Journal of Information Processing Vol.21 No.4 590–598 (Oct. 2013)

[DOI: 10.2197/ipsjjip.21.590]

Regular Paper

New Construction Methods of Secret Sharing Schemes Based on Authorized Subsets

Kouya Tochikubo[1,a)]

Received: November 29, 2012, Accepted: June 14, 2013

Abstract: We propose new construction methods of secret sharing schemes realizing general access structures. Our proposed construction methods are perfect secret sharing schemes and include Shamir's (k, n)-threshold schemes as a special case. Furthermore, except for some access structures for which the efficiency is the same as the previous ones, the proposed construction methods are more efficient than Benaloh and Leichter's scheme and the scheme I of TUM05.

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

1. Introduction

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 [2], [3]. In his schemes, a secret K is divided twice by using (k, n)-threshold schemes. In 1987, Ito, Saito and Nishizeki proposed a secret sharing scheme for general access structures [4]. Their scheme can realize an arbitrary access structure by assigning one or more shares to each participant. In 1988, Benaloh and Leichter proposed a secret sharing scheme for general access structures based on a monotone-circuit [5]. In Ito, Saito and Nishizeki's scheme, the shares are obtained by only one (k, k)-threshold scheme based on unauthorized subsets. In contrast, many (k, k)-threshold schemes are used to obtain shares based on authorized subsets in Benaloh and Leichter's scheme.

Usually, each participant is assigned one share in many secret sharing schemes, including (k, n)-threshold schemes. On the other hand, secret sharing schemes for general access structures are realized by assigning one or more shares to each participant in general. 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 by small shares is desirable. However, Ito, Saito and Nishizeki's scheme and Benaloh and Leichter's scheme are impractical in this respect when the size of the access structure and that of the adversary structure are very large, respectively. For example, when we use these schemes to implement the access structure of a (k, n)-threshold scheme, each of n participants has to hold $\binom{n-1}{k-1}$ shares. Of course, only one share is distributed to each participant if we use Shamir's (k, n)-threshold scheme.

A secret sharing scheme which is always more efficient than Benaloh and Leichter's scheme was proposed (TUM05) [6]. This scheme is also based on authorized subsets. On the other hand, secret sharing schemes which are always more efficient than Ito, Saito and Nishizeki's scheme were proposed [7], [8].

In this paper, we modify the scheme I of TUM05 [6] and the scheme of T08 [8] and propose new construction methods of secret sharing schemes realizing general access structures based on authorized subsets. The proposed construction methods are perfect and can reduce the number of shares distributed to each participant. Furthermore, we show that the proposed construction methods are more efficient than Benaloh and Leichter's scheme [5] and the scheme I of TUM05 [6] from the viewpoint of the number of shares distributed to each participant.

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. 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

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

[1] Department of Mathematical Information Engineering, College of Industrial Technology, Nihon University, Narashino, Chiba 275–8575, Japan

[a)] tochikubo.kouya@nihon-u.ac.jp

For any access structure Γ, there is a family of sets $\bar{\Gamma} = 2^{\mathcal{P}} - \Gamma$. $\bar{\Gamma}$ 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 $\mathcal{S}(A)$ given to a subset $A \subset \mathcal{P}$. 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.

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

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 the 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 [9], [10]. This implies that every 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. Therefore, we assume $\mathcal{K} = \mathcal{S} = Z_p$.

2.3 Secret Sharing Schemes Based Realizing General Access Structures

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, Benaloh and Leichter's scheme [5] is described as follows.

Benaloh and Leichter's scheme:

(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 $P \in A_i$ $(1 \le i \le m)$.

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, the scheme I of TUM05 [6] is described as follows.

Scheme I of TUM05:

(1) Let $\Gamma_{0-} = \{A \in \Gamma_0 : |A| \le l\}$, where $l = \max_{B \in \bar{\Gamma}} |B|$ and represent it as

$$\Gamma_{0-} = \{A_1, A_2, \cdots, A_d\}$$

with $d = |\Gamma_{0-}|$.

(2) Let $\mathcal{P}' = \{P \in X : X \in \Gamma_0 \text{ and } |X| > l\}$ and $n' = |\mathcal{P}'|$. Compute n' shares

$$S = \{s_1, s_2, \cdots, s_{n'}\}$$

for the secret K by using Shamir's $(l + 1, n')$-threshold scheme. Then, one distinct share in S is assigned to each $P \in \mathcal{P}'$.

(3) For every $A_i \in \Gamma_{0-}$, compute $|A_i|$ shares

$$S_i = \{s_{n'+i,1}, s_{n'+i,2}, \cdots, s_{n'+i,|A_i|}\}$$

by using Shamir's $(|A_i|, |A_i|)$-threshold scheme with K as a secret independently for $1 \le i \le d$. One distinct share in S_i is assigned to each $P \in A_i$ $(1 \le i \le d)$.

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

$$\Gamma_0 = \{A_1, A_2, \cdots, A_{10}\}$$

where

$$\begin{aligned} A_1 &= \{P_1, P_2, P_5\}, \\ A_2 &= \{P_1, P_3, P_5\}, \\ A_3 &= \{P_2, P_3, P_5\}, \\ A_4 &= \{P_1, P_3, P_6\}, \\ A_5 &= \{P_1, P_2, P_3, P_4\}, \\ A_6 &= \{P_1, P_2, P_4, P_6\}, \\ A_7 &= \{P_1, P_4, P_5, P_6\}, \\ A_8 &= \{P_2, P_3, P_4, P_6\}, \\ A_9 &= \{P_2, P_4, P_5, P_6\}, \\ A_{10} &= \{P_3, P_4, P_5, P_6\}. \end{aligned}$$

First, we consider Benaloh and Leichter's scheme. In this case, shares are distributed as follows:

$$\begin{aligned} P_1 &: s_{1,1}, s_{2,1}, s_{4,1}, s_{5,1}, s_{6,1}, s_{7,1} \\ P_2 &: s_{1,2}, s_{3,1}, s_{5,2}, s_{6,2}, s_{8,1}, s_{9,1} \\ P_3 &: s_{2,2}, s_{3,2}, s_{4,2}, s_{5,3}, s_{8,2}, s_{10,1} \\ P_4 &: s_{5,4}, s_{6,3}, s_{7,2}, s_{8,3}, s_{9,2}, s_{10,2} \\ P_5 &: s_{1,3}, s_{2,3}, s_{3,3}, s_{7,3}, s_{9,3}, s_{10,3} \\ P_6 &: s_{4,3}, s_{6,4}, s_{7,4}, s_{8,4}, s_{9,4}, s_{10,4} \end{aligned}$$

where $s_{i,j}$ is computed by using Shamir's $(|A_i|, |A_i|)$-threshold scheme with K as a secret $(1 \le i \le 10,\ 1 \le j \le |A_i|)$.

