Eavesdropping on the quantum dialogue protocol in lossy channel*

Liu Heng(刘 恒)[a)†], Zhang Xiu-Lan(张秀兰)[b)], and Lü Hui(吕 辉)[a)]

[a)] *Department of Mathematics and Computer Science, Huainan Normal University, Huainan* 232038, *China*

[b)] *Department of Physics and Electronic Information, Huainan Normal University, Huainan* 232038, *China*

(Received 10 February 2011; revised manuscript received 7 March 2011)

We present an improved eavesdropping scheme on the quantum dialogue protocol in lossy channel, which is based on the strategies of Wójcik [*Phys. Rev. Lett.* **90** 157901 (2003)] and ZML [*Phys. Lett.* A **333** 46 (2004)] attack schemes. We show that our attack scheme doubles the domain of Eve's eavesdropping and Eve can gain more information of the communication with less risk of being detected. Finally, a possible improvement for the dialogue protocol security is proposed.

Keywords: quantum dialogue, eavesdropper, transmission efficiency

PACS: 03.67.Hk **DOI:** 10.1088/1674-1056/20/7/070305

1. Introduction

Communication security with quantum key distribution (QKD) has been one of the important features of quantum information theory. After the pioneering work by Bennett and Brassard published in 1984,[1] a variety of quantum secret communication protocols have been proposed.[2−6] Recently, attention has been paid to new kinds of quantum cryptographic protocols called quantum secure direct communication (QSDC).[7−17] Different from the QKDs, the QSDC transmits the secret message directly without establishing any shared secret key. So it is more demanding for the security than the QKDs. The ping–pong protocol[9] presented by Boström and Felbinger is famous among the various QSDC schemes. However, the ping–pong protocol can be attacked without eavesdropping, i.e., it is insecure against a disturbance attack.[18,19] Very recently, based on the ping–pong protocol, a novel bidirectional QSDC protocol (namely quantum dialogue protocol) is proposed by Nguyen.[20] It is claimed that two users can effectively exchange their secret messages simultaneously. Although the quantum dialogue protocol has been proved secure against an entangle-measure attack and a disturbance attack,[20,21] it unfortunately turns out to be vulnerable to an intercept-and-resend attack.[22] The quantum efficiency claimed in quantum dialogue protocol is not achievable.[23] Subsequently, Nguyen[24] has improved the dialogue protocol to guarantee its security against the intercept-and-resend attack by combining two types of control modes.

The criterion for practical and secure protocol was specified by Brassard, Lütken-haus, Mor and Sanders:[25] "In order to be practical and secure, a quantum key distribution scheme must be based on existing or nearly existing technology, but its security must be guaranteed against an eavesdropper with unlimited computing power whose technology is limited only by the laws of quantum mechanics." Therefore, it is very necessary and essential to consider the security of communication protocols under practical conditions. Along this line, for analyzing the security of the ping–pong protocol in practical channels, Wójcik[26] has presented an eavesdropping scheme, in which Eve can hide in the channel losses and eavesdrop on information of communication without being detected if she replaces the original lossy channel with a better one. Subsequently, Zhang, Man and Li improved Wójcik's attack scheme and proved that Eve can attack all the transmitted bits in a larger domain of quantum channel transmission efficiency (namely ZML scheme).[27]

*Project supported by the Natural Science Foundation of the Anhui Higher Education Institutions of China (Grant No. KJ2011Z359).

†Corresponding author. E-mail: bmunichen@sina.com

© 2011 Chinese Physical Society and IOP Publishing Ltd

In this paper, we consider the security of the quantum dialogue protocol in the case with quantum channel losses. First, we point out a misuse of the original Wójcik attack scheme, which has been adopted to prove the security of the quantum dialogue protocol with lossy channels in Ref. [24]. Secondly, an improved attack scheme based on the ideas of Wójcik and ZML attack schemes is proposed. We show that in this improved scheme Eve can gain more information of the communication with less risk of being detected. Finally, a possible improvement for the dialogue protocol security is proposed.

