

一般アクセス構造を実現する秘密分散法の情報比の評価

日大生産工(院) ○伊藤詩子

日大生産工 柄窪孝也

1 まえがき

秘密分散法は、暗号で利用する鍵等の秘密情報を安全に保管するために利用されている。秘密情報を分散情報として複数の管理者に振り分けることにより、一部の振り分けられた分散情報が明らかになったとしても、元の情報を推測することが不可能なため情報の盗難・紛失対策に有効な技術である。秘密分散法の一方式である (k, n) しきい値法[1]では、 n 人の分散情報のうち、任意の k 人以上の管理者グループ(アクセス集合)のみ実現可能なため、非常に限定的な場合でしか使用できないことが分かる。そのため、アクセス構造を限定しない一般アクセス構造を実現する秘密分散法が提案されるが、どの手法も管理者に多くの分散情報を割り当てることで実現している。元の秘密情報と管理者が管理する分散情報とのサイズの比(情報比)に注目すると、 (k, n) しきい値法のように最適な秘密分散法の情報比は1であるが、それ以外の多くの場合は管理者がもつ分散情報は多いため情報比は小さくなり、効率が悪くなってしまふ。JacksonとMarinは5人以下の全ての管理者グループ180通りの情報比を明らかにしている[2]。

本稿では、1988年に提案されたBenalohとLeichterによる一般アクセス構造を実現する秘密分散法[3]と、アクセス構造を分割して、BenalohとLeichterの手法を複数回適用して情報比を改善可能にした秘密分散法[4]の2つを、それぞれ5人以下の管理者のすべての場合に適用し、情報比を評価する。

2 秘密分散法

(k, n) しきい値法では、秘密情報を n 個の分散情報に分割し、得られた分散情報を n 人の管理者で管理する。秘密情報を復元する場合、 n 人の管理者の中から任意の k 人が集まり、管理している分散情報を用いることで元の秘密情報の計算を行う。この手法では、任意の k 個の分散情報を集めることで元の秘密情報を復元す

ることが出来るが、 $k-1$ 個の分散情報では元の秘密情報に関する情報をまったく得ることが出来ないということ(完全性)を情報理論的に証明できる。

P を大きい素数とし、 (k, n) しきい値法の分散情報は、有限体 Z_P 上の $k-1$ 次多項式から得られる。 (k, n) しきい値法で実現可能なアクセス構造 Γ は、 $\Gamma = \{A \subset Z_P : |A| \geq k\}$ である。

$\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ を n 人の管理者の集合とし、 $\mathcal{K}$ 、 $\mathcal{S}$ をそれぞれの秘密情報の集合、分散情報の集合とする。アクセス構造 $\Gamma(\subset Z_P)$ を秘密情報を復元できる権限をもつ $\mathcal{P}$ の部分集合と定義する。 Γ の極小元の集合を極小アクセス集合と呼び、 Γ_0 と表す。

完全秘密分散法の情報比 ρ と管理者 P_i の情報比は以下のように定義される。

$$\rho = \min\{\rho_i : 1 \leq i \leq n\}$$

$$\rho_i = \frac{\log|\mathcal{K}|}{\log|\mathcal{S}(P_i)|}$$

$\mathcal{S}(P_i)$ は P_i が受け取る可能性がある分散情報である。情報比は $\rho = 1$ が最適である。

$\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ 、 $K \in \mathcal{K}$ および Γ_0 に対し、BenalohとLeichterの手法(BL88)は以下の通りである[3]。

- (1) 極小アクセス構造 Γ_0 を $\Gamma_0 = \{A_1, A_2, \dots, A_m\}$ とし、すべての $A_i \in \Gamma_0$ に対し秘密 K に対する分散情報 $s_{i,1}, s_{i,2}, \dots, s_{i,|A_i|}$ を $(|A_i|, |A_i|)$ しきい値法で独立に求める($1 \leq i \leq m$)。
- (2) 各 $P \in A_i$ に対し、 $s_{i,1}, s_{i,2}, \dots, s_{i,|A_i|}$ から異なる分散情報を1つ割り当てる($1 \leq i \leq m$)。

