Computer Security Symposium 2019
21 - 24 October 2019

XORベース秘密分散法の新しい証明法

島 幸司[1,a)]　土井 洋[1,b)]

概要：情報の盗難対策や紛失対策を同時に満たすような秘密情報の分散管理の方法として秘密分散法が知られている．また，さまざまな計算コストの小さい秘密分散法が提案されている．本研究では，藤井らと栗原らのそれぞれの XOR ベース秘密分散法を参考に，巡回行列を活用した新しい証明法を与える．また，実用性を見据えて，ソフトウェア実装評価を示す．

キーワード：秘密分散法，XOR ベース，巡回行列，ソフトウェア実装

New Proof Techniques of XOR-based Secret Sharing Schemes

Koji Shima[1,a)]　Hiroshi Doi[1,b)]

Abstract: Secret sharing schemes are known to simultaneously satisfy the need to distribute and manage secret information to prevent information theft and loss. Several secret sharing schemes with low computational costs also have been proposed. In this study, we provide new proof techniques that actively use circulant matrices by referring to Fujii et al.'s and Kurihara et al.'s XOR-based secret sharing schemes. Moreover, considering practical use, we present an evaluation of our software implementation.

Keywords: secret sharing scheme, XOR-based, circulant matrix, software implementation

1. はじめに

情報の盗難対策や紛失対策を同時に満たすような秘密情報の分散管理の方法として秘密分散法が知られている．1979 年に Blakley [1] と Shamir [2] はそれぞれ独自に (k, n) しきい値法と呼ばれる秘密分散法の概念を提案した．Shamir の (k, n) しきい値法は秘密情報を n 個のシェアに分散し，n 個のシェアの中から任意の k 個を集めれば元の秘密情報を復元でき，任意の $k-1$ 個のシェアからは元の秘密情報に関する情報が全く得られない．このため，シェアの一部が漏えいしても元の秘密情報は安全であり，シェアの一部が紛失しても元の秘密情報を復元できる．

1.1 秘密分散法

Shamir の (k, n) しきい値法は $k-1$ 次多項式を用いるため，計算コストが大きい．そのため，排他的論理和演算（XOR）のみを用いて秘密情報の分散および復元ができる秘密分散法が提案されている．XOR ベースの (k, n) しきい値秘密分散法では，藤井ら [3] の手法や栗原ら [4], [5] の手法が知られている．また，栗原ら [6] は XOR のみを用いた (k, L, n) ランプ型秘密分散法を提案した．

1.2 高速化

GF(2^L) 上の演算は高速化に貢献するが，1 回の乗算に複数回の XOR 演算を要する [7], [8]．ルックアップテーブル方式を用いて，この演算コストを 1 回にできるが，実質的に $L = 8$ に限られる [8]．L の拡張には，GF(2^{64}) の乗算の高速化テクニックが知られている [9]．一方で，拡張された CPU 命令セットを用いるため，IoT に代表される組み込み機器のようにすべてのハードウェアに適用できるわけではない．純粋な XOR 演算のみなら，対象のハードウェアがサポートする XOR 演算の最大ビット長を利用し高速化に貢献する．

[1] 情報セキュリティ大学院大学
Institute of Information Security
[a)] dgs164101@iisec.ac.jp
[b)] doi@iisec.ac.jp

1.3 本研究の貢献

(k,n) しきい値秘密分散法 [3], [4], [5] と (k,L,n) ランプ型秘密分散法 [6] の $L=1$ の場合を参考に，XOR ベース (k,n) しきい値秘密分散法の新しい証明法を提供する．構成法は [6] の $L=1$ と同等であるが，[4], [5] の差分として明示する．本研究の貢献は次のように要約できる．

- 巡回行列を活用した新しい証明法を与える．
- n が小さいとき，シェア生成は [4], [5] の手法に比べて効率的である．

2. 準備

2.1 表記法と定義

- $\oplus$ はビット単位の XOR を表す．
- $||$ はバイナリ列の連結を表す．
- p は素数である．
- $n \in \mathbb{N}$ は $p \geq n$ の参加者数を表す．
- 乱数，分割された秘密情報とシェア，それらの XOR の項や確率変数，行列の添え字の値は GF(p) の要素である．すなわち，$X_{c(a\pm b)}$ は $X_{c(a\pm b) \bmod p}$ を表す．
- $H(X)$ は確率変数 X のエントロピーを表す．
- $\xleftarrow{\$} \mathcal{X}$ は有限集合 $\mathcal{X}$ から $|\mathcal{X}|$ ビットの乱数を生成する関数を表す．
- $\gcd(a,b)$ は a と b の最大公約数を表す．
- $\deg(f(x))$ は 多項式 $f(x)$ の次数を表す．

2.2 行列に関する表記法と定義

- $i,j \in \{0,1,\cdots,t-1\}$ として，$t \times t$ 行列 $[a_{(i,j)}]$ を表す．すなわち，0 行 0 列から始まる．
- $\mathbf{I}_t$ は $t \times t$ 単位行列を表す．
- $\boldsymbol{O}$ は零行列を表す．
- $\xleftarrow{\circ}$ または $\xrightarrow{\circ}$ は行基本変形を表す．

2.3 巡回行列

$t \times t$ 行列 $\mathbf{C}$ が

$$\mathbf{C} = \begin{bmatrix} c_0 & c_1 & \cdots & c_{t-2} & c_{t-1} \\ c_{t-1} & c_0 & \cdots & \cdots & c_{t-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ c_2 & \cdots & c_{t-1} & c_0 & c_1 \\ c_1 & c_2 & \cdots & c_{t-1} & c_0 \end{bmatrix}$$

の形であるとき，$\mathbf{C}$ を巡回行列または循環行列と呼ぶ．巡回行列 $\mathbf{A},\mathbf{B}$ に対して，$\mathbf{A}+\mathbf{B}$ や $\mathbf{AB}$ は巡回行列である．また，巡回行列は和と積について可換である．巡回行列は 1 つの t 次ベクトルで表すことができる．本稿では，$\mathbf{C} = (c_0, c_1, \cdots, c_{t-2}, c_{t-1})$ と表す．多項式 $c(x) = \sum_{i=0}^{t-1} c_i x^i$ を $\mathbf{C}$ の随伴多項式と呼ぶ．また，$\mathbf{C}$ において，0 でない c_i の総数を重みと呼ぶ．

[13], [14] により，定理 2.1 が分析されている．

定理 2.1 巡回行列 $\mathbf{C} = (c_0, c_1, \cdots, c_{t-2}, c_{t-1})$ とする．随伴多項式 $c(x)$ に対して $d = \deg(\gcd(x^t + 1, c(x)))$ とするとき，$\mathbf{C}$ の階数は $t-d$ である．

2.4 GF(2) 上の巡回行列

GF(2) 上の $t \times t$ 巡回行列の記法と性質を示す．

- i 番目の成分のみが 1 である重み 1 の巡回行列を g_i と表す．添え字の法は t とする．
- g_0 は単位行列を表す．また，$1 \stackrel{\text{def}}{=} g_0 = \mathbf{I}_t$ と定義する．
- 積について，$g_a \times g_b = g_{a+b}$, $(g_a)^b = g_{ab}$ である．
- 分配法則について，$(g_a + g_b) \times g_c = g_{a+c} + g_{b+c}$, $g_a \times (g_b + g_c) = g_{a+b} + g_{a+c}$ である．

次に，重みが偶数の GF(2) 上の $t \times t$ 巡回行列についての性質をいくつか記す．

補題 2.1 重みが偶数の GF(2) 上の $t \times t$ 巡回行列について，次を満たす．
(1) 0 行目から $t-2$ 行目の和は $t-1$ 行目と等しい
(2) 0 列目から $t-2$ 列目の和は $t-1$ 列目と等しい

補題 2.2 重みが 2 の GF(2) 上の $t \times t$ 巡回行列は乗法逆元を持たない．

2.5 完全秘密分散法

[10] の定義 2 と定義 3 において，完全秘密分散法は次の条件を満たす必要があると示している．

[正当性] アクセス構造に属するすべての集合 B は秘密に関する情報を得る．

[完全性] アクセス構造に属さないすべての集合 T は秘密に関する情報を一切得ない．

言い換えれば，ある与えられた確率分布の中での秘密情報に関する確率変数を S，ある与えられた確率分布の中での権限を持つすべての集合 B のシェアに関する確率変数を S_B，ある与えられた確率分布の中での権限を持たないすべての集合 T のシェアに関する確率変数を S_T としたとき，完全秘密分散法は次の条件を必要とする．

[正当性] $H(S|S_B) = 0$.

