ISSN 2186-5647

2-50

シェアの再分配なしにアクセス構造を更新可能な完全な(k,n)しきい値秘密分散法に関する考察

日大生産工(院)　○相澤 直樹　　日大生産工　栃窪 孝也

1. まえがき

秘密分散法は、秘密情報を安全に保管する方法として利用されている。秘密分散法の一手法である(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をいくつかのシェアと呼ばれる断片情報に分割し、一定以上のシェアから秘密を再び構成することができる手法である。しかし、秘密分散を行った後、時間経過によって秘密を復元する前に、しきい値を更新することが望まれる場合がある。例えば、既に幾つかのシェアが漏洩してしまい、しきい値を増加させて安全性を高める場合、シェアの欠損のため、しきい値を減少させ安全性の要件を緩和させる場合などが挙げられる。この問題を解決するために様々な手法が提案されてきた。一番簡易な方法は、再びディーラーが新しいシェアを再分配することである。ただし、ディーラーと管理者の間で常に安全な通信路が確保されていることが前提であり、現実的でない。田村らとKeithらはシェアの再分配を必要としない手法を提案している[2][3]。ただし、田村らの手法は事前に更新のための準備が不要という利点はあるが、しきい値の更新が増加の場合は、秘密を変える必要がある。前田らやZhifangらは、事前の準備は必要だが、更新時にディーラーが不要で、更新後はランプ型になる手法を提案している[4][5]。

本稿では、事前に複数の異なる次数の多項式から生成されたシェアをあらかじめ多段的に持つ完全なしきい値更新可能な秘密分散法を提案し、N個の更新可能なしきい値を備える拡張したZhifangらの手法と比較することで、その効率を評価する。

2. 秘密分散法

2.1 Shamirの秘密分散法

sを集合Sに属する秘密とする。秘密sはn個のシェア$v_1,\dots,v_n$に分割される。$\boldsymbol{P}=\{P_1,\dots,P_n\}$をシェアの管理者の集合とする。$n$個のシェアのうち、少なくとも$k$個が集まれば、元の秘密情報$s$を復元できるが、$k-1$個のシェアでは一切の秘密情報を復元することができない。復元にはLagrangeの補間公式を用いる。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、有限体K上での(k,n)しきい値法は次の手順で構成される。

分散段階：

(1) Dは、$a_1,\cdots,a_{k-1}\in K$をランダムに選び、秘密値である定数項を$s\in K$とし、以下の式のような有限体上の$k-1$次の多項式を作成する。

$$f(x)=s+\sum_{l=1}^{k-1}a_l x^l \in K$$

(2) 秘密でない互いに異なる非零の要素を$x_1,\dots,x_n\in K$として、Dはシェア$v_i=f(x_i)$を計算し、P_iにv_iを送信する。$(1\le i\le n)$

(3) Dは、$a_1,\cdots,a_{k-1}$を破棄する。

復元段階：

(1) k人の$P_1,\cdots,P_k$から$(v_1,\cdots,v_k)$を受け取る。

(2) 上記のシェアと各管理者のx_lから、sをLagrangeの補間公式によって復元する。

$$s=\sum_{l=1}^{k}f(x_l)\prod_{m=1,m\neq l}^{k}\frac{x_m}{(x_l-x_m)}\in K$$

ここで、集合Aを$A\subset\boldsymbol{P}$の参加者が保有するシェアの集合、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、シェアの集合$A\subset\boldsymbol{P}$が秘密のsを復元できる。このようなAをアクセス集合と呼ぶ。また、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ぶ。(k,n)しきい値法では、一般的に次のような性質を持つ。

$$\begin{cases} H(S|A)=0 & \text{任意の}|A|\ge k \\ H(S|A)\le H(S) & \text{任意の}|A|<k \end{cases}$$

