Recursive General Secret Sharing Scheme Based on Authorized Subsets

Utako Itoh and Kouya Tochikubo

***Abstract*—The basic idea of secret sharing is that a dealer distributes a piece of information about a secret to each participant in such a way that authorized subsets of participants can reconstruct the secret but unauthorized subsets of participants cannot determine the secret. We propose a new secret sharing scheme realizing general access structures, which is based on authorized subsets. The proposed scheme is perfect and can reduce the number of shares distributed to one specified participant. In the implementation of secret sharing schemes for general access structures, an important issue is the number of shares distributed to each participant. We can apply the proposed scheme to the same access structure recursively. That is, the proposed scheme can reduce the number of shares distributed to another participant once again by applying the proposed scheme recursively. We apply the proposed scheme to all access structures on five participants in order to evaluate the efficiency of the proposed scheme.**

***Index Terms*—Secret sharing scheme, general access structure, (k, n)-threshold scheme.**

I. 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 using polynomial derivatives [6]. Farrás and Padró formalized the concept of hierarchical access structure [7]. Secret sharing schemes based on graph access structures were also proposed [8]-[10]. These schemes obtain the optimal information rates for some access structures, but these schemes cannot be applied to 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 [11]. Their scheme can realize an arbitrary access structure by assigning one or more shares to each participant. Benaloh and Leichter proposed a secret sharing scheme for general access structures based on a monotone-circuit [12]. Secret sharing schemes which have an explicit assignment algorithm for any access structure are categorized by two types. One type is schemes based on unauthorized subsets [11], [13], [14]. Another type is schemes based on authorized subsets [12], [15], [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.

In this paper, we modify Benaloh and Leichter's scheme [12] and propose a new secret sharing scheme realizing general access structures, which is based on authorized subsets. The proposed scheme is perfect and can reduce the number of shares distributed to one specified participant. We can apply the proposed scheme to the same access structure recursively. That is, the proposed scheme can reduce the number of shares distributed to another participant once again by applying the proposed scheme recursively. We show that the proposed scheme is more efficient than or equal to Benaloh and Leichter's scheme [12] for any access structure. Furthermore, we show that the proposed scheme is more efficient than or equal to Ito, Saito and Nishizeki's scheme [11] for all 180 access structures on five participants.

II. Preliminaries

A. Secret Sharing Scheme

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a set of n participants. Let $D(\notin \mathcal{P})$ denote a dealer who selects a secret and distributes a share to each participant. Let $\mathcal{K}$ and $\mathcal{S}$ denote a secret set and a share set, respectively. For sets A and B, we denote a difference set by $A - B$. 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:

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

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

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

Manuscript received June 13, 2018; revised October 15, 2018. This work was supported by JSPS KAKENHI Grant Number 15K00192.

U. Itoh and K. Tochikubo are with the Department of Mathematical Information Engineering, Graduate School of Industrial Technology, Nihon University, Narashino-shi, Chiba 275-8575, Japan (e-mail: ciut16001@g.nihon-u.ac.jp, tochikubo.kouya@nihon-u.ac.jp).

doi: 10.18178/ijmlc.2019.9.1.768

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 [17] defined as

$$\rho = \min\{\rho_i : 1 \le i \le n\},$$

$$\rho_i = \frac{\log|\mathcal{K}|}{\log|\mathcal{S}(P_i)|}$$

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 $\rho = 1$. Throughout the paper, p is a large prime, and let Z_p be a finite field with p elements. In this paper, we assume $\mathcal{K} = \mathcal{S} = Z_p$.

B. Shamir's Threshold Scheme

Shamir's (k, n)-threshold scheme is described as follows [1]:

1) A dealer 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 D wants to share a secret $K \in Z_p$, D chooses $k-1$ elements $a_1, a_2, \cdots, a_{k-1}$ from Z_p independently with the uniform distribution.
3) 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 [17], [18]. 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 minimal access structure of (k, n)-threshold scheme is described as follows:

$$\Gamma_0 = \{A \in 2^{\mathcal{P}} : |A| = k\}.$$

C. Secret Sharing Scheme Based on Complete Multipartite Graph

Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$. Suppose $\mathcal{P}$ can be partitioned into subsets $V_1, \cdots, V_l$ and Γ_0 can be formed by

$$\Gamma_0 = \{\{x, y\} : x \in V_i, y \in V_j, 1 \le i, j \le l, i \ne j\}.$$

Then there is an ideal secret sharing scheme realizing the access structure. In this case, we can obtain a complete multipartite graph with vertex set $\mathcal{P}$ and edge set Γ_0. Actually, we can realize the access structure as follows.

