L-011

秘密分散法に用いるラテン方陣の探索
Search of Latin square for Secret sharing scheme

中村 紅葉† 西川 峻平† 足立 智子†
Kouyou Nakamura Shunpei Nishikawa Tomoko Adachi

1. はじめに

秘密分散法は、1 つの秘密情報を複数人で分散して管理するための方法として知られており、1979 年に Shamir によって発案された技術である。秘密分散法では、秘密情報を複数のシェアまたはシャドウと呼ばれるデータに分割する。このシャドウはある決められた組み合わせが揃ったときに限り、元の秘密情報が復元される。すなわち、復元の条件を満たさないシャドウのみが流出しても元の秘密情報が漏れないことが保証される[1]。

秘密分散法にはさまざまな方法があるが、本稿では 2022 年の足立・竹内[2]によるラテン方陣を用いた秘密分散法を取り扱う。我々はラテン方陣の性質を調査し、この秘密分散法に適したラテン方陣を探索した。

2. Shamir のしきい値法

秘密情報をsとし、sは整数とする。まず、秘密情報sの所有者(ディーラ)がsからn個のシャドウ$(y_1, \dots, y_n)$を生成する。次にディーラは参加者$(P_1, \dots, P_n)$に各々シャドウ$(y_1, \dots, y_n)$を秘密裏に渡す。その後任意のk人の参加者が協力してk個のシャドウを集め、所定の計算をすることにより秘密情報sを復元できる。このときのkをしきい値と言い、このような考え方を Shamir の(k, n)しきい値法という[1]。本節では、[3]および[4]を基にして、Shamir のしきい値法を、(1)準備、(2)シャドウの配布、(3)秘密情報の再構築の 3 段階に分けて説明する。

2.1 準備

ディーラは$\mathbb{Z}_p$の要素から、0 ではない別々のものをn個選び出し、$x_i, 1 \le i \le n$と記述する(ここでは$p \ge n+1$を要求している)。$1 \le i \le n$に対し、ディーラは値x_iを参加者P_iに与える。x_iという値は公開されている。

2.2 シャドウの配布

1. ディーラが秘密情報$s \in \mathbb{Z}_p$を分散したいものとする。ディーラは$\mathbb{Z}_p$から$k-1$個の要素$a_1, \dots, a_{k-1}$を(ランダムに)選ぶ。
2. $1 \le i \le n$に対し、ディーラは$y_i = f(x_i)$を以下の式の下で計算する。
$$y_i = f(x_i) = s + a_1 x_i + a_2 x_i^2 + \cdots + a_{k-1} x_i^{k-1}$$
3. $1 \le i \le n$に対し、ディーラはシャドウy_iをP_iに配布する。

2.3 秘密情報の再構築

参加者の内k人集まれば、秘密情報sについて次のラグランジュ補間公式を用いて再構築することができる。

$$s = f(0) = \sum_{j=1}^{k} y_{i_j} \prod_{1 \le t \le k, t \ne j} \frac{0 - x_{i_k}}{x_{i_j} - x_{i_k}}$$

3. ラテン方陣を用いた秘密分散法

ラテン方陣を用いた代表的な秘密分散法として、Cooper の手法[5]、Stones の手法[6]、足立・竹内[2]が挙げられる。しかし Cooper の手法は安全性の面で難点があり、Stones の手法は計算量の面で難点がある。本節では足立・竹内[2]による(2,2)しきい値法の構成を説明する。

3.1 準備

ディーラと 2 人の参加者であるP_1, P_2がいる。またラテン方陣$L(a, b)$のすべての情報は公開される。ここで作成されるラテン方陣の数は1個である。ラテン方陣の行番号として$Q = \mathbb{Z}_q = \{0,1,2, \dots, q-1\}$の要素を並べ(並び方は公開している)、その中の一つの行番号$X \in Q$を秘密情報とする。

3.2 シャドウの配布

ディーラは、ラテン方陣の列番号として$Q = \mathbb{Z}_q = \{0,1,2, \dots, q-1\}$の要素を並べ(並び方は公開している)、その中の一つの列番号$Y \in Q$をシャドウとして参加者P_1に配布する。またディーラはシャドウ$Z = X \times Y$を計算し、参加者P_2に配布する。

3.3 秘密情報の再構築

参加者P_1とP_2が集まればシャドウYとZが同時に分かるので、$X = Z \times (Y)^{-1}$の値を求めることで秘密情報Xを再構築することができる。

