信州大学工学部

学士論文

秘密分散法の非確率的な定義について

指導教員　西新 幹彦 准教授

学科　電気電子工学科
学籍番号　09T2019J
氏名　大草 健人

2015 年 3 月 19 日

目次

1　はじめに

昨今の日本は情報化が進み，各々が多くの情報を管理しなければならない状態になっている．管理するにあたって，情報の紛失と情報の漏洩の二点に注意する必要がある．情報の紛失を防ぐにはコピーを多く用意すれば良いが，コピーを増やした分，情報の漏洩の確率は高まってしまう．かといって，情報をコピーをとらず管理しておくと情報を紛失した際復元ができなくなる．これら二つの問題を同時に解決する方法として秘密分散法がある．秘密分散法の代表的なシナリオでは，管理しておきたい情報 (秘密情報) をもとに，ディーラーと呼ばれる者がシェアをつくる．そのシェアを各ユーザーに配布しておき，秘密情報が必要なときにユーザーが集まることによってシェアから秘密情報を復元できる．決められたシェアの組み合わせでしか秘密情報は復元できないことになっているので，情報の紛失と情報の漏洩の二点を同時に解決できる．一例として完全型 (k, n) しきい値法がある．これは n 個のシェアを作り，そのうちの k 個集まれば秘密情報を復元できるというものである．また $k-1$ 個以下のシェアからでは，秘密情報について全く漏れがないというのもこの方法の特徴である．このような秘密の復元や，必要数未満のシェアでは秘密が全く漏れないという秘密分散法の安全性について厳密に議論する際は，秘密情報を確率変数と考え，そのエントロピーが使われる [1]．そしてその結果が，秘密分散法の定義となっている．しかし，これらについて写像の概念を用いて説明することができるのではないか，また秘密分散法の定義についても，確率を用いず定義することができるのではないかと考えた．

以上のことから本論文では，確率を用いず写像の概念だけで秘密分散法を定義した．その際，確率的な秘密分散法との関係についても検討した．その結果，秘密情報とシェアのサイズが等しいという前提の下であれば，確率的な秘密分散法は非確率的な秘密分散法でもあることが分かった．また非確率的な秘密分散法は，シェアの取りうる値の上に一様分布を導入することにより，確率的な秘密分散法となることが分かった．

2　確率的な秘密分散法

まず，確率的な秘密分散法の定義について議論していく．

2.1　定義

秘密情報 S およびシェア $W_j(j = 1, \cdots, n)$ があり，いずれもある有限集合上の値をとるものとする．S，W_j は共に確率変数とする．

定義 1　秘密情報 S とシェア $(W_1, W_2, ..., W_n)$ が次の 2 条件を満たすとき完全型 (k, n) しき

い値型秘密分散法をなすという [1].

1. 任意の相違なる k 個のシェア $(W_{j_1}, W_{j_2}, ..., W_{j_k})$ から S が正しく復号できる．つまり，

$$H(S|W_{j_1}, W_{j_2}, ..., W_{j_k}) = 0 \tag{1}$$

という式が成り立つ．

2. 任意の $k-1$ 個のシェアから秘密情報 S は全く得られない．つまり

$$H(S|W_{j_1}, W_{j_2}, ..., W_{j_{k-1}}) = H(S) \tag{2}$$

という式が成り立つ．

上記で定義される完全型 (k, n) しきい値型秘密分散法のことを本論文では確率的な (k, n) 秘密分散法，または単に確率的な秘密分散法と呼ぶ．また，この確率的な秘密分散法に対して，次の定理が成り立つ．

定理 1　確率的な秘密分散法において，任意のシェア W_j のエントロピー $H(W_j)$ は次式を満たさなければならない．

$$H(W_j) \geq H(S) \tag{3}$$

(証明)

