Journal of Information Processing Vol.24 No.5 772–780 (Sep. 2016)

[DOI: 10.2197/ipsjjip.24.772]

Regular Paper

New General Secret Sharing Scheme Based on Unauthorized Subsets: Improvement of Information Rates for Specified Participants

Kouya Tochikubo[1,a)]

Received: December 3, 2015, Accepted: June 2, 2016

Abstract: We propose a new secret sharing scheme realizing general access structures, which is based on unauthorized subsets. In the proposed scheme, we can select a subset of participants without restrictions and reduce the number of shares distributed to any participant who belongs to the selected subset.

Keywords: (k, n)-threshold scheme, secret sharing scheme, general access structure

1. Introduction

In 1979, Blakley and Shamir independently introduced the concept of secret sharing [1], [2]. In Shamir's (k, n)-threshold scheme [1], every group of k participants can recover the secret K, but no group of less than k participants can get any information about the secret from their shares. The collection of all authorized subsets of participants is called the access structure. A (k, n)-threshold scheme can only realize particular access structures that contain all subsets of k or more participants. Secret sharing schemes realizing more general access structures than that of a threshold scheme were studied by numerous authors. Koyama proposed secret sharing schemes for multi-groups [3]. Simmons studied secret sharing schemes realizing multilevel access structures [4], [5]. Subsequently, Tassa proposed a hierarchical threshold scheme [6]. Dijk generalized the vector space construction by Brickell [7] and proposed the linear construction [8]. Stinson proposed the decomposition construction [9]. These schemes obtain the optimal information rates for some access structures, but these schemes cannot be applied to many access structures or do not have explicit share assignment algorithms for many access structures.

On the other hand, Ito, Saito and Nishizeki proposed a secret sharing scheme for general access structures and showed an explicit share assignment algorithm for any access structure [10]. Secret sharing schemes which have an explicit assignment algorithm for any access structure are categorized by three types. One type is schemes based on unauthorized subsets [10], [11], [12]. Another type is schemes based on authorized subsets [13], [14], [15]. Yet another type is a scheme based on both unauthorized subsets and authorized subsets (IYO07) [16].

In the implementation of secret sharing schemes for general access structures, an important issue is the number of shares distributed to each participant. Obviously, a scheme constructed of small shares is desirable. However, in general, the proposed secret sharing schemes for general access structures are impractical in this respect when the size of the access structure is very large.

Suppose that we want to apply secret sharing schemes to a company. Here, we consider a section which consists of two managers and 20 staff members. A secret can be recovered by a group of two managers or groups of one manager and two staff members. In this case, every manager belongs to 191 minimal authorized subsets and every staff member belongs to 38 minimal authorized subsets. We shall realize this access structure by applying Benaloh and Leichter's scheme [13]. Then, each manager has to hold 191 shares and each staff member has to hold 38 shares. In 2015, a new secret sharing scheme realizing general access structures was proposed (T15) [17]. This scheme is based on authorized subsets and the first scheme that can reduce the number of shares distributed to specified participants. In the scheme A of T15, we can select a subset of participants without restrictions and reduce the number of shares distributed to any participant who belongs to the selected subset. In the above case, by selecting two managers as a subset of participants we can reduce the number of shares distributed to each manager to 2 if we employ the scheme A of T15. Therefore, in secret sharing schemes reducing the numbers of shares distributed to specified participants is quite useful.

In this paper, we modify the scheme A of T08 [12] and the scheme A of T15 [17] and propose a new secret sharing scheme realizing general access structures, which is based on the unauthorized subsets and can reduce the number of shares distributed to specified participants. Thus, we can select a subset of participants without restrictions and reduce the number of shares distributed to any participant who belongs to the selected subset as well as the scheme A of T15. In the above case, by selecting two managers as a subset of participants we can also reduce the num-

[1] Department of Mathematical Information Engineering, College of Industrial Technology, Nihon University, Narashino, Chiba 275–8575, Japan
[a)] tochikubo.kouya@nihon-u.ac.jp

ber of shares distributed to each manager to 2, if we employ our proposed scheme.

2. Preliminaries

2.1 Secret Sharing Scheme

Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be a set of n participants. Let $\mathcal{D}(\notin \mathcal{P})$ denote a dealer who selects a secret and distribute a share to each participant. Let $\mathcal{K}$ and $\mathcal{S}$ denote a secret set and a share set, respectively. $\mathcal{S}(A)$ denotes the shares assigned to a subset $A \subset \mathcal{P}$. The access structure $\Gamma(\subset 2^{\mathcal{P}})$ is the family of subsets of $\mathcal{P}$ which contains the sets of participants qualified to recover the secret. For any authorized subset $A \in \Gamma$, any superset of A is also an authorized subset. Hence, the access structure should satisfy the monotone property:

$$A \in \Gamma, A \subset A' \subset \mathcal{P} \Rightarrow A' \in \Gamma.$$

Let Γ_0 be a family of the minimal sets in Γ, called the minimal access structure. Γ_0 is denoted by

$$\Gamma_0 = \{A \in \Gamma : A' \not\subset A \text{ for all } A' \in \Gamma - \{A\}\}.$$

For any access structure Γ, there is a family of sets $\bar{\Gamma} = 2^{\mathcal{P}} - \Gamma$. Here, $\bar{\Gamma}$ contains the sets of participants unqualified to recover the secret. The family of maximal sets in $\bar{\Gamma}$ is denoted by $\bar{\Gamma}_1$. That is,

$$\bar{\Gamma}_1 = \{B \in \bar{\Gamma} : B \not\subset B' \text{ for all } B' \in \bar{\Gamma} - \{B\}\}.$$

Let $p_{\mathcal{K}}$ be a probability distribution on $\mathcal{K}$. Let $p_{\mathcal{S}(A)}$ be a probability distribution on the shares $\mathcal{S}(A)$. Usually a secret K is chosen from $\mathcal{K}$ with the uniform distribution. A secret sharing scheme is perfect if

$$H(K|A) = \begin{cases} 0 & (\text{if } A \in \Gamma) \\ H(K) & (\text{if } A \notin \Gamma), \end{cases}$$

where $H(K)$ and $H(K|A)$ denote the entropy of $p_{\mathcal{K}}$ and the conditional entropy defined by the joint probability distribution $p_{\mathcal{K}\times\mathcal{S}(A)}$, respectively.

In general, the efficiency of a perfect secret sharing scheme is measured by the information rate ρ [18] defined as

$$\rho = \min\{\rho_i : 1 \le i \le n\},\ \rho_i = \log|\mathcal{K}|/\log|\mathcal{S}(P_i)|$$

where $\mathcal{S}(P_i)$ denotes the set of possible shares that P_i might receive. ρ_i is the information rate for P_i. Obviously, a high information rate is desirable. A perfect secret sharing scheme is ideal if $\rho = 1$.

2.2 Shamir's (k, n)-threshold Scheme

Throughout the paper, p is a large prime, and let Z_p be a finite field with p elements. Shamir's (k, n)-threshold scheme is described as follows [1]:

(1) A dealer $\mathcal{D}$ chooses n distinct nonzero elements of Z_p, denoted by $x_1, x_2, \cdots, x_n$. The values x_i are public.

