

# On Multiplicative Secret Sharing Schemes Realizing Graph Access Structures

Ventzislav Nikov<sup>1</sup> and Svetla Nikova<sup>2</sup>

<sup>1</sup> TASS Belgium

`venci.nikov@gmail.com`

<sup>2</sup> Department Electrical Engineering, ESAT/COSIC,

Katholieke Universiteit Leuven, Belgium

`svetla.nikova@esat.kuleuven.be`

**Abstract.** In this paper we consider graph access structures and we show that such an access structure can be realized by a (strongly) multiplicative monotone span program if and only if the privacy structure contains at least three (resp. four) maximal sets. Thus, we obtain a new family of access structures with an explicit construction that is both ideal and strongly multiplicative. Until now only three families of strongly multiplicative access structures are known: the Shamir's threshold secret sharing scheme as well as the recently proposed quasi-threshold construction by Chen and Cramer and the hierarchical threshold construction by Kasper *et al.*

Another way to construct access structures from graphs has been shown by Liu *et al.* Namely, the access structure is based on the connectivity of a given graph. The authors have constructed an ideal multiplicative MSP computing the proposed access structure. We provide refined characterization of this access structure.

## 1 Introduction

After the seminal paper by Cramer *et al.* [3], who introduced Monotone Span Programs (MSP) as a tool to describe linear secret sharing schemes, the problem of finding constructions for MSP with certain properties arose. In particular, interesting are constructions of ideal multiplicative and strongly multiplicative MSP, since such access structures are used for multi-party computation. So far, only a few strongly multiplicative constructions are known: the Shamir's threshold secret sharing scheme as well as the recently proposed quasi-threshold construction by Chen and Cramer and the hierarchical threshold construction by Kasper *et al.* In this paper we consider access structures based on graphs and we provide a construction of a MSP which realizes such access structures and possesses the (strongly) multiplicative property. We also prove some properties of the access structures based on the connectivity of a graph from [5]. We will start with some notation.

**Access Structures:** Denote the *participants* (players) of the scheme by  $P_i$ ,  $1 \leq i \leq n$ , the set of all *players* by  $\mathcal{P} = \{P_1, \dots, P_n\}$  and the set of all subsets of  $\mathcal{P}$  (i.e. the power set of  $\mathcal{P}$ ) by  $P(\mathcal{P})$ . Denote the *dealer* of the scheme by  $\mathcal{D}$ . As usual let us call

the groups which are allowed to reconstruct the secret *qualified* (authorized) and the groups which should not be able to obtain any information about the secret *forbidden* (unqualified). The set of qualified groups is denoted by  $\Gamma$  ( $\Gamma \subseteq P(\mathcal{P})$ ) and the set of forbidden groups by  $\Delta$  ( $\Delta \subseteq P(\mathcal{P})$ ).

The set  $\Gamma$  is called *monotone increasing* if for each set  $A$  in  $\Gamma$  also each superset of  $A$  is in  $\Gamma$ . Similarly,  $\Delta$  is called *monotone decreasing*, if for each set  $B$  in  $\Delta$  also each subset of  $B$  is in  $\Delta$ . A monotone increasing set  $\Gamma$  can be efficiently described by the set  $\Gamma^-$  consisting of the *minimal elements (sets)* in  $\Gamma$ , i.e. the elements in  $\Gamma$  for which no proper subset is also in  $\Gamma$ . Similarly, the set  $\Delta^+$  consists of the *maximal elements (sets)* in  $\Delta$ , i.e. the elements in  $\Delta$  for which no proper superset is also in  $\Delta$ . By definition  $\Gamma \cap \Delta = \emptyset$ . As usual we consider the case when the union of  $\Gamma$  and  $\Delta$  is equal to  $P(\mathcal{P})$  (so,  $\Gamma$  is equal to  $\Delta^c$ , the complement of  $\Delta$ ). Then it is said that  $\Gamma$  is *access structure* and that  $\Delta$  is *privacy structure*.

