Int J Theor Phys (2011) 50:2703–2707
DOI 10.1007/s10773-011-0768-0

Comment on "Quantum Key Distribution and Quantum Authentication Based on Entangled State"

Toung-Shang Wei · Chia-Wei Tsai · Tzonelih Hwang

Received: 27 September 2010 / Accepted: 16 March 2011 / Published online: 29 March 2011

Abstract Shi et al. (Phys. Lett. A 281:83–87, 2001) proposed a scheme which allows simultaneous realization of quantum key distribution and quantum authentication. However, this study points out a weakness in Shi et al.'s scheme, in which a malicious user can impersonate a legitimate participant without being detected. Furthermore, an improved scheme is proposed to avoid this weakness.

Keywords Quantum key distribution and quantum authentication

1 Introduction

Distributing a secure key between two remote participants is an important issue in cryptography. In 1984, Bennett and Brassard [1] used the property of quantum mechanics to establish the first quantum key distribution (QKD) protocol (also called BB84 protocol). After that, many QKD protocols [2–9] have been proposed. The security of these protocols heavily depends on the assumption that the classical channel is either unjammable or authenticated. In practice, however, the assumption of an unjammable or authenticated channel seems impractical. Therefore, how to assure authentication features in a QKD protocol becomes an important issue for design of QKD. Various quantum authentication (QA) protocols [10–20] thus have been proposed. Among these protocols, Shi et al. [13] used a pre-shared entangled state between two participants to propose a scheme in which QKD and QA can be simultaneously realized. The participants can authenticate each other and also distribute a secure key without classical channel. However, this study points out a weakness in Shi et al.'s scheme. While a malicious user performs an intercept-and-resend attack, he/she can impersonate a legitimate participant without being detected. This study also tries to enhance Shi et al.'s protocol to avoid this weakness.

T.-S. Wei · C.-W. Tsai · T. Hwang (✉)
Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan 70101, Taiwan
e-mail: hwangtl@csie.ncku.edu.tw

The rest of paper is organized as follows. Section 2 firstly reviews Shi et al.'s scheme. Then, an intercept-and-resend attack is shown in Sect. 3 and an improved scheme is presented in Sect. 4. Finally, a short conclusion is given in Sect. 5.

2 Review of Shi et al.'s Scheme

Suppose that two participants, Alice and Bob, have pre-shared n EPR pairs in state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, e.g., the first particle of each EPR pair is held by Alice and the second one is held by Bob. Shi et al.'s scheme allows Alice and Bob to distribute a secure key as follows:

Step 1. Bob randomly performs one of the two local unitary operations $\{I, \sigma_x\}$ on his particles and sends them to Alice, where $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$.

Step 2. Alice performs Bell measurement on the corresponding EPR pair. If there is no error, then the measuring results will be either $|\Psi^-\rangle$ or $|\Phi^-\rangle$; on the other hand, if there are measuring results in either $|\Psi^+\rangle$ or $|\Phi^+\rangle$, then it implies that the received particles are disturbed by the outsider, where $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are the four EPR pairs. In this way, Alice makes sure that the particles are indeed from Bob.

Step 3. By letting both the state $|\Psi^-\rangle$ and the operation I represent the binary bit "0" and the state $|\Phi^-\rangle$ and the operation σ_x represent to the binary bit "1". Alice and Bob can also share a key sequence.

It is obvious that both QKD and QA are simultaneously achieved without any classical communication.

3 An Intercept-and-Resend Attack

In the following, we show how a malicious user, Eve, can impersonate Bob without being detected by Alice. Eve intercepts each particle sent by Bob, measures it with the X-basis $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), . \ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, and then resends the measured particle to Alice. Because the encoded state of EPR pair is either $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle)$ or $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|-+\rangle + |+-\rangle)$, the measuring results of Eve will be either $|+-\rangle$ or $|-+\rangle$. And since Alice's particles now are not entangled with the measured ones by Eve, if Alice performs the Bell measurement, she will obtain the measuring result $|\Psi^-\rangle$ or $|\Phi^-\rangle$, each with 50% probability. Obviously, Alice will never find the existence of Eve. Although Eve can not eventually share a secret key with Alice (Eve has no information about Alice's measuring results), Eve indeed successfully disrupts the protocol. Alice can not correctly authenticate Bob and also she could not make sure if she really shares a secret key with Bob after the execution of the protocol. Thus, Shi et al.'s scheme fails to achieve QKD and QA simultaneously under the attack.