2. The improved eavesdropping scheme

Let us start with a brief description of the improved quantum dialogue protocol.[24] Suppose there are two legitimate users (Alice and Bob) and they want to simultaneously transmit their messages to each other. Bob first prepares a large enough number of Einstein–Podolsky–Rosen (EPR) pairs all in the state $|\Psi_{00}\rangle_{\rm ht} = (|01\rangle_{\rm ht} + |10\rangle_{\rm ht})/\sqrt{2}$, where h stands for "home", t stands for "travel" and $\{|0\rangle\ , |1\rangle\}$ characterize the two degree freedom of a qubit. He encodes his bits (k_n,l_n) ($k_n, l_n \in \{0,1\}$) by applying an unitary operation C_{k_n,l_n} on the state $|\Psi_{00}\rangle_{\rm ht}$, where $C^{\rm t}_{0,0}$, $C^{\rm t}_{0,1}$, $C^{\rm t}_{1,0}$ and $C^{\rm t}_{1,1}$ denote the Pauli matrices $I^{\rm t}$, $\sigma^{\rm t}_x$, $\sigma^{\rm t}_z$ and $\mathrm{i}\sigma^{\rm t}_y$, respectively. It can be obtained that $|\Psi_{k,l}\rangle_{\rm ht} = C^{\rm t}_{k,l}|\Psi_{00}\rangle_{\rm ht}$, where the four Bell states are:

$$\begin{aligned}
|\Psi_{00}\rangle_{\rm ht} &= (|01\rangle_{\rm ht} + |10\rangle_{\rm ht})/\sqrt{2},\\
|\Psi_{01}\rangle_{\rm ht} &= (|00\rangle_{\rm ht} + |11\rangle_{\rm ht})/\sqrt{2},\\
|\Psi_{10}\rangle_{\rm ht} &= (|01\rangle_{\rm ht} - |10\rangle_{\rm ht})/\sqrt{2},\\
|\Psi_{11}\rangle_{\rm ht} &= (|00\rangle_{\rm ht} - |11\rangle_{\rm ht})/\sqrt{2}. \qquad (1)
\end{aligned}$$

Then Bob keeps one qubit (home qubit) with him and sends the other (travel qubit) to Alice.

Alice confirms to Bob that she has received the qubit and then decides to switch either to a control mode of type 1 (CM1) or to a message mode (MM). She informs Bob of her decision. In CM1, Alice measures the travel qubit in the basis $B_z = \{|0\rangle, |1\rangle\}$, Bob measures the home qubit in the same basis B_z and then they compare their own results with each other and find out whether Eve is on line. In MM, Alice encodes her bits (i_n, j_n) (i_n, $j_n \in \{0,1\}$) by performing either of the four operations C_{i_n,j_n} on the travel qubit and sends it back to Bob. Bob receives the encoded travel qubit, performs the Bell measurement on the qubit pair to obtain the result $|\Psi_{x_n,y_n}\rangle_{\rm ht}$ and decodes Alice's bits as ($i_n = x_n \oplus k_n, j_n = y_n \oplus l_n$). Then Bob decides to switch either to a control mode of type 2 (CM2) or to a message mode (MM). In CM2, Bob asks Alice to send him her (i_n, j_n) and checks the security of their dialogue. If both ($i_n = x_n \oplus k_n$) and ($j_n = y_n \oplus l_n$) hold, the process continues, otherwise aborts. In MM, Bob publicly announces his Bell measurement results (x_n, y_n), so Alice can decode Bob's bits as ($k_n = x_n \oplus i_n$, $l_n = y_n \oplus j_n$).

