A New Family of Ideal Multipartite Access Structure Based on MSP

Jun Xu* Jiwen Zeng Xiaomin Zha

November 3, 2006

Abstract

In this article we introduce the multipartite access structure and the composite access structure. A new family of the multipartite access structure will be given, we will provide secret sharing scheme realizing it based on MSP and also prove it is ideal.

key words : secret sharing schemes, monotone span programs, multipartite access structure.

1 Introduction

Secret sharing schemes are methods designed to share a secret among a group of participants in such a way that the secret can be reconstruct only by specified groups of participant, if non-allowed coalitions cannot obtain any information about the secret. Then the scheme is said to be perfect. Let $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ be the set of players. The family of qualified subsets $\Gamma \subseteq 2^p$ is called the access structure if it is closed under taking supersets ($A \in \Gamma, A \subset B \Rightarrow B \in \Gamma$). Thus the set of minimal elements in Γ, denoted Γ^m, determines the whole structure Γ and it is called the basis of Γ.

One of the basic paraments of a secret sharing scheme $\sum$ is its information rate which is the rate between the length (in bits) of the secret and the maximum length of the shares of the participants:

$$\rho(\Sigma, \Gamma, K) = \rho(\Sigma) = \frac{\log_2 |K|}{\max_p(\log_2 |S(p)|)},$$

*School of Mathematical Sciences,Xiamen University,Xiamen 361005,P.R.China.xujunxmu@126.com

where K is set of all possible secrets for $\sum$ and $S(p)$ is set of all possible shares for p $\in \mathcal{P}$. A scheme $\sum$ is called *ideal* if $\rho(\Sigma) = 1$. But figuring out an ideal secret sharing scheme realizing an access structure is still very difficult. Notice that in general we always have $\rho(\Sigma) \leq 1$. An access structure Γ is called ideal if there is an ideal scheme realizing it. More generally we define the optimal information rate of the structure Γ as

$$\rho^*(\Gamma) = \sup(\rho(\Sigma, \Gamma, K))$$

where the supremum is taken over all possible Σ and K for Γ. A particular class of secret sharing schemes is that of (t, n) threshold schemes which were introduced independently by Blakley [1] and Shamir [5], where the access structure consists of all subsets of $\mathcal{P}$ with at least t out of n participants. That is, Γ_0=$\{A|A \subset \mathcal{P}, |A| = t\}$. Monotone span programs (MSP) were introduced by Karchmer and Wigdreson[6] to construct (t,n)-threshold schemes.

We consider the multipartite access structures: the set of players is divided into K disjoint entities and all players in each entity play exactly the same role inside the access structure. when K=1, the threshold access structure is regarded as the multipartite access structure. And K $\geq$ 2, some multipartite access structures are discussed by [3,7,9]. We will also consider the composite access structure, it can be useful for sharing secrets when the set of participants is divided into several groups, each of them with its own family of authorized coalitions. These access structures have many applications in real life, for example persons were divided by some groups according to their position or responsibilities in company and department.

Many families of multipartite access structure have been discussed in the [9], their proofs are existential, but not constructive. Here we will give a new family of the multipartite access structure and its proof is constructive and useful.

The rest of this paper is organized as follows. In Section 2 we give some concepts about the monotone span program(MSP) and the definition of composition access structure and the general multipartite access structure. In Section 3 we construct the MSP about a kind of composite access structure and we illustrate it could prove the family of multipartite is ideal. We will conclude our work about the multipartite access structure in section 4.

2 preliminaries

Definition 1. *[6] A Monotone Span Program (MSP) $\mathcal{M}$ is a quadruple ($\mathcal{F}$,M,$\overrightarrow{t}$, φ), where $\mathcal{F}$ is a finite field, M is a matrix (with m rows and $d \leq m$ columns) over $\mathcal{F}$, $\varphi : \{1, \cdots, m\} \rightarrow \{1, \cdots, n\}$ is a surjection function and $\overrightarrow{t}$ is a fixed non-zero vector, called target vector. The size of $\mathcal{M}$ is the number m of rows and is denoted as size($\mathcal{M}$).*

As φ labels each row with a number i from $[1, \cdots, m]$ that corresponds to player $P_{\varphi(i)}$. we can think of each player as being the *owner* of one or more rows.