シェア W_j および $k-1$ 個の W_{j_l} が全て相異なる場合，次のように下界が求められる．

$$\begin{aligned} H(W_j) &\geq H(W_j|W_{i_1}, W_{i_2}, ..., W_{i_{k-1}}) \\ &\geq H(W_j|W_{i_1}, W_{i_2}, ..., W_{i_{k-1}}) - H(W_j|W_{i_1}, W_{i_2}, ..., W_{i_{k-1}}, S) \\ &= I(S; W_j|W_{i_1}, W_{i_2}, ..., W_{i_{k-1}}) \\ &= H(S|W_{i_1}, W_{i_2}, ..., W_{i_{k-1}}) - H(S|W_{i_1}, W_{i_2}, ..., W_{i_{k-1}}, W_j) \\ &= H(S) \end{aligned} \tag{4}$$

ここで，最後の等式は式 (1)(2) による．

なお，一般の秘密分散法では秘密情報がとる値の集合とシェアがとる値の集合は同じである必要はないが，本論文では秘密情報もシェアも同一の集合から値をとる場合のみを扱う．

2.2　実現例

確率的な秘密分散法を実現する方法として Shamir の多項式補間法 [2] がある．秘密情報からシェアを作る手順や秘密を復元する手順は次の通りである．

秘密情報やシェアは有限体 $\mathbb{F}$ 上に値をとるとする．（もともとの S の値域が有限体でないとしたら十分大きな有限体を考えればよい．）秘密情報 S の分布は任意でよい．係数 $a_1, a_2, ..., a_{k-1}$ を $\mathbb{F}$ 上に一様に分布する確率変数とし，多項式

$$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + S \tag{5}$$

を定める．これを元に，ディーラーが互いに相異なる非零の $x_i \in \mathbb{F}(i = 1, 2, ..., n)$ に対し，

$$W_i = f(x_i) \tag{6}$$

を作る．この W_i をシェアとし，ユーザーにそれぞれ秘密裏に配布する．$S, a_1, ..., a_{k-1}$ については非公開とする．

シェア保有者が協力して k 個のシェアを集めることによって，式 (5) をもとめることができ，秘密情報 S を復元できる．さらに，$k-1$ 個のシェアからでは未知数が k 個ある式 (5) をもとめられず，秘密情報 S を一意に定めることができないため，復元できない．

3 非確率的な秘密分散法の定義の提案

ここで，確率を用いない秘密分散法の定義を提案する．

3.1 非確率的な定義

秘密情報 s およびシェア w_j がある有限集合 $\mathbb{F}$ 上の値をとるものとする．

定義 2(提案) 秘密情報 s のシェア $(w_1, w_2, ..., w_n)$ が次の 2 条件を満たすとき非確率的な秘密分散法をなすという．

1. ある写像 $\psi : (\mathbb{N} \times \mathbb{F})^k \to \mathbb{F}$ が存在し，

$$s = \psi(j_1, w_{j_1}, j_2, w_{j_2}, ..., j_k, w_{j_k}) \tag{7}$$

が成り立つ．ここに $\mathbb{N} \triangleq \{1, \cdots, n\}$ である．ただし，$j_1, j_2, ..., j_k$ は互いに相異なる．この時の ψ は復号器としての役割を果たす．

2.$\mathbb{F} = \psi(j_1, w_{j_1}, j_2, w_{j_2}, ..., j_{k-1}, w_{j_{k-1}}, j_k, \mathbb{F})$ となる．すなわち，

$$g(\cdot) = \psi(j_1, w_{j_1}, j_2, w_{j_2}, ..., j_{k-1}, w_{j_{k-1}}, j_k, \cdot) \tag{8}$$

が全単射となる．

式 (7) は k 個のシェアから秘密情報を復元できることを意味する．また，式 (8) が全単射の関係にあるということは k 個目の値を取り替えると，得られる値が $\mathbb{F}$ 上で重複することなく取り変わるということを意味する．つまり，$k-1$ 個のシェアが集まったとしても，秘密情報について情報が得られていないということである．

3.2 非確率的な秘密分散法の例

非確率的な秘密分散法の定義を満たすものが存在しなければ定義として意味をなさない．実は 2.2 節で説明した Shamir の多項式補間法は非確率的な秘密分散法でもある．シェアの作り方は基本的に 2.2 節と同じで，秘密情報 s と係数 $a_1, \cdots, a_{k-1}$ の値は非公開であるが，これらは確率変数ではない．

