Abstract Submitted
for the MAR09 Meeting of
The American Physical Society

Quantum key distribution with an unknown and untrusted source
YI ZHAO, BING QI, HOI-KWONG LO, Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto — The security of a standard bi-directional "plug & play" quantum key distribution (QKD) system has been an open question for a long time. This is mainly because its source is equivalently controlled by an eavesdropper, which means the source is unknown and untrusted. Qualitative discussion on this subject has been made previously. In this paper, we present the first quantitative security analysis on a general class of QKD protocols whose sources are unknown and untrusted. The securities of standard BB84 protocol, weak+vacuum decoy state protocol, and one-decoy decoy state protocol, with unknown and untrusted sources are rigorously proved. We derive rigorous lower bounds to the secure key generation rates of the above three protocols. Our numerical simulation results show that QKD with an untrusted source gives a key generation rate that is close to that with a trusted source. Our work is published in [1].

[1] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A, 77:052327 (2008).

Yi Zhao

Date submitted: 19 Nov 2008 Electronic form version 1.4