# On the Computational Collapse of Unknown Quantum States

Louis Salvail
*Department of Computer Science*
*Aarhus University*
*Ny Munkegade*
*8000 Aarhus C.*
*DENMARK*

**Abstract**

Assume a computationally binding string commitment schemes is used to force the receiver of BB84 qubits to measure upon reception. Since measuring induces an irreversible collapse to the received quantum state, even given extra information after the measurement was performed does not allow the receiver to evaluate reliably some predicates applied to the classical bits encoded in the received state.We call quantum measurement commitment (QMC) this important quantum primitive that allows, among other things, to implement oblivious transfer securely according a computational assumption.

An adversary to QMC is one that can both provide valid proof of having measured the received states while still being able to evaluate a predicate applied to the classical content of the encoding. We describe the first quantum black-box reduction for the security of QMC to the binding property of the string commitment. We characterize a class of quantum adversaries against QMC that can be transformed into adversaries against a weak form for the binding property for the string commitment. As an application, we show how an oblivious transfer computationally secure against the receiver and unconditionally secure against the sender can be based upon any unconditionally concealing string commitment satisfying a weak computational binding property. In contrast, Yao's proof of security for quantum oblivious

transfer does not apply in the computational setting since it assumes the commitments are modeled by a perfect classical black-box. Such a black-box approach fails to capture all possible quantum attacks that can be mounted by the adversary.

Joint work with Claude Crépeau, Paul Dumais, and Dominic Mayers.