For any set of players $B \subseteq P$ consider the matrix consisting of the rows these players own in M, as is common,we shall denote M_B. But we should stay aware of the difference between M_B for $B \subseteq P$ and for $B \subseteq \{1, \cdots, m\}$.

An MSP is said to compute a(complete)access structure Γ when $\varepsilon \in im({M_A}^T)$ if and only if A is a member of Γ. We say that A is accepted by $\mathcal{M}$ if and only if $A \in \Gamma$. Otherwise we say A is rejected by $\mathcal{M}$, in other words, the players in A can construct the secret precise if the rows they own contain in their linear span the target vector of $\mathcal{M}$.

Definition 2. *[10] If Γ_1, Γ_2, $\cdots$, Γ_k are defined on participants set X_1, X_2, $\cdots$, X_k respectively. $\Gamma_1+\Gamma_2+\cdots+\Gamma_k$ and $\Gamma_1 \times \Gamma_2 \cdots \times \Gamma_k$ defined on $X_1 \cup X_2 \cup \cdots \cup X_k$ such that for* A $\subseteq X_1 \cup X_2 \cup \cdots \cup X_k$.

$$A \in \Gamma_1 + \Gamma_2 + \cdots + \Gamma_k \Longleftrightarrow A \cap X_1 \in \Gamma_1 \text{ or } A \cap X_2 \in \Gamma_2 \text{ or } \cdots \text{ or } A \cap X_k \in \Gamma_k.$$
$$A \in \Gamma_1 \times \Gamma_2 \cdots \times \Gamma_k \Longleftrightarrow A \cap X_1 \in \Gamma_1 \text{ and } A \cap X_2 \in \Gamma_2 \text{ and } \cdots \text{ and } A \cap X_k \in \Gamma_k.$$

Let σ be any permutation of $\mathcal{P}$, $\sigma(\Gamma)=\{\sigma(A)|A \in \Gamma\}$. Now we introduce multipartite access structures.

Definition 3. *[8] An access structure Γ defined in the set of player $\mathcal{P}$ is multipartite of partition $X_1, \cdots, X_k$ if $\sigma(\Gamma) = \Gamma$ for any permutation σ of $\mathcal{P}$ with $\sigma(X_1) = X_1, \cdots, \sigma(X_k) = X_k$. Then Γ is $(X_1, \cdots, X_k)$-multipartite or k-multipartite.*

Proposition 1. *[9] Any access structure is a multipartite access structure.*

Proof: Let τ_{pq} be a permutation of $\mathcal{P}$, the transposition of two participants p, q in $\mathcal{P}$ for two participants p,q $\in \mathcal{P}$. $\tau_{pq}(\Gamma)=\{\tau_{pq}(A)|A \in \Gamma\}$. In order to find participants with the same role in the structure we define the relation : p $\sim$ q if and only if $\tau_{pq}(\Gamma) = \Gamma$. Obviously the binary relation $\sim$ is an equivalence relation. Therefore we can consider the quotient $\mathcal{P}/\sim = \{X_1, \cdots, X_k\}$. Where $X_1, \cdots, X_k$ are the equivalence classes determined by the relation $\sim$. Let σ be a permutation of $\mathcal{P}$ with $\sigma(X_1) = X_1, \cdots, \sigma(X_k) = X_k$. It is obvious that $\sigma=\sigma_1 \circ \cdots \circ \sigma_k$ with $\sigma_i(X_i) = X_i$ and $\sigma_i(p_j) = p_j$ for any player $p_j \in \mathcal{P} - X_i$. This directly implies $\sigma(\Gamma) = \Gamma$. So any access structure is a multipartite access structure.

