conferenceseries.com

J Laser Opt Photonics 2017, 4:3(Suppl)
DOI: 10.4172/2469-410X-C1-015

2nd International Conference on

Quantum Physics and Quantum Technology

September 25-26, 2017 Berlin, Germany

Key-leakage evaluation of authentication in quantum key distribution with finite resources

Chun Zhou, Wan-Su Bao, Hong-Wei Li, Yang Wang and **Mu-Sheng Jiang**
Zhengzhou Information Science and Technology Institute, China

Partially information leakages of generation key undoubtedly influence the security of practical Quantum Key Distribution (QKD) system. In this paper, based on finite-key analysis and deep investigation on privacy amplification, we present a method for characterizing information leakages gained by adversary in each authentication round and therefore take the theory derived by J. Cederlöf and J-Ä. Larsson [IEEE Trans. Inf. Theory, 54, 1735 (2008)] into practical case. As the authentication key is fed from one round of generation keys to the next except the first round, by considering its security weakness due to information leakages and finite size effect, we further propose a universal formula for calculating the lifetime of initial authentication key used in QKD with finite resources. Numerical simulations indicate that our bound for estimating information leakages strictly characterizes the stability of practical QKD against information-leakage based attacks and our calculation formula in terms of lifetime can precisely evaluate the usage time of initial authentication key. Our work provides a practical solution for evaluating authentication security of QKD.

2010thzz@sina.com