量子複数秘密分散に関する考察

早稲田 篤志[†,††] 双紙 正和[††] 宮地 充子[††]

量子秘密分散法（Quantum Secret Sharing Schemes，QSSS）は，Hillery ら[7] によって初めて提案されて以来，さまざまな手法が提案されている．しかしながら，秘密分散法の一種である複数秘密分散法の量子への拡張はいまだなされていない．そこで本論文では，Smith によって提案された Monotone Span Programs（MSP）を用いた一般的な access 構造を持つ量子秘密分散法[14] 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．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．

Consideration for Quantum Multi-secret Sharing

Atsushi Waseda,[†,††] Masakazu Soshi[††] and Atsuko Miyaji[††]

A quantum secret sharing scheme (QSSS) was proposed by Hillery [7] for the first time. Afterwards, various QSSS have been so far proposed. Especially, much attention has been paid to QSSS with general access structures proposed by Smith which utilizes Monotone Span Programs (MSP) [14]. However, the extension to quantum multi-secret sharing schemes has not been done yet. This paper proposes for the first time quantum multi-secret sharing schemes for distinct secrets according to each authorized set by using MSP, and considers security conditions which quantum multi-secret sharing schemes should satisfy. Furthermore, we give the theoretical evaluation of our proposal, and construct QSSS two secret quantum states.

1. はじめに

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などの計算量的困難性に依存している．しかし，量子コンピュータが実現されると，これらの既存の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暗号の研究がさかんに行われている．

量子暗号の分野の 1 つに量子秘密分散法（Quantum Secret Sharing Scheme，QSSS）がある．この量子秘密分散法は 1999 年に Hillery らによって初めて提案された[7]．このプロトコルは HBB QSSS と呼ばれ，3 量子以上のエンタングル状態である GHZ 状態を利用しており，分散情報をすべて集めると復元が可能な満場一致法である．その後，Cleve ら[3] や Gottesman [6] 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 による monotone span programs（MSP）を用いた任意の access 構造を持つ量子秘密分散法[14] 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[1] など，多くの量子秘密分散プロトコルが提案されている．しかし，上述の量子秘密分散法は 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，bit 情報による秘密を bit 情報に分散させる古典的な秘密分散法には，複数の秘密を分散する複数秘密分散法[2] が存在する．

そこで本論文では，有資格集合に応じて複数の異なる秘密量子状態を復元できる量子複数秘密分散法を，MSP を用いて初めて提案する．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．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

† 独立行政法人情報通信研究機構
National Institute of Information and Communications Technology（NICT）
†† 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology（JAIST）

本研究は著者が北陸先端科学技術大学院大学に在籍時に行われた．

子複数秘密分散が構成可能であることを示す．

本論文の構成は以下のとおりである．まず，2 章で，準備として本論文で使用される記法および諸定義について簡単に述べる．3 章では，Smith により提案された，秘密の量子状態 1 つを MSP を用いて分散させる量子秘密分散法について紹介する．4 章では，複数の量子状態を分散させる量子複数秘密分散法を定義したあと，Smith の手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．最後に 5 章で結論を述べる．

2. 準　　備

この章では本論文における用語の諸定義を行う．まず，2.1 節で量子状態について定義を行い，2.2 節では，秘密分散法と，提案手法で使用している monotone span programs（MSP）について述べる．

2.1 量子状態

本節では量子状態に関する諸定義を行う．なお，用語などのより詳しい解説については文献 10) を参照されたい．

- 純粋状態：
  純粋状態は，Hilbert 空間における，ノルムが 1 のベクトルとして表される．すなわち，$\mathcal{H}$ を n 次元 Hilbert 空間とし，$|0\rangle, |1\rangle, \cdots, |n-1\rangle$ を $\mathcal{H}$ の正規直交基底とするとき，（$\mathcal{H}$ における）任意の n 次元純粋状態は，$|\psi\rangle = \sum_{i=0}^{n-1} a_i |i\rangle$ $(a_i \in \mathbb{C})$ と表すことができる．ここで，$\sum_i |a_i|^2 = 1$ である．
- 混合状態：
  混合状態は，純粋状態 $|\psi_i\rangle$ の確率分布 $(p_i, |\psi_i\rangle)$ で与えられる（$0 \le p_i \le 1$，$\sum_i p_i = 1$）．このとき，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．
- 部分トレースと縮約密度演算子：
  ρ^{AB} を，系 A と B からなる量子状態の密度演算子とする．ここで，系 A の恒等写像を I_A とし，系 B の次元を N_B，その正規直交基底を $|\phi_j\rangle$ とすると，系 B 上の部分トレースは，$\mathrm{Tr}_B(\rho^{AB}) = \sum_{j=1}^{N_B} (I_A \otimes \langle\phi_j|)\rho^{AB}(I_A \otimes |\phi_j\rangle)$ により定義される．さらに，この部分トレースにより，系 A の縮約密度演算子 ρ^A が，$\rho^A = \mathrm{Tr}_B(\rho^{AB})$ として定義される．
- 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．ここで，系 A の正規直交基底を $|i^A\rangle$ とし，ρ^A の正規直交分解を $\rho^A = \sum p_i |i^A\rangle\langle i^A|$ とすると，R 上における A と同じ正規直交系 $|i^R\rangle$ を用いて，ρ^A の純粋化を $|\psi\rangle = \sum \sqrt{p_i}\,|i^R\rangle|i^A\rangle$ とすることができる．
- 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，$S(A) = S(\rho^A) = -\mathrm{Tr}(\rho^A \log \rho^A)$ として定義される．ここで，Tr はトレースを表す．また，ρ^A の固有値を λ_i 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 が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，条件付きエントロピー，相互情報量についてもそれぞれ以下のように定義できる．
  - 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，$S(A,B) = -\mathrm{Tr}(\rho^{AB} \log \rho^{AB})$ として定義される．
  - 系 B の状態が知られているときの系 A のエントロピーを条件付きエントロピーといい，$S(A\,|\,B) = S(A,B) - S(B)$ により定義される．
  - 系 A と B が共通に持つ情報量の尺度を相互情報量といい，$I(A:B) = S(A) + S(B) - S(A,B)$ として定義される．