The simplest access structure is called  $(k, n)$ -threshold, denoted by  $T_{k,n}$ , if all subsets of  $\mathcal{P}$  with at least  $k + 1$  participants are qualified and any subset of up to  $k$  players is forbidden. A privacy structure  $\Delta$  is called  $\mathcal{Q}^\ell$  if no  $\ell$  sets in  $\Delta$  cover the full set  $\mathcal{P}$  of players.

**Secret Sharing Schemes:** A secret sharing scheme with an access structure  $\Gamma$  is a pair (*Share, Reconstruct*) of protocols (phases) namely, the *sharing phase*, where dealer  $\mathcal{D}$  shares to the players a secret  $s \in \mathbb{F}$ , and the *reconstruction phase*, where the players try to reconstruct  $s$ , such that the following two properties hold: *Privacy:* The players of any set  $B \in \Delta$  learn nothing about the secret  $s$  as a result of the sharing phase. *Correctness:* The secret  $s$  can be computed by any set of players  $A \in \Gamma$ .

An SSS is *ideal* if the share of every participant and the secret are equal in size. An access structure  $\Gamma$  is called *ideal* if there is an ideal SSS realizing  $\Gamma$ .

**Monotone Span Programs:** Any Linear SSS (LSSS) with arbitrary monotone access structures can conveniently be described by the following model in linear algebra: A monotone span program (MSP)  $\mathcal{M}$  is a quadruple  $(\mathbb{F}, M, \psi, \varepsilon)$ , where  $\mathbb{F}$  is a finite field,  $M$  is a matrix (with  $m \geq n$  rows and  $d \leq m$  columns),  $\psi : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$  is a surjective function and  $\varepsilon \in \mathbb{F}^d$  is a *target vector*. The size of  $\mathcal{M}$  is the number of rows  $m$ .

Function  $\psi$  assigns each row to a participant. An MSP is said *to compute* an access structure  $\Gamma$  when  $\varepsilon \in \text{im}(M_A^T)$  if and only if  $A$  is a member of  $\Gamma$ . We denote such an access structure by  $\Gamma(\mathcal{M})$ . It is said that  $A$  is *accepted* by  $\mathcal{M}$  if and only if  $A \in \Gamma$ , otherwise it is said that  $A$  is *rejected* by  $\mathcal{M}$ . In other words, the players in  $A$  can reconstruct the secret precisely if the rows they own contain in their linear span the target vector of  $\mathcal{M}$ , and otherwise they get no information about the secret.

For example, in Shamir's  $(k, n)$ -threshold scheme, the dealer chooses a random degree  $k$  polynomial  $P(x)$  subject to  $P(0) = s$  and gives participant  $P_u$  a share  $P(\alpha_u)$ , where  $\alpha_u$  is a non-zero field element. In terms of MSPs, participant  $P_u$  then holds a row  $(1, \alpha_u, \dots, \alpha_u^k)$ . An MSP is called ideal if  $m = n$ , so each participant holds exactly one row. Unless explicitly stated otherwise, we assume that the target vector is  $\varepsilon = (1, 0, \dots, 0)$ .

Any MSP  $\mathcal{M}$  can then be used to construct an LSSS as follows: to share  $s$ , the dealer chooses a random vector  $\mathbf{r} \in \mathbb{F}^{d-1}$ , computes a vector of  $m$  shares  $\mathbf{s} = M(s, \mathbf{r})$  and gives share  $s_i$  to participant  $\psi(i)$ . That is, each participant receives shares corresponding to the rows he holds. A set of participants can then reconstruct  $s$  if and only if the rows they hold contain in their linear span the target vector  $\varepsilon$ , i.e. a set  $A$  is accepted by  $\mathcal{M}$  there exists a so-called *recombination vector* (column)  $\boldsymbol{\lambda}$  such that  $M_A^T \boldsymbol{\lambda} = \varepsilon$ . Using the recombination vector  $\boldsymbol{\lambda}$  it is easy to see that the following relation holds  $\langle \boldsymbol{\lambda}, M_A(s, \mathbf{r})^T \rangle = \langle M_A^T \boldsymbol{\lambda}, (s, \mathbf{r})^T \rangle = \langle \varepsilon, (s, \mathbf{r})^T \rangle = s$  for any secret  $s$  and any random vector  $\mathbf{r}$ . Notice that the vector  $\varepsilon \notin \text{im}(M_B^T)$  if and only if there exists a vector  $\mathbf{k} \in \mathbb{F}^d$  such that  $M_B \mathbf{k} = \mathbf{0}$  and  $\mathbf{k}_1 = 1$ .

