標数 2 の有限体上の一般的な階層に適用可能な階層的秘密分散法の研究

島 幸司[†1]　土井 洋[†1]

概要：参加者をレベルに分割し，そのレベルで分割された参加者のグループ間で秘密を共有する階層的秘密分散法が知られている．著者らは秘密分散後の秘密消去の容易性，すなわち，秘密情報の削除が必須参加者のシェアの削除で保証されることを狙いに階層的秘密分散法に着目し，導関数と Birkhoff 補間を使った Tassa のアイデアを継承しつつ，標数 2 の有限体上への適用が可能な$(\{1,k\},n)$階層的秘密分散法を CSEC72 で提案した．本稿では，Birkhoff 補間と標数 2 の有限体上の導関数を工夫することで，一般的な階層に適用可能かつ高速な階層的秘密分散法を提案し，その実装評価を報告する．

キーワード：秘密分散法，階層的秘密分散法，導関数，Birkhoff 補間，標数 2 の有限体

A study on hierarchical secret sharing schemes applicable to any level over finite fields of characteristic 2

Koji Shima[†1]　Hiroshi Doi[†1]

Abstract: Some of hierarchical secret sharing schemes are known in the way that the secret is shared among a group of participants that is partitioned into levels. We look at hierarchical secret sharing schemes in the purpose of the ease of deleting the secret after it is distributed, that is, the reliability of data deletion depends on the deletion of the shares of the indispensable participants. In CSEC72, we proposed a $(\{1,k\},n)$ hierarchical secret sharing scheme applying to finite fields of characteristic 2 through Tassa's idea of using derivatives and Birkhoff interpolation. In this paper, we devise a method for Birkhoff interpolation and derivatives over finite fields of characteristic 2, and propose a fast hierarchical secret sharing scheme applicable to any level with the implementation evaluation.

Keywords: Secret sharing scheme, hierarchical secret sharing scheme, derivative, Birkhoff interpolation, finite fields of characteristic 2

1. はじめに

秘密情報の安全な保管は情報の盗難対策や紛失対策に見られるように情報化社会においてニーズが高い．この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を分散管理するため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．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，$k-1$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という特徴がある．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，かつ，シェアの一部が紛失しても元の秘密情報を復元できる．

一方で，参加者をレベルに分割し，そのレベルで分割された参加者のグループ間で秘密を共有する階層的秘密分散法が知られている．その中で，金庫を開けるには 3 人の従業員が必要で，少なくとも 1 人は部長といったシナリオに見られるように，最小限の高いレベルの参加者が必要とされる秘密分散法がある．Tassa [3][4]は導関数を導入し，Birkhoff 補間問題に注力している．

この階層的秘密分散法は秘密情報の復元に必須参加者を必要とするため，秘密消去の容易性を狙える．すなわち，秘密情報の削除が必須参加者のシェアの削除で保証されるからである．たとえば，実用上の想定として，緊急性によるデータ消去の保証やデータ消去の確実性について，必須参加者のシェアの削除を拠り所にできることである．そこで，2015 年に著者ら[5]は高速化を見据え，Tassa の導関数利用のアイデアを標数 2 の有限体上に適用した$(\{1,3\},n)$階層的秘密分散法の実現性を述べ，2016 年に著者ら[6]は標数 2 の有限体上の$(\{1,k\},n)$階層的秘密分散法を提案した．また，著者ら[5]は藤井らの排他的倫理和演算のみを用いた$(2,n)$しきい値法をベースにした階層的秘密分散法のアイデアを述べ，2016 年に著者ら[7]は排他的論理和をベースに必須参加者数を限定した$(\{1,3\},n)$階層的秘密分散法を提案した．

†1 情報セキュリティ大学院大学
Institute of Information Security

1.1 秘密分散法の高速化

Shamir の(k,n)しきい値法は$k \leq n$を満たす任意のkとnに対して実現可能であるが，秘密情報の分散および復元において，$k-1$次多項式を処理する必要があるため，計算コストが大きい. 2005 年に藤井ら[8]は排他的倫理和演算のみを用いて秘密情報の分散および復元を行うことができる$(2,n)$しきい値法を提案した．2008 年に栗原ら[9]は排他的論理和演算のみを用いた$(3,n)$しきい値法を提案し，nがあまり大きくなければ，Shamir のしきい値法と比較して非常に効率の良い計算コストが得られた．同年に栗原ら[10]は排他的論理和演算のみを用いた(k,n)しきい値法を提案し，nがあまり大きくなければ，Shamir のしきい値法と比較して，より効率の良い計算コストが得られることを，$(k,n)=(4,5)$を例に示している．また，同年に栗原ら[11]はその拡張として，シェアのサイズを小さくするランプ型（*ramp*）秘密分散法[12]に対して, 拡張手法の要約を紹介し, 2009 年に高速なランプ型秘密分散法を提案した[13]. さらに, 2011 年に栗原ら[14]は GF(2^n)上の乗算コストが加算の排他的倫理和演算の処理コストに対して大きいことを踏まえ，Feng ら[15], Blömer ら[16]の有限体の行列表現の定理を用いて，GF(q)上の行列ベクトルの下で GF(q^n) 上の行列表現の要素とベクトル表現の要素の乗算を考察し，行列とベクトルの乗算が GF(2)の加算と乗算で実装できることを示し高速化に貢献した．なお，ほかの排他的論理和を用いた秘密分散法として，松尾ら[17]の技術が知られている．また，須賀[18] 柯ら[19] 尾崎ら[20] の研究もなされている．

1.2 本研究の貢献

本研究では，高速化と秘密消去の容易性に着目する．すなわち，秘密分散法とその周辺の課題の中で，ビッグデータに向けた性能向上の必要性が求められる背景から高速化に着目する．また，秘密情報の分散後において，(k,n)秘密分散法では, 秘密情報の削除が$n-k$個より多くのシェアの削除で保証されるが，階層的秘密分散法では，秘密情報の削除が必須参加者のシェアの削除で保証される. このため，秘密消去の容易性を狙うシナリオに階層的秘密分散法は適した手法と言える.