例1. $\mathcal{P} = \{a, b, c, d, e\}$ とし、アクセス構造 $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$ を

$$\begin{aligned} A_1 &= \{a, b\} \\ A_2 &= \{a, c\} \\ A_3 &= \{b, c, d\} \\ A_4 &= \{a, d, e\} \end{aligned}$$

とする。

この場合、分散情報は以下のように割り当てられる。

- a: $s_{1,1}, s_{2,1}, s_{4,1}$
- b: $s_{1,2}, s_{3,1}$
- c: $s_{2,2}, s_{3,2}$
- d: $s_{3,3}, s_{4,2}$
- e: $s_{4,3}$

この例では管理者aに3個の分散情報が割り当てられており、情報比は1/3となる。

3 複数回適用可能な手法

$\mathcal{P} = \{P_1, P_2, \dots, P_n\}$, $K \in \mathcal{K}$, Γ_0 および $P' \in \mathcal{P}$ に対して、複数回適用可能な手法(IT16)は以下の通りである[4]。

- (1) $\Gamma_0^{(1)} = \{A \subset P - \{P'\} : A \cup \{P'\} \in \Gamma_0\}$ とし、 $\Gamma_0^{(1)} = \{A_1^{(1)}, A_2^{(1)}, \dots, A_l^{(1)}\}$ と表す。
- (2) $\Gamma_0^{(0)} = \Gamma_0 - \Gamma_0^{(1)}$ とし、 $\Gamma_0^{(0)} = \{A_1^{(0)}, A_2^{(0)}, \dots, A_m^{(0)}\}$ と表す。
- (3) (2,2)しきい値法により、秘密 K に対する2個の分散情報 w_1 と w_2 を求め、 w_2 を P' に割り当てる。
- (4) すべての $A_i^{(1)} \in \Gamma_0^{(1)}$ に対し、 $(|A_i^{(1)}|, |A_i^{(1)}|)$ しきい値法で秘密 w_1 に対する $|A_i^{(1)}|$ 個の分散情報 $s_{i,1}, s_{i,2}, \dots, s_{i,|A_i^{(1)}|}$ を独立に求め、各 $P \in A_i^{(1)}$ に対し、異なる分散情報を1つ割り当てる($1 \leq i \leq l$)。
- (5) すべての $A_i^{(0)} \in \Gamma_0^{(0)}$ に対し、 $(|A_i^{(0)}|, |A_i^{(0)}|)$ しきい値法で秘密 K に対する $|A_i^{(0)}|$ 個の分散情報 $s'_{i,1}, s'_{i,2}, \dots, s'_{i,|A_i^{(0)}|}$ を独立に求め、各 $P \in A_i^{(0)}$ に対し、異なる分散情報を1つ割り当てる($1 \leq i \leq m$)。

例 2. 例 1 と同じアクセス構造を IT16 で実現する。

- $P' = a$ の場合 $\Gamma_0^{(1)} = \{A_1^{(1)}, A_2^{(1)}, A_3^{(1)}\}$ 、 $\Gamma_0^{(0)} = \{A_1^{(0)}\}$ となる。ただし

$$A_1^{(1)} = \{b\}$$

$$A_2^{(1)} = \{c\}$$

$$A_3^{(1)} = \{d, e\}$$

$$A_1^{(0)} = \{b, c, d\}$$
 とする。
- (2,2)しきい値法により、秘密 K に対する2個の分散情報 w_1 と w_2 を求める。
- $A_1^{(1)} = \{b\} \in \Gamma_0^{(1)}$ に対し、 w_1 に対する1($= |A_1^{(1)}|$)個の分散情報 $s_{1,1}(= w_1)$ を求める。
- $A_2^{(1)} = \{c\} \in \Gamma_0^{(1)}$ に対し、 w_1 に対する1($= |A_2^{(1)}|$)個の分散情報 $s_{2,1}(= w_1)$ を求める。
- $A_3^{(1)} = \{d, e\} \in \Gamma_0^{(1)}$ に対し、(2,2)しきい値法で w_1 に対する2($= |A_3^{(1)}|$)個の分散情報