Next, we consider the scheme I of TUM05. Since $l = 3$, we have $\Gamma_{0-} = \{A_1, A_2, A_3, A_4\}$. In this case, we have $\mathcal{P} = \mathcal{P}'$. Compute 6 shares

$$S = \{s'_1, s'_2, \cdots, s'_6\}$$

for the secret K by using Shamir's $(4,6)$-threshold scheme. For A_1, A_2, A_3 and A_4, compute shares as follows:

$$\begin{aligned} S_1 &= \{s'_{7,1}, s'_{7,2}, s'_{7,3}\},\\ S_2 &= \{s'_{8,1}, s'_{8,2}, s'_{8,3}\},\\ S_3 &= \{s'_{9,1}, s'_{9,2}, s'_{9,3}\},\\ S_4 &= \{s'_{10,1}, s'_{10,2}, s'_{10,3}\}, \end{aligned}$$

where $s'_{6+i,j}$ is computed by using Shamir's $(|A_i|, |A_i|)$-threshold scheme with K as a secret $(1 \le i \le 4,\ 1 \le j \le |A_i|)$. In this case, shares are distributed as follows:

$$\begin{aligned} &P_1 : s'_1, s'_{7,1}, s'_{8,1}, s'_{10,1}\\ &P_2 : s'_2, s'_{7,2}, s'_{9,1}\\ &P_3 : s'_3, s'_{8,2}, s'_{9,2}, s'_{10,2}\\ &P_4 : s'_4\\ &P_5 : s'_5, s'_{7,3}, s'_{8,3}, s'_{9,3}\\ &P_6 : s'_6, s'_{10,3}. \end{aligned}$$

The scheme I of TUM05 does not need to generate shares corresponding to the minimal authorized subsets whose sizes are more than $l+1$, where l is the largest size of unauthorized subsets, though it needs an additional share for each participant in $\mathcal{P}'$.

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, the scheme A of T08 [8] 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

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

This scheme can reduce the number of shares distributed to $P \notin Z_i$ $(1 \le i \le r)$.

3. Proposed Construction Method A

Here, we describe a new secret sharing scheme realizing general access structures. The scheme A of T08 [8] can reduce the number of shares distributed to each participant by dividing $\bar{\Gamma}_1$ into disjoint subsets. On the other hand, the proposed construction method A can reduce the number of shares distributed to each participant by dividing Γ_{0-} into disjoint subsets in the same manner as the scheme A of T08. For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, the proposed construction method A is described as follows.

Proposed Construction Method A:

(1) Let $\Gamma_{0-} = \{A \in \Gamma_0 : |A| \le l\}$, where $l = \max_{B \in \bar{\Gamma}} |B|$.

(2) Divide Γ_{0-} into disjoint subsets

$$\Gamma_{0-}^{(0)}, \Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$$

such that $\Gamma_{0-}^{(i)} (1 \le i \le r)$ satisfies

$$\Gamma_{0-}^{(i)} = \{A \in \Gamma_{0-} \ :\ Z_i \subset A\} \text{ and } |\Gamma_{0-}^{(i)}| \ge 2$$

for some $Z_i \subset \mathcal{P}$ and

$$\Gamma_{0-}^{(0)} = \Gamma_{0-} - \bigcup_{1 \le i \le r} \Gamma_{0-}^{(i)}.$$

Let $d_i = \left|\Gamma_{0-}^{(i)}\right|$ and represent $\Gamma_{0-}^{(i)}$ as

$$\Gamma_{0-}^{(i)} = \{A_{i,1}, A_{i,2}, \cdots, A_{i,d_i}\} \ \ (0 \le i \le r).$$

(3) Let $\mathcal{P}' = \{P \in X : X \in \Gamma_0 \text{ and } |X| > l\}$ and $n' = |\mathcal{P}'|$. Compute n' shares

$$S = \{s_1, s_2, \cdots, s_{n'}\}$$

for the secret K by using Shamir's $(l + 1, n')$-threshold scheme. Then, one distinct share in S is assigned to each $P \in \mathcal{P}'$.

(4) For every $A_{0,i} \in \Gamma_{0-}^{(0)}$, compute $|A_{0,i}|$ shares

$$S_i = \{s_{n'+i,1}, s_{n'+i,2}, \cdots, s_{n'+i,|A_{0,i}|}\}$$

by using Shamir's $(|A_{0,i}|, |A_{0,i}|)$-threshold scheme with K as a secret independently for $1 \le i \le d_0$. One distinct share in S_i is assigned to each $P \in A_{0,i}$ $(1 \le i \le d_0)$.

(5) For every Z_i, compute $|Z_i| + 1$ shares

$$S_{d_0+i} = \{s_{n'+d_0+i,1}, s_{n'+d_0+i,2}, \cdots, s_{n'+d_0+i,|Z_i|+1}\}$$

by using Shamir's $(|Z_i|+1, |Z_i|+1)$-threshold scheme with K as a secret independently for $1 \le i \le r$. One distinct share in $S_{d_0+i} - \{s_{n'+d_0+i,1}\}$ is assigned to each $P \in Z_i$ $(1 \le i \le r)$.

(6) For every $A_{i,j} \in \Gamma_{0-}^{(i)}$, if $|A_{i,j} - Z_i| \ge 2$, compute $|A_{i,j} - Z_i|$ shares

$$S'_{i,j} = \{s'_{i,j,1}, s'_{i,j,2}, \cdots, s'_{i,j,|A_{i,j}-Z_i|}\}$$

by using Shamir's $(|A_{i,j}-Z_i|, |A_{i,j}-Z_i|)$-threshold scheme with $s_{n'+d_0+i,1}$ as a secret independently for $1 \le i \le r, 1 \le j \le d_i$. One distinct share in $S'_{i,j}$ is assigned to each $P \in A_{i,j}-Z_i$ $(1 \le i \le r, 1 \le j \le d_i)$. If $|A_{i,j} - Z_i| = 1$, then $s_{n'+d_0+i,1}$ is assigned to $P \in A_{i,j} - Z_i$ $(1 \le i \le r, 1 \le j \le d_i)$.