4 The Enhanced Scheme

This section tries to enhance Shi et al.'s scheme by adding $|\Psi^+\rangle$, another type of EPR pair, in the initial states of the protocol to avoid the above mentioned weakness. Section 4.1 proposes the enhanced scheme and Sect. 4.2 analyzed its security.

Table 1 The relations between Bob's operations and Alice's measuring results

Initial state	Bob's operation	Alice's measuring result	Bit information
$\|\Psi^-\rangle$	I	$\|\Psi^-\rangle$	0
	σ_x	$\|\Phi^-\rangle$	1
		$\|\Psi^+\rangle, \|\Phi^+\rangle$	Error
$\|\Psi^+\rangle$	I	$\|\Psi^+\rangle$	0
	σ_z	$\|\Psi^-\rangle$	1
		$\|\Phi^+\rangle, \|\Phi^-\rangle$	Error

4.1 The Scheme

In Shi et al.'s scheme, the EPR pairs pre-shared by Alice and Bob are all in $|\Psi^-\rangle$ and Bob performs one of the two operations $\{I, \sigma_x\}$ to encode his secret key. Therefore, the measuring results obtained by Alice are either $|\Psi^-\rangle$ or $|\Phi^-\rangle$. This makes Eve easily escape from Alice's detection and thus causes the above weakness. To overcome the problem, let us assume that the n EPR pairs shared between Alice and Bob are ether in $|\Psi^-\rangle$ or in $|\Psi^+\rangle$, and they both know the states their particles are in. Then they proceed the following steps.

Step 1. If the pre-shared state is $|\Psi^-\rangle$, Bob randomly performs one of the two local unitary operations $\{I, \sigma_x\}$ on his particles; otherwise he randomly performs one of the two unitary operation $\{I, \sigma_z\}$ on his particles and sends the encoded particles to Alice, where $\sigma_x = |0\rangle\langle 0| - |1\rangle\langle 1|$. Here, I and σ_x (or σ_z) denote the binary bit "0" and "1", respectively.

Step 2. Alice performs Bell measurement on the corresponding EPR pair. If the measuring result is in error (e.g., Alice obtains $|\Phi^-\rangle$, but the initial state is $|\Psi^+\rangle$, see also Table 1), then she believes that these particles are not from Bob and then aborts this communication.

Step 3. By letting $|\Psi^-\rangle$ and $|\Phi^-\rangle$ represent the binary bit "0" and "1" respectively if the initial state is $|\Psi^-\rangle$; $|\Psi^+\rangle$ and $|\Psi^-\rangle$ represent the binary bit "0" and "1" respectively if the initial state is $|\Psi^+\rangle$.

Table 1 shows the relations between Bob's operations and Alice's measuring results. According to Table 1, if the initial is $|\Psi^-\rangle$ then, Alice's measuring result should be ether $|\Psi^-\rangle$ or $|\Phi^-\rangle$; otherwise, it is in error and it implies that a malicious user, Eve, may exist in the communication.

4.2 Security Analysis

This section shows that Eve can be detected with the probability $(1 - (\frac{3}{4})^n)$ in the enhanced scheme if he performs the intercept-and resend attack on the enhanced scheme.

For simplify, let us first consider the case $n = 1$. Suppose that the initial state is $|\Psi^+\rangle$. Then, after Bob encodes his particle, the corresponding encoded state is either $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle)$ or $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle)$. If Eve uses the X-basis $\{|+\rangle, |-\rangle\}$ to measure Bob's particles, then the state will be reduced to a product state. Thus, Alice's measuring result will be in one of the four EPR pair $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, each with the probability of 25%. Thus, in this case, according to Table 1, Eve may be detected if the measuring result is not $|\Psi^+\rangle$ or not $|\Psi^-\rangle$, i.e., Eve will be detected with 50% probability. On the other hand, if Eve use the Z-basis then he will not be detected. Similarly, in the case that the initial state is in $|\Psi^-\rangle$, Eve will not be detected if X-basis is used to measure Bob's

particles. But she will be detected with 50% probability if Z-basis is used. Without knowing initial state, the probability of Eve to be detected is thus 25%. That is the probability of not being able to detect Eve is $\frac{3}{4}$ for $n = 1$. Therefore, for n states, the probability of Eve being detected is $(1 - (\frac{3}{4})^n)$. While n is large enough, the probability of Eve being detected is approximately 100%. That is, Eve can not impersonate Bob and disturb the secret key without being detected by Alice. The improved scheme is secure under the proposed intercept-and-resend attack.

