ISSN 2186-5647

2-1

シェアの再配布なしにしきい値を削減可能な階層型秘密分散法

日大生産工(院)　○相澤 直樹　　日大生産工　栃窪 孝也

1. はじめに

秘密分散法の一方式である(k,n)しきい値法は、1979年にShamir[1]とBlakleyによってそれぞれ独立に提案された。秘密情報をシェアと呼ばれるn個の断片情報に分割し、k個以上のシェアから秘密情報を復元することができるが、$k-1$個以下だと秘密情報を復元することができない秘密情報の分散管理に有効な手法である。秘密の復元が可能なシェアの管理者集合をアクセス集合、それらから成る集合族をアクセス構造と呼ぶとき、(k,n)しきい値法はk個以上のシェアを回収することでアクセス集合となる。また、Simmonsは(k,n)しきい値法のアクセス構造を拡張し、管理者を権限に応じて分割する階層型秘密分散法を検討した[2]。その後、2007年にTassaは導関数を用いた理想的な階層型秘密分散法を提案した[3]。一方で、アクセス構造を柔軟に更新することを可能とする手法についても研究されている。1999年に田村らは、シェアの再配布なしに、しきい値を更新する手法(以下TCSS)を提案した[4]。

本研究は、Tassaの階層型秘密分散法において、田村らのTCSSを一部適用させ、各階層に対応するしきい値を安全に削減する手法について提案する。

2. 秘密分散法

Sを集合$\boldsymbol{S}$に属する秘密とする。Sはn個のシェア$s_1,\ldots,s_n$に分割される。$\boldsymbol{\mathcal{P}}=\{P_1,\ldots,P_n\}$をシェアの管理者の集合とする。ここで集合$A\subseteq\boldsymbol{\mathcal{P}}$を$A$の管理者が保有する任意のシェア集合、シャノンのエントロピー関数を$H(*)$と表す。秘密のエントロピーを$H(S)$、シェアのエントロピーを$H(A)$としたとき、$H(S|A)=0$であれば、AはSを復元できる。このようなAをアクセス集合と呼ぶ。すべてのアクセス集合からなる集合をアクセス構造と呼び$\Gamma\subset 2^{\boldsymbol{\mathcal{P}}}$と表す。$(k,n)$しきい値法のような秘密分散法は、以下の性質を持ち、完全な秘密分散法と呼ばれ、情報理論的安全性を持つことが知られる。

$$\begin{cases} H(S|A)=0 & |A|\geq k \\ H(S|A)=H(S) & |A|<k \end{cases}$$

つまり、(k,n)しきい値法はn個のシェアのうち、少なくともk個が集まればアクセス集合となりSを復元できるが、$k-1$個以下のシェアでは一切の秘密を復元することができない。完全な秘密分散法であり、各シェアサイズが秘密情報のサイズと等しいとき理想的であるという。Shamirの(k,n)しきい値法、ならびに後述のTassaの階層型秘密分散法は理想的である。シェアの生成には定数項がSのk次多項式を用い、秘密の復元は集めたシェアを既知の値、係数を未知の値として連立一次方程式を立て、計算を行うことでSを求める。ここで、大きな素数pに対し、位数pの有限体を$\mathbb{Z}_p\ (\boldsymbol{S}=\mathbb{Z}_p)$とする。$P_i$にシェアを配布する者をディーラー(以下$D$)とすると、$\mathbb{Z}_p$上での$(k,n)$しきい値法は以下の手順で構成される。

分散段階：

(i) Dは、$a_1,\cdots,a_{k-1}\in\mathbb{Z}_p$を無作為に選び、秘密値である定数項を$S\in\mathbb{Z}_p$とし、以下の式のような有限体上の $k-1$次の多項式（以下シェア生成多項式）を作成する。

$$f(x)=S+\sum_{l=1}^{k-1}a_l x^l\ \in\mathbb{Z}_p \qquad (1)$$

(ii) 各管理者への識別子として、秘密でない互いに異なる非零の要素を$x_1,\ldots,x_n\in\mathbb{Z}_p$とし、$D$はシェア$s_i=f(x_i)$を計算した後、各$P_i$に$s_i$を送信する。$(1\leq i\leq n)$

