Secret Sharing Schemes with General Access Structure Based on MSPs

Jun Xu
Department of Mathematics, Xiamen University, Xiamen, 361005, China
Email: xujunxmu@126.com

Xiaomin Zha
Department of Mathematics, Xiamen University, Xiamen, 361005, China
Email: sunnyrain1115@126.com

***Abstract*— In this paper we introduce two operations of access structure to build large monotone span programs MSPs from small MSPs. Furthermore, we point out a new method of constructing secret sharing schemes realizing any access structure, using MSPs.**

***Index Terms*— secret sharing schemes, monotone span programs, access structure**

I. Introduction

Secret sharing schemes are methods designed to split a secret among a group of participants in such a way that the secret can be reconstructed only by specified groups of participant (called *authorized sets*) while unauthorized groups of participants cannot do so. The scheme is called *perfect* if any unauthorized group, even if they pool their shares, has no any information about the secret (in the information-theoretic sense). Let P=$\{p_1, p_2, \ldots, p_n\}$ be the set of participants. The family of authorized subsets $\Gamma \subseteq 2^P$ is called the *access structure*, which is closed under taking supersets $(A \in \Gamma, A \subset B \Rightarrow B \in \Gamma)$. The set of minimal elements in Γ, denoted by Γ_0, uniquely determines the access structure Γ and is called the *basis* of Γ. The family of unauthorized subsets $\Delta \subseteq 2^P$ is sometimes called the *adversary structure*, which is monotonically decreasing: $A \in \triangle, A \supset B \Rightarrow B \in \Delta$. The set of maximal elements in Δ, denoted by Δ^+, uniquely determines the structure of Δ. It is obvious that $\Gamma \cap \Delta$=$\emptyset$. If the union of Γ and Δ is equal to 2^P (so Γ is equal to Δ^c, the complement of $\triangle$), then we say the access structure is complete. The dual access structure $\Gamma^\perp$ of an access structure Γ defined on P is the collection of sets $A \subseteq P$ such that $P \setminus A$=$A^c \in \Delta$.

A particular class of secret sharing schemes is that of (t, n) threshold schemes which were introduced independently by Blakley [1] and Shamir [3], where the (t, n) threshold access structure consists of all subsets of P with at least t out of n participants. That is, Γ_0=$\{A \big| A \subset P, |A| = t\}$. When $t = n$ the (n, n) threshold access structure only consists of P. Monotone span programs (MSPs) were introduced by Karchmer and Wigderson[8] to construct (t, n) threshold schemes. In what follows, for short we shall denote a (t, n) threshold access structure simply by (t, n).

It is obvious that there are large numbers of access structures defined on the set of participants, P. The problem is whether there exists secret sharing scheme realizing any access structure. In fact, this problem has been solved by M.Ito, A.Saito, T.Nishizeki[8]. But in this paper we mainly study the $+$(sum) and $\times$ (product) operations of access structures in order to construct large MSPs from small MSPs and present a new solution of constructing secret sharing scheme realizing any access structure.

The paper is organized as follows. In Section II we recall the concepts related to secret sharing schemes and give the definition of the monotone span program (MSP). We also define various operations for the general access structure and show how to use the MSP to realize a (t,n)-threshold scheme. In Section III we give a construction of secret sharing schemes with general access structures from the MSPs, using the operations on access structures introduced. Finally we conclude the work in Section IV .

II. Preliminaries

Definition 1. [4] Suppose we have a perfect secret sharing scheme realizing an access structure Γ. The information rate for p_i the ratio

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{(\log_2 |S(p_i)|)},$$

where $\mathcal{K}$ is set of all possible secrets for the perfect secret sharing scheme and $S(p_i)$ is set of all possible shares for $p_i \in P$. The information rate of the scheme is denoted by ρ and is defined as

$$\rho = \min\{\rho_i : 1 \leq i \leq n\}.$$

The motivation for this definition is as follows. Since the key K comes from a finite set $\mathcal{K}$, we can think of K as being represented by a bit-string of length $\log_2 |\mathcal{K}|$, by using a binary encoding, for example. In a similar way, a share given to p_i can be represented by a bit-string of length $\log_2 |S(p_i)|$. Intuitively, p_i receives $\log_2 |S(p_i)|$ bits of information(in his or her share), but the information content of the key is$\log_2 |\mathcal{K}|$ bits. Thus ρ_i is the ratio of the number of bits in a share to the number of bits in a share to the number of bits in the key. A secret sharing scheme is called *ideal* if $\rho = 1$.