Example 2: We shall realize the access structure of Example 1 by the proposed construction method A.

- Divide Γ_{0-} into disjoint subsets

$$\begin{aligned}\Gamma_{0-}^{(0)} &= \{A_{0,1}\},\\ \Gamma_{0-}^{(1)} &= \{A_{1,1}, A_{1,2}, A_{1,3}\}\end{aligned}$$

where $A_{0,1} = A_4$ and $A_{1,j} = A_j$ $(1 \le j \le 3)$. In this case,

$$Z_1 = \{P_5\}.$$

- Since $l = 3$ and $|\mathcal{P}'| = |\mathcal{P}| = 6$, compute 6 shares

$$S = \{s_1, s_2, \cdots, s_6\}$$

for the secret K by using Shamir's $(4, 6)$-threshold scheme.

- For $A_{0,1} \in \Gamma_{0-}^{(0)}$, compute $3(= |A_{0,1}|)$ shares

$$S_1 = \{s_{7,1}, s_{7,2}, s_{7,3}\}$$

by using Shamir's $(3, 3)$-threshold scheme with K as a secret.

- For Z_1, compute $2(= |Z_1| + 1)$ shares

$$S_2 = \{s_{8,1}, s_{8,2}\}$$

by using Shamir's $(2, 2)$-threshold scheme with K as a secret.

- For $A_{1,j} \in \Gamma_{0-}^{(1)}$, compute $|A_{1,j} - Z_1|$ shares

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

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

$$S'_{1,3} = \{s'_{1,3,1}, s'_{1,3,2}\},$$

by using Shamir's $(|A_{1,j} - Z_1|, |A_{1,j} - Z_1|)$-threshold scheme with $s_{8,1}$ as a secret $(1 \le j \le 3)$.

- In this case, shares are distributed as follows:

$$\begin{aligned}P_1 &: s_1, s_{7,1}, s'_{1,1,1}, s'_{1,2,1}\\ P_2 &: s_2, s'_{1,1,2}, s'_{1,3,1}\\ P_3 &: s_3, s_{7,2}, s'_{1,2,2}, s'_{1,3,2}\\ P_4 &: s_4\\ P_5 &: s_5, s_{8,2}\\ P_6 &: s_6, s_{7,3}.\end{aligned}$$

The proposed construction method A can reduce the number of shares distributed to each participant in Z_i $(1 \le i \le r)$.

Remarks: In the proposed construction method, once $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$ are determined, Z_i's cannot be determined uniquely. It is difficult to show an algorithm to find optimal $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$ and Z_i's when n and $|\Gamma_0|$ are very large. Here we show a practical algorithm to determine $\Gamma_{0-}^{(i)}$ and Z_i from $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(i-1)}$ though the algorithm cannot guarantee the optimality of $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$ and Z_i's.

(i) Determine $b = \max_{P\in\mathcal{P}} |\{X \in \Gamma_{0-} - \Gamma_{0-}^{(1)} \cup \cdots \cup \Gamma_{0-}^{(i-1)} : P \in X\}|$.

(ii) If $b \ge 2$, select one participant $P \in \mathcal{P}$ such that

$$|\{X \in \Gamma_{0-} - \Gamma_{0-}^{(1)} \cup \cdots \cup \Gamma_{0-}^{(i-1)} : P \in X\}| = b.$$

(iii) If $b \ge 2$, set $Z_i = \{P\}$ and $\Gamma_{0-}^{(i)} = \{X \in \Gamma_{0-} - \Gamma_{0-}^{(1)} \cup \cdots \cup \Gamma_{0-}^{(i-1)} : P \in X\}$.

Here, we show some properties of the proposed construction method A.

Theorem 1 For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ and any access structure $\Gamma(\subset 2^{\mathcal{P}})$, distribute shares for a secret K by using the proposed construction method A. 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 denote the shares in S assigned to $X \subset \mathcal{P}$. Similarly, let X_{S_i} and $X_{S'_{j,k}}$ denote the shares in S_i assigned to X $(1 \le i \le d_0+r)$, the shares in $S'_{j,k}$ assigned to X $(1 \le j \le r, 1 \le k \le d_j)$, respectively. At first, we show $H(K|X) = 0$ for any $X \in \Gamma$.

(Case i) $X \in \Gamma$ and $|X| \ge l + 1$: In this case,

$$|X_S| \ge l + 1.$$

Since $s_1, \cdots, s_{n'}$ are shares computed by Shamir's $(l+1, n')$-threshold scheme with K as a secret, we immediately obtain

$$\begin{aligned}H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}},\\ &\qquad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}})\\ &\le H(K|X_S)\\ &= 0. \end{aligned} \tag{1}$$

(Case ii) $X \le l$ and $A_{0,i} \subset X$ for some $A_{0,i} \in \Gamma_{0-}^{(0)}$: In this case,

$$|X_{S_i}| = |A_{0,i}|.$$

Since $s_{n'+i,1}, \cdots, s_{n'+i,|A_{0,i}|}$ are shares computed by Shamir's $(|A_{0,i}|, |A_{0,i}|)$-threshold scheme with K as a secret, we immediately obtain

$$\begin{aligned}H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}},\\ &\qquad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}})\\ &\le H(K|X_{S_i})\\ &= 0. \end{aligned} \tag{2}$$

