A-011

ラテン方陣のシンボル候補を含む漏洩
Leakage of candidate symbols in Latin square

樋渡 サム† 沢瀬 光‡ 足立 智子†
Samu Hiwatashi Hikaru Sawase Tomoko Adachi

1. はじめに

部分ラテン方陣(空白あり)は、ヒント(セルの場所とシンボル)から、空白セルのシンボルが一意に定まることや候補が絞られることがある。Cooper 等[1]はラテン方陣を秘密情報とする秘密分散法を提案した。この秘密分散法[1]は、復元されない場合にも秘密情報の一部が漏洩する。シンボルが一意に定まる場合について、八木等[2]は情報漏洩率を調べた。本研究では、シンボル候補が絞られた時点で漏洩したとみなし、新しい情報漏洩率を定め、実験的に調べる。

2. 先行研究の結果

2.1 ラテン方陣を秘密とする秘密分散法

秘密分散法は、秘密にしたい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。秘密分散法に関する全般的な知識は文献 [3]を参照。

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。部分ラテン方陣のシンボル有セル(ヒント)はラテン方陣(解)を求めるパズルになる。ヒントをシャドウとし、解を秘密とするこのパズルが、[1]の秘密分散法である。

2.2 シンボルが一意の場合の情報漏洩率

足立等[4]は、[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および配布したシャドウの個数 k に伴う情報漏洩率$H_1(n,k)$を定義した。

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

ここで、配布シャドウの集合は部分ラテン方陣Aである。ラテン方陣の規則により、シャドウの集合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$B \setminus A$の要素(その個数をh_Aとする)は、配布していないにもかかわらず秘密情報Lの要素の一部が漏洩したことになる。

ラテン方陣の位数nが大きくなると、$H_1(n,k)$のように全通り調べられない。配布したシャドウは、漏洩に含めない形にしたい。そこで、八木等[2]は、配布シャドウ数 kを分子から分母に移動し、ランダムな試行回数rを使って、情報漏洩率を$H_2(n,k)$として定め直した。

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

これらの情報漏洩率H_1, H_2は、どちらもシンボルが一意に定まる場合についてである。

†静岡理工科大学
Shizuoka Institute of Science and Technology
‡株式会社静岡情報処理センター
Shizuoka Information Processing Center Co., Ltd.

3. 提案手法

3.1 ラテン方陣のシンボル候補が一意ではない場合

ヒント(シャドウ)はラテン方陣(秘密)を求めるパズル(秘密分散法)になる。ラテン方陣の性質上、ヒント(配布されたシャドウ)から、空白セルのシンボルが一意に定まったり、シンボルの候補が絞られたりすることがある。

ヒントの個数をkとし、ヒントが配置された部分ラテン方陣をAとする。Aに対して、シンボルが一意に定まったセルの個数をh_Aとし、一意に定まったシンボル有セル(漏洩量h_A)が配置された方陣をBとする。

シンボル候補がj通りに絞られたセルの個数を$h_A^{(j)}$とする。特にj=1 の場合は、$h_A^{(1)}$=h_Aである。本稿では、$j \geq 2$ として、$h_A^{(j)}$を考える

シンボルが一意に定まる場合については、先行研究[2,4]で情報漏洩率を調べた。本研究では、シンボル候補がj通りに絞られた時点で 1/jの漏洩とみなし、新しい情報漏洩率$H_3(n,k)$を定義する。

$$H_3(n,k) = \frac{1}{r} \sum_{\substack{A \\ |A|=k}} \frac{h_A + h'_A}{n^2-k}$$

ここで、h'_Aは次式で定める。

$$h'_A = \sum_{2 \leq j \leq n} \frac{h_A^{(j)}}{j}$$

3.2 実験概要

本研究では、部分ラテン方陣におけるシンボル候補を含む新しい情報漏洩率$H_3(n,k)$を、先行研究の情報漏洩率$H_2(n,k)$と比較して評価する。そのために、Python によるシミュレーション実験を行う。ラテン方陣の位数n、配布ヒント数k、および試行回数rを固定し、ランダムにヒントを配置して部分ラテン方陣を生成し、以下の手順で情報漏洩率H_2, H_3を算出する。