秘密を復元するための復号器は次のようにして導くことができる．まず式 (5)(6) より

$$\begin{bmatrix} w_{j_1} \\ w_{j_2} \\ \vdots \\ w_{j_k} \end{bmatrix} = \begin{bmatrix} x_{j_1}^{k-1} & x_{j_1}^{k-2} & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ x_{j_k}^{k-1} & x_{j_k}^{k-2} & \dots & 1 \end{bmatrix} \begin{bmatrix} a_{k-1} \\ a_{k-2} \\ \vdots \\ s \end{bmatrix}$$

となる．この時右辺の正方行列が，ヴァンデルモンド行列となっているため逆行列が存在する．両辺にその逆行列をかけると，

$$\begin{bmatrix} a_{k-1} \\ a_{k-2} \\ \vdots \\ s \end{bmatrix} = \begin{bmatrix} x_{j_1}^{k-1} & x_{j_1}^{k-2} & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ x_{j_k}^{k-1} & x_{j_k}^{k-2} & \dots & 1 \end{bmatrix}^{-1} \begin{bmatrix} w_{j_1} \\ w_{j_2} \\ \vdots \\ w_{j_k} \end{bmatrix}$$

となる．右辺の逆行列の k 行目部分を $[\cdots]$ と置くと，

$$[\cdots] \begin{bmatrix} w_{j_1} \\ w_{j_2} \\ \vdots \\ w_{j_k} \end{bmatrix} = s$$

となる．これはある復号器 ψ に $j_1, w_{j_1}, j_2, w_{j_2}, ..., j_k, w_{j_k}$ の値をいれると秘密情報 s が復号できるということを示している．つまり，

$$s = [\cdots] \begin{bmatrix} w_{j_1} \\ w_{j_2} \\ \vdots \\ w_{j_k} \end{bmatrix} = \psi(j_1, w_{j_1}, j_2, w_{j_2}, ..., j_k, w_{j_k})$$

となり，これは (7) 式と一致する．ここで，復号器 ψ は非公開情報を含んでいないので，公開しても構わないことに注意されたい．

また，x_i が相異なる非零の値であることから $[\cdots]$ の各要素も非零であることがいえる．したがって，s の値は $w_{j_1}, \cdots, w_{j_k}$ のすべてに依存し，有限体の演算の性質から s と w_{j_k} が 1 対 1 であることがわかる．このことから，$k-1$ 個のシェアから秘密情報 S は復元できない．よって，非確率的な秘密分散法になっている．

4　ラテン方陣と非確率的な秘密分散法

4.1　ラテン方陣

本論文ではシェアのサイズと秘密情報 S のサイズが等しいと仮定しているので，3 章で述べた ψ という復号器は，複数のラテン方陣 (又は，ラテン超立方体) で表すことができる．n 行 n 列の正方形のますの中に，n 種類の記号をそれぞれ n 個ずつおいて，各行各列のなかに重複した記号のないようにしたものを n 次のラテン方陣という．この特徴から，シェアをラテン方陣のますの座標を与えることにより，任意の k 個のシェアで秘密情報の一点が定まり (秘密の復元)，また $k-1$ 個のシェアではラテン方陣内の取りうる値に全ての記号が現れる (秘密の安全性) ような復号器を実現できる．図 1 に 6 次のラテン方陣の例を示す．