When practical lossy channel is considered, in the Wójcik and ZML attack schemes, Eve can replace the original lossy channel with a better one and then eavesdrop on the ping–pong protocol about encoding operations with a two-component xy auxiliary system.[26,27] Apparently, the original scheme by Wójcik is especially designed for the ping–pong protocol, where Alice applies one out of the two encoding operations ($I^{\rm t}$ or $\sigma^{\rm t}_z$). The Wójcik's explicit scheme involves the measurement of the polarization of the y-photon, yielding 1 bit information. We notice that these procedures have been mechanically misused in the quantum dialogue protocol to prove the security of the communication in the case of lossy channel.[24] In the dialogue protocol, the sender performs one of the four operations ($I^{\rm t}$, $\sigma^{\rm t}_x$, $\sigma^{\rm t}_z$ and $\mathrm{i}\sigma^{\rm t}_y$) to transmit two classical bits to the receiver, while in the ping–pong protocol only one classical bit has been transmitted in every message.[9] In other words, the capacity of the quantum dialogue protocol is double that of the ping–pong protocol,[28] therefore by only eavesdropping the result ($|0\rangle$ or $|1\rangle$) of the measurement on the polarization of the y-photon, it is difficult for Eve to distinguish the unitary operations performed by Alice in the dialogue protocol. So, those original attack schemes, if not modified, would not effectively work on the quantum dialogue protocol. And Eve not only can not gain enough information about the four encoding operations, but also has to be at the risk of being detected with very high probability 5/8.[24]

Now along the strategies of Wójcik and ZML attack schemes, we present an improved eavesdropping scheme. The lossy quantum channel is described by a single photon transmission efficiency. Obviously, Eve has no access to the home photon but can manipulate the travel photon when it goes from Bob to Alice and back from Alice to Bob. Different from Wójcik and ZML attack schemes, our eavesdropping scheme (outlined in Fig. 1) starts with preparing three auxil-

iary spatial modes (x, y, z) in the state $|\mathrm{vac}\rangle_\mathrm{x}|0\rangle_\mathrm{y}|0\rangle_\mathrm{z}$, where $|\mathrm{vac}\rangle$ denotes the empty mode. The state of the whole system thus is $|\mathrm{initial}\rangle = |\Psi_{00}\rangle_\mathrm{ht}|\mathrm{vac}\rangle_\mathrm{x}|0\rangle_\mathrm{y}|0\rangle_\mathrm{z}$.

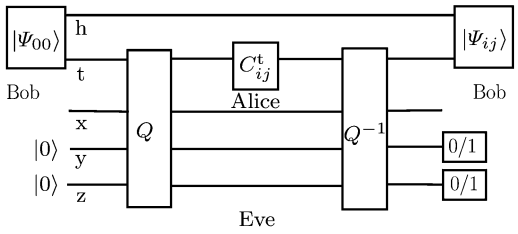


Fig. 1. Eavesdropping on the quantum dialogue protocol.

Same as Wójcik and ZML attack schemes, Eve attacks the quantum channel twice, the first time during the transmission from Bob to Alice (B–A attack) and the second time during the transmission from Alice to Bob (A–B attack). When Bob performs his operation (say $C^\mathrm{t}_{k,l} = I$, the other three operations have similar results) on the travel qubit and sends the travel photon to Alice, Eve attacks the quantum channel by manipulating the travel photon through the following unitary operation,

$$Q = U_\mathrm{xtz}N_\mathrm{xz}T_\mathrm{txy},$$

where $T = N_\mathrm{xy}C_\mathrm{ytx}N_\mathrm{ty}C_\mathrm{txy}H_\mathrm{y}$ is the same as that defined in the ZML scheme,[27] $U_\mathrm{xtz} = N_\mathrm{xt}N_\mathrm{tz}N_\mathrm{xt}$ is constructed by three symmetrical CNot gates (presented in Fig. 2), N represents the CNot gate, H is the Hadamard gate and C stands for the so-called three-mode controlled polarizing beam splitter (CPBS) gate, which is constructed by four CNot gates and a polarizing beam splitter transmitting (reflecting) photons in the state $|0\rangle(|1\rangle)$.