**Multiplicative MSPs:** Intuitively, an LSSS is (*strongly*) *multiplicative* if each player  $P_i$  can, from his shares of secrets  $s_1$  and  $s_2$ , compute shares of the product  $s_1 s_2$  in such a way that all players together (respectively, any set of honest players) are able to reconstruct this product. Note that to compute the shares of the sum  $s_1 + s_2$  is trivial when LSSS are used. It is well known that a Shamir secret sharing scheme with  $n$  participants and threshold  $k$  is multiplicative if and only if  $k < n/2$  and strongly multiplicative if and only if  $k < n/3$ .

Cramer *et al.* proposed in [3] an approach to build a multi-party computation protocol from any LSSS, provided that the LSSS is (strongly) multiplicative. It is well known that a necessary condition given MSP to be (strongly) multiplicative is that it computes access structure with  $\mathcal{Q}^2$  ( $\mathcal{Q}^3$ ) privacy structure. Moreover, Cramer *et al.* have demonstrated an efficient construction that renders any LSSS with a  $\mathcal{Q}^2$  access structure (i.e., any access structure for which multiplicativity is possible at all) into a multiplicative scheme that computes the same access structure and has size at most twice the original scheme [3]. But the authors of [6] have shown that the blow-up can be avoided by simply sharing one of the secrets with the given MSP and the other by its dual MSP. Hence it is interesting to look only for constructions of ideal multiplicative MSPs.

On the other hand, no similar result is known for achieving strong multiplicativity, where the general construction is exponential in the size of the original scheme. In fact, there are only three known families of access structures with an explicit construction that is strongly multiplicative (and ideal): the simple Shamir's threshold scheme, a quasi-threshold construction recently proposed by Chen and Cramer [2] and the hierarchical threshold construction even more recently proposed by Kasper et al. [4]. For (strongly) multiplicative MSP the authors of [6] have proven that the access structure computed by the product MSP has the following property  $\Gamma(\mathcal{M} \diamond \mathcal{M}) \subseteq \Gamma(\mathcal{M}) \uplus \Gamma(\mathcal{M})$ .

## 2 Graph Access Structures

A *graph access structure* (GAS) [1, 7] on  $\mathcal{P}$  has the property that  $|A| = 2$  for all  $A \in \Gamma^-$ , that is, the minimal sets correspond to edges of a (connected) graph on  $n$  vertices. Informally, the players are represented by vertices where two players are allowed or forbidden to reconstruct the secret, according to whether or not there is an edge connecting them. The access structure  $\Gamma = \Gamma(G)$  defined by a graph  $G$  with

vertex set  $V(G)$  and edge set  $E = E(G)$  is the access structure defined on the set of participants  $\mathcal{P} = V(G)$  having minimal sets  $\Gamma^- = E(G)$ .

Denote by  $\Delta(A) = \{B | B \subseteq A\}$ , then any privacy structure  $\Delta$  can be described as  $\Delta = \bigcup_{A \in \Delta^+} \Delta(A)$ . In case of GAS Brickell, Davenport [1] and Stinson [7] have proven that it is ideal if and only if the maximal sets of the privacy structure have the following property:  $A \cap B = \emptyset$  for any  $A, B \in \Delta^+$ .

