量子理論を用いた安全なプロトコルに関する研究

早稲田 篤志
北陸先端科学技術大学院大学

2007 年 1 月 5 日

論文の内容の要旨

量子セキュリティの分野の 1 つに量子コイン投げ (Quantum Coin Flipping) や量子秘密分散法 (Quantum Secret Sharing Scheme, QSSS) がある．量子コイン投げは 84 年に Bennett と Brassard により提案され，量子秘密分散法は，99 年に Hillery らによって初めて提案された．2 者間で行う量子コイン投げは，片方が不正を行うと，コイン投げの結果が c であると納得させられる確率に，$Prob(c = 0) \leq 1/2 + \epsilon$，$Prob(c = 1) \leq 1/2 + \epsilon$ という偏りが生じる．この ϵ をバイアスという．このバイアス ϵ について，いかなる不正を行なっても $\epsilon = 0$ とする理想的な量子コイン投げプロトコルは存在しないことが，Lo と Chau により示されている．そのため，ϵ を可能な限り小さくするようなプロトコルの提案が求められている．また，量子秘密分散法について現行のプロトコルは 1 つの秘密の分散を目標としており，複数の秘密を分散することはできない．一方，classical な秘密分散法には複数秘密を分散する複数秘密分散法が存在する．本論文では n 次元量子状態を使用する量子コイン投げと秘密の量子状態を複数持つ量子複数秘密分散法を提案する．量子コイン投げについては Ambainis により提案された 3 次元量子状態を持ちバイアスが 0.25 である量子コイン投げを拡張して実現する．そのため，まず n 次元量子状態の構成法を提案し，次にコイン投げプロトコルを提案する．次に，この提案プロトコルを解析し，片方のバイアスを犠牲にすることで，もう片方のバイアスを任意に小さくすることが可能であることを示す．これにより，様々な状況への適用が期待できる．また，量子複数秘密分散法について Smith によって提案された Monotone Span Programs (MSP) を用いた一般的な Access 構造をもつ量子秘密分散法に基づき，有資格集合に応じて異なる秘密情報が復元できる量子複数秘密分散法を初めて提案する．また，量子情報理論において量子複数秘密分散法が安全に構成されるために満たすべき条件を定義し，提案手法の理論的評価を行う．さらに，実際に秘密を 2 状態として量子複数秘密分散を構成する．この結果，MSP に用いた行列の条件を明確にし，理論的に量子複数秘密分散が構成可能であることを示す．

キーワード:　量子セキュリティ，コイン投げ，秘密分散法