Information Leakage Problem in High-Capacity Quantum Secure Communication with Authentication Using Einstein–Podolsky–Rosen Pairs *

Zhi-Hao Liu(刘志昊)[1,2,3], Han-Wu Chen(陈汉武)[1,2**], Wen-Jie Liu(刘文杰)[4]

[1]*School of Computer Science and Engineering, Southeast University, Nanjing 211189*

[2]*Key Laboratory of Computer Network and Information Integration (Ministry of Education), Southeast University, Nanjing 211189*

[3]*Centre for Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*

[4]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044*

(Received 14 March 2016)

The information leakage problem often exists in bidirectional quantum secure direct communication or quantum dialogue. In this work, we find that this problem also exists in the one-way quantum secure communication protocol [Chin. Phys. Lett. 32 (2015) 050301]. Specifically, the first bit of every four-bit message block is leaked out without awareness. A way to improve the information leakage problem is given.

PACS: 03.67.Dd, 03.67.Hk DOI: 10.1088/0256-307X/33/7/070305

How to protect the privacy and to keep the security of communicated or stored data is of great importance especially in the cloud computing and cloud storage environment.[1–6] An efficient way to solve the problem is that the data are encrypted by a secret key. However, how to securely distribute this key is not easy for two remote users. Thus to simplify this, in classical cryptography, key distribution is based on the unproven computational complexity of hard mathematical problems. Differently, quantum cryptography[7] makes the cryptography build on physical principles. Thus a correctly designed quantum cryptography protocol has the unconditional security in theory. This attracts many researchers to throw themselves into the research of quantum cryptography.

However, numerous quantum cryptography protocols have some security problems. Many active attack strategies have been put forward, such as the intercept–resend attack,[8] the entanglement swapping attack,[9,10] the teleportation attack,[11] the dense coding attack,[12–14] the denial of service attack,[15] the correlation-extractability attack and its general case.[16–19]

There is another kind of security problem, called the information leakage problem in which anyone who gains the public information from the public classical channels can deduce some useful information. The information leakage problem often exists in bidirectional quantum secure direct communication (QSDC) or quantum dialogue (QD).[20–26]

Recently, Xiao *et al.*[27] put forward a really novel one-way quantum secure communication (QSC) protocol using EPR pairs and dense encoding. It was claimed that this protocol has a very high capacity as each EPR pair can carry four classical bits by the XOR operation and an auxiliary photon. Thus they thought that the major advantage of this protocol is its efficiency. However, if we consider more carefully, we can find that the first bit of every four-bit message block is actually leaked out without awareness. That is, only three bits are securely transmitted.

To describe the information leakage problem explicitly, we firstly describe the information transmission of this QSC protocol in brief. Since we are not concerned about the security against active attacks in this study, the security checking procedures are not discussed. The transmission of the ith four-bit message block will be taken as an example.

(1) The sender Alice prepares a Bell state $|\phi^+\rangle_{\rm AB}$, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then she sends particle B to the receiver Bob. (2) Alice and Bob check whether the particle B is securely transmitted. (3) According to the ith four-bit message block that Alice wants to send, Alice prepares an auxiliary particle P. Specifically, if the four-bit message block is 0000, 1011, 1101 or 0110, she will prepare $|0\rangle$; if the four-bit message block is 0101, 0011, 1000 or 1110, she will prepare $|1\rangle$; if the four-bit message block is 1010, 0001, 0111 or 1100, she will prepare $|+\rangle$; if the four-bit message block is 1111, 0100, 0010 or 1001, she will prepare $|-\rangle$ (please see Table 2 in Ref. [27]). At the same time, Alice uses a recording bit I_i to represent the basis information of particle P. If P is $|0\rangle$ or $|1\rangle$, I_i will be 0; otherwise I_i will be 1. Next, Alice performs unitary operation on particle A according to the ith four-bit message block. Specifically, if the four-bit message block is 0000, 1010, 0101 or 1111, she will perform U_{00} on A to transform the state $|\phi^+\rangle_{\rm AB}$ to $|\phi^+\rangle_{\rm AB}$, where $U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|$; if the four-bit message block is 0001, 0100, 1110 or 1011, she will perform U_{01} on A to transform the state $|\phi^+\rangle_{\rm AB}$ to $|\psi^+\rangle_{\rm AB}$,

*Supported by the National Natural Science Foundation of China under Grant Nos 61502101 and 61170321, the Natural Science Foundation of Jiangsu Province under Grant No BK20140651, and Funded by PAPD and CICAEET.