1) Compute l shares $s_1, s_2, \cdots, s_l$ by using a $(2, l)$-threshold scheme with K as a secret.
2) s_i is assigned to each $P \in V_i$ $(1 \le i \le l)$.

D. General Secret Sharing Schemes

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, Benaloh and Leichter's scheme [12] 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 $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5\}$, consider the following access structure

$$\Gamma_0 = \{A_1, A_2, \cdots, A_7\}$$

where

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

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

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

where $s_{i,j}$ is computed by using Shamir's $(|A_i|, |A_i|)$-threshold scheme with K as a secret $(1 \le i \le 7, 1 \le j \le |A_i|)$.

In this example, 14/5 shares are distributed on average. This scheme executes one threshold scheme for each minimal authorized subset. A disadvantage of this scheme is that the number of shares distributed to each participant becomes large as the size of Γ_0 gets large.

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, Ito, Saito and Nishizeki's scheme [11] is described as follows.

Ito, Saito and Nishizeki's scheme:

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 Shamir's (t, t)-threshold scheme.

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

$$g_{ISN}(P_i) = \{w_j : P_i \notin B_j \in \bar{\Gamma}_1, 1 \le j \le t\} = \bigcup_{\substack{1 \le j \le t \\ P_i \notin B_j}} \{w_j\}. \#(1)$$

Example 2: We shall realize the access structure of Example 1 by Ito, Saito and Nishizeki's scheme. In this case, $\bar{\Gamma}_1$ is given by

$$\bar{\Gamma}_1 = \{B_1, B_2, B_3\},$$

where

$$B_1 = \{P_3, P_4\},$$
$$B_2 = \{P_1, P_5\},$$
$$B_3 = \{P_2, P_5\}.$$

1) Since $|\bar{\Gamma}_1| = 3$, compute 3 shares

$$w_1, w_2, w_3$$

by using a (3,3)-threshold scheme for the secret K.

2) According to the function g_{ISN}, distribute shares as follows:

$$g_{ISN}(P_1) = \{w_1, w_3\},$$
$$g_{ISN}(P_2) = \{w_1, w_2\},$$
$$g_{ISN}(P_3) = \{w_2, w_3\},$$
$$g_{ISN}(P_4) = \{w_2, w_3\},$$
$$g_{ISN}(P_5) = \{w_1\}.$$

In this scheme, to recover the secret a group $X \subset \mathcal{P}$ need to collect all shares. If X $\subset B_j \in \bar{\Gamma}_1, X$ cannot collect the share w_j. On the other hand, If X $\in \Gamma$, then there exists $P \in X$ such that $P \in X - B_j$ for all $B_j (1 \le j \le t)$. Thus, X can collect $w_1, \cdots, w_t$ and recover the secret. In this example, 9/5 shares are distributed on average. This scheme needs one share for each maximal unauthorized subset. Thus this scheme needs $|\bar{\Gamma}_1|$ shares in total. A disadvantage of this scheme is that the number of shares distributed to each participant becomes large as the size of $\bar{\Gamma}_1$ gets large.

III. Proposed Scheme

Here, we modify Benaloh and Leichter's scheme [12] and propose a new secret sharing scheme realizing general access structures, which is based on authorized subsets. The proposed scheme is perfect and can reduce the number of shares distributed to one specified participant $P' \in \mathcal{P}$ by dividing into Γ_0 according to P'. Furthermore, we can apply the proposed scheme to the same access structure recursively. The proposed scheme is more efficient than or equal to Benaloh and Leichter's scheme [12] for any access structure.

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

Proposed Scheme:

1) Let $\Gamma_0^{(1)} = \{A \subset \mathcal{P} - \{P'\} : A \cup \{P'\} \in \Gamma_0\}$ and represent it as

$$\Gamma_0^{(1)} = \{A_1^{(1)}, A_2^{(1)}, \cdots, A_l^{(1)}\}.$$

2) Let $\Gamma_0^{(0)} = \{A \in \Gamma_0 : P' \notin A\}$ and represent it as

$$\Gamma_0^{(0)} = \{A_1^{(0)}, A_2^{(0)}, \cdots, A_m^{(0)}\}.$$

3) compute 2 shares

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

by using Shamir's (2,2)-threshold scheme with K as a secret w_2 is assigned to $P' \in \mathcal{P}$.

