Highly Efficient Quantum Key Distribution Immune to All Detector Attacks

Wen-Fei Cao, Yi-Zheng Zhen, Yu-Lin Zheng, Zeng-Bing Chen, Nai-Le Liu, Kai Chen, and Jian-Wei Pan

[1] *National Laboratory for Physical Sciences at Microscale and Department of Modern Physics University of Science and Technology of China, Hefei, 230026, P.R. China and*

[2] *CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

Abstract

Vulnerabilities and imperfections of single-photon detectors have been shown to compromise security for quantum key distribution (QKD). The measurement-device-independent QKD (MDI-QKD) appears to be the most appealing solution to solve the issues. However, in practice one faces severe obstacles of having significantly low key generation rate, difficult two photon interferences, and remote synchronization etc. In this letter, we propose a highly efficient and simple quantum key distribution scheme to remove all of these drawbacks. Our proposal can be implemented with only small modifications over the standard decoy BB84 system. Remarkably it enjoys both the advantages of high key generation rate (being almost two orders of magnitude higher than that based on conventional MDI-QKD) comparable to the normal decoy system, and security against any detector side channel attack. Most favorably one can achieve complete Bell state measurements with resort to single photon interference, which reduces experimental costs significantly. Our approach enables utilization of high speed and efficient secure communication, particularly in real-life scenario of both metropolitan and intercity QKD network, with an attack free fashion from arbitrary detector side channels.