最初に、位数nのラテン方陣を用意する。すべてのセルのシンボルを消し、空白セルにする。ランダムにk個のセルにシンボル(ヒント)を埋め込み、部分ラテン方陣Aとする。ラテン方陣のルールから一意に定まるシンボルを埋め込み、部分ラテン方陣Bとする。このとき、シンボルが一意に定まるセルの個数を数え上げ、h_Aとして出力する。シンボル候補がj通りに定まるセルの個数を数え上げ、$h_A^{(j)}$として出力する。これを一つの試行とし、r回試行を繰り返す。最後に、情報漏洩率H_2, H_3を算出する。

位数n=5,6,7,8,9、ヒント数kの範囲は $1 \leq k \leq n^2-1$、試行回数r=1000 として実施する。各試行における部分ラテン方陣の状態(A,B)や、候補数ごとのセル分布$h_A^{(j)}$、情報漏洩量(h_A, h'_A)を出力する。また、ヒント数kごとに、情報漏洩量(h_A, h'_A)の平均値(「平均漏洩量h, h'」と呼ぶ)を出力し、情報漏洩率$H_2(n,k)$, $H_3(n,k)$を評価する。

4. 結果および考察

4.1 位数n = 5の場合の結果

定義より$H_2(n,k) \leq H_3(n,k)$が成り立つので、その差を実験結果より調べる。本節では、位数n=5 のラテン方陣に関する結果を述べる。

表 1 は、位数n=5 の実験において、ヒント数k毎に、シンボルが一意に定まる場合(従来の手法)における平均漏洩量hと情報漏洩率H_2、シンボル候補を含む場合(本研究の手法)における平均漏洩量h'と情報漏洩率H_3の算出値をまとめたものである。また、図 1 は、表 1 を基に作成した情報漏洩率H_2, H_3のグラフである。ヒント数k[個]を横軸に取り、漏洩率[%]を縦軸に取った。

表 1 より、差分$H_3 - H_2$はk=9 のとき最大値 0.3496 を取った。$1 \leq k \leq 4$のとき $0.2 < H_3 - H_2 < 0.3$ であり、$5 \leq k \leq 12$のとき$H_3 - H_2 > 0.3$ であり、$13 \leq k \leq 15$のとき $0.2 < H_3 - H_2 < 0.3$ であり、$16 \leq k \leq 18$のとき $0.1 < H_3 - H_2 < 0.2$ であり、$19 \leq k$ のとき $0 \leq H_3 - H_2 < 0.1$ であった。図 1 より、ヒント数k(横軸)に対して、情報漏洩率H_3の上がり具合は、情報漏洩率H_2の上がり具合に比べて緩やかであった。

表 1　位数n=5 の漏洩量h,h'と情報漏洩率H_2, H_3

位数5		シンボルが一意に定まる		シンボル候補を含む		差分
ヒント数k	試行回数r	平均漏洩量h	漏洩率H2	平均漏洩量h'	漏洩率H3	H3-H2
1	1000	0.0000	0.0000	5.2000	0.2167	0.2167
2	1000	0.0000	0.0000	5.4154	0.2355	0.2355
3	1000	0.0000	0.0000	5.6550	0.2570	0.2570
4	1000	0.0280	0.0013	5.8826	0.2815	0.2802
5	1000	0.1510	0.0075	6.0435	0.3097	0.3022
6	1000	0.3660	0.0193	6.1198	0.3414	0.3221
7	1000	0.7060	0.0392	6.1077	0.3785	0.3393
8	1000	1.1950	0.0703	5.9199	0.4185	0.3482
9	1000	1.7910	0.1119	5.5934	0.4615	0.3496
10	1000	2.4180	0.1612	5.2088	0.5085	0.3473
11	1000	3.1680	0.2263	4.6601	0.5592	0.3329
12	1000	3.7900	0.2915	4.0845	0.6057	0.3142
13	1000	4.5250	0.3771	3.4132	0.6615	0.2844
14	1000	5.0930	0.4630	2.7561	0.7136	0.2506
15	1000	5.5180	0.5518	2.1331	0.7651	0.2133
16	1000	5.7570	0.6397	1.5678	0.8139	0.1742
17	1000	5.7120	0.7140	1.1173	0.8537	0.1397
18	1000	5.5310	0.7901	0.7248	0.8937	0.1036
19	1000	5.1830	0.8638	0.4050	0.9313	0.0675
20	1000	4.5720	0.9144	0.2135	0.9571	0.0427
21	1000	3.8370	0.9593	0.0815	0.9796	0.0203
22	1000	2.9650	0.9883	0.0175	0.9942	0.0059
23	1000	2.0000	1.0000	0.0000	1.0000	0.0000
24	1000	1.0000	1.0000	0.0000	1.0000	0.0000