$s_{3,1}, s_{3,2}$ を求める。

- $A_1^{(0)} = \{b, c, d\} \in \Gamma_0^{(0)}$ に対し、(3,3)しきい値法で K に対する3($= |A_1^{(0)}|$)個の分散情報 $s'_{1,1}, s'_{1,2}, s'_{1,3}$ を求める。

この場合、分散情報は以下のように割り当てられる。

- a: w_2
- b: $s_{1,1}, s'_{1,1}$
- c: $s_{2,1}, s'_{1,2}$
- d: $s_{3,1}, s'_{1,3}$
- e: $s_{3,2}$

例2では1/2という情報比が得られる。例1、2のアクセス構造の情報比の上限は3/5である。得られた値を比較すると情報比の上限には及ばないが、IT16はBL88より良い情報比を得ることが出来る。

4 情報比の評価

JacksonとMarinによって明らかにされた5人以下の管理者グループ180通りの情報比と、それにBL88とIT16を適用し、まとめたものが付録1である。結果としてIT16は任意のアクセス構造に対し、BL88に比べ高い情報比を得る。しかし情報比の上限と比較すると同等かそれ以下の効率の悪い情報比となっている。付録1の63番のアクセス構造を例にIT16の改良を考える。グラフ構造の同型を利用し $a \cong e$ とし、63番から e を含む極小元の集合を除くと $\{a, b\}, \{a, c\}, \{a, d\}$ となる。 $P' = a$ としてIT16を適用すると、このアクセス構造では情報比を1/2から1と改善することができる。

参考文献

- [1] A. Shamir, "How to share a secret," *Commun. ACM*, vol.22, no.11, pp.612-613, 1979.
- [2] Wen-Ai Jackson and Keith M. Marin, "Perfect Secret Sharing Schemes on Five Participants," *Designs, Codes and Cryptography*, 9, pp.267-286, 1996.
- [3] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," *Proc. CRYPTO'88*, pp.27-35, 1988.
- [4] 伊藤詩子, 梶窪孝也, "極小アクセス集合に基づく秘密分散法の情報比", 電子情報通信学会基礎・境界ソサイエティ/NOLTAソサイエティ大会講演論文集, pp.104, 2016.
- [5] D. R. Stinson, *Cryptography: Theory and practice*, CRC Press, 2005.

付録1 5人以下のアクセス構造の情報比(値が2つ並んでいるものは、情報比の上限の範囲を表す)