In the multipartite access structure $\mathcal{P}$ is the set of participants and $\mathcal{P}= X_1 \cup \cdots \cup X_k$ is a partition of $\mathcal{P}$(that is $\emptyset \neq X_i \neq \mathcal{P}$, $X_i \cap X_j = \emptyset$, if i $\neq$ j and $\cup_{i=1}^{k} X_i = \mathcal{P}$). Let us write $|X_i| = n_i$ and $n = \sum_{i=1}^{K} n_i$. For a set A $\subseteq \mathcal{P}$ we denote $A_i = A \cap X_i$. Obviously $A = A_1 \cup \cdots \cup A_k$. For $i = 1, \cdots, k$, let Γ_i be an access structure on X_i and let Γ_0 be an access structure on the quotient $\mathcal{P}/\sim = \{X_1, \cdots, X_k\}$.

Definition 4. *[2] With the notion as above the composite access structure of* Γ_1, $\cdots$, Γ_k, *following* Γ_0, *denoted by* $\Gamma_0[\Gamma_1, \cdots, \Gamma_k]$, *is defined as follows*

$$\begin{aligned} \Gamma_0[\Gamma_1, \cdots, \Gamma_k] &= \{A \in \mathcal{P} |\ \exists B \in \Gamma_0 \quad such\ that \quad A_i \in \Gamma_i \quad for\ all \quad X_i \in B\} \\ &= \cup_{B \in \Gamma_0} \{A \in \mathcal{P} | A_i \in \Gamma_i \quad for\ all \quad X_i \in B\} \end{aligned}$$

$\Gamma_0[\Gamma_1, \ldots, \Gamma_k]$ is an access structure defined on $\mathcal{P}$, if A $\in \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$, then $\exists$ B $\in \Gamma_0$, for all $X_i \in$ B, $A_i = A \cap X_i \in \Gamma_i$. A $\subset A' \subset \mathcal{P}$, then $\exists$ the same B $\in \Gamma_0$, $A' \cap X_i \supset A \cap X_i$, so $A' \cap X_i \in \Gamma_i$. We have $A' \in \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$. A coalition $A \subseteq \mathcal{P}$ is authorized if and only if it includes, as subsets, authorized coalitions in enough of the components Γ_1, $\cdots$, Γ_k to constitute an authorized subsets for Γ_0.

3 a family of multipartite access structure

Any access structure Γ is *multipartite* of partition X_1, X_2, $\cdots$, X_k defined in the set of players $\mathcal{P}$ if $\sigma(\Gamma) = \Gamma$ for any permutation σ of $\mathcal{P}$ with $\sigma_i(X_i) = X_i$, let Γ_i is an threshold access structure defined on X_i, $i = 1, \cdots, k$. Let Γ_0 is an threshold access structure defined on $\mathcal{P}/\sim = \{X_1, \cdots, X_k\}$. Let $\Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$ is composite access structure which could be computed by MSP. It has been discussed widely in [3], but we will give a new proof about it. So we have the following lemma.

Lemma 1. *Let* $\Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$ *is composite access structure.* Γ_0 *is threshold access structure defined on* $\mathcal{P}/\sim = \{X_1, \cdots, X_k\}$ *which is computed by the MSP* $\mathcal{N}_0$, Γ_i *is threshold access structure defined on* X_i *which is computed by the MSP* $\mathcal{M}_i$ *for* $i = 1, \cdots, k$. *Then there exists an MSP* $\mathcal{M}$ *computing* $\Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$ *of size* $m=|\mathcal{P}|$.