(2) Suppose $\mathcal{D}$ wants to share a secret $K \in Z_p$, $\mathcal{D}$ chooses $k-1$ elements $a_1, a_2, \cdots a_{k-1}$ from Z_p independently with a uniform distribution.

(3) $\mathcal{D}$ distributes the share $s_i = f(x_i)$ to P_i $(1 \le i \le n)$, where

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1}$$

is a polynomial over Z_p.

It is known that Shamir's (k, n)-threshold scheme is perfect and ideal [18], [19]. This implies that every group of k participants can recover the secret K, but no group of less than k participants can get any information about the secret.

The access structure of (k, n)-threshold scheme is described as follows:

$$\Gamma = \{A \in 2^{\mathcal{P}} : |A| \ge k\}.$$

In this paper, every share is computed by using Shamir's (k, n)-threshold scheme though any ideal threshold scheme can be used instead of Shamir's (k, n)-threshold scheme for $k \ne n$, and more simple schemes can be used instead of Shamir's (n, n)-threshold scheme. Therefore, we assume $\mathcal{K} = \mathcal{S} = Z_p$.

2.3 Secret Sharing Schemes Based on Authorized Subsets

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, Benaloh and Leichter's scheme [13] is described as follows.

Benaloh and Leichter's scheme (BL88):

(1) Let $\Gamma_0 = \{A_1, A_2, \cdots, A_m\}$. For $A_i \in \Gamma_0$, compute $|A_i|$ shares

$$s_{i,1}, s_{i,2}, \cdots, s_{i,|A_i|}$$

by using an $(|A_i|, |A_i|)$-threshold scheme with K as a secret independently for $1 \le i \le m$.

(2) One distinct share from

$$s_{i,1}, s_{i,2}, \cdots, s_{i,|A_i|}$$

is assigned to each $P \in A_i$ $(1 \le i \le m)$.

Example 1: For $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6\}$, consider the following access structure

$$\Gamma_0 = \{A_1, A_2, \cdots, A_6\}$$

where

$$\begin{aligned} A_1 &= \{P_1, P_2, P_5, P_6\}, \\ A_2 &= \{P_2, P_3, P_5, P_6\}, \\ A_3 &= \{P_2, P_4, P_5, P_6\}, \\ A_4 &= \{P_3, P_4, P_5, P_6\}, \\ A_5 &= \{P_1, P_2, P_3, P_4, P_5\}, \\ A_6 &= \{P_1, P_2, P_3, P_4, P_6\}. \end{aligned}$$

We shall realize this access structure by Benaloh and Leichter's scheme. In this case, shares are distributed as follows:

$$\begin{aligned} P_1 &: s_{1,1}, s_{5,1}, s_{6,1} \\ P_2 &: s_{1,2}, s_{2,1}, s_{3,1}, s_{5,2}, s_{6,2} \\ P_3 &: s_{2,2}, s_{4,1}, s_{5,3}, s_{6,3} \\ P_4 &: s_{3,2}, s_{4,2}, s_{5,4}, s_{6,4} \\ P_5 &: s_{1,3}, s_{2,3}, s_{3,3}, s_{4,3}, s_{5,5} \\ P_6 &: s_{1,4}, s_{2,4}, s_{3,4}, s_{4,4}, s_{6,5} \end{aligned}$$

where $s_{i,j}$ is computed by using Shamir's $(|A_i|, |A_i|)$-threshold scheme with K as a secret $(1 \le i \le 6,\ 1 \le j \le |A_i|)$.

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $\mathcal{Q}(\subset \mathcal{P})$, $K \in \mathcal{K}$ and Γ, the scheme A

of T15 [17] is described as follows.

Scheme A of T15:

(1) Let $\mathcal{A}' = \{C \subset Q : Q \cap A = C \text{ for some } A \in \Gamma_0\}$ and represent it as

$$\mathcal{A}' = \{C'_1, C'_2, \cdots, C'_m\}.$$

(2) For $C'_i \in \mathcal{A}'$, let

$$\mathcal{A}_i = \{B \subset \mathcal{P} - Q : B \cap C'_i = \phi \text{ and } B \cup C'_i = A \text{ for some } A \in \Gamma_0\}$$

and represent it as

$$\mathcal{A}_i = \{C_{i1}, C_{i2}, \cdots, C_{i|\mathcal{A}_i|}\}.$$

(3) For $C'_i \in \mathcal{A}'$,

(i) if $C'_i = \phi$ then

$$S_i = \{w_i\} \text{ and } w_i = K,$$

(ii) if $C'_i \neq \phi$ and $\mathcal{A}_i = \{\phi\}$ then

$$S_i = \{w'_i\} \text{ and } w'_i = K,$$

(iii) if $C'_i \neq \phi$ and $\mathcal{A}_i \neq \{\phi\}$ then compute 2 shares

$$S_i = \{w_i, w'_i\}$$

by using Shamir's $(2, 2)$-threshold scheme with K as a secret independently for $1 \leq i \leq m$.

(4) For $C'_i \in \mathcal{A}'$, if $C'_i = \phi$ then

$$S_{1,i} = \phi,$$

else compute $|C'_i|$ shares

$$S_{1,i} = \{s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|C'_i|}\}$$

by using Shamir's $(|C'_i|, |C'_i|)$-threshold scheme with w'_i as a secret independently for $1 \leq i \leq m$. One distinct share in $S_{1,i}$ is assigned to each $P \in C'_i$ $(1 \leq i \leq m)$.

(5) For $C_{ij} \in \mathcal{A}_i$, if $C_{ij} = \phi$ then

$$S_{2,i,j} = \phi,$$

else compute $|C_{ij}|$ shares

$$S_{2,i,j} = \{s_{i,j,1}, s_{i,j,2}, \cdots, s_{i,j,|C_{ij}|}\}$$

by using Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with w_i as a secret independently for $1 \leq i \leq m, 1 \leq j \leq |\mathcal{A}_i|$. One distinct share in $S_{2,i,j}$ is assigned to each $P \in C_{ij}$ $(1 \leq i \leq m, 1 \leq j \leq |\mathcal{A}_i|)$.

Example 2: Let $Q = \{P_1, P_2\}$. We shall realize the access structure of Example 1 by the proposed scheme A of T15.

