

再帰的に適用可能な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。1987年に伊藤、斉藤、西関は極大非アクセス集合に基づくアクセス構造を限定しない秘密分散法(一般アクセス構造を実現する秘密分散法)を提案している[2]。また、1988年にBenalohとLeichterも極小アクセス集合に基づく一般アクセス構造を実現する手法を提案している[3]。これらの手法は、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、一般アクセス構造を実現する手法の場合は、管理者がもつ分散情報が多くなるため情報比は小さくなり、効率が悪くなってしまう。

本稿では、伊藤、斉藤、西関の手法(ISN87)とBenalohとLeichterによる手法(BL88)、そして、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(IT16)[4]をJacksonとMarinが明らかにした5人以下の全ての管理者グループ180通りのアクセス構造[5]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、 $\Gamma = \{A \subset 2^P : |A| \geq k\}$ 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 $\Gamma(\subset 2^P)$ 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。また、 $\bar{\Gamma} = 2^P - \Gamma$ と定義し、 $\bar{\Gamma}_1$ を $\bar{\Gamma}$ の極大元の集合とする。

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。

3. 伊藤、斉藤、西関の手法

$\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ 、 $K \in \mathcal{K}$ および Γ_0 に対し、伊藤、斉藤、西関の手法(ISN87)は以下の通りである[2]。

- (1) 極小アクセス構造 Γ_0 を $\Gamma_0 = \{A_1, A_2, \dots, A_m\}$ とし極大非アクセス構造を $\bar{\Gamma}_1 = \{B_1, B_2, \dots, B_t\}$ とする。
- (2) 秘密 K に対して、 (t, t) しきい値法により分散情報 $S = \{w_1, \dots, w_t\}$ を求める。
- (3) 各管理人 P_i に対し、関数 $g: \mathcal{P} \rightarrow 2^S$ により分散情報を以下のように割り当てる。

$$g(P_i) = \{w_j : P_i \notin B_j \in \bar{\Gamma}_1, 1 \leq j \leq t\}$$

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。

- このとき極大非アクセス構造は $\bar{\Gamma}_1 = \{B_1, B_2, B_3, B_4, B_5\}$ となる。ただし、
 $B_1 = \{a, d\}$
 $B_2 = \{a, e\}$
 $B_3 = \{b, c, e\}$
 $B_4 = \{b, d, e\}$
 $B_5 = \{c, d, e\}$
 である。
- 得られた $\bar{\Gamma}_1$ に対応して $S = \{w_1, w_2, w_3, w_4, w_5\}$ を (5,5) しきい値法により求める。
- 関数 g より、分散情報は以下のように割り当てられる。
 $a: w_3, w_4, w_5$
 $b: w_1, w_2, w_5$
 $c: w_1, w_2, w_4$
 $d: w_2, w_3$
 $e: w_1$

この例では管理者 a, b, c 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。

4. BenalohとLeichterの手法

$\mathcal{P} = \{P_1, P_2, \dots, P_n\}$, $K \in \mathcal{K}$ 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2. 例1と同じアクセス構造でBL88を実現する。 A_i に対して、秘密 K に対するそれぞれの $|A_i|$ 個の分散情報を求める。このとき、分散情報は以下のように割り当てられる ($1 \leq i \leq 4$)。

$$\begin{aligned} a: & s_{1,1}, s_{2,1}, s_{4,1} \\ b: & s_{1,2}, s_{3,1} \\ c: & s_{2,2}, s_{3,2} \\ d: & s_{3,3}, s_{4,2} \\ e: & s_{4,3} \end{aligned}$$

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。

5. 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 ($1 \leq i \leq m$)。

なお、IT16 は $\Gamma_0^{(1)}$ と $\Gamma_0^{(0)}$ に対して再帰的にIT16を適用することができる。

例3. 例1と同じアクセス構造でIT16を実現する。

- $P' = a$ 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

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 3 では管理者b、c、dに2個の分散情報が割り当てられており、情報比は1/2となる。