Notice that in general we always have $\rho \leq 1$. An access structure Γ is called ideal if there is an ideal scheme realizing it.

Definition 2. [5]*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 $\mathcal{F}$, $\varphi : \{1, \ldots, m\} \rightarrow \{1, \ldots, n\}$ is a surjection function and $\overrightarrow{t}$ is a fixed non-zero vector, called target vector. The size of $\mathcal{M}$ is the number of rows, m, and is denoted as size($\mathcal{M}$).*

As φ labels each row with a number i from $\{1, \ldots, m\}$, corresponding to participant $P_{\varphi(i)}$, we can think of each participant as being the "$owner$" of one or more rows. Also consider a "$function$" from $\{p_1, p_2, \ldots, p_n\}$ to $\{1, \ldots, m\}$, which gives for every participant p_i the set of rows owned by him (denoted by $\phi(p_i)$). In other words, ϕ can be viewed as the "$inverse$" of φ. For any set of participants $A \subseteq P$, let M_A be the submatrix consisting of the rows these participants own in M. But we should stay aware of the difference between M_A for $A \subseteq P$ and for $A \subseteq \{1, \ldots, m\}$.

An MSP is said to compute the access structure Γ when $\overrightarrow{t} \in Im((M_A)^T)$ if and only if A is a member of Γ. In other words the participants in A can construct the secret if and only if the target vector is the transposition of some linear combination of the rows they own. We say that A is accepted by $\mathcal{M}$ if and only if $A \in \Gamma$. Otherwise we say A is rejected by $\mathcal{M}$. Note that the change of the basis for the vector space will result in changing the target vector as well: If ($\mathcal{F}$, M, $\overrightarrow{t}$, φ) computes the access structure Γ then for any invertible matrix B with appropriate dimensions ($\mathcal{F}$, MB^T, $B\overrightarrow{t}$, φ) computes the same access structure Γ, since for all $A \subset P$ the following holds:

$$\overrightarrow{t} \in Im((M_A)^T) \Longleftrightarrow B\overrightarrow{t} \in Im(((MB^T)_A)^T).$$

Remark 1: In this paper, T stands for the transposition of a matrix or vector.

Remark 2: $Im((M_A)^T)$ is the space of the transposition of all linear combinations of rows participants own in A.

Remark 3: $\overrightarrow{t} \in Im((M_A)^T) \Longleftrightarrow \exists\ x \in \mathcal{F}^d$, $\overrightarrow{t} = (M_A)^T x \Longleftrightarrow \forall\ d \times d$ invertible matrix B, $B\overrightarrow{t} = B((M_A)^T x) = ((M_A B^T)^T)x = ((MB^T)_A)^T x \Longleftrightarrow B\overrightarrow{t} \in Im(((MB^T)_A)^T)$.

Theorem 1. [3,5]*Any (t, n)-threshold access structure defined on P=$\{p_1, p_2, \ldots, p_n\}$ can be computed by MSP ($\mathcal{F}$, M, ε, φ) with the matrix of size n. ε= $[1, 0, \ldots, 0]^T$ $\in \mathcal{F}^t$, $x_i \in \mathcal{F}$, $1 \leq i \leq n$,*

$$M = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{t-1} \end{pmatrix} \begin{matrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{matrix}$$