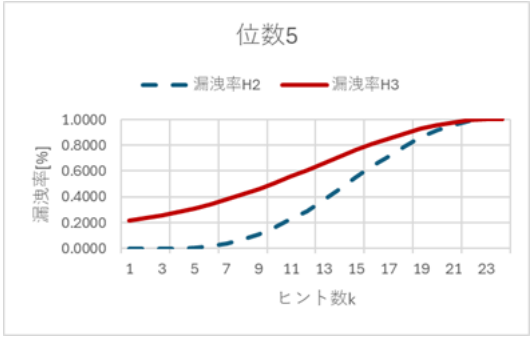
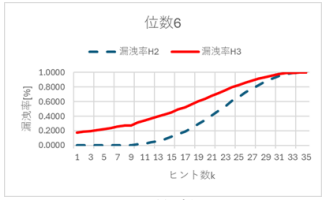


図 1　位数n=5 の情報漏洩率H_2, H_3

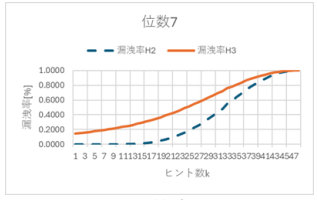
4.2 位数n = 6,7,8,9の場合の結果

本節では、位数n=6,7,8,9 に関する結果を述べる。ヒント数k[個]に対する情報漏洩率H_2, H_3 [%]を図 2 に示す。

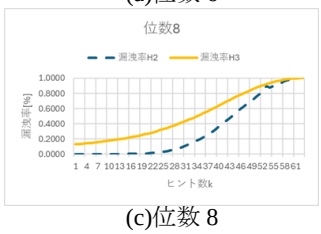
差分$H_3 - H_2$の最大値は、n=6 の場合 0.3384(k=15)、n=7 の場合 0.3331(k=23)、n=8 の場合 0.3279(k=33)、n=9 の場合 0.3247(k=44)であった。位数nの値が大きくなるほど、差分$H_3 - H_2$の最大値は減少していることがわかった。図 2 を見ると、位数nの値が大きくなるほど、情報漏洩率H_2, H_3 の差が縮まっていることがわかる。



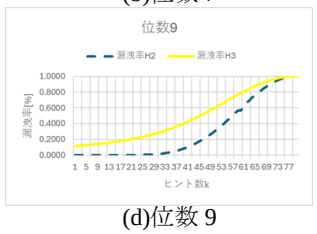
(a)位数 6



(b)位数 7



(c)位数 8



(d)位数 9

図 2　位数n=6,7,8,9 の情報漏洩率H_2, H_3

4.3 考察

本節では、情報漏洩率H_3について位数n=5,6,7,8,9 を比較する。位数nが異なるものを比較するために、図 3 では横軸にヒント数の割合k/n^2を取った。

位数nが小さい方がグラフは左に寄っており、情報漏洩率が高くなる。ヒント数の割合k/n^2 (横軸)に対する情報漏洩率H_3の上がり具合は、位数nが大きくなるほど緩やかになっている。この理由は、位数nが大きくなるほど、各セルの候補数が増え、一意に定まるセル数hの割合が相対的に減少するためである。

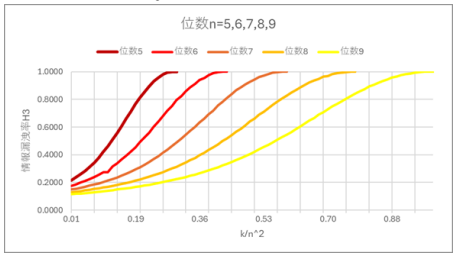


図 3　位数n=5,6,7,8,9 の情報漏洩率H_3

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] 八木康裕, 野沢友希, 沢瀬光, 足立智子, “部分ラテン方陣の特徴と秘密情報の漏洩”, 第 23 回情報科学技術フォーラム (FIT2024), 予稿集, no.1, pp.73-74, 2024.
[3] 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. (原著 : D. R. Stinson, “Cryptography : Theory and Practice” , CRC Press, Inc., 1995.).
[4] 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.