例 1 から例 3 の結果をまとめたものが表 1 となる。

表1.各手法による結果

	IT16	BL88	ISN88
a	w_2	$s_{1,1}, s_{2,1}, s_{4,1}$	w_3, w_4, w_5
b	$s_{1,1}, s'_{1,1}$	$s_{1,2}, s_{3,1}$	w_1, w_2, w_5
c	$s_{2,1}, s'_{1,2}$	$s_{2,2}, s_{3,2}$	w_1, w_2, w_4
d	$s_{3,1}, s'_{1,3}$	$s_{3,3}, s_{4,2}$	w_2, w_3
e	$s_{3,2}$	$s_{4,3}$	w_1

BL88とISN88では情報比が1/3であるが、IT16では情報比が1/2となり情報比が改善されていることが分かる。

6. 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通りに、BL88、ISN87、IT16さらに、IT16を再帰的に複数回適用した手法(IT16_複)を適用し、得られた情報比をまとめたものが付録1である。その結果からBL88とISN87に関する結果をまとめたのが表2、IT16、IT16_複、BL88との比較の結果をまとめたのが表3、IT16_複とISN87との比較の結果をまとめたものが表4である。

表2.BL88とISN87の情報比の比較

	アクセス構造数
BL88の方がISN87より情報比が高い	57
BL88とISN87の情報比が等しい	66
ISN87の方がBL88より情報比が高い	57

表2の結果から情報比がBL88の方が高かったアクセス構造とISN87の方が高かったアクセス構造は同じ数となった。また情報比が等しくなったものは66となった。この結果から

BL88とISN87ではアクセス構造によっては手法を使い分ける方がよいことがわかる。

表3.IT16_複、IT16、BL88の情報比の比較

	アクセス構造数
IT16_複の方がIT16より情報比が高い	78
IT16_複とIT16の情報比が等しい	102
IT16の方がBL88より情報比が高い	72
IT16とBL88の情報比が等しい	108

表3の結果からIT16とIT16_複は多くのアクセス構造で情報比を改善できることがわかる。

表4. IT16_複とISN87の情報比の比較

	アクセス構造数
IT16_複の方がISN87より情報比が高い	127
IT16_複とISN87の情報比が等しい	47
ISN87の方がIT16_複より情報比が高い	6

表4から多くのアクセス構造でIT16_複はISN87よりも効率がよいことがわかる。なお、グラフ構造の同型を利用することで極小元の集合を除きIT16を適用すると情報比をさらに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] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure", *Proceedings of IEEE Global Telecommunications Conference, Globecom87*, pp.99-102, 1987.
- [3] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," *Proc. CRYPTO'88*, pp.27-35, 1988.
- [4] 伊藤詩子, 柝窪孝也, "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] Wen-Ai Jackson and Keith M. Marin, "Perfect secret sharing schemes on five participants," *Designs, Codes and Cryptography*, 9, pp.267-286, 1996.