Proof: Let $X_i=\{p_{i1}, \cdots, p_{in_i}\}$ for i $= 1, \cdots, k$. Suppose the threshold access structure

Γ_0 is computed by MSP

$$N_0 = \begin{pmatrix} 1 & m_{01} & m_{01}^2 & \cdots & m_{01}^{d-1} \\ 1 & m_{02} & m_{02}^2 & \cdots & x_{02}^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & m_{0k} & m_{0k}^2 & \cdots & m_{0k}^{d-1} \end{pmatrix} \begin{matrix} X_1 \\ X_2 \\ \vdots \\ X_k \end{matrix}$$

here d $\leq$ k. We construct the matrix as follows:

$$N_i = \begin{pmatrix} 1 & m_{0i} & m_{0i}^2 & \cdots & m_{0i}^{d-1} \\ 1 & m_{0i} & m_{0i}^2 & \cdots & x_{0i}^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & m_{0i} & m_{0i}^2 & \cdots & m_{0i}^{d-1} \end{pmatrix} \begin{matrix} p_{i1} \\ p_{i2} \\ \vdots \\ p_{in_i} \end{matrix}$$

here $i = 1, 2, \ldots, k$. The threshold access structure Γ_i is computed by the MSP $\mathcal{M}_i$.

$$M_i = \begin{pmatrix} 1 & x_{i1} & x_{i1}^2 & \cdots & x_{i1}^{t_i-1} \\ 1 & x_{i2} & x_{i2}^2 & \cdots & x_{i2}^{t_i-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{in_i} & x_{in_i}^2 & \cdots & x_{in_i}^{t_i-1} \end{pmatrix} \begin{matrix} p_{i1} \\ p_{i2} \\ \vdots \\ p_{in_i} \end{matrix}$$

Let $M_i = (\mathbf{1} M_i^{(2)})$. Then the MSP $\mathcal{M}$

$$M = \begin{pmatrix} N_1 & M_1^{(2)} & 0 & 0 & \cdots & 0 \\ N_2 & 0 & M_2^{(2)} & 0 & \cdots & 0 \\ N_3 & 0 & 0 & M_3^{(2)} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ N_k & 0 & 0 & 0 & \cdots & M_k^{(2)} \end{pmatrix}$$

computes $\Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$. Then M is a $(n \times (d - K + t_1 + t_2 + \cdots + t_k))$ matrix. The labelling of M is carried over in a natural way from M_i and N_i, $i = 1, \cdots, k$.

Now we will show that this MSP computes the access structure $\Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$. If A $\in \Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_k]$ if and only of $\exists$ B $\in \Gamma_0$ such that A $\cap X_i \in \Gamma_i$, for all $X_i \in$ B, then A $\cap X_i \in \Gamma_i \Longrightarrow (1, \ldots, 0)^T \in Im((M_i)_{A \cap X_i})^T \Longrightarrow (0, \ldots, 0)^T \in Im(((M_i^{(2)})_{A \cap X_i})^T) \Longrightarrow (1, m_{0i}, m_{0i}^2, \ldots, m_{0i}^{(d-1)}, 0, \ldots, 0)^T \in Im(M_{A \cap X_i})^T$. Because B $\in \Gamma_0$ and for all $X_i \in$ B, $(1, \ldots, 0)^T \in Im((N_0)_B)^T$ and the number of the column vector $(1, m_{0i}, m_{0i}^2, \ldots, m_{0i}^{(d-1)})$ is greater than or equal to d, then $(1, \ldots, 0)^T \in Im((M_A)^T)$.

If $(1, \ldots, 0)^T \in Im((M_A)^T)$, if $\mathcal{P}_i \subseteq A$ satisfies for any i $\in$ 1, ..., K $\Longrightarrow (0, \ldots, 0)^T \in Im((M_i^{(2)})_{A \cap X_i})^T) \Longrightarrow |A \cap X_i| \geq t_i \Longrightarrow (1, \ldots, 0)^T \in Im((M_i)_{A \cap X_i})^T \Longrightarrow A \cap X_i \in$

Γ_i. Let $B = \{\mathcal{P}_i | \mathcal{P}_i \subseteq A, i = 1, \ldots, k\}$, $(1, \ldots, 0)^T \in Im((M_A)^T) \Longrightarrow (1, \ldots, 0)^T \in Im(((N_0)_B)^T) \Longrightarrow$ B $\in \Gamma_0$. So A $\in \Gamma$. Thus $\mathcal{M}$ computes Γ and the size of $\mathcal{M}$ is $|\mathcal{P}|$.

