Journal of Information Processing Vol.23 No.5 570–578 (Sep. 2015)

[DOI: 10.2197/ipsjjip.23.570]

Regular Paper

New Secret Sharing Schemes Realizing General Access Structures

Kouya Tochikubo[1,a)]

Received: November 13, 2014, Accepted: June 5, 2015

Abstract: We propose new secret sharing schemes realizing general access structures. Our proposed schemes are perfect secret sharing schemes and can reduce the number of shares distributed to specified participants. Furthermore, for any access structure, the proposed schemes are more efficient than the previous results based on authorized subsets.

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

1. Introduction

In Shamir's (k, n)-threshold scheme [1], every 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 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 is very large. 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. On the other hand, only one share is distributed to each participant if we employ Shamir's (k, n)-threshold scheme.

Secret sharing schemes based on unauthorized subsets have also been proposed [6], [7]. These schemes can realize any access structures by using two or more threshold schemes and are more efficient than Ito, Saito and Nishizeki's scheme. A secret sharing scheme based on authorized subsets was proposed (TUM05) [8]. This scheme is always more efficient than Benaloh and Leichter's scheme. Iwamoto, Yamamoto and Ogawa proposed a secret sharing by integer programming [9]. Their scheme is optimal from the viewpoint of the number of shares distributed to each participant when only one threshold scheme is used.

Suppose that we want to apply secret sharing schemes to a company in order to prevent the client information from leaking out. The client information is encrypted with a key. And the key is divided into shares. Because of the hierarchy structure of the company, some managers may belong to a lot of authorized subsets and unauthorized subsets. As a result, the managers have to hold a lot of shares. Here, we consider a section which consists of two managers and 20 staff members. The secret key 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 20 maximal unauthorized subsets. On the other hand, every staff member belongs to 38 minimal authorized subsets and 3 maximal unauthorized subsets. We shall realize this access structure by Benaloh and Leichter's scheme. Then, each manager has to hold 191 shares and each staff member has to hold 38 shares. By contrast, we can reduce the number of shares distributed to each manager to 2 if we employ one of our proposed schemes. Thus, secret sharing schemes reducing the numbers of shares distributed to specified participants are quite useful.

In this paper, we modify Benaloh and Leichter's scheme [5] and the scheme I of TUM05 [8] and propose new secret sharing schemes realizing general access structures, which are perfect and can reduce the number of shares distributed to specified participants. The proposed schemes are more efficient than Benaloh and Leichter's scheme [5] and the scheme I of TUM05 [8] 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 distributes a share to each

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

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

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

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

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.

In general, the efficiency of a perfect secret sharing scheme is measured by the information rate ρ [10] 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. 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 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 and ideal [10], [11]. 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 [*1]. 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 [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 $P \in A_i$ $(1 \le i \le m)$.

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 $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, the scheme I of TUM05 [8] 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 $n' = |\mathcal{P}'|$.

[*1] The shares of the proposed schemes do not depend on the mechanism of Shamir's (k, n)-threshold scheme. Any ideal threshold schemes can be used instead of Shamir's (k, n)-threshold scheme with $k \ne n$, and more simple schemes can be used instead of Shamir's (n, n)-threshold scheme.

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 $1 \leq i \leq d$. One distinct share in S_i is assigned to each $P \in A_i$ $(1 \leq i \leq d)$.

Example 2: We shall realize the access structure of Example 1 by the the scheme I of TUM05. For this access structure, $\bar{\Gamma}_1$ is given by

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

Since $l = \max_{B\in\bar{\Gamma}} |B| = \max_{B\in\bar{\Gamma}_1} |B| = 4$, 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 $(5, 6)$-threshold scheme. For A_1, A_2, A_3 and A_4, compute shares as follows:

$$\begin{aligned}S_1 &= \{s_{7,1}, s_{7,2}, s_{7,3}, s_{7,4}\},\\ S_2 &= \{s_{8,1}, s_{8,2}, s_{8,3}, s_{8,4}\},\\ S_3 &= \{s_{9,1}, s_{9,2}, s_{9,3}, s_{9,4}\},\\ S_4 &= \{s_{10,1}, s_{10,2}, s_{10,3}, s_{10,4}\},\end{aligned}$$