(Case iii) $X \le l$ and $A_{i,j} \subset X$ for some $A_{i,j} \in \Gamma_{0-}^{(i)}$ $(1 \le i \le r,\ 1 \le j \le d_i)$: In this case,

$$\left|X_{S'_{i,j}}\right| = \left|S'_{i,j}\right|.$$

Since $s'_{i,j,1}, \cdots, s'_{i,j,|A_{i,j}-Z_i|}$ are shares computed by Shamir's $(|A_{i,j} - Z_i|, |A_{i,j} - Z_i|)$-threshold scheme with $s_{n'+d_0+i,1}$ as a secret, X can recover $s_{n'+d_0+i,1}$. Thus, in this case, we have

$$|X_{S_{d_0+i}}| = |Z_i| + 1.$$

Since $s_{n'+d_0+i,1}, \cdots, s_{n'+d_0+i,|Z_i|+1}$ are shares computed by Shamir's $(|Z_i| + 1, |Z_i| + 1)$-threshold scheme with K as a secret, we obtain

$$\begin{aligned} H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\qquad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}}) \\ &\leq H(K|X_{S_{d_0+i}}, X_{S'_{i,j}}) \\ &= 0. \end{aligned} \tag{3}$$

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

Next we show $H(K|X) = H(K)$ for any $X \notin \Gamma$. For any $X \in \bar{\Gamma}$, we have $|X| \leq l$. This implies

$$H(K|X_S) = H(K). \tag{4}$$

From the property of the access structure and the definition of $\Gamma^{(0)}_{0-}$, for any $A_{0,i} \in \Gamma^{(0)}_{0-}$, we have $A_{0,i} \not\subset X$. Thus, we have

$$H(K|X_{S_i}) = H(K).$$

This implies

$$H(X_{S_i}|K) = H(X_{S_i}). \tag{5}$$

Similarly, from the definition of $\Gamma^{(i)}_{0-}, Z_i$ and $A_{i,j}$ $(1 \leq i \leq r,\ 1 \leq j \leq d_i)$, we have

$$(A_{i,1} - Z_i) \not\subset X,\ (A_{i,2} - Z_i) \not\subset X, \cdots, (A_{i,d_i} - Z_i) \not\subset X$$

or

$$Z_i \not\subset X.$$

Thus, we have

$$H(K|X_{S_{d_0+i}}, X_{S'_{i,1}}, \cdots, X_{S'_{i,d_i}}) = H(K).$$

This also implies

$$\begin{aligned} &H(X_{S_{d_0+i}}, X_{S'_{i,1}}, \cdots, X_{S'_{i,d_i}}|K) \\ &\quad = H(X_{S_{d_0+i}}, X_{S'_{i,1}}, \cdots, X_{S'_{i,d_i}}). \end{aligned} \tag{6}$$

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

$$\begin{aligned} H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\qquad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}}) \\ &= H(K|X_S) \\ &\quad + H(X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\qquad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}}|X_S, K) \\ &\quad - H(X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\qquad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}}|X_S). \end{aligned} \tag{7}$$

From the chain rule for entropy and the definition of $S, S_1, \cdots S_{d_0+r}, S'_{1,1}, \cdots, S'_{r,d_r}$, we have

$$\begin{aligned} &H(X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\quad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}}|X_S, K) \\ &= \sum_{t=1}^{d_0} H(X_{S_t}|X_S, K, X_{S_1}, \cdots, X_{S_{t-1}}) \\ &\quad + \sum_{t=1}^{r} H(X_{S_{d_0+t}}, X_{S'_{t,1}}, \cdots, X_{S'_{t,d_t}}|X_S, K, \\ &\qquad\qquad X_{S_1}, \cdots, X_{S_{d_0+t-1}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\qquad\qquad X_{S'_{2,1}}, \cdots, X_{S'_{t-1,1}}, \cdots X_{S'_{t-1,d_{t-1}}}) \\ &= \sum_{t=1}^{d_0} H(X_{S_t}|K) + \sum_{t=1}^{r} H(X_{S_{d_0+t}}, X_{S'_{t,1}}, \cdots, X_{S'_{t,d_t}}|K) \\ &= \sum_{t=1}^{d_0} H(X_{S_t}) + \sum_{t=1}^{r} H(X_{S_{d_0+t}}, X_{S'_{t,1}}, \cdots, X_{S'_{t,d_t}}). \end{aligned} \tag{8}$$

The last equality comes from Eqs. (5) and (6). On the other hand, we have

$$\begin{aligned} &H(X_{S_1}, \cdots, X_{S_{d_0+r}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\quad X_{S'_{2,1}}, \cdots, X_{S'_{r,1}}, \cdots, X_{S'_{r,d_r}}|X_S) \\ &= \sum_{t=1}^{d_0} H(X_{S_t}|X_S, X_{S_1}, \cdots, X_{S_{t-1}}) \\ &\quad + \sum_{t=1}^{r} H(X_{S_{d_0+t}}, X_{S'_{t,1}}, \cdots, X_{S'_{t,d_t}}|X_S, \\ &\qquad\qquad X_{S_1}, \cdots, X_{S_{d_0+t-1}}, X_{S'_{1,1}}, \cdots, X_{S'_{1,d_1}}, \\ &\qquad\qquad X_{S'_{2,1}}, \cdots, X_{S'_{t-1,1}}, \cdots X_{S'_{t-1,d_{t-1}}}) \\ &\leq \sum_{t=1}^{d_0} H(X_{S_t}) + \sum_{t=1}^{r} H(X_{S_{d_0+t}}, X_{S'_{t,1}}, \cdots, X_{S'_{t,d_t}}). \end{aligned} \tag{9}$$

Substituting Eqs. (4), (8) and (9) into Eq. (7), we obtain $H(K|X) \geq H(K)$. Since $H(K|X) \leq H(K)$ is obvious, we have $H(K|X) = H(K)$. □

The next theorem shows that the proposed construction method A includes Shamir's (k, n)-threshold schemes as a special case.

Theorem 2 Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$. If $\Gamma = \{A \in 2^{\mathcal{P}} : |A| \geq k\}$, then the proposed construction method A coincides with Shamir's (k, n)-threshold scheme.

Proof: In this access structure, we have $l = k - 1$, $n' = n$ and $\Gamma_{0-} = \phi$. Then, $S = \{s_1, s_2, \cdots, s_{n'}\}$ is obtained by using Shamir's $(l+1, n')$-threshold scheme, and one distinct share in S is assigned to each $P \in \mathcal{P}$. Thus, the proposed construction method A coincides with Shamir's (k, n)-threshold scheme. □

Let $N_A(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the proposed construction method A. Similarly, let $N_{BL}(P)$ and $N_{TUM1}(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using Benaloh and Leichter's scheme and the scheme I of TUM05, respectively. The next theorem shows the proposed construction method A is the most efficient of the three from the viewpoint of the number of shares distributed to each participant.