**Corresponding author. Email: hw_chen@seu.edu.cn

© 2016 Chinese Physical Society and IOP Publishing Ltd

where $U_{01} = |0\rangle\langle 1| + |1\rangle\langle 0|$; if the four-bit message block is 0010, 1000, 0111 or 1101, she will perform U_{10} on A to transform the state $|\phi^+\rangle_{\rm AB}$ to $|\psi^-\rangle_{\rm AB}$, where $U_{10} = |0\rangle\langle 1| - |1\rangle\langle 0|$; if the four-bit message block is 0011, 1100, 0110 or 1001, she will perform U_{11} on A to transform the state $|\phi^+\rangle_{\rm AB}$ to $|\phi^-\rangle_{\rm AB}$, where $U_{11} = |0\rangle\langle 0| - |1\rangle\langle 1|$ (please see Table 1 in Ref. [27]). Meanwhile, Alice obtains a bit h_i which is the XOR value of the four bits of the message block. Then she encrypts I_i by h_i to obtain I_i' ($I_i' = I_i \oplus h_i$). Afterward, Alice sends particles A and P to Bob. (4) Alice sends I_i' to Bob via a classical channel. (5) Bob makes the Bell-basis measurement on particles A and B and obtains h_i. Then he decrypts I_i and thus he measures particle P with the right basis. Finally, he can deduce Alice's four-bit message block.

Now we explain the reason why the information leakage problem exists in the original one-way QSC protocol. The only public information anyone (we say Eve hereafter) can obtain is I_i'. In step (4) of the original protocol,[27] Alice sends the classical bit I_i' to Bob via a classical channel, where $I_i' = I_i \oplus h_i$, and I_i represents the basis information of the auxiliary particle P; h_i denotes the XOR value of the four bits of the ith message block. Unfortunately, obtaining the bit I_i' Eve can infer some useful information.

(I) If $I_i' = 0$, Eve can immediately deduce that the four-bit message block Alice transmitted is one of the blocks 0000, 0001, 0010, 0011, 0100, 0101, 0110 or 0111. We will give the detailed reasons here. When $I_i' = 0$, we have $h_i = 0$, $I_i = 0$ or $h_i = 1$, $I_i = 1$. According to Tables 1 and 2 in Ref. [27], one can obtain that: if $h_i = 0$, $I_i = 0$, then the four-bit message block Alice transmitted will be 0000, 0101, 0110 or 0011; if $h_i = 1$, $I_i = 1$, then the four-bit message block Alice transmitted will be 0001, 0010, 0100 or 0111.

(II) If $I_i' = 1$, Eve can immediately deduce that the four-bit message block Alice transmitted is one of the blocks, i.e. 1000, 1001, 1010, 1011, 1100, 1101, 1110 or 1111.

Obviously, I_i' is equal to the first bit of the four-bit message block in either situation. That is, Eve can obtain the first bit of the four-bit message block.

In fact, the reason why the information leakage problem exists is the original one-way QSC protocol can be expressed in another way. Assume that the four-bit message block is denoted as $b_1b_2b_3b_4$. If carefully considering according to Table 2 in Ref. [27], one can find that $I_i = b_2 \oplus b_3 \oplus b_4$. In addition, it has been known that $h_i = b_1 \oplus b_2 \oplus b_3 \oplus b_4$. Thus we have $I_i' = I_i \oplus h_i = b_1$. It shows that, obtaining the public bit I_i' Eve in fact can obtain the first bit of the four-bit message block.