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

$$\begin{aligned}P_1 &: s_1, s_{7,1}\\ P_2 &: s_2, s_{7,2}, s_{8,1}, s_{9,1}\\ P_3 &: s_3, s_{8,2}, s_{10,1}\\ P_4 &: s_4, s_{9,2}, s_{10,2}\\ P_5 &: s_5, s_{7,3}, s_{8,3}, s_{9,3}, s_{10,3}\\ P_6 &: s_6, s_{7,4}, s_{8,4}, s_{9,4}, s_{10,4}.\end{aligned}$$

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 $\mathcal{P}'$.

3. Proposed Scheme A

Here, we modify Benaloh and Leichter's scheme [5] 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 into Γ_0 according to the subsets of Q. On the other hand, the number of shares distributed to $P \in \mathcal{P} - Q$ is equal to that of Benaloh and Leichter's scheme.

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

Proposed Scheme A:

(1) Let $\mathcal{A}' = \{C \subset Q : Q \cap A = C$ 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

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

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

- 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. 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 $1 \le i \le 2$. 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 $1 \le i \le 3, 1 \le j \le |\mathcal{A}_i|$.

- In this case, shares are distributed as follows:

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

The proposed scheme A can reduce the number of shares distributed to each participant $P \in \mathcal{Q}(\subset \mathcal{P})$. On the other hand, for any $P \in \mathcal{P} - \mathcal{Q}$, the number of shares distributed to P is equal to that of Benaloh and Leichter's scheme. Here, we show some properties of the proposed scheme A.

Theorem 1 Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be a set of n participants. For any $\mathcal{Q}(\subset \mathcal{P})$ and any access structure $\Gamma(\subset 2^{\mathcal{P}})$, distribute shares for a secret K by using the proposed scheme 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 $X_{S_{1,i}}$ and $X_{S_{2,i,j}}$ denote the shares in $S_{1,i}$ and $S_{2,i,j}$ assigned to X, respectively($1 \le i \le m, 1 \le j \le |\mathcal{A}_i|$). 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

$$C'_i \cup C_{ij} = A \subset X.$$

In this case, we have

$$|X_{S_{1,i}}| = |C'_i| \text{ and } |X_{S_{2,i,j}}| = |C_{ij}|.$$

X can recover w_i since $s_{i,j,1}, s_{i,j,2}, \cdots, s_{i,j,|C_{ij}|}$ are shares computed by Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with w_i as a secret. Similarly, If $C'_i \neq \phi$, X can recover w'_i since $s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|C'_i|}$ are shares computed by Shamir's $(|C'_i|, |C'_i|)$-threshold scheme with w'_i as a secret. From the definition of S_i, we immediately obtain

$$\begin{aligned} &H(K|X) \\ &= H(K|X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}) \\ &\le H(K|X_{S_{1,i}}, X_{S_{2,i,j}}) \\ &= 0. \end{aligned}$$

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 $\mathcal{A}_i, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, for any $A_i \in \Gamma_0$, we have

$$C'_i \not\subset X \text{ or } C_{ij} \not\subset X \ (1 \le j \le |\mathcal{A}_i|).$$

This implies

$$H(K|X_{S_{1,i}}, X_{S_{2,i,j}}) = H(K).$$

for $1 \le i \le m, 1 \le j \le |\mathcal{A}_i|$. From the definition of S_i, we have

$$H(K|X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}) = H(K)$$

for $1 \le i \le m$. This implies

$$\begin{aligned} &H(X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}|K) \\ &= H(X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}). \end{aligned} \tag{1}$$