2.2 秘密分散法と Monotone Span Programs

秘密分散法とは，ある秘密情報 S について，有資格集合の参加者のシェア（S の分散情報）を集めると S が復元できるが，禁止集合の参加者のシェアでは S に関する情報がいっさい洩れないような符号化方式をいう．さらに，有資格集合の族を access 構造といい，禁止集合の族を adversary 構造という．例として，参加者の集合を $\{A,B,C\}$ とし，参加者 A と B，または，A と C が集まるときのみ秘密 S が復元できるような秘密分散を考える．このとき，S の access 構造は $\Gamma_S = \{\{A,B\},\{A,C\},\{A,B,C\}\}$ であり，adversary 構造は $\mathcal{A}_S = \{\emptyset,\{A\},\{B\},\{C\},\{B,C\}\}$ と

表 1 記号
Table 1 List of notation.

$M^\top$	行列 M の転置行列
$Im(M)$	行列 M の像空間
$\mathrm{rank}(M)$	行列 M の階数
$\mathbb{F}_q^e$	$\mathbb{F}_q$ 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 における恒等写像
$\langle\psi\|\phi\rangle$	ベクトル $\|\psi\rangle$ と $\|\phi\rangle$ の内積

なる．秘密が複数存在する場合については，各秘密について独立に access 構造，adversary 構造を考える．

秘密分散法には，n 個のシェアのうち，任意の t 個のシェアで秘密が復元される (t,n) 閾値法[13] や，その閾値 t が変更可能な閾値変更可秘密分散法[15]，複数の秘密を分散する複数秘密分散法[2] などが存在する．秘密情報やシェアに量子状態を利用する量子秘密分散法には，任意のアクセス構造を持つもの[14] や，シェアをすべて集めると復元可能な満場一致法[1),7)]，(t,n) 閾値法[3] など提案されている．一方，閾値変更可秘密分散法や複数秘密分散法などを量子状態を用いて実現したものは提案されていない．

ここで，秘密分散法の構成で利用される monotone span program（MSP）[14] について述べる．まず，$\mathbb{F}_q$ を位数 q の有限体とする．リテラル☆の集合 $\mathcal{P}$ 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．MSP の説明および本論文の以降で用いられる記号について，**表 1** にまとめる．

以上から span program[9] について定義する．

定義 1 リテラルの集合 $\mathcal{P}$ 上の *span program* とは，(1) 位数 q の有限体 $\mathbb{F}_q$，(2) $\mathbb{F}_q$ 上の $d \times e$ 行列 M，(3) M の行を割り振る関数 $g : \{1,\cdots,d\} \to \{x_i^j \,|\, x_i \in \mathcal{P}, j \in \{0,1\}\}$，(4) 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 4 つ組 $(\mathbb{F}_q, M, g, \mathbf{e})$ として定義される．ただし，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．ここで，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，(i) $g(k) = x_i$ かつ $x_i \in A$，あるいは，(ii) $g(k) = \overline{x_i}$ 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，M_A により生成される部分空間に $\mathbf{e}$ が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．さらに，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，$\mathrm{MSP}(\mathbb{F}_q, M, g, \mathbf{e})$ 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．また，span program のサイズとは，行列 M の列の数のことをいう．

残念ながら，一般的な monotone function f を計算する 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[5]．しかしながら，特に，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，$\mathbf{e} = \mathbf{e}_1$ の場合については，M を列数 t の Vandermonde 行列とすることにより，f を計算する MSP を構成できることが知られている．

秘密分散法で，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，秘密分散において対応する adversary 構造は，$\mathcal{A}_f = \{B \subseteq \mathcal{P} \,|\, f(B) = 0\}$ として定義することができる．

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 $\mathcal{P}$ を秘密分散における参加者の集合とし，参加者を g の像のリテラルと見なす．g は，シェアを各参加者に割り振る関数として使用される．また，ここでの span program は monotone である．さらに，M を適用してシェアを作成する．M の行数である d は，シェアの数に対応する．特に，$n \times t$ Vandermonde 行列により構成された MSP については，その MSP で計算される 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，$\mathcal{P}$ を，参加者の集合と，参加者の持つシェアの集合という 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，$P = \{P_1, \ldots, P_n\}$ と表記することがある．

☆ 命題変数，あるいはその否定．

3. Monotone Span Program を用いた量子秘密分散法

この章では，最初に量子秘密分散法を定義し，次に既存研究として，MSP を用いた（単一）量子秘密分散法[14] を紹介する．

定義 2 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[8]．

(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，$I(R:B) = 0$.