(iii) Dは、$S,a_1,\cdots,a_{k-1}$を破棄する。

復元段階：

(i) 秘密の復元を試みる管理者集合を、$\{P_{i,1},P_{i,2},\cdots,P_{i,k}\}$とする。このとき、シェア生成多項式(1)により、

$$s_{x_{i,j}}=S+a_1x_{i,j}+x_2{x_{i,j}}^2+\cdots+a_{k-1}{x_{i,j}}^{k-1}\in\mathbb{Z}_p$$

と表すことができる$(1\leq j\leq k)$。これは、$\mathbb{Z}_p$上の行列を用いることで以下のように表すことができる。

$$\begin{pmatrix}1 & x_{i,1} & \cdots & x_{i,1}^{k-1}\\ 1 & x_{i,2} & \cdots & x_{i,2}^{k-1}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & x_{i,k} & \cdots & x_{i,k}^{k-1}\end{pmatrix}\begin{pmatrix}S\\ a_1\\ \vdots\\ a_{k-1}\end{pmatrix}=\begin{pmatrix}s_{x_{i,1}}\\ s_{x_{i,2}}\\ \vdots\\ s_{x_{i,k}}\end{pmatrix} \qquad (2)$$

係数行列はVandermonde行列と呼ばれ、各行が初項1で公比が差積に等しい線型独立な行列となる。

Some Considerations on Threshold Changeable Hierarchical Secret Sharing Schemes

Naoki Aizawa and Kouya Tochikubo

(ii) (2)の連立一次方程式を解くことで秘密値Sを求めることができる。

(2)の係数行列をMx、k個の未知の係数をベクトル$\mathbf{a}$、管理者のシェアをベクトル$\mathbf{s}$としたとき、$Mx\cdot\mathbf{a}=\mathbf{s}$において、$\mathbf{a}$の全ての要素がただ1つの解をもつことは、秘密を含むk次の多項式$f(x)$の係数が一意に求まることであり、つまり、秘密が復元できることを意味する。$Mx\cdot\mathbf{a}=\mathbf{s}$が1つの解をもつ必要十分条件は、行列の階数(以下rank)が以下の条件を満たすときであり、(k,n)しきい値法は、$\mathbf{s}$がk個以上のとき、条件を満たす。

$$\operatorname{rank} Mx=\operatorname{rank}(Mx,\mathbf{s})=k \tag{3}$$

また、$\operatorname{rank}(Mx,\mathbf{s})=k$は$Mx$が$k\times k$の正則行列であることと同値である。

3. 階層型秘密分散法

しきい値法の分散処理によって各管理者が 1 つのシェアを保有する場合、いずれの管理者も権限は平等である。しかし、企業等の役職や階級が存在する組織では、管理者を権限に応じて分割し、階層構造をもたせる必要が生じる。例えば、銀行の金庫の鍵を復元するのに 3 人の従業員が立ち合う必要があるが、従業員のうち少なくとも 1 人は部長が必ずシェアを提供するシナリオが考えられる。Tassa は、この最小限の高いレベルの参加者が必要とされる階層型秘密分散法を、導関数を用いることで実現した。n人の管理者集合$\boldsymbol{\mathcal{P}}$、階層レベルiの管理者集合を$\mathcal{U}_i$と表現したm階層を考えたとき、階層構造を以下のように定義する。

$$\boldsymbol{\mathcal{P}}=\bigcup_{i=0}^{m}\mathcal{U}_i,\ \mathcal{U}_i\cap\mathcal{U}_j=\emptyset,\qquad 0\le i<j\le m$$

