Title	量子理論を用いた安全なプロトコルに関する研究
Author(s)	早稲田，篤志
Citation	
Issue Date	2007-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/3563
Rights	
Description	Supervisor:宮地　充子，情報科学研究科，博士

博 士 論 文

量子理論を用いた安全なプロトコルに関する研究

指導教官　宮地 充子 准教授

北陸先端科学技術大学院大学
情報科学研究科情報システム学専攻

早稲田 篤志

平成 19 年 3 月

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1984年にBennettとBrassard[8]により提案され，量子秘密分散法は，1999年にHilleryら[27]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$\epsilon$をバイアスという．このバイアス$\epsilon$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[32]．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[12]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[3]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[44]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．

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[8] 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[32]. 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.

目 次

図 目 次

表 目 次

第 1章

はじめに

昨今の情報漏洩事件や個人情報保護法などにより，セキュリティ技術への関心が高まっている．そのため，セキュリティ確保のための研究や商品開発は多くの研究機関，企業において重要な分野に位置付けられている．この機密情報を守るためのセキュリティ技術の歴史は，古く紀元前までさかのぼる．この時代のセキュリティ技術は秘密鍵暗号が中心であり，安全性も暗号化に使用する鍵のみならず，暗号化方式そのものをも秘匿することで守られていた．その後 1970 年代後半に Deffie と Hellman による公開鍵暗号の概念の提案，秘密鍵暗号 DES の暗号プロトコルの公開などがあり，現代暗号の研究が始められた．現代暗号には公開鍵暗号，秘密鍵暗号，電子署名やハッシュ関数，鍵共有法，認証法，秘密分散法や，これらの応用である電子投票や電子現金などが含まれる．現代暗号の特徴として，現行で使用されているコンピュータを用いて攻撃をかけたとき，解読が難しいという点が挙げられる．すなわち，これらの現在利用されている暗号の安全性は，素因数分解問題や離散対数問題，NP 完全問題などの計算量的困難性にその多くが依存しているといえる．しかし，量子コンピュータが実現されると，これらの問題のうち，素因数分解問題や離散対数問題は多項式時間で解読されることが証明されている．そこで，安全性の根拠を計算量的安全性ではなく，量子の物理的性質におく量子セキュリティの研究が盛んに行われている．なお，以降では量子状態を使用しないプロトコルについては classical なプロトコルと呼称する

1.1 量子セキュリティ

量子セキュリティは1970年代にWiesnerによってアイデアが提案されたことにより始まった．その後1980年代に入ってからBennettらにより再発見され，特に1984年にBennettらにより提案されたBB84プロトコル[8]はその後の研究の中心として，安全性評価や実験が行われている．このBB84プロトコルは2者間で鍵共有を行うプロトコルであり，盗聴者が存在するときは高確率で検知することができるプロトコルである．通信には光子を用い，プロトコルは以下のようになる．

1. Aliceは乱数bitの0(又は1)に対し，符号化$|0\rangle$か$|0'\rangle$(または$|1\rangle$か$|1'\rangle$)の偏光を持つ光子をBobに送る．
2. Bobは$|0\rangle$と$|1\rangle$を正しく測定できる基底か，$|0'\rangle$と$|1'\rangle$を正しく測定できる基底を選んで測定し，選んだ基底を公開する．ここで，正しく測定できない基底を選ぶと，Bobが選んだ基底のどちらかにランダムに変化する．
3. Aliceは正しく測定できる基底を選んだ光子がどれかを公開し，Bobはそれ以外の測定結果を破棄する．
4. 任意にk個の結果を選び，そのときの結果を比較する．一つでも結果が異なるものがあれば盗聴者が存在するものとして共有結果を破棄する．

量子には未知の量子状態のコピーを行うことができないという性質がある．そのため，盗聴者には通信に使用されている量子状態をコピーすることができない．加えて，正しい基底を選ばなかった場合について撹乱することなく量子測定を行うことも非常に困難であるという量子の性質が存在するため，高い確率で盗聴者の存在を検出することが可能となっている．このような特性はこれまでのプロトコルが持たなかったことから非常に注目され，通常量子暗号といえばこのBB84プロトコルを始めとした鍵共有法と，その共有鍵を使用したone time padの暗号の組み合わせを指す事が多い．

BB84以降は様々な現代暗号のプロトコルが量子状態を使用して再構成されている．BB84と同時に提案された量子コイン投げ(Quantum Coin Flipping)，1983年にWiesnerにより提示された量子紛失通信(Quantum ovlivious transfer)[51]，1999年にHilleryらにより量子秘密分散法(Quantum Secret Sharing Scheme, QSSS)[27]

が提案され，Barnum らによる量子メッセージ認証 [6]，Gu らによる量子パスワード [26] などが挙げられる．さらに，2000 年には量子計算機を暗号時や復号時に使用する岡本らの量子計算暗号 [38] の提案された．量子計算暗号は他の量子セキュリティと異なり，量子状態そのものは使用しない．そのため，他の量子セキュリティのプロトコルと違い，量子計算機における計算量的安全性が安全性の根拠となっている．一方，他の量子セキュリティプロトコルは量子原理を積極的に取り入れている．一般的に量子状態を使用したプロトコルは，classical なプロトコルが持たない，量子の物理的な性質を用いて安全性を定義できる．その結果，安全性を計算量で定義された classical なプロトコルよりも，安全なプロトコルを構成できる可能性がある．しかしながら，いまだ量子セキュリティに拡張することを行っていないプロトコルも存在する．より高度なセキュリティプロトコルを構成するためには，その構成要素となるプロトコルが量子状態で拡張されていることが重要である．

1.2 本論文の内容と成果

本論文では，これら量子セキュリティ技術のうち，量子コイン投げと量子秘密分散法についての研究を行った．これらは高度なセキュリティプロトコルを構成するときの基盤となるプロトコルであり，非常に重要である．

1.2.1 量子コイン投げ

量子コイン投げは Brassard らにより 1984 年に提案された [8]．この 2 者間で行なわれる量子コイン投げは，片方が不正を行うとコイン投げの結果を出す確率に偏り ϵ が生じる．この偏りをバイアスといい，このバイアス ϵ を 0 とする理想的なプロトコルは存在しないということが知られている [32]．そのため，このバイアス ϵ を可能な限り小さくするプロトコルが求められている．このとき，不正の方針によりコイン投げには 2 つの種類が存在する．両者が 1bit の共有情報を任意に操作しようとする strong 量子コイン投げと，コイン投げに勝とうとする weak 量子コイン投げである [3]．weak 量子コイン投げにおいては，負けるための不正について

は考慮しない．例えば，Spekkens らにより提案された weak 量子コイン投げプロトコルにおいて勝つために不正を行った場合，バイアス $\epsilon = 1/\sqrt{2} - 1/2$ となり，strong 量子コイン投げよりも小さいバイアスを実現している．しかしながら，負けるための不正を行った場合，その不正は確実に成功 (バイアス $\epsilon = 0.5$) するという問題がある．したがって，本論文ではこのうち strong 量子コイン投げを対象としたプロトコルを提案している．strong 量子コイン投げの例として，Ambainis により提案された量子コイン投げプロトコルが存在する [3]．Ambainis のプロトコルは 3 次元量子状態を使い，バイアス $\epsilon = 0.25$ を実現している．

本論文では，Ambainis の手法が 3 次元量子状態を使用していたのに対し，使用する量子状態を一般的な n 次元量子状態に拡張したプロトコルを提案する．このプロトコルを使用すると，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できることを示す．この結果から，提案プロトコルは様々な状況への適用が期待できる．また，両者のバイアスを均等にすると，Ambainis により提案されたプロトコルと同じバイアス $\epsilon = 0.25$ となるという結果が得られる．この結果は，Ambainis のプロトコルが提案プロトコルの特別な場合であることを示している．

1.2.2 量子秘密分散法

量子秘密分散法は 1999 年に Hillery らによって初めて提案された [27]．このプロトコルは HBB QSSS と呼ばれ，3 粒子以上の量子絡み合い状態である GHZ 状態を利用しており，分散情報を全て集めると復元が可能な満場一致法である．その後，Cleve ら [16] や Gottesman[23]，今井ら [28] によって量子秘密分散法に関する条件が考察された．さらに，Smith により提案された Monotone Span Programs (MSP) を用いた任意の Access 構造における量子秘密分散法 [44] や，Bandyopadhyay による量子テレポーテーションを用いた満場一致法 [5] など，多くの量子秘密分散法が提案されている [18, 37, 40]．このような量子秘密分散法は大きく 2 つに分けることができる．1 つは古典情報の秘密を，量子状態を用いて分散符号化するもので，BB84 プロトコルのように量子系の性質を使用して，古典的メッセージの分散符号化することを考えたものである．もう一つは，量子状態そのものを分散符号化する

ものである．後者の量子秘密分散法の目的は，実験結果や，量子コンピュータの演算結果，秘密通信の媒体などの，測定等が行われる前の重要な量子状態を分散共有することにある．このように，今後量子計算機などの発展により重要となるであろう量子状態の保存，分散共有に関して，量子秘密分散法は重要な研究分野であるといえる．しかしながら，classical な秘密分散法の持つ様々な機能について，量子秘密分散法には拡張されていないものが存在する．例を挙げると，classical な秘密分散法には複数の秘密を分散する複数秘密分散法 [12] が存在するが，複数の量子状態を分散させる量子複数秘密分散法はいまだ提案されていない．

本論文ではこの点に着目し，MSP を用いて有資格集合に応じて複数の異なる量子秘密状態を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の満たすべき条件を明らかにし，提案手法の理論的評価を行う．さらに，実際に秘密が量子 2 状態の量子複数秘密分散を構成する．これにより，MSP で用いる行列の条件を明らかにし，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．

1.3 本論文の構成

本論文の構成は以下の通りである．

まず，第 2 章では準備として，本論文で使用される記法及び諸定義などについて述べる．

第 3 章では既存研究として，提案プロトコルの基となった Ambainis の量子コイン投げプロトコルと，Smith の量子秘密分散法を中心に，量子コイン投げ，量子秘密分散プロトコルを紹介する．

第 4 章では量子コイン投げについて Ambainis の量子コイン投げを拡張し，n 次元量子状態を用いて構成した提案プロトコルを述べ，その評価を行う．

第 5 章では量子複数秘密分散法を定義したあと，Smith の量子秘密分散法を拡張した量子複数秘密分散法を提案し，理論的評価を行う．その後，2 つの秘密を持つ場合についての構成例を示す．

第 6 章ではこの研究の今後の展望を述べ，最後に第 7 章で結論を述べる．

第 2章

準備

本章では，準備として本論文における用語等の諸定義を行う．まず，2.1 で量子情報理論で使われる Dirac の記法についてまとめ，2.2 節で量子状態について定義を行い，2.3 節では量子計算機と量子アルゴリズムについて簡単に紹介する．

2.1 記法

まず，本論文で使用する Dirac の記法とそれに関連する記法について表 2.1 にまとめる．

2.2 量子状態

本節では，量子論における公理の紹介や状態に関する諸定義を行う．なお，用語等のより詳しい解説については，文献 [36] や [25] を参照されたい．

第一に，量子状態とそれが記述される系の持つべき性質について，公理を紹介する．

公理 1 任意の孤立した物理系に関して，系の状態空間と呼ぶ *Hilbert* 空間が存在する．系はその状態空間の単位ベクトルである状態ベクトルによって完全に記述される．

表 2.1: Dirac の記法とそれに関連する記法

$\mathbb{F}_q$	位数 q の有限体
$\mathbb{C}$	複素数
z^*	複素数 z の複素共役
$\mathcal{H}_A$	系 A に対するヒルベルト空間
$\|\psi\rangle$	列ベクトル．Ket とも呼ばれる．
$\langle\psi\|$	$\|\psi\rangle$ に双対なベクトル．Bra とも呼ばれる
$\langle\psi\|\phi\rangle$	$\|\psi\rangle$ と $\|\phi\rangle$ の内積
$\|\psi\rangle \otimes \|\phi\rangle$	$\|\psi\rangle$ と $\|\phi\rangle$ のテンソル積
$\|\psi\rangle\|\phi\rangle$	$\|\psi\rangle$ と $\|\phi\rangle$ のテンソル積の簡略記号
$\|\psi, \phi\rangle$	$\|\psi\rangle$ と $\|\phi\rangle$ のテンソル積の簡略記号
A^*	行列 A の複素共役
$A^\top$	行列 A の転置行列
$A^\dagger$	行列 A の Hermite 行列
$\langle\psi\|A\|\phi\rangle$	$\|\psi\rangle$ と $A\|\phi\rangle$ の内積
$Im(A)$	行列 A の像空間
$\mathrm{rank}(A)$	行列 A の階数
$\mathbb{F}_q^e$	$\mathbb{F}_q$ 上の要素を持つ e 次元行ベクトル
$\mathbf{e}_j$	j 列目の要素のみ 1 で, 他の要素が 0 の e 次元行ベクトル
I_R	系 R に対する恒等写像

最も簡単な系の例はqubitである．qubitは2次元量子空間を持ち，$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ と $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ がその状態空間の基底を構成する．このとき，任意のqubitの状態ベクトル $|\psi\rangle$ は $|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ で書くことができる．ここで $a, b \in \mathbb{C}$ であり，単位ベクトルであることから $|a|^2 + |b|^2 = 1$ である．このとき，$|\psi\rangle$ が単位ベクトルであるという条件 $\langle\psi|\psi\rangle$ を正規化条件という．

以下では状態の種類として，純粋状態と混合状態を紹介する．

純粋状態

n 次元 *Hilbert* 空間を $\mathcal{H}$ とすると，n 次元の純粋状態はノルムが *1* のベクトル $|\psi\rangle \in \mathcal{H}$ で表わされる．$|0\rangle, |1\rangle, \cdots, |n-1\rangle$ を $\mathcal{H}$ の正規直交基底としたとき，任意の純粋状態は $|\psi\rangle = \sum_{i=0}^{n-1} a_i|i\rangle$ $(a_i \in \mathbb{C})$ で与えられる．また $|\psi\rangle$ はノルムが *1* なので，$\sum_i |a_i|^2 = 1$ である．

混合状態

混合状態は純粋状態 $|\psi_i\rangle$ の確率分布 $(p_i, |\psi_i\rangle), 0 \leq p_i \leq 1, \sum_i p_i = 1$ で与えられ，量子状態は確率 p_i で $|\psi_i\rangle$ となる．また，混合状態は密度演算子 $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ によっても記述できる．

第2の公理として，量子状態の変化について紹介する．

公理 2 閉じた量子系の時間発展はユニタリ変換で記述される．このことをユニタリ発展という．純粋状態 $|\psi\rangle$ が U でユニタリ発展した場合は，$U|\psi\rangle$ となる．また，密度行列 ρ が U でユニタリ発展した場合は，$U\rho U^\dagger$ となる．

同様にqubitの例で説明する．ある時間 t_0 で $|\psi_{t_0}\rangle = a|0\rangle + b|1\rangle$ であった量子状態について，この量子状態が時間 t_1 で量子回路において量子ゲートの一つであるHadamardゲートを通ったと仮定する．このとき，Hadamardゲートを表すユニタリ行列 H は以下で表される．

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

この行列は Hadamard 行列と呼ばれる．このとき，時間 t_1 での量子状態は以下のようになる．

$$\begin{aligned} |\psi_{t_1}\rangle &= H|\psi_{t_0}\rangle \\ &= \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle. \end{aligned}$$

Hadamard 変換以外の重要な例として，qubit に対する量子ゲートである Pauli の X 行列，Z 行列などがある．それぞれ以下のような行列であり，また，Pauli の X 行列は bit 反転行列，Z 行列は位相反転行列とも呼ばれる．

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

さらに，重要な量子操作に関する定理として，no-cloning 定理がある．

no-cloning 定理

未知の量子状態 $|\phi\rangle$ について，完全に同じ量子状態を複製する量子操作は存在しない．

これらは 1qubit に対する操作であるが，2 つ以上の系にまたがる量子操作としては，部分トレース演算や純粋化などが存在する．それらを紹介する前に，2 つ以上の系にまたがる量子状態を記述するための公理を紹介する．

公理 3 複合物理系の状態空間は，その複合系を構成する物理系の状態空間のテンソル積で与えられる．さらに，i 番目の系の状態が $|\psi_i\rangle$ であるとき，これらを要素とする系の状態は $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ となる．また，i 番目の系の状態が密度行列 ρ_i であるとき，これらを要素とする系の状態は $\rho_1 \otimes \cdots \otimes \rho_n$ となる．

系が 2 つにまたがる量子操作として，縮約密度演算子，純粋化を紹介する．

縮約密度演算子

系 A と B からなる量子状態の密度演算子を ρ^{AB} とする．この量子状態に対し，系 A の縮約密度演算子は $\rho^A = \mathrm{Tr}_B(\rho^{AB})$ で定義される．ただし，Tr_B は系 B 上の部分トレースと呼ばれ，系 B の次元を N_B，正規直交基底を $|\phi_j\rangle$ とし，系 A の恒等写像を I_A とすると，$\mathrm{Tr}_B\,\rho^{AB}$ は $\mathrm{Tr}_B\,\rho^{AB} = \sum_{j=1}^{N_B}(I_A \otimes \langle\phi_j|)\rho^{AB}(I_A \otimes |\phi_j\rangle)$ で定義される．

純粋化

系 A における密度演算子 ρ^A に対し，$\rho^A = \mathrm{Tr}_R(|RA\rangle\langle RA|)$ を満たすような，系 A と補助系 R からなる純粋状態 $|RA\rangle$ を求める操作を純粋化という．系 A の正規直交基底 $|i^A\rangle$，ρ^A の正規直交分解 $\rho^A = \sum p_i |i^A\rangle\langle i^A|$，$A$ と同じ状態空間 R の正規直交基底 $|i^R\rangle$ としたとき，ρ^A の純粋化は $|\psi\rangle = \sum \sqrt{p_i}|i^R\rangle|i^A\rangle$ で与えられる．

また，公理 3 により，量子論でもっとも興味深い現象である絡み合い状態について定義できる．

絡み合い状態

Hilbert 空間 $\mathcal{H}$ における純粋状態が，それより小さな次元を持つ *Hilbelt* 空間の *2* つの量子状態のテンソル積として与えられないとき，その状態は絡み合っているという．また，$\mathcal{H}^A \otimes \mathcal{H}^B$ からなる絡み合い状態 $|\phi\rangle$ の絡み合いの尺度 $E(\phi)$ は，ρ を $|\phi\rangle$ の密度演算子とすると，*von Neumann* エントロピーの概念を用いて $E(\phi) = -\mathrm{Tr}\,\rho^A \log \rho^A = -\mathrm{Tr}\,\rho^B \log \rho^B$ で与えられる．特に，*2* 量子の最大絡み合い状態を *EPR* 状態，又はベル状態といい，*3* 量子以上の最大絡み合い状態を *GHZ* 状態という．

第 4 の公理は，量子状態の測定に関する公理である．

公理 4 量子測定は測定作用素の集合 $\{M_m\}$ で記述される．m は実験で生じる測定結果を表す．量子状態 $|\psi\rangle$ を測定した場合に結果 m が得られる確率 $p(m)$ は，$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ で以下で表される．このとき，測定後の系の状態は以下のようになる．

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}.$$

また，確率の総和は *1* であることから，測定作用素について完全性の式 $\sum_m M_m^\dagger M_m = I$ を満たす．

また，量子状態として密度演算子 ρ を測定した場合，測定結果 m が得られる確率 $p(m)$ は $p(m) = \mathrm{Tr}(M_m^\dagger M_m \rho)$ であり，測定後の系の状態は以下のようになる．

$$\frac{M_m \rho M_m^\dagger}{\sqrt{\mathrm{Tr}(M_m^\dagger M_m \rho)}}.$$

同様に，1qubit の量子状態に対して測定を行ったときの例を述べる．量子状態 $|\psi\rangle = a|0\rangle + b|1\rangle$ に対し，それぞれの基底方向で測定するため，$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$，$M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ の 2 つの測定作用素を定義する．この 2 つの作用素が完全性の式を満たしていることは容易に確かめられる．このとき，測定結果 0 を得られる確率 $p(0)$ と測定後の状態は，それぞれ以下のようになる．

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = \begin{pmatrix} a^* & b^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2.$$

$$\text{測定後の状態}: \frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle.$$

同様に，測定結果 1 を得られる確率 $p(1)$ と測定後の状態は，それぞれ以下のようになる．

$$p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle = \begin{pmatrix} a^* & b^* \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |b|^2.$$

$$\text{測定後の状態}: \frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle.$$

量子測定のついて，よく使用される測定に POVM(positive operator-valued measure) がある．POVM は完全性の式 $\sum_m E_m = I$ と，$p(m) = \langle\psi|E_m|\psi\rangle$ となる正値演算子集合 $\{E_m\}$ で定義される測定である．このとき $M_m = \sqrt{E_m}$ とすることで測定の公理を満たす．この測定は測定結果の確率に興味がある場合に有効であり，例えば，2 つの非直交状態を正確に識別することは通常では不可能であるが，POVM を使用することで，識別することができた場合には必ず正しいような測定を実現できる．

以上で，量子力学における基本公理 4 つと，それらに直接関係のある用語を定義した．以降ではこれらの公理から導かれる用語として，忠実度と von Neumann エントロピー，アクセシブル情報量を紹介する．

忠実度

忠実度は，2 つの状態 ρ^A と ρ^B の間の距離の尺度である．ここで，ρ^A と ρ^B の間の忠実度を $F(\rho^A, \rho^B)$ と表す．

さらに，忠実度について以下の二つの補題が知られている．

補題 1 [2, 33] 拡大空間 $H \otimes K$ の状態 $|\psi^A\rangle$ と $|\psi^B\rangle$ から，系 K の状態を部分トレースで取り除いた状態を，それぞれ ρ^A と ρ^B とする．このとき $\rho^A = \rho^B$ ならば，系 K の状態を変換することで，$|\psi^A\rangle$ を $|\psi^B\rangle$ に変換することができる．

