Abstract Submitted
for the MAR11 Meeting of
The American Physical Society

Achieving the physical limits of the bounded-storage model PRABHA MANDAYAM, Caltech, STEPHANIE WEHNER, Centre for Quantum Technologies — The security of most cryptographic systems in use today is based on the premise that certain computational problems are hard to solve for the adversary. However, recent cryptographic models such as the bounded-storage model and the noisy-storage model, are based on more physical assumptions regarding the two parties' resources and allow us to obtain security without relying on any additional hardness results. In the bounded-storage model, where the adversary's quantum storage is limited, it is known that security can be achieved if the adversary can store strictly less then half of the qubits transmitted during the protocol. It has been an open question whether security can still be achieved if the adversary's storage were any larger. Here, we answer this question positively and demonstrate a two-party protocol which is secure as long as the adversary cannot store even a small fraction of the transmitted pulses. This not only settles the question, but also highlights the sharp contrast to classical bounded storage, where it is known that security can only be obtained if the adversary's classical storage is at most quadratic in the storage required by the honest players. In the more general setting of the noisy-storage model, where the adversary's memory is simply assumed to be imperfect, we show that our protocol extends security to a larger class of noisy quantum memories. (Reference: arXiV - quant-ph 1009.1596)

Prabha Mandayam Doddamane
California Institute of Technology

Date submitted: 19 Nov 2010 Electronic form version 1.4