4. 提案手法とその結果

位数qのラテン方陣とは、$q \times q$の方陣にq種類の数を入れ、どの縦の列、横の行もちょうど 1 個ずつ出現するように配置したものである[7]。我々は秘密分散法に適するラテン方陣として、3 種類の型を取り上げ、探索した。

4.1 $L_1(q; k)$型のラテン方陣

方陣の第 1 行に、$0, 1, \dots, q-1$のq個の数を並べる。方陣の第 2 行に、第 1 行を$k (1 \le k \le q-1)$ずつシフトした$k, k+1, \dots, k+q-1 \ (mod\ q)$の$q$個の数を並べる。方陣の第 3 行に、第 2 行を$k$ずつシフトした$2k, 2\,k+1, \dots, 2k+q-1 \ (mod\ q)$の$q$個の数を並べる。同様にして、方陣の第$i$行$(i = 2, 3, \dots, q)$に、第$i-1$行を$k$ずつシフトした$(i-1)k, (i-1)k+1, \dots, (i-1)k+q-1 \ (mod\ q)$の$q$個の数を並べる。このようにして得られた$q \times q$の方陣は、$GCD(q, k) = 1$であるとき、位数$q$のラテン方陣になる。このラテン方陣を$L_1(q; k)$型と呼ぶ。

図 1 は位数$q = 5$のラテン方陣において$k = 1$および$k = 2$のラテン方陣$L_1(5; 1), L_1(5; 2)$である。すなわち図(a)は 1 行

†静岡理工科大学情報学部コンピュータシステム学科
Department of computer Science, Faculty of Informatics, Shizuoka Institute of Science and Technology

目から 1 つずつ、図(b)は 1 行目から 2 つずつシフトした形のラテン方陣である。

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

(a) $L_1(5;1)$

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

(b) $L_1(5;2)$

図 1　位数 5 の$L_1(q;k)$型のラテン方陣

結果 1　$L_1(k)$において作成できるラテン方陣の個数は$\varphi(q)$個である。ここで、$\varphi(q)$は、qと互いに素な$1 \le k \le q-1$な整数kの個数であり、オイラーのφ関数と呼ばれる。

特に、位数qが素数の場合、$L_1(q;k)$型のラテン方陣の個数は$q-1$個である。

$$\varphi(q) = \#\{k \mid 1 \le k \le q-1, GCD(k,q) = 1\}$$

4.2 $L_2(q;a,b)$型のラテン方陣

任意の 2 つの正整数をa,bとする。方陣の第 1 行に$0, a, 2a, \dots, (q-1)a \ (mod\ q)$の$q$個の数を並べる。方陣の第 2 行に第 1 行に$b$を加えた$b, b+a, b+2a, \dots, b+(q-1)a \ (mod\ q)$の$q$個の数を並べる。方陣の第 3 行に第 2 行に$b$を加えた$2b, 2b+a, 2b+2a, \dots, 2b+(q-1)a \ (mod\ q)$の$q$個の数を並べる。同様に、方陣の第$i$行に第$i-1$行に$b$を加えた$(q-1)b, (q-1)b+a, (q-1)b+2a, \dots, (q-1)b+(q-1)a \ (mod\ q)$の$q$個の数を並べる。このようにして得られた方陣は$GCD(a,q) = GCD(b,q) = GCD(a+b,q) = GCD(a-b,q) = 1$のとき、位数$q$のラテン方陣になる。このラテン方陣を$L_2(q;a,b)$型と呼ぶ。

$$\begin{bmatrix} 0 & a & 2a & \cdots & (q-1)a \\ b & b+a & b+2a & \cdots & b+(q-1)a \\ 2b & 2b+a & 2b+2a & \cdots & 2b+(q-1)a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (q-1)b & (q-1)b+a & (q-1)b+2a & \cdots & (q-1)b+(q-1)a \end{bmatrix}$$

図 2　$L_2(q;a,b)$型のラテン方陣

結果 2　位数qが素数の場合、$L_2(q;a,b)$型において作成できるラテン方陣の個数は$(q-1)\times(q-3)$個である。

4.3 $L_3(p^e)$型のラテン方陣

素数pと正整数$e \ge 1$を用いて$q = p^e$とする。方陣の第 1 行および第 1 列に$0, 1, 2, \dots, q-1 \ (mod\ q)$の$q$個の数を並べる。任意の第$i$行第$j$列には$(i-1)+(j-1) \ (mod\ q)$を並べる。このようにして得られた方陣は、位数$q$のラテン方陣である。このラテン方陣を$L_3(p^e)$型と呼ぶ。

