A-009

部分ラテン方陣の特徴と秘密情報の漏洩

Features of Partial Latin Squares and Leakage of Secret

八木 康裕† 野澤 友希† 沢瀬 光† 足立 智子†
Kohsuke Yagi Yuki Nozawa Hikaru Sawase Tomoko Adachi

1. はじめに

ラテン方陣を秘密情報とする秘密分散法に Cooper 等[1]の手法がある。足立・西川・中村[2]は、ラテン方陣の位数 n が 5 以下の場合に情報漏洩率を計算し、その部分的漏洩に関する考察を与えた。[2]で定めた情報漏洩率は、あらかじめ参加者に配布したシェアの個数も含めている。[2]のアルゴリズムでは位数 $n=6$の場合は処理できなかった。

本研究では、シェアを漏洩に含めない形で情報漏洩率を定め直す。アルゴリズムを改良し、ラテン方陣の位数 n が 4 , 9 の場合に新しい情報漏洩率を調べる。

2. 先行研究の結果

2.1 ラテン方陣の性質

位数 n のラテン方陣とは、大きさ$n \times n$ の方陣に、どの行、どの列にもシンボルが 1 回ずつ出現する方陣のことである。部分ラテン方陣とは、ラテン方陣のいくつかのセルからシンボルを消したものである。部分ラテン方陣が後述の UC セットなら、シンボル有セル(ヒント)からラテン方陣(解)を求めるパズルになる。ヒントの場所によって、シンボルが一意に定まる空白セルの個数が異なる。

位数 $n=m^2$ のラテン方陣は、Z_{m^2}と同型な方陣(以降 I 型と記す)$Z_m \times Z_m$と同型な方陣(以降 II 型と記す)がある。$n=4=2^2$の場合、図 1(a)は I 型、(b)は II 型の例である。

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

(a)I 型

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

(b) II 型

図 1　位数 4 のラテン方陣

部分ラテン方陣において、条件 1 を満たすものを UC セット(Uniquely Completable Set)、条件 1,2 を満たすものをクリティカルセット(Critical Set , 以降 CS と記す)という。

条件 1. 今ある要素からラテン方陣を作成できる

条件 2. 一つでも要素が欠けるとラテン方陣の作成不可

また、ラテン方陣の CS の要素数が最小になるものをミニマルクリティカルセット(Minimal Critical Set , 以降 MCS と記す)という。I 型のラテン方陣の MCS の要素数は、位数 n が奇数の場合は $\frac{n^2-1}{4}$ 個、偶数の場合は $\frac{n^2}{4}$ 個となる。ラテン方陣の性質は[3,4]に詳しい。

† 静岡理工科大学
Shizuoka Institute of Science and Technology

2.2 ラテン方陣を用いた秘密分散法

秘密分散法は、秘密にしたい情報(秘密情報)を複数の参加者で分散管理する暗号である。各参加者に配布される分散情報は、シェアまたはシャドウと呼ばれる。秘密分散法にはしきい値法やアクセス構造がある。秘密分散法に関する全般的な知識は[5]を参照。Cooper 等[1]はラテン方陣を用いたアクセス構造を提案した。ラテン方陣を秘密情報とし、CS または MCS の要素をシェアとしている。

2.3 情報漏洩率

足立・西川・中村[2]は、Cooper 等[1]の手法に関する安全性を評価する基準として、秘密情報であるラテン方陣 L の位数nおよび配布したシェアの個数 k に伴う情報漏洩率 $H_1(n,k)$を定義した。

$$H_1(n,k)=\frac{1}{{}_{n^2}C_k}\sum_{\substack{A\\|A|=k}}\frac{k+h_A}{n^2}=\frac{n^2!}{k!\,(n^2-k)!}\sum_{\substack{A\\|A|=k}}\frac{k+h_A}{n^2}$$

配布シェアの集合を A とする。ラテン方陣の規則により、シェアの集合 A から $B(\subset L)$が作成でき、秘密情報 L が部分的に復元される。Bから A を除いた集合 $B\backslash A$ の要素は、配布していないにもかかわらず秘密情報 L の要素の一部が判明したことになり、漏洩したシェアになる。集合 $B\backslash A$ の要素の個数をh_Aとする。h_Aは漏洩したシェアの個数である。