- Since $Q = \{P_1, P_2\}$, $\mathcal{A}'$ is defined by

$$\mathcal{A}' = \{C'_1, C'_2, C'_3\}$$

where

$$C'_1 = \{P_1, P_2\},$$
$$C'_2 = \{P_2\},$$
$$C'_3 = \phi.$$

- $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are defined by

$$\mathcal{A}_1 = \{\{P_5, P_6\}, \{P_3, P_4, P_5\}, \{P_3, P_4, P_6\}\},$$
$$\mathcal{A}_2 = \{\{P_3, P_5, P_6\}, \{P_4, P_5, P_6\}\},$$
$$\mathcal{A}_3 = \{\{P_3, P_4, P_5, P_6\}\}.$$

- For $C'_1, C'_2 \in \mathcal{A}'$, compute 2 shares

$$S_1 = \{w_1, w'_1\},$$
$$S_2 = \{w_2, w'_2\}$$

by using Shamir's $(2, 2)$-threshold scheme with K as a secret independently. Since $C'_3 = \phi$, we set

$$S_3 = \{w_3\} \text{ and } w_3 = K.$$

- For $C'_1, C'_2 \in \mathcal{A}'$, compute $|C'_i|$ shares

$$S_{1,1} = \{s'_{1,1}, s'_{1,2}\},$$
$$S_{1,2} = \{s'_{2,1}\}$$

by using $(|C'_i|, |C'_i|)$-threshold scheme with w'_i as a secret independently for $1 \leq i \leq 2$. Since $C'_3 = \phi$, we set

$$S_{1,3} = \phi.$$

- For $C_{ij} \in \mathcal{A}_i$, compute $|C_{ij}|$ shares

$$S_{2,1,1} = \{s_{1,1,1}, s_{1,1,2}\},$$
$$S_{2,1,2} = \{s_{1,2,1}, s_{1,2,2}, s_{1,2,3}\},$$
$$S_{2,1,3} = \{s_{1,3,1}, s_{1,3,2}, s_{1,3,3}\},$$
$$S_{2,2,1} = \{s_{2,1,1}, s_{2,1,2}, s_{2,1,3}\},$$
$$S_{2,2,2} = \{s_{2,2,1}, s_{2,2,2}, s_{2,2,3}\},$$
$$S_{2,3,1} = \{s_{3,1,1}, s_{3,1,2}, s_{3,1,3}, s_{3,1,4}\}$$

by using Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with w_i as a secret independently for $1 \leq i \leq 3, 1 \leq j \leq |\mathcal{A}_i|$.

- In this case, shares are distributed as follows:

$$P_1 : s'_{1,1}$$
$$P_2 : s'_{1,2}, s'_{2,1}$$
$$P_3 : s_{1,2,1}, s_{1,3,1}, s_{2,1,1}, s_{3,1,1}$$
$$P_4 : s_{1,2,2}, s_{1,3,2}, s_{2,2,1}, s_{3,1,2}$$
$$P_5 : s_{1,1,1}, s_{1,2,3}, s_{2,1,2}, s_{2,2,2}, s_{3,1,3}$$
$$P_6 : s_{1,1,2}, s_{1,3,3}, s_{2,1,3}, s_{2,2,3}, s_{3,1,4}.$$

We can select a subset of participants $Q(\subset \mathcal{P})$ without restrictions. This scheme can reduce the number of shares distributed to each participant $P \in Q$. On the other hand, for any $P \in \mathcal{P} - Q$, the number of shares distributed to P is equal to that of Benaloh and Leichter's scheme.

2.4 Secret Sharing Schemes Based on Unauthorized Subsets

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, Ito, Saito and Nishizeki's scheme [10] is described as follows.

Ito, Saito and Nishizeki's Scheme (ISN87):

(1) Let $\bar{\Gamma}_1 = \{B_1, B_2, \cdots, B_t\}$. Compute $t(= |\bar{\Gamma}_1|)$ shares

$$S = \{w_1, w_2, \cdots, w_t\}$$

for the secret K by using a (t, t)-threshold scheme.

(2) Distribute shares to $P_i \in \mathcal{P}$ $(1 \le i \le n)$ according to the function $g : \mathcal{P} \to 2^S$ defined as

$$\begin{aligned} g(P_i) &= \{w_j : P_i \notin B_j \in \bar{\Gamma}_1, 1 \le j \le t\} \\ &= \bigcup_{\substack{1 \le j \le t \\ P_i \notin B_j}} \{w_j\}. \end{aligned}$$

Example 3: We shall realize the access structure of Example 1 by Ito, Saito and Nishizeki's scheme. For this access structure, $\bar{\Gamma}_1$ is given by

$$\begin{aligned} \bar{\Gamma}_1 = \{&\{P_2, P_5, P_6\}, \{P_1, P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_5\}, \\ &\{P_1, P_2, P_4, P_5\}, \{P_1, P_3, P_4, P_5\}, \{P_2, P_3, P_4, P_5\}, \\ &\{P_1, P_2, P_3, P_6\}, \{P_1, P_2, P_4, P_6\}, \{P_1, P_3, P_4, P_6\}, \\ &\{P_2, P_3, P_4, P_6\}, \{P_1, P_3, P_5, P_6\}, \{P_1, P_4, P_5, P_6\}\}. \end{aligned}$$

(1) Since $|\bar{\Gamma}_1| = 12$, compute 12 shares

$$w_1, w_2, \cdots, w_{12}$$

by using a $(12, 12)$-threshold scheme for the secret K.

(2) According to the function g, distribute shares as follows:

$$\begin{aligned} g(P_1) &= \{w_1, w_6, w_{10}\}, \\ g(P_2) &= \{w_5, w_9, w_{11}, w_{12}\}, \\ g(P_3) &= \{w_1, w_4, w_8, w_{12}\}, \\ g(P_4) &= \{w_1, w_3, w_7, w_{11}\}, \\ g(P_5) &= \{w_2, w_7, w_8, w_9, w_{10}\}, \\ g(P_6) &= \{w_2, w_3, w_4, w_5, w_6\}. \end{aligned}$$

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, the scheme A of T08 [12] is described as follows.

Scheme A of T08:

(1) Divide $\bar{\Gamma}_1$ into disjoint subsets

$$\bar{\Gamma}_1^{(0)}, \bar{\Gamma}_1^{(1)}, \cdots, \bar{\Gamma}_1^{(r)}$$

such that $\bar{\Gamma}_1^{(i)} (1 \le i \le r)$ satisfies

$$\bar{\Gamma}_1^{(i)} = \{Z_i \cup \{P\} \ : \ P \in Y_i\}$$

or

$$\bar{\Gamma}_1^{(i)} = \{Z_i \cup Y_i - \{P\} \ : \ P \in Y_i\}$$

for some $Y_i \subset \mathcal{P}$ and $Z_i \subset \mathcal{P} (Y_i \cap Z_i = \phi)$ and

$$\bar{\Gamma}_1^{(0)} = \bar{\Gamma}_1 - \left\{ \bigcup_{1 \le i \le r} \bar{\Gamma}_1^{(i)} \right\}.$$

Let $d = \left|\bar{\Gamma}_1^{(0)}\right|$ and represent $\bar{\Gamma}_1^{(0)}$, $e_i (1 \le i \le r)$ and $Y_i (1 \le i \le r)$ as

$$\bar{\Gamma}_1^{(0)} = \{B_1, B_2, \cdots, B_d\},$$

$$e_i = |X| \quad (X \in \bar{\Gamma}_1^{(i)})$$

and

$$Y_i = \{P_{i_1}, P_{i_2}, \cdots, P_{i_{|Y_i|}}\},$$

respectively.

(2) Compute $d + r$ shares

$$S = \{s_1, s_2, \cdots, s_{d+r}\}$$

for the secret K by using Shamir's $(d + r, d + r)$-threshold scheme.

