Abstract Submitted
for the MAR06 Meeting of
The American Physical Society

Quantum Cryptography in Existing Telecommunications Infrastructure DANIEL ROGERS[1], JOSHUA BIENFANG, ALAN MINK, BARRY HERSHMAN, ANASTASE NAKASSIS, XIAO TANG, LIJUN MA, DAVID SU, CARL WILLIAMS, CHARLES CLARK, National Institute of Standards and Technology — Quantum cryptography has shown the potential for ultra-secure communications. However, all systems demonstrated to date operate at speeds that make them impractical for performing continuous one-time-pad encryption of today's broadband communications. By adapting clock and data recovery techniques from modern telecommunications engineering practice, and by designing and implementing expeditious error correction and privacy amplification algorithms, we have demonstrated error-corrected and privacy-amplified key rates up to 1.0 Mbps over a free-space link with a 1.25 Gbps clock. Using new detectors with improved timing resolution, careful wavelength selection and an increased clock speed, we expect to quadruple the transmission rate over a 1.5 km free-space link. We have identified scalable solutions for delivering sustained one-time-pad encryption at 10 Mbps, thus making it possible to integrate quantum cryptography with first-generation Ethernet protocols.

[1]also with the University of Maryland Chemical Physics Program

Daniel Rogers

Date submitted: 30 Nov 2005 Electronic form version 1.4