Review of How to Share a Quantum Secret [1]

Haobei Song

University of Waterloo

March 28 2017

Abstract

Secret sharing also known as secret splitting has been developed considerably ever since its invention in 1979. With the emerging of quantum computing, study of secret sharing protocols implemented by quantum physics becomes an active area filled with interest and intrigue due to the eccentric properties from quantum mechanics such as entanglement and interference between quantum states. In a (k, n) threshold scheme, a secret quantum state could be transformed into n shares and kept by different participants among whom only k or more shares combined can reconstruct the secret, with another restriction that any set of shares fewer than k contain no information at all about the secret and thus cannot be used to reconstruct the secret. This paper then shows that it is the "no-cloning theorem" solely that places the restriction on the existence of the threshold schemes (k, n) where $n \leq 2k$, along with the algorithms for constructiong all of the threshold schemes belonging to this category efficiently. In addition, it also explains the reason why the shares distributed by a (k, n) threshold scheme with $k \leq n \leq 2k - 1$ must be in a global mixed state.

1 Introduction

1.1 Preview

Since the first time the concept of secret sharing was proposed independently by Adi Shamir[2] and George Blakley[3] in 1979, it has gained appreciable attention and has been studied extensively in quantum computing. Secret sharing also known as secret splitting is refered to as protocols or methods for secret dstribution among a gathering of parties each of whom is provided with a share of the secret. Secret sharing is widely employed in cryptographic key management within information industries and considered of more and more importance as the concept of sharing information on internet has become extensively accepted by more and more people. Suppose the secret is distributed into n shares, then a (k, n) scheme is defined as a method or protocol such that any set of k or more shares can be used to reconstruct the secret, but any set of less than k shares carry absolutely no information at all about the secret divided. For example, three keys to the vault are assigned to three clerks in a bank. They can open the vault with whichever two clerks present, but no one could open the vault by himself. Besides, one alone has no idea at all about the structure of the locker on the vault at all. This method or protocol of dividing the keys (shares of the secret) is a $(2, 3)$ threshold scheme.

1.2 Quantum Setting

A secret sharing protocol with respect to quantum states starts with a random states with no beforehand knowledge about the state.

References

[1] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” *Phys. Rev. Lett.*, vol. 83, pp. 648–651, Jul 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.83.648

[2] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979. [Online]. Available: http://doi.acm.org/10.1145/359168.359176

[3] G. R. Blakley, “Safeguarding cryptographic keys,” *Managing Requirements Knowledge, International Workshop on*, vol. 00, p. 313, 1899.