付録1. 5人以下の情報比

	アクセス構造	BL88	IT16	IT16 変	ISN87
1	a + b + c + d + e	1	1	1	1
2	a + b + c + d	1	1	1	2
3	a + b + c + d + e	2	1	1	2
4	a + b + c + d + e + d	2	2	2	3
5	a + b + c + d	1	1	1	3
6	a + b + c + d + e + b	3	2	2	3
7	a + b + c + d + e + c	3	3	2	3
8	a + b + c + d + e + c + d	3	3	3	4
9	a + b + c + d + e	3	1	1	2
10	a + b + c + d + e + c + d	3	2	2	4
11	a + b + c + d + e	2	2	2	3
12	a + b + c + d + e + c + d	2	2	2	2
13	a + b + c + d + e	2	2	2	4
14	a + b + c + d	1	1	1	4
15	a + b + c + d	2	1	1	3
16	a + b + c + d + e + c + d	2	2	2	5
17	a + b + c + d	2	2	1	3
18	a + b + c + d + e + b + d	3	2	2	4
19	a + b + c + d + e + b + d + c	3	3	3	6
20	a + b + c + d	1	1	1	4
21	a + b + c + d + e + b + d + c + a	4	3	3	3
22	a + b + c + d + e + b + d + c + a + b	4	4	3	3
23	a + b + c + d + e + b + d + c + a + b + c	4	4	3	3
24	a + b + c + d + e + b + d + c + a + b + c + d	4	4	4	4
25	a + b + c + d + e + b + d + a	4	3	2	2
26	a + b + c + d + e + b + d + a + b	4	4	2	2
27	a + b + c + d + e + b + d + a + b + c	4	4	3	4
28	a + b + c + d + e + b + d + a + b + c	4	3	3	3
29	a + b + c + d + e + b + d + a + b + c + d	4	3	3	2
30	a + b + c + d + e + b + d + a + b + c + d	4	3	3	4
31	a + b + c + d + e + b + d + c	3	3	3	3
32	a + b + c + d + e + b + d + c + d	3	3	3	2
33	a + b + c + d + e + b + d + c + d	3	3	3	4
34	a + b + c + d + e + a	4	2	2	2
35	a + b + c + d + e + a + d	4	2	2	4
36	a + b + c + d + e + a + d + b	4	3	2	3
37	a + b + c + d + e + a + d + b + c	4	3	3	5
38	a + b + c + d + e + a + b	3	3	2	2
39	a + b + c + d + e + a + b + d	3	3	2	3
40	a + b + c + d + e + a + b + d + c	3	3	3	4
41	a + b + c + d + e + a + d	3	2	2	4
42	a + b + c + d + e + a + d + b	3	3	2	3
43	a + b + c + d + e + a + d + b + c	3	3	3	5
44	a + b + c + d + e	2	2	2	4
45	a + b + c + d + e	3	2	2	3
46	a + b + c + d + e + b + d	3	3	2	4
47	a + b + c + d + e + b + d + c	3	3	3	5
48	a + b + c + d + e + b + d + a	4	2	2	3
49	a + b + c + d + e + b + d + a + b	4	3	2	3
50	a + b + c + d + e + b + d + a + b + c	4	4	3	4
51	a + b + c + d + e + b + d + a + b + c + d	4	4	4	6
52	a + b + c + d + e + b + d + c	3	3	2	3
53	a + b + c + d + e + b + d + c + b	3	3	3	4
54	a + b + c + d + e + b + d + c + b + c	3	3	3	3
55	a + b + c + d + e + b + d + c + b + c + d	3	3	3	5
56	a + b + c + d + e + b + d + c + b	3	3	2	3
57	a + b + c + d + e + b + d + c + b + d	4	3	3	4
58	a + b + c + d + e + b + d + c + b + d + c	4	4	3	6
59	a + b + c + d + e + a	4	1	1	1
60	a + b + c + d + e + a + b + c	4	2	2	4
61	a + b + c + d + e + a + b	3	2	2	2
62	a + b + c + d + e + a + b + c	3	2	2	2
63	a + b + c + d + e + a + b + c + d	3	3	2	1
64	a + b + c + d + e + a + b + c + d	3	2	2	3
65	a + b + c + d + e + a + b + c	3	2	2	3
66	a + b + c + d + e + a + b + c + d	3	3	2	3
67	a + b + c + d + e + a + b + c + d + c	3	3	3	4
68	a + b + c + d + e + a + b + c + d	3	2	2	4
69	a + b + c + d + e + a + b + c + d	3	3	2	3
70	a + b + c + d + e + a + b + c + d + e	3	3	3	4
71	a + b + c + d + e + a + b + c	2	2	2	3
72	a + b + c + d + e + a + b + c + d	2	2	2	3
73	a + b + c + d + e + a + b + c + d + e	3	2	2	4
74	a + b + c + d + e + a + b + c	3	2	2	3
75	a + b + c + d + e + a + b + c + d	3	3	2	3
76	a + b + c + d + e + a + b + c + d + e	3	3	3	5
77	a + b + c + d + e + a + b + c + d	3	3	2	4
78	a + b + c + d + e + a + b + c + d	2	2	2	2
79	a + b + c + d + e + a + b + c + d	3	3	2	3
80	a + b + c + d + e + a + b + c + d + e	3	3	2	5
81	a + b + c + d + e + a + b + c + d + e	3	3	2	3
82	a + b + c + d + e + a + b + c + d + e + b	4	3	3	4
83	a + b + c + d + e + a + b + c + d + e + b + c	4	4	3	6
84	a + b + c + d + e + a + b + c + d + e + b	4	3	2	4
85	a + b + c + d + e + a + b + c + d + e + b + c	4	4	3	5
86	a + b + c + d + e + a + b + c + d + e	2	2	2	3
87	a + b + c + d + e + a + b + c + d + e	3	2	2	3
88	a + b + c + d + e + a + b + c + d + e + b	3	3	2	3
89	a + b + c + d + e + a + b + c + d + e + b + c	4	3	3	4
90	a + b + c + d + e + a + b + c + d + e	3	2	2	3