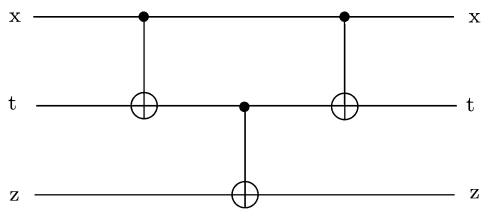


Fig. 2. The quantum logic gate U is constructed by three symmetrical CNot gates.

When acting on the initial state, the B–A attack transforms the whole system to the state $|\mathrm{B}-\mathrm{A}\rangle = Q|\mathrm{initial}\rangle$ of the form

$$\begin{aligned}&|\mathrm{B}-\mathrm{A}\rangle\\ &= \frac{1}{2}|0\rangle_\mathrm{h}(|\mathrm{vac}\rangle_\mathrm{t}|1\rangle_\mathrm{x}|0\rangle_\mathrm{y}|0\rangle_\mathrm{z} + |1\rangle_\mathrm{t}|1\rangle_\mathrm{x}|\mathrm{vac}\rangle_\mathrm{y}|0\rangle_\mathrm{z})\\ &\quad + \frac{1}{2}|1\rangle_\mathrm{h}(|0\rangle_\mathrm{t}|\mathrm{vac}\rangle_\mathrm{x}|1\rangle_\mathrm{y}|0\rangle_\mathrm{z} + |0\rangle_\mathrm{t}|0\rangle_\mathrm{x}|\mathrm{vac}\rangle_\mathrm{y}|0\rangle_\mathrm{z}).\end{aligned} \tag{2}$$

The state is almost the same as that obtained in the ZML scheme[27] except for an additional ancilla $|0\rangle_\mathrm{z}$. Suppose now that Alice switches to the CM1 and measures the state of the mode t, Eq. (2) tells us that after the B–A attack Alice will detect no photon with the probability of 1/4 and a photon, whose state is perfectly anticorrelated with the state of the home photon, with the probability of 3/4. Therefore, the probability of eavesdropping detection based on the correlation observation equals zero if the transmission efficiency of the quantum channel is not taken into account. This point is completely the same as that in the ZML scheme.[27] One can see that 25% channel loss is induced by the eavesdropping after the B–A attack.

Let us now analyse the performance of the scheme in the case of Alice operating in the message mode. After Alice performs an operation C_{i_n,j_n}, an A–B attack takes place. The A–B attack consists of an Q^{-1} operation. After the attack, the state of the system $|\mathrm{A}-\mathrm{B}\rangle = Q^{-1}C_{i,j}|\mathrm{B}-\mathrm{A}\rangle$ depends on the encoding operation performed by Alice. The final step of the eavesdropping scheme is a measurement of the polarization of y and z photons.

If Alice performs $C_{i,j} = C_{0,0}$ operation, then

$$\begin{aligned}|\mathrm{A}-\mathrm{B}\rangle_{00} &= \frac{1}{\sqrt{2}}\left(|01\rangle_\mathrm{ht} + |10\rangle_\mathrm{ht}\right)|0\rangle_\mathrm{y}|0\rangle_\mathrm{z}|\mathrm{vac}\rangle_\mathrm{x}\\ &= |\Psi_{00}\rangle_\mathrm{ht}|00\rangle_\mathrm{yz}|\mathrm{vac}\rangle_\mathrm{x}.\end{aligned} \tag{3}$$

Obviously, if Bob switches to CM2, he can gain Alice's information $(i,j=0,0)$ through a measurement on travel and home photons (result $|\Psi_{00}\rangle$). However, the information is also certainly known to Eve through a measurement on both y and z photons (result $|00\rangle_\mathrm{yz}$). In this case, Eve can gain Alice's information without being detected (eavesdropping probability $p_{00} = 1$). And the probability of eavesdropping detection is $d_{00} = 0$.

