Improving the security of secure deterministic communication scheme based on quantum remote state preparation*

Qin Su-Juan(秦素娟)† and Wen Qiao-Yan(温巧燕)

State Key Laboratory for Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

(Received 27 August 2008; revised manuscript received 22 July 2009)

The security of the quantum secure deterministic communication scheme [*Chin. Phys.* **16** (2007) 2549] is reexamined. A security loophole is pointed out. Taking advantage of this loophole, an eavesdropper can steal all the secret messages without being detected by an intercept-and-resend attack strategy. Furthermore, a possible improvement on this protocol is presented. It makes the modified protocol secure against this kind of attack.

Keywords: quantum secure direct communication, cryptanalysis, quantum cryptography, security

PACC: 0367

Cryptography is the technique allowing some parties to communicate over an open channel in a secure way. Quantum cryptography is the combination of quantum mechanics and cryptography, in which the security is assured by physical principles. Since Bennett and Brassard proposed the original quantum key distribution (QKD) protocol in 1984,[1] many studies have focused on this topic. Recently, a new concept in quantum cryptography, quantum secure direct communication (QSDC), was proposed,[2] in which messages are permitted to be communicated directly without establishing random keys first to encrypt them. Boström and Felbinger presented a ping–pong QSDC protocol in 2002.[3] However it is shown to be insecure against the DoS attack[4] and in the lossy channel.[5] Subsequently, Deng *et al.* proposed four criteria for a secure QSDC and gave two secure QSDC protocols.[6,7] Besides, based on different quantum carriers, many QSDC protocols were presented.[8−13]

As is well known, the main aim of quantum cryptography is to solve the problems in classical cryptosystems. Therefore, high security is not only an advantage of quantum cryptography but also the crucial requirement for it. Nevertheless, not all the proposed protocols can meet this requirement. Quite a few protocols were successfully attacked by subtle strategies.[4,14−21] Therefore, as in its classical counterpart, finding loopholes in the protocols and improving them is also desirable in quantum cryptography.

Recently, Guo *et al.* proposed a novel QSDC protocol (GCZ protocol) based on quantum error correction codes (QECC),[22] where a sender can transmit the messages in an imperfect quantum channel and the damaged qubits of the received state can be recovered by the receiver. The authors thought that the security of this protocol could be guaranteed by the transmission of the non-orthogonal quantum states. However, here we find an intercept-and-resend attack strategy in which Eve is allowed to elicit the secret message without being detected.

Now we come to briefly describe the GCZ protocol first. Alice wants to transmit her k-qubit secret messages $|c\rangle$ to Bob. She first encodes her secret messages $|c\rangle$ into n-qubit state $|c\rangle_L$ by using the stabilized quantum code (SQC) and then transmits all the n qubits one by one to Bob according to the following steps. For convenience, we use the same notations as those in Ref. [22].

(i) Bob prepares a two-qubit state

$$|\phi_1(h,t)\rangle = \frac{1}{\sqrt{2}}(|0_h\rangle\,|0_t\rangle + |1_h\rangle\,|1_t\rangle), \qquad (1)$$

where two subscripts h and t refer to photons p_h and

*Project supported by the National Natural Science Foundation of China (Grant Nos. 60873191 and 60821001), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 200800131016), the Foundation for Key Program of Ministry of Education of China (Grant No. 109014), the Beijing Nova Program, China (Grant No. 2008B51), the China Post-Doctoral Science Foundation (Grant No. 20090450018), and the Natural Science Foundation of Beijing, China (Grant No. 4072020).