□

以下では，この量子秘密分散法を MSP を用いて実現することを考える．そのためにまず，任意の正整数 t に対し，以下の 2 つの性質を持つ単射写像 $\vartheta : \mathbb{F}_q^t \to \mathcal{H}^{\otimes t}$ を考える[11]．ここで，$\mathcal{H}$ は，$\mathbb{C}$ 上の q 次元 Hilbert 空間とする．

(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，

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

この ϑ を用いて，$\mathbb{F}_q^t$ 上のベクトルや演算を $\mathcal{H}^{\otimes t}$ 上のものに自明に対応させることができる．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 1 列独立な $\mathbb{F}_q$ 上の $d \times e$ 行列 M に対して，$\theta_M : \mathcal{H}^{\otimes e} \to \mathcal{H}^{\otimes d}$ を

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

とする．ただし，$\left|\psi_1^i \cdots \psi_e^i\right\rangle$ 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[11]．

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 2 *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，$d \times e$ 行列 M を $\mathcal{P}$ 上における *MSP* の行列とし，A および B に対応する M の部分行列をそれぞれ 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[14]．

(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 は $\mathbb{F}_q^{e-1}$ 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．

補題 2 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いっさい漏れないことを意味している．

以上より，Smith による量子秘密分散法のプロトコルをここで述べる[14]．

ディーラによるシェアの生成および配付

(1) $\left|i^S\right\rangle$ 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

$$\rho_S = \sum_{i \in \mathbb{F}_q} p_i \left|i^S\right\rangle \left\langle i^S\right| \tag{1}$$

とする．式 (1) で表された秘密情報を，補助系 R で純粋化する．$\left|i^R\right\rangle$ を系 R での正規直交系とすると，

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

とおける．

(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) 系 P における i 番目の量子状態（$1 \le i \le d$）を，$g(i) = x_k$ を満たす参加者 $x_k \in \mathcal{P}$ に配付する．

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 2 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，

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

この V を復元行列という．

Smith のスキームは量子秘密分散の定義 2 を満たしていることが，文献 12) によって示されている．

4. 量子複数秘密分散法

本章では，複数の秘密の量子状態を持つ量子複数秘密分散法の定義を与えた後，MSP を用いた構成法を示す．

4.1 量子複数秘密分散法

まず，量子複数秘密分散法の定義を与える（定義 3）．

定義 3 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（$1 \le i \le m$）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 1 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 と補助系 T_i を分散させた量子操作に逆変換が存在しないことを示す[8]．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 2 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 4 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，すべ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． □

4.2 提 案 法

提案法は，MSP を用いた単一秘密の量子秘密分散法[14] を，複数秘密分散法に拡張することで構成される．シェアの生成は，Smith の方法と同じく，MSP における $\mathbb{F}_q$ 上の行列 M（正確には，それに対応する等長写像 θ_M）を適用することで行う．参加者の部分集合 A が j 番目の秘密状態の復元を行うときは，まず M から A および g によって部分行列 M_A を構成し，M_A によりターゲットベクトル $\mathbf{e}_j$ を作成することで行う．しかしながら，単一秘密分散法における MSP では，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に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．このとき，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 の構成によっては Secrecy を満たさない場合が存在する．その考察は 4.3 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 構造を持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および配付

(1) access 構造に対する MSP の 4 つ組 $(\mathbb{F}_q, M, g, \mathbf{e})$ を定める．ここで $\mathbf{e} = \{\mathbf{e}_1, \cdots, \mathbf{e}_m\}$ である．

(2) 複数の秘密の量子状態 S_j が，正規直交基底 $\left|i^{S_j}\right\rangle$（$i \in \mathbb{F}_q$）で張られる状態空間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．

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

さらに，秘密情報 S_j を補助系 R_j で純粋化する．このとき，R_j の正規直交系を $\left|i^{R_j}\right\rangle$ として，

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

とおける．

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

(4) 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．

(5) 参加者 x_k に対して，系 P における i 番目の量子状態を配付する（ただし，$g(i) = x_k$ とする）．なお，以降では簡単のため，$|\mathcal{P}| = d$ であり，k 番目の参加者 x_k に対し，$g(k) = x_k$ であるとする．

秘密情報の復元

次に，秘密情報の復元について述べる．

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 に適用することで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 2 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．

4.3 評　　価

4.2 節で提案した量子複数秘密分散法を，4.1 節の定義 3 に従い評価する．

定理 3 *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 を持つ *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，$t = \min\{|A| \mid A \in \Gamma_i, i = 1, \cdots, m\}$ に対して以下の *2* 条件を満たす．

(i) $d \geq t + m - 1$,

(ii) $e \geq t + m - 1$.

証明　定義 3 の Secrecy の式を展開し，移項すると，

$$S(R_1 \cdots R_m A) - S(T_i A) = S(R_i) \qquad (2)$$

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，以下では $S(R_1 \cdots R_m A)$ と $S(T_i A)$ を求める．ここで，任意のアクセス構造に対し，$t = \min\{|A| \mid A \in \Gamma_i, i = 1, \cdots, m\}$ 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（補題 4，5）を示すことができる．

補題 4 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) $\mathrm{rank}(M'_B) < m$，$e - m \leq t - 1$ の場合

$$\begin{aligned} &S(R_1 \cdots R_m A) \\ &= (e-m)\log q \\ &\quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} \\ &\quad p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m}. \end{aligned} \qquad (3)$$

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

$$\begin{aligned} &S(R_1 \cdots R_m A) \\ &= (t-1)\log q \\ &\quad - \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} \\ &\quad p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m}. \end{aligned} \qquad (4)$$

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

$$\begin{aligned} &S(R_1 \cdots R_m A) \\ &= (e-m)\log q + \sum_i^m S(S_i). \end{aligned} \qquad (5)$$

