Int J Theor Phys (2010) 49: 2210–2214
DOI 10.1007/s10773-010-0408-0

Simple Collaboration Eavesdropping on the Improved Multiparty Quantum Secret Sharing Protocol

Gan Gao

Received: 29 March 2010 / Accepted: 13 June 2010 / Published online: 23 June 2010

Abstract We propose a new attack strategy for the improvement n-party ($n \geq 4$) case [S. Lin, F. Gao, Q.Y. Wen, F.C. Zhu in Opt. Commun. 281:4553, 2008] of the multiparty quantum secret sharing protocol [Z.J. Zhang, G. Gao, X. Wang, L.F. Han, S.H. Shi in Opt. Commun. 269:418, 2007]. Our attack strategy is an interesting collaboration eavesdropping and much simpler than that in the paper [T.Y. Wang, Q.Y. Wen, F. Gao, S. Lin, F.C. Zhu in Phys. Lett. A 373:65, 2008].

Keywords Quantum secret sharing · Quantum teleportation · Bell state comparison

1 Introduction

In 1999, Hillery et al. introduced the principle of quantum mechanics into the field of secret sharing and proposed the first quantum secret sharing (QSS) protocol by using three-particle entangled Greenberger-Horne-Zeilinger (GHZ) state [1]. This protocol shows the basic idea of QSS very well, that is, a secret message is splitted into several pieces by a boss, and each agent holds a piece; and no subset of agents is sufficient to extract the boss's secret message, but the entire set is. Up to now, plenty of theoretical and experimental QSS protocols have been proposed [2–24]. So to speak, the QSS is progressing quickly and has attracted a lot of people. Part of people focused on the designing of new theoretical and experimental QSS protocols. The other part focused on the security analyzing of the QSS and pointed out the security leaks of some previous QSS protocols. Indeed, this is also an important studying point on the QSS because its security is rather complex, and both the outside eavesdropper's and the inside dishonest agent's attacks must be considered. Generally speaking, the attack

G. Gao (✉)
Department of Electrical Engineering, Tongling University, Tongling 244000, China
e-mail: gaogan0556@163.com

G. Gao
Engineering Technology Research Center of Optoelectronic Technology Appliance (Cultivating Base), AnHui Province, Tongling University, Tongling 244000, China

power of the dishonest agent is stronger because he (she) has a chance to tell a lie during the checking eavesdropping. Only if the lie is constructed successfully, he (she) can eavesdrop the boss's secret messages without introducing any error. Hence, we should mainly focus on the dishonest agent's attack while analyzing the security of QSS protocol. Recently, Zhang et al. utilize Einstein-Podolsky-Rosen (EPR) photon pairs and five local operations to propose a novel QSS protocol [17], in which almost all agents (except for Bob) obtain the sharing qualification by performing local operations. Since only Bell states are used, as far as a practical application is concerned, Zhang et al. QSS protocol is more convenient than Hillery et al.'s [1]. However, it is somewhat a pity that Zhang et al. protocol has a drawback of security, which is pointed out by Lin et al. [18]. Lin et al. think that the last agent may obtain Alice's secret messages without the helps of other agents, and they still give an improvement of Zhang et al. QSS protocol. Before long, Wang et al. [19] point out that the n-party ($n \geq 4$) cases in Lin et al. improved protocol [18] and in Zhang et al. original protocol [17] are not secure. Utilizing four-qubit states, they give a complex attack strategy, that is, the so-called collaboration eavesdropping. In this paper, we utilize Bell state to give another new attack strategy, which is much simpler than Wang et al.'s [19]. Before describing our attack, first, let us review Lin et al. improved four-party QSS protocol as follows:

(1) Bob prepares photons h and t in one of four Bell states: $\psi^{\pm}_{ht} = (|0\rangle|1\rangle \pm |1\rangle|0\rangle)_{ht}/\sqrt{2}$, $\phi^{\pm}_{ht} = (|0\rangle|0\rangle \pm |1\rangle|1\rangle)_{ht}/\sqrt{2}$. Then he sends photon t to Charlie and retains photon h in his site.

(2) After receiving photon t, firstly, Charlie ascertains whether photon t is a single photon [14]. If not, the communication will be terminated. Otherwise, he performs one of five operations: I, σ_x, σ_y, σ_z, H on photon t. The probabilities that five operations are selected by her are 1/8, 1/8, 1/8, 1/8 and 1/2, respectively. Here, $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $\sigma_y = |1\rangle\langle 0| - |0\rangle\langle 1|$, $\sigma_x = |0\rangle\langle 1| - |1\rangle\langle 0|$, $H = (|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|)/\sqrt{2}$. After performing his operation, Charlie sends photon t to Dick. After Dick receives photon t, his doing is same as Charlie's. Then he sends photon t to Alice.

