Abstract Submitted
for the DAMOP07 Meeting of
The American Physical Society

Quantum key distribution with entangled sources XIONGFENG MA, CHI-HANG FRED FUNG, HOI-KWONG LO, University of Toronto — We propose a model and a post-processing protocol for quantum key distribution (QKD) with entangled photons from a parametric down-conversion (PDC) source. We also investigate the entanglement PDC QKD with two-way classical communications. We find that the recurrence scheme increases the key rate and Gottesman-Lo protocol helps tolerate higher channel losses. By simulating a real QKD setup, we compare three implementations — entanglement PDC QKD, triggering PDC QKD and coherent state QKD. The simulation result suggests that the entanglement PDC QKD can tolerate higher channel losses than the coherent state QKD. On the other hand, the coherent state QKD with decoy states is able to achieve highest key rate in the low and medium-loss regime. By applying Gottesman-Lo two-way post-processing protocol, the entanglement PDC QKD can tolerate up to 70dB combined channel losses (35dB for each channel) provided that the PDC source is placed in between Alice and Bob rather than at Alice's side. Since a 35dB channel loss is similar to the estimated loss in a satellite to ground quantum transmission, our result is in agreement with the suggestion in the literature that secure QKD between two ground locations via an *untrusted* satellite with an entanglement-based PDC source appears to be technologically feasible.

Xiongfeng Ma
University of Toronto

Date submitted: 03 Feb 2007 Electronic form version 1.4