これらの着眼点から，導関数を用いた Tassa のアイデアを継承しつつ, 標数 2 の有限体上の$(\mathbf{k},n)$階層的秘密分散法を提案する．詳細は 3.2 節で述べるが，標数 2 の有限体の場合，$k \geq 2$とするk階導関数の結果は常に 0 になるため，そのままでは有意なシェアを生成できない．そこで，導関数を工夫することで，この問題を解決しつつ，Birkhoff 補間を適用できるようにする. この$(\mathbf{k},n)$階層的秘密分散法から，実運用上で有益と考えられるレベルの高い権限者が少なくとも 1 名を満たす$(\{1,k\},n)$階層的秘密分散法（$\mathbf{k}=\{1,k\}$）を実現することが可能であり，著者ら[6]の標数 2 の有限体上の$(\{1,k\},n)$階層的秘密分散法の効果が得られる.

2. 準備

2.1 完全秘密分散法

Beimel [21]は文献の定義 2 と定義 3 において，完全秘密分散法は次の条件を必要とすることを示している.

- [正当性] アクセス構造の中に属する権限を持つすべての集合Bは秘密に関する情報を得る.
- [完全性] アクセス構造の外に属する権限を持たないすべての集合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] $H(S|S_T)=H(S)$

2.2 理想的秘密分散法

Blundo ら[22][23]，栗原ら[9][10]の文献から，n人の参加者集合を$P=\{P_1,\dots,P_n\}$，秘密情報として可能性のある集合をS, 参加者P_iのシェアとして可能性のある集合をW_iとする秘密分散法が与えられたとき，その情報率を$\rho=\frac{H(S)}{\max_{P_i \in P} H(W_i)}$と定義する．$S$と$W_i$がどちらも一様な確率分布に従うとき，$\rho=\frac{\log_2|S|}{\max_{P_i \in P}\log_2|W_i|}$を測定できることが知られており，$\rho=1$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. また, 階層的秘密分散法においても, Tassa [4]と同じように言い換えることができる.

3. 関連研究

Tassa [3][4]は最小限の高いレベルの参加者が必要とされる$\mathbf{k}=\{k_i\}_{i=0}^{m}$，$0<k_0<\cdots<k_m$とする$(\mathbf{k},n)$階層的秘密分散法を次のアクセス構造$\Gamma$を用いて定義する.

$$\mathcal{U}=\bigcup_{i=0}^{m}\mathcal{U}_i,\ \mathcal{U}_i\cap\mathcal{U}_j=\emptyset,\ 0\leq i<j\leq m,$$
$$\Gamma=\left\{\mathcal{V}\subset\mathcal{U}:\left|\mathcal{V}\cap\left(\bigcup_{j=0}^{i}\mathcal{U}_j\right)\right|\geq k_i,\ \forall i\in\{0,1,\dots,m\}\right\} \quad (1)$$

$\mathcal{U}$をn人の参加者集合とするとき，階層レベルiの参加者集合$\mathcal{U}_i$と表現したm階層を考え, アクセス構造Γを満たすよ

うに各参加者$u \in \mathcal{U}$にシェアを割り当てる．たとえば，$\mathbf{k} = \{1,3\}$とすれば，2 階層で構成され，$\mathcal{U}_0$の必須参加者は 1 人以上，復元に 3 人以上の協力が必要な$(\{1,3\}, n)$階層的秘密分散法を意味する．

Tassa の実現方式は低いレベルの参加者だけでは秘密情報は復元できず，かつ理想的秘密分散法である．Shamir の(k,n)しきい値法と同じように，大きな有限体上の$k-1$次多項式$p(x)$の定数を秘密情報とする．kは最大しきい値k_mを用いて，$k = k_m$とする．各参加者$u \in \mathcal{U}$は同じuと表現される有限体上の識別子が与えられ，自身の階層の位置に依存する何らかのj階導関数値$p^{(j)}(u)$をシェアとして受け取る．より重要な参加者はより小さいi番目の参加者集合$\mathcal{U}_i$に所属し，より低いj階導関数を用いたシェアを得る．導関数を適切に選ぶことで，階層的秘密分散法の要求するアクセス構造を満たし，権限を持つ部分集合が協力して秘密情報の復元を試みる．

一方で，別の階層的な設定が研究されている．Shamir [2]はより重要な参加者にはより多くのシェアを与えることで階層的秘密分散法の達成を提案している．しかし，Tassa が指摘するように，Shamir の手法は参加者の部分集合の中で表現されるそれぞれのレベルで関係づけられたしきい値の加重平均で決まるため，低いレベルの参加者の部分集合が十分に大きいときは，低いレベルの参加者のみで秘密情報を復元できてしまう課題がある．また，Simmons [24]と Brickell [25]はそれぞれ Tassa とは別の階層的な設定を検討しているが，必要な参加者が各レベルに関連付けられるしきい値の中の最大値で決まるため，最小限の高いレベルの参加者が必要とされるシナリオは実現できない．

ここで, Tassa がどのように導関数値を用いて階層化を実現しているか，$\mathbf{k} = \{2,4,7\}$とする$(\{2,4,7\}, n)$階層的秘密分散法を例に述べる．最大しきい値は$k = 7$であるから，ディーラは定数項を秘密情報とした 6 次多項式$p(x)$をランダムに選択する．最上位の参加者$u \in \mathcal{U}_0$は$p(u)$，参加者$u \in \mathcal{U}_1$は$k_0 = 2$であるから$p''(u)$，参加者$u \in \mathcal{U}_2$は$k_1 = 4$であるから$p^{(4)}(u)$のそれぞれのシェアを得る．