(3) If $r > 0$, for $1 \le i \le r$, by using Shamir's $(e_i - |Z_i| + 1, |Y_i|)$-threshold scheme with s_{d+i} as a secret, compute $|Y_i|$ shares

$$S_{d+i} = \{s_{d+i,i_1}, s_{d+i,i_2}, \cdots, s_{d+i,i_{|Y_i|}}\},$$

independently for $1 \le i \le r$.

(4) Distribute shares to $P_i \in \mathcal{P}$ $(1 \le i \le n)$ according to the function defined as

$$\begin{aligned} g'(P_i) = &\left(\bigcup_{\substack{1 \le j \le d \\ P_i \notin B_j}} \{s_j\} \right) \\ &\cup \left(\bigcup_{\substack{1 \le j \le r \\ P_i \notin Y_j \cup Z_j}} \{s_{d+j}\} \right) \\ &\cup \left(\bigcup_{\substack{1 \le j \le r \\ P_i \in Y_j}} \{s_{d+j,i}\} \right). \end{aligned}$$

Example 4: We shall realize the access structure of Example 1 by the scheme A of T08.

- Divide $\bar{\Gamma}_1$ into disjoint subsets

$$\bar{\Gamma}_1^{(0)}, \bar{\Gamma}_1^{(1)}, \bar{\Gamma}_1^{(2)}, \bar{\Gamma}_1^{(3)}, \bar{\Gamma}_1^{(4)}$$

where

$$\begin{aligned} \bar{\Gamma}_1^{(0)} &= \{\{P_2, P_5, P_6\}\}, \\ \bar{\Gamma}_1^{(1)} &= \{\{P_1, P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_5\}, \{P_1, P_2, P_3, P_6\}\}, \\ \bar{\Gamma}_1^{(2)} &= \{\{P_1, P_2, P_4, P_5\}, \{P_1, P_3, P_4, P_5\}, \{P_2, P_3, P_4, P_5\}\}, \\ \bar{\Gamma}_1^{(3)} &= \{\{P_1, P_2, P_4, P_6\}, \{P_1, P_3, P_4, P_6\}, \{P_2, P_3, P_4, P_6\}\}, \\ \bar{\Gamma}_1^{(4)} &= \{\{P_1, P_3, P_5, P_6\}, \{P_1, P_4, P_5, P_6\}\}, \end{aligned}$$

and

$$\begin{aligned} Y_1 &= \{P_4, P_5, P_6\}, \\ Z_1 &= \{P_1, P_2, P_3\}, \\ e_1 &= 4, \\ Y_2 &= \{P_1, P_2, P_3\}, \\ Z_2 &= \{P_4, P_5\}, \\ e_2 &= 4, \\ Y_3 &= \{P_1, P_2, P_3\}, \\ Z_3 &= \{P_4, P_6\}, \\ e_3 &= 4, \end{aligned}$$

$$Y_4 = \{P_3, P_4\},$$
$$Z_4 = \{P_1, P_5, P_6\},$$
$$e_4 = 4.$$

- Since $d = 1$ and $r = 4$, compute 5 shares

$$S = \{s_1, s_2, \cdots, s_5\}$$

for the secret K by using Shamir's $(5, 5)$-threshold scheme.

- Since $r > 0$, by using Shamir's $(e_i - |Z_i| + 1, |Y_i|)$-threshold scheme with s_{1+i} as a secret, compute $S_{1+i}(1 \le i \le 4)$ as follows:

$$S_2 = \{s_{2,4}, s_{2,5}, s_{2,6}\},$$
$$S_3 = \{s_{3,1}, s_{3,2}, s_{3,3}\},$$
$$S_4 = \{s_{4,1}, s_{4,2}, s_{4,3}\},$$
$$S_5 = \{s_{5,3}, s_{5,4}\}.$$

- According to the function g', distribute shares as follows:

$$g'(P_1) = \{s_1, s_{3,1}, s_{4,1}\},$$
$$g'(P_2) = \{s_{3,2}, s_{4,2}, s_5\},$$
$$g'(P_3) = \{s_1, s_{3,3}, s_{4,3}, s_{5,3}\},$$
$$g'(P_4) = \{s_1, s_{2,4}, s_{5,4}\},$$
$$g'(P_5) = \{s_{2,5}, s_4\},$$
$$g'(P_6) = \{s_{2,6}, s_3\}.$$

This scheme can reduce the number of shares distributed to $P \notin Z_i$ $(1 \le i \le r)$. Thus, for any access structure, this scheme is more efficient than the scheme proposed by Ito, Saito and Nishizeki [10] from the viewpoint of the number of shares distributed to each participant.

Remarks In the scheme A of T08, $\bar{\Gamma}_1^{(1)}, \cdots, \bar{\Gamma}_1^{(r)}$ cannot be determined uniquely. When we select a large r, we can reduce the number of shares distributed to each participant though it is hard to find r. Of course, if we can choose $r = 0$, then this scheme is equivalent to Ito, Saito and Nishizeki's scheme and shares are distributed to each participant uniquely.

3. Proposed Scheme

Here, we modify the scheme A of T08 [12] and the scheme A of T15 [17] and propose a new secret sharing scheme realizing general access structures. The proposed scheme can reduce the number of shares distributed to $P \in Q(\subset \mathcal{P})$ by dividing Γ_0 according to the subsets of Q in the same way as the scheme A of T15 (Γ_0 dividing phase). Furthermore, in order to reduce the number of shares distributed to each participant $P \in \mathcal{P} - Q$ the scheme A of T08 is applied to each divided access structure in the proposed scheme (secret sharing phase for divided access structures). For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}, Q(\subset \mathcal{P})$, $K \in \mathcal{K}$ and Γ, the proposed scheme is described as follows.

Proposed Scheme:

(Γ_0 dividing phase)

(1) Let $\mathcal{A}' = \{C \subset Q : Q \cap A = C \text{ for some } A \in \Gamma_0\}$ and represent it as

$$\mathcal{A}' = \{C'_1, C'_2, \cdots, C'_m\}$$

and

$$C'_j = \{P'_{j_1}, P'_{j_2}, \cdots, P'_{j|C'_j|}\} \ (1 \le j \le m).$$

(2) For $C'_j \in \mathcal{A}'$, let

$$\mathcal{A}_j = \{B \subset \mathcal{P} - Q : B \cap C'_j = \phi \text{ and } B \cup C'_j = A \text{ for some } A \in \Gamma_0\}$$

and represent it as

$$\mathcal{A}_j = \{C_{j1}, C_{j2}, \cdots, C_{j|\mathcal{A}_j|}\}.$$

(3) For $C'_j \in \mathcal{A}'$,

(i) if $C'_j = \phi$ then

$$S'_j = \{w_j\} \text{ and } w_j = K,$$

(ii) if $C'_j \neq \phi$ and $\mathcal{A}_j = \{\phi\}$ then

$$S'_j = \{w'_j\} \text{ and } w'_j = K,$$

(iii) if $C'_j \neq \phi$ and $\mathcal{A}_j \neq \{\phi\}$ then compute 2 shares

$$S'_j = \{w_j, w'_j\}$$

by using Shamir's $(2, 2)$-threshold scheme with K as a secret independently for $1 \le j \le m$.