Let $X_1, \ldots, X_k$ be a partition of $\mathcal{P}$. We define the mapping $\upsilon : \mathcal{P} \longrightarrow \{1, 2, \ldots, k\}$ that assigns to every participant the entity he belongs to. We will use the notation υ_i=$\upsilon(p_i)$, meaning that the participants p_i belongs to the entity X_{υ_i}. For a subset of players $A \subset \mathcal{P}$, the set of entities represented by A as $\upsilon(A)$=$\{\upsilon(p_i) \mid p_i \in A\}$. First An access structure is given, then we get a partition of $\mathcal{P}$ according to participants play the same role in the same role in the access structure, Let us suppose Γ_i is threshold access structure defined on the partition X_i, i=1, 2, $\cdots$, k and Γ_0 is threshold access structure defined on $\mathcal{P}/\sim = \{X_1, \ldots, X_k\}$. If $\Gamma = \Gamma_0[\Gamma_1, \ldots, \Gamma_k]$, we have the following Theorem.

Theorem 1. *Let k, d, n_i, t_i be positive integer numbers with $d \leq k$, $t_i \leq n_i$ for i=1, 2, ..., k. Let $X_1, X_2, \ldots, X_k$ be a partition of $\mathcal{P}$. The multipartite access structure defined in the partition $X_1, X_2, \ldots, X_k$ by*

$$\Gamma = \{A \subseteq \mathcal{P} : |\upsilon(A)| \geq d \text{ and } |A \cap X_i| \geq t_i, i \in \{i_1, i_2, \cdots, i_d\}, \{i_1, i_2, \cdots, i_d\} \subset \{1, 2, \cdots, k\}\}$$

Then the multipartite access structure Γ is ideal.

Proof : Let Γ_0 be (d,k)-threshold access structure defined on $\mathcal{P}/\sim$ =$\{X_1, \ldots, X_k\}$, let Γ_i be (t_i, n_i)-threshold access structure defined on X_i for i=1,$\cdots$,K. $\Gamma = \Gamma_0[\Gamma_1, \ldots, \Gamma_k]$ is ideal access structure based on Lemma 1.

Corollary 1. *With the notion as above the multipartite access structure composite defined in the partition $X_1, X_2, \cdots, X_k$.*

$$if\ d = 1, \Gamma = (t_1, n_1) + (t_2, n_2) + \cdots + (t_k, n_k). \qquad (1)$$
$$if\ d = k, \Gamma = (t_1, n_1) \times (t_2, n_2) \times \cdots \times (t_k, n_k). \qquad (2)$$

Proof : if d=1, $\forall$ A $\in \Gamma$, $|A \cap X_1| \geq t_1$ or $|A \cap X_2| \geq t_2$ or $\cdots$ or $|A \cap X_k| \geq t_k$. So Γ=(t_1, n_1)+(t_2, n_2)+$\cdots$+(t_k, n_k) based on Definition 2. If d=k, $\forall$ A $\in \Gamma$, $|A \cap X_1| \geq t_1$ and $|A \cap X_2| \geq t_2$ and $\cdots$ and $|A \cap X_k| \geq t_k$. So Γ=$(t_1, n_1) \times (t_2, n_2) \times \cdots \times (t_k, n_k)$. It is also based on Definition 2.

We know that any access structure is multipartite access structure based on Proposition 1 and a particular interesting kind of access structure is threshold access structure. Now we could generalize this special threshold structure based on Theorem 1. It is ob-

vious that this multipartite access structure is a threshold access structure if k=1. It is composed by some small threshold access structures when k $\geq$ 2.