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

$$\begin{aligned} &S(R_1 \cdots R_m A) \\ &= (t-1)\log q + \sum_i^m S(S_i). \end{aligned} \qquad (6)$$

証明　$S(R_1 \cdots R_m A)$ 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．

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

☆ 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．

$$
\begin{aligned}
&M_A(i_1,\ldots,i_m,i_{m+1},\ldots,i_e)^\top\big\rangle\\
&\big\langle i'_1,\cdots,i'_m,M_A(i'_1,\ldots,i'_m,i_{m+1},\ldots,i_e)^\top\big|\\
&\times\big\langle M_B(i_1,\ldots,i_m,i_{m+1},\ldots,i_e)^\top\big|\\
&\big|M_B(i'_1,\ldots,i'_m,i_{m+1},\ldots,i_e)^\top\big\rangle. \qquad (7)
\end{aligned}
$$

まず，式 (7) の内積部分について考える．ここで，$B_x^{i_{m+1},\cdots,i_e}$ は，明らかに $\mathrm{rank}(M'_B) < m$ のときは複数の要素を持ち，$\mathrm{rank}(M'_B) \geq m$ のときにはただ 1 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) $\mathrm{rank}(M'_B) < m$ の場合

$B_x^{i_{m+1},\cdots,i_e}$ は複数の要素を持つので，式 (7) を $B_x^{i_{m+1},\cdots,i_e}$ を使って変形すると，

$$
\begin{aligned}
&\rho^{R_1\cdots R_mA}\\
&=\frac{1}{q^{e-m}}\sum_{i_{m+1}}\cdots\sum_{i_e}\sum_{x\in Im(M_B)}\\
&\qquad\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}\ \sum_{(i'_1,\cdots,i'_m)\in B_x^{i_{m+1},\cdots,i_e}}\\
&\qquad\sqrt{p_{1i_1}p_{1i'_1}\cdots p_{mi_m}p_{mi'_m}}\\
&\qquad\times|i_1,\cdots,i_m,\\
&\qquad M_A(i_1,\ldots,i_m,i_{m+1},\ldots,i_e)^\top\big\rangle\\
&\qquad\big\langle i'_1,\cdots,i'_m,\\
&\qquad M_A(i'_1,\ldots,i'_m,i_{m+1},\ldots,i_e)^\top\big|. \qquad (8)
\end{aligned}
$$

ここで，式 (8) 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．

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

このとき，式 (8) は，

$$
\begin{aligned}
&\rho^{R_1\cdots R_mA}\\
&=\frac{1}{q^{e-m}}\sum_{i_{m+1}}\cdots\sum_{i_e}\sum_{x\in Im(M_B)}\\
&\qquad\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}p_{1i_1}\cdots p_{mi_m}\\
&\qquad\times\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle\left\langle\phi_x^{i_{m+1},\cdots,i_e}\right|. \qquad (9)
\end{aligned}
$$

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．$e-m \leq \mathrm{rank}(M_A) = t-1$ 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，$\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle$ が同じベクトルになることはない．$e-m > \mathrm{rank}(M_A) = t-1$ 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 $\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle$ 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，

$$
\begin{aligned}
&S(R_1\cdots R_mA)\\
&=-\frac{1}{q^{e-m}}\sum_{i_{m+1}}\cdots\sum_{i_e}\sum_{x\in Im(M_B)}\\
&\qquad\sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}\\
&\qquad p_{1i_1}\cdots p_{mi_m}\log\frac{1}{q^{e-m}}p_{1i_1}\cdots p_{mi_m}\\
&=(e-m)\log q\\
&\quad-\sum_{x\in Im(M_B)}\ \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}\\
&\qquad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}. \qquad (10)
\end{aligned}
$$

(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 $\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle$ 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，$(i_1,\cdots,i_e)$ の組合せは $q^{e-m-(t-1)}$ 通り存在する．よって，式 (9) は以下のように変形される．

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

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，

$$
\begin{aligned}
&S(R_1\cdots R_mA)\\
&=-q^{t-1}\frac{1}{q^{t-1}}\\
&\qquad\sum_{x\in Im(M_B)}\ \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}\\
&\qquad p_{1i_1}\cdots p_{mi_m}\log\frac{1}{q^{t-1}}p_{1i_1}\cdots p_{mi_m}\\
&=(t-1)\log q
\end{aligned}
$$

$$- \sum_{x \in Im(M_B)} \sum_{(i_1,\cdots,i_m) \in B_x^{i_{m+1},\ldots,i_e}} p_{1i_1} \cdots p_{mi_m} \log p_{1i_1} \cdots p_{mi_m}. \quad (11)$$

(2) $\mathrm{rank}(M'_B) \geq m$ の場合

この場合は $B_x^{i_{m+1},\ldots,i_e}$ はただ 1 つの要素を持つ．すなわち，異なる $(i_1,\cdots,i_m)$ で $\left|M_B(i_1,\cdots,i_e)^\top\right\rangle$ が同じになることはない．よって，式 (7) は，以下のようになる．

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

次に，(1) と同様に，同じ固有ベクトルとなるものどうしをまとめる．

(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 $\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle$ 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，

$$\begin{aligned}&S(R_1\cdots R_m A) \\ &= -\frac{1}{q^{e-m}} \sum_{i_1} \cdots \sum_{i_e} \\ &\quad p_{1i_1} \cdots p_{mi_m} \log \frac{1}{q^{e-m}} p_{1i_1} \cdots p_{mi_m} \\ &= (e-m)\log q + \sum_i^m S(S_i). \quad (12)\end{aligned}$$