任意の$|A|<k$となる集合$A\subset\boldsymbol{P}$に対して、$H(S|A)=H(S)$が成立する場合、これを完全な秘密分散法という。完全であるとき、情報理論的安全となる。ここで完全な秘密分散法の情報比ρと管理者P_iに対する情報比ρ_iを以下のように定める。

$$\rho=\min\{\rho_i:1\le i\le n\},\ \rho_i=\frac{\log|S|}{\log|v_i|}$$

Some Considerations on Perfect Threshold Changeable Secret Sharing Schemes

Naoki Aizawa and Kouya Tochikubo

$\rho = 1$を満たす完全秘密分散法は、各シェアサイズが秘密情報のサイズとちょうど等しくなり理想的であるという。Shamir の(k, n)しきい値法は理想的である。

2.2 ランプ型秘密分散法

(k, n)しきい値法は、以下の性質を満たす場合、(c, k, n)ランプ型手法であると言う。

$$\begin{cases} H(S|A) = 0 & \text{任意の } |A| \geq k \\ 0 < H(S|A) \leq H(S) & \text{任意の } c < |A| < k \\ H(S|A) = H(S) & \text{任意の } |A| \leq c \end{cases}$$

ランプ型手法では、$\rho > 1$となり、各シェアサイズを秘密のサイズよりも小さくすることができるが、秘密に関する曖昧さが低下する。特定の値においては、秘密の一部が完全に復元されてしまう場合もある。

2.3 アクセス構造を更新可能な秘密分散法

本稿では、一度秘密分散を行った後にシェアの再配布をせずにしきい値を調整できるような手法を考え、これをしきい値可変法(以下TCSS)と呼ぶ。ただし、しきい値の更新前後で秘密自体は変更しない。Dは管理者から信頼されており、しきい値の更新が行われることを事前に想定している。また、シェアを受け取った管理者についても不正を働くことなく、各々が自発的に更新に参加する。更新は一度のみ実行され、更新時に管理者は不要なシェアを破棄する。このときディーラーは一切関与しない。

しきい値が更新されていない(k, n)しきい値法をΠで表し、更新後の$(k \to k', n)$しきい値法をΠ'で表す。将来更新する可能性があるしきい値の数をNとした場合は、しきい値を$k_1, \cdots, k_N$、状態を$\Pi_1, \cdots, \Pi_N$と表す。

3. Zhifangらの手法[5]

ZhifangらのTCSS手法は、更新後のしきい値の上限に合わせて複数の多項式を用意し、次数が最大の多項式の係数に秘密sを置く。復元時は複数回の計算によって多項式を順番に決定する。以下に手順を示す。

分散段階：

秘密を$s \in \mathbb{F}_q^{k_N - k + 1}$（$q > n$）とする。また、$x_1, \ldots, x_n \in \mathbb{F}_q$は、公開される$n$個の互いに異なる非零の要素であるとする。秘密$s$を共有するため、$D$は多項式$f_1, \ldots, f_{k_N - k + 1} \in \mathbb{F}_q[x]$をランダムに選択する。

$$\begin{aligned} f_1(x) &= a_{1,0} + a_{1,1}x + \cdots + a_{1,k-1}x^{k-1} \\ f_2(x) &= a_{2,0} + a_{2,1}x + \cdots + a_{2,k-1}x^{k-1} + a_{2,k}x^k \\ &\vdots \\ f_{k_N - k + 1}(x) &= a_{k_N - k + 1,0} + a_{k_N - k + 1,1}x + \cdots \\ &\quad + a_{k_N - k + 1, k_N - k}x^{k_N - k} + \cdots \\ &\quad + a_{k_N - k + 1, k_N - 1}x^{k_N - 1} \end{aligned}$$

ここで、秘密は

$$s = \left(a_{k_N - k + 1,0}, a_{k_N - k + 1,1}, \ldots, a_{k_N - k + 1, k_N - k}\right)$$

とする。また、$i \in [k_N - k + 1]$に対し、

$$f_i(x) = f_{i-1}(x) + x^{i-1}g_{i-1}(x)$$

が成立するよう、係数は$a_{i,i-1} = a_{i+1,i-1} = a_{i+2,i-1} = \cdots = a_{k_N - k + 1, i-1}$とする。ここで、$g_{i-1}(x) \in \mathbb{F}_q[x]$は$k$よりも小さい次数である。$D$は各参加者$P_i$に$k_N - k + 1$個のシェア$(f_1(x_j), f_2(x_j), \ldots, f_{k_N - k + 1}(x_j)) \in F_q^{k_N - k + 1} (j \in [\mathrm{n}])$を分配する。1つのシェアサイズは$\log|v_i| = \{1/(k_N - k + 1)\} \cdot \log|S|$となる。