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

$$\begin{aligned} &H(K|X) \\ &= H(K|X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}) \\ &= H(K) \\ &\quad +H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}|K) \\ &\quad -H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}). \end{aligned} \tag{2}$$

From the chain rule for entropy, we have

$$H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}|K)$$

$$
\begin{aligned}
&= \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}} | K, X_{S_{1,1}}, \cdots \\
&\qquad \cdots, X_{S_{1,t-1}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,t-1,|\mathcal{A}_{t-1}|}}) \\
&\overset{(*)}{=} \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}} | K) \\
&= \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}). \qquad (3)
\end{aligned}
$$

Here, $(*)$ comes from the fact that $X_{S_{1,1}}, \cdots, X_{S_{1,m}}$ and $X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}$ are mutually independent and the last equality comes from Eq. (1). On the other hand, we have

$$
\begin{aligned}
&H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}) \\
&= \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}} | X_{S_{1,1}}, \cdots \\
&\qquad \cdots, X_{S_{1,t-1}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,t-1,|\mathcal{A}_{t-1}|}}) \\
&\leq \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}). \qquad (4)
\end{aligned}
$$

Substituting Eqs. (3) and (4) into Eq. (2), 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 scheme A includes Benaloh and Leichter's scheme as a special case.

Theorem 2 If $Q = \phi$, then the proposed scheme A coincides with Benaloh and Leichter's scheme.

Proof: Since $Q = \phi$, we have

$$\mathcal{A}' = \{C'_1\}, C'_1 = \phi$$

and

$$\mathcal{A}_1 = \Gamma_0.$$

Thus, the proposed scheme A coincides with Benaloh and Leichter's scheme. □

Let $N_A(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the proposed scheme A. Similarly, let $N_{BL}(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using Benaloh and Leichter's scheme. The next theorem shows the proposed scheme A is more efficient than Benaloh and Leichter's scheme from the viewpoint of the number of shares distributed to each participant in $Q(\subset \mathcal{P})$.

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

$$
N_A(P) = \begin{cases} N_{BL}(P) - \sum_{i=1}^{m} |\{P\} \cap C'_i|(|\mathcal{A}_i| - 1) & (P \in Q) \\ N_{BL}(P) & (P \notin Q). \end{cases}
$$

Proof: From the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, $N_A(P)$ is obtained by

$$
\begin{aligned}
N_A(P) &= |\{C' \in \mathcal{A}' : P \in C'\}| \\
&= \sum_{i=1}^{m} |\{P\} \cap C'_i| \qquad (5)
\end{aligned}
$$

for $P \in Q$. On the other hand, $N_{BL}(P)$ is obtained by

$$N_{BL}(P) = |\{X \in \Gamma_0 : P \in X\}|. \qquad (6)$$

From the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, we have

$$\{X \in \Gamma_0 : P \in X\} = \bigcup_{i=1}^{m} \{C'_i \cup C : P \in C'_i, C \in \mathcal{A}_i\} \qquad (7)$$

for $P \in Q$. From Eqs. (6) and (7), we have

$$
\begin{aligned}
N_{BL}(P) &= \sum_{i=1}^{m} |\{C'_i \cup C : P \in C'_i, C \in \mathcal{A}_i\}| \\
&= \sum_{i=1}^{m} |\{P\} \cap C'_i| \cdot |\mathcal{A}_i| \qquad (8)
\end{aligned}
$$

for $P \in Q$.

