Abstract Submitted
for the DAMOP10 Meeting of
The American Physical Society

Implementation of an attack scheme on a practical QKD system
ANTIA LAMAS-LINARES, Centre for Quantum Technologies, Nat. Univ. Singapore, QIN LIU, NTNU Trondheim, ILJA GERHARDT, Centre for Quantum Technologies, Nat. Univ. Singapore, VADIM MAKAROV, NTNU Trondheim, CHRISTIAN KURTSIEFER, Centre for Quantum Technologies/Physics Dept, Nat. Univ. Singapore — We report on an experimental implementation of an attack of a practical quantum key distribution system [1], based on a vulnerability of single photon detectors [2]. An intercept/resend-like attack has been carried out which revealed 100% of the raw key generated between the legitimate communication partners. No increase of the error ratio was observed, which is usually considered a reliable witness for any eavesdropping attempt. We also present an experiment which shows that this attack is not revealed by key distribution protocols probing for eavesdroppers by testing a Bell inequality [3], and discuss implications for practical quantum key distribution.

[1] I. Marcikic, A. Lamas-Linares, C. Kurtsiefer, Appl. Phys. Lett. 89, 101122 (2006); [2] V. Makarov, New J. Phys. 11, 065003 (2009); [3] A. Ling et al., Phys. Rev. A 78, 020301(R), (2008)

Christian Kurtsiefer
Centre for Quantum Technologies, Nat. Univ. Singapore

Date submitted: 27 Jan 2010 Electronic form version 1.4