Abstract Submitted
for the MAR13 Meeting of
The American Physical Society

Quantum secret sharing with minimized quantum communication BEN FORTESCUE, Southern Illinois University, GILAD GOUR, University of Calgary — Standard techniques for sharing a quantum secret among multiple players (such that certain subsets of the players can recover the secret while others are denied all knowledge of the secret) require a large amount of quantum communication to distribute the secret, which is likely to be the most costly resource in any practical scheme. Two known methods for reducing this cost are the use of imperfect "ramp" secret sharing (in which security is sacrificed for efficiency) and classical encryption (in which certain elements of the players' shares consist of classical information only). We demonstrate how one may combine these methods to reduce the required quantum communication below what has been previously achieved, in some cases to a provable minimum, without any loss of security. The techniques involved are closely-related to the properties of stabilizer codes, and thus have strong potential for being adapted to a wide range of quantum secret sharing schemes.

Ben Fortescue
Southern Illinois University

Date submitted: 11 Dec 2012 Electronic form version 1.4