3.1 多項式補間

秘密情報の復元で連立方程式を解く代わりに多項式補間を利用すると，計算量削減により高速化に貢献する．しかし，シェアに導関数値が含まれると，Lagrange 補間や Newton 補間では秘密情報を復元できない．Hermite 補間は導関数値を含めた補間手法として知られているが，シェア$p'(x_1)$と同時に$p(x_1)$の値もシェアとして与えられる必要があるため，シェア配布の観点で制限が入る．Birkhoff 補間はこの制限を解消しうる．

(1) Birkhoff 補間

$G = \{g_0, g_1, \dots, g_N\}$を線形独立な$[\mathrm{a},\mathrm{b}]$で$n$回連続微分可能な$\mathbb{R}$上の関数列とし，線形結合$P = \sum_{k=0}^{N} a_k g_k, a_k \in \mathbb{R}$を$G$の多項式と呼ぶ．次式の$m \times (n+1)$補間行列

$$E = \left[e_{i,j}\right]_{i=1,j=0}^{m \quad n}, \qquad m \geq 1,\ n \geq 0,$$

は要素$e_{i,j}$が 0 または 1 であり，かつ，$\sum e_{i,j} = N+1$である．ただし，Eは空行を含まない．すなわち，すべての$j = 0, \dots n$に対して，$e_{i,j} = 0$となる行iは含まないとする．

今，$[\mathrm{a},\mathrm{b}]$で$x_1 < \cdots < x_m$とするm個の異なる点の集合$X = \{x_1, \dots, x_m\}$が与えられているとする．Birkhoff 補間問題[26][27]とは，$\langle E, X, G\rangle$の組と与えられたデータ$c_{i,j}$により，次の条件を満たす多項式pを見つけることである．

$$p^{(j)}(x_i) = c_{i,j}, \quad e_{i,j} = 1 \tag{2}$$

式(2)は$N+1$個の等式からなる．次の行列式が 0 以外のときに限り，$\langle E, X, G\rangle$の組が$c_{i,j}$の各集合に対して唯一の解を持つ．

$$D(E,X,G) = \det[g_0^{(j)}(x_i), \dots, g_N^{(j)}(x_i); e_{i,j} = 1] \tag{3}$$

式(3)は$(N+1) \times (N+1)$行列式の一行だけを示している．すなわち，$e_{i,j} = 1$の(i,j)の組に対応した行を示している．また，行の並びは$i < i'$または$i = i', j < j'$のときに(i,j)が(i',j')より先に並ぶ辞書的な順番とする．この$(N+1) \times (N+1)$行列を$A(E,X,G)$と表現すると，$D(E,X,G)$は次式で表せる．

$$D(E,X,G) = \det\big(A(E,X,G)\big) = |A(E,X,G)|$$

データ$c_{i,j}$が$c_{i,j} = p^{(j)}(x_i)$で与えられたとき，補間多項式は次式で与えられる．

$$p(x) = \sum_{j=0}^{N} \frac{D\big(E,X,G_j\big)}{D(E,X,G)} \cdot g_j(x) \tag{4}$$

G_jはGのg_jをpに置き換えた関数の集合で，たとえば，$G_1 = \{g_0, p, g_2, \dots, g_N\}$である．

(2) Birkhoff 補間の具体例

$g_0(x) = 1, g_1(x) = x, g_2(x) = x^2$において，すなわち，$G = \{1, x, x^2\}$において，次のように$X$と$E$が与えられたとする．

$$X = \{1,2,3\}, \qquad E = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

言い換えれば，次の値を満たす多項式$p(x) = \sum_{j=0}^{2} a_j x^j$を

探すことである．

$$p(1)=c_{1,0},\qquad p(2)=c_{2,0},\qquad p'(3)=c_{3,1}$$

具体的に$p(1)=15,\ p(2)=29,\ p'(3)=23$が与えられたとすると，次の多項式$p(x)$を得る．

$$D(E,X,G)=\begin{vmatrix} g_0(x_1) & g_1(x_1) & g_2(x_1)\\ g_0(x_2) & g_1(x_2) & g_2(x_2)\\ g_0'(x_3) & g_1'(x_3) & g_2'(x_3)\end{vmatrix}=\begin{vmatrix}1&1&1\\1&2&4\\0&1&6\end{vmatrix}=3,$$

$$D(E,X,G_0)=\begin{vmatrix} p(x_1) & g_1(x_1) & g_2(x_1)\\ p(x_2) & g_1(x_2) & g_2(x_2)\\ p'(x_3) & g_1'(x_3) & g_2'(x_3)\end{vmatrix}=\begin{vmatrix}15&1&1\\29&2&4\\23&1&6\end{vmatrix}=21,$$

$$D(E,X,G_1)=\begin{vmatrix} g_0(x_1) & p(x_1) & g_2(x_1)\\ g_0(x_2) & p(x_2) & g_2(x_2)\\ g_0'(x_3) & p'(x_3) & g_2'(x_3)\end{vmatrix}=\begin{vmatrix}1&15&1\\1&29&4\\0&23&6\end{vmatrix}=15,$$

$$D(E,X,G_2)=\begin{vmatrix} g_0(x_1) & g_1(x_1) & p(x_1)\\ g_0(x_2) & g_1(x_2) & p(x_2)\\ g_0'(x_3) & g_1'(x_3) & p'(x_3)\end{vmatrix}=\begin{vmatrix}1&1&15\\1&2&29\\0&1&23\end{vmatrix}=9,$$

$$p(x)=\sum_{j=0}^{2}\frac{D(E,X,G_j)}{D(E,X,G)}\cdot g_j(x)=7+5x+3x^2$$

十分大きい素数pにおいて，$p(x)=3x^2+5x+7 \mod p$でシェアが分散される階層的秘密分散法を考える．シェア$p(1)=15,\ p(2)=29,\ p'(3)=23$が集まると，秘密情報は次式で計算できる．

$$s=p(0)=\frac{D(E,X,G_0)}{D(E,X,G)}=\frac{21}{3}=7$$

3.2 著者らの$(\{1,k\},n)$階層的秘密分散法の課題

文献[6]より，標数 2 の拡大体上で微分すると，次数が偶数の項の結果は消えてしまう事実から，$k-1$個の変数を持つ多項式$p(x)$をランダムに選択し，$G=\{g_0,g_1,\dots,g_k\}$を