		情報比の上限	BL88	IT16
1	a + b + c + d + e	1	1	1
2	a + b + c + de	1	1	1
3	a + b + cd + ce	1	1/2	1
4	a + b + cd + ce + de	1	1/2	1
5	a + b + cde	1	1	1
6	a + bc + bd + cd + be	2/3	1/3	1/2
7	a + bc + bd + cd + be + ce	1	1/3	1/2
8	a + bc + bd + cd + be + ce + de	1	1/3	1/2
9	a + bc + bd + be	1	1/3	1
10	a + bc + bd + be + cde	2/3	1/3	1/2
11	a + bc + bd + ce	2/3	1/2	1/2
12	a + bc + bd + ce + de	1	1/2	1/2
13	a + bc + bd + cde	2/3	1/2	1/2
14	a + bc + de	1	1	1
15	a + bc + bde	1	1/2	1/2
16	a + bc + bde + cde	1	1/2	1/2
17	a + bcd + bce	1	1/2	1
18	a + bcd + bce + bde	1	1/3	1
19	a + bcd + bce + bde + cde	1	1/3	1/2
20	a + bcde	1	1	1
21	ab + ac + bc + ad + bd + cd + ae	2/3	1/4	1/2
22	ab + ac + bc + ad + bd + cd + ae + be	2/3	1/4	1/3
23	ab + ac + bc + ad + bd + cd + ae + be + ce	1	1/4	1/3
24	ab + ac + bc + ad + bd + cd + ae + be + ce + de	1	1/4	1/2
25	ab + ac + bc + ad + bd + ae	2/3	1/4	1/2
26	ab + ac + bc + ad + bd + ae + be	1	1/4	1/2
27	ab + ac + bc + ad + bd + ae + be + cde	2/3	1/4	1/3
28	ab + ac + bc + ad + bd + ae + ce	2/3	1/4	1/3
29	ab + ac + bc + ad + bd + ae + ce + de	1	1/2	1/2
30	ab + ac + bc + ad + bd + ae + cde	3/5 2/3	1/4	1/3
31	ab + ac + bc + ad + bd + ce	2/3	1/3	1/3
32	ab + ac + bc + ad + bd + ce + de	2/3	1/3	1/2
33	ab + ac + bc + ad + bd + cde	2/3	1/3	1/3
34	ab + ac + bc + ad + ae	2/3	1/4	1/2
35	ab + ac + bc + ad + ae + de	2/3	1/4	1/2
36	ab + ac + bc + ad + ae + bde	2/3	1/4	1/2
37	ab + ac + bc + ad + ae + bde + cde	2/3	1/4	1/3
38	ab + ac + bc + ad + be	2/3	1/3	1/2
39	ab + ac + bc + ad + be + de	2/3	1/3	1/2
40	ab + ac + bc + ad + be + cde	7/12 2/3	1/3	1/3
41	ab + ac + bc + ad + de	2/3	1/3	1/3
42	ab + ac + bc + ad + bde	2/3	1/3	1/2
43	ab + ac + bc + ad + bde + cde	2/3	1/3	1/3
44	ab + ac + bc + de	1	1/2	1/2
45	ab + ac + bc + ade	2/3	1/3	1/2
46	ab + ac + bc + ade + bde	1	1/3	1/2
47	ab + ac + bc + ade + bde + cde	1	1/3	1/3