Next we will show the example of how the result of Theorem 1 can be used in practice. Let the participants set be $\mathcal{P}$=$\{p_1, p_2, \cdots, p_9\}$. The minimal qualified subset of the access structure :

Γ^m =$\{\{p_1, p_2, p_3, p_4\},\ \{p_1, p_2, p_4, p_8\},\ \{p_1, p_3, p_4, p_8\},\ \{p_1, p_2, p_3, p_7\},\ \{p_1, p_3, p_7, p_8\},$
$\{p_1, p_2, p_7, p_8\},\ \{p_3, p_4, p_7, p_8\},\ \{p_2, p_3, p_4, p_7\},\ \{p_2, p_4, p_7, p_8\},\ \{p_1, p_4, p_5, p_6, p_9\},$
$\{p_1, p_5, p_6, p_7, p_9\},\ \{p_4, p_5, p_6, p_7, p_9\}, \{p_2, p_3, p_5, p_6, p_9\}, \{p_2, p_5, p_6, p_8, p_9\}, \{p_3, p_5, p_6, p_8, p_9\}\}$.

In order to find participants with the same role in the access structure, there is an equivalence relation: p $\sim$ q if and only if $\tau_{pq}(\Gamma) = \Gamma$, for p,q $\in \mathcal{P}$.We could verify $p_1 \sim p_4 \sim p_7$,$p_2 \sim p_3 \sim p_8$, $p_5 \sim p_6 \sim p_9$. There are three equivalence classes X_1=$\{p_1, p_4, p_7\}$,X_2=$\{p_2, p_3, p_8\}$,X_3=$\{p_5, p_6, p_9\}$. Let Γ_1 be (2,3)-threshold access structure defined on X_1, Γ_2 be (2,3)-threshold access structure defined on X_2 and Γ_3 be (3,3)-threshold access structure defined on X_3. Let Γ_0 be (2,3)-threshold access structure defined on $\mathcal{P}/\sim$ =$\{X_1, X_2, X_3\}$. So we easily get $\Gamma = \Gamma_0[\Gamma_1, \Gamma_2, \Gamma_3]$= (2,3)[(2,3),(2,3),(3,3)]. There exists MSPs $\mathcal{M}_1(F_{13}, M_1, \varphi_1, [1,0]^T)$,$\mathcal{M}_2(F_{13}, M_2, \varphi_2, [1,0]^T)$,$\mathcal{M}_3(F_{13}, M_3, \varphi_3, [1,0,0]^T)$ computing Γ_1,Γ_2,Γ_3 respectively. The matrix

$$M_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{matrix} p_1 \\ p_4 \\ p_7 \end{matrix}$$

The matrix

$$M_2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{matrix} p_2 \\ p_3 \\ p_8 \end{matrix}$$

The matrix

$$M_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \begin{matrix} p_5 \\ p_6 \\ p_9 \end{matrix}$$

There exists an MSP $\mathcal{N}_0(F_{13}, N_0, \varphi_0, [1,0,0]^T)$ computing Γ_0. The matrix

$$N_0 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{matrix} X_1 \\ X_2 \\ X_3 \end{matrix}$$

Then there exists an MSP $\mathcal{M}(F_{13}$,M,φ,$[1,0,0,0,0,0]^T)$ computing Γ.The matrix

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 2 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 1 & 1 \\ 1 & 3 & 0 & 0 & 2 & 4 \\ 1 & 1 & 3 & 0 & 0 & 0 \\ 1 & 2 & 0 & 3 & 0 & 0 \\ 1 & 3 & 0 & 0 & 3 & 9 \end{pmatrix} \begin{matrix} p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \\ p_8 \\ p_9 \end{matrix}$$