(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 $\left|\phi_x^{i_{m+1},\cdots,i_e}\right\rangle$ 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，$(i_1,\cdots,i_e)$ の組合せは $q^{e-m-(t-1)}$ 通りである．よって，

$$\begin{aligned}&\rho^{R_1\cdots R_m A} \\ &= \frac{q^{e-m-(t-1)}}{q^{e-m}} \sum_{i_1} \cdots \sum_{i_m} \sum_j \\ &\quad p_{1i_1} \cdots p_{mi_m} |\phi_j\rangle\langle\phi_j|.\end{aligned}$$

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

$$\begin{aligned}&S(R_1\cdots R_m A) \\ &= -q^{t-1}\frac{1}{q^{t-1}} \sum_{i_1} \cdots \sum_{i_m} \\ &\quad p_{1i_1} \cdots p_{mi_m} \log \frac{1}{q^{t-1}} p_{1i_1} \cdots p_{mi_m} \\ &= (t-1)\log q + \sum_i^m S(S_i). \quad (13)\end{aligned}$$

■

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 5 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 5 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) $\mathrm{rank}(M'_B) < m-1$，$e-(m-1) \leq t-1$ の場合

$$\begin{aligned}&S(R_2\cdots R_m A) \\ &= (e-m)\log q + S(S_1) \\ &\quad - \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} \\ &\quad (p_{2i_2} \cdots p_{mi_m} \log p_{2i_2} \cdots p_{mi_m}). \quad (14)\end{aligned}$$

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

$$\begin{aligned}&S(R_2\cdots R_m A) \\ &= (t-1)\log q \\ &\quad - \sum_{x \in Im(M_B)} \sum_{(i_2,\cdots,i_m) \in B_x^{i_1,i_{m+1},\ldots,i_e}} \\ &\quad (p_{2i_2} \cdots p_{mi_m} \log p_{2i_2 1} \cdots p_{mi_m}). \quad (15)\end{aligned}$$

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

$$\begin{aligned}&S(R_2\cdots R_m A) \\ &= (e-m)\log q + \sum_{i=1}^m S(S_i). \quad (16)\end{aligned}$$

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

$$\begin{aligned}&S(R_2\cdots R_m A) \\ &= (t-1)\log q + \sum_{i=2}^m S(S_i). \quad (17)\end{aligned}$$

証明 補題 4 と同様に証明できるため，省略する．■

補題 4，5 を用いて，定理 3 の (i) あるいは (ii) が満たされないとき，Secrecy が満たされないことを示す．

(1) $\mathrm{rank}(M'_B) < m-1$, $e-m \le t-2$ の場合
式 (3) と式 (14) より,

$$\begin{aligned}
&S(R_1\cdots R_mA) - S(R_2\cdots R_mA)\\
&= (e-m)\log q\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\quad -((e-m)\log q + S(S_1)\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_2,\cdots,i_m)\in B_x^{i_1,i_{m+1},\ldots,i_e}}\\
&\quad p_{2i_2}\cdots p_{mi_m}\log p_{2i_2}\cdots p_{mi_m})\\
&= -S(S_1)\\
&\quad + \sum_{x\in Im(M_B)} \sum_{(i_2,\cdots,i_m)\in B_x^{i_1,i_{m+1},\ldots,i_e}}\\
&\quad p_{2i_2}\cdots p_{mi_m}\log p_{2i_2}\cdots p_{mi_m}\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\neq S(S_1). \qquad (18)
\end{aligned}$$

よって, Secrecy は満たされない.

(2) $\mathrm{rank}(M'_B) < m-1$, $e-m = t-1$ の場合
式 (3) と式 (15) より,

$$\begin{aligned}
&S(R_1\cdots R_mA) - S(R_2\cdots R_mA)\\
&= ((e-m)\log q\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\quad -(-(t-1)\log q\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_2,\cdots,i_m)\in B_x^{i_1,i_{m+1},\ldots,i_e}}\\
&\quad p_{2i_2}\cdots p_{mi_m}\log p_{2i_2}\cdots p_{mi_m})\\
&\neq S(S_1). \qquad (19)
\end{aligned}$$

よって, Secrecy は満たされない.

(3) $\mathrm{rank}(M'_B) < m-1$, $e-m > t-1$ の場合
式 (4) と式 (15) より,

$$\begin{aligned}
&S(R_1\cdots R_mA) - S(R_2\cdots R_mA)\\
&= (t-1)\log q\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\quad -(-(t-1)\log q\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_2,\cdots,i_m)\in B_x^{i_1,i_{m+1},\ldots,i_e}}\\
&\quad p_{2i_2}\cdots p_{mi_m}\log p_{2i_2}\cdots p_{mi_m})\\
&= \sum_{x\in Im(M_B)} \sum_{(i_2,\cdots,i_m)\in B_x^{i_1,i_{m+1},\ldots,i_e}}\\
&\quad p_{2i_2}\cdots p_{mi_m}\log p_{2i_2}\cdots p_{mi_m}\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\neq S(S_1). \qquad (20)
\end{aligned}$$

よって, Secrecy は満たされない.

(4) $\mathrm{rank}(M'_B) = m-1$, $e-m \le t-2$ の場合
式 (3) と式 (16) より,

$$\begin{aligned}
&S(R_1\cdots R_mA) - S(R_2\cdots R_mA)\\
&= (e-m)\log q\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\quad - \left((e-m)\log q + \sum_{i=1}^{m} S(S_i)\right)\\
&= - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\quad - \sum_{i=1}^{m} S(S_i)\\
&\neq S(S_1). \qquad (21)
\end{aligned}$$

よって, Secrecy は満たされない.