ここで、$\mathbf{k}=\{k_i\}_{i=0}^{m},(k_{-1}=0<k_0<\cdots<k_m=k)$とするとき、$(\mathbf{k},n)$階層型秘密分散法は次のアクセス構造$\Gamma$で与えられる。

$$\Gamma=\left\{\mathcal{V}\subset\boldsymbol{\mathcal{P}}:\left|\mathcal{V}\cap\left(\bigcup_{j=0}^{i}\mathcal{U}_j\right)\right|\ge k_i,\forall_i\in\{0,1,\cdots,m\}\right\} \tag{4}$$

$\mathbf{k}=\{2,3,5\}$で考えた場合、Γ の下でシェアを受け取った管理者は、秘密の復元には、$\mathcal{U}_0$に属する管理者が2人以上、かつ$\mathcal{U}_0\cup\mathcal{U}_1$から3人以上、かつ$\mathcal{U}_0\cup\mathcal{U}_1\cup\mathcal{U}_2$から5人以上を必要とする。以下に(3)に基づくTassaの階層型秘密分散法の分散段階の手順を示す。

分散段階：

(i) (k,n)しきい値法の(i)と同様に、Dは(1)に基づくk次の多項式を設定する。

(ii) x_rを管理者$P_r\in\boldsymbol{\mathcal{P}}\ (1\le r\le n)$に対応する識別子としたとき、管理者$P_r$が階層$i$に属する、つまり$P_r\in\mathcal{U}_i\ (0\le i\le m)$であるならば、$D$は$x=x_r$における$f(x)$の$k_{i-1}$階微分の値$f^{(k_{i-1})}(x_r)$をシェアとし、配布する。

(iii) Dは、$S,a_1,\cdots,a_{k-1}$を破棄する。

例1) $\mathbf{k}=\{2,3,5\},\boldsymbol{\mathcal{P}}=\{P_1,\cdots,P_{16}\},\mathcal{U}_0=\{P_1,P_2,P_3,P_4,P_5\},\mathcal{U}_1=\{P_6,P_7,P_8,P_9,P_{10}\},\mathcal{U}_2=\{P_{11},P_{12},P_{13},P_{14},P_{15},P_{16}\}$の場合を考える。$\{x_1,\cdots,x_{16}\}$を管理者の識別要素とする。$D$は、無作為に選んだ係数$a_1\cdots a_4$を用いてシェア生成多項式を次のように設定する。

$$f(x)=S+a_1x+a_2x^2+a_3x^3+a_4x^4$$

- $\mathcal{U}_0=\{P_1,P_2,P_3,P_4,P_5\}$の場合
  $k_{-1}=0$より上記の$f(x)$を用いてシェア$s_i=f(x_i)\ (1\le i\le 5)$を生成し、$P_i$にそれを配布する。
- $\mathcal{U}_1=\{P_6,P_7,P_8,P_9,P_{10}\}$の場合
  $k_0=2$より$f^{(2)}(x)=2a_2+6a_3x+12a_4x^2$を用いてシェア$s_i=f^{(2)}(x_i)\ (6\le i\le 10)$を生成し、$P_i$にそれを配布する。
- $\mathcal{U}_2=\{P_{11},P_{12},P_{13},P_{14},P_{15},P_{16}\}$の場合
  $k_1=3$より$f^{(3)}(x)=6a_3+24a_4x$を用いてシェア$s_i=f^{(3)}(x_i)\ (11\le i\le 16)$を生成し、$P_i$にそれを配布する。

復元段階：

(i) $\mathbf{k}=\{k_i\}_{i=0}^{m}$において、秘密の復元を試みる管理者集合を$\{P_1,\cdots,P_{\ell_0},\cdots,P_{\ell_m}\}\ (0\le\cdots\le\ell_0\le\cdots\le\ell_m,\ \ell_i\ge k_i,\ 0\le i\le m)$とし、各階層に属する管理者の識別子要素を

$$\begin{gathered}x_1,\cdots,x_{\ell_0}\in\mathcal{U}_0\\ x_{\ell_0+1},\cdots,x_{\ell_1}\in\mathcal{U}_1\\ \vdots\\ x_{\ell_{m-1}+1}\cdots,x_{\ell_m}\in\mathcal{U}_m\end{gathered}$$