3. 提案手法

先行研究[2]で定めた情報漏洩率 H_1は、$\frac{k+n_A}{n^2}$ を計算している。シェアを漏洩に含めない形にするために、本研究では、$\frac{n_A}{n^2-k}$ で情報漏洩率$H_2(n,k)$を定め直す。

$$H_2(n,k)=\frac{1}{r}\sum_{\substack{A\\|A|=k}}\frac{h_A}{n^2-k}$$

ラテン方陣の用語では、先行研究[2]の情報漏洩 H_1は、ヒントの配布が全ての場合について数え上げている。提案手法の情報漏洩 H_2は、与えられたヒント数(シェアの個数)と一意にシンボルが定まるセルの個数(漏洩した個数)を合わせて計算している。本提案手法で定める情報漏洩率H_2は、与えられたヒント(シェア)数は含まず、一意にシンボルが定まる(漏洩した)セルの個数のみの割合を計算する。

先行研究[2]では C 言語で実験したが、本研究では python のライブラリ関数を用いて時間短縮を図り、バックトラック法を用いてアルゴリズムを改良した。

位数$n=$ 9 のラテン方陣で、ヒント(配布シェア)数kが 28 ~ 40 の場合に、ランダムに試行回数 2, 10, 100 回で、シンボルが一意に定まるセル(漏洩するシェア)の個数h_Aおよび情報漏洩率H_2を求める。

4. 結果及び考察

4.1 位数$n = 4$のラテン方陣の場合

[2]の結果をもとに、提案手法の情報漏洩率H_2を求め直し、I 型は表 1 に、II 型は表 2 にまとめた。情報漏洩率が 0%または 100%になるようなヒント数kの値は除いている。

表 1, 2 ではh_Aの値を 3 区切りでまとめた。例えば、表 1 のk =3 の行では、560 回のうち、h_A = 0 が 368 回、h_A= 1~3 が 192 回であった。

表 1　位数 4 の I 型ラテン方陣の漏洩率

ヒント数k (配布シェアの個数)	試行回数 (全通り) [回]	一意にシンボルが決まるセルの個数h (漏洩したシェアの個数) h=0	1~3	4~6	7~9	10~12	提案手法 漏洩率H2 [%]
3	560	368	192	0	0	0	4.62
4	1820	384	1104	300	0	32	16.92
5	4368	144	1872	1152	240	960	42.46
6	8008	160	2536	1168	0	4144	68.65
7	11440	48	1200	1968	8224	0	83.64
8	12870	18	288	1680	10884	0	91.38
9	11440	32	848	0	10560	0	95.48
10	8008	0	264	7744	0	0	97.80
11	4368	0	4	4320	0	0	98.92
12	1820	4	0	1816	0	0	99.78

表 2　位数 4 の II 型ラテン方陣の漏洩率

ヒント数k (配布シェアの個数)	試行回数 (全通り) [回]	一意にシンボルが決まるセルの個数h (漏洩したシェアの個数) h=0	1~3	4~6	7~9	10~12	提案手法 漏洩率H2 [%]
3	560	368	192	0	0	0	4.62
4	1820	344	1152	324	0	0	16.48
5	4368	144	1680	1728	720	96	33.27
6	8008	160	3384	3504	0	960	49.63
7	11440	48	1728	5904	3760	0	64.76
8	12870	18	432	5040	7380	0	77.34
9	11440	48	2544	0	8848	0	86.87
10	8008	0	792	7216	0	0	93.41
11	4368	0	144	4224	0	0	97.36
12	1820	12	0	1808	0	0	99.34

4.2 位数$n = 9$のラテン方陣の場合

ヒント(配布シェア)数kが 28 ~ 40 の場合に、ランダムに試行回数 2, 10, 100 回で、提案手法のアルゴリズムで情報漏洩率H_2を求め、I 型は表 3 に、II 型は表 4 にまとめた。表 3, 4 ではh_Aの値を 10 区切りでまとめた。ヒント(配布シェア)数kが 27 以下の場合は、実行時間が膨大であったため中断した。S

表 3　位数 9 の I 型ラテン方陣の漏洩率

ヒント数k (配布シェアの個数)	試行回数 (ランダム) [回]	一意にシンボルが決まるセルの個数 (漏洩したシェアの個数) h=0	1~10	11~20	21~30	31~40	41~50	提案手法 漏洩率H2 [%]	実行時間 [秒]
28	2	0	2	0	0	0	0	10.78	14063.28
29	2	1	1	0	0	0	0	0.96	596.2
30	2	1	1	0	0	0	0	2.94	484.84
31	2	1	8	1	0	0	0	5	169.61
32	10	1	8	1	0	0	0	8.78	1714.19
33	10	1	7	2	0	0	0	11.04	650.28
34	10	1	8	1	0	0	0	12.55	592.79
35	100	2	73	22	1	1	1	18.35	325.22
36	100	0	61	30	6	2	1	23.64	445.91
37	100	0	43	36	18	2	1	30.82	96.59
38	100	0	39	38	13	4	6	36.28	52.98
39	100	0	22	43	18	6	11	45.9	32.35
40	100	0	14	37	29	7	13	53.31	13.63