(5) $\mathrm{rank}(M'_B) = m-1$, $e-m = t-1$ の場合
式 (3) と式 (17) より,

$$\begin{aligned}
&S(R_1\cdots R_mA) - S(R_2\cdots R_mA)\\
&= (e-m)\log q\\
&\quad - \sum_{x\in Im(M_B)} \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\ldots,i_e}}\\
&\quad p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&\quad -(t-1)\log q + \sum_{i=2}^{m} S(S_i)\\
&\neq S(S_1). \qquad (22)
\end{aligned}$$

よって, Secrecy は満たされない.

(6) $\mathrm{rank}(M'_B) = m-1$, $e-m > t-1$ の場合
式 (4) と式 (17) より,

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

$$
\begin{aligned}
&p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&-\left((t-1)\log q+\sum_{i=2}^{m}S(S_i)\right)\\
=&-\sum_{x\in Im(M_B)}\ \sum_{(i_1,\cdots,i_m)\in B_x^{i_{m+1},\cdots,i_e}}\\
&p_{1i_1}\cdots p_{mi_m}\log p_{1i_1}\cdots p_{mi_m}\\
&-\sum_{i=2}^{m}S(S_i)\\
\neq\ & S(S_1). \qquad (23)
\end{aligned}
$$

よって，Secrecy は満たされない．

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

式 (5) と式 (16) より，

$$
\begin{aligned}
&S(R_1\cdots R_mA)-S(R_2\cdots R_mA)\\
&=(e-m)\log q+\sum_{i=1}^{m}S(S_i)\\
&\quad-\left((e-m)\log q+\sum_{i=1}^{m}S(S_i)\right)\\
&=0\\
&\neq S(S_1). \qquad (24)
\end{aligned}
$$

よって，Secrecy は満たされない．

以上から，$d=|A|+|B|$，$|B|\geq\mathrm{rank}(M'_B)$ 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 3 において，特に (m,t,d) 量子閾値複数秘密分散法の場合を考えると，以下の定理 6 が成り立つことがいえる．

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．

(i) $d\geq t+m-1$,

(ii) $e\geq t+m-1$.

証明 定理 3 より必要条件は満たしているので，以下では十分条件について考える．定理の条件の (i) を満たすとき $\mathrm{rank}(M'_B)\geq m$ である．このとき，補題 4，5 の条件を考えて，

(1) $\mathrm{rank}(M'_B)\geq m$，$e-m=t-1$ の場合

式 (5) と式 (17) より，

$$
\begin{aligned}
&S(R_1\cdots R_mA)-S(R_2\cdots R_mA)\\
&=(e-m)\log q+\sum_{i=1}^{m}S(S_i)\\
&\quad-\left((t-1)\log q+\sum_{i=2}^{m}S(S_i)\right)\\
&=S(S_1). \qquad (25)
\end{aligned}
$$

よって，Secrecy を満たす．

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

式 (6) と式 (17) より，

$$
\begin{aligned}
&S(R_1\cdots R_mA)-S(R_2\cdots R_mA)\\
&=(t-1)\log q+\sum_{i=1}^{m}S(S_i)\\
&\quad-\left((t-1)\log q+\sum_{i=2}^{m}S(S_i)\right)\\
&=S(S_1). \qquad (26)
\end{aligned}
$$

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 7 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は，$\forall A\in\Gamma_i$ $(1\leq i\leq m)$ に対し *Recoverability* を満たす．

証明 定理 3，補題 4 および 5 と同様にして示すことができる． ■

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 8 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．

証明 $t\leq m$ 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 1 列〜t 列からなる部分行列の逆行列でなければならず，残りの列は復元行列を適用す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 についてこれが成立するため，M の $t+1$ 列目以降は零行列となることがいえる．以上より，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[3] の単純な拡張により，以下の定理 9 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．

証明 (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[4),16)] に反する．

(2) (1) と同様 no-cloning 定理に反する．

■

最後に，付録 A.1 において $(2,3,4)$ 量子閾値複数秘密分散法を具体的に構成しているので，参照されたい．

5. ま と め

本論文では，複数の秘密量子状態を分散符号化する量子複数秘密分散法を定義し，その構成法として MSP を用いた方法を提案した．さらに本論文では，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，$t = \min\{|A| \mid A \in \Gamma_i, i = 1, \cdots, m\}$ 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 $m+t-1$ 列以上の列を持つ必要があることを示した．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を与えた．さらに，閾値 t と秘密の量子状態数 m の間に $t > m$ の関係が成り立たないとき，MSP を利用した (m,t,d) 量子閾値複数秘密分散法は存在しないことを示した．

謝辞 多くの有益な助言をくださいました査読者の方々に感謝します．本研究成果は文部科学省 21 世紀 COE プログラム，および，文部科学省科学技術振興調整費による．