(4) For $C'_j \in \mathcal{A}'$, if $C'_j \neq \phi$ then compute $|C'_j|$ shares

$$S'_{1,j} = \{s'_{j,j_1}, s'_{j,j_2}, \cdots, s'_{j,j_{|C'_j|}}\}$$

by using Shamir's $(|C'_j|, |C'_j|)$-threshold scheme with w'_j as a secret independently for $1 \le j \le m$.

(Secret sharing phase for divided access structures)

(5) Let $\bar{\Gamma}_{1,j}$ be the family of maximal unauthorized subsets for $\mathcal{P} - Q$ and the minimal access structure $\mathcal{A}_j$ $(1 \le j \le m)$.

(i) Divide $\bar{\Gamma}_{1,j}$ into disjoint subsets

$$\bar{\Gamma}_{1,j}^{(1)}, \cdots, \bar{\Gamma}_{1,j}^{(r_j)}$$

such that $\bar{\Gamma}_{1,j}^{(i)}(1 \le i \le r_j)$ satisfies

$$\bar{\Gamma}_{1,j}^{(i)} = \{Z_{j,i} \cup \{P\} \ : \ P \in Y_{j,i}\} \tag{1}$$

or

$$\bar{\Gamma}_{1,j}^{(i)} = \{Z_{j,i} \cup Y_{j,i} - \{P\} \ : \ P \in Y_{j,i}\} \tag{2}$$

for some $Y_{j,i} \subset \mathcal{P} - Q$ and $Z_{j,i} \subset \mathcal{P} - Q (Y_{j,i} \cap Z_{j,i} = \phi)$ and

$$\bar{\Gamma}_{1,j}^{(0)} = \bar{\Gamma}_{1,j} - \left\{ \bigcup_{1 \le i \le r_j} \bar{\Gamma}_{1,j}^{(i)} \right\}.$$

Let $d_j = \left|\bar{\Gamma}_{1,j}^{(0)}\right|$ and represent $\bar{\Gamma}_{1,j}^{(0)}$, $e_{j,i}(1 \le i \le r_j)$ and $Y_{j,i}(1 \le i \le r_j)$ as

$$\bar{\Gamma}_{1,j}^{(0)} = \{B_{j,1}, B_{j,2}, \cdots, B_{j,d_j}\},$$
$$e_{j,i} = |X| \quad (X \in \bar{\Gamma}_{1,j}^{(i)}) \tag{3}$$

and

$$Y_{j,i} = \{P_{j,i_1}, P_{j,i_2}, \cdots, P_{j,i_{|Y_{j,i}|}}\},$$

respectively.

(ii) Compute $d_j + r_j$ shares

$$S_j = \{s_{j,1}, s_{j,2}, \cdots, s_{j,d_j+r_j}\}$$

for the secret w_j by using Shamir's $(d_j + r_j, d_j + r_j)$-threshold scheme.

(iii) If $r_j > 0$, for $1 \le i \le r_j$, by using Shamir's $(e_{j,i} - |Z_{j,i}| + 1, |Y_{j,i}|)$-threshold scheme with s_{j,d_j+i} as a secret, compute $|Y_{j,i}|$ shares

$$S_{j,d_j+i} = \{s_{j,d_j+i,i_1}, s_{j,d_j+i,i_2}, \cdots, s_{j,d_j+i,i_{|Y_{j,i}|}}\},$$

independently for $1 \le i \le r_j$.

(6) Distribute shares to $P_i \in \mathcal{P}$ $(1 \le i \le n)$ according to the function defined as

$$g''(P_i) = \left(\bigcup_{\substack{1 \le j \le m \\ P_i \in C'_j}} \{s'_{j,i}\} \right) \cup \bigcup_{1 \le j \le m} \left\{ \left(\bigcup_{\substack{1 \le k \le d_j \\ P_i \notin B_{j,k} \cup Q}} \{s_{j,k}\} \right) \right. \tag{4}$$

$$\cup \left(\bigcup_{\substack{1 \le k \le r_j \\ P_i \notin Y_{j,k} \cup Z_{j,k} \cup Q}} \{s_{j,d_j+k}\} \right) \tag{5}$$

$$\left. \cup \left(\bigcup_{\substack{1 \le k \le r_j \\ P_i \in Y_{j,k}}} \{s_{j,d_j+k,i}\} \right) \right\}. \tag{6}$$

Example 5: Let $Q = \{P_1, P_2\}$. We shall realize the access structure of Example 1 by the proposed scheme.

(Γ_0 dividing phase)

- Since $Q = \{P_1, P_2\}$, $\mathcal{A}'$ is defined by

$$\mathcal{A}' = \{C'_1, C'_2, C'_3\}$$

where

$$C'_1 = \{P_1, P_2\},$$
$$C'_2 = \{P_2\},$$
$$C'_3 = \phi.$$

- $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are defined by

$$\mathcal{A}_1 = \{\{P_5, P_6\}, \{P_3, P_4, P_5\}, \{P_3, P_4, P_6\}\},$$
$$\mathcal{A}_2 = \{\{P_3, P_5, P_6\}, \{P_4, P_5, P_6\}\},$$
$$\mathcal{A}_3 = \{\{P_3, P_4, P_5, P_6\}\}.$$

- For $C'_1, C'_2 \in \mathcal{A}'$, compute 2 shares

$$S'_1 = \{w_1, w'_1\},$$
$$S'_2 = \{w_2, w'_2\}$$

by using Shamir's $(2, 2)$-threshold scheme with K as a secret independently. Since $C'_3 = \phi$, we set

$$S'_3 = \{w_3\} \text{ and } w_3 = K.$$

- For $C'_1, C'_2 \in \mathcal{A}'$, compute $|C'_j|$ shares

$$S'_{1,1} = \{s'_{1,1}, s'_{1,2}\},$$
$$S'_{1,2} = \{s'_{2,2}\}$$

by using $(|C'_j|, |C'_j|)$-threshold scheme with w'_j as a secret independently for $1 \le j \le 2$.

(Secret sharing phase for $\mathcal{A}_1$)

- For $\{P_3, P_4, P_5, P_6\}(= \mathcal{P} - Q)$ and $\mathcal{A}_1$, $\bar{\Gamma}_{1,1}$ is given by

$$\bar{\Gamma}_{1,1} = \{\{P_3, P_4\}, \{P_3, P_5\}, \{P_4, P_5\}, \{P_3, P_6\}, \{P_4, P_6\}\}.$$

- Divide $\bar{\Gamma}_{1,1}$ into disjoint subsets

$$\bar{\Gamma}^{(0)}_{1,1} = \phi,$$
$$\bar{\Gamma}^{(1)}_{1,1} = \{\{P_3, P_4\}, \{P_3, P_5\}, \{P_3, P_6\}\},$$
$$\bar{\Gamma}^{(2)}_{1,1} = \{\{P_4, P_5\}, \{P_4, P_6\}\},$$

and

$$Y_{1,1} = \{P_4, P_5, P_6\},$$
$$Z_{1,1} = \{P_3\},$$
$$e_{1,1} = 2,$$
$$Y_{1,2} = \{P_5, P_6\},$$
$$Z_{1,2} = \{P_4\},$$
$$e_{1,2} = 2.$$

- Since $d_1 = 0$ and $r_1 = 2$, compute 2 shares

$$S_1 = \{s_{1,1}, s_{1,2}\}$$

for the secret w_1 by using Shamir's $(2, 2)$-threshold scheme.