[完全性] $H(S|S_T) = H(S)$.

2.6 理想的秘密分散法

[4], [5], [11], [12] の文献から，n 人の参加者集合を $\mathcal{P} = \{P_1, \cdots, P_n\}$，秘密情報の集合を $\mathcal{S}$，参加者 P_i のシェアとして可能性のある集合を $\mathcal{W}_i$ とする秘密分散法が与えられたとき，その情報率を $\rho = \dfrac{H(S)}{\max\limits_{P_i \in \mathcal{P}} H(W_i)}$ と定義する．S と W_i はそれぞれ $s \in \mathcal{S}$, $w_i \in \mathcal{W}_i$ によって誘起される確率変数とする．$\mathcal{S}$ と $\mathcal{W}_i$ がどちらも一様な確率分布に

従うとき，$\rho = \frac{\log_2 |\mathcal{S}|}{\max_{P_i \in \mathcal{P}} \log_2 |\mathcal{W}_i|} = 1$ を満たす完全秘密分散法を理想的秘密分散法という．すなわち，各シェアのビット長は秘密情報のビット長よりは小さくできないが，これらのビット長が等しい場合，理想的秘密分散法となる．

3. 先行研究

栗原ら [4], [5] の (k, n) しきい値秘密分散法では，素数 $p(\geq n)$ を選び，秘密情報 $s \in \{0,1\}^{d(p-1)}$ を $s_1, \cdots, s_{p-1} \in \{0,1\}^d$ のブロックに等分割する．d はたとえば 8 や 64 である．分散アルゴリズムでは，秘密情報を等分割し，$(k-1)p-1$ 個の d ビットの乱数を生成する．(k, p) しきい値法に対応する一意に与えられる生成行列 $\mathbf{G}$ を用いてシェアを生成する．ここで，生成行列は $(p-1) \times p$ または $(p-1) \times (p-1)$ の GF(2) 上の行列を成分とする．復元アルゴリズムでは，復元に協力する参加者の各シェアを d ビットに等分割する．生成行列から k 人の参加者に対応する行列 $\mathbf{G}_k$ を得る．この行列は正方行列ではないが，ガウス消去法等を用いて秘密情報を得る．なお，栗原ら [6] のランプ型秘密分散法では，$\mathbf{G}_k$ が正方行列である．

4. 巡回行列を成分とする生成行列の検討

まず，重みが 2 の GF(2) 上の $p \times p$ 巡回行列，およびそれらの行列の積の階数について分析する．次に，$p \times p$ 巡回行列を成分とする秘密復元のための行列の階数を分析する．

4.1 GF(2) 上の重み 2 の巡回行列の積の階数

定理 2.1 を用いて階数を分析するため，重みが 2 の随伴多項式の性質を調べる．

補題 4.1 $a, b \geq 1$ とする．GF(2) 上の多項式 $x^a + 1, x^b + 1$ について，$\gcd(x^a + 1, x^b + 1) = x^{\gcd(a,b)} + 1$ である．

証明 $a = b$ のとき成立する．$a > b$ を考える．有限体 K 上の多項式 $A(x), B(x)$ の GCD は次の手順で求まる [15].

(1) $B(x) = 0$ なら，$A(x)$ を出力して終了する．

(2) $\deg(R(x)) < \deg(B(x))$ とする．$A(x) = B(x) \cdot Q(x) + R(x)$ となる $Q(x), R(x)$ を計算し，$A(x) \leftarrow B(x), B(x) \leftarrow R(x)$ と置き換え，手順 (1) に戻る．

次に，$A(x) = x^a + 1, B(x) = x^b + 1$ に限定して考える．整数 q, r を $a = b \cdot q + r$ となるように置く．ただし，$r < b$ である．$A(x) = B(x) \cdot Q(x) + R(x)$ となる $Q(x) = \sum_{i=1}^{q} x^{a-b \cdot i}$, $R(x) = x^r + 1$ が計算できる．$r = 0$ のとき $R(x) = 0$ である．ここで，$A(x), B(x)$ の次数 a, b にのみ注目すると，

(1) $b = 0$ なら，$x^a + 1$ を出力して終了する．

(2) $r < b$ とする．$a = b \cdot q + r$ となる q, r を計算し，$a \leftarrow b, b \leftarrow r$ と置き換え，手順 (1) に戻る．

ことになるが，このアルゴリズムは整数 a, b の GCD を求めるユークリッド互除法と同一である．したがって，$x^{\gcd(a,b)} + 1$ が出力される． □

補題 4.2 $0 \leq b < a < p$ とする．GF(2) 上の多項式 $x^a + x^b, x^p + 1$ について，$\gcd(x^a + x^b, x^p + 1) = x + 1$ である．

証明 $x^a + x^b = x^b(x^{a-b} + 1)$ となる．$\gcd(x^b, x^p + 1) = 1$ である．p は素数より $\gcd(a - b, p) = 1$ であり，補題 4.1 より $\gcd(x^{a-b} + 1, x^p + 1) = x + 1$ である．したがって，補題を証明できた． □

重みが 2 の GF(2) 上の $p \times p$ 巡回行列の積についても，同様の結果が得られる．

補題 4.3 $0 \leq b < a < p, 0 \leq d < c < p$ とする．GF(2) 上の多項式 $x^a + x^b, x^c + x^d, x^p + 1$ について，$\gcd((x^a + x^b) \cdot (x^c + x^d), x^p + 1) = x + 1$ である．

定理 4.1 $a \geq 0$ とする．GF(2) 上において，重みが 2 の $p \times p$ 巡回行列 $\mathbf{C}_0, \cdots, \mathbf{C}_a$ の積

$$\mathbf{C} = \mathbf{C}_0 \times \cdots \times \cdot \mathbf{C}_a = \prod_{l=0, i(l) \neq j(l)}^{a} (g_{i(l)} + g_{j(l)})$$

の階数は $p - 1$ である．

証明 $0 \leq l \leq a$ かつ $i(l) \neq j(l)$ について，$\mathbf{C}_l = g_{i(l)} + g_{j(l)}$ である．その随伴多項式は $c_l(x) = x^{i(l)} + x^{j(l)}$ である．$\mathbf{C}$ の随伴多項式は $c(x) = \prod_{l=0}^{a} c_l(x)$ となる．$0 \leq i(l), j(l) < p$ であり，$i(l) \neq j(l)$ であるので，補題 4.3 より，$\gcd(c(x), x^p + 1) = x + 1$ である．したがって，定理 2.1 より，$\mathbf{C}$ の階数は $p - 1$ である． □

4.2 行基本変形

(k, n) しきい値秘密分散法のシェア生成行列として，$p \times p$ 巡回行列を成分とする $n \cdot p \times k \cdot p$ 行列

$$\mathbf{G} = \begin{bmatrix} 1 & g_0 & g_0^2 & \cdots & g_0^{k-1} \\ 1 & g_1 & g_1^2 & \cdots & g_1^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & g_{n-1} & g_{n-1}^2 & \cdots & g_{n-1}^{k-1} \end{bmatrix} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{n-1} \end{bmatrix}$$

