Quantum Secret Sharing

James Mayclin and Keanu Spies

For our final project, we will be attempting to implement a reproduction of the Quantum Secret Sharing Algorithm described by Hillery et al (1998) [1] and Cleve et al (1999) [2].

Following the approach from Cleve, we will attempt to create a secret of arbitrary state (*k,n*) where *n* is the number of shares of entangled bits and *k* is the number of those shares required to uncover the state. This allows for a secure system protecting against at most *n - k - 1* untrustworthy recipients of the entangled bits. This algorithm has a wide variety of uses in cryptography and computer security and we believe it holds much promise for the future of these fields.

We will then analyze the effects of noise on the system and attempt to find methods of error correction which are viable in the case of secret sharing. We will examine the effects of noise across several different noise models, allowing to examine the susceptibility of this algorithm to increasingly large amounts of noise. This is of particular interest to Quantum Secret Sharing, due to the fact that we require all *k* keys to extract the secret, and that any of the *k - 1* keys contain no information. Therefore, if any single one of the *k* pieces of corrupted then we will not be able to successfully extract the quantum secret.

Bibliography:

[1] Quantum secret sharing, Mark Hillery (Hunter Coll.), Vladimir Buzek (Bratislava, Inst. Phys.), Andre Berthiaume (De Paul U.). Jun 1998. 6 pp. Published in Phys.Rev. A59 (1999) 1829

[2] How to share a quantum secret, Richard Cleve (Calgary U.), Daniel Gottesman (Los Alamos), Hoi-Kwong Lo (Hewlett-Packard, Bristol). Jan 1999. 5 pp. Published in Phys.Rev.Lett. 83 (1999) 648-651

page intentionally left blank