参 考 文 献

1) Bandyopadhyay, S.: Teleportation and secret sharing with pure entangled states, *Phys. Rev. A*, Vol.62, No.1, 012308 (2000).
2) Blundo, C., Santis, A.D., Crescenzo, G.D., Gaggia, A.G. and Vaccaro, U.: Multi-Secret Sharing Schemes, *Advances in Cryptology — CRYPTO '94*, Lecture Notes in Computer Science, Vol.839, pp.150–163 (1994).
3) 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).
4) Dieks, D.: Communication by EPR devices, *Phys. Rev. Lett. A*, Vol.92, No.6, pp.271–272 (1982).
5) Gál, A.: A characterization of span program size and improved lower bounds for monotone span programs, *Computational Complexity*, Vol.10, No.4, pp.277–296 (2001).
6) Gottesman, D.: Theory of quantum secret sharing, *Phys. Rev. A*, Vol.61, No.4, 042311 (2000).
7) Hillery, M., Bužek, V. and Berthiaume, A.: Quantum secret sharing, *Phys. Rev. A*, Vol.59, No.3, pp.1829–1834 (1999).
8) Imai, H., Müller-Quade, J., Nascimento, A.C., Tuyls, P. and Winter, A.: An Information Theoretical Model for Quantum Secret Sharing Schemes, *Quantum Information and Computation*, Vol.5, No.1, pp.69–80 (2005).
9) Karchmer, M. and Wigderson, A.: On Span Programs, *Proc. 8th Annual Structure in Complexity Theory Conference*, pp.102–111 (1993).
10) Nielsen, M.A. and Chuang, I.L.: *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
11) Rietjens, K.P.: An Information Theoretical Approach to Quantum Secret Sharing Schemes, Master's thesis, Department of Mathematics and Computing Science, Technische Universiteit Eindhoven (2004).
12) Rietjens, K.P., Schoenmakers, B. and Tuyls, P.: Quantum Information Theoretical Analysis of Various Constructions for Quantum Secret Sharing, *Proc. International Symposium on Information Theory — ISIT 2005*, Adelaide, Australia, pp.1598–1602 (2005).
13) Shamir, A.: How To Share a Secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
14) Smith, A.D.: Quantum secret sharing for general access structures, quant-ph/0001087 (2000).
15) Tamura, Y., Tada, M. and Okamoto, E.: Update of access structure in Shamir's (k,n) threshold scheme, *SCIS1999*, pp.469–474 (1999).
16) Wootters, W.K. and Zurek, W.H.: A single quantum cannot be cloned, *Nature*, Vol.299, pp.802–803 (1982).

付 録

A.1 構 成 例

この章では，量子複数秘密分散法の構成例として，量子閾値複数秘密分散法の例を示す．ここで，秘密が 1 つの場合の (t,d) 閾値秘密分散法については，閾値 t が列数となる Vandermonde 行列を用いることにより構成できることが知られている．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いえることに注意されたい．

以下では，量子閾値複数秘密分散法として，$\mathbb{F}_5$ 上で秘密 2 つと閾値 3 を持つものを具体的に構成する．

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．

$$|R_1S_1\rangle = \sum_{i_1=0}^{4} \sqrt{p_{1i_1}} \left|i_1^{R_1}\right\rangle \otimes \left|i_1^{S_1}\right\rangle,$$

$$|R_2S_2\rangle = \sum_{i_2=0}^{4} \sqrt{p_{2i_2}} \left|i_2^{R_2}\right\rangle \otimes \left|i_2^{S_2}\right\rangle.$$

(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 行をとると $\begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \end{pmatrix}$ を構成でき☆，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．

$$(I_{\mathcal{R}} \otimes \theta_M)|\mathcal{R}SE\rangle = |R_1R_2R_EP_1P_2P_3P_4P_5\rangle.$$

(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 \\
&\quad + |000202242\rangle + |000303313\rangle + |000404434\rangle \\
&\quad + |001001120\rangle + |001102241\rangle \\
&\quad + |001203312\rangle + |001304433\rangle + |001400004\rangle \\
&\quad + |002002240\rangle + |002103311\rangle \\
&\quad + |002204432\rangle + |002300003\rangle + |002401124\rangle \\
&\quad + |003003310\rangle + |003104431\rangle \\
&\quad + |003200002\rangle + |003301123\rangle + |003402244\rangle \\
&\quad + |004004430\rangle + |004100001\rangle \\
&\quad + |004201122\rangle + |004302243\rangle + |004403314\rangle) \\
&\quad + \sqrt{p_{10}p_{21}} \\
&\quad \times(|010011210\rangle + |010112331\rangle \\
&\quad + |010213402\rangle + |010314023\rangle + |010410144\rangle \\
&\quad + |011012330\rangle + |011113401\rangle \\
&\quad + |011214022\rangle + |011310143\rangle + |011411214\rangle \\
&\quad + |012013400\rangle + |012114021\rangle \\
&\quad + |012210142\rangle + |012311213\rangle + |012412334\rangle \\
&\quad + |013014020\rangle + |013110141\rangle \\
&\quad + |013211212\rangle + |013312333\rangle + |013413404\rangle \\
&\quad + |014010140\rangle + |014111211\rangle \\
&\quad + |014212332\rangle + |014313403\rangle + |014414024\rangle) \\
&\quad + \sqrt{p_{10}p_{22}} \\
&\quad \times(|020022420\rangle + |020123041\rangle \\
&\quad + |020224112\rangle + |020320233\rangle + |020421304\rangle \\
&\quad + |021023040\rangle + |021124111\rangle \\
&\quad + |021220232\rangle + |021321303\rangle + |021422424\rangle \\
&\quad + |022024110\rangle + |022120231\rangle \\
&\quad + |022221302\rangle + |022322423\rangle + |022423044\rangle \\
&\quad + |023020230\rangle + |023121301\rangle \\
&\quad + |023222422\rangle + |023323043\rangle + |023424114\rangle \\
&\quad + |024021300\rangle + |024122421\rangle \\
&\quad + |024223042\rangle + |024324113\rangle + |024420234\rangle) \\
&\quad + \sqrt{p_{10}p_{23}} \\
&\quad \times(|030033130\rangle + |030134201\rangle \\
&\quad + |030230322\rangle + |030331443\rangle + |030432014\rangle \\
&\quad + |031034200\rangle + |031130321\rangle \\
&\quad + |031231442\rangle + |031332013\rangle + |031433134\rangle \\
&\quad + |032030320\rangle + |032131441\rangle \\
&\quad + |032232012\rangle + |032333133\rangle + |032434204\rangle \\
&\quad + |033031440\rangle + |033132011\rangle \\
&\quad + |033233132\rangle + |033334203\rangle + |033430324\rangle \\
&\quad + |034032010\rangle + |034133131\rangle \\
&\quad + |034234202\rangle + |034330323\rangle + |034431444\rangle) \\
&\quad + \sqrt{p_{10}p_{24}} \\
&\quad \times(|040044340\rangle + |040140411\rangle \\
&\quad + |040241032\rangle + |040342103\rangle + |040443224\rangle \\
&\quad + |041040410\rangle + |041141031\rangle \\
&\quad + |041242102\rangle + |041343223\rangle + |041444344\rangle
\end{aligned}$$