Definition 3. [2,6]*Assume Γ_1 and Γ_2 are defined on P_1 and P_2 respectively. Then one can define the sum $\Gamma_1 + \Gamma_2$ and the product $\Gamma_1 \times \Gamma_2$ as the monotone access structures defined on $P_1 \cup P_2$ such that for $A \subseteq P_1 \cup P_2$*

$$A \in \Gamma_1 + \Gamma_2 \Longleftrightarrow A \cap P_1 \in \Gamma_1 \text{ or } A \cap P_2 \in \Gamma_2.$$
$$A \in \Gamma_1 \times \Gamma_2 \Longleftrightarrow A \cap P_1 \in \Gamma_1 \text{ and } A \cap P_2 \in \Gamma_2.$$

Remark: Naturally, the definition above can be extended to the case of more than two access structures, Assume $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$ are defined on P_1,P_2, ..., P_n respectively. Γ_1+Γ_2+...+Γ_n and $\Gamma_1 \times \Gamma_2 \ldots \times \Gamma_n$ are defined on $P_1 \cup P_2 \cup \ldots \cup P_n$ as follows, for $A \subseteq P_1 \cup P_2 \cup \ldots \cup P_n$.

$A \in \Gamma_1 + \Gamma_2 + \ldots + \Gamma_n \Longleftrightarrow A \cap P_1 \in \Gamma_1$ or $A \cap P_2 \in \Gamma_2$ or $\ldots$ or $A \cap P_n \in \Gamma_n$.

$A \in \Gamma_1 \times \Gamma_2 \ldots \times \Gamma_n \Longleftrightarrow A \cap P_1 \in \Gamma_1$ and $A \cap P_2 \in \Gamma_2$ and $\ldots$ and $A \cap P_n \in \Gamma_n$.

In the below Theorem 2 and Theorem 3, we set the target vector $\overrightarrow{t}$ of their MSPs to $\varepsilon := [1, 0, \ldots, 0]^T$.

Theorem 2. [5,6]*Let Γ_1 and Γ_2 be monotone access structures defined on P_1 and P_2 with MSPs $\mathcal{M}_1$ of size m_1 and $\mathcal{M}_2$ of size m_2 respectively. Then there exists an MSP $\mathcal{M}$ of size m_1 + m_2 that computes the sum $\Gamma_1 + \Gamma_2$.*

Remark 1: Suppose M_1, M_2 be corresponding matrices with MSPs $\mathcal{M}_1$, $\mathcal{M}_2$. Let $M_1 = (u_1, M_1^{(1)})$, $M_2 = (u_2, M_2^{(1)})$, where u_1, u_2 are their first columns. Then the MSP $\mathcal{M}$ with the matrix

$$M = \begin{bmatrix} u_1 & M^{(1)} & 0 \\ u_2 & 0 & M^{(2)} \end{bmatrix}$$

computes the sum $\Gamma_1 + \Gamma_2$. Note that M is a $(m_1 + m_2) \times (d_1 + d_2 - 1)$ matrix, and the labelling of M is carried over in a natural way from $\mathcal{M}_1$ and $\mathcal{M}_2$.

Remark 2: Given monotone access structures $\Gamma_1, \ldots, \Gamma_r$, with MSPs $\mathcal{M}_i$ of size m_i, we can obtain an MSP of size $m_1 + m_2 + \ldots + m_r$ by applying Theorem 2 $m-1$ times.

Theorem 3. [6] *Let Γ_1 and Γ_2 be monotone access structures defined on P_1 and P_2 with MSPs $\mathcal{M}_1$ of size m_1 and $\mathcal{M}_2$ of size m_2 respectively. Then there exists an MSP $\mathcal{M}$ of size $m_1 + m_2$ computing the product $\Gamma_1 \times \Gamma_2$.*

Remark 1: Suppose M_1, M_2 be corresponding matrices with MSPs $\mathcal{M}_1$, $\mathcal{M}_2$. Let $M_1 = (u_1, M_1^{(1)})$, $M_2 = (u_2, M_2^{(1)})$, where u_1, u_2 are their first columns. Then the MSP $\mathcal{M}$ with the matrix

$$M = \begin{bmatrix} u_1 & -u_1 & M^{(1)} & 0 \\ 0 & u_2 & 0 & M^{(2)} \end{bmatrix}$$

computes the product $\Gamma_1 \times \Gamma_2$. Note that M is a $(m_1 + m_2) \times (d_1 + d_2)$ matrix, and the labelling of M is carried over in a natural way from $\mathcal{M}_1$ and $\mathcal{M}_2$.

