Erratum: Improving the security of multiparty quantum secret sharing against Trojan horse attack [Phys. Rev. A 72, 044302 (2005)]

Fu-Guo Deng, Xi-Han Li, Hong-Yu Zhou, and Zhan-jun Zhang
(Received 18 February 2006; published 10 April 2006)

DOI: 10.1103/PhysRevA.73.049901 PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Ta, 89.70.+c, 99.10.Cd

We find that the version of the multiparty quantum secret-sharing scheme in our paper is secure for the Trojan horse attack with a multiphoton signal, but it is insecure for some special attacks. There are mainly two kinds of eavesdropping with which the agent Bob, who prepares the quantum signal, can steal the information of the operations done by the other agents. One is the fake-signal attack [1] with Einstein-Podolsky-Rosen (EPR) pairs. The other is the attack with invisible photons [2].

The fake-signal attack can work as follows. The agent Bob replaces the original single photons with a fake signal, a sequence of EPR pairs in the state

$$|\psi^-\rangle_{BC} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{BC}$$

and sends the sequence S_C (composed of the photon C in each EPR pair) to the agent Charlie. Charlie cannot detect this cheat as he only analyzes the error rate of the samples for which he chooses the same measuring bases (MBs) as those of Bob's and Bob can publish fake states for the samples. In detail, Bob measures his photon B with one of the MBs, σ_z and σ_x, when the correlated photon C is chosen by Charlie as a sample for the eavesdropping check. Bob publishes the state of the photon C, i.e., the anticorrelated state of the photon B. This cheating cannot be found out by Charlie as it does not introduce errors in the results. Moreover, Bob can read out the message encoded by Bob on the EPR pairs when Charlie chooses the message-coding mode as Bob can distinguish the four operations $\{I, U, H, \overline{H}\}$ with which the EPR pair is transmitted into one of another set of orthogonal states:

$$\left\{ |\psi^-\rangle, |\phi^+\rangle, \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^+\rangle), \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^+\rangle) \right\}.$$

Here

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{BC}$$

and

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{BC}.$$

In this way, Bob can steal Charlie's information freely and fully.

The attack with invisible photons is introduced in Ref. [2]. For this attack, any eavesdropper, say Eve, can insert some invisible photons in the original signal. As the parties cannot detect those photons with their detector and they operate the signal with the same operation in some a slot time, Eve can read out the information about the operations by capturing the invisible photons when they run through the quantum line again. This attack dose not increase the error rate of the samples.

For improving the security of the improved version of the multiparty quantum secret sharing (this paper), the agents should have the capability to prevent the eavesdropping from stealing the information with those two attack strategies above. For the attack with invisible photons, the agents can use a special filter to prevent the invisible photons from entering the operation system, similar to the process for filtering the photons from the background before the signal is sent to detector in quantum cryptography [3]. The fake-signal attack can succeed as the four operations $\{I, U, H, \overline{H}\}$ transform a Bell state into another group of orthogonal states. For a two-dimension two-photon entangled system, there are four orthogonal eigenvectors in each joint measuring basis. Agent Charlie can use more than four operations to make the Bell state in some of the nonorthogonal states that cannot be copied freely. So we can improve the security of the scheme with a small modification. That is, we replace the step (d) in page 3 (this paper) with the following paragraph.

(d) If P_m is very low and ϵ_r is lower than the threshold, Charlie encrypts almost all the remaining photons in S by choosing randomly one of the four unitary operations $\{I, U, H, \overline{H}\}$. Then he chooses some samples, say S_C, from the S sequence, and performs them with one of the two operations $\{\sigma_x, \sigma_z\}$ randomly, and continues to the next step. Otherwise he discards the results and repeats the quantum communication from the beginning.

In this way, we should add two sentences at the end of the step (e) as follows:

For the samples done by Charlie with the operations σ_x and σ_z, Charlie tells Alice the positions first and then Alice requires that Bob tells her their original states. Charlie publishes the operations for the samples S_C.

[1] Sujuan Qin, Qiaoyan Wen, and Fuchen Zhu (unpublished).
[2] Qing-Yu Cai, Phys. Lett. A **351**, 23 (2006).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