4) For $A_i^{(1)} \in \Gamma_0^{(1)}$, compute $|A_i^{(1)}|$ shares

$$S_{1,i} = \{s_{1,i,1}, s_{1,i,2}, \cdots, s_{1,i,|A_i^{(1)}|}\}$$

by using Shamir's $(|A_i^{(1)}|, |A_i^{(1)}|)$-threshold scheme with w_1 as a secret independently for $1 \le i \le l$. One distinct share from $S_{1,i}$ is assigned to each

$$P \in A_i^{(1)} \ (1 \le i \le l).$$

5) For $A_i^{(0)} \in \Gamma_0^{(0)}$, compute $|A_i^{(0)}|$ shares

$$S_{0,i} = \{s_{0,i,1}, s_{0,i,2}, \cdots, s_{0,i,|A_i^{(0)}|}\}$$

by using Shamir's $(|A_i^{(0)}|, |A_i^{(0)}|)$-threshold scheme with K as a secret independently for $1 \le i \le m$. One distinct share from $S_{0,i}$ is assigned to each

$$P \in A_i^{(0)} \ (1 \le i \le m).$$

Example 3: Let $P' = P_1$ and we shall realize the access structure of Example 1 by the proposed scheme.

1) $\Gamma_0^{(1)}$ is defined by

$$\Gamma_0^{(1)} = \{A_1^{(1)}, A_2^{(1)}, A_3^{(1)}\}$$

where

$$A_1^{(1)} = \{P_2\},$$
$$A_2^{(1)} = \{P_3\},$$
$$A_3^{(1)} = \{P_4\}.$$

2) $\Gamma_0^{(0)}$ is defined by

$$\Gamma_0^{(0)} = \{A_1^{(0)}, A_2^{(0)}, A_3^{(0)}, A_4^{(0)}\}$$

where

$$A_1^{(0)} = \{P_2, P_3\},$$
$$A_2^{(0)} = \{P_2, P_4\},$$

$$A_3^{(0)} = \{P_3, P_5\},$$
$$A_4^{(0)} = \{P_4, P_5\}.$$

3) compute 2 shares w_1, w_2 by using Shamir's $(2,2)$-threshold scheme with K as a secret. w_2 is assigned to P_1.
4) In this case, $|A_1^{(1)}| = |A_2^{(1)}| = |A_3^{(1)}| = 1$. For $A_i^{(1)} \in \Gamma_0^{(1)}$, set

$$s_{1,i,1} = w_1$$

and $s_{1,i,1}$ is assigned to $P \in A_i^{(1)}$ $(1 \le i \le 3)$.
5) In this case, $|A_1^{(0)}| = |A_2^{(0)}| = |A_3^{(0)}| = |A_4^{(0)}| = 2$. For $A_i^{(0)} \in \Gamma_0^{(0)}$, compute 2 shares

$$S_{0,i} = \{s_{0,i,1}, s_{0,i,2}\}$$

by using Shamir's $(2,2)$-threshold scheme with K as a secret independently for $1 \le i \le 4$. One distinct share from $S_{0,i}$ is assigned to each $P \in A_i^{(0)}$ $(1 \le i \le 4)$.
6) In this case, shares are distributed as follows:

$$P_1 : w_2,$$
$$P_2 : s_{1,1,1}, s_{0,1,1}, s_{0,2,1},$$
$$P_3 : s_{1,2,1}, s_{0,1,2}, s_{0,3,1},$$
$$P_4 : s_{1,3,1}, s_{0,2,2}, s_{0,4,1},$$
$$P_5 : s_{0,3,2}, s_{0,4,2}.$$

In this example, the proposed scheme can reduce the number of shares distributed to $P_1 \in \mathcal{P}$. Actually, the proposed scheme distributes 12/5 shares on average, which is smaller than 14/5 achieved by Benaloh and Leichter's scheme. Hence, the proposed scheme is more efficient than Benaloh and Leichter's scheme.

The next theorem shows that the proposed scheme is perfect.

Theorem 1: For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}, P' \in \mathcal{P}$ and any access structure $\Gamma(\subset 2^{\mathcal{P}})$, distribute shares for a secret K by using the proposed scheme. Then, for any subset $X \subset \mathcal{P}$,

$$\text{(a)} \quad X \in \Gamma \Rightarrow H(K|X) = 0,$$
$$\text{(b)} \quad X \notin \Gamma \Rightarrow H(K|X) = H(K).$$