☆ 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．

$$
\begin{aligned}
&+|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
\end{aligned}
$$

$$
\begin{aligned}
&+|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
\end{aligned}
$$

$$
\begin{aligned}
&+|442034420\rangle+|442130041\rangle\\
&+|442231112\rangle+|442332233\rangle+|442433304\rangle\\
&+|443030040\rangle+|443131111\rangle\\
&+|443232232\rangle+|443333303\rangle+|443434424\rangle\\
&+|444031110\rangle+|444132231\rangle\\
&+|444233302\rangle+|444334423\rangle+|444430044\rangle).
\end{aligned}
\tag{27}
$$

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

$$
V=\begin{pmatrix}3&3&2\\3&2&3\\1&3&3\end{pmatrix}. \tag{28}
$$

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

$$
\begin{aligned}
&+|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
\end{aligned}
$$

$$
\begin{aligned}
&+|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\\
&+|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{29}
$$

式 (29) を $|R_1,S_1\rangle$ に部分トレースをすると,

$$
\begin{aligned}
&\mathrm{Tr}_{R_2R_{E_1}R_{E_2}S_2P_3'P_4P_5}\left(\left|R_1R_2R_{E_1}R_{E_2}S_1S_2P_3'P_4P_5\right\rangle\right.\\
&\left.\left\langle R_1R_2R_{E_1}R_{E_2}S_1S_2P_3'P_4P_5\right|\right)\\
&=p_{10}\left(\frac{p_{20}}{5^2}\times25+\frac{p_{21}}{5^2}\times25+\frac{p_{22}}{5^2}\times25\right)|00\rangle\langle00|\\
&\quad+p_{11}\left(\frac{p_{20}}{5^2}\times25+\frac{p_{21}}{5^2}\times25+\frac{p_{22}}{5^2}\times25\right)|11\rangle\langle11|\\
&\quad+p_{12}\left(\frac{p_{20}}{5^2}\times25+\frac{p_{21}}{5^2}\times25+\frac{p_{22}}{5^2}\times25\right)|22\rangle\langle22|\\
&\quad+p_{13}\left(\frac{p_{20}}{5^2}\times25+\frac{p_{21}}{5^2}\times25+\frac{p_{22}}{5^2}\times25\right)|33\rangle\langle33|\\
&\quad+p_{14}\left(\frac{p_{20}}{5^2}\times25+\frac{p_{21}}{5^2}\times25+\frac{p_{22}}{5^2}\times25\right)|44\rangle\langle44|\\
&=p_{10}|00\rangle\langle00|+p_{11}|11\rangle\langle11|+p_{12}|22\rangle\langle22|\\
&\quad+p_{13}|33\rangle\langle33|+p_{14}|44\rangle\langle44|.
\end{aligned}
\tag{30}
$$

式 (30) は秘密 S_1 を純粋化したものの密度行列にほかならない．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．

(平成 18 年 8 月 30 日受付)
(平成 19 年 4 月 6 日採録)

早稲田篤志

2000 年電気通信大学電気通信学部電子情報学科卒業．2002 年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博士前期課程修了．2007 年同博士後期課程修了（博士（情報科学））．同年独立行政法人情報通信研究機構専攻研究員．情報セキュリティの研究に従事．

双紙　正和（正会員）

1991年東京大学工学部卒業，1993年同大学大学院理学系研究科情報科学専攻修了．電気通信大学大学院情報システム学研究科助手を経て，1999年から2003年1月まで北陸先端科学技術大学院大学情報科学研究科助手．2003年2月から同研究科特任准教授．現在に至る．情報セキュリティの研究に従事．博士（工学）．

宮地　充子（正会員）

1988年大阪大学理学部数学科卒業．1990年同大学大学院修士課程修了．同年松下電器産業株式会社入社．1998年北陸先端科学技術大学院大学・情報科学研究科准教授．現在に至る．2002〜2003年カリフォルニア大学デービス校客員研究員．情報セキュリティの研究に従事．博士（理学）．SCIS93若手論文賞，科学技術庁注目発明賞，平成13年度坂井記念特別賞，平成14年度標準化貢献賞，平成17年度功労感謝状，情報セキュリティ文化賞各受賞．電子情報通信学会，IACR，日本数学会各会員．