Similarly, $N_A(P)$ is obtained by

$$N_A(P) = \sum_{i=1}^{m} |\{C \in \mathcal{A}_i : P \in C\}| \qquad (9)$$

for $P \notin Q$. From the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, we have

$$\{X \in \Gamma_0 : P \in X\} = \bigcup_{i=1}^{m} \{C'_i \cup C : P \in C \in \mathcal{A}_i\} \qquad (10)$$

for $P \notin Q$. From Eqs. (6) and (10), we have

$$
\begin{aligned}
N_{BL}(P) &= \sum_{i=1}^{m} |\{C'_i \cup C : P \in C \in \mathcal{A}_i\}| \\
&= \sum_{i=1}^{m} |\{C \in \mathcal{A}_i : P \in C\}| \qquad (11)
\end{aligned}
$$

for $P \notin Q$. Theorem 3 is easily obtained by Eqs. (5), (8), (9) and (11). □

4. Proposed Scheme B

The proposed scheme A can reduce the number of shares distributed to $P \in Q$, but the number of shares distributed to $P \in \mathcal{P} - Q$ is equal to that of Benaloh and Leichter's scheme. Here, we apply Γ_{0-} of the scheme I of TUM05 [8] to the proposed scheme A and propose a new secret sharing scheme realizing general access structures. Since the scheme I of TUM05 is more efficient than Benaloh and Leichter's scheme, the proposed scheme B can also reduce the number of shares distributed to $P \in \mathcal{P} - Q$.

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}, Q(\subset \mathcal{P})$, $K \in \mathcal{K}$ and Γ, the proposed scheme B is described as follows.

Proposed Scheme B:

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

(2) Let $\mathcal{A}' = \{C \subset Q : Q \cap A = C$ for some $A \in \Gamma_{0-}\}$ and represent it as

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

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

$$\begin{aligned}\mathcal{A}_i = \{B \subset \mathcal{P} - \mathcal{Q} : B \cap C'_i = \phi \\ \text{and } B \cup C'_i = A \text{ for some } A \in \Gamma_{0-}\}\end{aligned}$$

and represent it as

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

(4) 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 $1 \leq i \leq d$.

(5) 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 $1 \leq i \leq d$. One distinct share in $S_{1,i}$ is assigned to each $P \in C'_i$ $(1 \leq i \leq d)$.

(6) 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 $1 \leq i \leq d, 1 \leq j \leq |\mathcal{A}_i|$. One distinct share in $S_{2,i,j}$ is assigned to each $P \in C_{ij}$ $(1 \leq i \leq d, 1 \leq j \leq |\mathcal{A}_i|)$.

Example 4: Let $\mathcal{Q} = \{P_1, P_2\}$. We shall realize the access structure of Example 1 by the proposed scheme B.

- Since $l = 4$, we have

$$\Gamma_{0-} = \{A_1, A_2, A_3, A_4\}$$

and $\mathcal{P} = \mathcal{P}'$. Compute 6 shares

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

for the secret K by using Shamir's $(5, 6)$-threshold scheme.

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

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

where

$$\begin{aligned} C'_1 &= \{P_1, P_2\}, \\ C'_2 &= \{P_2\}, \\ C'_3 &= \phi. \end{aligned}$$

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

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

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

$$\begin{aligned} S_1 &= \{w_1, w'_1\}, \\ S_2 &= \{w_2, w'_2\} \end{aligned}$$

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

$$\begin{aligned} S_{1,1} &= \{s'_{1,1}, s'_{1,2}\}, \\ S_{1,2} &= \{s'_{2,1}\} \end{aligned}$$

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

$$\begin{aligned} S_{2,1,1} &= \{s_{1,1,1}, s_{1,1,2}\}, \\ S_{2,2,1} &= \{s_{2,1,1}, s_{2,1,2}, s_{2,1,3}\}, \\ S_{2,2,2} &= \{s_{2,2,1}, s_{2,2,2}, s_{2,2,3}\}, \\ S_{2,3,1} &= \{s_{3,1,1}, s_{3,1,2}, s_{3,1,3}, s_{3,1,4}\} \end{aligned}$$

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:

$$\begin{aligned} P_1 &: s_1, s'_{1,1} \\ P_2 &: s_2, s'_{1,2}, s'_{2,1} \\ P_3 &: s_3, s_{2,1,1}, s_{3,1,1} \\ P_4 &: s_4, s_{2,2,1}, s_{3,1,2} \\ P_5 &: s_5, s_{1,1,1}, s_{2,1,2}, s_{2,2,2}, s_{3,1,3} \\ P_6 &: s_6, s_{1,1,2}, s_{2,1,3}, s_{2,2,3}, s_{3,1,4}. \end{aligned}$$

The number of shares distributed to $P \in \mathcal{P}$ is described in **Table 1**.