5 Conclusion

The study has pointed out that Shi et al.'s scheme can not simultaneously realize QKD protocol and QA protocol if a malicious user performs an intercept-and-resend attack to impersonate Bob. Alice does not detect the malicious user and thus she fails to authenticate the identity of Bob. Though the malicious user may not be able to share a secret key with Alice, Alice does not know if she has shared a key with Bob or not. Furthermore, this study enhances Shi et al.'s scheme to avoid this weakness by adding one extra initial state in the protocol. The security analysis shows that the enhanced scheme is free from this attack with a high probability. Thus, QKD and QA can now be simultaneously realized in the improved scheme.

Acknowledgements The authors would like to thank the National Science Council of the Republic of China, Taiwan for financially supporting this research under Contract No. NSC 98-2221-E-006-097-MY3.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing (invited paper). In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, Dec., pp. 175–179 (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
3. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 0323021 (2002)
4. Li, C., Song, H.S., Zhou, L., Wu, C.F.: A random quantum key distribution achieved by using Bell states. J. Opt. B, Quantum Semiclass. Opt. **5**(2), 155–157 (2003)
5. Song, D.: Secure key distribution by swapping quantum entanglement. Phys. Rev. A **69**(3), 034301 (2004)
6. Namiki, R., Hirono, T.: Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. Phys. Rev. A **74**, 032302 (2006)
7. Hwang, T., Lee, K.C.: EPR quantum key distribution protocols with potential 100% qubit efficiency. IET Proc. Inf. Secur. **1**, 43–45 (2007)
8. Hwang, H., Lee, K.C., Li, C.M.: Provably secure three-party authenticated quantum key distribution protocols. IEEE Trans. Dependable Secure Comput. **4**, 71–80 (2007)
9. Gan, G.: Quantum key distribution scheme with high efficiency. Commun. Theor. Phys. **51**(5), 820–822 (2009)
10. Dušek, M., Haderka, Q., Hendrych, M., Myška, R.: Quantum identification system. Phys. Rev. A **60**(1), 149–155 (1998)
11. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication in quantum key distribution. Phys. Rev. A **62**, 022305 (2000)
12. Zeng, G.H., Zhang, W.P.: Identity verification in quantum key distribution. Phys. Rev. A **61**, 022303 (2000)
13. Shi, B.S., Li, J., Liu, J.M., Fan, X.F., Guo, G.C.: Quantum key distribution and quantum authentication based on entangled state. Phys. Lett. A **281**, 83–87 (2001)
14. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Phys. Rev. A **64**, 062309 (2001)

15. Mihara, T.: Quantum identification schemes with entanglements. Phys. Rev. A **65**, 052326 (2002)
16. Li, X.O.: Quantum authentication using entangled states. Int. J. Found. Comput. Sci. **15**(4), 609–617 (2004)
17. Zhou, N.R., Zeng, G.H., Zeng, W.J., Zhu, F.H.: Cross-center quantum identification scheme based on teleportation and entanglement swapping. Opt. Commun. **254**, 380–388 (2005)
18. Zhang, Z.H., Zeng, G.H., Zhou, N.R., Xiong, J.: Quantum identity authentication based on ping-pong technique for photons. Phys. Lett. A **356**, 199–205 (2006)
19. Yang, Y.G., Wen, Q.Y., Zhu, F.C.: An efficient quantum secure direct communication scheme with authentication. Chin. Phys. B **16**(7), 1838–1842 (2007)
20. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Secure authentication of classical messages with single photons. Chin. Phys. B **18**(8), 3189–3192 (2009)