$$g_0(x)=1,\ g_1(x)=x,\ g_2(x)=x^3,\dots,g_{k-1}(x)=x^{2(k-2)+1},$$

と奇数次のみの項となるように設定する．具体的には，多項式$p(x)$と$p'(x)$は次の通りである．

$$p(x)=\sum_{i=1}^{k-1}a_i x^{2(i-1)+1}+s\in \mathrm{GF}(2^L)[x]$$

$$p'(x)=\sum_{i=1}^{k-1}a_i x^{2(i-1)}\in \mathrm{GF}(2^L)[x]$$

秘密情報の復元は Birkhoff 補間を適用することで標数 2 の有限体上の$(\{1,k\},n)$階層的秘密分散法を実現する．しかしながら，$k_0<k_1$とする$(\{k_0,k_1\},n)$階層的秘密分散法への一般化を考えると，k_0階導関数を必要とし，標数 2 の有限体上では次数が偶数の項の結果は消えてしまう事実からうまく実現できない．

4. 提案方式

n人の参加者集合$\mathcal{U}$をm階層のレベルに分け，$\mathbf{k}=\{k_i\}_{i=0}^{m}$とする標数 2 の有限体上の$(\mathbf{k},n)$階層的秘密分散法を提案する．アクセス構造は(1)と同じ定義である．

4.1 一般化の考察

3.2 節で示した課題を解決し，$(\mathbf{k},n)$階層的秘密分散法に一般化する．ここで，$(\{k_0,k\},n)$階層的秘密分散法を考えると，k_0階導関数を必要とすることから，標数 2 の有限体上の演算では，$k_0\geq 2$とするk_0階導関数は常に 0 になる．このため，k_0階導関数においても意味のある多項式が与えられるかが課題になる．そこで，導関数を用いる必要性を考察した．階層化を満たす視点において，与えられた関数の微分操作を繰り返すたび，その時の定数項が消えるルールは重要であるが，導関数の定義から導かれる

$$f^{(n)}(x)=\begin{cases}\displaystyle\sum_{i=0}^{k-1-n} {}_{i+n}\mathrm{P}_n\cdot a_{i+n}x^i & (k-1\geq n)\\ 0 & (k-1<n)\end{cases},a_0=s,$$

$${}_n\mathrm{P}_r=\frac{n!}{(n-r)!}=n(n-1)\cdots(n-r+1)$$

を用いて階層化する必要性はないと考えた．そこで，$k-1$次多項式$f(x)$のn階導関数$f^{(n)}(x)$は用いずに，$k-1$次多項式$f(x)$の次数をn回下げた関数$f^{[n]}(x)\in \mathrm{GF}(2^L)[x]$を定義し，

$$f^{[n]}(x)=\begin{cases}\displaystyle\sum_{i=0}^{k-1-n} a_{i+n}x^i & (k-1\geq n)\\ 0 & (k-1<n)\end{cases},a_0=s \qquad (5)$$

この関数をn階関数と呼ぶことにして階層化の実現に用いる．具体例として，$f(x)=3x^2+5x+7$に対する$f^{[1]}(x)=3x+5$であり，$f^{[2]}(x)=3$である．

4.2 $f^{[n]}(x)$を用いた場合の Birkhoff 補間の適用

関数$f^{[n]}(x)$を用いた階層的秘密分散を提案するために，Birkhoff 補間による復元を見据えた 2 つの補題を導入する．

補題 1：$n\times n$行列$F=\begin{bmatrix}a(1,1) & \cdots & a(1,n)\\ \vdots & \ddots & \vdots\\ a(n,1) & \cdots & a(n,n)\end{bmatrix}$が与えられたと

き，任意の$1 \le i \le n$，$1 \le k \le n$に対して，次式を満たす．

$$\sum_{j=1}^{n}(-1)^{i+j}\left|\tilde{F}(i,j)\right|a(k,j)=\begin{cases}|F| & (k=i)\\ 0 & (k\neq i)\end{cases} \qquad (6)$$

ここで，$\tilde{F}(i,j)$は行列Fからi行目とj列目を除いた$(n-1)\times(n-1)$行列の余因子行列とする．

証明：任意の$1 \le i \le n$から一つのiが選択されたとき，$k=i$となるkと$k\neq i$となるkのそれぞれについて，式(6)が成立するか証明する．

$k=i$のとき，行列式の性質から，左辺は$|F|$のi行目を余因子展開したものであり，等式(6)を満たす．

$k\neq i$のとき，左辺はその全体の符号を無視すると，i行目が$[a(k,1),\cdots,a(k,n)]$, $l(\neq i)$行目が$[a(l,1),\cdots,a(l,n)]$となる行列

$$F=\begin{bmatrix}a(1,1) & \cdots & a(1,n)\\ \vdots & & \vdots\\ a(k,1) & \cdots & a(k,n)\\ \vdots & & \vdots\\ a(n,1) & \cdots & a(n,n)\end{bmatrix}\begin{matrix}1\text{ 行目}\\ \vdots\\ i\text{行目}\\ \vdots\\ n\text{行目}\end{matrix}$$

の行列式を余因子展開したものになる．ところが，$k(\neq i)$行目も$[a(k,1),\cdots,a(k,n)]$である．よって，二つの行が一致するから，行列式の値は0であり，等式(6)を満たす．　□

補題 2：$n\times n$行列$FQ(j)$を行列Fのj列目を$\begin{bmatrix}q(1)\\ \vdots\\ q(n)\end{bmatrix}$で置き換えたものとする．

$$FQ(j)=\begin{bmatrix}a(1,1) & \cdots & q(1) & \cdots & a(1,n)\\ \vdots & & \vdots & & \vdots\\ a(n,1) & \cdots & q(n) & \cdots & a(n,n)\end{bmatrix}$$