を考える．以降，$\mathbf{G}$ の i 行目とは $\mathbf{g}_i$ を指す．参加者 P_x $(x = 0, \cdots, n-1)$ のシェアは x 行目から生成されることになる．$\mathbf{G}$ から任意に k 行を選んだ行列

$$\mathbf{G}_k = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{k-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-1} & x_{k-1}^2 & \cdots & x_{k-1}^{k-1} \end{bmatrix}$$

を考える．これは $x_0 = g_{t_0}, \cdots, x_{k-1} = g_{t_{k-1}}$ に対応する参加者 P_x $(x = t_0, \cdots, t_{k-1})$ が復元に協力すると考えることができる．$\mathbf{G}_k$ から Vandermonde 行列が連想されるが，巡回行列が逆行列を持たない場合があるので，注意

を要する．階数を分析するために，まず 0 行目を i 行目 $(i=1,\cdots,k-1)$ に加算する．その結果，$m(\geq 1)$ 行目は $(0, x_m+x_0, x_m^2+x_0^2, \cdots, x_,^{k-1}+x_0^{k-1})$ となる．ここで，補題 2.2 より，m 行目に $(x_m+x_0)^{-1}$ を乗ずることはできないが，以下の定理 4.2 を用いて，1 列目の 2 行目以降を行基本変形ですべて 0 にすることができる．

定理 4.2　重みが 2 の GF(2) 上の $p\times p$ 巡回行列 g_a+g_b と g_c+g_d が与えられたとき，$g_c+g_d = \mathbf{T}_{a,b}^{c,d}(g_a+g_b)$ となる GF(2) 上の $p\times p$ 巡回行列 $\mathbf{T}_{a,b}^{c,d}$ が存在する．

証明　重みが 2 なので，$a\not\equiv b \pmod p$ である．$t=(b-a)^{-1}(d-c) \mod p$ とすると，$0<(b-a)^{-1}<p$, $0<d-c<p$ であるから $0<t<p$ である．$t\neq 1$ のときは

$$\begin{aligned} g_{-a}(g_a+g_b) &= g_0+g_{b-a},\\ \sum_{i=0}^{t-1} g_{i(b-a)}(g_0+g_{b-a}) &= g_0+g_{d-c},\\ g_c(g_0+g_{d-c}) &= g_c+g_d \end{aligned}$$

となるので，$\mathbf{T}_{a,b}^{c,d} = g_c\sum_{i=0}^{t-1} g_{i(b-a)}g_{-a}$ と置けばよい．これは $t=1$ のとき，すなわち，$b-a\equiv d-c \pmod p$ のときも成立する．実際，$\mathbf{T}_{a,b}^{c,d}=g_{c-a}$ であり，$\mathbf{T}_{a,b}^{c,d}(g_a+g_b) = g_c+g_{b+c-a}=g_c+g_d$ となる．□

後述する定義 A.1.1 のとおり，$\mathbf{X}_{(a,b)}=x_a+x_b$ とする．

例 4.1　$\mathbf{G}_4$ を行基本変形で上三角行列に変形する．

$$\mathbf{G}_4^{(1)} = \begin{bmatrix} 1 & x_0 & x_0^2 & x_0^3\\ 0 & x_1+x_0 & x_1^2+x_0^2 & x_1^3+x_0^3\\ 0 & x_2+x_0 & x_2^2+x_0^2 & x_2^3+x_0^3\\ 0 & x_3+x_0 & x_3^2+x_0^2 & x_3^3+x_0^3 \end{bmatrix}$$

$$\mathbf{G}_4^{(2)} = \begin{bmatrix} 1 & x_0 & x_0^2 & x_0^3\\ 0 & \mathbf{X}_{(1,0)} & \mathbf{X}_{(1,0)}\mathbf{X}_{(1,0)} & \mathbf{X}_{(1,0)}a_1\\ 0 & 0 & \prod_{i=0}^{1}\mathbf{X}_{(2,i)} & \prod_{i=0}^{1}\mathbf{X}_{(2,i)}a_2\\ 0 & 0 & \prod_{i=0}^{1}\mathbf{X}_{(3,i)} & \prod_{i=0}^{1}\mathbf{X}_{(3,i)}a_3 \end{bmatrix}$$

$$\mathbf{G}_4^{(3)} = \begin{bmatrix} 1 & x_0 & x_0^2 & x_0^3\\ 0 & \mathbf{X}_{(1,0)} & \mathbf{X}_{(1,0)}\mathbf{X}_{(1,0)} & \mathbf{X}_{(1,0)}a_1\\ 0 & 0 & \prod_{i=0}^{1}\mathbf{X}_{(2,i)} & \prod_{i=0}^{1}\mathbf{X}_{(2,i)}a_2\\ 0 & 0 & 0 & \prod_{i=0}^{2}\mathbf{X}_{(3,i)} \end{bmatrix}$$

ここで，$a_1=x_1^2+x_1x_0+x_0^2, a_2=x_2+x_1+x_0, a_3=x_3+x_1+x_0$ である．また，$\mathbf{G}_4^{(1)}$ から $\mathbf{G}_4^{(2)}$，および $\mathbf{G}_4^{(2)}$ から $\mathbf{G}_4^{(3)}$ への変形では，定理 4.2 を利用している．□

例 4.1 で得られた $\mathbf{G}_4^{(3)}$ の階数は対角成分の階数の和となるが，対角成分の階数は定理 4.1 より求めることができる．

次に，一般化，すなわち $\mathbf{G}_k$ の行基本変形を考える．いくつか記号を定義する．

$$\mathbf{M}^{(t)} \stackrel{\text{def}}{=} \left[\mathbf{M}_{(i,j)}^{(t)}\right]_{i=t,\ j=t}^{k-1,k-1} \quad (t=1,\cdots,k-1),$$

$$\mathbf{G}_k \stackrel{\circ}{\to} \mathbf{G}_k^{(1)} = \left[\begin{array}{c|ccc} 1 & x_0 & \cdots & x_0^{k-1}\\ \hline 0 & \mathbf{M}_{(1,1)}^{(1)} & \cdots & \mathbf{M}_{(1,k-1)}^{(1)}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & \mathbf{M}_{(k-1,1)}^{(1)} & \cdots & \mathbf{M}_{(k-1,k-1)}^{(1)} \end{array}\right],$$

$$\mathbf{G}_k^{(1)} \stackrel{\circ}{\to} \cdots \stackrel{\circ}{\to} \mathbf{G}_k^{(t+1)} = \left[\begin{array}{ccc|ccc} 1 & x_0 & \cdots & & \cdots & x_0^{k-1}\\ & \mathbf{M}_{(1,1)}^{(1)} & \cdots & & \cdots & \mathbf{M}_{(1,k-1)}^{(1)}\\ & & \ddots & & & \vdots\\ & & & \mathbf{M}_{(t,t)}^{(t)} & \cdots & \mathbf{M}_{(t,k-1)}^{(t)}\\ \hline & \boldsymbol{O} & & & \mathbf{M}^{(t+1)} & \end{array}\right].$$

手順 4.1　$\mathbf{G}_k$ の行基本変形の手順を表す．

手順 1　0 行目を i 行目 $(i=1,\cdots,k-1)$ に加算する．

手順 2　定理 4.2 を用いて，m 行目に $\mathbf{T}_{m,0}^{i,0}\cdots\mathbf{T}_{m,m-1}^{i,m-1}$ を乗算したものを i 行目 $(i=m+1,\cdots,k-1)$ に加算する手順を $m=1,\cdots,k-2$ について繰り返す．すなわち，$\mathbf{M}_{(i,j)}^{(m+1)} = \mathbf{M}_{(i,j)}^{(m)} + \prod_{t=0}^{m-1}\mathbf{T}_{m,t}^{i,t}\mathbf{M}_{(m,j)}^{(m)}$ である．