補題 2 [50]

$$F(\rho^A, \rho^B) = \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho^A}\rho^B\sqrt{\rho^A}}\right)\right)^2.$$

von Neumann エントロピー

系 A における量子状態 ρ^A に対する *von Neumann* エントロピーは，$S(A) = S(\rho^A) = -\mathrm{Tr}(\rho^A \log \rho^A)$ で定義される．また，$\{\lambda_i\}$ を ρ^A の固有値とすると，*von Neumann* エントロピーは $S(\rho^A) = -\sum_i \lambda_i \log \lambda_i$ と定義することができる．ただし，$0 \log 0 = 0$ とする．

この von Neumann エントロピーの基本的性質を以下に述べる．

- エントロピーは非負である．また，エントロピーが 0 になるのは純粋状態のときのみ，かつそのときに限る．
- 結合系 AB で純粋状態であるとき，それぞれの系のエントロピーについて $S(A) = S(B)$ が成り立つ．

さらに，結合系における結合エントロピーや，条件付エントロピー，相互情報量はそれぞれ以下のように定義される．

- 系 A, B の結合エントロピーは，結合系 AB の量子状態を ρ^{AB} としたとき，$S(A, B) = -\mathrm{Tr}(\rho^{AB} \log \rho^{AB})$ で定義される．
- 系 B について分かっているときの系 A のエントロピーを条件付エントロピーといい，$S(A|B) = S(A, B) - S(B)$ で定義される．
- 系 A と B が共通にもつ情報量の尺度を相互情報量といい，$I(A : B) = S(A) + S(B) - S(A, B)$ で定義される．

アクセシブル情報量

情報源を固定したとき，量子測定過程を通して得られる最大情報量を，アクセシブル情報量という．このアクセシブル情報量の上限 m は，以下の *Holevo* 限界の定理により与えられる．

定理 1 （*Holevo* 限界）

$$m \leq S(\rho) - \sum_i p_i S(\rho_i) \tag{2.1}$$

2.3 量子計算機と量子アルゴリズム

量子計算機の数学的モデルである量子 Turing 機械は，1985 年に Deutsch により提案された [19]．通常の計算機が 0 か 1 かのどちらかしか採らない bit を使用するのに対し，量子計算機では 0 と 1 を任意の重ね合わせ状態で保持することができる量子 bit(qubit) を使用している．その後，1994 年に Shor のアルゴリズムが提案された [43] ことで，量子計算機実現のための研究が各所で行われている．量子計算機の実現方法としては，イオントラップ，NMR（核磁気共鳴，Nuclear Magnetic Resonance），量子ドットなどを使用したものがある．しかしながら，いずれも数 qubit の量子計算機に過ぎず，実用化にはまだ時間がかかるものと思われる．このような量子計算機を使用した量子アルゴリズムとしては，Shor のアルゴリズムと Grover のアルゴリズム [24] が有名である．Grover のアルゴリズムはデータベース検索のアルゴリズムであり，整列されていないデータ数 N のデータベースから，目的の項目を $O(\sqrt{N})$ で抽出するアルゴリズムである．Shor のアルゴリズムは素因数分解問題と離散対数問題を効率的に解くアルゴリズムである．これらの問題は多くのセキュリティプロトコルが安全性の根拠としていたため，量子計算機が注目を集めることになった．Shor のアルゴリズムについて，NMR を利用した量子計算機を用いて，7qubit で 15 の素因数分解に成功しているという事実があり，Shor のアルゴリズムが原理的に正しいことが証明されている．しかしながら，現実に使用されている暗号は 1024bit 長の合成数に対する素因数分解を安全性の根拠としており，現在実現している量子計算機の規模では脅威となりえない．

この量子計算機を導入した量子セキュリティとしては，量子計算暗号 [38] が存在する．量子計算暗号は暗号化や復号時に量子計算機を使用することを前提とし

た暗号である．

2.4 classical なプロトコル

2.4.1 共通鍵暗号

メッセージ秘匿を行う暗号方式の一つで，メッセージの送信者と受信者の持つ鍵が共通，又は片方の鍵からもう片方の鍵が容易に類推可能な暗号化方式である．同じくメッセージ秘匿を行う方法である公開鍵暗号に比べて，暗号化を高速に行えるという利点が存在する．その反面，送信相手ごとに鍵を持つ必要があるため，鍵の所有数が膨大になるという欠点が存在する．共通鍵暗号方式としては，ブロック暗号の RC6 や DES, AES，ストリーム暗号として RC4，one time pad といったものが存在する．量子原理を導入した共通鍵暗号としては Y-00[53] が存在する．

one time pad

one time pad は暗号化に使用する鍵を一回限りの使い捨てにする方法である．この場合は，情報理論的に安全であることが証明されているため，絶対に安全な方式ということができる．しかしながら，one time pad を使用するためには，互いに鍵として同じ乱数列を秘密に保持しなければならないという問題点が存在する．そこで，同じく量子原理に基づき盗聴を検出できる量子鍵共有を用いることで，絶対に安全な量子暗号を実現している．

2.4.2 公開鍵暗号

メッセージ秘匿を行う暗号方式の一つで，復号時に使用する秘密鍵が，暗号化に使用する鍵から容易に類推できない構成することで，暗号時に使用する鍵を公開鍵簿のようなもので公開することができる方式である．秘密鍵暗号が通信相手ごとに異なる鍵を秘密に保存しなければならなかったのに対し，公開鍵暗号では秘密に保持する鍵が自分の秘密鍵のみとなる利点がある．また，公開鍵暗号におけるプロトコルは，素因数分解問題や離散対数問題といった，計算機を用いて効

率的に解くアルゴリズムが見つかっていない数学上の問題を安全性の根拠としているものが多い．この素因数分解や離散対数問題は，量子計算機上で実行されるShor のアルゴリズムにより，効率的に解けることが分かっているため，量子計算機の実現に向けた研究が広く行われている．素因数分解問題ベースの公開鍵暗号としてはRSA 暗号やラビン暗号が，離散対数問題ベースのものとしてはElGamal暗号や楕円曲線暗号といったものが存在する．以下でRSA 暗号を紹介する．

鍵生成

1. 素数 p, q を選ぶ．$n = pq$ とする．λ_n =LCM$(p-1)(q-1)$ を計算する．
2. $e \in \mathbb{Z}/\lambda_n\mathbb{Z}$ を選び，$d = 1/e \pmod{\lambda_n}$ を計算する．
3. d を秘密鍵とし，e, n を公開鍵として公開する．

暗号化

1. 暗号化する平文を M とする．
2. $C = M^e \pmod{n}$ を計算し，C を暗号文として送信

復号

1. 暗号文 C を受け取る．
2. $M = C^d \pmod{n}$ を計算する．M が復元された平文である．

2.4.3 認証プロトコル

対象が正規のものであるかを確認するプロトコルであり，対象のものがユーザであるユーザ認証，メッセージであるメッセージ認証，クライアントであるクライアント認証などが存在する．これらの認証を電子データで行う場合，電子データは容易にコピーや改ざんが可能であることから，正規のもののみが知っている情報を使用し，同時に乱数を用いて認証を行うことが多い．この正規のもののみが知っている情報には，共通鍵暗号や公開鍵暗号の秘密鍵やパスワードなどが挙げられる．ここでは，最も簡単な共通鍵暗号を用いた認証方式を示す.

1. 検証者は乱数 r を生成し，認証者に送信.

2. 認証者はあらかじめ共有した鍵 K を用いて暗号化し，暗号文 $X = E_K(r)$ を検証者に送信.
3. 検証者は r を暗号化し，X となることを確認

量子認証方式としては，メッセージ認証として Howard らにより提案された手法 [6]，パスワード認証として Weedbrook らにより提案された手法 [26] などが存在する．

パスワード認証プロトコル

認証プロトコルのうち，正規のユーザのみが知っている情報としてパスワードを用いるものをパスワード認証プロトコルをいう．このパスワード認証プロトコルはコンピュータへのログイン時に利用されるだけではなく，銀行の ATM での暗証番号などもその一種であり，現在もっとも普及しているセキュリティプロトコルの一つである．通常パスワードは意味のある文字列であることから，その採りうるパスワードの集合を辞書といい，パスワードは検証者側において，一方向性関数などで暗号化されてデータベースに格納される．通常の認証において安全性を議論する場合，総当り攻撃よりも少ない計算量で攻撃ができたときに攻撃成功という．しかしながら，パスワード認証の場合は通常の認証と違い，総当り攻撃よりも効率の良い攻撃である辞書攻撃が可能である．辞書攻撃は辞書にある単語についてすべて暗号化し，そのデータが格納されているデータベースと比較することで行う攻撃をいう．したがって，この辞書攻撃よりも少ない計算量で攻撃ができたときに，攻撃成功といわれる．

2.4.4 鍵共有法

秘密鍵暗号などを使用するためには，事前に互いに鍵を共有しておかなければならない．この方法を鍵共有法という．方式としては Deffie-Hellman の鍵共有法などが挙げられる．以下で Deffile-Hellman の鍵共有法について記載する．

1. システムパラメータとして，素数 p とその乗法群 $(\mathbb{Z}/p\mathbb{Z})^*$，元 $g \in (\mathbb{Z}/p\mathbb{Z})^*$ を選び，公開する．

2. A は乱数 $x \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ を選び，$a = g^x \bmod p$ を計算し B へ送信.
3. B は乱数 $y \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ を選び，$b = g^y \bmod p$ を計算し A へ送信.
4. A は B から送られてきた b に対し，$k_A = b^x = g^{xy} \bmod p$ を計算し，k_A を共有鍵とする.
5. B は A から送られてきた a に対し，$k_B = a^y = g^{xy} \bmod p$ を計算し，k_B を共有鍵とする.

しかしながら，これらの方法は共有相手について認証等を行わないため，共有相手に成りすました攻撃者と共有を行ってしまう可能性が存在する．そこで，相手認証と組み合わせて使用することが一般的である．パスワード認証付き鍵共有法 (PAKE)[7, 1] などがその例として挙げられる．これらに量子原理を取り入れた量子鍵共有法としては，BB84[8] を始めとして数多く存在する．特に BB84 プロトコルは量子セキュリティのプロトコルとしては非常に有名であり，量子物理学の原理を利用して，盗聴を高確率で検出できるプロトコルとして注目を浴びている．しかし，これらと認証技術を効率的に組み合わせた方法は，いまだ提案されていない.

2.4.5 分散復号

公開鍵暗号を組織等で使用する場合，その組織宛てに送られた暗号文は，秘密鍵を持つ唯一人の人により復元されてしまう．これを防ぐための手段の一つとして，秘密分散法を利用した分散復号が存在する．この手法は，暗号文を復号するために使用する秘密鍵を複数のシェアに分割し，復号時においてはシェアを利用することで，秘密鍵そのものを復元することなく，暗号文の復号を行うプロトコルである．RSA 暗号の秘密鍵を N 人に分散し，N 人全員が集まると復号ができる RSA 分散復号は以下のようになる.

鍵生成

1. 素数 p, q を選ぶ．$n = pq$ とする．$\lambda_n =$LCM$(p-1)(q-1)$ を計算する.
2. $e \in \mathbb{Z}/\lambda_n\mathbb{Z}$ を選び，$d = 1/e \pmod{\lambda_n}$ を計算する.
3. $d = \sum_{i=1}^{N} d_i \pmod{\lambda_n}$ を計算し，d_i を各人の秘密鍵とし，e, n を公開鍵として公開する.

暗号化

1. 暗号化する平文を M とする．
2. $C = M^e \pmod{n}$ を計算し，C を暗号文として送信

復号

1. 暗号文 C を受け取る．
2. $M_i = C^{d_i} \pmod{n}$ を計算する．
3. $M = \prod i = 1^N M_i \pmod{n}$ を計算する．M が復元された平文である．

第 3章

既存研究

本章では，量子セキュリティのうち，研究の対象とした量子コイン投げと量子秘密分散法の既存研究について述べる

3.1 量子コイン投げ

3.1.1 概略

コイン投げプロトコルは離れた 2 者が電話などの通信手段を使用して，直接顔を合わすことなく情報の共有を行うプロトコルであり，マルチパーティプロトコルの一種に数えられる．実際のプロトコルは 1982 年に Blum により提案され [11]，以降暗号プロトコルのプリミティブとして研究が行われてきている [15]．コイン投げプロトコルについて，量子状態を使用して実現した量子コイン投げプロトコルは Brassard らにより 1984 年に提案され，このプロトコルは BB84 プロトコルとして知られている [8]．量子コイン投げは Strong と weak の 2 つが存在する．以下で，それらを定義する．

定義 1 *[3]*(**Strong Coin Flipping**)
バイアス ϵ をもつ，*strong* 量子コイン投げプロトコルとは，*Alice* と *Bob* の *2* 者間で通信を行い，以下を満たすような値 $c \in \{0, 1\}$ を互いに合意することである．

- *Alice* と *Bob* がともに正直な（プロトコルに従う）場合，その確率は $Prob(c = 0) = Prob(c = 1) = 1/2$ を満たす．

- 片方のみが正直で，もう片方が不正を行う場合，確率は $Prob(c=0) \leq 1/2+\epsilon, Prob(c=1) \leq 1/2+\epsilon$ で与えられる．この ϵ をバイアスという．

定義 2 (Weak Coin Flipping)
バイアス ϵ をもつ，*weak* 量子コイン投げプロトコルとは，*Alice* と *Bob* の 2 者間で通信を行い，以下を満たすような値 $c \in \{0,1\}$ を互いに合意することである．

- *Alice* と *Bob* がともに正直な（プロトコルに従う）場合，その確率は $Prob(c=0) = Prob(c=1) = 1/2$ を満たす．
- *Bob* が正直で，*Alice* が不正を行う場合，確率は $Prob(c=0) \leq 1/2+\epsilon$ で与えられる．
- *Alice* が正直で，*Bob* が不正を行う場合，確率は $Prob(c=1) \leq 1/2+\epsilon$ で与えられる．

以上の様に，weak コイン投げを strong 量子コイン投げと比較すると，Alice が不正をして $c=1$ に，Bob が不正をして $c=0$ とする場合については考慮しないという違いがあり，例えば，Spekkens らにより提案された weak 量子コイン投げ [46] では，weak コイン投げで考慮していない Alice が不正をして $c=1$ にする場合と，Bob が不正をして $c=0$ にする場合は，その不正成功確率は 1，すなわちそのバイアスは $\epsilon = 0.5$ となる．

また，量子コイン投げにおけるバイアス ϵ については，Lo と Chau により，$\epsilon = 0$ とする完全な量子コイン投げプロトコルは存在しないことが証明されている [32]．そこで，このバイアス ϵ を可能な限り小さくするプロトコルが求められている．その代表的な例として，strong コイン投げに対しては，Ambainis[3]，Colbeck[17] により提案された方法が，weak コイン投げの例としては Spekkens ら [46]，Mochon[35] により提案されたプロトコルなどが存在する．weak 量子コイン投げの例である Spekkens らによる方法と，Mochon により提案された方法のそれぞれのバイアスは $1/\sqrt{2}-1/2$，0.192 となっている．対して，strong 量子コイン投げについては，Ambainis や Colbeck により提案された手法などが存在する．これら 2 つのプロトコルのバイアスは $\epsilon = 0.25$ である．Colbeck のプロトコルは量子絡み合い状態を 2 状態使用したプロトコルである．実現の観点から見ると，量子絡み合い状態は利

用しないほうが望ましい．そこで，本研究では Ambainis のプロトコルは本論文で基とした strong 量子コイン投げプロトコルを提案する．

ここで，strong 量子コイン投げについて知られている定理について述べる．まず，Alice が不正を行い出力を $a \in \{0,1\}$ にできる確率を p_{a*}，Bob が不正を行い出力を $b \in \{0,1\}$ にできる確率を p_{*b} とする．このとき strong 量子コイン投げの定義から，$p_{a*} \leq \frac{1}{2} + \epsilon$，$p_{*b} \leq \frac{1}{2} + \epsilon$ が成り立つ．以上を使うと次の定理と系が成り立つ．

定理 2 *[31]*

$$p_{a*}p_{*b} \geq p_{ab}$$

系 1 *[31] strong* 量子コイン投げにおいて $\epsilon < 1/\sqrt{2} - 1/2$ とすることは不可能である．

系 1 を言い換えると，strong 量子コイン投げにおけるバイアスの理論的な下限は $1/\sqrt{2} - 1/2$ であるといえる．ここで，Ambainis や Colbeck により提案されたプロトコルはこの理論的な下限値に最も近いプロトコルであり，これより小さいバイアスを実現した strong 量子コイン投げプロトコルは知られていない．また，量子版に限らず，コイン投げプロトコルはビットコミットメントプロトコルを使用し，Alice の選んだ情報に対するコミットメントを証拠として送信することにより実現することが多い．しかしながら，この strong 量子コイン投げのバイアスの理論的な下限は，量子ビットコミットメントを使用した量子コイン投げでは実現できないことも知られている [45].

3.1.2 Ambainis の strong 量子コイン投げプロトコル

この節では，既存の量子コイン投げプロトコルとして Ambainis により提案された，bias $\epsilon = 0.25$ を持つ strong 量子コイン投げ [3] を紹介し，それを基にした 4 次元量子状態を使用したプロトコル [21] を紹介する．

まず，Ambainis により提案されたプロトコルを紹介する．このプロトコルにお

いて使用する 3 次元量子状態を紹介する．

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \cdots \ b=0, x=0, \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \cdots \ b=0, x=1, \\ \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle) & \cdots \ b=1, x=0, \\ \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) & \cdots \ b=1, x=1. \end{cases} \tag{3.1}$$

この量子状態を使用した量子コイン投げは，以下のようになる．

1. Alice は，$b, x \in \{0,1\}$ をランダムに選び，状態 $|\phi_{b,x}\rangle$ を Bob に送る．
2. Bob は，ランダムに $b' \in \{0,1\}$ を選び，Alice に送る．
3. Alice は，b, x を Bob に送る．
4. Bob は，(1) で受け取った状態 $|\phi_{b,x}\rangle$ が正しいものかを観測する．もし正しく観測できなければ，Alice が不正を行なったと判断し，プロトコルを停止する．
5. 正しく観測できたなら，$c = b \oplus b'$ をコイン投げの結果とする．

このプロトコルの bias は 0.25 であり，提案されているプロトコルとしては strong 量子コイン投げにおける理論的下限値 $1/\sqrt{2} - 1/2 \approx 0.20$ に最も近いプロトコルとなる．

Ambainis のプロトコルを基に，$|3\rangle$ を付け加えることで 4 次元量子状態を構成した量子コイン投げとしては，以下のものがあげられる [21]．

$$|\psi_{b,x,y}\rangle = \begin{cases} \sqrt{\frac{2}{3}}|\phi_{b,x}\rangle + \sqrt{\frac{1}{3}}|3\rangle & \cdots \ y=0, \\ \sqrt{\frac{2}{3}}|\phi_{b,x}\rangle - \sqrt{\frac{1}{3}}|3\rangle & \cdots \ y=1. \end{cases} \tag{3.2}$$

ここで，$|\phi_{b,x}\rangle$ は Ambainis により提案された量子状態である．このケースで Alice が不正を行なった場合の Alice のバイアス ϵ_{Alice} と，Bob が不正を行なった場合の Bob のバイアス ϵ_{Bob} を計算すると，$\epsilon_{Alice} = 1/3$ と $\epsilon_{Bob} = 1/6$ となり，Alice 側にバイアスが偏ることが分かっている．

3.1.3 Colbeck の strong 量子コイン投げプロトコル

この節では，Colbeck による strong 量子コイン投げプロトコル [17] を紹介する．このコイン投げは 2 者間で行い，量子絡み合い状態である EPR 状態を 2 つ使用している．

1. Alice は，$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ を 2 つ生成し，各々の 2qubit 目を Bob に送る．
2. Bob は，送られた 2 つの状態からランダムに片方を選び，Alice に送信.
3. Alice と Bob は選ばれた方の状態を $\{|0\rangle, |1\rangle\}$ 基底で測定し，その結果をコイン投げの結果とする.
4. Alice は選ばれなかった方の量子状態を Bob に送信.
5. Bob は，$|\phi\rangle$ であることをチェックする．失敗した場合は Alice が不正を行なったと判断し，プロトコルを停止する．

このプロトコルの bias はそれぞれ $\epsilon = 0.25$ を実現していて，Ambainis のプロトコルと同じく，strong 量子コイン投げにおける最も良い bias を実現したプロトコルである．

3.1.4 Spekkens らによる weak 量子コイン投げプロトコル

本節では，Spekkens らにより提案された量子コイン投げプロトコル [46] を紹介する．本プロトコルは Ambainis や Colbeck のプロトコルと異なる weak 量子コイン投げプロトコルであり，量子絡み合い状態を使用している．

1. Alice は，$|\phi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$ である量子絡み合い状態を生成し，系 B を Bob に送る．
2. Bob は，系 B を POVM において測定作用素 $\{E_0, E_1\}$ で測定し，測定結果 b を公開する．
3. $b = 0$ なら Bob は Alice に系 B の状態を送り返す．$b = 1$ なら Alice は Bob に系 A の量子状態を送信する．
4. 量子状態を受け取った側は $\{|\psi_b\rangle\langle\psi_b|, I - |\psi_b\rangle\langle\psi_b|\}$ で測定する．ただし，$|\psi_b\rangle = I \otimes \sqrt{E_b}|\psi\rangle / \sqrt{\langle\psi_b|I \otimes E_b|\psi_b\rangle}$ である．
   (a) $b = 0$ で，Alice が $|\psi_0\rangle\langle\psi_0|$ が得られたなら，Bob の勝利.
   (b) $b = 0$ で，Alice が $I - |\psi_0\rangle\langle\psi_0|$ が得られたなら，Bob が不正を行ったと判断して，プロトコルを停止.
   (c) $b = 1$ で，Bob が $|\psi_1\rangle\langle\psi_1|$ が得られたなら，Alice の勝利.
   (d) $b = 1$ で，Bob が $I - |\psi_1\rangle\langle\psi_1|$ が得られたなら，Alice が不正を行ったと判断

して，プロトコルを停止.