This result shows that the proposed schemes A and B can reduce the numbers of shares distributed to $P \in \mathcal{Q}$. The proposed scheme B does not require shares corresponding to authorized subsets A_5 and A_6. Thus, the proposed scheme B can also reduce

Table 1 Comparison of the number of shares distributed to $P \in \mathcal{P}$.

	P_1	P_2	P_3	P_4	P_5	P_6
Benaloh and Leichter's scheme	3	5	4	4	5	5
The scheme I of TUM05	2	4	3	3	5	5
The proposed scheme A	1	2	4	4	5	5
The proposed scheme B	2	3	3	3	5	5

the numbers of shares distributed to $P_3, P_4 (\in \mathcal{P} - Q)$. Here, we show some properties of the proposed scheme B.

Theorem 4 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 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 $X_{S_{1,i}}$ and $X_{S_{2,i,j}}$ denote the shares in $S_{1,i}$ and $S_{2,i,j}$ assigned to X, respectively$(1 \leq i \leq d, 1 \leq j \leq |\mathcal{A}_i|)$. At first, we show $H(K|X) = 0$ for any $X \in \Gamma$.

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

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

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

$$\begin{aligned} & H(K|X) \\ &= H(K|X_S, X_{S_{1,1}}, \cdots, X_{S_{1,d}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}) \\ &\leq H(K|X_S) \\ &= 0. \end{aligned}$$

(Case ii) $X \in \Gamma$ and $|X| \leq l$: From the property of the access structure and the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_d$ and $\mathcal{A}'$, there exists $A \in \Gamma_{0-}$ such that

$$C'_i \cup C_{ij} = A \subset X.$$

In this case, we have

$$|X_{S_{1,i}}| = |C'_i| \text{ and } |X_{S_{2,i,j}}| = |C_{ij}|.$$

X can recover w_i since $s_{i,j,1}, s_{i,j,2}, \cdots, s_{i,j,|C_{ij}|}$ are shares computed by Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with w_i as a secret. Similarly, If $C'_i \neq \phi$, X can recover w'_i since $s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|C'_i|}$ are shares computed by Shamir's $(|C'_i|, |C'_i|)$-threshold scheme with w'_i as a secret. From the definition of S_i, we immediately obtain

$$\begin{aligned} & H(K|X) \\ &= H(K|X_S, X_{S_{1,1}}, \cdots, X_{S_{1,d}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}) \\ &\leq H(K|X_{S_{1,i}}, X_{S_{2,i,j}}) \\ &= 0. \end{aligned}$$

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 $X \notin \Gamma$, we have $|X| \leq l$. This implies

$$H(K|X_S) = H(K). \tag{12}$$

From the property of the access structure and the definition of $\mathcal{A}_i, \cdots, \mathcal{A}_d$ and $\mathcal{A}'$, for any $A_i \in \Gamma_{0-}$, we have

$$C'_i \not\subset X \text{ or } C_{ij} \not\subset X \ (1 \leq j \leq |\mathcal{A}_i|).$$

This implies

$$H(K|X_{S_{1,i}}, X_{S_{2,i,j}}) = H(K).$$

for $1 \leq i \leq d, 1 \leq j \leq |\mathcal{A}_i|$. From the definition of S_i, we have

$$H(K|X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}) = H(K)$$

for $1 \leq i \leq d$. This implies

$$\begin{aligned} & H(X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}|K) \\ &= H(X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}). \end{aligned} \tag{13}$$