(3) After receiving photon t, Alice randomly switches between the control mode and the message mode. In the control mode, Alice randomly selects one action from the two choices: One is that she lets Bob use $\{|0\rangle, |1\rangle\}$ or $\{|h\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |v\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$ to measure photon h, and tell her his measurement outcome and initial Bell state. Then Alice requires Charlie and Dick to announce their operations. The other is that Alice first lets Charlie and Dick announce their operations, and then asks Bob to perform a measurement on photon h and tell her his measurement outcome and initial Bell state. Next, Alice uses correct measuring basis to measure photon t. By comparing her measurement outcome with the deduced outcome, Alice can judge whether quantum channel is secure. If the quantum channel is attacked, the communication is aborted. Otherwise, the transmission goes on to the step (1). In the message mode, Alice encodes her secret messages by performing a unitary operation (I, σ_x, σ_y, σ_z) on photon t. After her encoding, Alice sends all the t-photons of message mode as a sequence (t-sequence) to Bob in one communication. Before sending t-sequence, Alice prepares a certain number of single photons (checking photons) randomly in one of four states: $|0\rangle$, $|1\rangle$, $|h\rangle$, $|v\rangle$, and inserts these checking photons into t-sequence. And then, she sends t-sequence to Bob.

(4) After Bob receives the sequence, Alice tells Bob the positions of the checking photons in the t-sequence and the initial states of all checking photons. Bob takes out the checking photons and uses suitable measuring basis to measure them. And then, by comparing his

measurement outcomes and the initial states, Bob can judges whether quantum channel between Alice and him is secure. After confirming that no eavesdropping exists, they can extract Alice's secret messages if Bob, Charlie and Dick collaborate.

2 Our Attack Strategy for Lin et al. Improved QSS Protocol

We can see that, in Lin et al. improved four-party protocol [18], Alice employs some checking photons in order to prevent the last agent from eavesdropping. By measuring them, Bob can judge whether the quantum channel between him and Alice is eavesdropped. In contrast to Zhang et al. original protocol, Lin et al. improved protocol only adds one process to check the security of quantum channel between Alice and Bob. It seems that Lin et al. improved protocol becomes really secure. As a matter of fact, it is still insecure. Next, we propose a new attack for Lin et al. improved protocol as follows:

At the beginning, Bob prepares photons h and t in $\phi^-_{ht} = (|0\rangle|0\rangle - |1\rangle|1\rangle)_{ht}/\sqrt{2}$, and he sends photon t to Charlie and retains photon h in his site. After performing his operation on photon t, Charlie sends it to Dick. After receiving photon t, Dick stores it well and doesn't perform any operation on it. In advance, Dick prepares another EPR pair in ψ^-_{da}, and he sends photon a, instead of photon t, to Alice. In the control mode, as soon as Alice requires the agents to announce information, Bob immediately uses the basis $\{|0\rangle, |1\rangle\}$ to measure photon h, which will lead that photon t must be in a polarization state. Afterwards, Dick makes Bell state measurement on photons t and d. Obviously, the polarization state of photon t may be recovered on photon a, which is the quantum teleportation process. Comparing his Bell state measurement outcome with ψ^-_{da}, Dick will get one unitary operator. This kind of Bell state comparison method and its comparison steps can be consulted in the paper [25]. When Alice asks Bob, Charlie and Dick to publish information, Bob announces the measurement outcome on photon h and his preparing state ϕ^-_{ht}. Dick tells the lie that his operation is the unitary operator that he gets by comparing Bell states. As a result, no matter what the operation published (performed) by Charlie is, Bob's and Dick's cheating trick will not be detected by Alice. Here, we can't help asking why their cheating trick is not detected? Next, let us explain this. Suppose that Charlie's operation is I, Bob's measurement outcome on photon h is $|0\rangle_h$ $(|1\rangle_h)$. It is evident that photon t in Dick's hand must be in $|0\rangle_t$ $(|1\rangle_h)$. Note that since Dick and Bob don't know what Charlie's operation is, they can't deduce which state photon t is in. When Dick makes Bell state measurement on photons t and d, the quantum teleportation occurs as follows:

$$\begin{aligned} |0\rangle_t \psi^-_{da} &= \frac{1}{\sqrt{2}}(|0\rangle_t|0\rangle_d|1\rangle_a - |0\rangle_t|1\rangle_d|0\rangle_a) \\ &= \frac{1}{2}[\psi^-_{td}(-|0\rangle_a) + \psi^+_{td}(-|0\rangle_a) + \phi^-_{td}|1\rangle_a + \phi^+_{td}|1\rangle_a] \end{aligned} \tag{1}$$

$$\begin{aligned} |1\rangle_t \psi^-_{da} &= \frac{1}{\sqrt{2}}(|1\rangle_t|0\rangle_d|1\rangle_a - |1\rangle_t|1\rangle_d|0\rangle_a) \\ &= \frac{1}{2}[\psi^-_{td}(-|1\rangle_a) + \psi^+_{td}|1\rangle_a + \phi^-_{td}|0\rangle_a + \phi^+_{td}(-|0\rangle_a)] \end{aligned} \tag{2}$$

Provided that Dick's measurement outcome on photons t and d is ϕ^+_{td}, so photon a should be in $|1\rangle_a$ $(-|0\rangle_a)$. Next, Dick makes a Bell state comparison for ϕ^+_{td} and ψ^-_{da} [25], and gets the unitary operator, σ_y. According to the above content, when Alice requires all agents to publish their information, Bob's, Charlie's, Dick's are $|0\rangle_h$ ($|1\rangle_h$) and ϕ^-, I, σ_y, respectively. Assuming that Dick doesn't replace photon t with photon a, but honestly performs σ_y operation on photon t, and sends it to Alice. We may see that the state of photons h and t evolves as follows:

$$\phi_{ht}^- \longrightarrow (\sigma_y)_{Dick}(I)_{Charlie}\phi_{ht}^- = \sigma_y I \phi_{ht}^- = (|0\rangle|1\rangle + |1\rangle|0\rangle)_{ht}/\sqrt{2} \tag{3}$$

When Bob's measurement outcome on photon h is $|0\rangle_h$ ($|1\rangle_h$), photon t in Alice's hand must be in $|1\rangle_t$ ($|0\rangle_t$). It is evident that $|1\rangle_t$ ($|0\rangle_t$) and $|1\rangle_a$ ($-|0\rangle_a$) are the same states. So, in the case that Charlie's operation is I, Alice isn't able to detect Bob's and Dick's cheating trick because any error isn't introduced. If Charlie's operation is H, is their trick still feasible? Go on analyzing, the key can be obtained. When Bob's measurement outcome on photon h is $|0\rangle_h$ ($|1\rangle_h$), as $H\phi_{ht}^- = (|0\rangle|h\rangle - |1\rangle|v\rangle)_{ht}/\sqrt{2}$, photon t in Dick's hand should be in $|h\rangle_t$ ($|v\rangle_t$), and the quantum teleportation process may be written as follows:

$$\begin{aligned} |h\rangle_t \psi_{da}^- &= \frac{1}{\sqrt{2}}|h\rangle_t(|0\rangle_d|1\rangle_a - |1\rangle_d|0\rangle_a) \\ &= \frac{1}{2}[\psi_{td}^-(-|h\rangle_a) + \psi_{td}^+(-|v\rangle_a) + \phi_{td}^-|h\rangle_a + \phi_{td}^+(-|v\rangle_a)] \end{aligned} \tag{4}$$

$$\begin{aligned} |v\rangle_t \psi_{da}^- &= \frac{1}{\sqrt{2}}|t\rangle_t(|0\rangle_d|1\rangle_a - |1\rangle_d|0\rangle_a) \\ &= \frac{1}{2}[\psi_{td}^-(-|v\rangle_a) + \psi_{td}^+(-|h\rangle_a) + \phi_{td}^-(-|v\rangle_a) + \phi_{td}^+|h\rangle_a] \end{aligned} \tag{5}$$

Suppose that Dick's measurement outcome is ψ_{td}^+, and photon a should be in $-|v\rangle_a$ ($-|h\rangle_a$). Dick compares ψ_{td}^+ with ψ_{da}^- to get the unitary operator σ_z. If there is no replacing, after Charlie's H and Dick's σ_z are performed on photon t from ϕ_{ht}^-, the system state evolves as follow:

$$\phi_{ht}^- \longrightarrow H\phi_{ht}^- = (|0\rangle|h\rangle - |1\rangle|v\rangle)_{ht}/\sqrt{2} \longrightarrow \sigma_z H\phi_{ht}^- = (|0\rangle|v\rangle - |1\rangle|h\rangle)_{ht}/\sqrt{2} \tag{6}$$