更新段階：

各管理者が保有するシェアのうち$k' - k$個の$f_1(x_i) \cdots f_{k'-k}(x_i)$を破棄することで行われる。

復元段階：

しきい値の更新が起こらないΠの場合、任意の$A < k$の参加者は、f_1が$k - 1$次以下であることから、シェア$f_1(x_1), \ldots, f_1(x_k)$より多項式補間で$f_1$を決定することができる。ここで、$i \in [2, k_N - k + 1]$の場合を考える。今、$f_1, \ldots, f_{i-1}$が既に決定されているとすると、

$$g_{i-1}(x) = \frac{f_i(x) - f_{i-1}(x)}{x^{i-1}}$$

は$k - 1$次以下の多項式であるから、多項式補間を用いることで$f_{i-1}(x_1), \ldots, f_{i-1}(x_k)$並びに、$f_i(x_1), \ldots, f_i(x_k)$からLagrangeの補間公式に基づいた以下の式より、g_{i-1}を求めることができる。

$$g_{i-1}(x) = \sum_{l=1}^{k} \frac{f_i(x_l) - f_{i-1}(x_l)}{x^{i-1}} \prod_{m=1, l \neq m} \frac{x - x_m}{(x_l - x_m)}$$

f_{i-1}はすでに決定されているので、g_{i-1}から今度はf_iを決定することができる。以上より帰納的に$f_{k_N - k + 1}$を決定することができるので、$f_{k_N - k + 1}$の係数である秘密sを復元することができる。上記の手順は、しきい値が$k < k_j < k_N$の場合でも同様で、f_jを求めた後、$g_{i-1}(x) = (f_i(x) - f_{i-1}(x))/x^{i-1}$は$k$次以下、つまり$k_j$よりも小さな次数なので$g_{i-1}$を決定することができる。

更新後のしきい値が$k' = k_N$のΠ_Nで秘密を復元しようとした場合、任意のk_N人の管理者$(P_1, \ldots, P_{k_N})$は$f_{k_N - k + 1}$の次数がk_N以下より、k_N個のシェア$f_{k_N - k + 1}(x_1), \ldots, f_{k_N - k + 1}(x_{k_N})$から多項

式f_{kN-k+1}を決定することができる。したがって、秘密sを復元することが可能となる。

例1. $n=5$、素数qは十分大きく、将来更新する可能性があるしきい値の数をN=1、更新するしきい値を$2 \to 4$としたときに、Zhifangらの手法を適用した例を考える。
分散段階：
秘密を(1,3,5)として、多項式は$a_{1,0}=a_{2,0}=a_{3,0}=1, a_{2,1}=a_{3,2}=3$を満たす以下の$k'-k+1=4-2+1=3$個の式を用いる。

$$f_1(x)=1+2x$$
$$f_2(x)=1+3x+3x^2$$
$$f_3(x)=1+3x+5x^2+6x^3$$

$$(\ g_1(x)=1+3x,\ \ g_2(x)=2+6x\ )$$

各管理者における$x_1,x_2,x_3,x_4,x_5 \in \mathbb{F}_q$は簡単のため、$(x_1,x_2,x_3,x_4,x_5)=(1,2,3,4,5)$とする。管理者に分配するシェアは表1のようになる。

表1　管理者が所有するシェア

管理者	P_1	P_2	P_3	P_4	P_5
シェア	$f_1(1)$ $f_2(1)$ $f_3(1)$	$f_1(2)$ $f_2(2)$ $f_3(2)$	$f_1(3)$ $f_2(3)$ $f_3(3)$	$f_1(4)$ $f_2(4)$ $f_3(4)$	$f_1(5)$ $f_2(5)$ $f_3(5)$