Proof: Let $X_S, X_{S_{1,i}}$ and $X_{S_{0,j}}$ denote the shares in $S - \{w_1\}, S_{1,i}$ and $S_{0,j}$ assigned to X, respectively $(1 \le i \le l, 1 \le j \le m)$. At first, we show $H(K|X) = 0$ for any $X \in \Gamma$.
(Case i) $P' \notin X$: From the property of access structure and the definition of $\Gamma_0^{(0)}$, there exists $A_i^{(0)} \in \Gamma_0^{(0)}$ such that $A_i^{(0)} \subset X$. In this case, we have

$$|X_{S_{0,i}}| = |S_{0,i}|.$$

Since $s_{0,i,1}, s_{0,i,2}, \cdots, s_{0,i,|A_i^{(0)}|}$ are shares computed by Shamir's $(|A_i^{(0)}|, |A_i^{(0)}|)$-threshold scheme with K as a secret, we have

$$\begin{aligned} &H(K|X) \\ &= H(K|X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,m}}) \\ &\le H(K|X_{S_{0,i}}) \\ &= \mathbf{0}. \end{aligned} \tag{2}$$

(Case ii) $P' \in X$: From the property of access structure and the definition of $\Gamma_0^{(1)}$, there exists $A_i^{(1)} \in \Gamma_0^{(1)}$ such that $A_i^{(1)} \subset X$. In this case, we have

$$|X_S| = 1 \text{ and } |X_{S_{1,i}}| = |S_{1,i}|.$$

Since $s_{1,i,1}, s_{1,i,2}, \cdots, s_{1,i,|A_i^{(1)}|}$ are shares computed by Shamir's $(|A_i^{(1)}|, |A_i^{(1)}|)$-threshold scheme with w_1 as a secret, we have

$$\begin{aligned} &H(K|X) \\ &= H(K|X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,m}}) \\ &\le H(K|X_S, X_{S_{0,i}}) \\ &= \mathbf{0}. \end{aligned} \tag{3}$$

Since $H(K|X) \ge 0$ is obvious, we have

$$H(K|X) = 0$$

for any $X \in \Gamma$ from (2) and (3).

Next we show $H(K|X) = H(K)$ for any $X \notin \Gamma$.

(Case i) $P' \notin X$: From the property of the access structure and the definition of $\Gamma_0^{(0)}$ and $\Gamma_0^{(1)}$, we have

$$\boldsymbol{A_i^{(0)} \not\subset X \ (1 \le i \le m)} \tag{4}$$

and

$$\boldsymbol{|X_S| = 0}. \tag{5}$$

(Case ii) $P' \in X$: From the property of access structure and the definition of $\Gamma_0^{(0)}$ and $\Gamma_0^{(1)}$, we have

$$\boldsymbol{A_i^{(0)} \not\subset X \ (1 \le i \le m)} \tag{6}$$

and

$$\boldsymbol{A_i^{(1)} \not\subset X \ (1 \le i \le l)} \tag{7}$$

From (4) and (6), we have

$$H(K|X_{S_{0,i}}) = H(K)$$

for any $X \notin \Gamma$ $(1 \le i \le m)$. This implies

$$\boldsymbol{H(X_{S_{0,i}}|K) = H(X_{S_{0,i}})} \tag{8}$$

for any $X \notin \Gamma$ $(1 \le i \le m)$. From (5) and (7), we have

$$\boldsymbol{H(K|X_S, X_{S_{1,i}}) = H(K)} \tag{9}$$

for any $X \notin \Gamma$ $(1 \le i \le l)$. From the definition of S, $S_{1,1}, \cdots, S_{1,l}$ and (9), we have

$$H(K|X_S, X_{S_{1,1}}, X_{S_{1,2}}, \cdots, X_{S_{1,l}}) = H(K).$$

This implies

$$H(X_S, X_{S_{1,1}}, X_{S_{1,2}}, \cdots, X_{S_{1,l}}|K) = \boldsymbol{H(X_S, X_{S_{1,1}}, X_{S_{1,2}}, \cdots, X_{S_{1,l}})}. \quad (10)$$

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

$$\begin{aligned} &H(K|X) \\ &= H(K|X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,m}}) \\ &= H(K) \\ &\quad + H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,m}}|K) \\ &\quad \boldsymbol{- H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,m}})}. \end{aligned} \quad (11)$$

From the chain rule for entropy, we have

$$\begin{aligned} &H\left(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,m}}\middle|K\right) \\ &= H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}|K) \\ &\quad + \sum_{t=1}^{m} H(X_{S_{0,t}}|K, X_S, X_{S_{1,1}}, \cdots \\ &\qquad \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,t-1}}) \\ &\overset{(*)}{=} H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}|K) \\ &\quad + \sum_{t=1}^{m} H(X_{S_{0,t}}|K) \\ &= H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}) \\ &\quad + \boldsymbol{\sum_{t=1}^{m} H\left(X_{S_{0,t}}\right)}. \end{aligned} \quad (12)$$

