Abstract Submitted
for the DAMOP12 Meeting of
The American Physical Society

Unforgeable Noise-Tolerant Quantum Tokens NORMAN YAO, Harvard University, FERNANDO PASTAWSKI, Max Planck Institute for Quantum Optics, LIANG JIANG, IQI, California Institute of Technology, MIKHAIL LUKIN, Harvard University, IGNACIO CIRAC, Max Planck Institute for Quantum Optics
— The realization of devices which harness the laws of quantum mechanics represents an exciting challenge at the interface of modern technology and fundamental science. An exemplary paragon of the power of such quantum primitives is the concept of "quantum money." A dishonest holder of a quantum bank-note will invariably fail in any forging attempts; indeed, under assumptions of ideal measurements and decoherence-free memories such security is guaranteed by the no-cloning theorem. In any practical situation, however, noise, decoherence and operational imperfections abound. Thus, the development of secure "quantum money"-type primitives capable of tolerating realistic infidelities is of both practical and fundamental importance. Here, we propose a novel class of such protocols and demonstrate their tolerance to noise; moreover, we prove their rigorous security by determining tight fidelity thresholds. Our proposed protocols require only the ability to prepare, store and measure single qubit quantum memories, making their experimental realization accessible with current technologies.

Norman Yao
Harvard University

Date submitted: 30 Jan 2012 Electronic form version 1.4