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

$$\begin{aligned} & H(K|X) \\ &= H(K|X_S, X_{S_{1,1}}, \cdots, X_{S_{1,d}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}) \\ &= H(K|X_S) \\ &\quad + H(X_{S_{1,1}}, \cdots, X_{S_{1,d}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}|K, X_S) \\ &\quad - H(X_{S_{1,1}}, \cdots, X_{S_{1,d}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}|X_S). \end{aligned} \tag{14}$$

From the chain rule for entropy, we have

$$\begin{aligned} & H(X_{S_{1,1}}, \cdots, X_{S_{1,d}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}|K, X_S) \\ &= \sum_{t=1}^{d} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}|K, X_S, X_{S_{1,1}}, \cdots \\ &\qquad \cdots, X_{S_{1,t-1}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,t-1,|\mathcal{A}_{t-1}|}}) \\ &\overset{(*)}{=} \sum_{t=1}^{d} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}|K) \\ &= \sum_{t=1}^{d} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}). \end{aligned} \tag{15}$$

Here, $(*)$ comes from the fact that $X_S, X_{S_{1,1}}, \cdots, X_{S_{1,d}}$ and $X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}$ are mutually independent and the last equality comes from Eq. (13). On the other hand, we have

$$\begin{aligned} & H(X_{S_{1,1}}, \cdots, X_{S_{1,d}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,d,|\mathcal{A}_d|}}|X_S) \\ &= \sum_{t=1}^{d} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}|X_S, X_{S_{1,1}}, \cdots \\ &\qquad \cdots, X_{S_{1,t-1}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,t-1,|\mathcal{A}_{t-1}|}}) \\ &\leq \sum_{t=1}^{d} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}). \end{aligned} \tag{16}$$

Substituting Eqs. (12), (15) and (16) into Eq. (14), 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 scheme B includes the scheme I of TUM05 as a special case.

Theorem 5 If $Q = \phi$, then the proposed scheme B coincides with the scheme I of TUM05.

Proof: Since $Q = \phi$, we have

$$\mathcal{A}' = \{C'_1\}, C'_1 = \phi$$

and

$$\mathcal{A}_1 = \Gamma_{0-}.$$

Thus, the proposed scheme B coincides with the scheme I of TUM05. □

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

Theorem 6 Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$. If $\Gamma = \{A \in 2^{\mathcal{P}} : |A| \geq k\}$, then the proposed scheme B coincides with Shamir's (k, n)-threshold scheme for any $Q (\subset \mathcal{P})$.

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 scheme 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 scheme B. Similarly, let $N_{TUM}(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the scheme I of TUM05. The next theorem shows the proposed scheme B is more efficient than Benaloh and Leichter's scheme and the scheme I of TUM05 from the viewpoint of the number of shares distributed to each participant.

Theorem 7 For any $P \in \mathcal{P}$, the number of shares distributed to P is evaluated as follows:

$$N_B(P) = \begin{cases} N_{BL}(P) - \displaystyle\sum_{i=1}^{d} |\{P\} \cap C'_i|(|\mathcal{A}_i| - 1) \\ \qquad -\left| |\{X \in \Gamma_0 - \Gamma_{0-} : P \in X\}| - 1 \right|^+ \quad (P \in \mathcal{Q}) \\ \\ N_{BL}(P) \\ \qquad -\left| |\{X \in \Gamma_0 - \Gamma_{0-} : P \in X\}| - 1 \right|^+ \quad (P \notin \mathcal{Q}) \end{cases}$$

and

$$N_B(P) = \begin{cases} N_{TUM}(P) - \displaystyle\sum_{i=1}^{d} |\{P\} \cap C'_i|(|\mathcal{A}_i| - 1) & (P \in \mathcal{Q}) \\ N_{TUM}(P) & (P \notin \mathcal{Q}) \end{cases}$$

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

Proof: From the definition of Γ_{0-}, we have

$$N_{BL}(P) = |\{X \in \Gamma_{0-} : P \in X\}| + |\{X \in \Gamma_0 - \Gamma_{0-} : P \in X\}|$$

and

$$N_{TUM}(P) = |\{X \in \Gamma_{0-} : P \in X\}| + |\{P\} \cap \mathcal{P}'|. \tag{17}$$