	アクセス構造	BL88	IT16	IT16 変	ISN87
91	a + b + c + d + e + b + c + d + e	3	3	2	3
92	a + b + c + d + e	2	1	1	2
93	a + b + c + d + e	3	1	1	2
94	a + b + c + d + e + b + d	3	2	2	3
95	a + b + c + d + e + b + d + c + d	3	3	2	3
96	a + b + c + d + e + b + d + c	3	2	2	4
97	a + b + c + d + e	2	2	2	3
98	a + b + c + d + e + c + d	2	2	2	2
99	a + b + c + d + e	2	2	2	4
100	a + b + c + d + e	2	2	2	2
101	a + b + c + d + e + b + c	3	2	2	3
102	a + b + c + d + e + b + c + d + e	3	3	2	4
103	a + b + c + d + e + b + c + d + e + b + d	4	3	3	5
104	a + b + c + d + e + b + d	2	2	2	2
105	a + b + c + d + e + b + c + d + e	3	3	2	3
106	a + b + c + d + e + b + c + d + e	4	3	2	3
107	a + b + c + d + e + b + c + d + e	4	4	3	4
108	a + b + c + d + e + b + c + d + e + b + d	4	4	3	4
109	a + b + c + d + e + b + c + d + e + b + d + c + d	5	5	4	6
110	a + b + c + d + e + b + c + d + e + b + d + c + d	5	4	3	5
111	a + b + c + d + e + b + c + d + e + b + c + d + e	5	3	3	4
112	a + b + c + d + e + b + c + d + e + b + c + d + e	4	3	3	4
113	a + b + c + d + e + b + c + d + e + b + c + d + e	4	4	3	4
114	a + b + c + d + e + b + c + d + e + b + d	3	3	2	3
115	a + b + c + d + e + b + c + d + e + b + d + c + d	4	4	3	3
116	a + b + c + d + e + b + c + d + e + b + c + d + e	4	3	2	3
117	a + b + c + d + e + b + c + d + e	3	3	2	3
118	a + b + c + d + e + a	3	2	1	2
119	a + b + c + d + e + a + d + e	4	2	2	3
120	a + b + c + d + e + a + d + e + c + d	4	3	3	3
121	a + b + c + d + e + a + d + e + b + c + d	4	3	3	4
122	a + b + c + d + e + a + d + e + b + d	3	2	2	3
123	a + b + c + d + e + a + d + e + b + d + c + d	3	3	2	2
124	a + b + c + d + e + a + d + e	3	3	2	3
125	a + b + c + d + e + a + d + e + b + c + d	3	3	2	4
126	a + b + c + d + e + a + d + e + b + c	2	2	2	3
127	a + b + c + d + e + a + d + e + b + c + d	3	2	2	2
128	a + b + c + d + e + a + d + e	2	2	2	3
129	a + b + c + d + e + a + d + e + b + c + d	2	2	2	4
130	a + b + c + d + e	1	1	1	3
131	a + b + c + d + e	2	1	1	3
132	a + b + c + d + e + b + c + d	2	2	2	4
133	a + b + c + d + e + b + c + d + a + b	4	4	3	3
134	a + b + c + d + e + b + c + d + a + b + c + e	5	4	3	3
135	a + b + c + d + e + b + c + d + a + b + c + e	5	5	3	3
136	a + b + c + d + e + b + c + d + a + b + c + e + d + e	6	5	4	4
137	a + b + c + d + e + b + c + d + a + b + c + e + d + e + b + d	6	6	4	5
138	a + b + c + d + e + b + c + d + a + b + c + e + d + e + b + d + c + d	6	6	5	6
139	a + b + c + d + e + b + c + d + a + b + c + e + d + e	6	4	3	4