Theorem 3 For any $P \in \mathcal{P}$, the number of shares distributed to P is evaluated as follows:

$$N_A(P) = N_{TUM1}(P) - \sum_{1 \leq i \leq r} |\{P\} \cap Z_i| \cdot (d_i - 1),$$

$$\begin{aligned}N_A(P) = N_{BL}(P) &- \sum_{1\le i\le r} |\{P\}\cap Z_i|\cdot(d_i-1)\\ &-\Big||\{X\in\Gamma_0 : |X|>l, P\in X\}|-1\Big|^+,\end{aligned}$$

where $|x|^+ = \max\{0, x\}$.

Proof: $N_{BL}(P)$ is obtained by

$$N_{BL}(P) = |\{X\in\Gamma_0 : P\in X\}|.$$

Since the scheme I of TUM05 does not need to generate shares corresponding to $X\in\Gamma_0$ such that $|X|>l$ and needs one additional share for $P\in\{P\in X : X\in\Gamma_0 \text{ and } |X|>l\}$ $(=\mathcal{P}')$, we have

$$N_{TUM1}(P) = \begin{cases} |\{X\in\Gamma_{0-} : P\in X\}|+1 & (\text{if } P\in\mathcal{P}')\\ |\{X\in\Gamma_{0-} : P\in X\}| & (\text{if } P\notin\mathcal{P}')\end{cases}$$

for any $P\in\mathcal{P}$.

In the proposed construction method A, Γ_{0-} is divided into disjoint subsets

$$\Gamma_{0-}^{(0)}, \Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$$

and P is assigned only one share for $\Gamma_{0-}^{(i)}$ if $P\in Z_i$ $(1\le i\le r)$. Thus, $N_A(P)$ is obtained by

$$N_A(P) = \begin{cases} \left|\{X\in\Gamma_{0-}^{(0)} : P\in X\}\right|+1 & \\ \quad +\sum_{1\le i\le r}|\{P\}\cap Z_i| & (\text{if } P\in\mathcal{P}')\\ \quad +\sum_{1\le i\le r}\left|\{X\in\Gamma_{0-}^{(i)} : P\in X-Z_i\}\right| & \\ & \\ \left|\{X\in\Gamma_{0-}^{(0)} : P\in X\}\right| & \\ \quad +\sum_{1\le i\le r}|\{P\}\cap Z_i| & (\text{if } P\notin\mathcal{P}')\\ \quad +\sum_{1\le i\le r}\left|\{X\in\Gamma_{0-}^{(i)} : P\in X-Z_i\}\right| & \end{cases}$$

for any $P\in\mathcal{P}$.

On the other hand, from the definition of Z_i, we have

$$\begin{aligned}\left|\{X\in\Gamma_{0-}^{(i)} : P\in X\}\right| &= \left|\{X\in\Gamma_{0-}^{(i)} : P\in X-Z_i\}\right|\\ &\quad +|\{P\}\cap Z_i|\cdot d_i\end{aligned}$$

for any $1\le i\le r$. Theorem 3 is easily obtained by the above equations. □

Remarks: Since $d_i\ge 2$ $(1\le i\le r)$, we have

$$N_A(P)\le N_{BL}(P) \text{ and } N_A(P)\le N_{TUM1}(P)$$

for any $P\in\mathcal{P}$ and Γ. This shows that the proposed construction method A is more efficient than Benaloh and Leichter's scheme [5] and the scheme I of TUM05 [6].

4. Proposed Construction Method B

For $\mathcal{P}=\{P_1,P_2,\cdots,P_n\}$, $K\in\mathcal{K}$ and Γ, the proposed construction method B is described as follows.

Proposed Construction Method B:

(1) Let $\Gamma_{0-}=\{A\in\Gamma_0 : |A|\le l\}$, where $l=\max_{B\in\bar{\Gamma}}|B|$.

(2) Divide Γ_{0-} into disjoint subsets

$$\Gamma_{0-}^{(0)}, \Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$$

such that $\Gamma_{0-}^{(i)}(1\le i\le r)$ satisfies

$$\Gamma_{0-}^{(i)} = \{Z_i\cup C : C\subset Y_i \text{ and } |C|=e_i\} \text{ and } |\Gamma_{0-}^{(i)}|\ge 2$$

for some $e_i(1\le e_i\le l-1)$, $Y_i\subset\mathcal{P}$ and $Z_i\subset\mathcal{P}$ $(Y_i\cap Z_i=\phi)$ and

$$\Gamma_{0-}^{(0)} = \Gamma_{0-} - \bigcup_{1\le i\le r}\Gamma_{0-}^{(i)}.$$

Let $d=\left|\Gamma_{0-}^{(0)}\right|$ and represent $\Gamma_{0-}^{(0)}$ as

$$\Gamma_{0-}^{(0)} = \{A_1, A_2, \cdots, A_d\}.$$

(3) Let $\mathcal{P}'=\{P\in X : X\in\Gamma_0 \text{ and } |X|>l\}$ and $n'=|\mathcal{P}'|$. Compute n' shares

$$S=\{s_1,s_2,\cdots,s_{n'}\}$$

for the secret K by using Shamir's $(l+1,n')$-threshold scheme. Then, one distinct share in S is assigned to each $P\in\mathcal{P}'$.

(4) For every $A_i\in\Gamma_{0-}^{(0)}$, compute $|A_i|$ shares

$$S_i=\{s_{n'+i,1}, s_{n'+i,2},\cdots,s_{n'+i,|A_i|}\}$$

by using Shamir's $(|A_i|,|A_i|)$-threshold scheme with K as a secret independently for $1\le i\le d$. One distinct share in S_i is assigned to each $P\in A_i$ $(1\le i\le d)$.

(5) For every Z_i, compute $|Z_i|+1$ shares

$$S_{d+i}=\{s_{n'+d+i,1}, s_{n'+d+i,2},\cdots,s_{n'+d+i,|Z_i|+1}\}$$

by using Shamir's $(|Z_i|+1,|Z_i|+1)$-threshold scheme with K as a secret independently for $1\le i\le r$. One distinct share in $S_{d+i}-\{s_{n'+d+i,1}\}$ is assigned to each $P\in Z_i$ $(1\le i\le r)$.

