Abstract Submitted
for the MAR12 Meeting of
The American Physical Society

Thwarting the Photon Number Splitting Attack with Entanglement Enhanced BB84 Quantum Key Distribution CHRIS RICHARDSON, CARL SABOTTKE, Louisiana State University, ULVI YURTSEVER, MathSense Analytics, ANTIA LAMAS, National University of Singapore, JONATHAN DOWLING, Louisiana State University, PETR ANISIMOV, Stony Brook University — We develop an improvement to the weak laser pulse BB84 scheme for quantum key distribution, which utilizes entanglement to improve the security of the scheme and enhance its resilience to the photon number splitting attack. This protocol relies on the non-commutation of photon phase and number to detect an eavesdropper performing quantum non-demolition measurement on number. The potential advantages and disadvantages of this scheme are compared to the coherent decoy state solution. Most entanglement based quantum key distribution schemes rely on violations of Bell's inequalities to ensure security. However, this is not the strategy that our entanglement enhanced (EE) BB84 employs here. Instead, we detect Eve by introducing an entangled quantum state into the system that is sensitive to Eve's QND measurements. This allows for a recovery of an approximately linear dependence on transmittivity for the key rate. EE BB84 shares this advantage with coherent decoy state protocols as well as schemes that utilize strong phase reference pulses to eliminate Eve's ability to send Bob vacuum signals.

Chris Richardson
Louisiana State University

Date submitted: 29 Nov 2011 Electronic form version 1.4