- Since $r_1 > 0$, by using Shamir's $(e_{1,i} - |Z_{1,i}| + 1, |Y_{1,i}|)$-threshold scheme with $s_{1,i}$ as a secret, compute $S_{1,i} (1 \le i \le 2)$ as follows:

$$S_{1,1} = \{s_{1,1,4}, s_{1,1,5}, s_{1,1,6}\},$$
$$S_{1,2} = \{s_{1,2,5}, s_{1,2,6}\}.$$

(Secret sharing phase for $\mathcal{A}_2$)

- Similarly, for $\{P_3, P_4, P_5, P_6\}$ and $\mathcal{A}_2$, $\bar{\Gamma}_{1,2}$ is given by

$$\bar{\Gamma}_{1,2} = \{\{P_3, P_4, P_5\}, \{P_3, P_4, P_6\}, \{P_5, P_6\}\}.$$

- Divide $\bar{\Gamma}_{1,2}$ into disjoint subsets

$$\bar{\Gamma}^{(0)}_{1,2} = \{\{P_5, P_6\}\},$$
$$\bar{\Gamma}^{(1)}_{1,2} = \{\{P_3, P_4, P_5\}, \{P_3, P_4, P_6\}\},$$

and

$$Y_{2,1} = \{P_5, P_6\},$$
$$Z_{2,1} = \{P_3, P_4\},$$
$$e_{2,1} = 3.$$

- Since $d_2 = 1$ and $r_2 = 1$, compute 2 shares

$$S_2 = \{s_{2,1}, s_{2,2}\}$$

for the secret w_2 by using Shamir's $(2, 2)$-threshold scheme.

- Since $r_2 > 0$, by using Shamir's $(e_{2,1} - |Z_{2,1}| + 1, |Y_{2,1}|)$-threshold scheme with $s_{2,2}$ as a secret, compute $S_{2,2}$ as follows:

$$S_{2,2} = \{s_{2,2,5}, s_{2,2,6}\}.$$

(Secret sharing phase for $\mathcal{A}_3$)

- Similarly, for $\{P_3, P_4, P_5, P_6\}$ and $\mathcal{A}_3$, $\bar{\Gamma}_{1,3}$ is given by

$$\bar{\Gamma}_{1,3} = \{\{P_3, P_4, P_5\}, \{P_3, P_4, P_6\}, \{P_3, P_5, P_6\}, \{P_4, P_5, P_6\}\}.$$

- In this case, we set $r_3 = 0$ and $\bar{\Gamma}^{(0)}_{1,3} = \{B_{3,1}, B_{3,2}, B_{3,3}, B_{3,4}\}$ where

$$\begin{aligned} B_{3,1} &= \{\{P_3, P_4, P_5\}\}, \\ B_{3,2} &= \{\{P_3, P_4, P_6\}\}, \\ B_{3,3} &= \{\{P_3, P_5, P_6\}\}, \\ B_{3,4} &= \{\{P_4, P_5, P_6\}\}. \end{aligned}$$

- Since $d_3 = 4$ and $r_2 = 0$, compute 4 shares

$$S_3 = \{s_{3,1}, \cdots, s_{3,4}\}$$

for the secret w_3 by using Shamir's $(4, 4)$-threshold scheme.

- According to the function g'', distribute shares as follows:

$$\begin{aligned} g''(P_1) &= \{s'_{1,1}\}, \\ g''(P_2) &= \{s'_{1,2}, s'_{2,2}\}, \\ g''(P_3) &= \{s_{1,2}, s_{2,1}, s_{3,4}\}, \\ g''(P_4) &= \{s_{1,1,4}, s_{2,1}, s_{3,3}\}, \\ g''(P_5) &= \{s_{1,1,5}, s_{1,2,5}, s_{2,2,5}, s_{3,2}\}, \\ g''(P_6) &= \{s_{1,1,6}, s_{1,2,6}, s_{2,2,6}, s_{3,1}\}. \end{aligned}$$

We can select a subset of participants $Q(\subset \mathcal{P})$ without restriction. In this example, we select a subset of participants $Q = \{P_1, P_2\}$. The proposed scheme can reduce the number of shares distributed to $P \in Q$ by dividing Γ_0 into $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ according to the subsets of Q. Furthermore, in order to reduce the number of shares distributed to each participant $P \in \mathcal{P} - Q$ the scheme A of T08 is applied to divided access structures $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$. Here, we show some properties of the proposed scheme.

Theorem 1 Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be a set of n participants. For any $Q(\subset \mathcal{P})$ and any access structure $\Gamma(\subset 2^{\mathcal{P}})$, distribute shares for a secret K by using the proposed scheme. Then, for any subset $X \subset \mathcal{P}$,

(a) $X \in \Gamma \Rightarrow H(K|X) = 0$,

(b) $X \notin \Gamma \Rightarrow H(K|X) = H(K)$.

Proof: Let $X_{S'_{1,j}}$ denote the shares in $S'_{1,j}$ assigned to X $(1 \le j \le m)$. Let X_{S_j} be a set of shares in S_j which are assigned to X or can be recovered by X $(1 \le j \le m)$. At first, we show $H(K|X) = 0$ for any $X \in \Gamma$. From the property of the access structure and the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, there exists $A \in \Gamma_0$ such that

$$C'_j \cup C_{ji} = A \subset X.$$

Since C_{ji} is an authorized subset for $\mathcal{A}_j$, we have

$$|X_{S_j}| = d_j + r_j$$

from the definition of $S_j, S_{j,d_j+1}, \cdots, S_{j,d_j+r_j}$ and Theorem 1 of T08 [12]. Thus, X can recover w_j since $s_{j,1}, s_{j,2}, \cdots, s_{j,d_j+r_j}$ are shares computed by Shamir's $(d_j + r_j, d_j + r_j)$-threshold scheme with w_j as a secret. On the other hand, we have

$$|X_{S'_{1,j}}| = |C'_j|.$$

If $C'_j \neq \phi$, then X can recover w'_j since $s'_{j,j_1}, s'_{j,j_2}, \cdots, s'_{j,j_{|C'_j|}}$ are shares computed by Shamir's $(|C'_j|, |C'_j|)$-threshold scheme with w'_j as a secret. From the definition of S'_j, we immediately obtain

$$\begin{aligned} &H(K|X) \\ &= H(K|X_{S'_{1,1}}, \cdots, X_{S'_{1,m}}, X_{S_1}, \cdots, X_{S_m}) \\ &\le H(K|X_{S'_{1,j}}, X_{S_j}) \\ &= 0. \end{aligned}$$

Since $H(K|X) \ge 0$ is obvious, we have $H(K|X) = 0$ for any $X \in \Gamma$.

