Abstract Submitted
for the MAR16 Meeting of
The American Physical Society

A Contextuality Based Quantum Key Distribution Protocol[1]
JAMES TROUPE, The University of Texas at Austin — In 2005 Spekkens presented a generalization of noncontextuality that applies to imperfect measurements (POVMs) by allowing the underlying hidden variable model to be indeterministic. In addition, unlike traditional Bell-Kochen-Specker noncontextuality, HV models of a single qubit were shown to be *contextual* under this definition. Thus, not all single qubit POVM measurement outcomes can be modeled classically. Recently M. Pusey showed that, under certain conditions, exhibiting an anomalous weak value (i.e. values outside the eigenspectrum of the observable) implies contextuality. We will present a new single qubit prepare and measure QKD protocol that uses observation of anomalous weak values of particular observables to estimate the quantum channel error rate and certify the security of the channel. We also argue that it is the "degree" of contextuality of the noisy qubits exiting the channel that fundamentally determine the secure key rate. A benefit of this approach is that the security does not depend on the fair sampling assumption, and so is not compromised by Eve controlling Bob's measurement devices. Thus, it retains much of the benefit of "Measurement Device Independent" QKD protocols while only using single photon preparations and measurements.

[1]Supported by the Office of Naval Research under grant N00014-15-1-2225.

James Troupe
The University of Texas at Austin

Date submitted: 06 Nov 2015 Electronic form version 1.4