Here, $(*)$ comes from the definition of $\Gamma_0^{(0)}$ and $\Gamma_0^{(1)}$ and the fact that $X_{S_{0,1}}, \cdots, X_{S_{0,m}}$ are mutually independent and the last equality comes from (8) and (10). On the other hand, we have

$$\begin{aligned} &H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,m}}) \\ &= H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}) \\ &\quad + \sum_{t=1}^{m} H(X_{S_{0,t}}|X_S, X_{S_{1,1}}, \cdots \\ &\qquad \cdots, X_{S_{1,l}}, X_{S_{0,1}}, \cdots, X_{S_{0,t-1}}) \\ &\leq H(X_S, X_{S_{1,1}}, \cdots, X_{S_{1,l}}) \\ &\quad + \boldsymbol{\sum_{t=1}^{m} H\left(X_{S_{0,t}}\right)}. \end{aligned} \quad (13)$$

Substituting (12) and (13) into (11), we obtain $H(K|X) \geq H(K)$. Since $H(K|X) \leq H(K)$ is obvious, we have

$$H(K|X) = H(K).$$

Let $N(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the proposed scheme. 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 is more efficient than Benaloh and Leichter's scheme from the viewpoint of the number of shares distributed to $P' \in \mathcal{P}$.

Theorem 2: For any $P \in \mathcal{P}$, the number of shares distributed to P is evaluated as follows:

$$N(P) = \begin{cases} N_{BL}(P) - l + 1 & (P = P') \\ N_{BL}(P) & (P \neq P'). \end{cases}$$

Proof : From the definition of $\Gamma_0^{(1)}$, we have

$$\boldsymbol{(P')} = \mathbf{1} \quad (14)$$

and

$$\{X \in \Gamma_0 : P' \in X\} = \{X \cup \{P'\} : X \in \Gamma_0^{(1)}\}.$$

$N_{BL}(P)$ is obtain by

$$\begin{aligned} N_{BL}(P') &= |\{X \in \Gamma_0 : P' \in X\}| \\ &= |\{X \cup \{P'\} : X \in \Gamma_0^{(1)}\}| \\ &= |\Gamma_0^{(1)}| \\ &= \boldsymbol{l}. \end{aligned} \quad (15)$$

On the other hand, for $P \neq P'$, we have

$$\boldsymbol{N(P) = |\{X \in \Gamma_0^{(0)} : P \in X\}| + |\{X \in \Gamma_0^{(1)} : P \in X\}|}. \quad (16)$$

and

$$\begin{aligned} N_{BL}(P) &= |\{X \in \Gamma_0 : P \in X\}| \\ &= |\{X \in \Gamma_0^{(0)} : P \in \mathrm{X}\}| \\ &\quad + |\{X \cup \{P'\} : P \in X \in \Gamma_0^{(1)}\}| \\ &= |\{X \in \Gamma_0^{(0)} : P \in X\}| \\ &\quad + |\{X \in \Gamma_0^{(1)} : P \in X\}|. \end{aligned} \quad (17)$$

Theorem 2 is easily obtained by (14)-(17).

We can apply the proposed scheme to the same access structure recursively. That is, the proposed scheme can reduce the number of shares distributed to another participant once again by applying the proposed scheme recursively.

Example 4: We shall apply the proposed scheme to the access structure of Example 1 recursively.

1) Let $P'' = P_2$ and apply the proposed scheme to $\Gamma_0^{(0)}$ of Example 3 again. In this case, $\Gamma_0^{(01)}$ is defined by

$$\Gamma_0^{(01)} = \{A_1^{(01)}, A_2^{(01)}\}$$

where

$$A_1^{(01)} = \{P_3\},$$
$$A_2^{(01)} = \{P_4\}.$$

2) $\Gamma_0^{(00)}$ is defined by

$$\Gamma_0^{(00)} = \{A_1^{(00)}, A_2^{(00)}\}$$

where

$$A_1^{(00)} = \{P_3, P_5\},$$

$$A_2^{(00)} = \{P_4, P_5\}.$$

3) compute 2 shares w_1', w_2' by using Shamir's $(2,2)$-threshold scheme with K as a secret. w_2' is assigned to P_2.
4) Since $|A_1^{(01)}| = |A_2^{(01)}| = 1$, set

$$s'_{1,i,1} = w_1'$$

and $s'_{1,i,1}$ is assigned to $P \in A_i^{(01)}$ $(1 \le i \le 2)$.
5) Let $P''' = P_5$ and apply the proposed scheme to $\Gamma_0^{(00)}$ again. In this case, $\Gamma_0^{(001)}$ is defined by