(6) For every Y_i, if $e_i\ge 2$, compute $|Y_i|$ shares

$$S'_i=\{s'_{i,1}, s'_{i,2},\cdots,s'_{i,|Y_i|}\}$$

by using Shamir's $(e_i,|Y_i|)$-threshold scheme with $s_{n'+d+i,1}$ as a secret independently for $1\le i\le r$. One distinct share in S'_i is assigned to each $P\in Y_i$ $(1\le i\le r)$. If $e_i=1$, then $s_{n'+d+i,1}$ is assigned to all $P\in Y_i$ $(1\le i\le r)$.

Example 3: We shall realize the access structure of Example 1 by the proposed construction method B.

- Divide Γ_{0-} into disjoint subsets

  $$\Gamma_{0-}^{(0)}, \Gamma_{0-}^{(1)}$$

  where

  $$\begin{aligned}\Gamma_{0-}^{(0)} &= \{A_4\},\\ \Gamma_{0-}^{(1)} &= \{A_1,A_2,A_3\}.\end{aligned}$$

  In this case,

  $$\begin{aligned}Y_1 &= \{P_1,P_2,P_3\},\\ Z_1 &= \{P_5\},\\ e_1 &= 2.\end{aligned}$$

- Since $l=3$ and $|\mathcal{P}'|=|\mathcal{P}|=6$, compute 6 shares

  $$S=\{s_1,s_2,\cdots,s_6\}$$

  for the secret K by using Shamir's $(4,6)$-threshold scheme.

- For $A_4\in\Gamma_{0-}^{(0)}$, compute $3(=|A_4|)$ shares

$$S_1 = \{s_{7,1}, s_{7,2}, s_{7,3}\}$$

by using Shamir's $(3, 3)$-threshold scheme with K as a secret.

- For Z_1, compute $2(= |Z_1| + 1)$ shares

$$S_2 = \{s_{8,1}, s_{8,2}\}$$

by using Shamir's $(2, 2)$-threshold scheme with K as a secret.

- Since $e_1 = 2$, compute $3(= |Y_i|)$ shares

$$S'_1 = \{s'_{1,1}, s'_{1,2}, s'_{1,3}\}$$

by using Shamir's $(2, 3)$-threshold scheme with $s_{8,1}$ as a secret.

- In this case, shares are distributed as follows:

$$\begin{aligned} P_1 &: s_1, s_{7,1}, s'_{1,1} \\ P_2 &: s_2, s'_{1,2} \\ P_3 &: s_3, s_{7,2}, s'_{1,3} \\ P_4 &: s_4 \\ P_5 &: s_5, s_{8,2} \\ P_6 &: s_6, s_{7,3}. \end{aligned}$$

The proposed construction method B can also reduce the number of shares distributed to each participant in Y_1 $(1 \le i \le r)$.

Remarks: In the proposed construction method B, Y_i's and Z_i's cannot be determined uniquely either. It is difficult to show an algorithm to find optimal $\Gamma^{(1)}_{0-}, \cdots, \Gamma^{(r)}_{0-}$, Y_i's and Z_i's when n and $|\Gamma_0|$ are very large. Here we show an algorithm to find Y_i's and Z_i's.

- For every $Z \subset \mathcal{P}$, define

$$\mathcal{A} = \{A - Z : Z \subset A \in \Gamma_{0-}\}.$$

- Next, for every $Y \subset \mathcal{P}$, check whether $\{C \subset Y : |C| = e\}$ is a subset of $\mathcal{A}$ or not $(1 \le e \le l - 1)$.
- If $\{C \subset Y : |C| = e\} \subset \mathcal{A}$ for some Y and e, then Y and Z satisfy the condition (2) of the proposed construction method B.

Here, we show some properties of the proposed construction method B.

Theorem 4 For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ and any access structure $\Gamma (\subset 2^{\mathcal{P}})$, distribute shares for a secret K by using the proposed construction method B. 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 denote the shares in S assigned to $X \subset \mathcal{P}$. Similarly, let X_{S_i} and $X_{S'_j}$ denote the shares in S_i assigned to X $(1 \le i \le d + r)$ and the shares in S'_j assigned to X $(1 \le j \le r)$, respectively. At first, we show $H(K|X) = 0$ for any $X \in \Gamma$.

(Case i) $X \in \Gamma$ and $|X| \ge l + 1$: In this case,

$$|X_S| \ge l + 1.$$

Since $s_1, \cdots, s_{n'}$ are shares computed by Shamir's $(l + 1, n')$-threshold scheme with K as a secret, we immediately obtain

$$\begin{aligned} H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r}) \\ &\le H(K|X_S) \\ &= 0. \end{aligned} \tag{10}$$

(Case ii) $X \le l$ and $A_i \subset X$ for some $A_i \in \Gamma^{(0)}_{0-}$: In this case,

$$|X_{S_i}| = |A_i|.$$

Since $s_{n'+i,1}, \cdots, s_{n'+i,|A_i|}$ are shares computed by Shamir's $(|A_i|, |A_i|)$-threshold scheme with K as a secret, we immediately obtain

$$\begin{aligned} H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r}) \\ &\le H(K|X_{S_i}) \\ &= 0. \end{aligned} \tag{11}$$

(Case iii) $X \le l$ and $A \subset X$ for some $A \in \Gamma^{(i)}_{0-}$ $(1 \le i \le r)$: In this case,

$$|X_{S_{d+i}}| = |Z_i| \text{ and } |X_{S'_i}| \ge e_i.$$

Since $s_{n'+d+i,1}, \cdots, s_{n'+d+i,|Z_i|+1}$ are shares computed by Shamir's $(|Z_i| + 1, |Z_i| + 1)$-threshold scheme with K as a secret and $s'_{i,1}, \cdots, s'_{i,|Y_i|}$ are shares computed by Shamir's $(e_i, |Y_i|)$-threshold scheme with $s_{n'+d+i,1}$ as a secret, we obtain

$$\begin{aligned} H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r}) \\ &\le H(K|X_{S_{d+i}}, X_{S'_i}) \\ &= 0. \end{aligned} \tag{12}$$