このプロトコルの bias は $\epsilon = 1/\sqrt{2} - 1/2 \approx 0.20$ であり，Ambainis や Colbeck のプロトコルよりも小さい bias となっている．しかしながら，このプロトコルは weak コイン投げであるので，敗北するための不正は確率 1 で行うことができる．すなわち，Alice が意図的に負けようとする場合は，1. で $p(1) = \langle\psi'|E_0|\psi'\rangle = 1$ となるような状態を送信することで，Bob が意図的に負けようとする場合は，2. において $b = 1$ と公開し，4. において測定を行わずに $|\psi_1\rangle\langle\psi_1|$ が得られたとすることで実現できる．このとき，不正を検知することはできないという相違点がある．

3.2 量子秘密分散法

3.2.1 概略

秘密分散法とは，秘密情報 S の分散情報であるシェアを参加者の集合 $\mathcal{P}$ に配布し，有資格集合の参加者のシェアを集めると秘密 S が復元でき，禁止集合の参加者のシェアでは S に関する情報が一切洩れない符号化方式をいい，1979 年に Shamir[42] と Blakley[9] により独立に提案された．ここで有資格集合の族を Access 構造 Γ，禁止集合の族を Adversary 構造 $\mathcal{A}$ といい，定義より $\Gamma \cap \mathcal{A} = \emptyset$ である．また，$\Gamma \cup \mathcal{A} = 2^{\mathcal{P}}$ であるとき，その秘密分散法は完全であるという．秘密分散法には様々な分類が存在する．アクセス構造における分類としては以下が挙げられる．

- (t, n) 閾値法:n 個のシェアのうち，任意の t 個のシェアで秘密が復元できる [42].
- 満場一致法:n 個のシェアのうち，n 個すべて集めなければ秘密を復元できない [42].

また，その他に追加できる機能として以下のようなものがある．

- 閾値変更:(t, n) 閾値法における閾値 t を分散後に変更できる [47].
- 複数秘密:同時に分散符号化できる秘密の数を複数個にする [12].

- 検証可能:各参加者が正しく計算されたシェアを用いて，正しく復元手続きを行っていることを検証できる [14].

- Ramp 型:秘密の情報を一部漏洩させることで，分散効率を上げる [10].

秘密分散法に対して，量子状態を使用した量子秘密分散法は 1999 年に Hillery らにより提案された [27]．この方法では秘密である量子状態を GHZ 状態を用いて分散した満場一致法を実現している．同年に Cleve らにより (t, n) 閾値法 [16]，2000 年に Smith により以下の定理 3 を満たす任意のアクセス構造を持つ量子秘密分散法 [44] が提案されている．一方，追加機能において量子秘密分散法への拡張がなされているものは，Ramp 型スキーム [37] や検証可能 [18] があり，閾値変更や複数秘密などの機能を持った量子秘密分散法は実現されていない．

量子秘密分散法では量子論からの制約により，秘密分散を構成できるアクセス構造に制限がある．

定理 3 *[23]* アクセス構造 Γ が *monotone* 性を持ち，かつ *no-cloning* 定理を満たすとき，かつそのときに限り，アクセス構造が Γ となる量子秘密分散法が存在する．

この定理を (t, n) 閾値法に当てはめると以下の系が得られる．

系 2 *[27]* $n \geq 2t$ となる (t, n) 閾値量子秘密分散法は存在しない．

次に，秘密分散法の構成で利用される Monotone Span Program[44] について述べる．まず，$\mathbb{F}_q$ を位数 q の有限体とする．集合 $\mathcal{P}$ 上における Monotone Function f とは，$2^{\mathcal{P}}$ から $\{0, 1\}$ への関数であり，$A \subseteq B \Rightarrow f(A) \leq f(B)$ を満たす関数である．以上から Span Program[29] について定義する．

定義 3 リテラル[1]の集合 $\mathcal{P}$ 上の *Span Program* とは，位数 q の有限体 $\mathbb{F}_q$，$\mathbb{F}_q$ 上の $d \times e$ 行列 M，M の行を割り振る関数 $g : \{1, \cdots, d\} \to \{x_i^j | x_i \in \mathcal{P}, j \in \{0, 1\}\}$，ある与えられた非零のベクトル $\mathbf{e} \in \mathbb{F}_q^e \setminus \mathbf{0}$ の四つ組 $(\mathbb{F}_q, M, g, \mathbf{e})$ で定義される．ここで任意の $x_i \in \mathcal{P}$ について，$x_i^1 = x_i, x_i^0 = \overline{x_i}$ とし，$\mathbf{0}$ は零ベクトルとする．ある入力 $A \subseteq \mathcal{P}$ が与えられたとき，M のある k 行目について，*(1)* $g(k) = x_i$ かつ

[1]命題変数，あるいはその否定.

$x_i \in A$，あるいは，*(2)* $g(k) = \overline{x_i}$ かつ $x_i \notin A$ であるとする．このような行からなる M の部分行列を M_A とする．

このとき，*Span Program* が受理するとは，$\mathbf{e}$ が M_A により生成される部分空間に含まれることをいう．

また，g のすべての像が正のリテラルであるとき，Span Program は monotone であるという．f を Monotone Function とし，任意の $\emptyset \neq A \subset \mathcal{P}$ について

$$f(A) = 1 \Leftrightarrow \mathbf{e} \in Im(M_A^\top)$$

を満たすとき，Monotone Span Program $(\mathbb{F}_q, M, g, \mathbf{e})$ は f を計算するという．そのため，$\mathbf{e}$ はターゲットベクトルと呼ばれる．さらに Span Program のサイズとは行列 M の列の数のことをいう．特に，f の入力を X としたとき，与えられた t に対し，$|X| \geq t$ のとき $f(X) = 1$ となる Monotone Function f と，$\mathbf{e} = \mathbf{e}_1$ を考える．この f を計算する MSP は M を列数 t の Vandermonde 行列とすることにより構成できる．しかしながら一般の Monotone Function f に対応する MSP の効率的な求め方は知られておらず，Span Program のサイズの下限値についても興味の対象となっている [22].

秘密分散法において，Access 構造と Adversary 構造はともに monotone 性を有する．したがって，Adversary 構造 $\mathcal{A}$ による Monotone Function $f_{\mathcal{A}}$ は，

$$f_{\mathcal{A}}(B) = \begin{cases} 0 & (B \in \mathcal{A}), \\ 1 & (B \notin \mathcal{A}). \end{cases}$$

として定義できる．逆に，Monotone Function f が与えられたとき，秘密分散法の Adversary 構造は $\mathcal{A}_f = \{B \subseteq \mathcal{P} | f(B) = 0\}$ と定義される．

次に，MSP を用いた秘密分散法の概要を述べる．MSP による秘密分散法では，ターゲットベクトルとして $\mathbf{e} = \mathbf{e}_1$ を用いる．さらに，集合 $\mathcal{P}$ は秘密分散法の参加者の集合であり，参加者を g の像のリテラルとみなし，g はシェアを各参加者に割り振る関数として使用する．したがって，使用される Span Program は monotone である．M はシェアの作成に使用し，その行数である d はシェア数に対応する．特に $n \times t$ の Vandermonde 行列により構成された MSP で計算する Monotone Function f は，(t, n) 閾値秘密分散法の Adversary 構造と一致する．

本論文の以降では，$\mathcal{P}$ について，参加者の集合と，参加者の持つシェアの集合の 2 つの意味で用いる．また，特に参加者のシェアであることを明記する場合については，$P = \{P_1, \ldots, P_n\}$ を用いて表す．また，$d \times e$ の行列 M による写像とは $(a_1, \cdots, a_e) \in \mathbb{F}_q^e \mapsto M(a_1, \cdots, a_e)^\top$ を表す．

3.2.2 Cleve らの量子秘密分散プロトコル

本節では既存研究の一つとして，Cleve らにより提案された $(2, 3)$ 閾値量子秘密分散法 [16] を紹介する．このプロトコルは量子状態の秘密を量子状態のシェアに分散する秘密分散法であり，3 次元量子状態 (*qutrit*) を用いて構成する．

• ディーラによるシェアの生成及び配付

(1) 秘密量子状態を $\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$ とする．

(2) 以下のように分散符号化する．

$$\begin{aligned}
&\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \\
&\quad \mapsto \quad \alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |210\rangle)
\end{aligned}$$

(3) 各 qutrit を参加者に配布する．

• 秘密情報の復元

例として一人目と二人目で復元するとする．

(1) 二人目のシェアに一人目のシェアを法 3 の基で加算する．

$$\begin{aligned}
&\alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |210\rangle) \\
&\quad \mapsto \quad \alpha(|000\rangle + |121\rangle + |212\rangle) + \beta(|012\rangle + |100\rangle + |221\rangle) + \gamma(|021\rangle + |112\rangle + |200\rangle)
\end{aligned}$$

(2) 一人目のシェアに二人目のシェアを法 3 の基で加算する．

$$\begin{aligned}
&\alpha(|000\rangle + |121\rangle + |212\rangle) + \beta(|012\rangle + |100\rangle + |221\rangle) + \gamma(|021\rangle + |112\rangle + |200\rangle) \\
&\quad \mapsto \quad \alpha(|000\rangle + |021\rangle + |012\rangle) + \beta(|112\rangle + |100\rangle + |121\rangle) + \gamma(|221\rangle + |212\rangle + |200\rangle) \\
&\quad = \quad (\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)(|00\rangle + |21\rangle + |12\rangle)
\end{aligned}$$

以上より第 1qutrit が秘密情報となっている．

3.2.3 Smith の量子秘密分散プロトコル

この節では，量子秘密分散法の情報理論による定義 [28] を紹介し，既存研究として，MSP $(\mathbb{F}_q, M, g)$ を用いた，1 つの秘密の量子状態を分散する秘密分散法を，任意の Access 構造で実現する量子秘密分散法 [44] を紹介する．

定義 4 *[28]* 参加者の集合を $\mathcal{P}$，秘密の量子状態を S とし，S の純粋化に使用した補助系を R とする．また S を分散した量子状態のシェアを $\{P_1, \ldots, P_n\}$ とし，その *Access* 構造を Γ とする．このとき，量子秘密分散法は以下を満たすものとして定義される．

1. *Recoverability*
   任意の $A \in \Gamma$ に対し，$I(R:A) = I(R:S)$.
2. *Secrecy*
   任意の $B \notin \Gamma$ に対し，$I(R:B) = 0$.

ここで 任意の正整数 t に対し，以下の 2 つの性質をもつ単射写像 $\vartheta : \mathbb{F}_q^t \to \mathcal{H}^{\otimes t}$ を考える [40].

1. $\forall (a_1, \ldots, a_t) \in \mathbb{F}_q^t$, について $\vartheta((a_1, \ldots, a_t)^\top) = |a_1, \ldots, a_t\rangle$.

2. ϑ の任意の 2 つの像 $|a_1, \cdots, a_t\rangle$, $|a'_1, \cdots, a'_t\rangle$ に対して，

$$\langle a_1, \cdots, a_t | a'_1, \cdots, a'_t \rangle \quad = \quad \begin{cases} 1 & \text{if } (a_1, \cdots, a_t) = (a'_1, \cdots, a'_t), \\ 0 & \text{otherwise.} \end{cases}$$

この ϑ により，$\mathbb{F}_q^t$ 上でなされた定義などはすべて，$\mathcal{H}^{\otimes t}$ 上に拡張することができる．以降では，$|a_1, \ldots, a_t\rangle$ は $\vartheta((a_1, \ldots, a_t)^\top)$ を表すとする．

定理 4 *[40]* 列独立な $\mathbb{F}_q$ 上の $d \times e$ の行列 M に対して，$\theta_M : \mathcal{H}^{\otimes e} \to \mathcal{H}^{\otimes d}$ を

$$\theta_M(\sum_i \alpha_i |\psi_1^i \psi_2^i \cdots \psi_e^i\rangle) \quad = \quad \sum_i \alpha_i \left| M(\psi_1^i, \psi_2^i, \ldots, \psi_e^i)^\top \right\rangle$$

とする．ただし，$|\psi_1^i \cdots \psi_e^i\rangle$ を $\mathcal{H}^{\otimes e}$ の正規直交基底とする．このとき θ_M は等長写像である．

以上から，$\mathbb{F}_q$ 上の操作 M により，$\mathcal{H}^{\otimes e}$ 上の量子操作 θ_M が導出されることがいえる．

次に，Smith の手法において秘密の復元が可能であることを保証する補題を与える．

補題 3 *[44] QSSS* において，$A \subseteq \mathcal{P}$ を有資格集合とし，$B \subseteq \mathcal{P}$ を禁止集合とする．また，M を $\mathcal{P}$ 上における *MSP* の行列とし，A 及び B に対応する M の部分行列を M_A，M_B とする．このとき，任意の $s \in \mathbb{F}_q$ に対し以下を満たす $\mathbb{F}_q$ 上の行列 V が存在する．

1. $v_1 M_A \begin{pmatrix} s \\ a \end{pmatrix} = s.$

2. $\begin{pmatrix} V' M_A \\ M_B \end{pmatrix} \begin{pmatrix} s \\ a \end{pmatrix}$ は s とは独立した分布である．

ここで，a を $\mathbb{F}_q^{m-1}$ の任意の要素とし，v_1 は V の *1* 行目の行ベクトル，V' は V の *1* 行目を除いた行列を表す．

この補題の（1）は，M_A に対し $v_1 M_A = (1\ 0\ \cdots\ 0)$ となるベクトル v_1 が存在すること，すなわち秘密情報が復元可能であることを意味し，（2）は禁止集合に対して，秘密に関する情報が一切漏れないことを意味している．

次に，Smith による量子秘密分散法のプロトコルを紹介する [44].

- **ディーラによるシェアの生成及び配付**

(1) $|i^S\rangle$ を秘密量子状態の系 S の正規直交基底とし，秘密情報の量子状態を正規直交分解した状態を

$$\rho_S = \sum_{i \in \mathbb{F}_q} p_i |i^S\rangle\langle i^S| \tag{3.3}$$

とする．3.3 式で表された秘密情報を，秘密状態の空間と同じ状態空間である補助系 R で純粋化する．$|i^R\rangle$ を系 R での正規直交基底とすると，

$$|RS\rangle \ = \ \sum_{i \in \mathbb{F}_q} \sqrt{p_i} |i^R\rangle \otimes |i^S\rangle$$

となる．

(2) 状態 $|E\rangle = 1/\sqrt{q^{e-1}} \sum_{a \in \mathbb{F}_q^{e-1}} |a\rangle$ を用意する．

(3) ディーラは合成系 RSE に対して，$I_R \otimes \theta_M : \mathcal{H}_R \otimes \mathcal{H}_S \otimes \mathcal{H}_E \to \mathcal{H}_R \otimes \mathcal{H}_P$ を適用する．結果として

$$(I_R \otimes \theta_M)(|RS\rangle \otimes |E\rangle) = |RP\rangle$$

となる．

(4) 参加者 $x_k \in \mathcal{P}$ に対して，$M_{g^{-1}(x_k)}$ で生成された系の量子状態を配付する．

- **秘密情報の復元**

A を有資格集合とし，$B = \mathcal{P} \setminus A$ とする．このとき，補題 3 の行列 V に対応する等長写像 θ_V を考えることができる．この θ_V を系 A に適用することによって秘密情報を復元することができる．すなわち，

$$\begin{aligned} &(I_R \otimes \theta_V \otimes I_B)(|RAB\rangle) \\ &= \ |RS\rangle \otimes \frac{1}{\sqrt{q^{e-1}}} \sum_{a \in \mathbb{F}_q^{e-1}} |V' M_A(s,a)^\top\rangle \otimes |M_B(s,a)^\top\rangle. \end{aligned}$$

この V を復元行列という．

Smith のスキームは，文献 [41] によって定義 4 を満たしていることが示されている．

第 4章

量子コイン投げ

本章では，本論文の一つ目の成果である量子コイン投げについて述べる．4.1 節では 3.1.2 節で述べた Ambainis のプロトコルを基とした提案方式を，4.2 節において，提案プロトコルの評価を行う．

4.1 提案方式

この節では，本稿で提案する strong 量子コイン投げプロトコルについて述べる．量子コイン投げプロトコルでは，n 次元量子状態を使用するため，まずその量子状態を定義する．

4.1.1 n 次元量子状態の構成

3.1.2 節において，Ambainis のプロトコルに新たな次元を導入し 4 次元量子状態とした場合，Alice 側に bias が偏ることが分かっていると述べた．これは同様に状態を付加していくことで n 次元量子状態を実現しても，Alice 側にバイアスを偏らせることはできるが，Bob 側にバイアスを偏らせることはできないことを意味する．つまり，Alice，Bob の両方にバイアスを偏らせることが可能な量子状態の構成法については今まで知られていない．そこで，我々は Alice と Bob の両方にバイアスを任意に偏らせることができるように，新たな状態の構成法を以下のように提案する．

1. 必要とされるバイアスに対応した量子の次元数 n と，$t \in \{0, \ldots, n\}$ を選ぶ．ただし $n - t \equiv 0 \pmod 2$ を満たすものとする．(バイアスと n, t のより具体的な関係については補題 4, 5 を参照)
2. 高さ $h = t + (n-t)/2$ となる完全 2 分木を考える．ここで，各々の葉に状態名に対応する番号付け $b, x_1, \ldots, x_{h-1}$ を行う．ただし，$b \in \{0, 1\}$ であり，$x_i \in \{0, 1\}$ $(i = 1, \ \ldots, \ h-1)$ である．
3. 下記に従い，各レベル（根からの距離）ごとの節点に状態 $\pm|0\rangle$，$\pm|1\rangle$，…，$\pm|n-1\rangle$ を割り振る．
   (a) レベル 1 のとき，
      i. $t = 0$ ならば，片方の節点に $+|0\rangle$ を，もう片方の節点に $+|1\rangle$ を割り振る．
      ii. $t \neq 0$ ならば，両方の節点に $+|0\rangle$ を割り振る．
   (b) レベル $2 \leq \ell \leq t$ のとき，
      同じ親からなる 2 節点のうちの片方に $+|\ell-1\rangle$ を，もう片方の節点に $-|\ell-1\rangle$ を割り振る．
   (c) レベル $t < \ell \leq h$ のとき，
      i. 木の右半分については，同じ親からなる 2 節点のうち，片方の節点に $+|t+2(\ell-t-1)\rangle$ を，もう片方の節点に $-|t+2(\ell-t-1)\rangle$ を割り振る．
      ii. 木の左半分については，同じ親からなる 2 節点のうち，片方の節点に $+|t+2(\ell-t-1)+1\rangle$ を，もう片方の節点に $-|t+2(\ell-t-1)+1\rangle$ を割り振る．
4. 根から葉 $b, x_1, \ldots, x_{h-1}$ までの経路上の節点に割り振られた状態を $a_i|y_i\rangle (a_i \in \{+1, -1\}, 1 \leq i \leq h)$ とする．このとき，量子状態 $|\phi_{b,x_1,\ldots,x_{h-1}}\rangle$ を以下のように定義する．

$$|\phi_{b,x_1,\ldots,x_{h-1}}\rangle = \frac{1}{\sqrt{h}} \sum_{i=1}^{h} a_i|y_i\rangle. \tag{4.1}$$

例として，$\epsilon_{Alice} = 1/3$ と $\epsilon_{Bob} = 1/6$ とする場合，その 2 分木は図 1 のようになり，$n = 4$，$t = 2$ とした場合の 2 分木に対応する．この木により，状態 $|\phi_{010}\rangle$ は $(|0\rangle - |1\rangle + |2\rangle)/\sqrt{3}$ で与えられることが分かる．

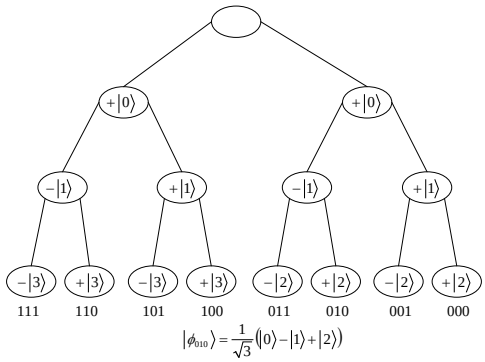

図 4.1: $n = 4$，$t = 2$，$|\phi_{010}\rangle$ の場合

4.1.2 量子コイン投げプロトコル

4.1.1 節において定義された，n 次元量子状態を使用した strong 量子コイン投げを定義する．

1. Alice は，$b, x_1, \ldots, x_{h-1} \in \{0, 1\}$ をランダムに選び，状態 $|\phi_{b,x_1,\ldots,x_{h-1}}\rangle$ を Bob に送る．
2. Bob は，ランダムに $b' \in \{0, 1\}$ を選び，Alice に送る．
3. Alice は，$b, x_1, \ldots, x_{h-1}$ を Bob に送る．
4. Bob は，(1) で受け取った状態 $|\phi_{b,x_1,\ldots,x_{h-1}}\rangle$ が正しいものかを観測する[1]．もし正しく観測できなければ，Alice が不正を行なったと判断し，プロトコルを停止する．
5. 正しく観測できたなら，$c = b \oplus b'$ をコイン投げの結果とする．

4.2 評価

この節では，提案した n 次元量子状態を使用した量子コイン投げにおいて，Alice 又は Bob が不正を行なって $b \oplus b' = 0$（$b \oplus b' = 1$）が得られる確率を計算する．なお，攻撃モデルは Ambainis によるモデル [3] と同様のモデルである．

[1]観測は，送られてきた量子状態から Gram-Schmidt の直交化法などの方法を用いることで正規直交基底を量子状態の次元数分だけ作成し，それに対応する測定作用素を生成して行う．

