Review of How to Share a Quantum Secret

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 $k, nthresholdscheme, asecretquantums$ $cloningtheorem"solelythatplacestherestrictionontheexistenceofthethresholdschemesk, nwhere$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 $k, nthresholdschemewith$k $\leq n \leq 2k-1$ must be in a global mixed state.

1 Introduction

Since the first time the concept of secret sharing was put forward independently by Adi Shamir and George Blakley in 1979, it has gained tremendous attention and 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.