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 $X \notin \Gamma$. For any $X \in \bar{\Gamma}$, we have $|X| \le l$. This implies

$$H(K|X_S) = H(K). \tag{13}$$

From the property of the access structure and the definition of $\Gamma^{(0)}_{0-}$, for any $A_i \in \Gamma^{(0)}_{0-}$, we have $A_i \not\subset X$. Thus, we have

$$H(K|X_{S_i}) = H(K).$$

This implies

$$H(X_{S_i}|K) = H(X_{S_i}). \tag{14}$$

Similarly, from the definition of $\Gamma^{(i)}_{0-}$, Y_i and Z_i $(1 \le i \le r)$, we have

$$Z_i \not\subset X \text{ or } |X \cap Y_i| \le e_i - 1.$$

Thus, we have

$$H(K|X_{S_{d+i}}, X_{S'_i}) = H(K).$$

This also implies

$$H(X_{S_{d+i}}, X_{S'_i}|K) = H(X_{S_{d+i}}, X_{S'_i}). \tag{15}$$

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

$$\begin{aligned} H(K|X) &= H(K|X_S, X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r}) \\ &= H(K|X_S) \end{aligned}$$

$$
\begin{aligned}
&+ H(X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r} | X_S, K) \\
&- H(X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r} | X_S). \qquad (16)
\end{aligned}
$$

From the chain rule for entropy and the definition of $S, S_1, \cdots S_{d+r}, S'_1, \cdots, S'_r$, we have

$$
\begin{aligned}
&H(X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r} | X_S, K) \\
&= \sum_{t=1}^{d} H(X_{S_t} | X_S, K, X_{S_1}, \cdots, X_{S_{t-1}}) \\
&\quad + \sum_{t=1}^{r} H(X_{S_{d+t}}, X_{S'_t} | X_S, K, X_{S_1}, \cdots, X_{S_{d+t-1}}, X_{S'_1}, \cdots X_{S'_{t-1}}) \\
&= \sum_{t=1}^{d} H(X_{S_t} | K) + \sum_{t=1}^{r} H(X_{S_{d+t}}, X_{S'_t} | K) \\
&= \sum_{t=1}^{d} H(X_{S_t}) + \sum_{t=1}^{r} H(X_{S_{d+t}}, X_{S'_t}). \qquad (17)
\end{aligned}
$$

The last equality comes from Eqs. (14) and (15). On the other hand, we have

$$
\begin{aligned}
&H(X_{S_1}, \cdots, X_{S_{d+r}}, X_{S'_1}, \cdots X_{S'_r} | X_S) \\
&= \sum_{t=1}^{d} H(X_{S_t} | X_S, X_{S_1}, \cdots, X_{S_{t-1}}) \\
&\quad + \sum_{t=1}^{r} H(X_{S_{d+t}}, X_{S'_t} | X_S, X_{S_1}, \cdots, X_{S_{d+t-1}}, X_{S'_1}, \cdots X_{S'_{t-1}}) \\
&\leq \sum_{t=1}^{d} H(X_{S_t}) + \sum_{t=1}^{r} H(X_{S_{d+t}}, X_{S'_t}). \qquad (18)
\end{aligned}
$$

Substituting Eqs. (13), (17) and (18) into Eq. (16), we obtain $H(K|X) \geq H(K)$. Since $H(K|X) \leq H(K)$ is obvious, we have $H(K|X) = H(K)$. □

The next theorem shows that the proposed construction method B includes Shamir's (k, n)-threshold schemes as a special case.

Theorem 5 Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$. If $\Gamma = \{A \in 2^{\mathcal{P}} : |A| \geq k\}$, then the proposed construction method B coincides with Shamir's (k, n)-threshold scheme.

Proof: In this access structure, we have $l = k - 1$, $n' = n$ and $\Gamma_{0-} = \phi$. Then, $S = \{s_1, s_2, \cdots, s_{n'}\}$ is obtained by using Shamir's $(l+1, n')$-threshold scheme, and one distinct share in S is assigned to each $P \in \mathcal{P}$. Thus, the proposed construction method B coincides with Shamir's (k, n)-threshold scheme. □

Let $N_B(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the proposed construction method B. The next theorem shows the efficiency of the proposed construction method B.

Theorem 6 For any $P \in \mathcal{P}$, the number of shares distributed to P is evaluated as follows:

$$
\begin{aligned}
N_B(P) &= N_{TUM1}(P) \\
&\quad - \sum_{1 \leq i \leq r} \left| |\{X \in \Gamma_{0-}^{(i)} : P \in X\}| - 1 \right|^+, \\
N_B(P) &= N_{BL}(P) \\
&\quad - \sum_{1 \leq i \leq r} \left| |\{X \in \Gamma_{0-}^{(i)} : P \in X\}| - 1 \right|^+ \\
&\quad - \left| |\{X \in \Gamma_0 : |X| > l, P \in X\}| - 1 \right|^+,
\end{aligned}
$$

where $|x|^+ = \max\{0, x\}$.

Proof: In the proposed construction method B, Γ_{0-} is divided into disjoint subsets

$$\Gamma_{0-}^{(0)}, \Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$$

and P is assigned one share for $\Gamma_{0-}^{(i)}$ if $P \in Y_i \cup Z_i$ $(1 \leq i \leq r)$. Thus, $N_B(P)$ is obtained by

$$
N_B(P) = \begin{cases}
\left| \{X \in \Gamma_{0-}^{(0)} : P \in X\} \right| + 1 \\
\quad + \sum_{1 \leq i \leq r} |\{P\} \cap (Y_i \cup Z_i)| \quad (\text{if } P \in \mathcal{P}') \\
\left| \{X \in \Gamma_{0-}^{(0)} : P \in X\} \right| \\
\quad + \sum_{1 \leq i \leq r} |\{P\} \cap (Y_i \cup Z_i)| \quad (\text{if } P \notin \mathcal{P}')
\end{cases}
$$

for any $P \in \mathcal{P}$. Theorem 6 is easily obtained by the above equation and the result of Theorem 3. □