48	ab + ac + ad + bcd + ae	3/5	1/4	1/2
49	ab + ac + ad + bcd + ae + bce	2/3	1/4	1/2
50	ab + ac + ad + bcd + ae + bce + bde	2/3	1/4	1/2
51	ab + ac + ad + bcd + ae + bce + bde + cde	2/3	1/4	1/3
52	ab + ac + ad + bcd + be	2/3	1/3	1/2
53	ab + ac + ad + bcd + be + ce	3/5 2/3	1/3	1/3
54	ab + ac + ad + bcd + be + ce + de	2/3	1/3	1/2
55	ab + ac + ad + bcd + be + cde	2/3	1/3	1/3
56	ab + ac + ad + bcd + bce	3/5	1/3	1/2
57	ab + ac + ad + bcd + bce + bde	2/3	1/3	1/2
58	ab + ac + ad + bcd + bce + bde + cde	2/3	1/4	1/3
59	ab + ac + ad + ae	1	1/4	1
60	ab + ac + ad + ae + bcde	2/3	1/3	1/2
61	ab + ac + ad + be	2/3	1/3	1/2
62	ab + ac + ad + be + ce	2/3	1/3	1/2
63	ab + ac + ad + be + ce + de	1	1/3	1/2
64	ab + ac + ad + be + cde	2/3	1/3	1/2
65	ab + ac + ad + bce	3/5	1/3	1/2
66	ab + ac + ad + bce + bde + cde	2/3	1/3	1/3
67	ab + ac + ad + bce + bde	2/3	1/3	1/2
68	ab + ac + ad + bcde	3/5	1/3	1/2
69	ab + ac + bd + cd + bce	2/3	1/3	1/2
70	ab + ac + bd + cd + bce + ade	2/3	1/3	1/3
71	ab + ac + bd + ce	2/3	1/2	1/2
72	ab + ac + bd + ce + de	2/3	1/2	1/2
73	ab + ac + bd + ce + ade	3/5 2/3	1/3	1/2
74	ab + ac + bd + bce	3/5	1/3	1/2
75	ab + ac + bd + bce + ade	2/3	1/3	1/2
76	ab + ac + bd + bce + ade + cde	2/3	1/3	1/3
77	ab + ac + bd + bcd + cde	2/3	1/3	1/3
78	ab + ac + bd + cde	2/3	1/2	1/2
79	ab + ac + bcd + bce	2/3	1/3	1/2
80	ab + ac + bcd + bce + de	2/3	1/3	1/2
81	ab + ac + bcd + bce + ade	3/5	1/3	1/2
82	ab + ac + bcd + bce + ade + bde	3/5 2/3	1/3	1/2
83	ab + ac + bcd + bce + ade + bde + cde	2/3	1/4	1/2
84	ab + ac + bcd + bce + bde	3/5	1/4	1/2
85	ab + ac + bcd + bce + bde + cde	2/3	1/4	1/2
86	ab + ac + bcd + de	2/3	1/2	1/2
87	ab + ac + bcd + ade	3/5	1/3	1/2
88	ab + ac + bcd + ade + bde	2/3	1/3	1/2
89	ab + ac + bcd + ade + bde + cde	2/3	1/3	1/2
90	ab + ac + bcd + bde	3/5	1/3	1/2
91	ab + ac + bcd + bde + cde	2/3	1/3	1/2
92	ab + ac + de	1	1/2	1
93	ab + ac + ade	1	1/3	1