Next we show $H(K|X) = H(K)$ for any $X \notin \Gamma$. From the property of the access structure and the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, for any $A \in \Gamma_0$, we have

$$C'_j \not\subset X \text{ or } C_{ji} \not\subset X \ (1 \le j \le m, 1 \le i \le |\mathcal{A}_j|).$$

Thus, from the definition of $S_j, S_{j,d_j+1}, \cdots, S_{j,d_j+r_j}$ and Theorem 1 of T08, we have

$$|X_{S_j}| < d_j + r_j \quad \text{or} \quad |X_{S'_{1,j}}| < |C'_j|$$

for $1 \le j \le m, 1 \le i \le |\mathcal{A}_j|$. Thus, we have

$$H(K|X_{S'_{1,j}}, X_{S_j}) = H(K)$$

for $1 \le j \le m, 1 \le i \le |\mathcal{A}_j|$. This implies

$$H(X_{S'_{1,j}}, X_{S_j}|K) = H(X_{S'_{1,j}}, X_{S_j}). \tag{7}$$

In order to show $H(K|X) = H(K)$, we expand $H(K|X)$ as follows:

$$\begin{aligned} H(K|X) &= H(K|X_{S'_{1,1}}, \cdots, X_{S'_{1,m}}, X_{S_1}, \cdots, X_{S_m}) \\ &= H(K) + H(X_{S'_{1,1}}, \cdots, X_{S'_{1,m}}, X_{S_1}, \cdots, X_{S_m}|K) \\ &\quad - H(X_{S'_{1,1}}, \cdots, X_{S'_{1,m}}, X_{S_1}, \cdots, X_{S_m}). \end{aligned} \tag{8}$$

From the chain rule for entropy, we have

$$\begin{aligned} &H(X_{S'_{1,1}}, \cdots, X_{S'_{1,m}}, X_{S_1}, \cdots, X_{S_m}|K) \\ &= \sum_{t=1}^{m} H(X_{S'_{1,t}}, X_{S_t}|K, X_{S'_{1,1}}, \cdots \\ &\qquad \cdots, X_{S'_{1,t-1}}, X_{S_1}, \cdots, X_{S_{t-1}}) \\ &\overset{(*)}{=} \sum_{t=1}^{m} H(X_{S'_{1,t}}, X_{S_t}|K) \\ &= \sum_{t=1}^{m} H(X_{S'_{1,t}}, X_{S_t}). \end{aligned} \tag{9}$$

Here, $(*)$ comes from the fact that $X_{S'_{1,1}}, \cdots, X_{S'_{1,m}}$ and $X_{S_1}, \cdots, X_{S_m}$ are mutually independent and the last equality comes from Eq. (7). On the other hand, we have

$$\begin{aligned} &H(X_{S'_{1,1}}, \cdots, X_{S'_{1,m}}, X_{S_1}, \cdots, X_{S_m}) \\ &= \sum_{t=1}^{m} H(X_{S'_{1,t}}, X_{S_t}|X_{S'_{1,1}}, \cdots \\ &\qquad \cdots, X_{S'_{1,t-1}}, X_{S_1}, \cdots, X_{S_{t-1}}) \\ &\le \sum_{t=1}^{m} H(X_{S'_{1,t}}, X_{S_t}). \end{aligned} \tag{10}$$

Substituting Eqs. (9) and (10) into Eq. (8), we obtain $H(K|X) \ge H(K)$. Since $H(K|X) \le H(K)$ is obvious, we have $H(K|X) = H(K)$. □

4. Evaluation of the Efficiency

The information rates for $P_i \in \mathcal{P}$ for the access structure of Example 1 are described in **Table 1**.

This result shows that the scheme A of T15 and the proposed scheme can reduce the number of shares distributed to $P \in Q$. In general, we can improve the information rate when we select participants who are assigned the most shares. It is noted that we can select a subset of participants Q without restrictions in the proposed scheme.

From Eq. (6) and the fact that s_{j,d_j+k} or $s_{j,d_j+k,i}$ are assigned to P_i if $P_i \notin Z_{j,i}(1 \le j \le m, 1 \le i \le r_j)$, $|g''(P)|$ is evaluated as follows:

$$|g''(P)| = \begin{cases} \displaystyle\sum_{1\le j\le m} |\{P\} \cap C'_j| & (P \in Q) \\ \displaystyle\sum_{1\le j\le m} \left\{ \left| \left\{ X \in \bar{\Gamma}^{(0)}_{1,j} : P \notin X \right\} \right| \right. & \\ \quad \left. + \displaystyle\sum_{1\le i\le r_j} \left| \{P\} \cap (\mathcal{P} - Z_{j,i}) \right| \right\} & (P \in \mathcal{P} - Q). \end{cases} \tag{11}$$

On the other hand, let $N_{T15_A}(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the scheme A of T15. Then, we have

$$N_{T15_A}(P) = \begin{cases} \displaystyle\sum_{1\le j\le m} |\{P\} \cap C'_j| & (P \in Q) \\ \left| \{ X \in \Gamma_0 : P \in X \} \right| & (P \in \mathcal{P} - Q). \end{cases} \tag{12}$$

Equations (11) and (12) show that the efficiencies of the scheme A of T15 and the proposed scheme are equal for $P \in Q$ and the efficiencies depend on the access structure for $P \in \mathcal{P} - Q$.

Here, we show two examples in order to evaluate the efficiency of the proposed scheme.

Example 6: For $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6\}$, consider the following access structure

$$\begin{aligned} \Gamma'_0 = \{ & \{P_1, P_3, P_4, P_5\}, \{P_1, P_3, P_5, P_6\}, \{P_1, P_4, P_5, P_6\}, \\ & \{P_3, P_4, P_5, P_6\}, \{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_5\}, \\ & \{P_2, P_3, P_5\}, \{P_2, P_4, P_5\}, \{P_1, P_2, P_6\}, \{P_2, P_3, P_6\}, \\ & \{P_2, P_4, P_6\}, \{P_2, P_5, P_6\}\}. \end{aligned}$$

For this access structure, $\bar{\Gamma}'_1$ is given by

$$\begin{aligned} \bar{\Gamma}'_1 = \{ & \{P_1, P_3, P_4, P_6\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_5\}, \{P_1, P_4, P_5\}, \\ & \{P_3, P_4, P_5\}, \{P_1, P_5, P_6\}, \{P_3, P_5, P_6\}, \{P_4, P_5, P_6\}, \\ & \{P_2, P_3\}, \{P_2, P_5\}, \{P_2, P_6\}\}. \end{aligned}$$

We shall realize the access structure Γ'_0 by schemes which have an explicit assignment algorithm for any access structure. The information rates for $P_i \in \mathcal{P}$ are described in **Table 2**.

Table 2 shows that IYO07 and the proposed scheme obtain the best information rate in this example. It is noted that the proposed scheme obtains the best information rate even if the efficiency with respect to Q is discussed. The scheme A of T15 and the proposed scheme can reduce the number of shares distributed to $P \in Q$. Of course, the efficiencies depend on the access structure for $P \in \mathcal{P} - Q$.

Example 7: For $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6\}$, consider the following access structure

Table 1 Comparison of the information rates for the access structure of Example 1.

