A study of secure protocol by quantum theory

Atsushi Waseda
School of Information Science,
Japan Advanced Institute of Science and Technology

March 22, 2007

Abstract

Quantum Coin Flipping (QCF) and Quantum Secret Sharing (QSS) are one of the important fields of quantum security. QCF protocol was proposed by Bennett and Brassard in 1984 and QSS scheme was proposed by Hillery et al. in 1999. Suppose that two players execute a quantum coin flipping protocol to reach an agreement on a value c. If one of them is dishonest, then deviation of a *bias* ϵ from probability $1/2$ arises, that is, $Prob(c = 0) \leq 1/2 + \epsilon$ and $Prob(c = 1) \leq 1/2 + \epsilon$. Lo and Chau showed that there is no quantum coin flipping with bias 0. This is why many study of quantum coin flipping protocols which make bias as small as possible have been made so fan. However, QSS schemes can distribute only one secret, which is rather inconvenient. On the other hand, secret sharing schemes can distribute two or more secret the traditional.

In this paper, we propose both quantum coin flipping with n-dimensional quantum state and quantum multi-secret sharing scheme. Regarding as quantum coin flipping, we propose a quantum coin flipping protocol with n dimensional quantum states by generalizing the protocol with 3 dimensional quantum states by Ambainis. In our protocol, we can reduce the bias of one player arbitrarily by accepting the increase of the bias of the other player. Our generalized protocol could be applied to various situations. Regarding as quantum secret sharing schemes, we propose, for the first time, quantum multi-secret sharing schemes with a distinct secret by using MSP, and investigate conditions of which quantum multi-secret sharing schemes should satisfy. Furthermore, we give the theoretical evaluation of our proposal, and construct QSSS with two secret quantum states concretely.

Key Words: quantum security, coin flipping, secret sharing schemes