**Theorem 1.** *An ideal graph access structure can be realized by (strongly) multiplicative monotone span program if and only if the privacy structure contains at least three (four) maximal sets.*

*Proof.* It is easy to prove that  $\Delta$  is  $\mathcal{Q}^\ell$  if and only if  $|\Delta^+| \geq \ell + 1$ . First, we will describe the MSP which computes an GAS with  $\ell + 1$  maximal sets. Denote by  $A_j$  for  $j = 1, \dots, \ell + 1$  all elements of  $\Delta^+$ . Notice that  $|A_j| \geq 1$ . For a set  $A_j$  provide different non-zero field element  $\alpha_j$ , then map any player  $P_i \in A_j$  with a row  $(1, \alpha_j)$ . In other

words the MSP is  $M = \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \\ \vdots & \vdots \\ 1 & \alpha_{\ell+1} \end{pmatrix}$  and  $\psi(j) = \{P_i | P_i \in A_j\}$  for  $j = 1, \dots, \ell + 1$ . Note

that  $\Gamma(\mathcal{M})^-$  consists of sets  $\{P_{i_1}, P_{i_2}\}$  such that  $P_{i_1} \in A_{j_1}, P_{i_2} \in A_{j_2}$  for  $A_j \in \Delta^+$  and  $j_1 \neq j_2$ .

Assume from now on that  $|\Delta^+| \geq 3$ , i.e.  $\ell \geq 2$ , which guarantees that the privacy

structure is at least  $\mathcal{Q}^2$ . Now following [3, 6] we obtain that  $M \diamond M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ \vdots & \vdots & \vdots \\ 1 & \alpha_{\ell+1} & \alpha_{\ell+1}^2 \end{pmatrix}$ .

Hence we can derive that  $\Gamma(\mathcal{M} \diamond \mathcal{M})^-$  consists of sets  $\{P_{i_1}, P_{i_2}, P_{i_3}\}$  such that  $P_{i_1} \in A_{j_1}, P_{i_2} \in A_{j_2}, P_{i_3} \in A_{j_3}$  for  $A_j \in \Delta^+$  and  $j_1 \neq j_2 \neq j_3$ , i.e.  $\Gamma(\mathcal{M} \diamond \mathcal{M}) = \Gamma(\mathcal{M}) \uplus \Gamma(\mathcal{M})$ .

Now assume  $|\Delta^+| \geq 3$  then all players together can reconstruct the product of the secrets shared by the product MSP  $\mathcal{M} \diamond \mathcal{M}$ . Hence by definition the MSP  $\mathcal{M}$  is multiplicative. Moreover when  $|\Delta^+| \geq 4$  the restriction of the product MSP  $\mathcal{M} \diamond \mathcal{M}$  to  $B^c$  for any  $B \in \Delta$  has at least 3 maximal forbidden sets (since at most one is reduced) and as it has already been shown such a MSP (i.e. this restricted MSP) is multiplicative. Once again by definition the MSP  $\mathcal{M}$  is strongly multiplicative.  $\square$

### 3 MSPs Based on Connectivity of Graphs

In [5] Liu et al. have proposed another way to construct access structures from graphs, i.e. the access structure is based on the connectivity of a given graph. For so defined access structure an ideal, multiplicative MSP which computes it is constructed. Consider a graph  $G$  with  $p$  vertices, set  $n = \binom{p}{2}$  and associate each edge with a player. Thus we have  $P_1, \dots, P_n$  players. Define the access structure  $\Gamma$  to be the set of sets  $A$  such that the spanning subgraph  $G(V, E_A)$  is a connected graph. Then it is easy to check that the access structure, defined in this way is  $\mathcal{Q}^2$  but not  $\mathcal{Q}^3$ .

Consider a basis  $\boldsymbol{\varepsilon}_i = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{F}^{p-1}$  (1 in the  $i$ -th place). For the  $i$ -th vertex ( $i = 1, \dots, p-1$ ) assign the vector  $\boldsymbol{v}_i = \sum_{j=1}^i \boldsymbol{\varepsilon}_j$  and  $\boldsymbol{v}_0 = \mathbf{0}$ . Hence the vector associated with an edge is obtained as the difference of the vectors associated with both adjacent vertices. Then the vector associated with the player  $P_i$  from the MSP computing the access structure is the vector associated with the corresponding to the player edge. Thus the MSP has an  $n \times (p-1)$  matrix  $M$  consisting of rows of the form  $\boldsymbol{e}_{i,j} = (0, \dots, 0, 1, \dots, 1, 0, \dots, 0)$  (i.e. first  $i$  zeros, then  $j$  ones and end with  $p-1-(i+j)$  zeros) for  $0 \geq i \geq p-2$ ,  $1 \geq j \geq p-1$ , s.t.  $i+j \leq p-1$ . The target vector  $\boldsymbol{\varepsilon}$  is equal to  $\sum_{j=1}^{p-1} \boldsymbol{v}_j = (p-1, p-2, p-3, \dots, 1)$ . The authors of [5] have shown that the ideal MSP, constructed in this way, is multiplicative.