	P_1	P_2	P_3	P_4	P_5	P_6
ISN87 [10]	1/3	1/4	1/4	1/4	1/5	1/5
Scheme A of T08 [12]	1/3	1/3	1/4	1/3	1/2	1/2
BL88 [13]	1/3	1/5	1/4	1/4	1/5	1/5
Scheme A of T15 [17] *1	1	1/2	1/4	1/4	1/5	1/5
Scheme A of T15 [17] *2	1/3	1/5	1/4	1/4	1/2	1/2
Proposed scheme *1	1	1/2	1/3	1/3	1/4	1/4
Proposed scheme *2	1/3	1/3	1/4	1/4	1/2	1/2

Table 2 Comparison of the information rates for the access structure of Example 6.

	P_1	P_2	P_3	P_4	P_5	P_6
ISN87 [10]	1/6	1/7	1/6	1/6	1/4	1/6
Scheme I of T04 [11]	1/4	1/9	1/5	1/4	1/4	1/5
Scheme A of T08 [12]	1/3	1/3	1/4	1/3	1/3	1/3
BL88 [13]	1/6	1/9	1/7	1/6	1/8	1/7
Scheme I of TUM05 [14]	1/6	1/9	1/7	1/6	1/8	1/7
Method A of T13 [15]	1/6	1/6	1/4	1/4	1/4	1/3
IYO07 [16]	1/2	1/4	1	1/2	1/2	1
Scheme A of T15 [17] *3	1/6	1	1/7	1/6	1/8	1/7
Scheme A of T15 [17] *4	1/2	1/2	1/7	1/6	1/8	1/7
Proposed scheme *3	1/2	1	1/4	1/3	1/3	1/4
Proposed scheme *4	1/2	1/2	1/4	1/3	1/4	1/4

Table 3 Comparison of the information rates for the access structure of Example 7.

	P_1	P_2	P_3	P_4	P_5	P_6
Linear construction [8]	2/3	2/3	2/3	2/3	2/3	1
Proposed scheme *5	1	1/3	1/2	1/2	1	1

$$\begin{aligned} \Gamma''_0 = \{ & \{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}, \{P_2, P_5\}, \{P_4, P_5\}, \\ & \{P_5, P_6\}\}. \end{aligned}$$

It is known that the optimal information rate for Γ''_0 is 2/3, which is obtained when we employ the linear construction. As mentioned above, the linear construction obtains the optimal information rates for some access structures, but this scheme does not have explicit share assignment algorithms for many access structures. The information rates for $P_i \in \mathcal{P}$ are described in **Table 3**.

Table 3 shows that the proposed scheme can reduce the number of shares distributed to $P \in Q = \{P_1, P_5\}$ though the proposed scheme cannot obtain the optimal information rate.

5. Conclusion

We have proposed a new secret sharing scheme realizing general access structures. Our proposed scheme is perfect and can reduce the number of shares distributed to specified participants. Thus, we can select a subset of participants without restrictions and reduce the number of shares distributed to any participant who belongs to the selected subset as well as the scheme A of T15. The scheme A of T15 is based on authorized subsets. On the other hand, our proposed scheme is based on unauthorized subsets.

Acknowledgments This work was supported by JSPS KAKENHI Grant Number 15K00192.

*1 $Q = \{P_1, P_2\}, \mathcal{A}' = \{\{P_1, P_2\}, \{P_2\}, \phi\}$.
*2 $Q = \{P_5, P_6\}, \mathcal{A}' = \{\{P_5, P_6\}, \{P_5\}, \{P_6\}\}$.
*3 $Q = \{P_2\}, \mathcal{A}' = \{\{P_2\}, \phi\}$.
*4 $Q = \{P_1, P_2\}, \mathcal{A}' = \{\{P_1, P_2\}, \{P_1\}, \{P_2\}, \phi\}$.
*5 $Q = \{P_1, P_5\}, \mathcal{A}' = \{\{P_1\}, \{P_5\}, \phi\}$.

References

[1] Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
[2] Blakley, G.: Safeguarding cryptographic keys, *Proc. AFIPS*, Vol.48, pp.313–317 (1979).
[3] Koyama, K: Cryptographic key sharing methods for multi-groups and security analysis, *Trans. IECE*, Vol.E66, No.1, pp.13–20 (1983).
[4] Simmons, G.: How to (really) share a secret, *Proc. CRYPTO '88*, pp.390–448 (1988).
[5] Simmons, G.: Prepositioned shared secret and/or shared control schemes, *Proc. EUROCRYPT '89*, pp.436–467 (1989).
[6] Tassa, T.: Hierarchical threshold secret sharing, *Journal of Cryptology*, Vol.20, pp.237–264 (2007).
[7] Brickell, E.: Some ideal secret sharing schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol.9, pp.105–113 (1989).
[8] Dijk, M.: A linear construction of secret sharing schemes, *Designs, Codes and Cryptography*, Vol.12, No.2, pp.161–201 (1997).
[9] Stinson, D.R.: Decomposition constructions for secret-sharing schemes, *IEEE Trans. IT*, Vol.40, No.1, pp.118–125 (1994).
[10] Ito, M., Saito, A. and Nishizeki, T.: Secret sharing scheme realizing general access structure, *Proc. IEEE Globecom '87*, pp.99–102 (1987).
[11] Tochikubo, K.: Efficient secret sharing schemes realizing general access structures, *IEICE Trans. Fundamentals*, Vol.E87-A, No.7, pp.1788–1797 (2004).
[12] Tochikubo, K.: Efficient secret sharing schemes based on unauthorized subsets, *IEICE Trans. Fundamentals*, Vol.E91-A, No.10, pp.2860–2867 (2008).
[13] Benaloh, J. and Leichter, J.: Generalized secret sharing and monotone functions, *Proc. CRYPTO '88*, pp.27–35 (1988).
[14] Tochikubo, K., Uyematsu, T. and Matsumoto, R.: Efficient secret sharing schemes based on authorized subsets, *IEICE Trans. Fundamentals*, Vol.E88-A, No.1, pp.322–326 (2005).
[15] Tochikubo, K.: New construction methods of secret sharing schemes based on authorized subsets, *J. Inf. Process.*, Vol.21, No.4, pp.590–598 (2013)
[16] Iwamoto, M., Yamamoto, H. and Ogawa, H.: Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures, *IEICE Trans. Fundamentals*, Vol.E90-A, No.1, pp.101–112 (2007).
[17] Tochikubo, K.: New secret sharing schemes realizing general access structures, *J. Inf. Process.*, Vol.23, No.5, pp.570–578 (2015).
[18] Stinson, D.R.: *Cryptography: Theory and practice 3rd edition*, CRC Press (2005).
[19] Karnin, E.D., Greene, J.W. and Hellman, M.E.: On secret sharing systems, *IEEE Trans. IT*, Vol.29, No.1, pp.35–41 (1983).

Kouya Tochikubo received his B.S. degree from Tokyo University of Science, his M.S. degree from Japan Advanced Institute of Science and Technology and his D.E. degree from Tokyo Institute of Technology in 1996, 1998 and 2004, respectively. He joined the Systems Integration Technology Center, Toshiba Corporation in 1998. Currently, he is an associate professor in the Department of Mathematical Information Engineering, College of Industrial Technology, Nihon University. He was a visiting professor at the University of Waterloo from 2012 to 2013. He received the SCIS Paper Award and the IEICE Best Paper Award in 2002 and 2005, respectively.