When Bob's measurement outcome on photon h is $|0\rangle_h$ ($|1\rangle_h$), photon t in Alice's hand must be in $|v\rangle_t$ ($|h\rangle_t$). Obviously, $|v\rangle_t$ ($|h\rangle_t$) and $-|v\rangle_a$ ($-|h\rangle_a$) are the same states. Similarly, Alice can't detect Bob's and Dick's cheating trick in the case that Charlie's operation is H. For the other cases (Charlie's other unitary operations, Dick's other comparison operators), only if Bob and Dick collaborate, their replacing trick may occur *as of old* and isn't detected. Here, in order to save space of a whole page, we don't list out the other cases again. When the message mode is switched into, since Alice doesn't detect Bob's and Dick's replacing trick, further, she regards photon a as photon t and encodes her secret messages by performing a unitary operation on it. Then she sends photon a to Bob. After receiving photon a, Bob and Dick make Bell state measurement on photons a and d, and easily obtain Alice's secret messages without Charlie's helps. So far, we successfully propose a new attack strategy for Lin et al. improved four-party QSS protocol [18]. It is evident that this attack is much simpler than that in the paper [19], and only two-photon EPR pair is used. In addition, the photons that need to be transmitted in our attack strategy are reduced greatly. In the end, we hope that this kind of attack strategy is noticed in the future related research since it to combine Bell state comparison and quantum teleportation is very special.

Acknowledgements I thank my parents for their encouragements. This work is supported by the Natural Science Foundation of AnHui Province under Grant No. KJ2010B236.

References

1. Hillery, M., Buzk, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
2. Gottesman, D.: Phys. Rev. A **61**, 042311 (1999)
3. Cleve, R., Gottesman, D., Lo, H.K.: Phys. Rev. Lett. **83**, 648 (1999)
4. Karimipour, V., Bahraminasab, A.: Phys. Rev. A **65**, 042320 (2000)
5. Bandyopadhyay, S.: Phys. Rev. A **62**, 012308 (2000)
6. Tittel, W., Zbinden, H., Gisin, N.: Phys. Rev. A **63**, 042301 (2001)
7. Yang, C.P., Gea-Banacloche, J.: J. Opt. B, Qantum Semiclass. Opt. **3**, 407 (2001)
8. Chau, H.F.: Phys. Rev. A **66**, 060302 (2002)
9. Bagherinezhad, S., Karimipour, V.: Phys. Rev. A **67**, 044302 (2003)
10. Hsu, L.Y.: Phys. Rev. A **68**, 022306 (2003)
11. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Phys. Rev. Lett. **92**, 177903 (2004)
12. Zhang, Y.Q., Jin, X.R., Zhang, S.: Phys. Lett. A **341**, 380 (2005)
13. Deng, F.G., Li, X.H., et al.: Phys. Lett. A **354**, 190 (2006)
14. Song, J., Zhang, S.: Chin. Phys. Lett. **23**, 1383 (2006)
15. Li, Y.M., Zhang, K.S., Peng, K.C.: Phys. Lett. A **324**, 420 (2004)
16. Liu, W.T., Liang, L.M., Li, C.Z., Yuan, J.M.: Chin. Phys. Lett. **5**, 1147 (2007)
17. Zhang, Z.J., Gao, G., Wang, X., Han, L.F., Shi, S.H.: Opt. Commun. **269**, 418 (2007)
18. Lin, S., Gao, F., Wen, Q.Y., Zhu, F.C.: Opt. Commun. **281**, 4553 (2008)
19. Wang, T.Y., Wen, Q.Y., Gao, F., Zhu, F.C.: Phys. Lett. A **373**, 65 (2008)
20. Xue, Z.Y., Yi, Y.M., Cao, Z.L.: Chin. Phys. **15**, 1421 (2006)
21. Deng, F.G., Li, X.H., Zhou, H.Y.: Phys. Lett. A **372**, 1957 (2008)
22. Gao, G.: Opt. Commun. **282**, 4464 (2009)
23. Gao, G.: Commun. Theor. Phys. **52**, 421 (2009)
24. Gao, G.: Opt. Commun. **283**, 2997 (2010)
25. Gao, G.: Opt. Commun. **281**, 876 (2008)