定理 4.3　手順 4.1 で $\mathbf{G}_k$ を行基本変形し，$\mathbf{G}_k^{(k-1)}$ を得る．このとき，$m=1,\cdots,k-1$ について，$\mathbf{M}_{(m,m)}^{(m)} = \prod_{t=0}^{m-1}\mathbf{X}_{(m,t)}$ である．

証明は付録 A.1 に示す．

定理 4.4　行列 $\mathbf{G}_k$ の階数は $k(p-1)+1$ である．また，$\mathbf{M}^{(1)}$ の階数は $(k-1)(p-1)$ である．

証明　定理 4.3 で得られた $\mathbf{M}_{(m,m)}^{(m)}$ の階数を考える．定理 4.1 より，$1\leq m\leq k-1$ について，$\mathbf{M}_{(m,m)}^{(m)}$ の階数は $p-1$ である．よって，$\mathbf{M}^{(1)}$ の階数は $(k-1)(p-1)$ で，$\mathbf{G}_k$ の階数は $p+(k-1)(p-1)=k(p-1)+1$ である．□

5. (k,n) しきい値秘密分散法

秘密情報 $s\in\{0,1\}^{d(p-1)}$ を $s_0,\cdots,s_{p-2}\in\{0,1\}^d$ のブロックに等分割する．d はたとえば 8 や 64 である．ディーラは参加者 P_x $(x=0,\cdots,n-1)$ にシェア w_x を秘密裏に分散する．n が合成数なら，$p>n$ となる (k,p) しきい値法を用いてシェア $w_0,\cdots,w_{n-1}$ を秘密裏に分散する．ここで，ベクトル $\mathbf{w}_{(i)},\mathbf{s},\mathbf{r},\mathbf{e}$ を定義する．

- $\mathbf{w}_{(i)} = \left[w_{(i,0)},\cdots,w_{(i,p-2)}\right]^{\mathsf{T}}$
- $\mathbf{s} = (s_0,\cdots,s_{p-2})^{\mathsf{T}}$
- $\mathbf{r} = (r_0^0,\cdots,r_{p-2}^0,\cdots,r_0^{k-2},\cdots,r_{p-2}^{k-2})^{\mathsf{T}}$
- $\mathbf{e} = \begin{bmatrix}\mathbf{r}\\ \mathbf{s}\end{bmatrix}$

5.1　シェア生成

行列 $\mathbf{G}$ を構成する各 $p\times p$ 巡回行列の $p-1$ 行目と $p-1$

列目を削除した行列 $\bar{g}_i^j$ と $\bar{1}$ を考える．これらの行列で構成される行列 $\bar{\mathbf{G}}$ を用いて，$\mathbf{w} = \bar{\mathbf{G}} \cdot \mathbf{e}$ となる

$$\mathbf{w} = \begin{bmatrix} \mathbf{w}_{(0)} \\ \mathbf{w}_{(1)} \\ \vdots \\ \mathbf{w}_{(n-1)} \end{bmatrix} = \begin{bmatrix} \bar{1} & \bar{g}_0 & \bar{g}_0^2 & \cdots & \bar{g}_0^{k-1} \\ \bar{1} & \bar{g}_1 & \bar{g}_1^2 & \cdots & \bar{g}_1^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \bar{1} & \bar{g}_{n-1} & \bar{g}_{n-1}^2 & \cdots & \bar{g}_{n-1}^{k-1} \end{bmatrix} \mathbf{e}$$

を与える．表 1 は分散アルゴリズムである．[4], [5] との差分を下線で示す．Step 1 は秘密情報を等分割する．[4], [5] と添え字が異なる．Step 2 は $(k-1)(p-1)$ 個の d ビットの乱数を生成する．[4], [5] では，$(k-1)p-1$ であり，本研究の構成法は $r_{p-1}^i \leftarrow \{0\}^d$ とみなせる．Step 3 はシェアを生成する．(k,p) しきい値法に対応する一意に与えられるベクトル $\mathbf{v}_{(i,j)}$ を用いて $w_{(i,j)} = \mathbf{v}_{(i,j)} \cdot \mathbf{e}$ とみることができる．$k=3, p=5$ ならば，$\mathbf{v}_{(1,0)} = (1000\ 0100\ 0010)$ である．[4], [5] では，添え字と $i = 0, \cdots, n-1$ について $\bar{g}_i^{k-1}$ は $\bar{g}_i^{p-1}$ の差分がある．

表 1 分散アルゴリズム
Table 1 The distribution algorithm.

Input: $s \in \{0,1\}^{d(p-1)}$
Output: $(w_0, \cdots w_{n-1})$

1: $\underline{s_{p-1} \leftarrow \{0\}^d}, \underline{s_0 || \cdots || s_{p-2}} \leftarrow s$
2: for $i \leftarrow 0$ to $k-2$:
  for $j \leftarrow 0$ to $\underline{p-2}$:
    $r_j^i \xleftarrow{\$} \{0,1\}^d$
  $\underline{r_{p-1}^i \leftarrow \{0\}^d}$ (discard r_{p-1}^0)
3: for $i \leftarrow 0$ to $n-1$:
  for $j \leftarrow 0$ to $p-2$:
    $w_{(i,j)} \leftarrow \left(\bigoplus_{h=0}^{k-2} r_{h \cdot i+j}^h\right) \oplus s_{\underline{(k-1)\cdot i+j}}$
  $w_i \leftarrow w_{(i,0)} || \cdots || w_{(i,p-2)}$
4: return $(w_0, \cdots w_{n-1})$

5.2 復元

参加者 P_x $(x = t_0, \cdots, t_{k-1})$ が復元に協力し，$\bar{x}_0 = \bar{g}_{t_0}, \cdots, \bar{x}_{k-1} = \bar{g}_{t_{k-1}}$ とするとき，

$$\bar{\mathbf{G}}_k = \begin{bmatrix} \bar{1} & \bar{x}_0 & \cdots & \bar{x}_0^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{1} & \bar{x}_{k-1} & \cdots & \bar{x}_{k-1}^{k-1} \end{bmatrix}, \mathbf{w}_k = \begin{bmatrix} \mathbf{w}_{(t_0)} \\ \vdots \\ \mathbf{w}_{(t_{k-1})} \end{bmatrix}$$

を用いて，$\mathbf{e} = \bar{\mathbf{G}}_k^{-1} \mathbf{w}_k$ である．表 2 は復元アルゴリズムである．[4], [5] との差分を下線で示す．Step 1 で各シェアを d ビットに等分割する．Step 2 は $k(p-1)$ 次元ベクトル $\mathbf{w}_k$ を生成する．Step 3 で $\mathbf{M}$ を取得する．Step 4 で $\mathbf{M} \cdot \mathbf{w}_k$ を計算し $s_0, \cdots, s_{p-2}$ を復元する．Step 5 でそれらを連結し秘密情報 s を得る．Step F1 で $w_{(t_i,j)} = \mathbf{v}_{(t_i,j)} \cdot \mathbf{e}$ となるベクトル $\mathbf{v}_{(t_i,j)}$ を得る．Step F2 で $k(p-1) \times k(p-1)$ 行列 $\bar{\mathbf{G}}_k$ を得る．[4], [5] では，$k(p-1) \times (kp-2)$ 行列である．Step F3 は行列 $\left[\bar{\mathbf{G}}_k\ \mathbf{I}_{k(p-1)}\right]$ を階段行列 $[\mathbf{G}'\ \mathbf{J}]$ に変形する．$\mathbf{G}'$ と $\mathbf{J}$ はそれぞれ $\bar{\mathbf{G}}_k$ と $\mathbf{I}_{k(p-1)}$ に対応する．行列 $[\mathbf{G}'\ \mathbf{J}]$ は行列 $\boldsymbol{O}, \mathbf{G}'_0, \mathbf{G}'_1, \mathbf{G}'_2, \mathbf{J}_0, \mathbf{J}_1$ のブロックに分けて考える．Step F4 で行列 $[\mathbf{G}'_0\ \mathbf{J}_0]$ を行列 $[\mathbf{I}_{p-1}\ \mathbf{M}]$ に変形し，Step F5 で $(p-1) \times k(p-1)$ 行列 $\mathbf{M}$ を出力する．

表 2 復元アルゴリズム
Table 2 The recovery algorithm.