表 4　位数 9 の II 型ラテン方陣の漏洩率

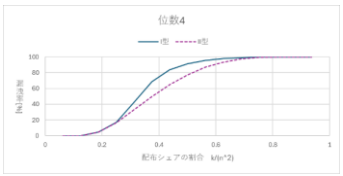
ヒント数k (配布シェアの個数)	試行回数 (ランダム) [回]	一意にシンボルが決まるセルの個数 (漏洩したシェアの個数) h=0	1~10	11~20	21~30	31~40	41~50	提案手法 漏洩率H2 [%]	実行時間 [秒]
28	2	1	1	0	0	0	0	1.89	4460.78
29	2	1	1	0	0	0	0	0.96	808.87
30	2	0	2	0	0	0	0	5.88	550.64
31	2	0	2	0	0	0	0	9	22.18
32	10	0	10	0	0	0	0	8.78	330.08
33	10	1	9	0	0	0	0	7.92	67.19
34	10	0	7	3	0	0	0	15.32	114.58
35	100	2	69	26	3	0	0	18.43	172.37
36	100	0	57	35	4	3	1	24.71	119.098
37	100	1	52	35	10	2	0	26.48	50.99
38	100	0	31	42	19	8	0	37.02	18.85
39	100	0	28	40	22	9	1	41.48	10.44
40	100	0	13	35	41	9	1	50.22	5.98

4.3 考察

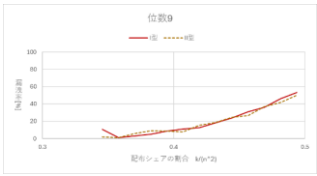
I 型のラテン方陣の MCS の要素数は、位数 n が奇数の場合は $\frac{n^2-1}{4}$ 個、偶数の場合は $\frac{n^2}{4}$ 個となるから、ラテン方陣の要素数n^2に対する MCS の要素数の割合は約 25%となる。そこで、横軸を配布シェアの割合$\frac{k^2}{n}$ とし、縦軸を情報漏洩率H_2としてグラフを作成し、図 2 にまとめた。図 2(a)は位数 4(I 型と II 型)、(b)は位数 9(I 型と II 型)、(c)は I 型(位数 4, 9)、(d)は II 型(位数 4, 9)である。

位数 4 では I 型より II 型の方が漏洩率は低いが、位数 9 では I 型と II 型で漏洩率はあまり変わらない。I 型, II 型どちらも位数 4 より位数 9 の方が漏洩率は低い。

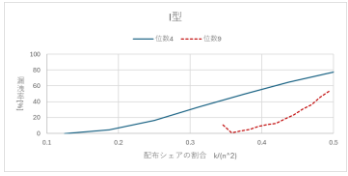
位数 9 の I 型ラテン方陣の MCS の要素数は 20 個である。ヒント(配布シェア)数kが 20 近辺での漏洩個数h_Aを求めるために、さらにアルゴリズムの改善が必要である。



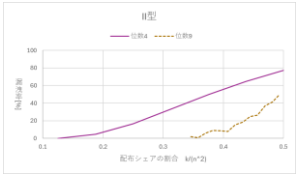
(a)位数 4(I 型と II 型)



(b)位数 9(I 型と II 型)



(c) I 型(位数 4, 9)



(d) II 型(位数 4, 9)

図 2　配布シェアの割合に対する情報漏洩率

参考文献

[1] J. Cooper, D. Donovan, and J. Seberry, Secret sharing schemes arising from Latin squares, Bulletin of the Institute of Combinatorics and its Applications, vol.12, pp.33-43, 1994.
[2] 足立 智子・西川 峻平・中村 紅葉, “ラテン方陣を秘密情報とする部分的漏洩に関する一考察,” 信学技報, vol.123, no.149, IT2024-7, EMM2024-7, pp.31-36, 2024 年 5 月
[3] C. F. Laywine and G. L. Mullen, Discrete Mathmatics Using Latin Square, John Wiley and Sons, Inc., Toronto, 1998.
[4] D. Keedwell and J. Denes, Latin squares and their applications, 2nd ed., North-Holland, London, 2015.
[5] ダグラス・スティンソン 著, 櫻井幸一 訳, 「暗号理論の基礎」, 共立出版株式会 社, 東京, 1996.11.01. (原著 : D. R. Stinson, “Cryptography : Theory and Practice, ” CRC Press, Inc., 1995.),.