5. Analysis of the Proposed Construction Methods

We can consider that Benaloh and Leichter's scheme realizes any access structure from the description of the boolean circuit. There is a one-to-one correspondence between a boolean circuit and a boolean formulae which contain the operators ∧ ("and") and ∨ ("or"). It is easy to construct a boolean circuit from the disjunctive normal form boolean formula

$$\bigvee_{A \in \Gamma_0} \left(\bigwedge_{P_i \in A} P_i \right).$$

Since the scheme I of TUM05 does not need to generate shares corresponding to the minimal authorized subsets in $\Gamma_0 - \Gamma_{0-}$, the boolean formula for the scheme I of TUM05 is

$$\bigvee_{A \in \Gamma_{0-}} \left(\bigwedge_{P_i \in A} P_i \right).$$

For the access structure of Example 1, the scheme I of TUM05 has only to deal with

$$
\begin{aligned}
&(P_1 \wedge P_2 \wedge P_5) \vee (P_1 \wedge P_3 \wedge P_5) \\
&\quad \vee (P_2 \wedge P_3 \wedge P_5) \vee (P_1 \wedge P_3 \wedge P_6).
\end{aligned}
$$

On the other hand, we can consider that the proposed construction method A converts the boolean formula as follows:

$$
\begin{aligned}
&\overbrace{((\underbrace{(P_1 \wedge P_2) \vee (P_1 \wedge P_3) \vee (P_2 \wedge P_3)}_{(*)}) \wedge \underbrace{P_5}_{Z_1})}^{\Gamma_{0-}^{(1)}} \\
&\quad \vee (P_1 \wedge P_3 \wedge P_6).
\end{aligned}
$$

Thus, the proposed construction method A can reduce the number of shares distributed to each participant in Z_1. Of course, in order to reduce the number of shares the technique of this method can be applied for the boolean formula $(*)$ again.

Next, we consider the proposed construction method B. The technique of this method can be applied for more special access structures. In fact, the boolean formula $(*)$ is the access structure of the $(2, 3)$-threshold scheme where

$$\mathcal{P} = \{P_1, P_2, P_3\}.$$

Consequently, the proposed construction method B can also reduce the number of shares distributed to each participant in Y_1.

It is difficult to say which is better since the efficiencies of the proposed construction methods depend on the access structures.

In the proposed construction methods, $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$ 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 optimal $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$, Z_i's (and Y_i's). Of course, we can choose $r = 0$. Then, the proposed construction methods are equivalent to the scheme I of TUM05 and shares are distributed to each participant uniquely. Thus, in the proposed construction methods, we can select r flexibly in accordance with the intended use.

Since access structures are the family of sets in $\{P_1, \cdots, P_n\}$, there are $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$ of the proposed construction methods for many access structures. Here we consider the possible access structures for up to four participants. As shown in [9], there are 18 non-isomorphic access structures as follows:

$$\Gamma_{0,2-1} = \{\{P_1, P_2\}\}$$
$$\Gamma_{0,3-1} = \{\{P_1, P_2\}, \{P_2, P_3\}\}$$
$$\Gamma_{0,3-2} = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3\}\}$$
$$\Gamma_{0,3-3} = \{\{P_1, P_2, P_3\}\}$$
$$\Gamma_{0,4-1} = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\}$$
$$\Gamma_{0,4-2} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}$$
$$\Gamma_{0,4-3} = \{\{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_3, P_4\}\}$$
$$\Gamma_{0,4-4} = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\}$$
$$\Gamma_{0,4-5} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}\}$$
$$\Gamma_{0,4-6} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\}$$
$$\Gamma_{0,4-7} = \{\{P_1, P_2, P_3\}, \{P_1, P_4\}\}$$
$$\Gamma_{0,4-8} = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}\}$$
$$\Gamma_{0,4-9} = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}$$
$$\Gamma_{0,4-10} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}\}$$
$$\Gamma_{0,4-11} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_3, P_4\}\}$$
$$\Gamma_{0,4-12} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}\}$$
$$\Gamma_{0,4-13} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3, P_4\}\}$$
$$\Gamma_{0,4-14} = \{\{P_1, P_2, P_3, P_4\}\}.$$

$\Gamma_{0,2-1}, \Gamma_{0,3-2}, \Gamma_{0,3-3}, \Gamma_{0,4-6}, \Gamma_{0,4-11}, \Gamma_{0,4-13}$ and $\Gamma_{0,4-14}$ are access structures in which $\Gamma_{0-}^{(1)}, \cdots, \Gamma_{0-}^{(r)}$ of the proposed construction methods cannot be found. However the proposed construction methods can obtain the optimal assignments for $\Gamma_{0,2-1}, \Gamma_{0,3-2}, \Gamma_{0,3-3}, \Gamma_{0,4-6}, \Gamma_{0,4-13}$ and $\Gamma_{0,4-14}$. As a result, we know that the proposed construction methods cannot reduce the number of shares for $\Gamma_{0,4-11}$.

6. Conclusion

We have proposed new construction methods of secret sharing schemes realizing general access structures. Our proposed construction methods are perfect secret sharing schemes and can reduce the number of shares distributed to each participant. Furthermore, our proposed construction methods include Shamir's (k, n)-threshold schemes as a special case.

Acknowledgments This work was supported by KAKENHI 20700073.

References

[1] Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).

[2] Koyama, K.: Sharing cryptographic keys in multi-groups and its analysis, *Journal of IPSJ*, Vol.22, No.2, pp.81–88 (1981) (in Japanese).

[3] Koyama, K.: Cryptographic key sharing methods for multi-groups and security analysis, *IECE Trans.*, Vol.E66, No.1, pp.13–20 (1983).

[4] Ito, M., Saito, A. and Nishizeki, T.: Secret sharing scheme realizing general access structure, *Proc. IEEE Globecom '87*, pp.99–102 (1987).

[5] Benaloh, J. and Leichter, J.: Generalized secret sharing and monotone functions, *Proc. CRYPTO '88*, pp.27–35 (1988).

[6] 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).

[7] 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).

[8] Tochikubo, K.: Efficient secret sharing schemes based on unauthorized subsets, *IEICE Trans. Fundamentals*, Vol.E91-A, No.10, pp.2860–2867 (2008).

[9] Stinson, D.R.: Cryptography: Theory and practice 3rd edition, CRC Press (2005).

[10] 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, M.S. degree from Japan Advanced Institute of Science and Technology and D.E. degree from Tokyo Institute of Technology in 1996, 1998 and 2004, respectively. He joined 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 received the SCIS Paper Award and the IEICE Best Paper Award in 2002 and 2005, respectively.