とする。また、$\mathbf{r}:\mathbb{F}\to\mathbb{F}^k$を$\mathbf{r}(\alpha)=\{1,\alpha,\alpha^2,\cdots,\alpha^{k-1}\}$、$\mathbf{r}^{(i)}(\alpha)$を$\mathbf{r}(\alpha)$の$i$階微分$(i\ge 0)$、管理者が提出するシェアのベクトル空間を$\mathbf{s}^{\mathrm{T}}=(s_1,s_2,\cdots,s_{\ell_m})$と定義する。$k$個の未知の係数をベクトル空間$\mathbf{a}$で表すとき、復元に用いる係数行列$Mx,\mathbf{a},\mathbf{s}$は以下のようになる。

$$Mx=\begin{pmatrix}\mathbf{r}(x_1)\\ \vdots\\ \mathbf{r}(x_{\ell_0})\\ \mathbf{r}^{(k_0)}(x_{\ell_0+1})\\ \vdots\\ \mathbf{r}^{(k_0)}(x_{\ell_1})\\ \vdots\\ \mathbf{r}^{(k_{m-1})}(x_{\ell_{m-1}+1})\\ \vdots\\ \mathbf{r}^{(k_{m-1})}(x_{\ell_m})\end{pmatrix},\quad \mathbf{a}=\begin{pmatrix}S\\ a_1\\ \vdots\\ a_{k-1}\end{pmatrix},\quad \mathbf{s}=\begin{pmatrix}s_1\\ s_2\\ \vdots\\ s_{\ell_m}\end{pmatrix} \tag{5}$$

(ii) $Mx\cdot\mathbf{a}=\mathbf{s}$を解くことで、$\mathbf{a}$の全ての要素が求まり、秘密$S$を求めることができる。

さらに、Tassaは多項式補間を拡張した計算回数の削減が見込めるBrikhoff補間を用いた秘密の復元手法について提案している。

係数行列Mxは、管理者がそれぞれ異なる階層である場合、シェア生成多項式に導関数の式が含まれるためVandermonde行列にはならない。ここで、Mxの係数$a_{k_{i-1}},\cdots,a_{k_i-1}$に対応する(6)のような階層ごとに分割した区分行列を$Mx_i(0<i<m)$と表す。区分行列以外の要素は0である。

$$\begin{matrix} i=0 \\ i=1 \\ \vdots \\ i=m \end{matrix}\begin{pmatrix} \boxed{Mx_0} & & & \\ & \boxed{Mx_1} & & \\ & & \ddots & \\ & & & \boxed{Mx_m} \end{pmatrix} \quad (6)$$

各Mx_iはShamirのしきい値法と同じく、(3)を満たしたとき、(2)から対応する係数を求めることができる。全ての$0\le i\le m$に対して$\ell_i\ge k_i$であるとき、$Mx_0,\cdots Mx_m$のすべてが対応する係数を求めることができるので、管理者は秘密の復元が可能となる。

例2)　例1で設定された$(\mathbf{k},n)=(\{2,3,5\},16)$階層型秘密分散法について、アクセス集合の1つである管理者集合$\{P_1,P_2,P_6,P_{11},P_{12}\}$が秘密を復元する場合を考える。$Mx$は以下のようになる。

$$Mx=\begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 & x_1^4 \\ 1 & x_2 & x_2^2 & x_2^3 & x_2^4 \\ 0 & 0 & 2 & 6x_6 & 12x_6^2 \\ 0 & 0 & 0 & 6 & 24x_{11} \\ 0 & 0 & 0 & 6 & 24x_{12} \end{pmatrix}$$