まず，Alice が Bob に送信する状態を考える．もし Alice が $b=0$ を選んだ場合，Alice が送る混合状態 ρ^0 は，各状態 $|\phi_{0,x_1,\ldots,x_{h-1}}\rangle, x_i \in \{0,1\}$ を確率 $1/2^{h-1}$ の等確率で選んだものと等しい．同様に，Alice が $b=1$ を選んだ場合，Alice が送る混合状態 ρ^1 は，各状態 $|\phi_{1,x_1,\ldots,x_{h-1}}\rangle, x_i \in \{0,1\}$ を確率 $1/2^{h-1}$ の等確率で選んだものに等しい．以上から，密度行列 ρ^0 の i 行 j 列成分を ρ^0_{ij} とすると以下の式で与えられる：

$$
\begin{aligned}
\rho^0_{ii} &= \begin{cases} \frac{1}{h} & \cdots\ 1 \le i \le t, \text{または} \\ & \quad i = t+2k-1\ (1 \le k \le \frac{n-t}{2}), \\ 0 & \cdots\ i = t+2k\ (1 \le k \le \frac{n-t}{2}), \end{cases} \\
\rho^0_{ij} &= 0 \qquad \cdots\ \text{それ以外}.
\end{aligned}
$$

同様に ρ^1 の各成分は

$$
\begin{aligned}
\rho^1_{ii} &= \begin{cases} \frac{1}{h} & \cdots\ 1 \le i \le t, \text{ または,} \\ & \quad i = t+2k\ (1 \le k \le \frac{n-t}{2}), \\ 0 & \ldots\ i = t+2k-1\ (1 \le k \le \frac{n-t}{2}), \end{cases} \\
\rho^1_{ij} &= 0 \qquad \cdots\ \text{それ以外}.
\end{aligned}
$$

次に，$X = t/n\ (0 \le X \le 1)$ と定義する．X は，ρ^0 と ρ^1 の非直交度を表す尺度になっている．本論文ではこの X を使ってプロトコルの解析を行う．

4.2.1 Bob が不正を行う場合

まず，Bob が $b \oplus b' = 0$（$b \oplus b' = 1$）となるように不正を行う場合を考える．ここで，Bob の不正とは，Alice から送られてきた状態 $|\phi\rangle$ を，Bob が b' を選択する前に観測することで b を予測し，自分に都合の良い b' を選択することをいう．このときの Bob のバイアスについて以下が成り立つ．

補題 4 *Bob* のバイアス ϵ_{Bob} について以下が成り立つ：

$$
\epsilon_{Bob} = \frac{1}{4} - \left(\frac{3}{4} - \frac{1}{1+X}\right), \tag{4.2}
$$

ただし，$X = t/n$，n は量子状態の次元数，t は *Alice* が選ぶ量子状態すべてに共通する基底の数である．

Proof　文献 *[2]* の *Theorem 3* より，*Bob* が $b' = b$ を得られる確率は，高々以下のようになる．

$$\begin{aligned}\frac{1}{2} + \frac{\mathrm{Tr}\,|\rho^0 - \rho^1|}{4} &= \frac{1}{2} + \frac{n-t}{4h} \\ &= \frac{1}{2} + \frac{n-t}{2(n+t)} \\ &= \frac{1}{2} + \frac{1-X}{2(1+X)}. \end{aligned} \tag{4.3}$$

従って，*Bob* のバイアスは，以下のようになる．

$$\begin{aligned}\epsilon_{Bob} &= \frac{1-X}{2(1+X)} \\ &= \frac{1}{4} - \frac{3X-1}{4(1+X)} \\ &= \frac{1}{4} - \left(\frac{3}{4} - \frac{1}{1+X}\right). \end{aligned} \tag{4.4}$$

■

また，Kent[30] や Tsurumaru[49] は量子 n ビット列コミットメントに対し，アクセシブル情報量より，ビットが漏洩することを示している．そこで本プロトコルにおいて，Alice が送信した ρ のアクセシブル情報量 m を計算すると以下のようになる．

$$\begin{aligned} m &\leq -\rho \log \rho - \left(-\frac{1}{2}\rho^0 \log \rho^0 - \frac{1}{2}\rho^1 \log \rho^1\right) \\ &= \frac{1-X}{1+X} \leq 1 \end{aligned} \tag{4.5}$$

ここで $\rho = \rho^0/2 + \rho^1/2$ である．

本プロトコルでは，Alice のコインとして ρ^0 か ρ^1 を送信している．従ってアクセシブル情報量 m が 1 を超えてはならない．しかし，4.5 式より m は条件を満たしている．

これらの結果より，Bob の不正に対しバイアスを下げるには，X の値を大きくとればよいことが分かる．

4.2.2 Alice が不正をする場合

Alice が不正を行なって，$b \oplus b' = 0$ とできる確率を求める．ここでいう Alice の不正とは，本来 Bob に送信する状態 $|\phi\rangle$ とは異なった状態 $|\psi\rangle$ を送り，観測時に Bob に $|\psi\rangle$ を $|\phi\rangle$ であると納得させることをいう．なお，全く同じ議論が $b \oplus b' = 1$ とする場合についても成り立つ．このとき，Alice のバイアスについて以下が成り立つ．

補題 5 *Alice* のバイアス ϵ_{Alice} について，以下が成り立つ：

$$\epsilon_{Alice} = \frac{1}{4} + \left(\frac{3}{4} - \frac{1}{1+X}\right), \tag{4.6}$$

ただし，$X = t/n$，n は量子状態の次元数，t は *Alice* が選ぶ量子状態すべてに共通する基底の数である．

Proof 文献 *[3]* の *Lemma 6* と同様の方法により，*Alice* がプロトコルの *(1)* で使用する状態 ρ に対し，同じ不正成功確率で以下のような ρ' も *Bob* に送信することができる．

$$\rho' = \begin{pmatrix} \delta_0 & & & 0 \\ & \delta_1 & & \\ & & \ddots & \\ 0 & & & \delta_{n-1} \end{pmatrix};$$

$$\sum_{i=0}^{n-1} \delta_i = 1.$$

この ρ' は以下のように生成できる．以下の条件を満たす $n \times n$ の対角行列 U_i $(i = 0, \ldots, 2^{n-1})$ を用意する．

1. 対角成分 a_{ii} は，$a_{ii} \in \{1, -1\}$.
2. $i \neq j$ ならば，$U_i \neq U_j$ かつ $U_i \neq -U_j$.

このような行列 U_i は，以下の性質を持つ．

1. 任意の U_i $(1 \leq i \leq 2^{n-1})$ と $|\phi_{b,x}\rangle$ $(b \in \{0,1\}, 0 \leq x \leq 2^{h-1} - 1)$ に対し，$|\phi_{b,x}\rangle = U_i|\phi_{b,x'}\rangle$ となるような x' $(0 \leq x' \leq 2^{h-1} - 1)$ が存在する．

2. $U_i^\dagger = U_i$.

3. $U_i^2 = I$.

4. $U_i U_j U_i = U_j$.

U_i を用いることで，*0* か *1* が得られる確率が同じまま，*Alice* がプロトコルの *(1)* で使用する状態 $|\phi_{b,x}\rangle$ を，$U_i|\phi_{b,x}\rangle$ に置き換えることができる．以上から，*Alice* によって送られる状態の密度行列は，次の式で与えられる．

$$\rho' = \frac{1}{2^{n-1}} \sum_{i=1}^{2^{n-1}} U_i \rho U_i^\dagger. \tag{4.7}$$

よって，ρ' を以後の解析に用いる．まず，以下の補題 *6, 7* を証明する．

補題 6 *Alice* が *Bob* に対し，$b = 0$ と納得させる確率は高々 $F(\rho', \rho^0)$ である．

Proof *Alice* が *Bob* に対し，$b = 0$ であるという不正を行うために選択した状態 ρ' を純粋化すると *4.8* 式になるとする．

$$|\psi\rangle = \sum_i a_i |i\rangle|\psi_i\rangle \tag{4.8}$$

ここで，*Alice* は *Bob* に対して $b = 0$ であるという不正を行うので，$|\phi_{0,0\cdots00}\rangle, \cdots, |\phi_{0,1\cdots11}\rangle$ のいずれかであると納得させることになる．次に，$|\psi_i\rangle$ と $|\psi_j\rangle = U_k|\psi_i\rangle$ が同じグループになるようにグループ分けを行う．このグループについて以下が成り立つ．

1. $|\psi_i\rangle$ と $|\psi_j\rangle$ が同じグループに含まれている場合，$a_i = a_j$ である．

2. $|\psi_i'\rangle = U_k|\psi_i\rangle$ と $|\psi_j'\rangle = U_k|\psi_j\rangle$ について，$\langle\psi_i|\psi_i'\rangle = \langle\psi_j|\psi_j'\rangle$ が成り立つ．

以上から *4.8* 式は以下のように変形できる．

$$|\psi\rangle = \sum_i a_i \sum_{j=0}^{2^{h-1}-1} \frac{1}{\sqrt{2^{h-1}}} |i,j\rangle|\psi_{i,j}\rangle. \tag{4.9}$$

ここで $|\psi_i'\rangle = |\phi_i\rangle$ と置くと，$|\psi_i\rangle$ を $|\psi_i'\rangle$ として *Bob* に受理される確率は，$|\langle\psi_i|\psi_i'\rangle|^2$

で与えられる．従って，*Bob* が受理する確率の合計は，

$$\sum_i |a_i|^2 \frac{1}{2^{h-1}} \sum_{j=0}^{2^{h-1}-1} |\langle \psi_j | \psi'_j \rangle|^2. \tag{4.10}$$

である．

次に，$|\varphi_i\rangle$ と $|\varphi'_i\rangle$ を次のように表す．

$$|\varphi_i\rangle = \sum_{j=0}^{2^{h-1}-1} \frac{1}{\sqrt{2^{h-1}}} |i,j\rangle |\psi_{i,j}\rangle. \tag{4.11}$$

$$|\varphi'_i\rangle = \sum_{j=0}^{2^{h-1}-1} \frac{1}{\sqrt{2^{h-1}}} |i,j\rangle |\psi'_{i,j}\rangle. \tag{4.12}$$

このとき以下の式が得られる．

$$\langle \varphi_i | \varphi'_i \rangle = \frac{1}{2^{h-1}} \sum_{j=0}^{2^{h-1}-1} \langle \psi_j | \psi'_j \rangle = \langle \psi_{i,k} | \psi'_{i,k} \rangle \ (0 \le k \le 2^{h-1}-1). \tag{4.13}$$

よって *4.10* 式は以下の式に変形できる．

$$\sum_i |a_i|^2 |\langle \varphi_i | \varphi'_i \rangle|^2. \tag{4.14}$$

次に，ρ_i を確率 $1/2^{h-1}$ で状態 $|\psi_{i,j}\rangle$ $(0 \le j \le 2^{h-1}-1)$ を取る密度行列とすると，$\rho' = \sum_i |a_i|^2 \rho_i$ が成り立つ．$|\varphi_i\rangle$ と $|\varphi'_i\rangle$ は，ρ_i と ρ_0 を純粋化したものであるので，$|\langle \varphi_i | \varphi'_i \rangle|^2 \le F(\rho_i, \rho^0)$ が得られ，次式が得られる．

$$\sum_i |a_i|^2 |\langle \varphi_i | \varphi'_i \rangle|^2 \le \sum_i |a_i|^2 F(\rho_i, \rho^0). \tag{4.15}$$

最後に忠実度の凹性 *[36]* より，次式が得られる．

$$\begin{aligned} \sum_i |a_i|^2 F(\rho_i, \rho^0) &\le F(\sum_i |a_i|^2 \rho_i, \rho^0) \\ &= F(\rho, \rho^0). \end{aligned} \tag{4.16}$$

■

同様に以下が成り立つ．

補題 7 *Alice* が *Bob* に対し，$b = 1$ と納得させる確率は高々 $F(\rho', \rho^1)$ である．

以上を使用すると，文献 *[3]* の *Lemma 8* より，*Alice* が, $b \oplus b' = 0$ とできる確率は高々$(F(\rho', \rho^0) + F(\rho', \rho^1))/2$ であることが示されているので，補題 *2* より，

$$
\begin{aligned}
F(\rho', \rho^0) &= \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho'}\rho^0\sqrt{\rho'}}\right)\right)^2 \\
&= \left(\sqrt{\frac{\delta_0}{h}} + \ldots + \sqrt{\frac{\delta_{t-1}}{h}} + \sqrt{\frac{\delta_t}{h}}\right. \\
&\quad \left. + \sqrt{\frac{\delta_{t+2}}{h}} + \ldots + \sqrt{\frac{\delta_{n-2}}{h}}\right)^2 . \qquad (4.17)
\end{aligned}
$$

$$
\begin{aligned}
F(\rho', \rho^1) &= \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho'}\rho^1\sqrt{\rho'}}\right)\right)^2 \\
&= \left(\sqrt{\frac{\delta_0}{h}} + \ldots + \sqrt{\frac{\delta_{t-1}}{h}} + \sqrt{\frac{\delta_{t+1}}{h}}\right. \\
&\quad \left. + \sqrt{\frac{\delta_{t+3}}{h}} + \ldots + \sqrt{\frac{\delta_{n-1}}{h}}\right)^2 . \qquad (4.18)
\end{aligned}
$$

ここで $\sum_{i=0}^{n-1} \delta_i = 1$ である．

従って，

$$
\begin{aligned}
&\frac{1}{2}(F(\rho', \rho^0) + F(\rho', \rho^1)) \\
&\quad = \frac{1}{2h}\left(\left(\sqrt{\delta_0} + \ldots + \sqrt{\delta_{t-1}}\right.\right. \\
&\qquad \left. + \sqrt{\delta_t} + \sqrt{\delta_{t+2}} + \ldots + \sqrt{\delta_{n-2}}\right)^2 \\
&\qquad + \left(\sqrt{\delta_0} + \ldots + \sqrt{\delta_{t-1}}\right. \\
&\qquad \left.\left. + \sqrt{\delta_{t+1}} + \sqrt{\delta_{t+3}} + \ldots + \sqrt{\delta_{n-1}}\right)^2\right); \\
&\qquad \sum_{i=0}^{n-1} \delta_i = 1 \qquad (4.19)
\end{aligned}
$$

4.19 式は $\delta_0 = \delta_1 = \ldots = \delta_{t-1} = 4/(n+3t)$，$\delta_t = \delta_{t+1} = \ldots = \delta_{n-2} = \delta_{n-1} = 1/(n+3t)$ のとき，$(n+3t)/(4h) = (n+3t)/(2(n+t)) = 1/2+t/(n+t) = 1/2+X/(1+X)$ で最大になる．以上から *Alice* のバイアス ϵ_{Alice} は，以下のようになる．

$$
\begin{aligned}
\epsilon_{Alice} &= \frac{X}{1+X} \\
&= \frac{1}{4} + (\frac{3}{4} - \frac{1}{1+X}) \qquad (4.20)
\end{aligned}
$$

■

4.3 考察

この節では，提案プロトコルについて，いくつかの観点で議論する．

4.3.1 不正成功確率の妥当性

Alice が不正を行い出力を 1 にできる確率を p_{1*}，Bob が不正を行い出力を 1 にできる確率を p_{*1} としたとき，その確率は次の式を満たすことが知られている [4].

$$p_{1*}p_{*1} \geq \frac{1}{2}. \tag{4.21}$$

従って，$\max\{p_{1*}, p_{*1}\} \geq \frac{1}{\sqrt{2}}$ である．提案プロトコルでは，p_{1*} と p_{*1} は次で与えられる．

$$p_{1*} = \frac{1}{2} + \epsilon_{Alice} = \frac{3}{4} + \left(\frac{3}{4} - \frac{1}{1+X}\right), \tag{4.22}$$

$$p_{*1} = \frac{1}{2} + \epsilon_{Bob} = \frac{3}{4} - \left(\frac{3}{4} - \frac{1}{1+X}\right). \tag{4.23}$$

ここで $0 \leq X \leq 1$ であるから，$p_{1*}p_{*1} \geq 1/2$ を満たすことが分かる．このように，範囲内で任意に X をとっても 4.21 式に抵触しない．

4.3.2 アクセシブル情報量による漏洩

Alice は n 次元量子状態である ρ^0 か ρ^1 を，Bob に送信している．一般に，n 次元量子状態を使用した場合のアクセシブル情報量は $n \log n \geq 1$ となり，この場合は b の値が漏洩することになる [49]．しかし，Holevo 限界の定理と使用する状態を使い，厳密にアクセシブル情報量を求めると，提案プロトコルのアクセシブル情報量は $(1-X)/(1+X) \leq 1$ で与えられる．以上から提案プロトコルでは，アクセシブル情報量の観点から，b の値が漏洩することはないことが分かる．

4.3.3 Ambainis[3] のプロトコルとの関係

我々のプロトコルは，n と t を選択することで，Alice か Bob のバイアスを任意に選ぶことができるという特徴が存在する．これはまた，一度バイアスを決定すると，n と t の値も最小にすることができることも意味している．このように，提案プロトコルは様々な状況に応じて効率的に対応できる．さらに，大きな特徴として，一方のバイアスを増やすことで，もう一方のバイアスを任意に小さくすることができるという特徴がある．このことが有用に使用できる例として，下記のような乱数共有を挙げる．認証等において，二者間で乱数を共有することがよく行なわれる [34, 39]．この乱数共有ステップをコイン投げで実現することを考える．Bob は検証者である認証サーバ（又はセンタ）であると仮定し，Alice は正規のユーザ (Charlie) に成りすまして認証を行う攻撃者と仮定する．このとき，Alice は Charlie と Bob のやり取りから，乱数 r と，Charlie の秘密情報 x と r から作り出した情報 $I = f(x, r)$ を記録する．次に Alice は Charlie に成りすまし，認証を試みる．Alice としては乱数共有時に $r' = r$ とできれば I を使用することで Charlie に成りすますことができる．この例の場合，Bob はセンタであるため，Alice，Charlie という個人に比べ信用を置くというのは一般的に良く用いられる仮定である．従って，Bob のバイアスをある程度犠牲にし，Alice のバイアスを下げることができる．さらに，Alice は Charlie と Bob の間で共有された乱数 r に結果を合わせることが目的である．したがって，Alice が不正をして，共有する情報を $c = 0$ とする場合のみを考えている weak コイン投げでは対応ができないといえる．

ここで代表的な場合について表 1 にまとめる．

表 4.1: 代表的な場合のバイアス

X	0	$\frac{1}{3}$	1
ϵ_{Alice}	0	$\frac{1}{4}$	$\frac{1}{2}$
ϵ_{Bob}	$\frac{1}{2}$	$\frac{1}{4}$	0

この例のように，X のとり方により，Alice，Bob のバイアスは $0 \leq \epsilon \leq \frac{1}{2}$ から取ることができことが分かる．例として，$X = 1/3$ とすると，ϵ_{Alice} と ϵ_{Bob} は $1/4$ となり同じ値になる．これは，ちょうど Ambainis によるプロトコルと同じ結果に

なっている．すなわち，Ambainis のプロトコルは，提案プロトコルの特別な場合となっているといえる．また，提案プロトコルは，一方のバイアスを増やすことで，もう一方のバイアスを任意に小さくすることができるという Ambainis のプロトコルが持たない機能を持ち，Ambainis のプロトコルの拡張となっていることが分かる．

4.4 まとめ

本章では，Ambainis により提案された，3 次元量子状態を使用した量子コイン投げを拡張し，n 次元量子状態を使った量子コイン投げの提案を行なった．その結果，Alice と Bob のバイアスはそれぞれ $\epsilon_{Alice} = 1/4 + (3/4 - 1/(1+X))$，$\epsilon_{Bob} = 1/4 - (3/4 - 1/(1+X))$ という結果が得られた．これは一方のバイアスを犠牲にすることで，もう一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意味している．さらに，両者のバイアスを $\epsilon = 0$ とすることはできないが，片方のみならばバイアスを $\epsilon = 0$ とすることができることを示している．この結果より，様々な状況への適用が期待できる．また，$X = 1/3$ としたとき，$\epsilon_{Alice} = \epsilon_{Bob} = 1/4$ となり，Ambainis により提案されたコイン投げも，特別な場合として提案プロトコルに含まれているといえる．

第 5 章

量子秘密分散

本章では，本論文の二つ目の成果である量子秘密分散法について述べる．5.1 節で 3.2.3 で述べた Smith のプロトコルを基とした提案方法を，5.2 節において提案プロトコルの評価を行い，5.3 節において構成法に従い，秘密が量子状態 2 つであり，それを 4 人中 3 人が持つシェアにより復元できる量子複数秘密分散を構成する．

5.1 提案方式

本節では，複数の秘密の量子状態をもつ量子複数秘密分散法の定義を与えた後，構成法を示す．

5.1.1 量子複数秘密分散法

量子複数秘密分散法を以下のように定義する．

定義 5 参加者の集合を $\mathcal{P}$，秘密の量子状態の集合を $\{S_1, \ldots, S_m\}$ とする．各々の秘密 S_i に対し，純粋化に用いた補助系を R_i，*Access* 構造を Γ_i とする．さらに，各 Γ_i について $T_i = \{R_1, \ldots, R_m\} \setminus \{R_i\}$ とする．このとき，任意の i $(1 \leq i \leq m)$ について以下の *2* つの条件を満たすものを，量子複数秘密分散法と定義する．

1. Recoverability

任意の $A \in \Gamma_i$ に対し，$I(R_i : T_i A) = I(R_i : S_i)$.

2. Secrecy

任意の $B \notin \Gamma_i$ に対し，$I(R_i : T_i B) = 0$.