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

図 1　6 次のラテン方陣の例

4.2　非確率的 $(2,2)$ 秘密分散法のラテン方陣による表現

簡単な例として，6 次のラテン方陣を用いて非確率的な $(2,2)$ 秘密分散法を構成する．これはシェアを 2 つ (w_1, w_2) 作り，1 つのシェアでは秘密は復号できないというものである．この場合，任意の 6 次のラテン方陣を 1 つ用意すればよい（図 2)．このラテン方陣が復号器を表現している．(したがって公開してもよい.）ディーラーは秘密情報 s からシェアを次のように生成する．まず，一方のシェア w_1 の値は他人に知られないように勝手に選ぶ（確率的に選ぶという意味ではない)．次に，他方のシェア w_2 の値は，ラテン方陣の w_1 行 w_2 列の値が秘密情報 s と等しくなるように選ぶ．例えば図 2 のラテン方陣を用いる場合，$s=4$, $w_1=3$ であれば w_2 の値として 1 を選ぶ．復号の際は w_1 と w_2 の値からラテン方陣の w_1 行 w_2 列の値を読めば秘密情報が復元できることは明らかである．また，シェアが 1 つしかないときには，ラテン方陣を見ても各行各列にすべての記号が現れるので秘密情報 s は復号できない．

		w_2					
		0	1	2	3	4	5
	0	0	1	2	3	4	5
	1	1	2	3	4	5	0
w_1	2	2	3	4	5	0	1
	3	3	4	5	0	1	2
	4	4	5	0	1	2	3
	5	5	0	1	2	3	4

図 2　非確率的な $(2,2)$ 秘密分散法のための復号表の例

4.3　非確率的 (2,3) 秘密分散法のラテン方陣による表現

次に少し複雑な例として，非確率的な $(2,3)$ 秘密分散法を構成してみる．これはシェアを 3 つ作り，その内 2 つあれば s を復号できるというものである．この場合は前の例とは異なり，任意のラテン方陣というわけにはいかない．なぜなら，秘密情報 s を戻せるシェアの組み合わせは $(w_1,w_2),(w_2,w_3),(w_3,w_1)$ の 3 通りあることから，ラテン方陣が 3 つ必要であり，そのどれを使っても正しく秘密情報を戻せなければならないからである．このような制約を満たすラテン方陣を作るためには有限体の性質を用いればよい．以下で作り方の例を説明するが，これは Shamir の多項式補間法の復号器を表の形で表現していることに他ならない．

取りうる値の集合を位数 5 の有限体 $\mathbb{F}$ とする．1 次多項式 $f(x)=ax+s$ を考える．この式を元にシェアを 3 つ作るための式は

$$
\begin{aligned}
w_1 &= f(1) = a+s \\
w_2 &= f(2) = 2a+s \\
w_3 &= f(3) = 3a+s
\end{aligned}
$$

となる．これらから係数 a を消去して S についての 3 つの式にすると，

$$
\begin{aligned}
s &= 2w_1 - w_2 \\
s &= 3w_2 - 2w_3 \\
s &= 4w_1 + 2w_3
\end{aligned}
$$

となる．ここから，図 3 の復号器 ψ となるラテン方陣の表を作ることができる．表内の矢印では w_1,w_2,w_3 にかかっている係数を計算している．この表を用いて，前の例と同様に s とシェア一つを決定すると残りのシェアも決定する．またこの表もラテン方陣なのでシェア一つでは s は復号できない．

		w_2	0	1	2	3	4
			↓	↓	↓	↓	↓
w_1			0	1	2	3	4
0	→	0	0	4	3	2	1
1	→	2	2	1	0	4	3
2	→	4	4	3	2	1	0
3	→	1	1	0	4	3	2
4	→	3	3	2	1	0	4

		w_3	0	1	2	3	4
			↓	↓	↓	↓	↓
w_2			0	2	4	1	3
0	→	0	0	3	1	4	2
1	→	3	3	1	4	2	0
2	→	1	1	4	2	0	3
3	→	4	4	2	0	3	1
4	→	2	2	0	3	1	4

		w_3	0	1	2	3	4
			↓	↓	↓	↓	↓
w_1			0	2	4	1	3
0	→	0	0	2	4	1	3
1	→	4	4	1	3	0	2
2	→	3	3	0	2	4	1
3	→	2	2	4	1	3	0
4	→	1	1	3	0	2	4