**Proposition 1.** *The access structure based on connectivity of graphs [5] has the following properties:*

- (i) *The MSP computing the access structure is multiplicative but not strongly multiplicative, i.e.,  $\Gamma(\mathcal{M} \diamond \mathcal{M}) = \{\mathcal{P}\}$ .*
- (ii) *There are  $p$  pairs of sets  $A \in \Gamma^-$  and  $B \in \Delta^+$ , such that  $A \cup B = \mathcal{P}$ , where  $|B| = \binom{p-1}{2}$  and  $|A| = p-1$ .*

*Proof.* (i) Form a subgraph, derived from  $G$ , by removing all edges from a fixed vertex. Since the obtained graph is not connected the set of remaining edges (i.e. players) form a set  $B$  which is forbidden. Choose another vertex and in the same way construct another set  $B' \in \Delta$ . Let  $P_i$  be associated with the edge between the two fixed vertices. Then it is easy to be verified that  $B \cup B' = \mathcal{P} \setminus \{P_i\}$ . Using this observation it follows that  $\Gamma(\mathcal{M}) \uplus \Gamma(\mathcal{M}) = \{\mathcal{P}\}$ , hence  $\Gamma(\mathcal{M} \diamond \mathcal{M}) = \{\mathcal{P}\}$ , i.e., the MSP is multiplicative but not strongly multiplicative.

- (ii) Now we will characterize further the considered access structure. Observe that  $|B| = n-p+1 = \binom{p-1}{2}$  (also for  $B'$ ), and since  $|B \cup B'| = n-1$  we obtain that  $|B \cap B'| = n-2p+3$ . On the other hand consider the subgraph with edges all starting from a fixed vertex. This subgraph constitutes a set  $A$  which is qualified, since the graph is connected and  $|A| = p-1$ . Observe that  $A \cup B = \mathcal{P}$  when  $A$  and  $B$  are constructed from the same fixed vertex. Since there are  $p$  vertices then there are so many pairs of sets  $A \in \Gamma^-$  and  $B \in \Delta^+$  such that  $A \cup B = \mathcal{P}$ . It should be noted also that  $|B| > |A|$ .

□

## Acknowledgements

Svetla Nikova was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT and the IAPP- Belgian State - Belgian Science Policy BCRYPT.

## References

1. E. Brickell, D. Davenport. On the classification of the ideal secret sharing schemes, *J. Cryptology* 4, 1991, pp. 123–134.
2. H. Chen, R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields, *CRYPTO'06*, LNCS 4117, 2006, pp. 521–536.
3. R. Cramer, I. Damgard, U. Maurer. General Secure Multi-Party Computation from any Linear Secret Sharing Scheme, *EUROCRYPT'00*, LNCS 1807, 2000, pp. 316–334.
4. E. Kasper, V. Nikov, S. Nikova. Strongly Multiplicative Hierarchical Threshold Secret Sharing, submitted.
5. M. Liu, L. Xiao, Z. Zhang. Multiplicative Linear Secret Sharing Schemes Based on Connectivity of Graphs, *Cryptology ePrint Archive: Report 2005/142*.
6. V. Nikov, S. Nikova, B. Preneel. On Multiplicative Linear Secret Sharing Schemes, *INDOCRYPT'03*, LNCS 2904, 2003, pp. 135–147.
7. D. Stinson. Decomposition constructions for secret sharing schemes, *IEEE Trans. on Information Theory* 40, 1994, pp. 118–125.