この定義は秘密がひとつの秘密分散法を複数の秘密を持つように拡張したものである．すなわち,（1）は秘密 S_i を分散させた量子操作に対し，その逆変換が存在することを示している.（2）については系 B と標的の秘密以外の補助系 T_i を分散させた量子操作に対して，逆変換が存在しないことを示す [28]．また，秘密が S_1 のみの場合を考えると，その純粋化に用いた補助系は R_1 のみであり，したがって $T_1 = \emptyset$ であるので，定義 4 と一致する．

また，特別な Access 構造を持つ量子複数秘密分散法として，(m, t, d) 量子閾値複数秘密分散法を定義する．

定義 6 秘密状態を m 個，シェアを d 個とし，そのうち任意の t 個以上のシェアを集めることで全ての秘密の状態を復元できる量子複数秘密分散法を (m, t, d) 量子閾値複数秘密分散法という．

5.1.2 提案法

提案法は既存の MSP を用いた単一秘密の量子秘密分散法 [44] を複数秘密分散法に拡張することにより構成する．シェアの生成は，Smith の方法と同じく，MSP による $\mathbb{F}_q$ 上の行列 M に対応する等長写像 θ_M により行う．参加者の部分集合 A により j 番目の秘密状態の復元を行うときは，A と g で対応する M の部分行列 M_A から，ターゲットベクトル $\mathbf{e}_j$ を作成することにより行う．しかしながら，単一秘密分散法における MSP は，作成できるターゲットベクトルが 1 つであるため，量子複数秘密分散法へ単純に適用することはできない．そこで，複数のターゲットベクトルに適用できるように MSP を拡張する．しかしながら，MSP で構成された任意の単一秘密分散法が Secrecy を満たしていたのに対し，量子複数秘密分散法では，MSP の行列 M の採り方により Secrecy を満たさない場合が存在する．その考察は 5.2 節において行う．なお，本論文で提案する MSP の拡張法により，MSP を用いた古典の単一秘密分散法を，古典複数秘密分散法に拡張することもできる．しかしながら，量子秘密分散法においては，古典にはない純粋化などの量子操作が

存在する．したがって，それらについても考慮したうえで，拡張する必要がある．

以下では秘密状態が m 個あり，それぞれの秘密に関して任意の Access 構造をもつ量子複数秘密分散法を提案する．まず，シェアの生成と配布について述べる．

• ディーラによるシェアの生成及び配付

(1) 複数の秘密の量子状態が正規直交基底 $|i^{S_j}\rangle$ $(i \in \mathbb{F}_q)$ で張られる状態空間 S_j により与えられたとする．そのときの各秘密の量子状態の正規直交分解を以下のようにおく．

$$\begin{aligned}
\rho_{S_1} &= \sum_{i\in\mathbb{F}_q} p_{1i}|i^{S_1}\rangle\langle i^{S_1}|, \\
\rho_{S_2} &= \sum_{i\in\mathbb{F}_q} p_{2i}|i^{S_2}\rangle\langle i^{S_2}|, \\
&\vdots \\
\rho_{S_m} &= \sum_{i\in\mathbb{F}_q} p_{mi}|i^{S_m}\rangle\langle i^{S_m}|.
\end{aligned}$$

さらに，秘密情報 S_j を S_j と同じ状態空間 R_j で純粋化する．R_j の基底を $|i^{R_j}\rangle$ とすると，

$$|R_jS_j\rangle = \sum_{i\in\mathbb{F}_q} \sqrt{p_{ji}}|i^{R_j}\rangle \otimes |i^{S_j}\rangle$$

となる．

(2) 状態 $|R_EE\rangle = 1/\sqrt{q^{e-m}}\sum_{a\in\mathbb{F}_q^{e-m}} |a\rangle \otimes |a\rangle$[1]を用意する．

(3) ディーラは合成系 $\mathcal{R}SE$ に対して $I_{\mathcal{R}} \otimes \theta_M : \mathcal{H}_{\mathcal{R}} \otimes \mathcal{H}_S \otimes \mathcal{H}_E \to \mathcal{H}_{\mathcal{R}} \otimes \mathcal{H}_P$ を適用する．すなわち，

$$(I_{\mathcal{R}} \otimes \theta_M)(|\mathcal{R}S\rangle \otimes |E\rangle) = |\mathcal{R}P\rangle.$$

ここで $\mathcal{R} = |R_1 \cdots R_m\rangle \otimes |R_E\rangle$ とする．

(4) 参加者 x_k に対して，$M_{g^{-1}(x_k)}$ で生成された系の量子状態を配付する．

なお，以降では簡単化のため，$|\mathcal{P}| = d$ であり，k 番目の参加者 x_k に対し，$x_k = g(k)$ であるとする．

[1]評価におけるエントロピーの計算を簡単にするため純粋化した状態を使用.

• 秘密情報の復元

秘密 S_j を復元する Access 構造を Γ_j とし，$A \in \Gamma_j$ とする．V を，M に適用しターゲットベクトル $\mathbf{e}_j$ を生成する復元行列，すなわち，補題 3 の（1）を満たす行列 V とし，その等長写像を θ_V とする．系 A に θ_V を適用することにより，秘密情報を復元できる．

5.2 評価

5.1.2 節において提案した量子複数秘密分散法を，5.1.1 節の定義 5 に従い評価する．

定理 5 *MSP* を用いて構成した，m 個の秘密の量子状態と，各秘密 S_i に対して任意の *Access* 構造 Γ_i をもつ *QSSS* が *Secrecy* を満たすとする．このとき，d 行 e 列からなる *MSP* の行列 M は，$t = \min\{|A| \ |A \in \Gamma_i, i = 1, \cdots, m\}$ に対して以下の *2* 条件を満たす．

1. $d \geq t + m - 1$.

2. $e \geq t + m - 1$.

Proof 定義 *5* の *Secrecy* の式を展開し移項すると，

$$S(R_1 \cdots R_m A) - S(T_i A) = S(R_i) \tag{5.1}$$

となる．このうち，エントロピーと純粋化の性質から $S(R_i) = S(S_i)$ が成り立つ．したがって，$S(R_1 \cdots R_m A)$ と $S(T_i A)$ を求める．ここで，任意のアクセス構造に対し，$t = \min\{|A| \ |A \in \Gamma_i, i = 1, \cdots, m\}$ となるような (m, t, d) 量子閾値秘密分散法を考えることで，以下の *2* つの補題を与える．

補題 8 列独立な $d \times e$ 行列を持つ *MSP* を用いて構成された，(m, t, d) 量子閾値複数秘密分散法において，$|A| = t - 1$ となる集合 $A \subseteq \mathcal{P}$ について以下が成り立つ．ここで，$B = \mathcal{P} \setminus A$，$M'_B$ は M_B から $m + 1$ 列目以降を取り除いた行列とし，ある $x \in Im(M_B), i_{m+1}, \ldots, i_e$ に対し，

$$M_B(i_1, \cdots, i_m, i_{m+1}, \cdots, i_e)^\top \ = \ x$$

を満たす $(i_1,\ldots,i_m)$ の集合を $B_x^{i_{m+1},\ldots,i_e}$ とする．

(1-a) $rank(M'_B) < m, e-m \le t-1$ の場合

$$\begin{aligned} & S(R_1\cdots R_m A) \\ &= (e-m)\log q \\ &\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}. \end{aligned} \tag{5.2}$$

(1-b) $rank(M'_B) < m, e-m > t-1$ の場合

$$\begin{aligned} & S(R_1\cdots R_m A) \\ &= (t-1)\log q \\ &\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}. \end{aligned} \tag{5.3}$$

(2-a) $rank(M'_B) \ge m, e-m \le t-1$ の場合

$$S(R_1\cdots R_m A) = (e-m)\log q + \sum_i^m S(S_i). \tag{5.4}$$

(2-b) $rank(M'_B) \ge m, e-m > t-1$ の場合

$$S(R_1\cdots R_m A) = (t-1)\log q + \sum_i^m S(S_i). \tag{5.5}$$

Proof $S(R_1\cdots R_m A)$ を求めるため，$\rho^{R_1\cdots R_m A}$ を考え，その固有値を求める．

$$\begin{aligned} & \rho^{R_1\cdots R_m A} \\ &= \mathrm{Tr}_{R_E B}\,|\mathcal{R}AB\rangle\langle\mathcal{R}AB| \\ &= \frac{1}{q^{e-m}}\sum_{i_1,i'_1}\cdots\sum_{i_e,i'_e}\sqrt{p_{1i_1}p_{1i'_1}\cdots p_{mi_m}p_{mi'_m}} \\ &\quad \times\left|i_1,\cdots,i_m,M_A(i_1,\ldots,i_e)^\top\right\rangle\left\langle i'_1,\cdots,i'_m,M_A(i'_1,\ldots,i'_e)^\top\right| \\ &\quad \times\left\langle i_{m+1},\cdots,i_e,M_B(i_1,\ldots,i_e)^\top\right|\left.i'_{m+1},\cdots,i'_e,M_B(i'_1,\ldots,i'_e)^\top\right\rangle \\ &= \frac{1}{q^{e-m}}\sum_{i_1,i'_1}\cdots\sum_{i_m,i'_m}\sum_{i_{m+1}}\cdots\sum_{i_e} \end{aligned}$$

$$
\begin{aligned}
&\sqrt{p_{1i_1}p_{1i'_1}\cdots p_{mi_m}p_{mi'_m}}\\
&\times\left|i_1,\cdots,i_m,M_A(i_1,\ldots,i_m,i_{m+1},\ldots,i_e)^\top\right\rangle\\
&\left\langle i'_1,\cdots,i'_m,M_A(i'_1,\ldots,i'_m,i_{m+1},\ldots,i_e)^\top\right|\\
&\times\left\langle M_B(i_1,\ldots,i_m,i_{m+1},\ldots,i_e)^\top\ \middle|M_B(i'_1,\ldots,i'_m,i_{m+1},\ldots,i_e)^\top\right\rangle. \quad (5.6)
\end{aligned}
$$

まず，*5.6*式の内積部分について考える．ここで，$B_x^{i_{m+1},\ldots,i_e}$ は明らかに $rank(M'_B) < m$ のときは複数の要素を持ち，$rank(M'_B) \geq m$ のときには唯一つの要素を持つ．そこで，以降はこれらを場合分けして考える．

(1) $rank(M'_B) < m$ の場合

$B_x^{i_{m+1},\ldots,i_e}$ は複数の要素を持つので，*5.6*式を $B_x^{i_{m+1},\ldots,i_e}$ を使って変形すると，

$$
\begin{aligned}
&\rho^{R_1\cdots R_mA}\\
&= \frac{1}{q^{e-m}}\sum_{i_{m+1}}\cdots\sum_{i_e}\sum_{x\in Im(M_B)}\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\sum_{(i'_1,\cdots,i'_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad\sqrt{p_{1i_1}p_{1i'_1}\cdots p_{mi_m}p_{mi'_m}}\\
&\quad\times\left|i_1,\cdots,i_m,\,M_A(i_1,\ldots,i_m,i_{m+1},\ldots,i_e)^\top\right\rangle\\
&\quad\left\langle i'_1,\cdots,i'_m,M_A(i'_1,\ldots,i'_m,i_{m+1},\ldots,i_e)^\top\right|. \quad (5.7)
\end{aligned}
$$

ここで，*5.7*式の固有ベクトルとなるように，以下のようなベクトル $\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle$ を考える．

$$
\begin{aligned}
&\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle\\
&= \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\sqrt{\frac{p_{1i_1}\cdots p_{mi_m}}{\sum_{(i'_1,\cdots,i'_m)\in B_x^{i_{m+1},\ldots,i_e}}p_{1i'_1}\cdots p_{mi'_m}}}\\
&\quad\times\left|i_1,\cdots,i_m,M_A(i_1,\ldots,i_m,i_{m+1},\ldots,i_e)^\top\right\rangle.
\end{aligned}
$$

このとき，*5.7*式は，

$$
\begin{aligned}
&\rho^{R_1\cdots R_mA}\\
&= \frac{1}{q^{e-m}}\sum_{i_{m+1}}\cdots\sum_{i_e}\sum_{x\in Im(M_B)}\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}p_{1i_1}\cdots p_{mi_m}\\
&\quad\times\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle\left\langle\phi_x^{i_{m+1},\cdots,i_e}\right|. \quad (5.8)
\end{aligned}
$$

となる．次に，同じ固有ベクトルをまとめるため，さらに場合を分けて考える．$e-m \leq rank(M_A)=t-1$ のときは，与えられた $x \in Im(M)$ について，異なる $(i_{m+1},\cdots,i_e)$ の組に対し，$|\phi_x^{i_{m+1},\cdots,i_e}\rangle$ が同じベクトルになることはない．$e-m > rank(M_A)=t-1$ の場合は，異なる $(i_{m+1},\cdots,i_e)$ の組に対し，同じベクトルとなるものが存在することが分かる．

(1-a) $e-m \leq t-1$ の場合

異なる $(i_{m+1},\cdots,i_e)$ の組に対し，固有ベクトル $|\phi_x^{i_{m+1},\cdots,i_e}\rangle$ が同一になることはない．よって，このときのエントロピーは，

$$
\begin{aligned}
&S(R_1\cdots R_m A)\\
&= -\frac{1}{q^{e-m}}\sum_{i_{m+1}}\cdots\sum_{i_e}\sum_{x\in Im(M_B)}\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log\frac{1}{q^{e-m}}p_{1i_1}\cdots p_{mi_m}\\
&= (e-m)\log q\\
&\quad -\sum_{x\in Im(M_B)}\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}} p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}. \quad (5.9)
\end{aligned}
$$

(1-b) $e-m > t-1$ の場合

異なる $(i_{m+1},\cdots,i_e)$ の組に対し，固有ベクトル $|\phi_x^{i_{m+1},\cdots,i_e}\rangle$ が同一になるものが存在する．そのとき，各固有ベクトルを $|\phi_j\rangle$ とすると，各 $|\phi_j\rangle$ に対し，$(i_1,\cdots,i_e)$ の組み合わせは $q^{e-m-(t-1)}$ 通り存在する．よって，*5.8* 式は以下のように変形される．

$$
\begin{aligned}
&\rho^{R_1\cdots R_m A}\\
&= \frac{q^{e-m-(t-1)}}{q^{e-m}}\sum_{x\in Im(M_B)}\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}\sum_j p_{1i_1}\cdots p_{mi_m}|\phi_j\rangle\langle\phi_j|.
\end{aligned}
$$

固有ベクトル $|\phi_j\rangle$ は，全部で q^{t-1} 通り考えられるので，そのときのエントロピーは，

$$
\begin{aligned}
&S(R_1\cdots R_m A)\\
&= -q^{t-1}\frac{1}{q^{t-1}}
\end{aligned}
$$

$$
\begin{aligned}
& \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log \frac{1}{q^{t-1}} p_{1i_1} \cdots p_{mi_m} \\
= \ & (t-1) \log q \\
& - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m}. \quad (5.10)
\end{aligned}
$$

(2) $rank(M'_B) \geq m$ の場合

この場合は，$B_x^{i_{m+1},\ldots,i_e}$ は唯一つの要素を持つ．すなわち，異なる $(i_1, \cdots, i_m)$ で $|M_B(i_1, \cdots, i_e)^\top\rangle$ が同じになることはない．よって，*5.6* 式は，以下のようになる．

$$
\begin{aligned}
& \rho^{R_1 \cdots R_m A} \\
= \ & \frac{1}{q^{e-m}} \sum_{i_1} \cdots \sum_{i_e} p_{1i_1} \cdots p_{mi_m} \\
& \times \left| i_1, \cdots, i_m, M_A(i_1, \ldots, i_e)^\top \right\rangle \left\langle i_1, \cdots, i_m, M_A(i_1, \ldots, i_e)^\top \right| .
\end{aligned}
$$

次に，*(1)* と同様に，同じ固有ベクトルとなるもの同士をまとめる．

(2-a) $e - m \leq t - 1$ の場合

異なる $(i_{m+1}, \cdots, i_e)$ の組に対し，固有ベクトル $|\phi_x^{i_{m+1},\cdots,i_e}\rangle$ が同一になることはない．よって，このときのエントロピーは，

$$
\begin{aligned}
& S(R_1 \cdots R_m A) \\
= \ & -\frac{1}{q^{e-m}} \sum_{i_1} \cdots \sum_{i_e} p_{1i_1} \cdots p_{mi_m} \log \frac{1}{q^{e-m}} p_{1i_1} \cdots p_{mi_m} \\
= \ & (e-m) \log q + \sum_{i}^{m} S(S_i). \quad (5.11)
\end{aligned}
$$

(2-b) $e - m > t - 1$ の場合

異なる $(i_{m+1}, \cdots, i_e)$ の組に対し，固有ベクトル $|\phi_x^{i_{m+1},\cdots,i_e}\rangle$ が同一になるものが存在する．そのとき，各固有ベクトルを $|\phi_j\rangle$ とすると，それぞれの $|\phi_j\rangle$ に対し，$(i_1, \cdots, i_e)$ の組み合わせは $q^{e-m-(t-1)}$ 通りである．

よって，

$$\rho^{R_1\cdots R_m A} = \frac{q^{e-m-(t-1)}}{q^{e-m}}\sum_{i_1}\cdots\sum_{i_m}\sum_{j} p_{1i_1}\cdots p_{mi_m}\left|\phi_j\right\rangle\left\langle\phi_j\right|.$$

$|\phi_j\rangle$ は，q^{t-1} とおり考えられるので，そのときのエントロピーは，

$$\begin{aligned} S(R_1\cdots R_m A) &= -q^{t-1}\frac{1}{q^{t-1}}\sum_{i_1}\cdots\sum_{i_m} p_{1i_1}\cdots p_{mi_m}\log\frac{1}{q^{t-1}}p_{1i_1}\cdots p_{mi_m} \\ &= (t-1)\log q + \sum_{i}^{m} S(S_i). \end{aligned} \tag{5.12}$$

■

次に，S_1 を復元する場合を考え，$S(R_2\cdots R_m A)$ を計算する．その結果については補題 *9*が成り立つ．なお，S_1 以外の秘密についても同様に成り立つ．

補題 9 列独立な $d\times e$ 行列を持つ *MSP* を用いて構成された (m,t,d) 量子閾値複数秘密分散法において，$|A|=t-1$ となる集合 $A\subseteq\mathcal{P}$ について以下が成り立つ．ここで $B=\mathcal{P}\setminus A$，M'_B は M_B から $m+1$ 列目以降を取り除いた行列とし，ある $x\in Im(M_B), i_1, i_{m+1},\ldots,i_e$ に対し，

$$M_B(i_1,i_2\cdots,i_m,i_{m+1},\cdots,i_e)^{\top} = x.$$

を満たす $(i_2,\ldots,i_m)$ の集合を $B_x^{i_1,i_{m+1},\ldots,i_e}$ とする．

(1-a) $rank(M'_B)<m-1, e-(m-1)\le t-1$ の場合

$$\begin{aligned} S(R_2\cdots R_m A) &= (e-m)\log q + S(S_1) \\ &\quad - \sum_{x\in Im(M_B)}\sum_{(i_2,\cdots,i_m)\in B_x^{i_1,i_{m+1},\ldots,i_e}} (p_{2i_2}\cdots p_{mi_m}\log p_{2i_2}\cdots p_{mi_m}). \end{aligned} \tag{5.13}$$

(1-b) $rank(M'_B) < m-1, e-(m-1) > t-1$ の場合

$$
\begin{aligned}
& S(R_2 \cdots R_m A) \\
& = (t-1)\log q \\
& \quad - \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} (p_{2i_2} \cdots p_{mi_m} \log p_{2i_21} \cdots p_{mi_m}) \qquad (5.14)
\end{aligned}
$$

(2-a) $rank(M'_B) \geq m, e-(m-1) \leq t-1$ の場合

$$
S(R_2 \cdots R_m A) = (e-m)\log q + \sum_{i=1}^{m} S(S_i). \qquad (5.15)
$$

(2-b) $rank(M'_B) \geq m, e-(m-1) > t-1$ の場合

$$
S(R_2 \cdots R_m A) = (t-1)\log q + \sum_{i=2}^{m} S(S_i). \qquad (5.16)
$$

Proof 補題 *8* と同様に，$B_x^{i_1,i_{m+1},\ldots,i_e}$ と同一の固有ベクトルの存在で場合分けをすることで求められるため省略する． ■

補題 *8*，*9* から，*(1)* あるいは *(2)* を満たさないときに，*Secrecy* が満たされないことを示す．

1. $rank(M'_B) < m-1, e-m \leq t-2$ の場合
5.2 式と *5.13* 式より，

$$
\begin{aligned}
& S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\
& = (e-m)\log q \\
& \quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
& \quad -((e-m)\log q + S(S_1) \\
& \quad - \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} p_{2i_2} \cdots p_{mi_m} \log p_{2i_2} \cdots p_{mi_m})
\end{aligned}
$$

$$
\begin{aligned}
&= -S(S_1) \\
&\quad + \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} p_{2i_2} \cdots p_{mi_m} \log p_{2i_2} \cdots p_{mi_m} \\
&\quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
&\neq S(S_1). \qquad (5.17)
\end{aligned}
$$

よって，*Secrecy* は満たされない．

2. $rank(M'_B) < m-1, e-m = t-1$ の場合

5.2 式と *5.14* 式より，

$$
\begin{aligned}
&S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\
&= ((e-m)\log q \\
&\quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
&\quad -(-(t-1)\log q \\
&\quad - \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} p_{2i_2} \cdots p_{mi_m} \log p_{2i_2} \cdots p_{mi_m}) \\
&\neq S(S_1). \qquad (5.18)
\end{aligned}
$$

よって，*Secrecy* は満たされない．

3. $rank(M'_B) < m-1, e-m > t-1$ の場合

5.3 式と *5.14* 式より，

$$
\begin{aligned}
&S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\
&= (t-1)\log q \\
&\quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
&\quad -(-(t-1)\log q \\
&\quad - \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} p_{2i_2} \cdots p_{mi_m} \log p_{2i_2} \cdots p_{mi_m}) \\
&= \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} p_{2i_2} \cdots p_{mi_m} \log p_{2i_2} \cdots p_{mi_m} \\
&\quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m}
\end{aligned}
$$

$$\neq \quad S(S_1). \tag{5.19}$$

よって，*Secrecy* は満たされない．

4. $rank(M'_B) = m-1, e-m \leq t-2$ の場合

5.2 式と *5.15* 式より，

$$\begin{aligned}
& S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\
= \quad & (e-m)\log q \\
& - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
& -((e-m)\log q + \sum_{i=1}^{m} S(S_i)) \\
= \quad & - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
& - \sum_{i=1}^{m} S(S_i) \\
\neq \quad & S(S_1).
\end{aligned} \tag{5.20}$$

よって，*Secrecy* は満たされない．

5. $rank(M'_B) = m-1, e-m = t-1$ の場合

5.2 式と *5.16* 式より，

$$\begin{aligned}
& S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\
= \quad & (e-m)\log q \\
& - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
& -(t-1)\log q + \sum_{i=2}^{m} S(S_i) \\
\neq \quad & S(S_1).
\end{aligned} \tag{5.21}$$

よって，*Secrecy* は満たされない．

6. $rank(M'_B) = m-1, e-m > t-1$ の場合

5.3 式と *5.16* 式より，

$$S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A)$$

$$
\begin{aligned}
&= (t-1)\log q \\
&\quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
&\quad -(t-1)\log q + \sum_{i=2}^{m} S(S_i)) \\
&= - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m} \\
&\quad - \sum_{i=2}^{m} S(S_i) \\
&\neq S(S_1). \qquad (5.22)
\end{aligned}
$$

よって，*Secrecy* は満たされない．

7. $rank(M'_B) \geq m, e-m \leq t-2$ の場合

5.4 式と *5.15* 式より，

$$
\begin{aligned}
&S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\
&= (e-m)\log q + \sum_{i=1}^{m} S(S_i) - ((e-m)\log q + \sum_{i=1}^{m} S(S_i)) \\
&= 0 \\
&\neq S(S_1). \qquad (5.23)
\end{aligned}
$$

よって，*Secrecy* は満たされない．

以上から，$d = |A| + |B|$，$|B| \geq rank(M'_B)$ より，$d < t+m-1$ と $e < m+t-1$ のどちらか一方でも成り立っているときは，*Secrecy* が満たされない場合が存在することが示された． ■

定理 5 を，(m,t,d) 量子閾値複数秘密分散法について検証すると，以下の定理が成り立つ．

定理 6 *MSP* を用いて構成された (m,t,d) 量子閾値複数秘密分散法は，*Secrecy* を満たすとき，かつそのときに限り，以下の *2* 条件を満たす．

1. $d \geq t+m-1$.
2. $e \geq t+m-1$.