†Corresponding author. E-mail: qsujuan2003@163.com

© 2010 Chinese Physical Society and IOP Publishing Ltd

p_t in the entangled state, respectively. He performs I or H on p_t randomly and then sends p_t to Alice. Here $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $H = (1/\sqrt{2})(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$. After the operation, the state may be $|\phi_1(h,t)\rangle$ or $|\phi_2(h,t)\rangle$

$$|\phi_2(h,t)\rangle = \frac{1}{\sqrt{2}}(|0_h\rangle|+_t\rangle + |1_h\rangle|-_t\rangle). \quad (2)$$

(ii) Alice prepares a message qubit p_m in state $|\omega_{im}\rangle$. She entangles p_m with p_t by applying C_{tm} to them. Here C_{tm} denotes the controlled-NOT operation (CNOT) where p_t is the control qubit and p_m is the target qubit. As a result, the whole state will be converted into

$$\begin{aligned}|\Theta_1\rangle &= C_{tm}(|\phi_1(h,t)\rangle \otimes |\omega_{im}\rangle) \\ &= \frac{1}{\sqrt{2}}(|0_h\rangle|0_t\rangle|\omega_{im}\rangle + |1_h\rangle|1_t\rangle|\varpi_{im}\rangle), \quad (3)\end{aligned}$$

or

$$\begin{aligned}|\Theta_2\rangle &= C_{tm}(|\phi_2(h,t)\rangle \otimes |\omega_{im}\rangle) \\ &= \frac{1}{2}[|0_h\rangle(|0_t\rangle|\omega_{im}\rangle + |1_t\rangle|\varpi_{im}\rangle) \\ &\quad + |1_h\rangle(|0_t\rangle|\omega_{im}\rangle - |1_t\rangle|\varpi_{im}\rangle)]. \quad (4)\end{aligned}$$

Then Alice returns both photons, p_t and p_m, to Bob. Here $|\varpi_{im}\rangle = X|\omega_{im}\rangle$, and X is the bit flip operation.

(iii) When Bob receives both the photons, he performs some operations to check eavesdropping and obtain the secret message $|\omega_{im}\rangle$. Concretely, Bob performs the operations as follows:

$$|\Omega_1\rangle = C_{hm}(C_{mh}|\Theta_1\rangle) = |\omega_{ih}\rangle \otimes |\phi_1(t,m)\rangle, \quad (5)$$

or

$$|\Omega_2\rangle = C_{tm}(C_{mt}|\Theta_2\rangle) = |\omega_{it}\rangle \otimes |\phi_2(h,m)\rangle. \quad (6)$$

If $|\phi_1(t,m)\rangle = |\phi_1(h,t)\rangle$ or $|\phi_2(h,m)\rangle = |\phi_2(h,t)\rangle$, Bob thinks that the transmitted carrier state is perfect without being destroyed.

(iv) Alice and Bob perform the above steps for n runs to transmit her secret $|c\rangle_L$. Afterwards, Bob recovers the secret messages $|c\rangle$ from $|c\rangle_L$ by making use of the decoder of SQC.

The authors of Ref. [22] believed that the security of GCZ protocol was guaranteed by the non-orthogonality of transmitted photons and Eve could not obtain any useful information. However, a basic property of the CNOT operation was neglected, that is, one can disentangle the correlation between the control qubit and the target qubit by another CNOT operation. For example, if Eve has access to two photons, p_t and p_m, she can perform a CNOT operation to elicit the message $|\omega_{im}\rangle$.

Now we show how Eve utilizes this property to obtain the secret message. According to the basic assumption in cryptography, both the encoder and the decoder of SQC are public, that is, every one can know $|c\rangle$ once he obtains the message $|c\rangle_L$. Therefore, we need to discuss only how Eve can filch $|c\rangle_L$. Here we describe the attack strategy in detail.

(E1) Eve prepares k-qubit messages $|s\rangle$, which are used to replace the messages $|c\rangle$. She encodes them into n-qubit state $|s\rangle_L = |v_{1s}\rangle|v_{2s}\rangle\cdots|v_{ns}\rangle$ by using the encoder of SQC. Each photon in $|s\rangle_L$ is denoted as p_s.

