Abstract Submitted
for the MAR17 Meeting of
The American Physical Society

Symmetric Extendability of Quantum States, Bound Secrecy, and the Extreme Limits of Quantum Key Distribution SUMEET KHATRI, NORBERT LUTKENHAUS, University of Waterloo — Bound secret information is classical information that contains secrecy but from which secrecy cannot be extracted. The existence of bound secret information is currently unproven, and in this work we provide strong analytical and numerical evidence for its existence. Our work is tied to the noise-tolerance thresholds of quantum key distribution (QKD) protocols with public classical communication in which the classical data arises from measurement of quantum states.

First, we show how symmetric extendability of quantum states is related to distilling secret key from classical data. We then show how the existence of successful two-way classical protocols can be simplified to breaking the symmetric extendability through post-selection on error-correction codes. We show that repetition codes reproduce the known results on the noise-tolerance of two-way protocols in QKD and provide analytical and numerical evidence that they are optimal. For QKD protocols using a six-state setup, this means that the domain of bound secret information is characterized by a quantum bit-error rate between 27.6% and 33.3%.

Sumeet Khatri
University of Waterloo

Date submitted: 11 Nov 2016

Electronic form version 1.4