Proof　定理 *5* より必要条件は満たしている．十分条件について考える．定理の条件の *(1)* を満たすとき $rank(M'_B) \geq m$ である．このとき，補題 *8*，*9* の条件を考えて，

1. $rank(M'_B) \geq m, e-m = t-1$ の場合
   5.4 式と *5.16* 式より，

$$\begin{aligned} & S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\ &= (e-m)\log q + \sum_{i=1}^{m} S(S_i) - ((t-1)\log q + \sum_{i=2}^{m} S(S_i)) \\ &= S(S_1). \end{aligned} \tag{5.24}$$

   よって，*Secrecy* を満たす．
2. $rank(M'_B) \geq m, e-m > t-1$ の場合
   5.5 式と *5.16* 式より，

$$\begin{aligned} & S(R_1 \cdots R_m A) - S(R_2 \cdots R_m A) \\ &= (t-1)\log q + \sum_{i=1}^{m} S(S_i) - ((t-1)\log q + \sum_{i=2}^{m} S(S_i)) \\ &= S(S_1). \end{aligned} \tag{5.25}$$

   よって，*Secrecy* を満たす．

したがって，$d \geq t+m-1$ と $e \geq t+m-1$ の両方を満たしているときには *Secrecy* を満たす．以上から十分条件も満たしている．■

また，Recoverability については以下の定理が成り立つ．

定理 7 *MSP* を用いて構成された量子複数秘密分散法について，$\forall A \in \Gamma_i$ $(1 \leq \forall i \leq m)$ に対し *Recoverability* を満たす．

Proof　*Secrecy* を証明した補題 *8*，*9*，及び定理 *5* と同様に *Recoverability* の式を展開し，各 *von Neumann* エントロピーを計算すればよいので省略する．■

さらに，MSP を用いて構成された (m, t, d) 量子閾値複数秘密分散法について，以下の定理が成り立つ．

定理 8 *MSP* を用いて構成された (m,t,d) 量子閾値複数秘密分散法において，$t \leq m$ を満たす *QSSS* は存在しない．

Proof $t \leq m$ と仮定する．このとき，$|A| = t$ であり，定理 *6* より $e \geq 2t-1$ である．したがって，M_A は t 行 $2t-1$ 列よりも列が多い行列となる．これを復元する復元行列 V は M_A の前 t 列の逆行列でなければならず，残りの列を復元行列にかけると零行列とならなければならない．したがって，残りの列はすべて零の列ベクトルとなる．量子閾値複数秘密分散法であるので，任意の A について成り立つため，M の $t+1$ 列目以降は零行列である．したがって，M の列独立性を満たさないので，M に対応する等長写像 θ_M が存在しない． ■

量子複数秘密分散法について，秘密が 1 つの量子状態の場合について得られていた定理 [16] の単純な拡張により，以下の定理が得られる．

定理 9 *1.* (m,t,d) 量子閾値複数秘密分散法において，$2t \leq d$ となる *QSSS* は存在しない．

2. 量子複数秘密分散法において，任意の秘密 S_i に対して互いに素なシェア集合から秘密を復元できる *Access* 構造 Γ_i を持つ *QSSS* は存在しない．

Proof *1.* $2t \leq d$ となる量子複数秘密分散法が存在すると，互いに素なシェア集合から秘密の情報がそれぞれで復元できる．しかしながら，このことは *no-cloning* 定理 *[20, 52]* に反する．

2. (1) と同様 *no-cloning* 定理に反する．

■

5.3 構成例

この章では量子複数秘密分散の例として，$\mathbb{F}_5$ 上で，秘密 2 つと閾値 3 を持つ，量子閾値複数秘密分散法を具体的に構成する．秘密が 1 つの場合の (t,d) 閾値秘密分散法では列数が閾値 t となる Vandermonde 行列を用いることにより構成することができた．しかしながら (m,t,d) 量子閾値複数秘密分散法は定理 6 より M の行数と列数がそれぞれ $t+m-1$ 以上でなければ Secrecy を満たさない．Vandermonde

行列で構成するためには列数が閾値 t でなければならず，$t \geq t+m-1$ となるのは明らかに $m=1$，すなわち秘密が 1 つの場合のみである．以上から，(m,t,d) 量子閾値複数秘密分散法は Vandermonde 行列では構成できないことが分かる．

シェアの配布

1. ディーラは以下の秘密の量子状態を純粋化し用意する．

$$
\begin{aligned}
|R_1S_1\rangle &= \sum_{i_1=0}^{4} \sqrt{p_{1i_1}}|i_1^{R_1}\rangle \otimes |i_1^{S_1}\rangle, \\
|R_2S_2\rangle &= \sum_{i_2=0}^{4} \sqrt{p_{2i_2}}|i_2^{R_2}\rangle \otimes |i_2^{S_2}\rangle.
\end{aligned}
$$

2. $t+m-1=4$ であるので，次の行列 M' を考える．

$$
M' = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 2 \end{pmatrix}.
$$

この行列は，任意に 3 行を取ると $\mathbf{e}_1$ と $\mathbf{e}_2$) の 2 つの行ベクトルを構成でき[2]，定理 6 の条件を満たしているので Secrecy も満たす．よって，秘密 2 状態，閾値 3 の量子閾値複数秘密分散法になる．しかし，この行列は列独立性を満たさないので，対応する等長写像が存在しない．そこで，列独立となるように補助的にシェアを作り出す 1 行を加えて M とする．

$$
M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.
$$

3. 補助状態として $|R_EE\rangle = \frac{1}{5^2}\sum_{a\in\mathbb{F}_5^2}|a\rangle \otimes |a\rangle$ を用意する．
4. M に対応する等長写像 θ_M を用いて分散する．

$$
\begin{aligned}
&(I_{\mathcal{R}} \otimes \theta_M)|\mathcal{R}SE\rangle \\
&\quad = |R_1R_2R_EP_1P_2P_3P_4P_5\rangle.
\end{aligned}
$$

[2]任意の 3 行とその前 3 列からなる部分行列に逆行列が存在するため．この逆行列を復元時の行列 V として使用する．

5. $P_1, \cdots, P_4$ をシェアとして参加者に配布する．P_5 についてはシェアとして使用せず，ディーラが保存する．

このとき分散した結果は以下のようになる．

$$
\begin{aligned}
&|R_1R_2R_{E_1}R_{E_2}P_1P_2P_3P_4P_5\rangle \\
&= \frac{1}{\sqrt{5^2}}(\sqrt{p_{10}p_{20}} \\
&\quad \times(|000000000\rangle + |000101121\rangle + |000202242\rangle + |000303313\rangle + |000404434\rangle \\
&\quad +|001001120\rangle + |001102241\rangle + |001203312\rangle + |001304433\rangle + |001400004\rangle \\
&\quad +|002002240\rangle + |002103311\rangle + |002204432\rangle + |002300003\rangle + |002401124\rangle \\
&\quad +|003003310\rangle + |003104431\rangle + |003200002\rangle + |003301123\rangle + |003402244\rangle \\
&\quad +|004004430\rangle + |004100001\rangle + |004201122\rangle + |004302243\rangle + |004403314\rangle) \\
&\quad +\sqrt{p_{10}p_{21}} \\
&\quad \times(|010011210\rangle + |010112331\rangle + |010213402\rangle + |010314023\rangle + |010410144\rangle \\
&\quad +|011012330\rangle + |011113401\rangle + |011214022\rangle + |011310143\rangle + |011411214\rangle \\
&\quad +|012013400\rangle + |012114021\rangle + |012210142\rangle + |012311213\rangle + |012412334\rangle \\
&\quad +|013014020\rangle + |013110141\rangle + |013211212\rangle + |013312333\rangle + |013413404\rangle \\
&\quad +|014010140\rangle + |014111211\rangle + |014212332\rangle + |014313403\rangle + |014414024\rangle) \\
&\quad +\sqrt{p_{10}p_{22}} \\
&\quad \times(|020022420\rangle + |020123041\rangle + |020224112\rangle + |020320233\rangle + |020421304\rangle \\
&\quad +|021023040\rangle + |021124111\rangle + |021220232\rangle + |021321303\rangle + |021422424\rangle \\
&\quad +|022024110\rangle + |022120231\rangle + |022221302\rangle + |022322423\rangle + |022423044\rangle \\
&\quad +|023020230\rangle + |023121301\rangle + |023222422\rangle + |023323043\rangle + |023424114\rangle \\
&\quad +|024021300\rangle + |024122421\rangle + |024223042\rangle + |024324113\rangle + |024420234\rangle) \\
&\quad +\sqrt{p_{10}p_{23}} \\
&\quad \times(|030033130\rangle + |030134201\rangle + |030230322\rangle + |030331443\rangle + |030432014\rangle \\
&\quad +|031034200\rangle + |031130321\rangle + |031231442\rangle + |031332013\rangle + |031433134\rangle \\
&\quad +|032030320\rangle + |032131441\rangle + |032232012\rangle + |032333133\rangle + |032434204\rangle \\
&\quad +|033031440\rangle + |033132011\rangle + |033233132\rangle + |033334203\rangle + |033430324\rangle \\
&\quad +|034032010\rangle + |034133131\rangle + |034234202\rangle + |034330323\rangle + |034431444\rangle) \\
&\quad +\sqrt{p_{10}p_{24}}
\end{aligned}
$$

$\times(|040044340\rangle + |040140411\rangle + |040241032\rangle + |040342103\rangle + |040443224\rangle$
$+|041040410\rangle + |041141031\rangle + |041242102\rangle + |041343223\rangle + |041444344\rangle$
$+|042041030\rangle + |042142101\rangle + |042243222\rangle + |042344343\rangle + |042440414\rangle$
$+|043042100\rangle + |043143221\rangle + |043244342\rangle + |043340413\rangle + |043441034\rangle$
$+|044043220\rangle + |044144341\rangle + |044240412\rangle + |044341033\rangle + |044442104\rangle)$
$+\sqrt{p_{11}p_{20}}$
$\times(|100012110\rangle + |100113231\rangle + |100214302\rangle + |100310423\rangle + |100411044\rangle$
$+|101013230\rangle + |101114301\rangle + |101210422\rangle + |101311043\rangle + |101412114\rangle$
$+|102014300\rangle + |102110421\rangle + |102211042\rangle + |102312113\rangle + |102413234\rangle$
$+|103010420\rangle + |103111041\rangle + |103212112\rangle + |103313233\rangle + |103414304\rangle$
$+|104011040\rangle + |104112111\rangle + |104213232\rangle + |104314303\rangle + |104410424\rangle)$
$+\sqrt{p_{11}p_{21}}$
$\times(|110023320\rangle + |110124441\rangle + |110220012\rangle + |110321133\rangle + |110422204\rangle$
$+|111024440\rangle + |111120011\rangle + |111221132\rangle + |111322203\rangle + |111423324\rangle$
$+|112020010\rangle + |112121131\rangle + |112222202\rangle + |112323323\rangle + |112424444\rangle$
$+|113021130\rangle + |113122201\rangle + |113223322\rangle + |113324443\rangle + |113420014\rangle$
$+|114022200\rangle + |114123321\rangle + |114224442\rangle + |114320013\rangle + |114421134\rangle)$
$+\sqrt{p_{11}p_{22}}$
$\times(|120034030\rangle + |120130101\rangle + |120231222\rangle + |120332343\rangle + |120433414\rangle$
$+|121030100\rangle + |121131221\rangle + |121232342\rangle + |121333413\rangle + |121434034\rangle$
$+|122031220\rangle + |122132341\rangle + |122233412\rangle + |122334033\rangle + |122430104\rangle$
$+|123032340\rangle + |123133411\rangle + |123234032\rangle + |123330103\rangle + |123431224\rangle$
$+|124033410\rangle + |124134031\rangle + |124230102\rangle + |124331223\rangle + |124432344\rangle)$
$+\sqrt{p_{11}p_{23}}$
$\times(|130040240\rangle + |130141311\rangle + |130242432\rangle + |130343003\rangle + |130444124\rangle$
$+|131041310\rangle + |131142431\rangle + |131243002\rangle + |131344123\rangle + |131440244\rangle$
$+|132042430\rangle + |132143001\rangle + |132244122\rangle + |132340243\rangle + |132441314\rangle$
$+|133043000\rangle + |133144121\rangle + |133240242\rangle + |133341313\rangle + |133442434\rangle$
$+|134044120\rangle + |134140241\rangle + |134241312\rangle + |134342433\rangle + |134443004\rangle)$
$+\sqrt{p_{11}p_{24}}$
$\times(|140001400\rangle + |140102021\rangle + |140203142\rangle + |140304213\rangle + |140400334\rangle$

$+|141002020\rangle + |141103141\rangle + |141204212\rangle + |141300333\rangle + |141401404\rangle$
$+|142003140\rangle + |142104211\rangle + |142200332\rangle + |142301403\rangle + |142402024\rangle$
$+|143004210\rangle + |143100331\rangle + |143201402\rangle + |143302023\rangle + |143403144\rangle$
$+|144000330\rangle + |144101401\rangle + |144202022\rangle + |144303143\rangle + |144404214\rangle)$
$+\sqrt{p_{12}p_{20}}$
$\times(|200024220\rangle + |200120341\rangle + |200221412\rangle + |200322033\rangle + |200423104\rangle$
$+|201020340\rangle + |201121411\rangle + |201222032\rangle + |201323103\rangle + |201424224\rangle$
$+|202021410\rangle + |202122031\rangle + |202223102\rangle + |202324223\rangle + |202420344\rangle$
$+|203022030\rangle + |203123101\rangle + |203224222\rangle + |203320343\rangle + |203421414\rangle$
$+|204023100\rangle + |204124221\rangle + |204220342\rangle + |204321413\rangle + |204422034\rangle)$
$+\sqrt{p_{12}p_{21}}$
$\times(|210030430\rangle + |210131001\rangle + |210232122\rangle + |210333243\rangle + |210434314\rangle$
$+|211031000\rangle + |211132121\rangle + |211233242\rangle + |211334313\rangle + |211430434\rangle$
$+|212032120\rangle + |212133241\rangle + |212234312\rangle + |212330433\rangle + |212431004\rangle$
$+|213033240\rangle + |213134311\rangle + |213230432\rangle + |213331003\rangle + |213432124\rangle$
$+|214034310\rangle + |214130431\rangle + |214231002\rangle + |214332123\rangle + |214433244\rangle)$
$+\sqrt{p_{12}p_{22}}$
$\times(|220041140\rangle + |220142211\rangle + |220243332\rangle + |220344403\rangle + |220440024\rangle$
$+|221042210\rangle + |221143331\rangle + |221244402\rangle + |221340023\rangle + |221441144\rangle$
$+|222043330\rangle + |222144401\rangle + |222240022\rangle + |222341143\rangle + |222442214\rangle$
$+|223044400\rangle + |223140021\rangle + |223241142\rangle + |223342213\rangle + |223443334\rangle$
$+|224040020\rangle + |224141141\rangle + |224242212\rangle + |224343333\rangle + |224444404\rangle)$
$+\sqrt{p_{12}p_{23}}$
$\times(|230002300\rangle + |230103421\rangle + |230204042\rangle + |230300113\rangle + |230401234\rangle$
$+|231003420\rangle + |231104041\rangle + |231200112\rangle + |231301233\rangle + |231402304\rangle$
$+|232004040\rangle + |232100111\rangle + |232201232\rangle + |232302303\rangle + |232403424\rangle$
$+|233000110\rangle + |233101231\rangle + |233202302\rangle + |233303423\rangle + |233404044\rangle$
$+|234001230\rangle + |234102301\rangle + |234203422\rangle + |234304043\rangle + |234400114\rangle)$
$+\sqrt{p_{12}p_{24}}$
$\times(|240013010\rangle + |240114131\rangle + |240210202\rangle + |240311323\rangle + |240412444\rangle$
$+|241014130\rangle + |241110201\rangle + |241211322\rangle + |241312443\rangle + |241413014\rangle$

$+|242010200\rangle + |242111321\rangle + |242212442\rangle + |242313013\rangle + |242414134\rangle$
$+|243011320\rangle + |243112441\rangle + |243213012\rangle + |243314133\rangle + |243410204\rangle$
$+|244012440\rangle + |244113011\rangle + |244214132\rangle + |244310203\rangle + |244411324\rangle)$
$+\sqrt{p_{13}p_{20}}$
$\times(|300031330\rangle + |300132401\rangle + |300233022\rangle + |300334143\rangle + |300430214\rangle$
$+|301032400\rangle + |301133021\rangle + |301234142\rangle + |301330213\rangle + |301431334\rangle$
$+|302033020\rangle + |302134141\rangle + |302230212\rangle + |302331333\rangle + |302432404\rangle$
$+|303034140\rangle + |303130211\rangle + |303231332\rangle + |303332403\rangle + |303433024\rangle$
$+|304030210\rangle + |304131331\rangle + |304232402\rangle + |304333023\rangle + |304434144\rangle)$
$+\sqrt{p_{13}p_{21}}$
$\times(|310042040\rangle + |310143111\rangle + |310244232\rangle + |310340303\rangle + |310441424\rangle$
$+|311043110\rangle + |311144231\rangle + |311240302\rangle + |311341423\rangle + |311442044\rangle$
$+|312044230\rangle + |312140301\rangle + |312241422\rangle + |312342043\rangle + |312443114\rangle$
$+|313040300\rangle + |313141421\rangle + |313242042\rangle + |313343113\rangle + |313444234\rangle$
$+|314041420\rangle + |314142041\rangle + |314243112\rangle + |314344233\rangle + |314440304\rangle)$
$+\sqrt{p_{13}p_{22}}$
$\times(|320003200\rangle + |320104321\rangle + |320200442\rangle + |320301013\rangle + |320402134\rangle$
$+|321004320\rangle + |321100441\rangle + |321201012\rangle + |321302133\rangle + |321403204\rangle$
$+|322000440\rangle + |322101011\rangle + |322202132\rangle + |322303203\rangle + |322404324\rangle$
$+|323001010\rangle + |323102131\rangle + |323203202\rangle + |323304323\rangle + |323400444\rangle$
$+|324002130\rangle + |324103201\rangle + |324204322\rangle + |324300443\rangle + |324401014\rangle)$
$+\sqrt{p_{13}p_{23}}$
$\times(|330014410\rangle + |330110031\rangle + |330211102\rangle + |330312223\rangle + |330413344\rangle$
$+|331010030\rangle + |331111101\rangle + |331212222\rangle + |331313343\rangle + |331414414\rangle$
$+|332011100\rangle + |332112221\rangle + |332213342\rangle + |332314413\rangle + |332410034\rangle$
$+|333012220\rangle + |333113341\rangle + |333214412\rangle + |333310033\rangle + |333411104\rangle$
$+|334013340\rangle + |334114411\rangle + |334210032\rangle + |334311103\rangle + |334412224\rangle)$
$+\sqrt{p_{13}p_{24}}$
$\times(|340020120\rangle + |340121241\rangle + |340222312\rangle + |340323433\rangle + |340424004\rangle$
$+|341021240\rangle + |341122311\rangle + |341223432\rangle + |341324003\rangle + |341420124\rangle$
$+|342022310\rangle + |342123431\rangle + |342224002\rangle + |342320123\rangle + |342421244\rangle$

$+|343023430\rangle + |343124001\rangle + |343220122\rangle + |343321243\rangle + |343422314\rangle$