$$\Gamma_0^{(001)} = \{A_1^{(001)}, A_2^{(001)}\}$$

where

$$A_1^{(001)} = \{P_3\},$$
$$A_2^{(001)} = \{P_4\}$$

and $\Gamma_0^{(000)} = \phi$.
6) compute 2 shares w_1'', w_2'' by using Shamir's $(2,2)$-threshold scheme with K as a secret. w_2'' is assigned to P_5.
7) Since $|A_1^{(001)}| = |A_2^{(001)}| = 1$, set

$$s''_{1,i,1} = w_1''$$

and $s''_{1,i,1}$ is assigned to $P \in A_i^{(001)}$ $(1 \le i \le 2)$.
8) In this case, shares are distributed as follows:

$$P_1 : w_2,$$
$$P_2 : s_{1,1,1}, w_2',$$
$$P_3 : s_{1,2,1}, s'_{1,1,1}, s''_{1,1,1},$$
$$P_4 : s_{1,3,1}, s'_{1,2,1}, s''_{1,2,1},$$
$$P_5 : w_2''.$$

In this example, the proposed scheme can reduce the number of shares distributed to P_2, P_5 as well as P_1. Actually, the proposed scheme distributes 2 shares on average.

The proposed scheme can yet reduce the number of shares distributed to each participant if $\Gamma_1^{(0)}$ or $\Gamma_0^{(0)}$ forms a complete multipartite graph.

Example 5: From Example 4, $\Gamma_0^{(0)}$ of Example 3 is denoted by

$$\Gamma_0^{(0)} = V_1 \cup V_2$$

where

$$V_1 = \{P_2, P_5\},$$
$$V_2 = \{P_3, P_4\}.$$

In this case, shares are distributed as follows:

$$P_1 : w_2,$$
$$P_2 : s_{1,1,1}, w_2',$$
$$P_3 : s_{1,2,1}, s'_{1,1,1},$$
$$P_4 : s_{1,3,1}, s'_{1,2,1},$$
$$P_5 : w_2'.$$

In this example, the proposed scheme can reduce the number of shares distributed to P_3, P_4 besides P_1, P_2, P_5. Actually, the proposed scheme distributes 8/5 shares on average.

IV. Evaluation of Efficiency

Here, we consider the efficiency of the proposed scheme. Let $N'(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the proposed scheme recursively. Similarly, let $N''(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the property of complete multipartite graphs and the proposed scheme recursively. Here, we denote the total number of shares distributed to all participants by

$$N_{BL} = \sum_{P \in \mathcal{P}} N_{BL}(P),$$
$$N = \sum_{P \in \mathcal{P}} N(P),$$
$$N' = \sum_{P \in \mathcal{P}} N'(P),$$
$$N'' = \sum_{P \in \mathcal{P}} N''(P),$$
$$g_{ISN} = \sum_{P \in \mathcal{P}} g_{ISN}(P).$$

From Theorem 3 and the definition of $\Gamma_0^{(0)}$ and $\Gamma_0^{(1)}$, we have

$$N'' \le N' \le N_{BL}.$$

For all 180 access structures on five participants clarified by Jackson and Martin [19], we obtain N_{BL}, N, N', N'' and g_{ISN} in order to evaluate the efficiency of the proposed scheme. Table I shows the number of shares distributed to participants by these five schemes. We summarize the comparison among N_{BL}, N, N' and N'' in Table II. For 173 access structures, N is smaller than N_{BL}. For 143 access structures, we can reduce the number of shares distributed to participants by applying the proposed scheme recursively. The proposed scheme can yet reduce the number of shares distributed to each participant by using the property of complete multipartite graphs for 40 access structures.

We summarize the comparison among between N'' and g_{ISN} in Table III. For 169 access structures, N'' is smaller than g_{ISN}. There is no access structure for which Ito, Saito and Nishizeki's scheme is better.

