Protocols of quantum key agreement solely using Bell states and Bell measurement

Chitra Shukla[1,2], Anirban Pathak[1]

[1]Jaypee Institute of Information Technology, A-10, Sector-62, Noida 201307, India

[2]Graduate School of Information Science Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan

Abstract

Two protocols of quantum key agreement (QKA) that solely use Bell state and Bell measurement, are proposed. The first protocol of QKA proposed here is designed for two-party QKA, whereas the second protocol is designed for multi-party QKA [1]. The proposed protocols are also generalized to implement QKA using a set of multi-partite entangled states (e.g., 4-qubit cluster state and Ω state etc.). It is also be interesting to note that these protocols of QKA are similar to quantum string bit generation (multi-bit generalization of quantum string coin flipping (QSCF) [2]) and we investigate the comparision between proposed QKA and QSCF and especially with classical protocols which are secure with respect to some specific conditions. Security of the proposed protocols arises from the monogamy of entanglement [3], [4]. This is in contrast to the existing protocols of QKA where security arises from the use of non-orthogonal state (non-commutativity principle) [5]. On the other hand, the security of proposed QKA depends on the reliability of the random number generators (QRNG) of each party. QKA guarantees a random bit string even if one of the participants has a reliable QRNG. It offers the promise that in the device independent version, QKA may allow Alice and Bob to share a secure key under noisier conditions than QKD, because the burden of randomness is now shared between both parties. Efficiency of the proposed QKA protocols are also ananlysed. Further, it is shown that all the quantum systems that are useful for implementation of quantum dialogue (QD) and most of the protocols of secure direct quantum communication can be modified to implement protocols of QKA.

Keywords: Quantum key agreement, multi-party key agreement, orthogonal-state-based quantum key agreement.

References

[1] C. Shukla, N. Alam, A. Pathak, Quantum Inf. Process. **13** (2014) 2391-2405.

[2] J. Barrett, S. Massar, Phys. Rev. A **69**, (2004) 022322.

[3] C. Shukla, A. Pathak and R. Srikanth, Int. J. Quant. Info. **10** (2012) 1241009.

[4] P. Yadav, R. Srikanth and A. Pathak, Quantum Inf. Process.**13**, (2014) 2731-2743.

[5] S.-K. Chong and T. Hwang, Optic Commun. **283** (2010) 1192-1195.