$+|344024000\rangle + |344120121\rangle + |344221242\rangle + |344322313\rangle + |344423434\rangle)$

$+\sqrt{p_{14}p_{20}}$

$\times(|400043440\rangle + |400144011\rangle + |400240132\rangle + |400341203\rangle + |400442324\rangle$

$+|401044010\rangle + |401140131\rangle + |401241202\rangle + |401342323\rangle + |401443444\rangle$

$+|402040130\rangle + |402141201\rangle + |402242322\rangle + |402343443\rangle + |402444014\rangle$

$+|403041200\rangle + |403142321\rangle + |403243442\rangle + |403344013\rangle + |403440134\rangle$

$+|404042320\rangle + |404143441\rangle + |404244012\rangle + |404340133\rangle + |404441204\rangle)$

$+\sqrt{p_{14}p_{21}}$

$\times(|410004100\rangle + |410100221\rangle + |410201342\rangle + |410302413\rangle + |410403034\rangle$

$+|411000220\rangle + |411101341\rangle + |411202412\rangle + |411303033\rangle + |411404104\rangle$

$+|412001340\rangle + |412102411\rangle + |412203032\rangle + |412304103\rangle + |412400224\rangle$

$+|413002410\rangle + |413103031\rangle + |413204102\rangle + |413300223\rangle + |413401344\rangle$

$+|414003030\rangle + |414104101\rangle + |414200222\rangle + |414301343\rangle + |414402414\rangle)$

$+\sqrt{p_{14}p_{22}}$

$\times(|420010310\rangle + |420111431\rangle + |420212002\rangle + |420313123\rangle + |420414244\rangle$

$+|421011430\rangle + |421112001\rangle + |421213122\rangle + |421314243\rangle + |421410314\rangle$

$+|422012000\rangle + |422113121\rangle + |422214242\rangle + |422310313\rangle + |422411434\rangle$

$+|423013120\rangle + |423114241\rangle + |423210312\rangle + |423311433\rangle + |423412004\rangle$

$+|424014240\rangle + |424110311\rangle + |424211432\rangle + |424312003\rangle + |424413124\rangle)$

$+\sqrt{p_{14}p_{23}}$

$\times(|430021020\rangle + |430122141\rangle + |430223212\rangle + |430324333\rangle + |430420404\rangle$

$+|431022140\rangle + |431123211\rangle + |431224332\rangle + |431320403\rangle + |431421024\rangle$

$+|432023210\rangle + |432124331\rangle + |432220402\rangle + |432321023\rangle + |432422144\rangle$

$+|433024330\rangle + |433120401\rangle + |433221022\rangle + |433322143\rangle + |433423214\rangle$

$+|434020400\rangle + |434121021\rangle + |434222142\rangle + |434323213\rangle + |434424334\rangle)$

$+\sqrt{p_{14}p_{24}}$

$\times(|440032230\rangle + |440133301\rangle + |440234422\rangle + |440330043\rangle + |440431114\rangle$

$+|441033300\rangle + |441134421\rangle + |441230042\rangle + |441331113\rangle + |441432234\rangle$

$+|442034420\rangle + |442130041\rangle + |442231112\rangle + |442332233\rangle + |442433304\rangle$

$+|443030040\rangle + |443131111\rangle + |443232232\rangle + |443333303\rangle + |443434424\rangle$

$$+|444031110\rangle+|444132231\rangle+|444233302\rangle+|444334423\rangle+|444430044\rangle)) \tag{5.26}$$

これを，$\{P_1, P_2, P_3\}$ で復元することを考える．V として，以下の値を取る．

$$V = \begin{pmatrix} 3 & 3 & 2 \\ 3 & 2 & 3 \\ 1 & 3 & 3 \end{pmatrix}. \tag{5.27}$$

この V は列独立性を満たすので，対応する等長写像 θ_V が存在する．よって，θ_V を使って復元すると，

$$\begin{aligned}
&(I_{\mathcal{R}} \otimes \theta_V \otimes I_{P_4,P_5})|R_1R_2R_{E_1}R_{E_2}P_1P_2P_3P_4P_5\rangle \\
&= \frac{1}{\sqrt{5^2}}(\sqrt{p_{10}p_{20}} \\
&\quad \times(|000000000\rangle+|000100121\rangle+|000200242\rangle+|000300313\rangle+|000400434\rangle \\
&\quad +|001000120\rangle+|001100241\rangle+|001200312\rangle+|001300433\rangle+|001400004\rangle \\
&\quad +|002000240\rangle+|002100311\rangle+|002200432\rangle+|002300003\rangle+|002400124\rangle \\
&\quad +|003000310\rangle+|003100431\rangle+|003200002\rangle+|003300123\rangle+|003400244\rangle \\
&\quad +|004000430\rangle+|004100001\rangle+|004200122\rangle+|004300243\rangle+|004400314\rangle)) \\
&\quad +\sqrt{p_{10}p_{21}} \\
&\quad \times(|010001010\rangle+|010101131\rangle+|010201202\rangle+|010301323\rangle+|010401444\rangle \\
&\quad +|011001130\rangle+|011101201\rangle+|011201322\rangle+|011301443\rangle+|011401014\rangle \\
&\quad +|012001200\rangle+|012101321\rangle+|012201442\rangle+|012301013\rangle+|012401134\rangle \\
&\quad +|013001320\rangle+|013101441\rangle+|013201012\rangle+|013301133\rangle+|013401204\rangle \\
&\quad +|014001440\rangle+|014101011\rangle+|014201132\rangle+|014301203\rangle+|014401324\rangle)) \\
&\quad +\sqrt{p_{10}p_{22}} \\
&\quad \times(|020002020\rangle+|020102141\rangle+|020202212\rangle+|020302333\rangle+|020402404\rangle \\
&\quad +|021002140\rangle+|021102211\rangle+|021202332\rangle+|021302403\rangle+|021402024\rangle \\
&\quad +|022002210\rangle+|022102331\rangle+|022202402\rangle+|022302023\rangle+|022402144\rangle \\
&\quad +|023002330\rangle+|023102401\rangle+|023202022\rangle+|023302143\rangle+|023402214\rangle \\
&\quad +|024002400\rangle+|024102021\rangle+|024202142\rangle+|024302213\rangle+|024402334\rangle)) \\
&\quad +\sqrt{p_{10}p_{23}} \\
&\quad \times(|030003030\rangle+|030103101\rangle+|030203222\rangle+|030303343\rangle+|030403414\rangle \\
&\quad +|031003100\rangle+|031103221\rangle+|031203342\rangle+|031303413\rangle+|031403034\rangle \\
&\quad +|032003220\rangle+|032103341\rangle+|032203412\rangle+|032303033\rangle+|032403104\rangle
\end{aligned}$$

$+|033003340\rangle + |033103411\rangle + |033203032\rangle + |033303103\rangle + |033403224\rangle$

$+|034003410\rangle + |034103031\rangle + |034203102\rangle + |034303223\rangle + |034403344\rangle)$

$+\sqrt{p_{10}p_{24}}$

$\times(|040004040\rangle + |040104111\rangle + |040204232\rangle + |040304303\rangle + |040404424\rangle$

$+|041004110\rangle + |041104231\rangle + |041204302\rangle + |041304423\rangle + |041404044\rangle$

$+|042004230\rangle + |042104301\rangle + |042204422\rangle + |042304043\rangle + |042404114\rangle$

$+|043004300\rangle + |043104421\rangle + |043204042\rangle + |043304113\rangle + |043404234\rangle$

$+|044004420\rangle + |044104041\rangle + |044204112\rangle + |044304233\rangle + |044404304\rangle)$

$+\sqrt{p_{11}p_{20}}$

$\times(|100010010\rangle + |100110131\rangle + |100210202\rangle + |100310323\rangle + |100410444\rangle$

$+|101010130\rangle + |101110201\rangle + |101210322\rangle + |101310443\rangle + |101410014\rangle$

$+|102010200\rangle + |102110321\rangle + |102210442\rangle + |102310013\rangle + |102410134\rangle$

$+|103010320\rangle + |103110441\rangle + |103210012\rangle + |103310133\rangle + |103410204\rangle$

$+|104010440\rangle + |104110011\rangle + |104210132\rangle + |104310203\rangle + |104410324\rangle)$

$+\sqrt{p_{11}p_{21}}$

$\times(|110011020\rangle + |110111141\rangle + |110211212\rangle + |110311333\rangle + |110411404\rangle$

$+|111011140\rangle + |111111211\rangle + |111211332\rangle + |111311403\rangle + |111411024\rangle$

$+|112011210\rangle + |112111331\rangle + |112211402\rangle + |112311023\rangle + |112411144\rangle$

$+|113011330\rangle + |113111401\rangle + |113211022\rangle + |113311143\rangle + |113411214\rangle$

$+|114011400\rangle + |114111021\rangle + |114211142\rangle + |114311213\rangle + |114411334\rangle)$

$+\sqrt{p_{11}p_{22}}$

$\times(|120012030\rangle + |120112101\rangle + |120212222\rangle + |120312343\rangle + |120412414\rangle$

$+|121012100\rangle + |121112221\rangle + |121212342\rangle + |121312413\rangle + |121412034\rangle$

$+|122012220\rangle + |122112341\rangle + |122212412\rangle + |122312033\rangle + |122412104\rangle$

$+|123012340\rangle + |123112411\rangle + |123212032\rangle + |123312103\rangle + |123412224\rangle$

$+|124012410\rangle + |124112031\rangle + |124212102\rangle + |124312223\rangle + |124412344\rangle)$

$+\sqrt{p_{11}p_{23}}$

$\times(|130013040\rangle + |130113111\rangle + |130213232\rangle + |130313303\rangle + |130413424\rangle$

$+|131013110\rangle + |131113231\rangle + |131213302\rangle + |131313423\rangle + |131413044\rangle$

$+|132013230\rangle + |132113301\rangle + |132213422\rangle + |132313043\rangle + |132413114\rangle$

$+|133013300\rangle + |133113421\rangle + |133213042\rangle + |133313113\rangle + |133413234\rangle$

$+|134013420\rangle + |134113041\rangle + |134213112\rangle + |134313233\rangle + |134413304\rangle)$

$+\sqrt{p_{11}p_{24}}$

$\times(|140014000\rangle + |140114121\rangle + |140214242\rangle + |140314313\rangle + |140414434\rangle$

$+|141014120\rangle + |141114241\rangle + |141214312\rangle + |141314433\rangle + |141414004\rangle$

$+|142014240\rangle + |142114311\rangle + |142214432\rangle + |142314003\rangle + |142414124\rangle$

$+|143014310\rangle + |143114431\rangle + |143214002\rangle + |143314123\rangle + |143414244\rangle$

$+|144014430\rangle + |144114001\rangle + |144214122\rangle + |144314243\rangle + |144414314\rangle)$

$+\sqrt{p_{12}p_{20}}$

$\times(|200020020\rangle + |200120141\rangle + |200220212\rangle + |200320333\rangle + |200420404\rangle$

$+|201020140\rangle + |201120211\rangle + |201220332\rangle + |201320403\rangle + |201420024\rangle$

$+|202020210\rangle + |202120331\rangle + |202220402\rangle + |202320023\rangle + |202420144\rangle$

$+|203020330\rangle + |203120401\rangle + |203220022\rangle + |203320143\rangle + |203420214\rangle$

$+|204020400\rangle + |204120021\rangle + |204220142\rangle + |204320213\rangle + |204420334\rangle)$

$+\sqrt{p_{12}p_{21}}$

$\times(|210021030\rangle + |210121101\rangle + |210221222\rangle + |210321343\rangle + |210421414\rangle$

$+|211021100\rangle + |211121221\rangle + |211221342\rangle + |211321413\rangle + |211421034\rangle$

$+|212021220\rangle + |212121341\rangle + |212221412\rangle + |212321033\rangle + |212421104\rangle$

$+|213021340\rangle + |213121411\rangle + |213221032\rangle + |213321103\rangle + |213421224\rangle$

$+|214021410\rangle + |214121031\rangle + |214221102\rangle + |214321223\rangle + |214421344\rangle)$

$+\sqrt{p_{12}p_{22}}$

$\times(|220022040\rangle + |220122111\rangle + |220222232\rangle + |220322303\rangle + |220422424\rangle$

$+|221022110\rangle + |221122231\rangle + |221222302\rangle + |221322423\rangle + |221422044\rangle$

$+|222022230\rangle + |222122301\rangle + |222222422\rangle + |222322043\rangle + |222422114\rangle$

$+|223022300\rangle + |223122421\rangle + |223222042\rangle + |223322113\rangle + |223422234\rangle$

$+|224022420\rangle + |224122041\rangle + |224222112\rangle + |224322233\rangle + |224422304\rangle)$

$+\sqrt{p_{12}p_{23}}$

$\times(|230023000\rangle + |230123121\rangle + |230223242\rangle + |230323313\rangle + |230423434\rangle$

$+|231023120\rangle + |231123241\rangle + |231223312\rangle + |231323433\rangle + |231423004\rangle$

$+|232023240\rangle + |232123311\rangle + |232223432\rangle + |232323003\rangle + |232402314\rangle$

$+|233023310\rangle + |233123431\rangle + |233223002\rangle + |233323123\rangle + |233423244\rangle$

$+|234023430\rangle + |234123001\rangle + |234223122\rangle + |234323243\rangle + |234423314\rangle)$

$+\sqrt{p_{12}p_{24}}$

$\times(|240024010\rangle + |240124131\rangle + |240224202\rangle + |240324323\rangle + |240424444\rangle$

$+|241024130\rangle + |241124201\rangle + |241224322\rangle + |241324443\rangle + |241424014\rangle$

$+|242024200\rangle + |242124321\rangle + |242224442\rangle + |242324013\rangle + |242424134\rangle$

$+|243024320\rangle + |243124441\rangle + |243224012\rangle + |243324133\rangle + |243424204\rangle$

$+|244024440\rangle + |244124011\rangle + |244224132\rangle + |244324203\rangle + |244424324\rangle)$

$+\sqrt{p_{13}p_{20}}$

$\times(|300030030\rangle + |300130101\rangle + |300230222\rangle + |300330343\rangle + |300430414\rangle$

$+|301030100\rangle + |301130221\rangle + |301230342\rangle + |301330413\rangle + |301430034\rangle$

$+|302030220\rangle + |302130341\rangle + |302230412\rangle + |302330033\rangle + |302430104\rangle$

$+|303030340\rangle + |303130411\rangle + |303230032\rangle + |303330103\rangle + |303430224\rangle$

$+|304030410\rangle + |304130031\rangle + |304230102\rangle + |304330223\rangle + |304430344\rangle)$

$+\sqrt{p_{13}p_{21}}$

$\times(|310031040\rangle + |310131111\rangle + |310231232\rangle + |310331303\rangle + |310431424\rangle$

$+|311031110\rangle + |311131231\rangle + |311231302\rangle + |311331423\rangle + |311431044\rangle$

$+|312031230\rangle + |312131301\rangle + |312231422\rangle + |312331043\rangle + |312431114\rangle$

$+|313031300\rangle + |313131421\rangle + |313231042\rangle + |313331113\rangle + |313431234\rangle$

$+|314031420\rangle + |314131041\rangle + |314231112\rangle + |314331233\rangle + |314431304\rangle)$

$+\sqrt{p_{13}p_{22}}$

$\times(|320032000\rangle + |320132121\rangle + |320232242\rangle + |320332313\rangle + |320432434\rangle$

$+|321032120\rangle + |321132241\rangle + |321232312\rangle + |321332433\rangle + |321432004\rangle$

$+|322032240\rangle + |322132311\rangle + |322232432\rangle + |322332003\rangle + |322432124\rangle$

$+|323032310\rangle + |323132431\rangle + |323232002\rangle + |323332123\rangle + |323432244\rangle$

$+|324032430\rangle + |324132001\rangle + |324232122\rangle + |324332243\rangle + |324432314\rangle)$

$+\sqrt{p_{13}p_{23}}$

$\times(|330033010\rangle + |330133131\rangle + |330233202\rangle + |330333323\rangle + |330433444\rangle$

$+|331033130\rangle + |331133201\rangle + |331233322\rangle + |331333443\rangle + |331433014\rangle$

$+|332033200\rangle + |332333221\rangle + |332233442\rangle + |332333013\rangle + |332433134\rangle$

$+|333033320\rangle + |333133441\rangle + |333233012\rangle + |333333133\rangle + |333433204\rangle$

$+|334033440\rangle + |334133011\rangle + |334233132\rangle + |334333203\rangle + |334433324\rangle)$

$+\sqrt{p_{13}p_{24}}$

$\times(|340034020\rangle + |340134141\rangle + |340234212\rangle + |340334333\rangle + |340434404\rangle$
$+|341034140\rangle + |341134211\rangle + |341234332\rangle + |341334403\rangle + |341434024\rangle$
$+|342034210\rangle + |342134331\rangle + |342234402\rangle + |342334023\rangle + |342434144\rangle$
$+|343034330\rangle + |343134401\rangle + |343234022\rangle + |343334143\rangle + |343434214\rangle$
$+|344034400\rangle + |344134021\rangle + |344234142\rangle + |344334213\rangle + |344434334\rangle)$
$+\sqrt{p_{14}p_{20}}$
$\times(|400040040\rangle + |400140111\rangle + |400240232\rangle + |400340303\rangle + |400440424\rangle$
$+|401040110\rangle + |401140231\rangle + |401240302\rangle + |401340423\rangle + |401440044\rangle$
$+|402040230\rangle + |402140301\rangle + |402240422\rangle + |402340043\rangle + |402440114\rangle$
$+|403040300\rangle + |403140421\rangle + |403240042\rangle + |403340113\rangle + |403440234\rangle$
$+|404040420\rangle + |404140041\rangle + |404240112\rangle + |404340233\rangle + |404440304\rangle)$
$+\sqrt{p_{14}p_{21}}$
$\times(|410041000\rangle + |410141121\rangle + |410241242\rangle + |410341313\rangle + |410441434\rangle$
$+|411041120\rangle + |411141241\rangle + |411241312\rangle + |411341433\rangle + |411441004\rangle$
$+|412041240\rangle + |412141311\rangle + |412241432\rangle + |412341003\rangle + |412441124\rangle$
$+|413041310\rangle + |413141431\rangle + |413241002\rangle + |413341123\rangle + |413441244\rangle$
$+|414041430\rangle + |414141001\rangle + |414241122\rangle + |414341243\rangle + |414441314\rangle)$
$+\sqrt{p_{14}p_{22}}$
$\times(|420042010\rangle + |420142131\rangle + |420242202\rangle + |420342323\rangle + |420442444\rangle$
$+|421042130\rangle + |421142201\rangle + |421242322\rangle + |421342443\rangle + |421442014\rangle$
$+|422042200\rangle + |422142321\rangle + |422242442\rangle + |422342013\rangle + |422442134\rangle$
$+|423042320\rangle + |423142441\rangle + |423242012\rangle + |423342133\rangle + |423442204\rangle$
$+|424042440\rangle + |424142011\rangle + |424242132\rangle + |424342203\rangle + |424442324\rangle)$
$+\sqrt{p_{14}p_{23}}$
$\times(|430043020\rangle + |430143141\rangle + |430243212\rangle + |430343333\rangle + |430443404\rangle$
$+|431043140\rangle + |431143211\rangle + |431243332\rangle + |431343403\rangle + |431443024\rangle$
$+|432043210\rangle + |432143331\rangle + |432243402\rangle + |432343023\rangle + |432443144\rangle$
$+|433043330\rangle + |433143401\rangle + |433243022\rangle + |433343143\rangle + |433443214\rangle$
$+|434043400\rangle + |434143021\rangle + |434243142\rangle + |434343213\rangle + |434443334\rangle)$
$+\sqrt{p_{14}p_{24}}$
$\times(|440044030\rangle + |440144101\rangle + |440244222\rangle + |440344343\rangle + |440444414\rangle$

$$
\begin{aligned}
&+|441044100\rangle+|441144221\rangle+|441244342\rangle+|441344413\rangle+|441444034\rangle\\
&+|442044220\rangle+|442144341\rangle+|442244412\rangle+|442344033\rangle+|442444104\rangle\\
&+|443044340\rangle+|443144411\rangle+|443244032\rangle+|443344103\rangle+|443444224\rangle\\
&+|444044410\rangle+|444144031\rangle+|444244102\rangle+|444344223\rangle+|444444344\rangle)
\end{aligned}
\tag{5.28}
$$

5.28 式を $|R_1, S_1\rangle$ に部分トレースをすると，

$$
\begin{aligned}
&\mathrm{Tr}_{R_2R_{E_1}R_{E_2}S_2P_3'P_4P_5}\,|R_1R_2R_{E_1}R_{E_2}S_1S_2P_3'P_4P_5\rangle\\
&\langle R_1R_2R_{E_1}R_{E_2}S_1S_2P_3'P_4P_5|\\
&= p_{10}\left(\frac{p_{20}}{5^2}\times 25+\frac{p_{21}}{5^2}\times 25+\frac{p_{22}}{5^2}\times 25\right)|00\rangle\langle 00|\\
&\quad +p_{11}\left(\frac{p_{20}}{5^2}\times 25+\frac{p_{21}}{5^2}\times 25+\frac{p_{22}}{5^2}\times 25\right)|11\rangle\langle 11|\\
&\quad +p_{12}\left(\frac{p_{20}}{5^2}\times 25+\frac{p_{21}}{5^2}\times 25+\frac{p_{22}}{5^2}\times 25\right)|22\rangle\langle 22|\\
&\quad +p_{13}\left(\frac{p_{20}}{5^2}\times 25+\frac{p_{21}}{5^2}\times 25+\frac{p_{22}}{5^2}\times 25\right)|33\rangle\langle 33|\\
&\quad +p_{14}\left(\frac{p_{20}}{5^2}\times 25+\frac{p_{21}}{5^2}\times 25+\frac{p_{22}}{5^2}\times 25\right)|44\rangle\langle 44|\\
&= p_{10}|00\rangle\langle 00|+p_{11}|11\rangle\langle 11|+p_{12}|22\rangle\langle 22|+p_{13}|33\rangle\langle 33|+p_{14}|44\rangle\langle 44|.
\end{aligned}
\tag{5.29}
$$