(2,5)しきい値法での復元段階：
P_1,P_2の管理者が秘密を復元するとき、$(f_1(1),f_2(1),f_3(1),\ f_1(2),f_2(2),f_3(2))$を用いる。
(1) $f_1(1),f_1(2)$より、多項式補間によって$f_1(x)=1+2x$を復元する。g_1は2次以下より、$f_1(1),f_1(2)$と$f_2(1),\ f_2(2)$から多項式補間により、$g_1(x)=1+3x$を復元する。
(2) (1)より、f_1,g_1が求まったので、

$$f_2(x)=f_1(x)+x^1 g_1(x)=1+3x+3x^2$$

よりf_2を求めることができる。ここで、g_2は2次以下より、$f_2(1),\ f_2(2)$と$f_3(1),\ f_3(2)$から多項式補間により、$g_2(x)=2+6x$を復元する。
(3) (2)より、f_2,g_2が求まったので、

$$f_3(x)=f_2(x)+x^2 g_2(x)=1+3x+5x^2+6x^3$$

よりf_3を求めることができる。よってf_3の部分係数である秘密(1,3,5)が求まる。必要なシェアサイズは以下のようになる。

$$\log|f_1(1)|+\log|f_2(1)|+\log|f_3(1)|+\log|f_1(2)|$$
$$+\log|f_2(2)|+\log|f_3(2)|=\frac{1}{3}\log|S|\times 6=2\log|S|$$

(2,5) → (4,5)しきい値法での復元段階：
P_1,P_2,P_3,P_4の管理者が秘密を復元するとき、$(f_3(1),f_3(2),f_3(3),f_3(4))$とLagrangeの補間公式により、多項式$f_3$を求めることで部分係数である秘密(1,3,5)が求まる。必要なシェアサイズは、

$$\log|f_3(1)|+\log|f_3(2)|+\log|f_3(3)|+\log|f_3(4)|$$
$$=\frac{1}{3}\log|S|\times 4=\frac{4}{3}\log|S|$$

となる。

4.　提案手法

本稿では、事前に複数の異なる次数の多項式から生成されたシェアを多段的に持つ完全なTCSS手法を提案する。
分散段階：
秘密$s \in \mathbb{F}_q\ (q>n)$で共有するため、$D$は各$j \in [N+1]$に対し、更新後のしきい値を$k_j$としてShamirの$(k_j,n)$しきい値法を定数項がいずれも秘密$s$で独立に構築する。つまり、$f_j$の次数が$k_j$より小さく、$f_j(0)=s$となる係数が任意の$N+1$個の多項式$f_1,\dots,f_{N+1} \in \mathbb{F}_q[x]$を独立に用意する。

$$f_1(x)=s+a_{1,1}x+\cdots+\ a_{1,k-1}x^{k-1}$$
$$\vdots$$
$$f_j(x)=s+a_{j,1}x+\cdots+a_{j,k-1}x^{k-1}\cdots+a_{j,k_j-1}x^{k_j-1}$$
$$\vdots$$
$$f_{N+1}(x)=s+a_{N+1,1}x+\cdots+a_{N+1,k_N-1}x^{k_N-1}$$

公開される$x_1,\dots,x_n \in \mathbb{F}_q$を$n$個の互いに異なる非零の要素とする。各参加者$P_i\ (i \in [n])$は$N+1$個のシェア$(f_1(x_i),f_2(x_i),\dots,f_{N+1}(x_i))$を受け取る。1つのシェアサイズは$\log|v_i|=\log|S|$となる。
更新段階：
管理者はしきい値の更新が確定した段階で、新しいしきい値$k_j\ (j \in [N+1])$に対応するシェアを残し、それ以外を破棄する。
復元段階：
Lagrangeの補間公式から秘密を復元する。