ここで、まず最下層$\mathcal{U}_2$の管理者のみが揃った場合を考える。$\mathcal{U}_2$のシェア生成多項式$f^{(3)}(x)$は1次式であるため、例えば$\{P_{11},P_{12}\}\subset\mathcal{U}_2,\mathbf{s}_2=(s_{11},s_{12})$のみについて、以下のように$Mx_2$を表すと、(2)に基づいた連立方程式解くことで係数a_3,a_4の値が求められる。

$$Mx_2=\begin{pmatrix} 6 & 24x_{11} \\ 6 & 24x_{12} \end{pmatrix}$$

Mx_2, $(Mx_2,\mathbf{s}_2)$が(3)を満たすことは自明である。同様に、$\mathcal{U}_1$は$f^{(2)}(x)$が2次式より、$\{P_6,P_7,P_8\}\subset\mathcal{U}_1$は$a_2,a_3,a_4$を求められるが、このとき、$P_7,P_8\in\mathcal{U}_1$を最下層に属す$P_{11},P_{12}\in\mathcal{U}_2$に替え、$P_6,P_{11},P_{12}$とした場合であっても、$Mx_1$は以下のようになり、$a_2,a_3,a_4$を求めることができる。

$$Mx_1=(2)$$

P_6,P_7,P_{11}とした場合でも(3)を満たし、a_2,a_3,a_4を求めることができる。さらに、$\{P_1,P_2,P_3,P_4,P_5\}\subset\mathcal{U}_0$の管理者で$\mathbf{a}^{\mathrm{T}}=(S,a_1,a_2,a_3,a_4)$を求める(秘密$S$を復元する)場合、これは通常のShamirの$(5,n)$しきい値法であり(2)より秘密を復元することができる。これまでのことを踏まえて、ここでも$P_3,P_4,P_5\in\mathcal{U}_0$を当初示した$P_6\in\mathcal{U}_1,P_{11},P_{12}\in\mathcal{U}_2$に置き換えることが可能で、係数行列$Mx$のブロック$Mx_0$は次のようになる。

$$Mx_0=\begin{pmatrix} 1 & x_1 \\ 1 & x_2 \end{pmatrix}$$

Mx_2,Mx_1,Mx_0のすべてにおいて、(3)の条件を満たし、係数を求めることができるので、管理者集合$\{P_1,P_2,P_6,P_{11},P_{12}\}$は秘密を復元することができる。

4.　提案手法

田村らが提案した一部係数をブロードキャストすることでしきい値を削減するTCSSをTassaの階層型秘密分散法(4)に適用し、任意の層と、それより下位層のしきい値を連動的に削減可能な階層型秘密分散法を提案する。前提条件として、削減の主導者はしきい値の削減時にシェア生成多項式の係数を利用するため、それを保持し続ける必要がある。また、削減処理は一度ずつ行われるとする。具体的な削減手順を以下に示す。

更新段階： $\mathbf{k}=\{k_0,\cdots,k_r,\cdots,k_m\}$の階層型秘密分散法において$r$階層のしきい値を$k_r$から$k_r'=k_r-1$となるように削減するとき、シェア生成多項式の係数$a_{k_{r-1}}$をブロードキャストする。ただし、$r=0$のときは、$a_0$が秘密なので、$a_1$をブロードキャストする。このとき、連動して$r$階層より下位の全ての各階層しきい値は、$r$階層で削減した分と同じだけ減少する為、$\mathbf{k}'=\{k_0,\cdots,k_r-1,\cdots,k_m-1\}$となる。$k_r'$は自身より1つ上位階層のしきい値$k_{r-1}$まで削減することが可能である。