任意の$1 \le k \le n$に対して，次式を満たす．

$$\sum_{j=1}^{n}|FQ(j)|a(k,j)=q(k)\times|F| \qquad (7)$$

証明：$|FQ(j)|$について，j列目を余因子展開すると，

$$\sum_{i=1}^{n}(-1)^{i+j}\left|\tilde{F}(i,j)\right|q(i)$$

である．等式(7)の左辺は最後に補題 1 を用いて次のように展開できる．

$$\begin{aligned}\sum_{j=1}^{n}|FQ(j)|a(k,j)&=\sum_{j=1}^{n}\sum_{i=1}^{n}(-1)^{i+j}\left|\tilde{F}(i,j)\right|q(i)\,a(k,j)\\ &=\sum_{i=1}^{n}\sum_{j=1}^{n}(-1)^{i+j}\left|\tilde{F}(i,j)\right|q(i)\,a(k,j)\\ &=\sum_{i=1}^{n}q(i)\sum_{j=1}^{n}(-1)^{i+j}\left|\tilde{F}(i,j)\right|a(k,j)\\ &=q(k)\times|F|\end{aligned}$$

よって，補題 2 が証明された．　□

定理 1：

n階導関数$f^{(n)}(x)$の代わりにn階関数$f^{[n]}(x)$を利用しても Birkhoff 補間の式(4)は成り立つ．

証明：補題 2 を用いて Birkhoff 補間を満たすか証明する．以下，$D(E,X,G)\neq 0$とする．満たすべきは

$$p(x)\cdot D(E,X,G)=\sum_{j=0}^{N}D\left(E,X,G_j\right)\cdot g_j(x) \qquad (8)$$

である．$\mathbf{k}=\{k_i\}_{i=0}^{m}$の$(\mathbf{k},n)$階層的秘密分散法では，$N=k_m-1$であり，$x=x_1$, …, x_{k_m}について式(8)を満たす必要がある．一般性を失うことなく，$1,\ldots,k_0$番目が最上位階層$\mathcal{U}_0$の参加者，$k_0+1,\ldots,k_1$番目が階層$\mathcal{U}_1$の参加者と順番に階層$\mathcal{U}_m$まで参加者を割り当てると，補題 2 の$q(i)$と Birkhoff 補間に渡す秘密情報のシェアとの関係を次のように設定することができる．

$$\begin{gathered}q(1)=p(x_1),\cdots,q(k_0)=p\left(x_{k_0}\right),\\ q(k_0+1)=p^{(k_0)}\left(x_{k_0+1}\right),\cdots,q(k_1)=p^{(k_0)}\left(x_{k_1}\right),\\ \cdots\\ q(k_{m-1}+1)=p^{(k_{m-1})}\left(x_{k_{m-1}+1}\right),\cdots,q(k_m)=p^{(k_{m-1})}\left(x_{k_m}\right)\end{gathered}$$

また，$k_m\times k_m$行列Fを以下のようにおく．ただし，j(=1,…, k_m)列目だけを示している．

$$F=\begin{bmatrix}a(1,j)\\ \vdots\\ a(k_0,j)\\ a(k_0+1,j)\\ \vdots\\ a(k_1,j)\\ \vdots\\ a(k_{m-1}+1,j)\\ \vdots\\ a(k_m,j)\end{bmatrix}=\begin{bmatrix}g_{j-1}(x_1)\\ \vdots\\ g_{j-1}\left(x_{k_0}\right)\\ g_{j-1}^{(k_0)}\left(x_{k_0+1}\right)\\ \vdots\\ g_{j-1}^{(k_0)}\left(x_{k_1}\right)\\ \vdots\\ g_{j-1}^{(k_{m-1})}\left(x_{k_{m-1}+1}\right)\\ \vdots\\ g_{j-1}^{(k_{m-1})}\left(x_{k_m}\right)\end{bmatrix}$$

すると，$D(E,X,G)$は行列Fであり，$D(E,X,G_j)$も$j=0,\ldots,k_m-1$とする$FQ(j+1)$である．$x=x_1,\ldots,x_{k_m}$に対応するkは$k=1,\ldots,k_m$であることに注意すると，

$$\sum_{j=0}^{N=k_m-1} D(E,X,G_j)\cdot g_j(x)=\sum_{j=1}^{k_m}|FQ(j)|\cdot a(k,j)$$
$$=q(k)\times|F|=p(x)\cdot D(E,X,G)$$

であり，補題 2 を用いて Birkhoff 補間が有効に働くことが確認できた．□

定理 1 から，秘密情報のシェアが導関数の定義から導かれる値である必要性がないことを意味し，微分を前提とした数値演算が行われないn階関数$f^{[n]}(x)$を用いることができる．

4.3 分散と復元

アクセス構造(1)を満たす$\mathbf{k}=\{k_i\}_{i=0}^m$, $0<k_0<\cdots<k_m$とする$(\mathbf{k},n)$階層的秘密分散法の分散と復元を述べる．秘密情報の復元に必要な全体の参加者数は$k=k_m$である．

(1) 分散アルゴリズム

ディーラは次のランダムな多項式$p(x)\in \mathrm{GF}(2^L)[x]$を選択する．

$$p(x)=\sum_{i=0}^{k-1}a_i x^i\in \mathrm{GF}(2^L)[x],\qquad a_0=s \tag{9}$$

ディーラは参加者$u\in\mathcal{U}$について, $\mathrm{GF}(2^L)$の要素で識別子を与える．簡単に$u\in\mathcal{U}$に対応する識別子もuと表現する．

ディーラは参加者$u\in\mathcal{U}_i$に$p^{[k_{i-1}]}(u)$のシェアを秘密裏に配布する．この手順をすべての参加者に対して行う．ここで，$k_{-1}=0$とし，$p^{[n]}(x)$は(5)の定義である．