Input: $(w_{t_0}, \cdots, w_{t_{k-1}})$
Output: s

1: for $i \leftarrow 0$ to $k-1$:
  $w_{(t_i,0)} || \cdots || w_{(t_i,p-2)} \leftarrow w_{t_i}$
2: $\mathbf{w}_k \leftarrow (w_{(t_0,0)}, \cdots, w_{(t_0,p-2)}, \cdots, w_{(t_{k-1},0)}, \cdots, w_{(t_{k-1},p-2)})^\mathsf{T}$
3: $\mathbf{M} \leftarrow F_{MAT}(t_0, \cdots, t_{k-1})$
4: $(\underline{s_0, \cdots, s_{p-2}})^\mathsf{T} \leftarrow \mathbf{M} \cdot \mathbf{w}_k$
5: $s \leftarrow \underline{s_0 || \cdots || s_{p-2}}$
6: return s

$F_{MAT}(t_0, \cdots, t_{k-1})$

F1: for $i \leftarrow 0$ to $k-1$:
  for $j \leftarrow 0$ to $p-2$:
    $\mathbf{v}_{(t_i,j)} \leftarrow w_{(t_i,j)} = \mathbf{v}_{(t_i,j)} \cdot \mathbf{e}$
F2: $\underline{\bar{\mathbf{G}}_k} \leftarrow (\mathbf{v}_{(t_0,0)}, \cdots, \mathbf{v}_{(t_{k-1},p-2)})^\mathsf{T}$
F3: $\left[\begin{array}{ccc:c} \mathbf{G}'_2 & \mathbf{G}'_1 & \mathbf{J}_1 \\ \boldsymbol{O} & \mathbf{G}'_0 & \mathbf{J}_0 \end{array}\right] = [\mathbf{G}'\ \mathbf{J}] \xleftarrow{\circ} \left[\bar{\mathbf{G}}_k\ \mathbf{I}_{k(p-1)}\right]$
F4: $\left[\begin{array}{ccc:c} \mathbf{G}'_2 & \mathbf{G}'_1 & \mathbf{J}_1 \\ \boldsymbol{O} & \mathbf{I}_{p-1} & \mathbf{M} \end{array}\right] \xleftarrow{\circ} [\mathbf{G}'\ \mathbf{J}]$
F5: return $\mathbf{M}$

5.3 シェア生成と復元の例

$(3,5)$ しきい値法を考える．$\mathbf{w} = \bar{\mathbf{G}} \cdot \mathbf{e}$ から参加者 P_i のシェア $w_i = w_{(i,0)} || \cdots || w_{(i,3)}$ が生成される．すなわち，

$$\mathbf{w} = \begin{bmatrix} \underline{\mathbf{w}_{(0)}} \\ \underline{\mathbf{w}_{(1)}} \\ \underline{\mathbf{w}_{(2)}} \\ \underline{\mathbf{w}_{(3)}} \\ \mathbf{w}_{(4)} \end{bmatrix} = \begin{bmatrix} w_{(0,0)} \\ w_{(0,1)} \\ w_{(0,2)} \\ \underline{w_{(0,3)}} \\ w_{(1,0)} \\ w_{(1,1)} \\ w_{(1,2)} \\ \vdots \\ w_{(3,1)} \\ w_{(3,2)} \\ \underline{w_{(3,3)}} \\ w_{(4,0)} \\ w_{(4,1)} \\ w_{(4,2)} \\ w_{(4,3)} \end{bmatrix} = \begin{bmatrix} 1000\ 1000\ 1000 \\ 0100\ 0100\ 0100 \\ 0010\ 0010\ 0010 \\ \underline{0001\ 0001\ 0001} \\ 1000\ 0100\ 0010 \\ 0100\ 0010\ 0001 \\ 0010\ 0001\ 0000 \\ \vdots \\ 0100\ 0000\ 0010 \\ 0010\ 1000\ 0001 \\ \underline{0001\ 0100\ 0000} \\ 1000\ 0000\ 0001 \\ 0100\ 1000\ 0000 \\ 0010\ 0100\ 1000 \\ 0001\ 0010\ 0100 \end{bmatrix} \begin{bmatrix} r_0^0 \\ r_1^0 \\ r_2^0 \\ \underline{r_3^0} \\ r_0^1 \\ r_1^1 \\ r_2^1 \\ \underline{r_3^1} \\ s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}$$

である．P_0, P_3, P_4 が復元に協力するとき，

$$\left[\bar{\mathbf{G}}_3\ \mathbf{I}_{12}\right] =$$
$$\left[\begin{array}{cccc}
1000\ 1000\ 1000 & 1000\ 0000\ 0000 \\
0100\ 0100\ 0100 & 0100\ 0000\ 0000 \\
0010\ 0010\ 0010 & 0010\ 0000\ 0000 \\
0001\ 0001\ 0001 & 0001\ 0000\ 0000 \\
\hdashline
1000\ 0001\ 0100 & 0000\ 1000\ 0000 \\
0100\ 0000\ 0010 & 0000\ 0100\ 0000 \\
0010\ 1000\ 0001 & 0000\ 0010\ 0000 \\
0001\ 0100\ 0000 & 0000\ 0001\ 0000 \\
\hdashline
1000\ 0000\ 0001 & 0000\ 0000\ 1000 \\
0100\ 1000\ 0000 & 0000\ 0000\ 0100 \\
0010\ 0100\ 1000 & 0000\ 0000\ 0010 \\
0001\ 0010\ 0100 & 0000\ 0000\ 0001
\end{array}\right],$$

$$\left[\bar{\mathbf{G}}_3\ \mathbf{I}_{12}\right] \overset{\circ}{\rightarrow}$$
$$\left[\begin{array}{cccc}
1000\ 1000\ 1000 & 1000\ 0000\ 0000 \\
0100\ 0100\ 0100 & 0100\ 0000\ 0000 \\
0010\ 0010\ 0010 & 0010\ 0000\ 0000 \\
0001\ 0001\ 0001 & 0001\ 0000\ 0000 \\
\hdashline
0000\ 1001\ 1100 & 1000\ 1000\ 0000 \\
0000\ 0100\ 0110 & 0100\ 0100\ 0000 \\
0000\ 0011\ 1111 & 1010\ 1010\ 0000 \\
0000\ 0001\ 0111 & 0101\ 0101\ 0000 \\
\hdashline
0000\ 0000\ \underline{1000} & \underline{1110\ 0111\ 1001} \\
0000\ 0000\ \underline{0100} & \underline{1001\ 1011\ 0010} \\
0000\ 0000\ \underline{0010} & \underline{0101\ 1101\ 1000} \\
0000\ 0000\ \underline{0001} & \underline{0011\ 1110\ 1101}
\end{array}\right],$$

$$\mathbf{s} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 1110\ 0111\ 1001 \\ 1001\ 1011\ 0010 \\ 0101\ 1101\ 1000 \\ 0011\ 1110\ 1101 \end{bmatrix} \begin{bmatrix} \mathbf{w}_{(0)} \\ \mathbf{w}_{(3)} \\ \mathbf{w}_{(4)} \end{bmatrix}$$

