6W-06

極小アクセス構造に基づく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

伊藤 詩子 †　　栃窪 孝也 ‡
† 日本大学大学院生産工学研究科数理情報工学専攻　　‡ 日本大学生産工学部数理情報工学科

1 はじめに

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う。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 (BL88) 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 1 回適用したものと複数回適用した場合の 3 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、情報比を評価した。

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。$\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ 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 $\Gamma(\subset 2^{\mathcal{P}})$ 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。(k,n) しきい値法で実現可能なアクセス構造 Γ は、$\Gamma = \{A \subset \mathcal{P} : |A| \geq k\}$ である。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。

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

(1) $\Gamma_0 = \{A_1, A_2, \cdots, A_m\}$ とし、すべての $A_i \in \Gamma_0$ に対し、秘密 K に対する $|A_i|$ 個の分散情報 $s_{i,1}, s_{i,2}, \cdots, s_{i,|A_i|}$ 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、$s_{i,1}, s_{i,2}, \cdots, s_{i,|A_i|}$ から異なる分散情報を 1 つ割り当てる $(1 \leq i \leq m)$。

例 1.
$\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5\}$ とし、$\Gamma_0 = \{A_1, A_2, A_3, A_4, A_5\}$ を

$$\begin{aligned} A_1 &= \{P_1, P_2\} \\ A_2 &= \{P_1, P_3, P_4\} \\ A_3 &= \{P_2, P_3, P_4\} \\ A_4 &= \{P_1, P_3, P_5\} \\ A_5 &= \{P_3, P_4, P_5\} \end{aligned}$$

とする。このとき、Benaloh と Leichter の手法 (BL88) を適用すると分散情報は以下のように割り当てられる。

$$\begin{aligned} P_1 &: s_{1,1},\ s_{2,1},\ s_{4,1} \\ P_2 &: s_{1,2},\ s_{3,1} \\ P_3 &: s_{2,2},\ s_{3,2},\ s_{4,2},\ s_{5,1} \\ P_4 &: s_{2,3},\ s_{3,3},\ s_{5,2} \\ P_5 &: s_{4,3},\ s_{5,3} \end{aligned}$$

3 IT16

$\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$、$K \in \mathcal{K}$、$\Gamma_0$ および $P' \in \mathcal{P}$ に対して、IT16 は以下の通りである [4]。

(1) $\Gamma_0^{(1)} = \{A \subset \mathcal{P} - \{P'\} : A \cup \{P'\} \in \Gamma_0\}$ とし、$\Gamma_0^{(1)} = \{A_1^{(1)}, A_2^{(1)}, \cdots, A_l^{(1)}\}$ と表す。

(2) $\Gamma_0^{(0)} = \Gamma_0 - \Gamma_0^{(1)}$ とし、$\Gamma_0^{(1)} = \{A_1^{(0)}, A_2^{(0)}, \cdots, A_m^{(0)}\}$ と表す。

Infomation Rates for Genera Secret Sharring Schemes Based on Authorized Subsets
†Utako Itoh, Nihon University
‡Koya Tochikubo, Nihon University

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.

(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 $s_{i,1}, s_{i,2}, \cdots, s_{i,|A_i^{(1)}|}$ 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 $|A_i^{(1)}|$ 個の分散情報 $s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|A_i^{(0)}|}$ 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.
$P' = P_3$ とし、例 1 と同じアクセス構造に対して IT16 を適用する。$\Gamma_0^{(1)} = \{A_1^{(1)}, A_2^{(1)}, A_3^{(1)}, A_4^{(1)}\}$、$\Gamma_0^{(0)} = \{A_1^{(0)}\}$ となる。ただし、

$$
\begin{aligned}
A_1^{(1)} &= \{P_1, P_4\} \\
A_2^{(1)} &= \{P_2, P_4\} \\
A_3^{(1)} &= \{P_1, P_5\} \\
A_4^{(1)} &= \{P_4, P_5\} \\
A_1^{(0)} &= \{P_1, P_2\}
\end{aligned}
$$

である。このとき分散情報は以下のように割り当てられる。

$$
\begin{aligned}
P_1 &: s_{1,1},\ s_{3,1},\ s'_{1,1} \\
P_2 &: s_{2,1},\ s'_{1,2} \\
P_3 &: w_2 \\
P_4 &: s_{1,2},\ s_{2,2},\ s_{4,1} \\
P_5 &: s_{3,2},\ s_{4,2}
\end{aligned}
$$

例 3.
例 1 と同じアクセス構造で IT16 を複数回適用する。例 2 では、$P' = P_3$ とし、Γ_0 を

$$
\begin{aligned}
\Gamma_0^{(1)} &= \{\{P_1, P_4\}, \{P_2, P_4\}, \{P_1, P_5\}, \{P_4, P_5\}\} \\
\Gamma_0^{(0)} &= \{\{P_1, P_2\}\}
\end{aligned}
$$

と分割している。$\Gamma_0^{(1)}$ に対し、$P'' = P_1$ として IT16 を適用すると、$\Gamma_0^{(1)}$ は、

$$
\begin{aligned}
\Gamma_0^{'(1)} &= \{\{P_4\}, \{P_5\}\} \\
\Gamma_0^{'(0)} &= \{\{P_2, P_4\}, \{P_4, P_5\}\}
\end{aligned}
$$

と分割できる。さらに、$\Gamma_0^{'(0)}$ に対し、$P''' = P_4$ として IT16 を適用すると、$\Gamma_0^{'(0)}$ は、

$$
\begin{aligned}
\Gamma_0^{''(1)} &= \{\{P_2\}, \{P_5\}\} \\
\Gamma_0^{''(0)} &= \phi
\end{aligned}
$$

と分割できる。この場合、分散情報は以下のように割り当てられる。

$$
\begin{aligned}
P_1 &: w'_2,\ s'_{1,1} \\
P_2 &: s'_{1,2},\ s'''_{1,1} \\
P_3 &: w_2 \\
P_4 &: w''_2,\ s''_{1,1} \\
P_5 &: s''_{2,1},\ s'''_{2,1}
\end{aligned}
$$

4 評価

Jackson と Marin によって明らかにされた 5 人以下の管理者の 180 通りのアクセス構造に対し、BL88、IT16 を 1 回適用したもの (IT16-1)、IT16 を複数回適用したもの (IT16-複) の 3 通りで情報比を評価した (表 1)。IT16-1 は、70 のアクセス構造で BL88 よりも高い情報比を得ることができた。IT16-複は、127 アクセス構造で BL88 よりも高い情報比を得ることができ、72 のアクセス構造で IT16-1 よりも高い情報比を得ることができた。

表 1: 情報比を改善できたアクセス構造の個数

	BL88 より改善	IT16-1 より改善
IT16-1	70	-
IT16-複	127	72

5 まとめ

本稿では、5 人以下の管理者の 180 通りのアクセス構造に対して、BL88、IT16 を 1 回適用したもの (IT16-1)、IT16 を複数回適用したもの (IT16-複) の 3 通りで情報比を評価した。その結果 IT16 を複数回行うと BL88 に比べ 127 個のアクセス構造で情報比が改善され、IT16 を一回行うよりも 72 個のアクセス構造で情報比が改善された。

謝辞 本研究は JSPS 科研費 15K00192 の助成を受けたものです。

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, “Genera-lized secret sharing and monotone functions,” Proc. CRYPTO ’88, pp.27-35, 1988.

[4] 伊藤 詩子, 栃窪 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.

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.