例として，$k_0=3,k_1=4,k_2=6$とする$(\{3,4,6\},n)$階層的秘密分散法を考える．$k=k_2=6$であるから, ディーラはランダムな 5 次多項式$p(x)$を選択し, 定数項を秘密情報sとする．ここでは，$p(x)=\sum_{i=1}^5 a_i x^i+s\in \mathrm{GF}(2^L)[x]$が選択されたとする．参加者$u\in\mathcal{U}_0$は$p(u)$，参加者$u\in\mathcal{U}_1$は$p^{[3]}(u)=\sum_{i=0}^2 a_{i+3}u^i$，参加者$u\in\mathcal{U}_2$は$p^{[4]}(u)=\sum_{i=0}^1 a_{i+4}u^i$のシェアをそれぞれ受け取る．

(2) 復元アルゴリズム

アクセス構造(1)を満たすk人が復元に協力する．n階関数$p^{[n]}(x)$のシェアを含み，定理 1 と Birkhoff 補間を用いて次のように秘密情報sを復元できる．

$$s=p(0)=\frac{D(E,X,G_0)}{D(E,X,G)}$$

例として，$k_0=3,k_1=4,k_2=6$とする$(\{3,4,6\},n)$階層的秘密分散法を考える．表 1 のように，$\mathcal{U}_0$から 3 人，$\mathcal{U}_0\cup\mathcal{U}_1$から 5 人, 全体から 6 人の参加者が復元に協力する. なお, $(\{3,4,6\},n)$階層的秘密分散法においては, $\mathcal{U}_0\cup\mathcal{U}_1$からは 4 人以上の参加者が協力すればよい.

表 1　復元のための参加者とそのシェア
Table 1　Participants and the shares for recovery.

参加者	シェア
$u_1\in\mathcal{U}_0$	$p(u_1)$
$u_2\in\mathcal{U}_0$	$p(u_2)$
$u_3\in\mathcal{U}_0$	$p(u_3)$
$u_4\in\mathcal{U}_1$	$p^{[3]}(u_4)$
$u_5\in\mathcal{U}_1$	$p^{[3]}(u_5)$
$u_6\in\mathcal{U}_2$	$p^{[4]}(u_6)$

次の$D(E,X,G)$と$D(E,X,G_0)$で秘密情報を復元できる．

$$D(E,X,G_0)=\begin{vmatrix} p(u_1) & u_1 & u_1^2 & u_1^3 & u_1^4 & u_1^5\\ p(u_2) & u_2 & u_2^2 & u_2^3 & u_2^4 & u_2^5\\ p(u_3) & u_3 & u_3^2 & u_3^3 & u_3^4 & u_3^5\\ p^{[3]}(u_4) & 0 & 0 & 1 & u_4 & u_4^2\\ p^{[3]}(u_5) & 0 & 0 & 1 & u_5 & u_5^2\\ p^{[4]}(u_6) & 0 & 0 & 0 & 1 & u_6 \end{vmatrix},$$

$$D(E,X,G)=\begin{vmatrix} 1 & u_1 & u_1^2 & u_1^3 & u_1^4 & u_1^5\\ 1 & u_2 & u_2^2 & u_2^3 & u_2^4 & u_2^5\\ 1 & u_3 & u_3^2 & u_3^3 & u_3^4 & u_3^5\\ 0 & 0 & 0 & 1 & u_4 & u_4^2\\ 0 & 0 & 0 & 1 & u_5 & u_5^2\\ 0 & 0 & 0 & 0 & 1 & u_6 \end{vmatrix}$$

4.4 安全性

$\mathbf{k}=\{k_i\}_{i=0}^m$の$(\mathbf{k},n)$階層的秘密分散法において，2.1 節の完全性を満たすか考察する．$k=k_m$とする．

Tassa [4]の定理 3.2 を用いる．アクセス構造Γにおいて，$\mathcal{V}\in\Gamma$が$|\mathcal{V}|=k$となる最小限の権限を持つすべての部分集合であると仮定するとき，その対応する正方行列$M_{\mathcal{V}}$は$\det(M_{\mathcal{V}})\neq 0$であり，このとき完全性を満たすという．

ここで, $M_{\mathcal{V}}$は復元に協力する参加者のシェアを生成する行列にあたるが，この定理を提案手法に適用し完全性を証明する．このため，$M_{\mathcal{V}}$に着目して差分を詳しく述べる．

$\mathcal{V}=\{v_1,\ldots,v_{|\mathcal{V}|}\}\subset\mathcal{U}=\cup_{i=0}^m\mathcal{U}_i$とする. $0\le l_0\le\cdots\le l_m=|\mathcal{V}|$において，次の参加者の割り当てを仮定する．

$$v_1,\cdots,v_{l_0}\in\mathcal{U}_0,$$
$$v_{l_0+1},\cdots,v_{l_1}\in\mathcal{U}_1,$$
$$\vdots$$
$$v_{l_{m-1}+1},\cdots,v_{l_m}\in\mathcal{U}_m$$

すべての$0 \le i \le m$について，$l_i \ge k_i$のときに限り$\mathcal{V}$はアクセス構造(1)を満たす．4.3 節によるシェアの配布は式(9)の$p(x)$の係数ベクトル$\mathbf{a} = (s, a_1, \ldots, a_{k-1})^T$と参加者$u \in \mathcal{U}_i$のシェア$\sigma(u)$を用いて次のように表せる．

$$\sigma(u) = \mathbf{r}^{(k_{i-1})}(u) \cdot \mathbf{a}$$

ここで，$\mathbf{r}(x) = (1, x, x^2, \ldots, x^{k-1})$と定義し，$i \ge 0$に対して$\mathbf{r}^{(i)}(x)$は$\mathbf{r}(x)$ベクトルの定義式(5)による$i$階関数を表す．たとえば，$\mathbf{r}^{(1)}(x) = (0, 1, x, \ldots, x^{k-2})$である．Tassa の定理 3.2 では$\mathbf{r}(x)$ベクトルの$i$階導関数であり，この点が提案方式の差分である．

