

Abstract Submitted
for the MAR15 Meeting of
The American Physical Society

A Weak Value Based QKD Protocol Robust Against Detector Attacks JAMES TROUPE, Applied Research Laboratories, University of Texas at Austin — We propose a variation of the BB84 quantum key distribution protocol that utilizes the properties of weak values to insure the validity of the quantum bit error rate estimates used to detect an eavesdropper. The protocol is shown theoretically to be secure against recently demonstrated attacks utilizing detector blinding and control and should also be robust against all detector based hacking. Importantly, the new protocol promises to achieve this additional security without negatively impacting the secure key generation rate as compared to that originally promised by the standard BB84 scheme. Implementation of the weak measurements needed by the protocol should be very feasible using standard quantum optical techniques.

James Troupe
Applied Research Laboratories, University of Texas at Austin

Date submitted: 14 Nov 2014

Electronic form version 1.4