図 3 非確率的な $(2,3)$ 秘密分散法のための復号表の例

4.4 有限体の存在しない位数の秘密分散法の構成

また，有限体の存在しないサイズの秘密情報でも，前述のラテン方陣を組み合わせることで実現可能な場合がある．例として秘密情報のサイズが 20 のものを考える．この時の復号表の例を図 4 に示す．図 4 の下の表をまず作り，シェアとなる w_a, w_b をさらに秘密分散させたものの復号表が上の二つの表となる．シェアをユーザーに配布する際に，$(w_{a1}, w_{b1}), (w_{a2}, w_{b2})$ のようにペアで配る．これにより秘密情報のサイズが有限体の存在しない 20 でも秘密分散法が構成できる．

5 確率的秘密分散法と非確率的秘密分散法の関係

非確率的な秘密分散法について検討した結果，確率的な秘密分散法と非確率的な秘密分散法の関係が明らかになった．

w_a		w_{a2}			
		0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
w_{a1}	2	2	3	0	1
	3	3	0	1	2

w_b		w_{b2}				
		0	1	2	3	4
	0	0	1	2	3	4
	1	1	2	3	4	0
w_{b1}	2	2	3	4	0	1
	3	3	4	0	1	2
	4	4	0	1	2	3

		w_b				
		0	1	2	3	4
	0	0	1	2	3	4
w_a	1	5	6	7	8	9
	2	10	11	12	13	14
	3	15	16	17	18	19

図 4　秘密のサイズ 20 の秘密分散法の復号表の例

5.1　非確率的な秘密分散法ならば確率的な秘密分散法である条件

定理 2　シェアと秘密情報がともに $\mathbb{F}$ 上に値をとるとき，非確率的な秘密分散法のシェアが一様分布であれば，それらは確率的秘密分散法をなす．

(証明) 確率変数 $S, W_1, ..., W_{k-1}$ を考え，互いに独立とする．S の分布は任意，$W_1, ..., W_{k-1}$ は全て一様分布とする．非確率的な秘密分散法の定義より，

$$s = \psi(j_1, w_{j_1}, ..., j_k, w_k) \tag{9}$$

となるような ψ が存在する．$\psi(j_1, w_{j_1}, j_2, w_{j_2}, ..., j_{k-1}, w_{j_{k-1}}, j_k, \cdot)$ は全単射であることに注意し，この逆関数を $\varphi(\cdot, j_1, w_{j_1}, ..., j_{k-1}, w_{j_{k-1}}, j_k)$ と表す．確率変数 $W_i (i = k, ..., n)$ を $W_i = \varphi(S, 1, W_1, 2, W_2, ..., k-1, W_{k-1}, i)$ と定める．

すると，式 (9) より $W_i (i = 1, ..., n)$ の中の任意の k 個に対し，

$$S = \psi(j_1, W_{j_1}, ..., j_k, W_{j_k}) \tag{10}$$

が成り立つので，

$$H(S|W_{j_1}, ..., W_{j_k}) = 0 \tag{11}$$

となる．

一方，$S = s, W_{j_1} = w_{j_1}, ..., W_{j_{k-1}} = w_{j_{k-1}}$ のとき，$W_i (i = 1, ..., k-1)$ は，

$$\begin{aligned} W_i &= \varphi(S, j_1, W_{j_1}, ..., j_{k-1}, W_{j_{k-1}}, i) \\ &= \varphi(s, j_1, w_{j_1}, ..., j_{k-1}, w_{j_{k-1}}, i) \\ &\triangleq w_i \end{aligned}$$

と書けるので，

$$\begin{aligned} &\Pr\{S = s, W_{j_1} = w_{j_1}, ..., W_{j_{k-1}} = w_{j_{k-1}}\} \\ &= \Pr\{S = s, W_1 = w_1, ..., W_{k-1} = w_{k-1}\} \\ &= \Pr\{S = s\} \cdot \Pr\{W_1 = w_1, ..., W_{k-1} = w_{k-1}\} \\ &= \Pr\{S = s\} \cdot = \frac{1}{|\mathbb{F}|^{k-1}} \end{aligned} \tag{12}$$