ただし、削減の結果、任意の上位層と下位層のしきい値が等しくなった場合は、(4)に基づく階層構造そのものが変更される特殊な例となる。

$a_{k_{r-1}}$をブロードキャストした結果、復元の際は(4)の$\mathbf{a}$はその係数分だけ未知の元が減少し、

$$(\mathbf{a}')^{\mathrm{T}}=(S,a_1,\cdots,a_{k_{r-1}-1},a_{k_{r-1}+1},\cdots,a_{k-1})$$

となる。同時に、係数行列Mxの$\mathbf{r}(\alpha)$は、

$$\mathbf{r}'(\alpha)=(1,\alpha,\cdots,\alpha^{k_{r-1}-1},\alpha^{k_{r-1}+1},\cdots,\alpha^{k-1})$$

となり、(5)の行列Mxの列数は$(k-1)$に減る。この新たな係数行列をMx'としたとき(3)より、すべての$\mathbf{a}'$がただ1つの解をもつ条件は$\mathrm{rank}\,Mx'=\mathrm{rank}(Mx',\mathbf{s})=k-1$である。ここで、高階微分によって下層になるほど係数を含む項は、次数の低い方から徐々に切り捨てられるので、ブロードキャストした係数$a_{k_{r-1}}$はr階層目までの

シェア生成多項式に含まれ、行の非零要素が減少するが、$r+1$ 階層目以降のシェア生成多項式に係数$a_{k_{r-1}}$は含まれず、行の非零要素は減少しない。これによってMx_rは列数が減り、$f(x)$は$k-1$次の多項式のままであるが、$\mathbf{k}'=\{k_0,\cdots,k_r-1,\cdots,k_m-1\}$で秘密を復元することができるアクセス構造$\Gamma'$となる。ただし、管理者が保持するシェア $\mathbf{s}$ は、復元の際にブロードキャストした係数がシェア生成多項式に含まれる場合に、係数と識別子の積の$k_{j-1}(0<j<r)$階微分をシェアから減算する必要がある。

例3) $\mathbf{k}=\{k_0,k_1,k_2\}=\{2,4,6\}$, $\mathcal{P}=\{P_1,\cdots,P_{12}\}$, $\mathcal{U}_0=\{P_1,P_2\}$, $\mathcal{U}_1=\{P_3,P_4,P_5,P_6\}$, $\mathcal{U}_2=\{P_7,P_8,P_9,P_{10},P_{11},P_{12}\}$とし、$\{x_1,\cdots,x_{12}\}$を管理者の識別子とする。このとき、$\mathbf{k}=\{2,4,6\}$から$\mathbf{k}'=\{2,3,5\}$に削減する場合を考える。$(\mathbf{k},n)=(\{2,4,6\},12)$秘密分散後、管理者$P_j(1<j<12)$はシェア$s_j$を保持している。管理者集合$\{P_1,P_2\}\subset\mathcal{U}_0,\{P_3,P_4\}\subset\mathcal{U}_1,\{P_7,P_8\}\subset\mathcal{U}_2$が、$\mathbf{a}^{\mathrm{T}}=(S,a_1,a_2,a_3,a_4,a_5)$を求めるための$Mx,\mathbf{s}$は次のようになる。

$$Mx=\left(\begin{array}{cc:cc:cc}1&x_1&x_1^2&x_1^3&x_1^4&x_1^5\\1&x_2&x_2^2&x_2^3&x_2^4&x_2^5\\\hdashline0&0&2&6x_3&12x_3^2&20x_3^3\\0&0&2&6x_4&12x_4^2&20x_4^3\\\hdashline0&0&0&0&24&120x_7\\0&0&0&0&24&120x_8\end{array}\right),\quad \mathbf{s}=\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_7\\s_8\end{pmatrix}$$