例2.　例1と同様の条件でしきい値の更新を想定した場合に提案手法を適応した例を考える。
分散段階：
秘密を1とし、Shamirの秘密分散法に基づいた$N+1=2$個の独立した多項式を選択する。

$$f_1(x)=1+2x$$
$$f_2(x)=1+5x+7x^2+9x^3$$

表 3　手法の比較

	各管理者の保有シェア情報比	更新後の復元に要するシェア情報比	復元時の計算量(多項式補間の回数)	更新後のしきい値上限	情報理論的安全
Zhifangらの手法	1	$\frac{k_N - k + 1}{k'(k_N - k' + 1)}$	$k_N - k' + 1$	$k < k' \leq n$	×
提案手法	$\frac{1}{N+1}$	$\frac{1}{k'}$	1	$k' \leq n$	○

管理者に分配するシェアは表2のようになる。

表 2　管理者が所有するシェア

管理者	P_1	P_2	P_3	P_4	P_5
シェア	$f_1(1)$ $f_2(1)$	$f_1(2)$ $f_2(2)$	$f_1(3)$ $f_2(3)$	$f_1(4)$ $f_2(4)$	$f_1(5)$ $f_2(5)$

(2,5)しきい値法での復元段階：
P_1, P_2 の管理者が秘密を復元するとき、$(f_1(1), f_1(2))$を用いて通常のShamirの秘密分散法と同様にLagrangeの補間公式を用いて求める。必要なシェアサイズは、

$$\log|f_1(1)| + \log|f_1(2)| = \log|S| \times 2 = 2\log|S|$$

となる。

(2,5) → (4,5)しきい値法での復元段階：
P_1, P_2, P_3, P_4の管理者が秘密を復元するとき、$(f_2(1), f_2(2), f_2(3), f_2(4))$ を用いて通常のShamirの秘密分散法と同様にLagrangeの補間公式を用いて求める。必要なシェアサイズは、

$$\log|f_2(1)| + \log|f_2(2)| + \log|f_2(3)| + \log|f_2(4)| = \log|S| \times 4 = 4\log|S|$$

となる。

例2では、従来手法の例1に比べて初期に配布するシェアや復元に要するシェア数自体は少ないか、多くて同じである。しかし、秘密に対して各管理者が保有するシェアと復元に要するシェアのサイズは、提案手法では増加している。

5. 効率の評価

従来のZhifangらの手法と提案手法の双方をシェアのサイズ、計算量、更新後のしきい値の上限、安全性の観点から比較を行った。結果を表3に示す。安全性では、従来の手法では更新後にランプ型となったが、提案手法は更新後も完全な秘密分散法(情報理論的安全)を実現した。各管理者の保有シェアサイズに関しては、従来手法は更新に関わらず$\rho = 1$だが、提案手法は更新する可能性があるしきい値数に依存する。しかし、しきい値数が限定されている場合は、提案手法でもある程度の効率上昇を見込むことが可能である。また、提案手法は準備済みのしきい値範囲内に更新が制限されるのに対し、従来手法は更新可能なしきい値の上限以下であれば自由にしきい値を調整することが可能である。計算量については、従来手法は更新するしきい値に依存するが、提案手法は1回の多項式補間のみである。さらに、更新後のしきい値の上限は、従来手法は必ず更新後にしきい値を増加させる必要が生じる。

これらの手法は更新時に一部シェアを放棄せず使用する管理者の不正を想定していない。今後の課題は、管理者が信頼できない場合に耐性のある手法の検討が挙げられる。その他に、秘密分散後に管理者の登録を解除し、そのシェアを無効にする手法の検討などが挙げられる。

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] 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 (SCIS’99), vol.1, pp.469-474, 1999.

[3] K.M. Martin, J. Pieprzyk, R. Safavi-Naini, H. Wang, “Changing thresholds in the absence of secure channels,” ACISP’99, Proceedings of the 4th, LNCS, vol. 1587, Springer, pp.177-191, 1999.

[4] A. Maeda, A. Miyaji, M. Tada, “Efficient and unconditionally secure verifiable threshold changeable scheme,” ACISP’ 2001, Proceedings of the 6th, LNCS, vol. 2119, Springer, pp.403-416, 2001.

[5] Zhang Z, Chee YM, Ling S, Liu M, Wang H. “Threshold changeable secret sharing schemes revisited,” Theoretical Computer Science 2012 418(1), pp.106-115, 2012.