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

(a) $L_3(5^1)$

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

(b) $L_3(2^2)$

0	1	α	$1+\alpha$
1	α	$1+\alpha$	0
α	$1+\alpha$	0	1
$1+\alpha$	0	1	α

(c) $L_3(2^2)$

図 3　$L_3(p^e)$型のラテン方陣

図 2 は$L_3(p^e)$型のラテン方陣である。(a)は$q = 5^1$でのラテン方陣であり、(b) は$q = 2^2$でのラテン方陣である。ここで、位数qが素数であるとき、すなわち$q = p^1$であるとき、$L_1(p;1)$ 型と$L_3(p^1)$型は同じラテン方陣になる。例えば第 4.1 節の図 1(a)と図 3(a)を比べると同じ形である。

$e \ge 2$の場合、$GF(p)$上の原始既約多項式$f(x) = x^e + \cdots$の根をαとして、有限体$GF(p)$のe次拡大を考える。図 2(c)は、F_2上の原始既約多項式$x^2 + x + 1$の根をαとして、有限体$GF(2)$の2次拡大$F_4 = \{0, 1, \alpha, 1+\alpha\}$の要素を用いてラテン方陣を表した。$\alpha, 1+\alpha$をそれぞれ$2, 3$と表記すると、図 2(b)になる。

結果 3　$L_3(p^e)$型のラテン方陣の個数は$q-1$個である。

5. 探索の結果および結論

第 4 節で説明した 3 種類の型のラテン方陣について探索した結果を表 1 として示す。表 1 では位数qでの 3 種類の型のラテン方陣の個数とその探索時間をまとめている。

表 1　3 種類の型のラテン方陣の個数と探索時間

ラテン方陣の大きさ(q)	L_1(q;k)			L_2(q;a,b)			L_3(p^e)			
	q	個数	時間[ms]	q	個数	時間[ms]	q	原始既約多項式を求める時間[ms]	個数	ラテン方陣を求める時間[ms]
約10^2	101	100	0.00	101	9800	0.00	128	0.00	127	0.00
約10^3	1009	1008	0.00	1009	1014048	243	1024	0.00	1023	2909
約10^4	10007	10006	0.00	10007	100100024	33733	8192	80.0	8191	2148192

今回、3 種類の型のラテン方陣について探索を行ったが、各々の特徴として$L_1(q;k)$型は作成時間がほぼ 0.00[ms]で時間が短いが、ラテン方陣の作成個数は 2 番目に少ない。$L_2(q;a,b)$型はラテン方陣の作成個数が多く、作成時間は 2 番目に短い。$L_3(p^e)$型は原始既約多項式を考えるため作成時間が長く、作成個数が少ない。これらの結果から 3 つの型の中では$L_2(q;a,b)$型が秘密分散法に用いるラテン方陣として最も適当であるといえる。

6. おわりに

本稿では、秘密分散法に用いるラテン方陣として 3 つの型を探索した。この他にもラテン方陣は様々あるので、秘密分散法に用いるものとして適当なラテン方陣を探索していきたい。

参考文献

[1] 土井洋, “秘密分散法とその応用について”, 情報セキュリティ情報科学, 第 4 巻, pp.137-149 (2012).

[2] 足立智子, 竹内泉, “ラテン方陣を用いた新しい秘密分散法”, 2022 年日本応用数理学会年会一般講演, E3-5-4 (2022).

[3] Stinson, D.R., 櫻井幸一訳, “暗号理論の基礎”, 共立出版, (1996).

[4] Shamir, A., “How to share a secret”, Communication of the ACM, Vol.22, No.11, pp.612–613 (1979).

[5] Cooper, J., Donovan, D., Seberry, J., “Secret sharing schemes arising from Latin squares”, Bulletin of the Institute of Combinatorics and its Applications, Vol.12, pp.33–43 (1994).

[6] Stones, R.J., Su, M., Liu, X., Wang, G., Lin, S., “A Latin square autotopism secret sharing scheme”, Designs, Codes and Cryptography, Vol.80, No.3, pp.635–650 (2016).

[7] Laywine C.F., Mullen G.L., “Discrete Mathmatics Using Latin Square”, John Wiley & Sons, Inc., (1998).