Abstract Submitted
for the MAR09 Meeting of
The American Physical Society

Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems YI ZHAO, CHI-HANG F. FUNG, BING QI, CHRISTINE CHEN, HOI-KWONG LO, Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto — Quantum key distribution (QKD) systems can send signals over more than 100 km standard optical fiber and are widely believed to be secure. Here, we show experimentally for the first time a technologically feasible attack, namely the time-shift attack, against a commercial QKD system. Our result shows that, contrary to popular belief, an eavesdropper, Eve, has a non-negligible probability ($\sim$4%) to break the security of the system. Eve's success is due to the well-known detection efficiency loophole in the experimental testing of Bell inequalities. Therefore, the detection efficiency loophole plays a key role not only in fundamental physics, but also in technological applications such as QKD. Our work is published in [1].

[1] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A, 78:042333 (2008).

Yi Zhao

Date submitted: 03 Dec 2008 Electronic form version 1.4