で復元できる．

5.4 正当性と完全性

正当性を考える．5.2 節の $k(p-1)\times k(p-1)$ 行列 $\bar{\mathbf{G}}_k$ について，0 行目を i 行目 $(i=1,\cdots,k-1)$ に加算すると，

$$\bar{\mathbf{G}}_k \overset{\circ}{\rightarrow} \bar{\mathbf{G}}_k^{(1)} = \left[\begin{array}{c|ccc} \bar{1} & \bar{x}_0 & \cdots & \bar{x}_0^{k-1} \\ \hline 0 & \bar{\mathbf{M}}_{(1,1)}^{(\bar{1})} & \cdots & \bar{\mathbf{M}}_{(1,k-1)}^{(\bar{1})} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \bar{\mathbf{M}}_{(k-1,1)}^{(1)} & \cdots & \bar{\mathbf{M}}_{(k-1,k-1)}^{(1)} \end{array}\right],$$

$$\bar{\mathbf{M}}^{(1)} = \begin{bmatrix} \bar{x}_1+\bar{x}_0 & \cdots & \bar{x}_1^{k-1}+\bar{x}_0^{k-1} \\ \vdots & \ddots & \vdots \\ \bar{x}_{k-1}+\bar{x}_0 & \cdots & \bar{x}_{k-1}^{k-1}+\bar{x}_0^{k-1} \end{bmatrix}$$

を得る．$(k-1)(p-1)\times(k-1)(p-1)$ 行列 $\bar{\mathbf{M}}^{(1)}$ を考える．$\bar{\mathbf{M}}_{(i,j)}^{(1)}$ の 0 行目から $p-2$ 行目の和を $p-2$ 行目の直後に追加する．列も同様に追加する．すると，$\bar{\mathbf{M}}^{(1)}$ は $\mathbf{M}^{(1)}$ に変形できる．この操作は補題 2.1 より，線形従属な行や列を追加しているだけなので，階数は変わらない．定理 4.4 より，$\bar{\mathbf{M}}^{(1)}$ の階数は $\mathbf{M}^{(1)}$ の階数と同じ $(k-1)(p-1)$ である．したがって，$\bar{\mathbf{G}}_k$ の階数は $k(p-1)$ であり，$\bar{\mathbf{G}}_k$ は逆行列を持つので，正当性を満たす．

完全性を考える．$1\le L\le k-1$ とする．L 人の参加者 P_x $(x=t_0,\cdots,t_{L-1})$ が復元に協力するとき，秘密情報に関する情報は全く得られないことを示す．5.2 節を参考に，$\mathbf{w}_L=\bar{\mathbf{G}}_L\cdot\mathbf{e}$ である．$\mathbf{s}$ の要素と $\mathbf{r}$ の要素が互いに独立していて，$\mathbf{r}$ の要素は一様な確率 $1/2^d$ の有限集合 $\{0,1\}^d$ から選択されると仮定する．ここで，

$$\mathbf{w}_L = \bar{\mathbf{G}}_L\begin{bmatrix}\mathbf{r}\\ \mathbf{s}\end{bmatrix} = \bar{\mathbf{G}}_L\begin{bmatrix}\mathbf{r}\\ 0\end{bmatrix} + \bar{\mathbf{G}}_L\begin{bmatrix}0\\ \mathbf{s}\end{bmatrix} = \bar{\mathbf{U}}\cdot\mathbf{r}+\bar{\mathbf{V}}\cdot\mathbf{s}$$

となる $\bar{\mathbf{G}}_L=[\bar{\mathbf{U}}\ \bar{\mathbf{V}}]$ を考える．$\bar{\mathbf{U}}$ のすべての行は線形独立であるから，$\bar{\mathbf{U}}\cdot\mathbf{r}$ のすべての要素は互いに独立であり $\{0,1\}^d$ 上の一様分布の d ビット乱数である．したがって，$\bar{\mathbf{U}}\cdot\mathbf{r}$ は $\{0,1\}^{dL(p-1)}$ 上の一様分布である．次に，$\mathbf{w}'$ が固定値 $\mathbf{w}_L$ を表すと仮定したとき，$\mathbf{w}_L=\mathbf{w}'$ となる $\mathbf{w}_L$ が任意の $\bar{\mathbf{V}}\cdot\mathbf{s}$ から一様な確率 $(1/2)^{dL(p-1)}$ で取得できる．$\mathbf{s}$ は $\mathbf{w}_L$ と独立しているので，秘密情報に関する情報は全く得られない．

表 3 測定環境
Table 3 Test environment.

CPU	Intel ® Celeron ® Processor G1820
	2.70GHz × 2, 2MB cache
RAM	3.6GB
OS	CentOS 7 Linux 3.10.0-229.20.1.el7.x86_64
言語	C 言語
コンパイラ	gcc 4.8.3 (-O3 -flto -DNDEBUG)

6. ソフトウェア実装

いくつかの k,n を与えて実装を行い，例として 888,710 バイトのファイルを復元する実験を行った．測定環境は表 3 の汎用 PC の環境 1 台を準備した．

表 4 に実験結果を示す．$d=64$ を使用した．乱数生成は Xorshift を使用し，分散速度は乱数生成の時間を含む．各速度は 30 回計測した平均値である．分散について，n が小さいとき，本研究の構成法は [4], [5] の手法に比べて速いことが確認できた．分散について，復元に協力する参加者と行基本変形によって得られる $\mathbf{M}$ に含まれる XOR 演算の個数に依存するため，処理速度の有意な違いはなかった．

7. おわりに

(k,n) しきい値秘密分散法 [3], [4], [5] と (k,L,n) ランプ型秘密分散法 [6] の $L=1$ の場合を参考に，XOR ベース

表 4　実験結果

Table 4　Experimental results.

(k,n)	分散速度（Mbps）		復元速度（Mbps）	
	本研究	[4]	本研究	[4]
(3, 5)	1553.63	1262.45	7640.79	7678.44
(3, 11)	113.29	104.12	1747.30	1733.62
(3, 43)	11.14	11.00	209.30	201.18
(4, 5)	1116.33	664.57	4531.31	4409.23
(5, 7)	311.96	274.85	1885.87	1672.97

(k,n) しきい値秘密分散法の新しい証明法を提供した．n が小さいとき，シェア生成は [4], [5] の手法に比べて効率的であることが実測で確認できた．

謝辞　本研究の一部は JSPS 科研費 JP18K11306 の助成を受けたものである．

参考文献

[1] Blakley, G.R.: Safeguarding cryptographic keys, *AFIPS*, Vol.48, pp.313–317 (1979).

[2] Shamir, A.: How to share a secret, *Commun. ACM*, Vol.22, No.11, pp.612–613 (1979).

[3] 藤井吉弘，栃窪孝也，保坂範和，多田美奈子，加藤岳久：排他的論理和を用いた (k,n) しきい値法の構成法，*IEICE Technical Report*, ISEC 2007-5 (2007).

[4] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T.: On a Fast (k,n)-Threshold Secret Sharing Scheme, *IEICE Trans. Fundamentals*, Vol.E91-A, No.9, pp.2365–2378 (2008).

[5] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T.: A New (k,n)-Threshold Secret Sharing Scheme and Its Extension, *ISC 2008*, LNCS 5222, pp.455–470 (2008).

[6] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T.: A Fast (k,L,n)-Threshold Ramp Secret Sharing Scheme, *IEICE Trans. Fundamentals*, Vol.E92-A, No.8, pp.1808–1821 (2009).

[7] Kurihara, J. and Uyematsu, T.: A Novel Realization of Threshold Schemes over Binary Field Extensions, *IEICE Trans. Fundamentals*, Vol.E94-A, No.6, pp.1375–1380 (2011).

[8] Shima, K. and Doi, H.: A Hierarchical Secret Sharing Scheme over Finite Fields of Characteristic 2, *Journal of Information Processing*, Vol.25, pp.875–883 (2017).

[9] 五十嵐大, 露崎浩太, 川原祐人: SHSS: オブジェクトストレージ向けの超高速秘密分散ライブラリ, 情報処理学会, 第 70 回 CSEC 研究会 (2015).

