Abstract Submitted
for the MAR15 Meeting of
The American Physical Society

Quantum rewinding via phase estimation[1] GELO NOEL TABIA, University of Tartu — In cryptography, the notion of a zero-knowledge proof was introduced by Goldwasser, Micali, and Rackoff [1]. An interactive proof system is said to be zero-knowledge if any verifier interacting with an honest prover learns nothing beyond the validity of the statement being proven. With recent advances in quantum information technologies, it has become interesting to ask if classical zero-knowledge proof systems remain secure against adversaries with quantum computers. The standard approach to show the zero-knowledge property involves constructing a simulator for a malicious verifier that can be rewinded to a previous step when the simulation fails. In the quantum setting, the simulator can be described by a quantum circuit that takes an arbitrary quantum state as auxiliary input but rewinding becomes a nontrivial issue. Watrous proposed a quantum rewinding technique in the case where the simulation's success probability is independent of the auxiliary input [2]. Here I present a more general quantum rewinding scheme that employs the quantum phase estimation algorithm. References: [1] S. Goldwasser, S. Micali, and C. Rackoff, SIAM J. Comput. 18(1) 186-208, 1989. [2] J. Watrous, SIAM J. Comput. 39(1) 25-58, 2009.

[1] This work was funded by institutional research grant IUT2-1 from the Estonian Research Council and by the European Union through the European Regional Development Fund.

Gelo Noel Tabia
Institute of Computer Science, University of Tartu

Date submitted: 14 Nov 2014

Electronic form version 1.4