Let the secret s=3 $\in F_{13}$. The dealer distributes the share of secret, First he choose $(3,1,4,6,8,5)^T$, where the first element 3 is secret,but the other five numbers are random numbers from F_{13}. The share owned by p_1 is 8 (8=$\langle(1,1,1,0,0,0)^T,(3,1,4,6,8,5)^T\rangle$), the share owned by p_2 is 11(11=$\langle(1,2,0,1,0,0)^T,(3,1,4,6,8,5)^T\rangle$), the rest may be deduced by analogy. Let we verify any qualify subset in Γ could recover the secret. We might as well choose a qualify subset set A=$\{p_1,p_3,p_4,p_8\}$. The share owned by p_1 is 8, The share owned by p_3 is 4,The share owned by p_4 is 12 and The share owned by p_8 is 10. So the share owned by A is S_A=$(8,4,12,10)^T$. The matrix

$$M_A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 3 & 0 & 0 \end{pmatrix} \begin{matrix} p_1 \\ p_3 \\ p_4 \\ p_8 \end{matrix}$$

There exists the unique vector λ_A=$(4,10,11,2)^T$ satisfying $M_A^T\lambda_A$=$[1,0,0,0,0,0]^T$. Then $\langle S_A,\lambda_A\rangle$= $\langle(8,4,12,10)^T,(4,10,11,2)^T\rangle$=3=s. For any unqualified subset could not recover the secret, I may as well choose a unqualified subset B=$\{p_3,p_5,p_6,p_9\}$. the share owned by p_3 is 4, the share owned by p_5 is 6, the share owned by p_6 is 5 and the share owned by p_9 is 10. The share owned by B is S_B=$(4,6,5,10)^T$. The matrix

$$M_B = \begin{pmatrix} 1 & 2 & 0 & 2 & 0 & 0 \\ 1 & 3 & 0 & 0 & 1 & 1 \\ 1 & 3 & 0 & 0 & 2 & 4 \\ 1 & 3 & 0 & 0 & 3 & 9 \end{pmatrix} \begin{matrix} p_3 \\ p_5 \\ p_6 \\ p_9 \end{matrix}$$

Because $rank(M_B^T,[1,0,0,0,0,0]^T) \neq \text{rank}(M_B^T)$, there doesn't exist a vector λ_B satisfying $M_B^T\lambda_B$=$[1,0,0,0,0,0]^T$. So the participant set B doesn't recover the secret.The rest unqualified subset could be deduced by analogy.

4 Conclusions

In this paper we have showed the relation between the multipartite access structure and the composite access structure. Next we give a new family of multipartite access structure and prove that there is an ideal secret sharing realizing it. Finally,we illustrate some simple examples to show its applicants.

Acknowledgements

The authors would like to thank Yannan Lin for the valuable comments and remarks.

References

[1] G. R. Blakley. Safeguarding cryptographic keys. AFIPS Conference Proceedings. 48(1979), pp. 313-317.

[2] W. A. Jackson, K. Martin, C O'Keefe. Mutually Trusted Authority-Free Secret sharing Schemes, J.of Cryptology 10, 1997, pp. 261-289.

[3] C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. IEEE Trasactions on Information Theory, Vol.46, No.7, pp. 2596-2604(2000).

[4] E. Martínez-Moro, J. Mozo-Fernández and C. Munuera. Compounding Secret sharing Schemes. Manscript available at http://eprint.iacr.org/2003/048/(2002).

[5] A. Shamir, How to sharing s secret, Comm. ACM 22(11) (1979), 612-613.

[6] M. Karchmer, A. Wigderson. On Span programs, Proc. 8-th Annual structure in Complexity Theory Conference, San Diego, California, 18-21 May 1993. IEEE Computer Society Press, pp. 102-111.

[7] M. J. Collins. A note on ideal tripartite access structures. Manscript available at http://eprint.iacr.org/2002/193/(2002).

[8] P. Pudlak, J. Sgall. Algebraic models of computation and interpolation for algebraic proof systems, Proc. Feasible Arithmetic and proof complexity, LNCS, 1998, pp. 279-295.

[9] Javier Herranz and Germán Sáez. New results on multiparitite access structures. http://eprint.iacr.org/2006/048/(2006).

[10] K. Martin. New secret Sharing schemes from old, J.of Comb. Math. and Combin. Comput. 1993, pp. 65-77.