ここで、$\mathbf{k}'=\{2,3,5\}$となるよう、$0\le i\le 2$ の3階層のうち$i=1$層目のしきい値を1つ削減する(連動して2層目のしきい値についても1つ減少する)。$a_{k_{i-1}}=a_{k_0}=a_2$より、係数a_2をブロードキャストする。すると、$(\mathbf{a}')^{\mathbf{T}}=(S,a_1,a_3,a_4,a_5)$となり、先ほどの$Mx$は$a_2$に対応する3列目がすべて除外される。 $\mathbf{a}$ の未知数も1つ除外されたので、新たな係数行列Mx'は6次から5次の正方行列となり、復元に必要な総管理者数が6人から5人に変わる。$\{|\mathcal{U}_0|,|\mathcal{U}_0\cup\mathcal{U}_1|,|\mathcal{U}_0\cup\mathcal{U}_1\cup\mathcal{U}_2|\}=\{2,3,5\}$ となるよう、例えば管理者$P_4\in\mathcal{U}_1$を除外し、管理者P_1,P_2,P_3,P_7,P_8 $(\{P_1,P_2\}\subset\mathcal{U}_0,\{P_3\}\subset\mathcal{U}_1,\{P_7,P_8\}\subset\mathcal{U}_2)$で秘密の復元を試みるとする。すると、$Mx'$は以下のようになる。

$$Mx'=\left(\begin{array}{cc:c:cc}1&x_1&x_1^3&x_1^4&x_1^5\\1&x_2&x_2^3&x_2^4&x_2^5\\\hdashline0&0&6x_3&12x_3^2&20x_3^3\\\hdashline0&0&0&24&120x_7\\0&0&0&24&120x_8\end{array}\right)$$

このときMx'は(3)の条件を満たすので、$\mathbf{a}'$について、ただ一つの解を求めることができる。つまり、$\mathbf{k}'=\{2,3,5\}$での秘密の復元が可能となっている。

さらに、隣接する階層のしきい値を上位と下位で等しくなるまで削減することで、階層同士の結合や階層の無効化を行うことが可能である。任意の階層rとその直下の階層$r+1$について、k_{r+1}から$k'_{r+1}=k_r$ に削減したとき、$r+1$層と下位にあたる$r+2$層の双方が結合される。また、最下層$\mathcal{U}_m$のしきい値である$k_m=k$について、上位層$\mathcal{U}_{m-1}$のしきい値k_{m-1}と等しくすることで、最下層のシェアを完全に無効化することができる。

5. まとめ

本研究ではTassaの階層型秘密分散法(4)に、田村らのTCSSを適用させ、シェアの再配布なしに任意の階層と、それより下位層のしきい値を連動的に削減することが可能な階層型秘密分散法を提案した。同時に、末端層の無効化や隣接層の結合といった階層構造の一部変更が可能となった。これらは管理者のシェアをブロードキャストすることと同じ効果を持つが、係数で代用することができることを示している。

しかし、理想的なしきい値法を維持しながら下位層のしきい値には影響を与えずに上位層のしきい値のみを削減する手法については現時点で実現できていない。また、アクセス構造を柔軟に更新することを目指す場合、しきい値の削減だけでなく増加させることも望まれる。さらに、(4)とは異なるもう一方のTassaの階層型秘密分散法への適用ついての検討が今後の課題である。

謝辞 本研究はJSPS科研費21K11893の助成を受けたものです。

参考文献

[1] Adi Shamir, “How to share a secret,” Communications of the ACM, Vol.22, No.11, pp.612-613, 1979.

[2] G.J. Simmons, “How to (really) share a secret,” Advances in Cryptology—CRYPTO88, LNCS 403, Springer-Verlag, Berlin, pp.390‐448, 1990.

[3] Tamir Tassa, “Hierarchical Threshold Secret Sharing,” Journal of Cryptology 20(2), pp. 237‐264, 2007.

[4] Y. Tamura, M. Tada and E. Okamoto, “Update of access structure in Shamir’s (k, n) threshold scheme,” Proceedings of The 1999 Symposium on Cryptography and Information Security, vol.1, pp.469-474, 1999.