[10] Beimel, A.: Secret-Sharing Schemes, A Survey, *IWCC 2011*, LNCS 6639, pp.11–46 (2011).

[11] Blundo, C., De Santis, A., Gargano, L. and Vaccaro, U.: On the information rate of secret sharing schemes, *TCS*, Vol.154, pp.283–306 (1996).

[12] Blundo, C., De Santis, A., Gargano, L. and Vaccaro, U.: On the Information Rate of Secret Sharing Schemes, *Advances in Cryptology - CRYPTO '92*, LNCS 740, pp.149–169 (1993).

[13] Ingleton, A.W.: The Rank of Circulant Matrices, *Journal of the London Mathematical Society*, Vol.1, No.4, pp.445–460 (1956).

[14] Fabšič, T., Hromada, V., Stankovski, P., Zajac, P., Guo, Q. and Johansson, T.: A Reaction Attack on the QC-LDPC McEliece Cryptosystem, *International Workshop on Post-Quantum Cryptography*, LNCS 10346, pp.51–68 (2017).

[15] Cohen, H.: A Course in Computational Algebraic Number Theory, Graduate texts in mathematics 138, Springer (1996).

付　　録

A.1　定理 4.3 の証明

定義 A.1.1　$m \geq 0$ とする．

- $\mathbf{X}^m_{(a,b)} \stackrel{\text{def}}{=} x_a^m + x_b^m$
- $\mathbf{H}^m_{(a,b)} \stackrel{\text{def}}{=} \sum_{i=0}^m x_a^i x_b^{m-i}$ (斉次多項式)
- $\mathbf{A}^m_{(a,b,c)} \stackrel{\text{def}}{=} \mathbf{H}^m_{(a,c)} + \mathbf{H}^m_{(b,c)}$
- $\bar{\mathbf{A}}^m_{(a,b,c)} \stackrel{\text{def}}{=} \sum_{i=0}^m x_c^i \mathbf{H}^{m-i}_{(a,b)}$
- $\bar{\bar{\mathbf{A}}}^m_{(a,b,c,d)} \stackrel{\text{def}}{=} \bar{\mathbf{A}}^m_{(a,c,d)} + \bar{\mathbf{A}}^m_{(b,c,d)}$

定義 A.1.1 より，$\mathbf{X}^m_{(a,b)} = \mathbf{X}_{(a,b)}\mathbf{H}^{m-1}_{(a,b)}$，$\mathbf{H}^0_{(a,b)} = 1$，$\bar{\mathbf{A}}^0_{(a,b,c)} = 1$ である．

定義 A.1.2　$t(u) = \sum_{i=-1}^u t_i$，$t_{-1} = 0$ とする．

- $\bar{\mathbf{S}}^{(m)}_{(b)} \stackrel{\text{def}}{=} \prod_{u=0}^{m-3} (\sum_{t_u=0}^{b-m-t(u-1)} x_u^{t_u})$
- $\mathbf{S}^{(m)}_{(a,b)} \stackrel{\text{def}}{=} \begin{cases} \bar{\mathbf{S}}^{(m)}_{(b)} \bar{\mathbf{A}}^{b-m-t(m-3)}_{(a,m-1,m-2)} & (m \geq 3) \\ \bar{\mathbf{A}}^{b-2}_{(a,1,0)} & (m = 2) \end{cases}$
- $\mathbf{B}^{(m)}_{(a,b,c)} \stackrel{\text{def}}{=} \mathbf{S}^{(m)}_{(a,c)} + \mathbf{S}^{(m)}_{(b,c)} \quad (m \geq 2)$

たとえば，

$$\begin{aligned} \mathbf{S}^{(4)}_{(a,b)} &= \sum_{t_0=0}^{b-4-t(-1)} x_0^{t_0} \sum_{t_1=0}^{b-4-t(0)} x_1^{t_1} \bar{\mathbf{A}}^{b-4-t(1)}_{(a,3,2)} \\ &= \sum_{t_0=0}^{b-4} x_0^{t_0} \sum_{t_1=0}^{b-4-t_0} x_1^{t_1} \bar{\mathbf{A}}^{b-4-t_0-t_1}_{(a,3,2)} \end{aligned}$$

である．また，定義 A.1.2 より，常に $\mathbf{S}^{(m)}_{(m,m)} = 1$ である．

補題 A.1.1　定義 A.1.1 から，次の等式を満たす．

$$\mathbf{A}^m_{(a,b,c)} = \begin{cases} \mathbf{X}_{(a,b)} \bar{\mathbf{A}}^{m-1}_{(a,b,c)} & (m \geq 1) \\ 0 & (m = 0) \end{cases},$$

$$\bar{\bar{\mathbf{A}}}^m_{(a,b,c,d)} = \begin{cases} \mathbf{X}_{(a,b)} \sum_{i=0}^{m-1} x_d^i \bar{\mathbf{A}}^{m-1-i}_{(a,b,c)} & (m \geq 1) \\ 0 & (m = 0) \end{cases}$$

証明　定義より，$\mathbf{A}^0_{(a,b,c)} = 0$，$\bar{\bar{\mathbf{A}}}^0_{(a,b,c,d)} = 0$ である．次に，$m \geq 1$ のとき，

$$\begin{aligned} \mathbf{A}^m_{(a,b,c)} &= \mathbf{X}^m_{(a,b)} + \mathbf{H}^m_{(a,c)} + x_a^m + \mathbf{H}^m_{(b,c)} + x_b^m \\ &= \mathbf{X}^m_{(a,b)} + x_c(\mathbf{H}^{m-1}_{(a,c)} + \mathbf{H}^{m-1}_{(b,c)}) \\ &= \mathbf{X}^m_{(a,b)} + x_c \mathbf{A}^{m-1}_{(a,b,c)} \\ &= \mathbf{X}_{(a,b)}\mathbf{H}^{m-1}_{(a,b)} + x_c(\mathbf{X}_{(a,b)}\mathbf{H}^{m-2}_{(a,b)} + \\ &\quad x_c(\cdots + x_c \mathbf{X}_{(a,b)}) \cdots) \end{aligned}$$

$$= \mathbf{X}_{(a,b)} \sum_{i=0}^{m-1} x_c^i \mathbf{H}_{(a,b)}^{m-1-i}$$
$$= \mathbf{X}_{(a,b)} \bar{\mathbf{A}}_{(a,b,c)}^{m-1}$$

である．また，$\mathbf{A}_{(a,b,c)}^0 = 0$ であるから $m \geq 1$ のとき，

$$\begin{aligned}
\bar{\bar{\mathbf{A}}}_{(a,b,c,d)}^{m} &= \bar{\mathbf{A}}_{(a,c,d)}^{m} + \bar{\mathbf{A}}_{(b,c,d)}^{m} \\
&= \sum_{i=0}^{m} x_d^i (\mathbf{H}_{(a,c)}^{m-i} + \mathbf{H}_{(b,c)}^{m-i}) \\
&= \sum_{i=0}^{m} x_d^i \mathbf{A}_{(a,b,c)}^{m-i} \\
&= \sum_{i=0}^{m-1} x_d^i \mathbf{A}_{(a,b,c)}^{m-i} \\
&= \mathbf{X}_{(a,b)} \sum_{i=0}^{m-1} x_d^i \bar{\mathbf{A}}_{(a,b,c)}^{m-1-i}
\end{aligned}$$

である． □

定理 A.1.1 $m \geq 2$ のとき，次の等式を満たす．

$$\mathbf{B}_{(a,m,c)}^{(m)} = \mathbf{X}_{(a,m)} \mathbf{S}_{(a,c)}^{(m+1)}$$

証明 $m \geq 3$ のとき，

$$\bar{\bar{\mathbf{S}}}_{(c)}^{(m)} \stackrel{\text{def}}{=} \prod_{u=0}^{m-3} \Big(\sum_{t_u=0}^{c-(m+1)-t(u-1)} x_u^{t_u} \Big)$$