Remark 2: Given monotone access structures $\Gamma_1, \ldots, \Gamma_r$, with MSPs $\mathcal{M}_i$ of size m_i, we can obtain an MSP of size $m_1+m_2+\ldots+m_r$ by applying Theorem 3 $m-1$ times.

Remark 3: Given monotone access structures $\Gamma_1, \ldots, \Gamma_r$, with MSPs $\mathcal{M}_i$ of size m_i, we can obtain an MSP of size $m_1+m_2+\ldots+m_r$ computing $\Gamma_1 * \Gamma_2 * \ldots * \Gamma_r$($*$ is either + or $\times$) by applying Theorem 2 and Theorem 3 finite times.

III. The Operation

In this section, we study two operations on the access structures: +(sum) and $\times$(product).

Lemma 1. [7] *If Γ_1 and Γ_2 are defined on P_1 and P_2, respectively. Then the dual of the sum $\Gamma_1+\Gamma_2$ and the product $\Gamma_1 \times \Gamma_2$, as the monotone access structures defined on $P_1 \cup P_2$*, satisfy the following:

$$(\Gamma_1 \times \Gamma_2)^{\perp} = {\Gamma_1}^{\perp} + {\Gamma_2}^{\perp}, (\Gamma_1+\Gamma_2)^{\perp} = {\Gamma_1}^{\perp} \times {\Gamma_2}^{\perp}.$$

Demorgan's Rule. *Assume Γ_1, Γ_2 and Γ_3 are defined on P_1, P_2 and P_3, respectively. Then $\Gamma_1 \times (\Gamma_2+\Gamma_3)$ and $\Gamma_1+(\Gamma_2 \times \Gamma_3)$, as the monotone access structures defined on $P_1 \cup P_2 \cup P_3$*, satisfy the following

$$\Gamma_1 \times (\Gamma_2+\Gamma_3) = (\Gamma_1 \times \Gamma_2) + (\Gamma_1 \times \Gamma_3) \qquad (1)$$
$$\Gamma_1 + (\Gamma_2 \times \Gamma_3) = (\Gamma_1 + \Gamma_2) \times (\Gamma_1 + \Gamma_3) \qquad (2)$$

Proof :
$A \in \Gamma_1 \times (\Gamma_2+\Gamma_3)$
$\iff \begin{cases} A \cap P_1 \in \Gamma_1 \\ A \cap P_2 \in \Gamma_2 \end{cases}$ *or* $\begin{cases} A \cap P_1 \in \Gamma_1 \\ A \cap P_3 \in \Gamma_3 \end{cases}$
$\iff A \cap (P_1 \cup P_2) \in \Gamma_1 \times \Gamma_2$ or $A \cap (P_1 \cup P_3) \in \Gamma_1 \times \Gamma_3 \iff A \in (\Gamma_1 \times \Gamma_2) + (\Gamma_1 \times \Gamma_3)$.

$\Gamma_1 + (\Gamma_2 \times \Gamma_3) = (\Gamma_1^{\perp} \times (\Gamma_2^{\perp} + \Gamma_3^{\perp}))^{\perp} = ((\Gamma_1^{\perp} \times \Gamma_2^{\perp}) + (\Gamma_1^{\perp} \times \Gamma_3^{\perp}))^{\perp} = (\Gamma_1+\Gamma_2) \times (\Gamma_1+\Gamma_3)$.

Remark: There exists the MSPs computing both sides of the equalities (1) and (2), respectively. But we could improve the information rate if we use the left side of the equality.