TABLE I: COMPARISON OF THE NUMBER OF SHARES DISTRIBUTED TO PARTICIPANTS

#	N_{BL}	N	N'	N''	g_{ISN}
1	5	5	5	5	5
2	5	5	5	5	8
3	6	5	5	5	7
4	8	7	7	7	12
5	5	5	5	5	9
6	9	7	7	7	10
7	11	9	8	7	11
8	13	11	10	10	16
9	7	5	5	5	6
10	10	8	8	8	13
11	7	6	6	6	9
12	9	8	7	5	6
13	8	7	7	7	12
14	5	5	5	5	12
15	6	5	5	5	8
16	9	8	7	7	15
17	7	6	5	5	7
18	10	8	7	7	11
19	13	11	10	10	18
20	5	5	5	5	8
21	14	11	10	10	13
22	16	13	11	10	14
23	18	15	12	11	15
24	20	17	14	14	20
25	12	9	8	8	9
26	14	11	9	9	10
27	17	14	12	11	17
28	14	11	10	9	13
29	16	13	11	9	10
30	15	12	11	10	16
31	12	10	9	8	12
32	14	12	10	8	9
33	13	11	10	9	15
34	10	7	7	7	8
35	12	9	9	9	16
36	13	10	9	9	12
37	16	13	11	11	19
38	10	8	7	7	8
39	12	10	9	7	12
40	13	11	10	10	15
41	10	8	8	8	15
42	11	9	8	8	11
43	14	12	10	10	18
44	8	7	7	7	18
45	9	7	7	7	10
46	12	10	9	9	14
47	15	13	10	10	21
48	11	8	8	8	10
49	14	11	9	9	11
50	17	14	11	11	15
51	20	17	14	14	22
52	11	9	8	8	11
53	13	11	10	8	15
54	15	13	11	9	12
55	14	12	10	10	18
56	12	10	8	8	10
57	15	12	10	10	14
58	18	15	13	13	21
59	8	5	5	5	5
60	12	9	9	9	12
61	8	6	6	6	7
62	10	8	7	6	8
63	12	10	8	5	5
64	11	9	8	8	11
65	9	7	7	7	9
66	12	10	8	8	10
67	15	13	10	10	14
68	10	8	8	8	11
69	11	9	8	7	11
70	14	12	11	9	18
71	8	7	6	6	11
72	10	9	8	8	15
73	11	9	9	9	18
74	9	7	7	7	10
75	12	10	9	9	14
76	15	13	11	11	21
77	12	10	8	8	14
78	9	8	7	7	7
79	10	8	7	7	9
80	12	10	9	9	21
81	13	11	9	9	13
82	16	13	11	11	17
83	19	16	13	13	24
84	13	10	9	9	13
85	16	13	11	11	17
86	9	8	7	7	14
87	10	8	8	8	12
88	13	11	9	9	13
89	16	13	10	10	17
90	10	8	7	7	9
91	13	11	9	9	10
92	6	5	5	5	10
93	7	5	5	5	7
94	10	8	7	7	12
95	13	11	8	8	13
96	11	9	8	8	14
97	7	6	6	6	8
98	10	9	7	5	6
99	8	7	7	7	10
100	7	6	6	6	9
101	10	8	7	7	13
102	13	11	9	9	17
103	16	13	11	9	24
104	10	9	8	8	10
105	11	9	8	8	11
106	14	11	9	7	12
107	17	14	11	9	16
108	20	17	13	11	20
109	23	19	14	13	27
110	20	16	12	11	20
111	17	13	10	9	16
112	14	11	10	10	15
113	17	14	11	11	16
114	14	12	9	9	12
115	17	14	11	11	13
116	14	11	9	9	12
117	11	9	7	7	11
118	8	6	5	5	6
119	11	8	7	7	10
120	14	11	10	10	15
121	15	12	11	11	17
122	11	9	8	8	11
123	14	12	9	9	9
124	11	9	8	8	11
125	12	10	9	9	13
126	8	7	7	7	10
127	11	9	8	8	8
128	8	7	6	6	10
129	9	8	7	7	12
130	5	5	5	5	12
131	6	5	5	5	7
132	10	9	7	7	14
133	15	12	10	10	13
134	18	14	11	10	14
135	21	17	12	11	15
136	24	19	14	13	19
137	27	22	16	16	23
138	30	25	19	19	30
139	21	16	13	13	18
140	21	17	12	11	15
141	24	20	14	13	16
142	18	15	11	11	14
143	12	9	7	7	8
144	15	11	8	7	9
145	18	13	10	10	13
146	22	17	14	14	20
147	18	14	11	10	14
148	21	17	12	11	12
149	19	15	12	11	16
150	15	12	10	10	13
151	18	15	11	9	11
152	15	12	9	9	13
153	16	13	11	11	15
154	12	10	8	8	12
155	15	12	10	8	10
156	18	15	11	7	8
157	13	11	10	10	14
158	9	7	5	5	5
159	12	10	8	8	15
160	13	10	8	8	10
161	17	14	11	11	17
162	9	7	6	6	7
163	12	9	7	5	5
164	16	13	11	9	12
165	12	10	8	8	12
166	15	13	10	10	10
167	13	11	9	9	14
168	9	8	7	7	14
169	10	8	7	7	9
170	14	12	9	9	16
171	6	5	5	5	9
172	10	9	8	8	16
173	7	6	5	5	6
174	11	9	7	7	11
175	15	13	10	10	18
176	8	7	5	5	5
177	12	10	7	7	8
178	16	13	10	10	13
179	20	17	14	14	20
180	5	5	5	5	5