と定義すると，

$$\begin{aligned}
\mathbf{B}_{(a,b,c)}^{(m)} &= \mathbf{S}_{(a,c)}^{(m)} + \mathbf{S}_{(b,c)}^{(m)} \\
&= \bar{\mathbf{S}}_{(c)}^{(m)} (\bar{\mathbf{A}}_{(a,m-1,m-2)}^{c-m-t(m-3)} + \bar{\mathbf{A}}_{(b,m-1,m-2)}^{c-m-t(m-3)}) \\
&= \bar{\mathbf{S}}_{(c)}^{(m)} \bar{\bar{\mathbf{A}}}_{(a,b,m-1,m-2)}^{c-m-t(m-3)} \\
&= \prod_{u=0}^{m-3} \Big(\sum_{t_u=0}^{c-m-t(u-1)} x_u^{t_u} \Big) \bar{\bar{\mathbf{A}}}_{(a,b,m-1,m-2)}^{c-m-t(m-3)} \\
&= \bar{\bar{\mathbf{S}}}_{(c)}^{(m)} \bar{\bar{\mathbf{A}}}_{(a,b,m-1,m-2)}^{c-m-t(m-3)}
\end{aligned}$$

である．ここで，$\bar{\mathbf{S}}_{(c)}^{(m)}$ から $\bar{\bar{\mathbf{S}}}_{(c)}^{(m)}$ への変形を考える．たとえば，$m = 3$ の場合，$\mathbf{B}_{(a,b,c)}^{(3)} = \sum_{t_0=0}^{c-3} x_0^{t_0} \bar{\bar{\mathbf{A}}}_{(a,b,2,1)}^{c-3-t_0}$ である．$t_0 = c-3$ のとき，$\bar{\bar{\mathbf{A}}}_{(a,b,2,1)}^{0} = 0$ であるから，$\mathbf{B}_{(a,b,c)}^{(3)} = \sum_{t_0=0}^{c-4} x_0^{t_0} \bar{\bar{\mathbf{A}}}_{(a,b,2,1)}^{c-3-t_0}$ と考えてよい．一般的に，$\bar{\mathbf{S}}_{(c)}^{(m)}$ は $x_0^{t_0} x_1^{t_1} \cdots x_{m-3}^{t_{m-3}}$ と $\bar{\bar{\mathbf{A}}}_{(a,b,m-1,m-2)}^{c-m-t(m-3)}$ の乗算を行うが，$t(m-3) = c-m$ のとき，$\bar{\bar{\mathbf{A}}}_{(a,b,c,d)}^{0} = 0$ であるから，$\bar{\bar{\mathbf{S}}}_{(c)}^{(m)}$ に変形できる．次に，$b = m$ を考える．$m' = c-(m+1)-t(m-3)$ と置くと，補題 A.1.1 を使って，

$$\begin{aligned}
\mathbf{B}_{(a,m,c)}^{(m)} &= \mathbf{X}_{(a,m)} \bar{\bar{\mathbf{S}}}_{(c)}^{(m)} \sum_{i=0}^{m'} x_{m-2}^i \bar{\mathbf{A}}_{(a,m,m-1)}^{m'-i} \\
&= \mathbf{X}_{(a,m)} \prod_{u=0}^{m-2} \Big(\sum_{t_u=0}^{c-(m+1)-t(u-1)} x_u^{t_u} \Big) \bar{\mathbf{A}}_{(a,m,m-1)}^{c-(m+1)-t(m-2)} \\
&= \mathbf{X}_{(a,m)} \mathbf{S}_{(a,c)}^{(m+1)}
\end{aligned}$$

である．この式は $m = 2$ のときも成立する．すなわち，

$$\begin{aligned}
\mathbf{B}_{(a,2,c)}^{(2)} &= \mathbf{X}_{(a,2)} \mathbf{S}_{(a,c)}^{(3)} \\
&= \mathbf{X}_{(a,2)} \sum_{t_0=0}^{c-3} x_0^{t_0} \bar{\mathbf{A}}_{(a,2,1)}^{c-3-t_0} \\
&= \bar{\bar{\mathbf{A}}}_{(a,2,1,0)}^{c-2}
\end{aligned}$$

であるが，定義 A.1.2 より $\mathbf{B}_{(a,b,c)}^{(2)} = \mathbf{S}_{(a,c)}^{(2)} + \mathbf{S}_{(b,c)}^{(2)} = \bar{\mathbf{A}}_{(a,1,0)}^{c-2} + \bar{\mathbf{A}}_{(b,1,0)}^{c-2} = \bar{\bar{\mathbf{A}}}_{(a,b,1,0)}^{c-2}$ である． □

これらの結果を用いて，定理 4.3 の証明を与える．

証明 $m = 1$ のとき，$\mathbf{M}_{(i,j)}^{(1)} = \mathbf{X}_{(i,0)}^j$ であるから，定理を満たす．$m = 2, \cdots, k-1$ を考える．

$$\begin{aligned}
\mathbf{M}_{(i,j)}^{(m)} &= \mathbf{M}_{(i,j)}^{(m-1)} + \prod_{t=0}^{m-2} \mathbf{T}_{m-1,t}^{i,t} \mathbf{M}_{(m-1,j)}^{(m-1)} \\
&= \prod_{t=0}^{m-1} \mathbf{X}_{(i,t)} \mathbf{S}_{(i,j)}^{(m)} \qquad \text{(A.1)}
\end{aligned}$$

が成立するならば，定義 A.1.2 より $\mathbf{S}_{(m,m)}^{(m)} = 1$ であるから，$m = 2, \cdots, k-1$ についても定理を満たす．そこで，式 (A.1) を数学的帰納法で証明する．$i, j \in \{2, \cdots, k-1\}$ について，

$$\begin{aligned}
\mathbf{M}_{(i,j)}^{(2)} &= \mathbf{M}_{(i,j)}^{(1)} + \mathbf{T}_{1,0}^{i,0} \mathbf{M}_{(1,j)}^{(1)} \\
&= \mathbf{X}_{(i,0)}^j + \mathbf{T}_{1,0}^{i,0} \mathbf{X}_{(1,0)}^j \\
&= \mathbf{X}_{(i,0)} (\mathbf{H}_{(i,0)}^{j-1} + \mathbf{H}_{(1,0)}^{j-1}) \\
&= \mathbf{X}_{(i,0)} \mathbf{A}_{(i,1,0)}^{j-1} \\
&= \mathbf{X}_{(i,0)} \mathbf{X}_{(i,1)} \bar{\mathbf{A}}_{(i,1,0)}^{j-2} \\
&= \prod_{t=0}^{1} \mathbf{X}_{(i,t)} \mathbf{S}_{(i,j)}^{(2)}
\end{aligned}$$

であるから，$m = 2$ のとき，式 (A.1) を満たす．$i, j \in \{m, \cdots, k-1\}$ について，式 (A.1) が成立すると仮定すると，定義 A.1.2，定理 A.1.1 より，

$$\begin{aligned}
\mathbf{M}_{(i,j)}^{(m+1)} &= \mathbf{M}_{(i,j)}^{(m)} + \prod_{t=0}^{m-1} \mathbf{T}_{m,t}^{i,t} \mathbf{M}_{(m,j)}^{(m)} \\
&= \prod_{t=0}^{m-1} \mathbf{X}_{(i,t)} \mathbf{B}_{(i,m,j)}^{(m)} \\
&= \prod_{t=0}^{m} \mathbf{X}_{(i,t)} \mathbf{S}_{(i,j)}^{(m+1)}
\end{aligned}$$

が得られる．したがって，式 (A.1) を証明できた． □