Theorem 4. *Let Γ_1 and Γ_2 be monotone access structures defined on P_1 and P_2 with MSPs ($\mathcal{F}$, M_1, $\overrightarrow{1}$, φ_1) $\mathcal{M}_1$ of size m_1 and ($\mathcal{F}$, M_2, $\overrightarrow{1}$, φ_2) $\mathcal{M}_2$ of size m_2, respectively. Then there exists an MSP ($\mathcal{F}$, M, $\overrightarrow{1}$, φ) $\mathcal{M}$ of size m_1+m_2 that computes the product $\Gamma_1 \times \Gamma_2$.*

Proof : Suppose access structures Γ_1 and Γ_2 are computed by MSPs $\mathcal{M}_1$ and $\mathcal{M}_2$ for the target vector $\overrightarrow{1}$. Let M_1 be a $m_1 \times d_1$ matrix and M_2 be a $m_2 \times d_2$. Let M_1 and M_2 be the corresponding matrices. Then the MSP

$$M' = \begin{bmatrix} M_1 & \mathbf{0} \\ \mathbf{0} & M_2 \end{bmatrix}$$

computing $\Gamma_1 \times \Gamma_2$ for the target vector $\overrightarrow{1}$. The labelling of M' is carried over in the natural way from $\mathcal{M}_1$ and $\mathcal{M}_2$.

We show this MSP computes the access structure $\Gamma_1 \times \Gamma_2$. We have :

$$A \in \Gamma \iff (A \cap P_1 \in \Gamma_1 \text{ and } A \cap P_2 \in \Gamma_2)$$

$A \in \Gamma$ if and only if there exists the vector $\overrightarrow{\lambda}$ satisfying $(M'_A)^T \overrightarrow{\lambda} = \overrightarrow{1}$, here $\overrightarrow{\lambda} = (\overrightarrow{\lambda_1}^T, \overrightarrow{\lambda_2}^T)^T \in \mathcal{F}^{(m_1+m_2)}$, $\overrightarrow{\lambda_1} \in \mathcal{F}^{m_1}$, $\overrightarrow{\lambda_2} \in \mathcal{F}^{m_2}$ if and only if $((M_1)_{A \cap P_1})^T \overrightarrow{\lambda_1} = \overrightarrow{1}$ and $((M_2)_{A \cap P_2})^T \overrightarrow{\lambda_2} = \overrightarrow{1}$ if and only if $A \cap P_1 \in \Gamma_1$ and $A \cap P_2 \in \Gamma_2$.

Remark: In the Theorem 4 the first target vector $\overrightarrow{1} \in \mathcal{F}^{m_1}$, the second $\overrightarrow{1} \in \mathcal{F}^{m_2}$ and the third $\overrightarrow{1} \in \mathcal{F}^{m_1+m_2}$.

The below results show that there exists MSP which can compute any monotone access structure. Next we will consider it from the +(sum) operation of the access structure.

Theorem 5. *Let Γ be an access structure defined on P. Then there exists an MSP computing Γ.*

Proof : Suppose the set of minimal authorized subsets in Γ, denoted by Γ_0, is $\{A_1, \ldots, A_t\}$. Let $|A_i| = r_i, \forall i \in \{1, \ldots, t\}$. Because $A_i \subset \mathcal{P}$, we have $\bigcup_{i=1}^{t} A_i \subseteq P$, Let $P' = \bigcup_{i=1}^{t} A_i$. Let Γ_i be $(|A_i|, |A_i|)$-threshold access structure. For short we shall denote $\Gamma_i = (r_i, r_i)$. In fact, we can always assume $P' = P$. Indeed if $P' \neq P$ then there are some participants who belong to none of the minimal authorized subsets. Therefore these persons do not play any role in the system and thus can be removed from P.

$A \in \Gamma \iff A \cap A_1 \in (r_1, r_1)$ or $A \cap A_2 \in (r_2, r_2)$ or $\ldots$ or $A \cap A_t \in (r_t, r_t) \iff A \in (r_1, r_1) + (r_2, r_2) + \ldots + (r_t, r_t)$.