Of course, we can calculate the information quantity $I_{\rm E}$ that Eve can obtain from I_i' from the viewpoint of information theory. We have $I_{\rm E} = H(b_1b_2b_3b_4) + H(b_1b_2b_3b_4|I_i') = 4 + \frac{1}{8}\log\frac{1}{8} = 1$. That is, Eve obtains one bit of the four-bit message block. This is not allowed in a true QSC protocol.

Actually, only three quantum photons (an EPR pair and an auxiliary photon) are transmitted, thus at most three classical bits can be transmitted securely. As a result, if we want to improve this QSC protocol to a secure one, three bits at most can be transmitted. To change the original QSC protocol as little as possible, a possible way is that the first bit of each four-bit message block is not really used to transmit the secret message but only used as a redundant bit to assist in checking the security of the quantum channel. Thus Eve can still obtain the first bit of the four-bit block, but this bit is not the message bit anymore and will be discarded after communication.

In summary, the information leakage problem existing in the one-way QSC protocol proposed by Xiao *et al.*[27] has been pointed out. Then a way to improve it is put forward. Actually, the information leakage problem widely exists in QSC protocols but unfortunately little attention was paid to it. We hope that researchers could take deeper consideration to design true secure quantum communication protocols.

References

[1] Xie S and Wang Y 2014 *Wireless Personal Commun.* **78** 231
[2] Fu Z, Ren K, Shu J, Sun X and Huang F 2015 *IEEE Trans. Parallel & Distrib. Syst.* (in press)
[3] Fu Z, Sun X, Liu Q, Zhou L and Shu J 2015 *IEICE Trans. Commun.* **E98B** 190
[4] Ma T, Zhou J, Tang M, Tian Y, Al-Dhelaan A, Al-Rodhaan M and Lee S 2015 *IEICE Trans. Inf. Syst.* **E98D** 902
[5] Ren Y, Shen J, Wang J, Han J and Lee S 2015 *J. Internet Technol.* **16** 317
[6] Xia Z, Wang X, Sun X and Wang Q 2016 *IEEE Trans. Parallel & Distrib. Syst.* **27** 340
[7] Gisin N, Ribordy G G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[8] Liu Z H, Chen H W, Wang D and Li W Q 2014 *Quantum Inf. Process.* **13** 1345
[9] Zhang Y S, Li C F and Guo G C 2001 *Phys. Rev.* A **63** 036301
[10] Gao F, Qin S J and Wen Q Y 2007 *Quantum Inf. Comput.* **7** 329
[11] Gao F, Wen Q Y and Zhu F C 2008 *Chin. Phys.* B **17** 3189
[12] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101
[13] Hao L, Li J and Long G 2010 *Sci. Chin.: Phys. Mech. Astron.* **53** 491
[14] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *IEEE J. Quantum Electron.* **47** 630
[15] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[16] Gao F, Wen Q Y and Zhu F C 2007 *Phys. Lett.* A **360** 748
[17] Gao F, Qin S J, Wen Q Y and Zhu F C 2010 *Opt. Commun.* **283** 192
[18] Qin S J, Gao F, Guo F Z and Wen Q Y 2010 *Phys. Rev.* A **82** 036301
[19] Liu Z H, Chen H W, Liu W J, Xu J and Li Z Q 2011 *Int. J. Quantum Inf.* **9** 1329
[20] Gao F, Guo F Z, Wen Q Y and Zhu F C 2008 *Sci. Chin. G-Phys. Mech. Astron.* **51** 559
[21] Liu Z H and Chen H W 2013 *Chin. Phys. Lett.* **30** 079903
[22] Liu Z H and Chen H W 2013 *Chin. Phys. Lett.* **30** 079901
[23] Liu Z H, Chen H W, Liu W J and Xu J 2013 *Chin. Phys. Lett.* **30** 039901
[24] Gao G 2014 *Mod. Phys. Lett.* B **28** 1450094
[25] Ye T Y 2015 *Int. J. Theor. Phys.* **54** 1775
[26] Tan Y G and Cai Q Y 2008 *Int. J. Quantum Inf.* **6** 325
[27] Xiao M and Xu H W 2015 *Chin. Phys. Lett.* **32** 050301