If Alice performs $C_{i,j} = C_{1,0}$ operation, then

$$\begin{aligned}|\mathrm{A}-\mathrm{B}\rangle_{10} &= \frac{1}{\sqrt{2}}(|01\rangle_\mathrm{ht}|1\rangle_y|0\rangle_\mathrm{z}|\mathrm{vac}\rangle_\mathrm{x}\\ &\quad + |10\rangle_\mathrm{ht}|0\rangle_y|0\rangle_\mathrm{z}|\mathrm{vac}\rangle_\mathrm{x})\\ &= \frac{1}{2}\Big[(|\Psi_{00}\rangle_\mathrm{ht} + |\Psi_{10}\rangle_\mathrm{ht})|10\rangle_\mathrm{yz}\\ &\quad + (|\Psi_{00}\rangle_\mathrm{ht} - |\Psi_{10}\rangle_\mathrm{ht})|00\rangle_\mathrm{yz}\Big]|\mathrm{vac}\rangle_\mathrm{x}.\end{aligned} \tag{4}$$

After a similar analysis as above, based on Eq. (4) Eve has a probability of $p_{10} = 1/4$ to gain Alice's information $(i,j = 1,0)$ without being detected, while the probability of eavesdropping detection is $d_{10} = 1/2$.

If Alice performs $C_{i,j} = C_{0,1}$ operation, then

$$\begin{aligned}
&|\mathrm{A}-\mathrm{B}\rangle_{01}\\
&=\frac{1}{2\sqrt{2}}\Big[|01\rangle_{\mathrm{ht}}(|00\rangle_{\mathrm{yz}}+|10\rangle_{\mathrm{yz}})+|00\rangle_{\mathrm{ht}}(|01\rangle_{\mathrm{yz}}\\
&\quad+|11\rangle_{\mathrm{yz}})+|11\rangle_{\mathrm{ht}}(|01\rangle_{\mathrm{yz}}-|11\rangle_{\mathrm{yz}})\Big]|\mathrm{vac}\rangle_{\mathrm{x}}\\
&\quad+\frac{1}{2\sqrt{2}}|1\mathrm{vac}\rangle_{\mathrm{ht}}(|101\rangle_{\mathrm{xyz}}-|111\rangle_{\mathrm{xyz}})\\
&=\Big[\frac{1}{4}(|\Psi_{00}\rangle_{\mathrm{ht}}+|\Psi_{10}\rangle_{\mathrm{ht}})(|00\rangle_{\mathrm{yz}}+|10\rangle_{\mathrm{yz}})\\
&\quad+\frac{1}{2}|\Psi_{01}\rangle_{\mathrm{ht}}|01\rangle_{\mathrm{yz}}+\frac{1}{2}|\Psi_{11}\rangle_{\mathrm{ht}}|11\rangle_{\mathrm{yz}}\Big]|\mathrm{vac}\rangle_{\mathrm{x}}\\
&\quad+\frac{1}{2\sqrt{2}}|1\mathrm{vac}\rangle_{\mathrm{ht}}(|101\rangle_{\mathrm{xyz}}-|111\rangle_{\mathrm{xyz}}). \qquad (5)
\end{aligned}$$

After the Bell measurement, obviously there is a probability of 1/4 that Bob finds $|1\mathrm{vac}\rangle_{\mathrm{ht}}$, whose origin could be due to the lossy quantum channel. According to Eq. (5), Eve has a probability of $p_{01} = 3/8$ to gain Alice's information $(i, j = 0, 1)$ without being detected, while the probability of eavesdropping detection is $d_{01} = 1/2$.

