Abstract Submitted
for the MAR13 Meeting of
The American Physical Society

Quantum to classical randomness extractors STEPHANIE WEHNER, CQT, Singapore, MARIO BERTA, ETH Zurich, OMAR FAWZI, McGill University — The goal of randomness extraction is to distill (almost) perfect randomness from a weak source of randomness. When the source yields a classical string X, many extractor constructions are known. Yet, when considering a physical randomness source, X is itself ultimately the result of a measurement on an underlying quantum system. When characterizing the power of a source to supply randomness it is hence a natural question to ask, how much classical randomness we can extract from a quantum system. To tackle this question we here introduce the notion of quantum-to-classical randomness extractors (QC-extractors). We identify an entropic quantity that determines exactly how much randomness can be obtained. Furthermore, we provide constructions of QC-extractors based on measurements in a full set of mutually unbiased bases (MUBs), and certain single qubit measurements. As the first application, we show that any QC-extractor gives rise to entropic uncertainty relations with respect to quantum side information. Such relations were previously only known for two measurements. As the second application, we resolve the central open question in the noisy-storage model [Wehner et al., PRL 100, 220502 (2008)] by linking security to the quantum capacity of the adversary's storage device.

Stephanie Wehner
CQT, Singapore

Date submitted: 09 Nov 2012 Electronic form version 1.4