett.* **81** 3108
[7] Meyers D 1998 e-print quant-ph/9809025
[8] Lo H K and Chau H F 1999 *Science* **283** 2050
[9] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[10] Beige A et al 2002 *Acta Phys. Pol.* A **101** 357
[11] Bosström K et al 2002 *Phys. Rev. Lett.* **89** 187902
[12] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 108901
[13] Cai Q Y, Li B W 2004 *Phys. Rev.* A **69** 054301
[14] Deng F G et al 2003 *Phys. Rev.* A **68** 042317
[15] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento* B **119** 313
[16] Deng F G, Long G L 2004 *Phys. Rev.* A **69** 052319
[17] Gao T et al 2005 *J. Phys. A: Math. Gen.* **38** 5761
[18] Wang C et al 2005 *Opt. Commun.* **253** 15
[19] Wang J et al 2006 *Phys. Lett.* A **358** 256
[20] Cai Q Y, Li B W 2004 *Chin. Phys. Lett.* **21** 601
[21] Cai Q Y 2006 *Phys. Lett.* A **351** 23
[22] Wang C et al 2005 *Phys. Rev.* A **71** 044305
[23] Long G L et al 2007 *Front. Phys.* **2** 251
[24] Schneier B 1994 *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (New York: Wiley)
[25] Lee H, Lim J and Yang H 2006 *Phys. Rev.* A **73** 042305
[26] Zhang Z J et al 2007 *Phys. Rev.* A **75** 026301