140	a + b + c + d + e + b + c + d + a + b + c + e + d + e	5	5	3	3
141	a + b + c + d + e + b + c + d + a + b + c + e + d + e + c + d	5	5	4	4
142	a + b + c + d + e + b + c + d + a + b + c + d	4	4	3	3
143	a + b + c + d + e + b + c + d + a + b	4	3	2	2
144	a + b + c + d + e + b + c + d + a + b + c + e	5	3	2	2
145	a + b + c + d + e + b + c + d + a + b + c + e + d + e	6	3	3	3
146	a + b + c + d + e + b + c + d + a + b + c + e + d + e + b + c + d	6	4	4	4
147	a + b + c + d + e + b + c + d + a + b + c + e + d + e	5	4	3	3
148	a + b + c + d + e + b + c + d + a + b + c + e + d + e + c + d	5	4	3	3
149	a + b + c + d + e + b + c + d + a + b + c + e + d + e + b + c + d	5	4	3	4
150	a + b + c + d + e + b + c + d + a + b + c + e	4	4	3	3
151	a + b + c + d + e + b + c + d + a + b + c + e + c + d	4	4	3	3
152	a + b + c + d + e + b + c + d + a + b + c + d	4	3	2	3
153	a + b + c + d + e + b + c + d + a + b + c + d	4	4	3	4
154	a + b + c + d + e + b + c + d + a + b + c + d	3	3	2	3
155	a + b + c + d + e + b + c + d + a + b + c + d + e	4	3	3	3
156	a + b + c + d + e + b + c + d + a + b + c + d + e + c + d	4	4	3	2
157	a + b + c + d + e + b + c + d + a + b + c + d	3	3	3	4
158	a + b + c + d + e + a + b + c + d	3	3	1	1
159	a + b + c + d + e + a + b + c + d + e	3	3	2	3
160	a + b + c + d + e + a + b + c + d + e	4	3	2	3
161	a + b + c + d + e + a + b + c + d + e + b + c + d	4	4	3	4
162	a + b + c + d + e + a + b + c + d + e	3	2	2	2
163	a + b + c + d + e + a + b + c + d + e	4	2	2	1
164	a + b + c + d + e + a + b + c + d + e + b + c + d	4	3	3	4
165	a + b + c + d + e + a + b + c + d + e + b + c + d	3	3	2	3
166	a + b + c + d + e + a + b + c + d + e + b + c + d	3	3	3	2
167	a + b + c + d + e + a + b + c + d + e + b + c + d	3	3	2	4
168	a + b + c + d + e + a + b + c + d + e	2	2	2	3
169	a + b + c + d + e + a + b + c + d + e	3	2	2	3
170	a + b + c + d + e + a + b + c + d + e + b + c + d	3	3	2	4
171	a + b + c + d + e + a + b + c + d + e	2	1	1	2
172	a + b + c + d + e + a + b + c + d + e	2	2	2	4
173	a + b + c + d + e + a + b + c + d + e	2	2	1	2
174	a + b + c + d + e + a + b + c + d + e	3	2	2	3
175	a + b + c + d + e + a + b + c + d + e + b + c + d	3	3	3	4
176	a + b + c + d + e + a + b + c + d + e	2	2	1	1
177	a + b + c + d + e + a + b + c + d + e	3	3	2	2
178	a + b + c + d + e + a + b + c + d + e + b + c + d	4	3	3	3
179	a + b + c + d + e + a + b + c + d + e + b + c + d + e	4	4	4	4
180	a + b + c + d + e + a + b + c + d + e	1	1	1	1