Abstract Submitted
for the MAR17 Meeting of
The American Physical Society

BB84 with Weak Measurements, Greater Security with Fewer Assumptions[1] JAMES TROUPE, Applied Research Laboratories, University of Texas at Austin, JACOB FARINHOLT, Naval Surface Warfare Center, US Navy — Detector blinding attacks on prepare-and-measure QKD protocols allow an eavesdropper to take control of Bob's measurement device and mask her interactions with the signals. Measurement-device-independent QKD (MDI-QKD) was developed to avoid this "detector loophole" by altogether eliminating Bob's detectors. Parameter estimation and key extraction is performed based on the results of a joint Bell measurement on both Alice and Bob's signals. While this resolves the security loophole, the need for a Bell measurement requires both signals to arrive in the same timing window, leading to significant engineering challenges and/or a severe reduction in secure key rates. Here we propose a simpler method to avoid the detector loophole in a prepare-and-measure scenario. Namely, we show that it is possible to completely separate the parameter estimation from its dependency on Bob's measurement basis by making weak measurements immediately prior to Bob's detection and averaging these results conditioned only on the source. We show that this new protocol is as secure as MDI-QKD under detector attacks, is practical to implement, and provides a secure key rate equivalent to that promised by the original BB84 protocol.

[1]ONR grant N00014-15-1-2225.

James Troupe
Applied Research Laboratories, University of Texas at Austin

Date submitted: 11 Nov 2016 Electronic form version 1.4