TABLE III: COMPARISON BETWEEN N'' AND g_{ISN}

	The number of access structures
$N'' < g_{ISN}$	169
$N'' = g_{ISN}$	11
$N'' > g_{ISN}$	0

V. CONCLUSION

We have proposed a new secret sharing scheme realizing general access structures. The proposed scheme is perfect and can reduce the number of shares distributed to each participant. We can apply the proposed scheme to the same access structure recursively. The proposed scheme is more efficient than or equal to Benaloh and Leichter's scheme [12] for any access structure. Furthermore, we have shown that the proposed scheme is more efficient than or equal to Ito, Saito and Nishizeki's scheme [11] for all 180 access structures on five participants. We will compare the proposed scheme with the other general secret sharing schemes and evaluate the efficiencies in the follow-up work.

REFERENCES

[1] A. Shamir, "How to share a secret," *Comm. ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. Blakley, "Safeguarding cryptographic keys," *Proceedings of AFIPS*, vol. 48, pp. 313-317, 1979.

[3] K. Koyama, "Cryptographic key sharing methods for multi-groups and security analysis," *Trans. of the IECE*, vol. E66, no. 1, pp. 13-20, 1983.

[4] G. Simmons, "How to (really) share a secret," in *Proc CRYPTO*, vol. 88, pp. 390-448, 1988.

[5] G. Simmons, "Prepositioned shared secret and/or shared control schemes," in *Proc. EUROCRYPT*, vol. 89, pp. 436-467, 1989.

[6] T. Tassa, "Hierarchical threshold secret sharing," *Journal of Cryptology*, Vol. 20, pp.237-264, 2007.

[7] Farrás and C. Padró, "Ideal hierarchical secret sharing schemes," *IEEE Trans. on IT*, vol. 58, no. 5, pp. 3273-3286, 2012.

[8] H. Sun, H. Wang, B. Ku, and J. Pieprzyk, "Decomposition construction for secret sharing schemes with graph access structures in polynomial time," *SIAM Journal on Discrete Mathematics*, vol. 24, no. 2, pp. 617-638, 2010.

[9] L. Csirmaz, P. Ligeti, and G. Tardos, "Erdös-Pyber theorem for hypergraphs and secret sharing," *Graphs and Combinatorics*, vol. 31, no. 5, pp. 1335-1346, 2015.

[10] A. Beimel, Y. Mintz, and O. Farrás, "Secret-sharing schemes for very dense graphs," *Journal of Cryptology*, vol. 29, issue 2, pp. 336-362, 2016.

[11] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *Proc. IEEE Globecom*, vol. 87, pp. 99-102, 1987.

[12] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Proc. CRYPTO*, vol. 88, pp. 27-35, 1988.

[13] K. Tochikubo, "Efficient secret sharing schemes realizing general access structures," *IEICE Trans. Fundamentals*, vol. E87-A, no. 7, pp. 1788-1797, 2004.

[14] K. Tochikubo, "Efficient secret sharing schemes based on unauthorized subsets," *IEICE Trans. Fundamentals*, vol. E91-A, no. 10, pp. 2860-2867, 2008.

[15] K. Tochikubo, T. Uyematsu, and R. Matsumoto, "Efficient secret sharing schemes based on authorized subsets," *IEICE Trans. Fundamentals*, vol. E88-A, no. 1, pp. 322-326, 2005.

[16] K. Tochikubo, "New construction methods of secret sharing schemes based on authorized subsets," *Journal of Information Processing*, vol. 21, no. 4, pp. 590-598, 2013.

[17] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd edition, CRC Press, 2005.

[18] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. on IT*, vol. 29, no. 1, pp. 35-41, 1983.

[19] W. Jackson and K. M. Marin, "Perfect secret sharing schemes on five participants," *Designs, Codes and Cryptography*, vol. 9, issue 3, pp. 267-286, 1996.

Utako Itoh received her B.E. degree from Nihon University in 2016. Currently, she is a master's course student in the Department of Mathematical Information Engineering, Graduate School of Industrial Technology, Nihon University.

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. Dr. Tochikubo received the SCIS Paper Award and the Institute of Electronics, Information and Communication Engineers (IEICE) Best Paper Award in 2002 and 2005, respectively.