The last term of Eq. (17) comes from the fact that the scheme I of TUM05 needs one additional share for every $P \in \mathcal{P}'$. From the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_d$ and $\mathcal{A}'$, $N_B(P)$ is obtained by

$$N_B(P) = \begin{cases} |\{P\} \cap \mathcal{P}'| + \displaystyle\sum_{i=1}^{d} |\{P\} \cap C'_i| & (P \in \mathcal{Q}) \\ |\{P\} \cap \mathcal{P}'| + \displaystyle\sum_{i=1}^{d} |\{C \in \mathcal{A}_i : P \in C\}| & (P \notin \mathcal{Q}). \end{cases}$$

Theorem 7 is easily obtained by the above equations and the result of Theorem 3. □

5. Evaluation of the Efficiency

Here, we consider the efficiency of the proposed schemes. The proposed scheme A can reduce the number of shares distributed to each participant $P \in \mathcal{Q} (\subset \mathcal{P})$. The proposed scheme B can also reduce the number of shares distributed to each participant in $\mathcal{P} - \mathcal{Q}$. From Theorem 3 and 7, we immediately obtain

$$N_B(P) \leq N_A(P) \quad \text{for any} \quad P \notin \mathcal{Q}.$$

Next, we consider $P \in \mathcal{Q}$. From Eq. (5) and the proof of Theorem 7, we have

$$N_B(P) = N_A(P) + |\{P\} \cap \mathcal{P}'| - \sum_{X \in \mathcal{A}'_A - \mathcal{A}'_B} |\{P\} \cap X|, \tag{18}$$

where

$$\mathcal{A}'_A = \{C \subset \mathcal{Q} \ : \ \mathcal{Q} \cap A = C \text{ for some } A \in \Gamma_0\},$$
$$\mathcal{A}'_B = \{C \subset \mathcal{Q} \ : \ \mathcal{Q} \cap A = C \text{ for some } A \in \Gamma_{0-}\}.$$

This shows that the proposed scheme B is not always more efficient than the proposed scheme A for $P \in \mathcal{Q}$ and the efficiency depends on the access structure. In the worst case, Eq. (18) is evaluated by

$$N_B(P) \leq N_A(P) + 1.$$

Next, we consider the information rate ρ. The information rates of the proposed schemes A and B are denoted by

$$\rho_A = \min\{1/N_A(P) : P \in \mathcal{P}\}, \tag{19}$$
$$\rho_B = \min\{1/N_B(P) : P \in \mathcal{P}\}. \tag{20}$$

Equations (19) and (20) show that the efficiency of the proposed schemes gets higher as the number of shares distributed to participants becomes small. Thus, we can improve the information rate when we set

$$\mathcal{Q} = \{P \in \mathcal{P} : \rho_A = 1/N_A(P)\}$$

or

$$\mathcal{Q} = \{P \in \mathcal{P} : \rho_B = 1/N_B(P)\}.$$

6. Conclusion

We have proposed new secret sharing schemes realizing general access structures. Our proposed schemes are perfect secret sharing schemes and can reduce the number of shares distributed to specified participants. Furthermore, for any access structure, the proposed schemes are more efficient than the previous results [5], [8].

Acknowledgments The author would like to thank Professor D. Stinson in the David R. Cheriton School of Computer Science at the University of Waterloo for his helpful discussions and comments.

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, *Trans. IECE*, 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.: Efficient secret sharing schemes realizing general access structures, *IEICE Trans. Fundamentals*, Vol.E87-A, No.7, pp.1788–1797 (2004).

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

[8] 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).

[9] 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).

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

[11] 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 University of Waterloo from 2012 to 2013. He received the SCIS Paper Award and the IEICE Best Paper Award in 2002 and 2005, respectively.