If Alice performs $C_{i,j} = C_{1,1}$ operation, then

$$\begin{aligned}
&|\mathrm{A}-\mathrm{B}\rangle_{11}\\
&=\frac{1}{2\sqrt{2}}\Big[|01\rangle_{\mathrm{ht}}(|00\rangle_{\mathrm{yz}}+|10\rangle_{\mathrm{yz}})-|00\rangle_{\mathrm{ht}}(|01\rangle_{\mathrm{yz}}\\
&\quad+|11\rangle_{\mathrm{yz}})+|11\rangle_{\mathrm{ht}}(|01\rangle_{\mathrm{yz}}-|11\rangle_{\mathrm{yz}})\Big]|\mathrm{vac}\rangle_{\mathrm{x}}\\
&\quad+\frac{1}{2\sqrt{2}}|1\mathrm{vac}\rangle_{\mathrm{ht}}(|101\rangle_{\mathrm{xyz}}-|111\rangle_{\mathrm{xyz}})\\
&=\Big[\frac{1}{4}(|\Psi_{00}\rangle_{\mathrm{ht}}+|\Psi_{10}\rangle_{\mathrm{ht}})(|00\rangle_{\mathrm{yz}}+|10\rangle_{\mathrm{yz}})\\
&\quad-\frac{1}{2}|\Psi_{11}\rangle_{\mathrm{ht}}|01\rangle_{\mathrm{yz}}-\frac{1}{2}|\Psi_{01}\rangle_{\mathrm{ht}}|11\rangle_{\mathrm{yz}}\Big]|\mathrm{vac}\rangle_{\mathrm{x}}\\
&\quad+\frac{1}{2\sqrt{2}}|1\mathrm{vac}\rangle_{\mathrm{ht}}(|101\rangle_{\mathrm{xyz}}-|111\rangle_{\mathrm{xyz}}). \qquad (6)
\end{aligned}$$

In the same way, the results $p_{11} = 3/8$ and $d_{11} = 1/2$ are obtained, which are the same as that of $C_{0,1}$ operation.

Accordingly, the average probability for Eve to obtain the information without being detected and that of being detected per CM2 run are

$$P = \sum_{i=0}^{1}\sum_{j=0}^{1} q_{ij}p_{ij},$$
$$D = \sum_{i=0}^{1}\sum_{j=0}^{1} q_{ij}d_{ij},$$

respectively, where q_{ij} is the probability of the appearance of i and j in Alice's message. If one assumes that $q_{ij} = 1/4, \forall i, j \in \{0, 1\}$, then

$$P = \frac{1}{4}\sum_{i=0}^{1}\sum_{j=0}^{1} p_{ij} = \frac{7}{16},$$
$$D = \frac{1}{4}\sum_{i=0}^{1}\sum_{j=0}^{1} d_{ij} = \frac{3}{8}. \qquad (7)$$

It can been seen that Eve in our scheme has a probability of 7/16 to gain Alice's information without being detected, while she can not obtain any information if the original Wójcik attack scheme was used.[24] Moreover, once Eve gains Alice's information, she can also get Bob's information through eavesdropping on the classical channel between Alice and Bob.[23] On the other hand, the average detection probability of eavesdropping decreases by 25% compared to Nguyen's results. Furthermore, Eqs. (5) and (6) tell us that A–B attack produces 12.5% eavesdropping-induced channel loss. Hence, the level of channel loss induced by the eavesdropping is 37.5% (25% in B–A attack and 12.5% in A–B attack), less than that (50%) mentioned in Ref. [24]. This implies less channel loss induced by the eavesdropping and the higher transmission efficiency of quantum channel, in which Eve can be hidden. In this way, Eve can gain more information of the communication with less risk of being detected.

