1106-68-322 **Walter O Krawec*** (walter.krawec@gmail.com), Hoboken, NJ 07030. *Security in the Semi-Quantum Setting.*

Semi-Quantum Key Distribution (SQKD) protocols, introduced by Boyer et al. in 2007, allow a fully quantum A and a limited "classical" B to distill a secret key, secure against even an all powerful adversary E. These protocols rely on a two-way quantum communication channel making their security analysis difficult. We proved in [1] that, for certain families of protocols, we need only consider restricted attacks consisting of a bias and a single unitary. We extend this result to prove the security of a new multi-user SQKD protocol we devised (allowing two limited "classical" users, A and B, to distill a secret key with the help of an untrusted quantum server). We compute a lower bound, as a function only of the observed error rate, of this protocol's key generation rate in the asymptotic scenario. Our result demonstrates that the security of a SQKD protocol can be comparable to some "fully" quantum ones, which was an open question.

[1] W.O. Krawec, "Restricted Attacks on Semi-Quantum Key Distribution Protocols", Quantum Information Processing, 2014, DOI: 10.1007/s11128-014-0802-2 (Received September 03, 2014)