となり，さらに

$$\begin{aligned} &\Pr\{W_{j_1} = w_{j_1}, ..., W_{j_{k-1}} = w_{j_{k-1}}\} \\ &= \sum_s \Pr\{S = s, W_{j_1} = w_{j_1}, ..., W_{j_{k-1}} = w_{j_{k-1}}\} \\ &= \sum_s \Pr\{S = s\} \cdot \frac{1}{|\mathbb{F}|^{k-1}} \\ &= \frac{1}{|\mathbb{F}|^{k-1}} \end{aligned} \tag{13}$$

となる．すると式 (12)(13) より

$$\Pr\{S = s, W_{j_1} = w_{j_1}, ..., W_{j_{k-1}} = w_{j_{k-1}}\} = \Pr\{S = s\} \cdot \Pr\{W_{j_1} = w_{j_1}, ..., W_{j_{k-1}} = w_{j_{k-1}}\}$$

となるので，

$$H(S|W_{j_1}, ..., W_{j_{k-1}}) = H(S) \tag{14}$$

が成り立つ．

式 (11)(14) より，$S, W_1, ..., W_n$ は確率的秘密分散法をなす．□

5.2 確率的な秘密分散法ならば非確率的な秘密分散法である条件

定理 3 シェアと秘密情報のサイズが等しい時，確率的な秘密分散法は非確率的な秘密分散法ともいえる．

(証明) S とシェアが $\mathbb{F}$ 上に値をとる確率的な秘密分散法を考える．この時，S の分布は任意である．シェアは n 個 $(W_1, ...W_n)$ 存在し，k 個で秘密情報を復元できるので，

$$H(S|W_{j_1}, ..., W_{j_k}) = 0 \tag{15}$$

となる．これは，シェア k 個の値から S の値が確定することを意味するので，

$$S = \psi(j_1, W_{j_1}, ..., j_k, W_{j_k}) \tag{16}$$

なる写像 ψ が存在する．また，2.1 節定理 1 より，S がどんな分布でも

$$H(W_j) \geq H(S) \tag{17}$$

でなければならない．つまり，S が一様分布の場合 $H(S) = \log|\mathbb{F}|$ なので，$H(W_j) = \log|\mathbb{F}|$ となり，W_j も一様分布でなければならない．$k-1$ 個のシェアが集まったとき，さらに一つ k 個目のシェア (W_k) を加えることで秘密情報を復元できるが，その際に S がどんな値だとしても W_k の値を取り替えることのみで実現させなければならないので，ψ はちょうどラテン方陣，(またはラテン立方体，ラテン超立方体) でなければならない．ラテン方陣の各行各列に重複する記号は現れないということから，$\mathbb{F} = \psi(j_1, w_{j_1}, j_2, w_{j_2}, ..., j_{k-1}, w_{j_{k-1}}, j_k, \mathbb{F})$ となる．すなわち，

$$g(\cdot) = \psi(j_1, w_{j_1}, j_2, w_{j_2}, ..., j_{k-1}, w_{j_{k-1}}, j_k, \cdot) \tag{18}$$

が全単射となる．

式 (16) と式 (18) が全単射であることから，$S, W_1, ..., W_n$ は非確率的秘密分散法をなす．□

6 まとめ

秘密分散法の理解を深めることで確率的な秘密分散法をもとに非確率的な秘密分散法の定義を提案した．その際両者の関係性についても検討した．非確率的な秘密分散法をラテン方陣を用いて表現することができ，秘密が有限体を持たないサイズでも実現できる場合があることが分かった．秘密情報とシェアのサイズが等しいという前提の下であれば，確率的な秘密分散法は非確率的な秘密分散法となることが分かった．また，シェアの取りうる値の上に一様分布を導入することにより，非確率的な秘密分散法は確率的な秘密分散法となることが分かった．

今後の課題として，秘密情報とシェアのサイズが等しくない場合の関係性の検討が残っている．

謝辞

この研究を進めるにあたり指導していただいた西新幹彦准教授，また貴重なご意見を下さった長岡技術大学の武井由智准教授に感謝する．

参考文献

[1] 山本博資,「秘密分散法とそのバリエーション」, 数理解析研究所講究録, 1361 巻, pp.19-31, 2004 年.

[2] A. Shamir, “How to share a secret,” Communications of the ACM, no.22, pp.612–613, Nov. 1979.