For a potential eavesdropper, she needs to find out as much as possible about the encoding operations, which essentially is also the key of the communication. In our improved scheme, the domain of Eve's eavesdropping is double that of Wójcik and ZML attack schemes, i.e., it has been extended from only two operations to four operations. Moreover, suppose $q_{01} = q_{11} \approx 0$, one can see that our scheme has similar results with that of the ZML attack scheme.[27] So our scheme, as well as Wójcik and ZML attack schemes, can work on the ping–pong protocol. Assuming that in the quantum dialogue, the two parties have transmitted a large enough set of secret messages before they accomplish the security analysis such as CM2, the mutual information between Alice and Eve and between Alice and Bob can be calculated as

$$I_{\mathrm{AE}} = 2\frac{1}{4} - \frac{7}{16}\log 7 - \frac{3}{16}\log 3 \approx 0.725,$$
$$I_{\mathrm{AB}} = 2\frac{1}{8} - \frac{7}{16}\log 7 - \frac{3}{16}\log 3 \approx 0.6. \qquad (8)$$

One sees that the mutual information between Eve and Alice is greater than that between Bob and Alice. That is to say, some secret messages may have

been leaked to Eve in a practical channel, even Eve is detected by the users after a security analysis in CM2.

Let us now consider how to make the dialogue protocol more secure. In principle, we can not prevent the action of an eavesdropper, but we need to reduce the information leakage to a negligible small level.[29] Note that in the dialogue protocol there are three communication modes (CM1, CM2 and MM) depending on Alice's actual choice. When switching to the CM1, after Alice performs a measurement on the travel qubit in the basis B_z, she afterwards announces neither her chosen mode nor the result of the measurement, but continues to send the qubit to Bob like in the MM. That is to say, if Alice delays all the announcements about the chosen mode until Bob has received the travel qubit, Eve will not know the communication mode before she performs the A–B attack. As a result, it certainly leads to less information leakage and more traces of the A–B attack. Besides measuring the home photon's polarization, Bob can also check for any additional photon in the travel mode to detect the eavesdropper. Furthermore, Alice and Bob can also sacrifice some of their message bits to detect the eavesdropper.

3. Conclusion

In summary, we have pointed out the misuse of the original Wójcik attack scheme in the case of proving the security of the quantum dialogue protocol with a lossy channel. In this paper, based on the strategies of Wójcik and ZML attack schemes, an improved attack scheme working on the realistic implementation of the quantum dialogue protocol has been proposed. It has been proved that the domain of Eve's eavesdropping has been extended from only two encoding operations to four operations. Therefore, in the quantum dialogue protocol, Eve hidden in the lossy channel could gain more information about the communication with less risk of being detected compared to that in Ref. [24]. Finally, we also suggest a possible improvement for the dialogue protocol security.

Acknowledgement

The authors are very grateful to Yu Hai-Jun for the useful discussions.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings* Bangalore, India, p. 175
[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[3] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[5] Bruss D 1998 *Phys. Rev. Lett.* **81** 3018
[6] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[7] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357
[8] Mei F, Yu Y F and Zhang Z M 2010 *Chin. Phys.* B **19** 020308
[9] Boströem K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[10] Yang Y G, Wang Y H and Wen Q Y 2010 *Chin. Phy.* B **19** 070304
[11] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[12] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y and Deng F G 2006 *Chin. Phys. Lett.* **23** 1080
[13] Wang H S and Zeng G H 2008 *Chin. Phys.* B **92** 077902
[14] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[15] Lee H, Lim J and Yang H 2006 *Phys. Rev.* A **73** 042305
[16] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
[17] Zhan Y B 2005 *Chin. Phys.* **14** 1044
[18] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[19] Boströem K and Felbinger T *arXiv:quant-ph*/0708.2986
[20] Nguyen B A 2004 *Phys. Lett.* A **328** 6
[21] Jin X R, Ji X, Zhang Y Q, Zhang S, Hong S K, Yeon K H and Um C I 2006 *Phys. Lett.* A **354** 67
[22] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 22
[23] Tan Y G and Cai Q Y 2008 *Int. J. Quant. Inf.* **6** 325
[24] Nguyen B A 2005 *J. Kor. Phys. Soc.* **47** 562
[25] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[26] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[27] Zhang Z J, Man Z X and Li Y 2004 *Phys. Lett.* A **333** 46
[28] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301
[29] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Front. Phys. China* **2** 251