An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement

2010 J. Phys. A: Math. Theor. 43 209801

(http://iopscience.iop.org/1751-8121/43/20/209801)

J. Phys. A: Math. Theor. **43** (2010) 209801 (2pp) doi:10.1088/1751-8113/43/20/209801

Corrigendum

An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement

Yang Yu-Guang and Wen Qiao-Yan 2009 *J. Phys. A: Math. Theor.* **42** 055305

In the original paper [1], step (4) is in fact unnecessary and should be removed to improve the efficiency of the original protocol. And the protocol security will be ensured by the security check in steps (5) and (6).

In detail, in step (5) [1], to check whether the third party (TP) will cheat in the following announcement of his measurement outcomes in step (6) [1], Bob and Charlie perform the following two actions.

(i) They firstly require the TP to publish the initial states of the remaining intact EPR pairs in the original order he initially prepared.

(ii) Then Bob (Charlie) inserts the remaining intact EPR photons into the encoded photon sequence at the positions determined by the secret random value of l which is unknown to the TP. The secret insertion action corresponds to a secret permutation operation applied on the entire photon sequence.

In step (6) [1], after ensuring the security of the Bob-TP and Charlie-TP quantum channels, the TP takes a Bell-basis measurement on each of the two correlated photons received from Bob and Charlie with the two-photon entanglement basis $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ and publishes the measurement outcomes. Moreover, he still needs to publish the initial states of these EPR pairs in the order that he initially prepared. That is, he needs to publish the initial states of these EPR pairs in the original order he initially prepared though he does not attain the information about the permutation operation, i.e. the secret random value of l. The published initial states includes those of the encoded EPR pairs and those of the EPR pairs for checking the TP"s cheating. Bob and Charlie can judge whether the TP cheats by comparing the announcement of the initial states in step (6) with that of the initial states by the TP in step (5). When Bob and Charlie require the TP to publish the initial states of the remaining intact EPR pairs in the original order he initially prepared in step (5), the TP can do something according to Bob's and Charlie's requirements. That is, he either does nothing on the designated EPR pairs and announces randomly some values, or makes Bell-basis measurements and publishes the states of these EPR pairs according to the principle of entanglement swapping. However, because the TP does not know the secret random value of l, after the secret permutation operation is applied in step (5), he cannot discriminate between the encoded EPR pairs and those for checking cheating. Hence he guesses the correct positions of the EPR pairs for checking cheating with a negligible probability. And the TP's cheating attack is invalid in the second security check.

Hence, by the above analysis, one can very easily see that the first security check in step (4) is unnecessary and should be removed.

In addition, to improve the efficiency of the original quantum private comparison protocol, the secrets can be divided into many groups. In a certain round comparison, Bob and Charlie only compare a group of data. Once the result of the comparison is not equal in a certain round comparison, Bob and Charlie do not need to continue comparing the remaining data in the secret sequence. Thus, it will save lots of time and huge quantum resources.

1751-8113/10/209801+02$30.00

Acknowledgments

This work is supported by the National Nature Science Foundation of China (grant nos 60873191, 60821001); the Specialized Research Fund for the Doctoral Program of Higher Education (grant nos 20091103120014, 20090005110010); Beijing Natural Science Foundation (grant nos 1093015, 1102004); the Scientific Research Common Program of Beijing Municipal Commission of Education (grant no KM200810005004); the ISN open Foundation.

Reference

[1] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305