So $\Gamma = (r_1, r_1) + (r_2, r_2) + \ldots + (r_t, r_t)$, there exists an MSP $\mathcal{M}_i$ computing (r_i, r_i) based on Theorem 1, for $\forall i \in \{1, \ldots, t\}$. Suppose M_1, $\ldots$, M_t be corresponding matrices with MSPs $\mathcal{M}_1$, $\ldots$, $\mathcal{M}_t$. Let $M_1 = (u_1, M_1^{(1)})$, $M_2 = (u_2, M_2^{(1)})$, $\ldots$, $M_t = (u_t, M_t^{(1)})$, where $u_1 \ldots u_t$ are their first columns. Then the MSP with

$$M = \begin{bmatrix} u_1 & M_1^{(1)} & 0 & \ldots & 0 \\ u_2 & 0 & M_2^{(1)} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ u_t & 0 & 0 & \ldots & M_t^{(1)} \end{bmatrix}$$

computes $(r_1, r_1) + (r_2, r_2) + \ldots + (r_t, r_t)$. Here M is a $(m_1+m_2+\ldots+m_t) \times (d_1+d_2+\ldots+d_t-t+1)$, and the labelling of M is carried over in a natural way from $\mathcal{M}_1$, $\ldots$, $\mathcal{M}_t$, the target vector of $\mathcal{M}$ is $[1, 0, \ldots, 0]^T$. This result could be easily obtained by applying Theorem 2 $t-1$ times.

IV. Conclusion

In this paper we deal with the secret sharing schemes with the general access structure, we show that any access structure could be computed by the monotone span program, the proof is a simple and new method. To our regret, the information rates of some secret sharing schemes are quite low. In other words, the efficiency of these secret sharing schemes is not high. So we are going to consider how to construct ideal secret sharing schemes realizing some access structures and show some of its applications.

Acknowledgment

The authors would like to thank Jiwen Zeng, Yannan Lin and Huaxiong Wang for the valuable comments and remarks. The authors are very grateful to Christophe Tartary and the anonymous referees for their detailed comments and suggestions regarding this paper.

References

[1] G. Blakley, "Safeguarding Cryptographic Keys," *AFIPS Conference Proceedings*, **48**, 1979.
[2] K.M. Martin, " New Secret Sharing schemes from old," *Journal of Combinationatorial Mathematics and Combinatorial computing*, **14**(1993), 65-77.
[3] A. Shamir, " How to share a secret," *Comn.ACM.*, **22**(1979), 612-613.
[4] D.R. Stinson, " Cryptography: Theory and Practice," *CRC Press*, New York, 1995.
[5] M. Karchmer, A. Wigderson, " On Span Programs," *Proc.8-th Annual Structure in Complexity Theroy Conference*, San Diego, California, 18-21 May 1993, IEEE Computer Society Press, pp.102-111.
[6] V. Nikov, S. Nikova, " New monotone span Program from Old," *Cryrtology ePrint Archive:Report*, 2004/282.
[7] M. van Dijk, "Secret Sharing scheme and Secret Sharing generation," *PhD. Theis* 1997, TU Eindhoven.
[8] M. Ito, A. Saito, T. Nishizeki, "Secret sharing scheme realizing any access structure," *Proc. IEEE Globecom 87*. (1987) 99-102.

Jun Xu was born in Anhui Province of China On October 7st, 1982. He was admitted by Fuyang Normal College to pursue a bachelor degree in Mathematics in 2000, he was again admitted by Xiamen University to achieve master degree in Cryptography in 2004. The graduate education gave him a wide range of vision and taught him how to study the topic. He developed several professional interests in secret sharing schemes and multiparty computation.

Xiaomin Zha was born in Anhui Province of China On November 15th, 1980. He was admitted be Anhui Unversity to a bachelor degree in statistics in 1998, he was a teacher in Tongling College from 2002 to 2004, he was again admitted by Xiamen University to achieve master degree in Cryptography in 2004. He mainly study secret sharing schemes and digital signature.