Abstract Submitted
for the MAR07 Meeting of
The American Physical Society

Unconditional security at a low cost[1] XIONGFENG MA, University of Toronto, HOI-KWONG LO, HOI-KWONG LO TEAM — In this talk, I will discuss several post-processing schemes for quantum key distribution (QKD). I will compare QKD with and without decoy states. By simulating four QKD experiments and analyzing one decoy-state QKD experiment, we compare two data post-processing schemes based on security against individual attacks by Lütkenhaus, and unconditional security analysis by Gottesman-Lo-Lütkenhaus-Preskill. Our results show that these two schemes yield close performances. In QKD, since unconditional security is highly sought after, we conclude that one is better off considering unconditional security, rather than restricting to individual attacks. This work is appeared in Ref. [X. Ma, Phys. Rev. A *74*, 052325, (2006)].

[1]This work has been supported by CFI, CIAR, CIPI, Connaught, CRC, NSERC, OIT, PREA and the University of Toronto. X. Ma gratefully acknowledges Chinese Government Award for Outstanding Self-financed Students Abroad.

Xiongfeng Ma
University of Toronto

Date submitted: 20 Nov 2006 Electronic form version 1.4