秘密情報sの復元に協力する参加者$v_1, \ldots v_{l_m}$のシェアを用いて，$\boldsymbol{\sigma} = (\sigma(v_1), \ldots, \sigma(v_{l_m}))^T$とすると，$\boldsymbol{\sigma} = M_{\mathcal{V}} \cdot \mathbf{a}$となる未知のベクトル$\mathbf{a}$を解く必要がある．すなわち，

$$\begin{pmatrix} \sigma(v_1) \\ \vdots \\ \sigma(v_{l_m}) \end{pmatrix} = M_{\mathcal{V}} \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix}, M_{\mathcal{V}} = \begin{pmatrix} \mathbf{r}(v_1) \\ \vdots \\ \mathbf{r}(v_{l_0}) \\ \mathbf{r}^{(k_0)}(v_{l_0+1}) \\ \vdots \\ \mathbf{r}^{(k_0)}(v_{l_1}) \\ \cdots \\ \mathbf{r}^{(k_{m-1})}(v_{l_{m-1}+1}) \\ \vdots \\ \mathbf{r}^{(k_{m-1})}(v_{l_m}) \end{pmatrix}$$

から秘密情報sを求めることになる．この議論を通して，n階導関数$f^{(n)}(x)$の代わりにn階関数$f^{[n]}(x)$を利用しても矛盾はなく定理 3.2 を利用することができ，$\det(M_{\mathcal{V}}) \neq 0$が完全性の証明の根拠になる．

5. 実装評価

$\mathbf{k} = \{k_i\}_{i=0}^{m}$の$(\mathbf{k}, n)$階層的秘密分散法について，いくつかの$\mathbf{k}$を与えて実装を行い，888710 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 2 の汎用 PC の環境 1 台を準備した．

表 2　測定環境

Table 2　Test environment.

CPU	Intel® Celeron® CPU G1820 @ 2.70GHz×2
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)

性能に関連する gcc オプションを測定環境に示している．$\mathrm{GF}(2^L)$の演算について，L =8, 16, 32 でそれぞれLビットレジスタ長演算，L = 64, 128, 256 でそれぞれ 64 ビットレジスタ演算を用いた．また，加算は排他的論理和，乗算は Russian Peasant Multiplication アルゴリズム，除算は$x^{-1} = x^{2^L-2}$，シフト演算は左に 1 シフトする演算である．しかしながら，乗算や除算はLの値によらず計算コストが高いことがわかっているため[6]，本実験では，$\mathrm{GF}(2^8)$の使用に限定し，かつ$\mathrm{GF}(2^8)$の乗除算を事前計算するルックアップテーブル方式を用いた．具体的には，乗算の結果を2^{16}バイト分の配列に，除算の結果を2^{16}バイト分の配列にそれぞれ格納し，乗除算の計算が発生すればその配列を参照する．また，秘密情報を計算するときに必要な$D(E, X, G)$と$D(E, X, G_0)$の行列式は三角行列を求めた後，行列の対角線を乗算している．実験結果を表 3 に示す．

表 3　実験結果

Table 3　The results of the experiment.

階層$\mathbf{k}$	シェア/復元速度
{1,3}	$p(7)$ $p^{[1]}(14)$ $p^{[1]}(17)$ 100.92Mbps
	$p(2)$ $p(3)$ $p^{[1]}(8)$ 97.07Mbps
{2,4}	$p(6)$ $p(7)$ $p^{[2]}(14)$ $p^{[2]}(17)$ 63.19Mbps
	$p(1)$ $p(2)$ $p(3)$ $p^{[2]}(8)$ 59.79Mbps
{2,3,5}	$p(6)$ $p(7)$ $p^{[2]}(14)$ $p^{[3]}(24)$ $p^{[3]}(27)$ 35.40Mbps
	$p(1)$ $p(2)$ $p(3)$ $p^{[2]}(8)$ $p^{[3]}(27)$ 34.84Mbps
{2,4,6,10}	$p(6)$ $p(7)$ $p^{[2]}(14)$ $p^{[2]}(17)$ $p^{[4]}(24)$ $p^{[4]}(27)$ $p^{[6]}(34)$ $p^{[6]}(35)$ $p^{[6]}(37)$ $p^{[6]}(39)$ 7.84Mbps
	$p(1)$ $p(2)$ $p(3)$ $p^{[2]}(8)$ $p^{[2]}(9)$ $p^{[4]}(24)$ $p^{[4]}(27)$ $p^{[6]}(34)$ $p^{[6]}(37)$ $p^{[6]}(39)$ 7.57Mbps
{3,7,11,14,17}	$p(5)$ $p(6)$ $p(7)$ $p^{[3]}(14)$ $p^{[3]}(15)$ $p^{[3]}(17)$ $p^{[3]}(19)$ $p^{[7]}(24)$ $p^{[7]}(25)$ $p^{[7]}(27)$ $p^{[7]}(29)$ $p^{[11]}(34)$ $p^{[11]}(37)$ $p^{[11]}(39)$ $p^{[14]}(44)$ $p^{[14]}(47)$ $p^{[14]}(49)$ 1.62Mbps
	$p(1)$ $p(2)$ $p(3)$ $p(5)$ $p^{[3]}(8)$ $p^{[3]}(9)$ $p^{[3]}(14)$ $p^{[3]}(17)$ $p^{[7]}(24)$ $p^{[7]}(25)$ $p^{[7]}(27)$ $p^{[7]}(29)$ $p^{[11]}(34)$ $p^{[11]}(37)$ $p^{[11]}(39)$ $p^{[14]}(44)$ $p^{[14]}(47)$ 1.53Mbps

参加者nを 60 とする$(\{1,3\},n)$階層的秘密分散法において，約 97Mbps の結果が得られた．しかしながら，最適化が施された$k=3$とする$\mathrm{GF}(2^8)$上の$(\{1,k\},n)$階層的秘密分散法[6]の復元速度 970Mbps の 10%程度である．これは行列式の計算が汎用的な$k\times k$行列式を求める実装による理由である．本実装を$(\{1,k\},n)$階層的秘密分散法に限定して最適化を行うと，同様の高速な復元速度が得られる．