5.29 式は秘密 S_1 を純粋化したものの密度行列に他ならない．同様に秘密 S_2 も求めることができ，秘密の分散，および復元をすることができた．

5.4 まとめ

本章では，複数の量子状態を分散符号化する量子複数秘密分散法について定義を行ない，量子複数秘密分散法の構成法として MSP を用いた方法の提案を行い，その評価を行った．その結果，MSP を用いて Secrecy を満たすには少なくとも MSP の行列 M について $m+t-1$ 行以上の行と $m+t-1$ 列以上の列を持つ行列である必要があること，特に (m,t,d) 量子閾値複数秘密分散法においては Secrecy を満たす必要十分条件と，$t>m$ が成り立たなければ存在しないことがわかった．また，具体的な例として秘密情報として量子状態 2 つを持つ量子複数秘密分散法を提案法に従い構成し，分散と復元を行うことができること示した．

第 6 章

今後の展望

1994 年の Shor のアルゴリズムの提案により，量子計算機による素因数分解，離散対数問題の効率的な攻撃法が示されて以来，量子計算機の実現に向け研究が続けられている．現状では，classical な暗号法である RSA 暗号や楕円曲線暗号を破ることができるほどの性能を持つ量子計算機は作られていない．しかしながら，現行の計算機が半導体の開発により性能が飛躍的に伸びたように，新たな素子の開発により一気に研究が進む可能性もある．したがって，量子計算機に耐性のあるセキュリティプロトコルの提案は非常に重要であり，量子セキュリティの研究はこれからも長く続いていくことが見込まれる．

さらに，classical なセキュリティプロトコルにおいて，各プロトコル単位では安全性が証明されていても，それらを組み合わせることにより安全性が脆弱になる場合がある．そこで，2001 年に Canetti により UC というものが考えられた [13]. UC ではプロトコル単体で保証された安全性が，どのような結合・利用環境でも保持される．同様に，高次の量子セキュリティを考える場合は UC を考える必要があるが，現在 UC 安全であるような量子セキュリティプロトコルは研究されていない．したがって UC 安全な量子セキュリティプロトコルの提案も今後の課題である．

また，bit 情報を量子状態でシミュレートすることは効率的に行うことができるが，量子状態を bit 情報で効率的にシミュレートすることは難しいと考えられる[1]. したがって，

[1] Nqubit の情報を bit で表すためには 2^Nbit 必要と考えられる．

- bit 情報を量子状態を使用してセキュリティを確保する．
- 量子情報を量子状態を使用してセキュリティを確保する．

は独立に考えることが必要である．したがって，もっとも望ましいセキュリティプロトコルは,「量子情報を量子状態を使用してセキュリティを確保する」プロトコルであり，かつ「bit 情報を量子情報でシミュレートした場合は，bit 情報でセキュリティを確保したプロトコルより効率的で安全性が高い」プロトコルとなる．この観点でセキュリティプロトコルを見た場合，例えば秘密分散法については，bit 情報を分散する場合については，すでに bit 情報を使って情報理論的に安全な手法が提案されていることから，これ以上の安全性を持つプロトコルは存在しない．したがって，量子状態を使用する場合についても，bit 情報を利用するより効率的な手法を提案する必要があると思われる．しかしながら，量子状態を分散する秘密分散法については bit 情報を分散するプロトコルと比較することはできない．なぜなら，量子状態を bit 情報で表すことは効率的にできないと考えられるからである．この観点で，本論文で提案した量子コイン投げと量子複数秘密分散法について考察すると，量子複数秘密分散法については複数の量子状態を分散していることから，bit 情報を複数分散する複数秘密分散法と比較を行うことはできない．また，bit を利用するコイン投げが計算量的に安全なものを実現しているのに対し，量子コイン投げでは計算量的な安全性によらないプロトコルを提案している．したがって，計算量的安全性が使えない状況では有用であると考えられる．

本論文では，量子セキュリティのうち量子コイン投げと量子秘密分散法を扱った．これらのプロトコルは量子セキュリティにおける最も根幹にあるプロトコルであり，classical なセキュリティにおいてコイン投げや秘密分散法が重要であるのと同様の重要性がある．量子セキュリティでは高度なセキュリティを持つ有用性の高いプロトコルはいまだ少なく，また classical なセキュリティプロトコルにおいて有用とされているプロトコルについても，量子セキュリティへの拡張がなされていないものも数多くある．例えば池田らは閾値変更可能な秘密分散法を応用して鍵無効化方式を実現している [48]．この方式を量子化する場合，閾値変更を効率的に行える量子秘密分散法が必要である．しかしながら，このような量子秘密分散法の提案はいまだなされていない．したがって，このようなより高度なセ

キュリティシステムを構築するために，classical なセキュリティプロトコルにおいて有用とされているプロトコルについて，量子セキュリティへの拡張することが重要である．本論文では量子複数秘密分散法は初めての提案である．そこでこのプロトコルを応用したセキュリティプロトコルが提案できるものと期待でき，また，この量子複数秘密分散法の簡単な応用で，閾値を増やす方向への変更に限るが，量子閾値変更可秘密分散法を構築することもできる．その方法は，閾値変更前の (k, n) 閾値量子秘密分散法のシェアのうち，任意の k 個のシェアを秘密として，(k, k', n) 量子閾値複数秘密分散法で分配しなおすことである．ここで $k'(> k)$ は変更後の閾値とする．この方法では MSP の行列について，$k + k' - 1$ 行以上の行と $k + k' - 1$ 列以上の列を持つように採ることで，Secrecy の要件を満たすことができる．また，no-cloning 定理より，再配分に使用されたシェアを保存しておくことはできないので，classical な閾値法と違い，分散される秘密はそのままで閾値変更することができる．この方法では閾値変更を行うために一度ディーラの基にシェアを集めることが必要であり効率が悪い．したがって，この手法の効率化を図ることも重要な今後の課題である．

一方，classical な認証機能付き鍵共有法に PAKE[7, 1] が存在する．PAKE はパスワード認証により鍵共有相手の認証を行い，鍵の共有を行うプロトコルである．現在この PAKE に量子原理を取り入れた量子 PAKE に相当するものは存在しない．しかしながら，その構成要素として必要であろう量子鍵共有法 [8]，量子パスワード [26] や量子メッセージ認証 [6] などは存在している．しかしながら，これらを効率的に組み合わせて量子 PAKE を実現することはできていない．特に量子パスワードはパスワードとして量子状態を用いるため，classical な PAKE での使用法を流用できない．したがって，その方法を考える必要があり，今後の課題である．特に，鍵共有法における測定方法が量子パスワードでの検証方法に影響を与えることがないようにすることができれば実現できるのではないかと考えている．

第 7章

まとめ

本論文では strong 量子コイン投げと量子複数秘密分散法のプロトコルの提案を行った．

量子コイン投げについては，n 次元量子状態を使用した量子コイン投げの提案を行い，そのプロトコルのバイアスの評価を行った．その結果，t は Alice が選ぶ量子状態すべてに共通する基底数とし，$X = t/n$ とすると，各々のバイアスは $\epsilon_{Alice} = 1/4 + (3/4 - 1/(1+X))$，$\epsilon_{Bob} = 1/4 - (3/4 - 1/(1+X))$ という結果が得られた．この結果は片方のバイアスを任意に小さくすることができることを示している．特に，バイアスのバランスを崩すことで片方のみであればバイアスの理論的な下限である $1/2 - 1/\sqrt{2}$ を下回れることを示し，その関係は量子状態の構成時に導入した X で与えられることを示した．また，量子 n ビット列コミットメントにおいて，そのビット情報を漏洩することが示されている．提案プロトコルはこの量子 n ビット列コミットメントを使用したプロトコルの一種であると考えられるが，通信に利用した量子状態のアクセシブル情報量は，バイアスを決定するために定めた任意の X について，$(1-X)/(1+X) \leq 1$ で与えられることを示した．このことは，アクセシブル情報量の観点から，Alice が選んだビットを推測するのに十分な情報は与えていないことが分かる．最後に，バイアスのバランスをとった場合には，$X = 1/3$ のときに strong 量子コイン投げの現在の最良値である 0.25 となる．その場合の量子状態は提案プロトコルの基となった Ambainis のプロトコルにおける量子状態と等価であり，Ambainis のプロトコルを真に含んでいるといえる．

量子秘密分散法では秘密の量子状態を複数持つ量子複数秘密分散法を定義し，その構成法とその評価を行った．その結果，秘密の量子状態を m 個，それぞれの秘密 S_i に対する Access 構造を Γ_i，$t = \min\{|A| \ |A \in \Gamma_i, i = 1, \cdots, m\}$ としたとき，MSP を用いて Secrecy を満たす量子複数秘密分散法を構成するには，少なくとも MSP の行列 M について，$m+t-1$ 行以上の行と $m+t-1$ 列以上の列を持つ行列である必要があること，特に秘密の量子状態を m 個とし，シェア総数 d 個，そのうちの t 個のシェアによりすべての秘密を復元できる (m, t, d) 量子閾値複数秘密分散法においては，Secrecy を満たす必要十分条件と，閾値 t と秘密の量子状態数 m の間に，$t > m$ が成り立たなければ MSP を利用した (m, t, d) 量子閾値複数秘密分散法が存在しないことがわかった．最後に，実際に秘密が 2 状態であり，Secrecy を満たす量子複数秘密分散法を構成した．この量子複数秘密分散法は初めて提案された方法であり，classical なセキュリティプロトコルのうち，複数秘密分散法を使用しているプロトコルを量子化する端緒となることが期待される．

謝辞

本研究を遂行するにあたり，宮地充子准教授から数多くの御指示，御助言をいただきました．そして，本論文を構成するにあたり多くの有益なご指導をいただきました．宮地充子准教授の適切なご指導に感謝いたします.

双紙正和特任准教授には，日頃から精力的にご助力いただき，また，累積する問題の解決に多くの糸口を与えていただきました．双紙正和特任准教授のご指導と御助言に感謝いたします.

本学の金子 峰雄教授，平石 邦彦教授，そして東京工業大学大学院情報理工学研究科の田中圭介助教授には，数々の有益な助言をいただきましたことを，心より感謝致します.

さらに, 本論文をまとめるに当たって御協力いただいた宮地研究室の諸兄に厚く御礼申し上げます.

最後に，北陸先端科学技術大学院大学において研究をおこなう機会を与えてくれました両親に心から感謝とお礼を申し上げます.

参考文献

[1] Abdalla, M., Chevassut, O., Fouque, P.-A. and Pointcheval, D.: A Simple Threshold Authenticated Key Exchange from Short Secrets., *ASIACRYPT*, pp. 566–584 (2005).

[2] Aharonov, D., Ta-Shma, A., Vazirani, U. and Yao, A.: Quantum bit escrow, *Proceedings of STOC'00*, pp. 705–714 (2000).

[3] Ambainis, A.: A new protocol and lower bounds for quantum coin flipping, *J. Comput. Syst. Sci.*, Vol. 68, No. 2, pp. 398–416 (2004).

[4] Ambainis, A., Buhrman, H., Dodis, Y. and Rohrig, H.: Multiparty Quantum Coin Flipping, *CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, Washington, DC, USA, IEEE Computer Society, pp. 250–259 (2004).

[5] Bandyopadhyay, S.: Teleportation and secret sharing with pure entangled states, *Phys. Rev. A*, Vol. 62, No. 1, p. 012308 (2000).

[6] Barnum, H., Crepeau, C., Gottesman, D., Smith, A. and Tapp, A.: Authentication of Quantum Messages, *PROC.43RD ANNUAL IEEE SYMPOSIUM ON THE FOUNDATIONS OF COMPUTER S*, Vol. 02, p. 449 (2002).

[7] Bellovin, S. M. and Merritt, M.: Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 72–84 (1992).

[8] Bennett, C. H. and Brassard, G.: Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE international Conference*

on Computers, Systems and Signal Processing, Bangalore, India, New York, IEEE Press, p. 175 (1984).

[9] Blakley, G. R.: Safeguarding cryptographic keys, *Proc. AFIPS 1979 National Computer Conference*, pp. 313–317 (1979).

[10] Blakley, G. R. and Meadows, C.: Security of ramp schemes, *Proceedings of CRYPTO 84 on Advances in cryptology*, New York, NY, USA, Springer-Verlag New York, Inc., pp. 242–268 (1985).

[11] Blum, M.: Coin Flipping by Telephone - A Protocol for Solving Impossible Problems., *COMPCON*, pp. 133–137 (1982).

[12] Blundo, C., Santis, A. D., Crescenzo, G. D., Gaggia, A. G. and Vaccaro, U.: Multi-secret sharing schemes, *Advances in Cryptology – CRYPTO '94*, pp. 150–163 (1994).

[13] Canetti, R.: Universally Composable Security: A New Paradigm for Cryptographic Protocols, *IEEE Symposium on Foundations of Computer Science*, pp. 136–145 (2001).

[14] Chor, B., Goldwasser, S., Micali, S. and Awerbuch, B.: Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults (Extended Abstract), *FOCS*, pp. 383–395 (1985).

[15] Cleve, R.: Limits on the security of coin flips when half the processors are faulty, *STOC '86: Proceedings of the eighteenth annual ACM symposium on Theory of computing*, New York, NY, USA, ACM Press, pp. 364–369 (1986).

[16] Cleve, R., Gottesman, D. and Lo, H.-K.: How to share a quantum secret, *Phys. Rev. Lett.*, Vol. 83, No. 3, pp. 648–651 (1999).

[17] Colbeck, R.: A New Protocol For Strong Coin Tossing (2006). quant-ph/0609034.

[18] Crépeau, C., Gottesman, D. and Smith, A.: Approximate Quantum Error-Correcting Codes and Secret Sharing Schemes., *EUROCRYPT*, pp. 285–301 (2005).

[19] Deutsch, D.: Quantum theory, the Church-Turing principle and the universal quantum computer, *Proceedings of the Royal Society of London Ser. A*, Vol. A400, pp. 97–117 (1985).

[20] Dieks, D.: Communication by EPR devices, *Phys. Lett. A 92, 271* (1982).

[21] 福田明香，双紙正和，宮地充子：量子コイン投げにおけるバイアスの考察– 3 状態から４状態プロトコルへの拡張–，*TECHINICAL REPORT OF IEICE, ISEC2003-4* (2003).

[22] Gal, A.: A characterization of span program size and improved lower bounds for monotone span programs, *Comput. Complex.*, Vol. 10, No. 4, pp. 277–296 (2002).

[23] Gottesman, D.: Theory of quantum secret sharing, *Phys. Rev. A*, Vol. 61, No. 4, p. 042311 (2000).

[24] Grover, L. K.: A fast quantum mechanical algorithm for database search, *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, New York, NY, USA, ACM Press, pp. 212–219 (1996).

[25] Gruska, J.: *Quantum Computing*, Mcgraw Hill Book Co Ltd (1999).

[26] Gu, M. and Weedbrook, C.: Quantum Passwords (2005). quant-ph/0506255.

[27] Hillery, M., Bužek, V. and Berthiaume, A.: Quantum secret sharing, *Phys. Rev. A*, Vol. 59, No. 3, pp. 1829–1834 (1999).

[28] Imai, H., Muller-Quade, J., Nascimento, A., Tuyls, P. and Winter, A.: An information theoretical model for quantum secret sharing schemes, *Quantum Information and Computation (QIC)*, Vol. 5, No. 1, pp. 068–079 (2004). Preprint on quant-ph/0311136.

[29] Karchmer, M. and Wigderson, A.: On Span Programs, *Proceedings of the Eighth Annual Structure in Complexity Theory Conference*, pp. 102–111 (1993).

[30] Kent, A.: Quantum Bit String Commitment, *Phys. Rev. Lett.*, Vol. 90, No. 23, p. 237901 (2003).

[31] Kitaev, A. Y.: Quantum Coin Flipping (2002). Talk at QIP2003 (slides and video at MSRI).

[32] Lo, H. and Chau, H.: Why quantum bit commitment and ideal quantum coin tossing are impossible, *Physica D*, Vol. 120, pp. 177–187 (1998).

[33] Mayers, D.: Unconditionally Secure Quantum Bit Commitment is Impossible, *Phys. Rev. Lett.*, Vol. 78, No. 17, pp. 3414–3417 (1997).

[34] 宮地充子，菊池浩明：情報セキュリティ，オーム社 (2003).

[35] Mochon, C.: Quantum weak coin-flipping with bias of 0.192, *45th Annual IEEE Symposium on Foundations of Computer Science*, pp. 2–11 (2004).

[36] Nielsen, M. and Chuang, I.: *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[37] Ogawa, T., Sasaki, A., Iwamoto, M. and Yamamoto, H.: Quantum secret sharing schemes and reversibility of quantum operations, *Phys. Rev. A*, Vol. 72, p. 032318 (2005).

[38] Okamoto, T., Tanaka, K. and Uchiyama, S.: Quantum Public-Key Cryptosystems, *CRYPTO '00: Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, London, UK, Springer-Verlag, pp. 147–165 (2000).

[39] 岡本龍明，山本博資：現代暗号，産業図書 (1997).

[40] Rietjenst, K.: An information theoretical approach to quantum secret sharing schemes, Master's thesis, TECHNISCHE UNIVERSITEIT EINDHOVEN (2004).

[41] Rietjenst, K., Schoenmakers, B. and Tuyls, P.: Quantum information theoretical analysis of various constructions for quantum secret sharing, *Proceedings International Symposium on Information Theory (ISIT 2005)*, pp. 1598–1602 (2005).

[42] Shamir, A.: How to share a Secret, *Comm. ACM 22*, p. 612 (1979).

[43] Shor, P. W.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, *IEEE Symposium on Foundations of Computer Science*, pp. 124–134 (1994).

[44] Smith, A.: Quantum secret sharing for general access structures. quant-ph/0001087.

[45] Spekkens, R. W. and Rudolph, T.: Degrees of concealment and bindingness in quantum bit commitment protocols, *Phys. Rev. A*, Vol. 65, No. 1, p. 012310 (2001).

[46] Spekkens, R. W. and Rudolph, T.: Quantum Protocol for Cheat-Sensitive Weak Coin Flipping, *Phys. Rev. Lett.*, Vol. 89, No. 22, p. 227901 (2002).

[47] Tamura, Y., Tada, M. and Okamoto, E.: Update of sccess structure in Shamir's (k, n) threshold scheme, *SCIS1999*, pp. 469–474 (1999).

[48] 池田智孝，四方順司，　松本勉：無効化端末数変更可能な鍵無効化方式について，信学技報，ISEC2004-109, Vol. 104, No. 731, 京都，pp. 19–24 (2005).

[49] Tsurumaru, T.: Implementable quantum-bit-string commitment protocol, *Physical Review A (Atomic, Molecular, and Optical Physics)*, Vol. 71, No. 1, p. 012313 (2005).

[50] Uhlmann, A.: The 'transition probability' in the state space of *-algebra, *Report on Mathematical Physics*, Vol. 9, pp. 273–279 (1976).

[51] Wiesner, S.: Conjugate coding, *SIGACT News*, Vol. 15, No. 1, pp. 78–88 (1983).

[52] Wootters, W. K. and Zurek, W. H.: A single quantum cannot be cloned, *Nature 299, 802* (1982).

[53] Yuen, H. P.: KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation (2003).

本研究に関する発表論文

[1] 早稲田篤志，双紙正和，宮地充子: “量子複数秘密分散に関する考察”, 情報処理学会論文誌, 投稿中.

[2] 早稲田篤志，双紙正和，宮地充子: “n 次元量子状態を使用した量子コイン投げプロトコル”, 情報処理学会論文誌, Vol.46, No.8 (2005).

[3] A. Waseda, M. Soshi, and A. Miyaji: “n-state quantum coin flipping protocol”, International Conference on Information Technology - ITCC2005, Volume II, 776-777, 2005.

[4] 早稲田 篤志: “量子複数秘密分散の応用例”, 第 9 回北陸情報セキュリティ研究会 (2006-4).

[5] 早稲田 篤志: “量子セキュリティに関する研究”, 第 8 回北陸情報セキュリティ研究会 (2006-3).

[6] 早稲田篤志: “Study on Quantum Security”, JAIST 21 世紀 COE シンポジウム 2006「検証進化可能電子社会」(2006-3).

[7] 早稲田篤志，双紙正和，宮地充子: “MSP を使った量子複数秘密分散に関する考察”, IEICE Japan Tech. Rep., ISEC2005-119 (2005-12), 53-60.

[8] 早稲田 篤志: “MSP を使った量子複数秘密分散に関する考察”, 第 6 回北陸情報セキュリティ研究会 (2005-11).

[9] 早稲田 篤志: “量子複数秘密分散における一提案”, 第 4 回北陸情報セキュリティ研究会 (2005-7).

[10] 早稲田 篤志: “量子秘密分散について”, 第 3 回北陸情報セキュリティ研究会 (2005-6).

[11] 早稲田 篤志: “複数の秘密を持つ量子秘密分散法”, 第 1 回北陸情報セキュリティ研究会 (2005-4).

[12] 佐々木賢，早稲田篤志，双紙正和，宮地充子: “量子秘密分散に関する検討”, IEICE Japan Tech. Rep. , IT2004-71, ISEC2004-127, WBS2004-186 (2005-03), 7-11.

[13] 早稲田篤志: “Study on Quantum Security”, JAIST 21 世紀 COE シンポジウム 2005「検証進化可能電子社会」(2005-3).

[14] 早稲田篤志，双紙正和，宮地充子: “n 状態量子コイン投げプロトコル”, IEICE Japan Tech. Rep. , ISEC2004-10 (2004-05), 65-68.