(E2) For every run, when Alice sends the photons p_t and p_m out in step (ii), Eve intercepts and performs C_{tm} on them

$$C_{tm}|\Theta_1\rangle = |\phi_1(h,t)\rangle \otimes |\omega_{im}\rangle, \quad (7)$$

or

$$C_{tm}|\Theta_2\rangle = |\phi_2(h,t)\rangle \otimes |\omega_{im}\rangle. \quad (8)$$

Obviously, the message qubit p_m is disentangled from the carrier, and therefore, Eve can obtain the message $|\omega_{im}\rangle$. To avoid being detected, Eve needs to send a fake message qubit to Bob. She does the same operation on p_t and p_s as Alice, and then sends them to Bob.

It is easy to verify that Bob can obtain perfect carrier state without being destroyed in step (iii). Therefore, Bob cannot find Eve's eavesdropping in each run. After Eve has performed the step (E2) for n runs, she receives the state $|c\rangle_L$. Making use of the decoder of SQC, Eve can recover the secret messages $|c\rangle$. For Bob, he receives the state $|s\rangle_L$ and obtains the messages $|s\rangle$ instead of $|c\rangle$.

As shown above, by a CNOT operation Eve can obtain all the secret messages. At the same time, the carrier state holds unchanged, and hence no one can find her eavesdropping. Therefore, the GCZ protocol is insecure against this attack.

Now we consider how to improve the security of the GCZ protocol against this attack. It is worth while noticing that it may be insecure to transmit both the control qubit and the target qubit simultaneously according to the property of CNOT. In fact, it does not need to send the control qubit back to Bob in the GCZ protocol. According to the special property of Bell states, it is enough to recover the message only

by using p_h and p_m

$$C_{hm}\left|\Theta_1\right\rangle = \left|\phi_1(h,t)\right\rangle \otimes \left|\omega_{im}\right\rangle, \tag{9}$$

or

$$C_{hm}(H_h\left|\Theta_2\right\rangle) = \left|\phi_1(h,t)\right\rangle \otimes \left|\omega_{im}\right\rangle. \tag{10}$$

It can be seen from Eqs. (9) and (10) that Bob can disentangle the p_m with the carrier by some unitary operations on p_h and p_m. Therefore, to improve the security of the GCZ protocol, Alice can send only the qubit p_m to Bob after her CNOT operation.

However, it is still not enough to guarantee the security of the GCZ protocol after the above modification. Eve can also obtain the secret without being detected. For example, she prepares a fake Bell state and performs a man-in-the-middle attack by replacing p_t in step (i) with her fake photon in Bell state and disentangling the message photon after Alice has returned it. Actually, to design a secure QSDC protocol, there are some basic requirements.[7] First, eavesdropping detection should be executed before the secret message is encoded. In the GCZ protocol, there is no such process for ensuring that the carrier is transmitted safely. Therefore, we need to add an additional detecting process before the encoding operation performed by Alice in the GCZ protocol. Secondly, it is necessary to transmit a signal in a block manner since the security is assured by sampling a sufficiently large subset of instances from the first block. According to the two basic requirements, we modify the process of the GCZ protocol as follows.

(M1) Bob prepares $2n$ Bell states in the same state $|\phi_1(h,t)\rangle$. For each Bell state, he performs I or H on p_t randomly. Afterwards Bob sends all the p_t to Alice.

It is not difficult to find that the operation H is useless for the security since the transmitted qubit p_t is a maximal mixed state (its reduced density operator is $1/2$). Here, to retain the features of the original GCZ protocol, we will modify it as little as possible.

(M2) After Alice has received all the photons, she chooses n_1 ($n_1 < n$) photons from them and measures each of them in $\boldsymbol{Z}$ or $\boldsymbol{X}$ basis randomly. Then she publishes the positions and her measurement bases and outcomes. Bob measures the corresponding photons in $\boldsymbol{Z}$ or $\boldsymbol{X}$ basis according to her operations in (M1). Concretely, he measures the p_h in the same basis as that of Alice's measurement if he performs I in (M1), otherwise, he measures it in a different basis. If there exists no eavesdropper, their outcomes must satisfy the relations in Eqs. (11) and (12). Bob compares their outcomes and computes the error rate. If the error rate is lower than the threshold, the process continues