5.1 参加者の識別子の割り当て

秘密情報の復元において，$D(E,X,G)$の除算が必要で，唯一の解を持つためには$D(E,X,G)\neq 0$である必要がある．Tassa も文献[4]の 3.2 節で$D(E,X,G)=0$となる確率について評価している．本論文では，n階関数$f^{[n]}(x)$を用いた場合に$D(E,X,G)=0$がどれくらい存在するか実験し評価した．$\mathrm{GF}(2^8)$上の$(\{1,3\},255)$階層的秘密分散法において，必須参加者 1 人を含む 2,731,135=$({}_{255}\mathrm{C}_3)$通りの復元の組み合わせの中で$D(E,X,G)=0$は存在しない．一方，必須参加者 2 人を含む 2,731,135 通りの復元の組み合わせの中で約 0.40%にあたる 10795 個の$D(E,X,G)=0$が存在する．これはおよそ$1/2^8$の割合である．$\mathrm{GF}(2^{16})$を用いると，およそ$1/2^{16}$の割合であることが実験から確認できた．なお，$\mathrm{GF}(2^L)$の演算で用いた原始多項式は表 4 のとおりである．

表 4　原始多項式

Table 4　Primitive polynomials.

拡大体	原始多項式
$\mathrm{GF}(2^8)$	$x^8+x^4+x^3+x+1$
$\mathrm{GF}(2^{16})$	$x^{16}+x^{12}+x^3+x+1$

6. おわりに

高速化と秘密消去の容易性に着目し，標数 2 の有限体上の$(\mathbf{k},n)$階層的秘密分散法を提案した．秘密情報の分散後における秘密情報の削除が必須参加者のシェアの削除で保証される高速な$(\{1,k\},n)$階層的秘密分散法の一般化を与えている．任意の階層で実験できる実装の下，すなわち，特定の階層に利用を限定した最適化を含まない実装の下，汎用 PC を用いた実装評価により，$\mathbf{k}=\{1,3\}$の復元で，97Mbps 程度の処理で実現できることを確認した．安全性に関して詳細の証明を与えることは今後の課題である．

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] Tassa, T.: Hierarchical Threshold Secret Sharing, *TCC 2004*, LNCS 2951, pp.473-490 (2004).

[4] Tassa, T.: Hierarchical Threshold Secret Sharing, *Journal of Cryptology*, Vol.20, No.2, pp.237-264 (2007).

[5] 島幸司，土井洋：階層的秘密分散法の高速化に関する研究，*CSS2015*，3C4-5，pp.1327-1334 (2015).

[6] 島幸司，土井洋：標数 2 の有限体上の({1,k},n)階層的秘密分散法の研究，情報処理学会研究報告，第 72 回 CSEC 研究会 (2016).

[7] Shima K., Doi H.: ({1,3},n) hierarchical secret sharing scheme based on XOR operations for a small number of indispensable participants, *AsiaJCIS 2016* (2016).

[8] 藤井吉弘，多田美奈子，保坂範和，栃窪孝也，加藤岳久：高速な(2, n)閾値法の構成法とシステムへの応用，*CSS2005*，8C-2，pp.631-636 (2005).

[9] Kurihara J., Kiyomoto S., Fukushima K., Tanaka T.: A Fast (3,n) -Threshold Secret Sharing Scheme Using Exclusive-OR Operations, *IEICE Trans. Fundamentals*, Vol.E91-A, No.1, pp.127-138 (2008).

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

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

[12] 山本博資：(k,L,n)しきい値秘密分散システム，電子通信学会論文誌，Vol.J68-A，No.9，pp.945-952 (1985).

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

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

[15] Feng G. -L., Deng R. -H., Bao F.: Packet-loss resilient coding scheme with only XOR operations: *IEE Proc. Communications*, Vol.151, No.4 (2004).

[16] Blömer J., Kalfane M., Karp R., Karpinski M., Luby M., Zuckerman D.: An XOR-Based Erasure-Resilient Coding Scheme, *ICSI Technical Report TR-95-048* (1995).

[17] 松尾正克，武藤浩二：排他的論理和を用いた(k,n)しきい値秘密分散法，*Panasonic Technical Journal*，Vol.59，No.2 (2013).

[18] 須賀祐治：排他的論理和を用いた(k,n)閾値秘密分散法の新しい構成とその優位性について，*CSS2012*，pp.185-192 (2012).

[19] 柯陳毓トウ，穴田啓晃，川本淳平，モロゾフキリル，櫻井幸一：複数プロバイダに亘る分散ストレージのためのグループ横断秘密分散法，*SCIS2016*，3A1-3 (2016).

[20] 尾崎寛之，櫻井幸一：秘密分散に関するもう一つの安全性問題 --不公正暗号システム・再訪--，*SCIS2016*，3A1-5 (2016).

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

[22] 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).

[23] Blundo C., De Santis A., Gargano L., and Vaccaro U.: On the Information Rate of Secret Sharing Schemes, *CRYPTO 1992*, LNCS, Vol.740, pp.149-169 (1993).

[24] Simmons G. J.: How to (really) share a secret, *Advances in Cryptology - CRYPTO '88*, LNCS 403, pp.390-448 (1990).

[25] Brickell E. F.: Some ideal secret sharing schemes, *Advances in Cryptology - EUROCRYPT '89*, LNCS 434, pp.468-475 (1990).

[26] Lorentz G. G., Jetter K., Riemenschneider S. D.: Birkhoff Interpolation, Encyclopedia of Mathematics and its Applications 19 (1983, 1984).

[27] Lorentz G. G. and Zeller K. L.: Birkhoff Interpolation, *SIAM Journal on Numerical Analysis*, Vol.8, No.1, pp.43-48 (1971).