		情報比の上限	BL88	IT16
94	ab + ac + ade + bde	2/3	1/3	1/2
95	ab + ac + ade + bde + cde	1	1/3	1/2
96	ab + ac + ade + bcde	2/3	1/3	1/2
97	ab + ac + bde	2/3	1/2	1/2
98	ab + ac + bde + cde	1	1/2	1/2
99	ab + ac + bcde	2/3	1/2	1/2
100	ab + cd + ace	2/3	1/2	1/2
101	ab + cd + ace + bce	2/3	1/2	1/2
102	ab + cd + ace + bce + ade	1	1/3	1/2
103	ab + cd + ace + bce + ade + bde	1	1/3	1/3
104	ab + cd + ace + bde	1	1/2	1/2
105	ab + acd + bcd + ace	5/6	1/3	1/2
106	ab + acd + bcd + ace + bce	1	1/3	1/2
107	ab + acd + bcd + ace + bce + ade	3/5 2/3	1/4	1/2
108	ab + acd + bcd + ace + bce + ade + bde	1	1/4	1/2
109	ab + acd + bcd + ace + bce + ade + bde + cde	1	1/4	1/3
110	ab + acd + bcd + ace + bce + ade + cde	1	1/4	1/3
111	ab + acd + bcd + ace + bce + cde	2/3	1/3	1/2
112	ab + acd + bcd + ace + ade	2/3	1/4	1/2
113	ab + acd + bcd + ace + ade + cde	2/3	1/4	1/2
114	ab + acd + bcd + ace + bde	3/5	1/3	1/2
115	ab + acd + bcd + ace + bde + cde	1	1/4	1/2
116	ab + acd + bcd + ace + cde	2/3	1/4	1/2
117	ab + acd + bcd + cde	3/5	1/3	1/2
118	ab + acd + ace	1	1/3	1
119	ab + acd + ace + ade	1	1/4	1
120	ab + acd + ace + ade + cde	2/3	1/4	1/2
121	ab + acd + ace + ade + bcde	2/3	1/4	1/2
122	ab + acd + ace + bde	2/3	1/3	1/2
123	ab + acd + ace + bde + cde	2/3	1/3	1/2
124	ab + acd + ace + cde	2/3	1/3	1/2
125	ab + acd + ace + bcde	2/3	1/3	1/2
126	ab + acd + bce	2/3	1/2	1/2
127	ab + acd + bce + cde	2/3	1/3	1/2
128	ab + acd + cde	2/3	1/2	1/2
129	ab + acd + bcde	2/3	1/2	1/2
130	ab + cde	1	1	1
131	ab + acde	1	1	1
132	ab + acde + bcde	1	1/2	1/2
133	abc + abd + acd + bcd + abe	3/5	1/2	1/2
134	abc + abd + acd + bcd + abe + ace	2/3	1/4	1/2
135	abc + abd + acd + bcd + abe + ace + bce	1	1/5	1/2
136	abc + abd + acd + bcd + abe + ace + bce + ade	2/3	1/6	1/2
137	abc + abd + acd + bcd + abe + ace + bce + ade + bde	1	1/6	1/2
138	abc + abd + acd + bcd + abe + ace + bce + ade + bde + cde	1	1/6	1/3
139	abc + abd + acd + bcd + abe + ace + ade	2/3	1/6	1/2
140	abc + abd + acd + bcd + abe + ace + bde	3/5	1/5	1/2
141	abc + abd + acd + bcd + abe + ace + bde + cde	1	1/5	1/2
142	abc + abd + acd + bcd + abe + cde	3/5	1/4	1/3
143	abc + abd + acd + abe	2/3	1/4	1/2
144	abc + abd + acd + abe + ace	1	1/5	1
145	abc + abd + acd + abe + ace + ade	1	1/6	1
146	abc + abd + acd + abe + ace + ade + bcde	2/3	1/6	1/2
147	abc + abd + acd + abe + ace + bde	3/5	1/5	1/2
148	abc + abd + acd + abe + ace + bde + cde	2/3	1/5	1/2
149	abc + abd + acd + abe + ace + bcde	2/3	1/5	1/2
150	abc + abd + acd + abe + bce	3/5	1/4	1/2
151	abc + abd + acd + abe + bce + cde	3/5 2/3	1/4	1/2
152	abc + abd + acd + abe + cde	3/5 2/3	1/4	1/2
153	abc + abd + acd + abe + bcde	3/5	1/4	1/2
154	abc + abd + acd + bce	2/3	1/3	1/2
155	abc + abd + acd + bce + bde	2/3	1/4	1/2
156	abc + abd + acd + bce + bde + cde	1	1/4	1/2
157	abc + abd + acd + bcde	2/3	1/3	1/2
158	abc + abd + abe	1	1/3	1/2
159	abc + abd + abe + cde	3/5	1/3	1/2
160	abc + abd + abe + acde	2/3	1/4	1/2
161	abc + abd + abe + acde + bcde	3/5	1/4	1/2
162	abc + abd + ace	2/3	1/3	1/2
163	abc + abd + ace + ade	1	1/4	1/2
164	abc + abd + ace + ade + bcde	2/3	1/4	1/2
165	abc + abd + ace + bde	3/5	1/3	1/2
166	abc + abd + ace + bde + cde	2/3	1/3	1/3
167	abc + abd + ace + bcde	3/5	1/3	1/2
168	abc + abd + cde	3/5	1/3	1/2
169	abc + abd + acde	2/3	1/3	1/2
170	abc + abd + ace + acde + bcde	3/5	1/4	1/3
171	abc + ade	1	1/2	1/2
172	abc + ade + bcde	1	1/2	1/2
173	abc + abde	1	1/2	1
174	abc + abde + acde	1	1/3	1
175	abc + abde + acde + bcde	1	1/3	1/2
176	abcd + abce	1	1/2	1
177	abcd + abce + abde	1	1/3	1
178	abcd + abce + abde + acde	1	1/4	1/2
179	abcd + abce + abde + acde + bcde	1	1/4	1/2
180	abcde	1	1	1