$$\begin{aligned}\left|\phi_1(h,t)\right\rangle &= \frac{1}{\sqrt{2}}(\left|0_h\right\rangle\left|0_t\right\rangle + \left|1_h\right\rangle\left|1_t\right\rangle) \\ &= \frac{1}{\sqrt{2}}(\left|+_h\right\rangle\left|+_t\right\rangle + \left|-_h\right\rangle\left|-_t\right\rangle), \end{aligned}\tag{11}$$

$$\begin{aligned}\left|\phi_2(h,t)\right\rangle &= \frac{1}{\sqrt{2}}(\left|0_h\right\rangle\left|+_t\right\rangle + \left|1_h\right\rangle\left|-_t\right\rangle) \\ &= \frac{1}{\sqrt{2}}(\left|+_h\right\rangle\left|0_t\right\rangle + \left|-_h\right\rangle\left|1_t\right\rangle). \end{aligned}\tag{12}$$

(M3) Alice prepares the message photons according to $|c\rangle_L$. To prevent a denial-of-service (DoS) attack, she inserts $n - n_1$ decoy photons into the sequence of message photons randomly (each decoy photon is in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$). After knowing that the carriers have been transmitted safely, Alice performs C_{tm} on each p_t and p_m, and then sends p_m to Bob.

(M4) When Bob receives all the photons, he performs C_{hm} or $C_{hm}H_h$ to obtain the messages (see Eqs. (9) and (10)). Afterwards, Alice announces the positions and states of the decoy photons. Bob measures them in the right basis and compares the outcomes with Alice's announcement. If the error rate is lower than a certain threshold, Bob recovers the secret messages $|c\rangle$ from the remainder of the photons by making use of the decoder of SQC.

Up to now, we have proposed a possible improvement on the GCZ protocol. The modified protocol is secure by transmitting photons in block manner and introducing decoy states to authenticate the messages. In this way, if an eavesdropper attempts to eavesdrop the secret messages, her eavesdropping behaviours will be detected in steps (M2) and (M4). Actually, the modified protocol is essentially similar to the quantum Vernam cipher with entanglement as the key.[23] So it is secure against the intercept-and-resend attack.

In summary, we analysed the security of the GCZ protocol[22] and pointed out that an eavesdropper could elicit all the secret messages by an intercept-and-resend attack without inducing any disturbance. Finally, we present a possible improvement on the GCZ protocol via checking eavesdroppers before the secret message is encoded and authenticating the message by using decoy states. With these modifications, the GCZ protocol is secure against the presented intercept-and-resend attack.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE Press) p. 175

[2] Beige A, Englert B G and Kurtsiefer H 2002 *Acta Phys. Pol.* A **101** 357

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

[4] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801

[5] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

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

[7] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[8] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301

[9] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501

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

[11] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

[12] Zhang X L, Zhang Y X and Wei H 2009 *Chin. Phys.* B **18** 435

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

[14] Qin S J, Gao F, Wen Q Y and Zhu F C 2007 *Phys. Rev.* A **76** 062324

[15] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[16] Qin S J , Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101

[17] Du J Z, Qin S J, Wen Q Y and Zhu F C 2006 *Phys. Rev.* A **74** 016301

[18] Gao F, Qin S J, Wen Q Y and Zhu F C 2007 *Quantum Inf. Comput.* **7** 329

[19] Gao F, Wen Q Y and Zhu F C 2008 *Chin. Phys.* B **17** 3189

[20] Qin S J, Wen Q Y and Zhu F C 2007 *J. Phys.* B: *At. Mol. Opt. Phys.* **40** 4661

[21] Wang T Y, Qin S J, Wen Q Y and Zhu F C 2008 *Acta Phys. Sin.* **57** 7452 (in Chinese)

[22] Guo Y, Chen Z G and Zeng G H 2007 *Chin. Phys.* **16** 2549

[23] Leung D W 2002 *Quantum Inf. Comput.* **2** 14