

# Strongly Multiplicative Hierarchical Threshold Secret Sharing

Emilia Käsper<sup>1</sup>, Venzislav Nikov<sup>2</sup>, and Svetla Nikova<sup>1</sup>

<sup>1</sup> K.U. Leuven, ESAT/COSIC

<sup>2</sup> TASS Belgium

{emilia.kasper, svetla.nikova}@esat.kuleuven.be, venci.nikov@gmail.com

**Abstract.** We consider multi-party computation (MPC) in a hierarchical setting, where participants have different capabilities depending on their position in the hierarchy. First, we give necessary conditions for multiplication of secrets in a hierarchical threshold linear secret sharing scheme (LSSS). Starting with known ideal constructions, we then propose a modified scheme with improved multiplication properties. We give sufficient conditions for the new scheme to be (strongly) multiplicative and show that our construction is almost optimal in the number of required participants. Thus, we obtain a new class of strongly multiplicative LSSS with explicit ideal constructions. Such LSSS are also useful outside the MPC setting, since they have an efficient algorithm for reconstructing secrets in the presence of errors.

**Keywords.** Secret sharing schemes, multipartite access structures, multi-party computation, strong multiplicativity.

## 1 Introduction

### 1.1 Motivation

In threshold secret sharing, a secret is shared amongst  $n$  participants and can only be reconstructed by more than  $t$  of them together. Such schemes have found numerous applications such as key escrow, distributed file storage and distributed computation. However, in threshold schemes, all participants play an equal role and cannot be distinguished according to trust or authority, whereas in many real-life situations, hierarchies are required. Consider an example from the military. Let the secret be the “nuclear button” of a country and suppose that it can only be accessed by two ministers, or a minister and a general, but not by two generals. In this case, a 2-out-of- $n$  threshold scheme is clearly not suitable, since any two generals could pool their shares together to bypass access control. Secret sharing schemes that take into account hierarchies were the first non-threshold schemes considered in the literature [10, 11, 1].

In this paper, we investigate the *multiplicativity* of hierarchical schemes. Multiplicativity allows participants, holding shares of two secrets  $s$  and  $s'$ , to privately compute shares of the product  $ss'$  without revealing the original secrets. *Strong* multiplicativity further guarantees that in the presence of an active adversary, honest participants can still compute such shares. A simple solution for

multiplication of secrets exists for the Shamir threshold scheme [6]. In general, however, it is not known how to efficiently construct a strongly multiplicative linear secret sharing scheme (LSSS) with the desired non-threshold access structure. Thus, we tackle a more specific problem and show how to achieve strong multiplicativity for a class of access structures.

Strongly multiplicative schemes turn out to be useful even outside the context of multiplying secrets, since they are resistant to errors in shares. Although in any LSSS with a  $\mathcal{Q}_3$  access structure, the secret is uniquely determined even if the shares submitted by corrupted participants contain errors, it is not known how to locate such errors efficiently. An efficient secret reconstruction algorithm is only known for strongly multiplicative LSSS [4]. This implicit “built-in” verifiability makes strongly multiplicative schemes an attractive building block for multi-party computation (MPC) protocols.

## 1.2 Related Work

**Hierarchical Secret Sharing.** Hierarchical threshold secret sharing is a natural extension of simple threshold secret sharing and has been studied by several authors, using slightly different assumptions. Shamir proposed a threshold scheme and further introduced hierarchies by giving higher-level participants a greater number of shares [10]. This results in a weighted threshold access structure: if there are  $m$  levels and participants at level  $i$  hold  $w_i$  shares, then a subset of them can recover the secret if and only if  $w_1 p_1 + \dots + w_m p_m > t$ , where  $p_i$  is the number of participants present at level  $i$ . Let  $w = \max_i w_i$  be the highest weight; Shamir’s hierarchical scheme then has information rate  $1/w$ .

Simmons and Brickell independently considered a different setting where participants are also divided into levels, but each level  $i$  is associated with a different threshold  $t_i$  [11, 1]. A subset of participants can recover the secret if *for some*  $i$ , their total number at levels  $1, \dots, i$  exceeds the threshold  $t_i$ . The scheme proposed by Simmons has information rate  $1/t$ , where  $t$  is the highest threshold, whereas Brickell’s solution is ideal. However, both schemes suffer from inefficiency, since the dealer is required to check possibly exponentially many matrices for non-singularity.

The schemes of Shamir, Simmons and Brickell allow a sufficient number of participants from even the lowest level to reconstruct the secret. Thus, they still do not address our “nuclear button” example, where at least one minister must always be present. Tassa recently proposed a third setting where each level is again associated with a different threshold  $t_i$ , but this time, *for every level*  $i$ , more than  $t_i$  participants from that or higher levels must be present in order to reconstruct the secret [12]. He notes that the threshold scheme provides a simple construction: the secret  $s$  is divided into  $m$  random parts,  $s = s_1 + \dots + s_m$ , and part  $s_i$  is secret-shared with threshold  $t_i$  amongst the participants from levels  $1, \dots, i$ . Again, the resulting scheme is not ideal: participants from level 1 receive  $m$  shares. More interestingly, Tassa also proposed efficient ideal constructions for his setting as well as for the setting of Simmons and Brickell. Both solutions are

based on a generalization of Lagrange interpolation. In this paper, we use these two schemes to construct strongly multiplicative hierarchical threshold schemes.

Finally, hierarchical secret sharing has also been studied in the more general setting of multipartite access structures, where the set of participants is divided into several disjoint subsets and all participants in the same subset play an equivalent role. Farràs et al. give necessary and sufficient conditions for a multipartite access structure to be ideal and apply these results to characterize ideal tripartite structures [5]. While these results study the question whether an access structure can be realized with an ideal LSSS *at all*, for all practical purposes one is clearly interested in an *explicit* efficient construction. For all access structures that we consider in this paper, explicit ideal constructions have already been given. We proceed to study the (strong) multiplicativity of these particular constructions.

**(Strongly) Multiplicative Secret Sharing.** It is well known that a Shamir secret sharing scheme with  $n$  participants and threshold  $t$  is multiplicative if and only if  $t < n/2$  and strongly multiplicative if and only if  $t < n/3$ . Moreover, Cramer et al. 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 has the same access structure and has size at most twice the original scheme [3]. 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 two known families of access structures with an explicit construction that is both ideal and strongly multiplicative: the simple threshold scheme and a quasi-threshold construction recently proposed by Chen and Cramer [2].

### 1.3 Our Contributions

In this paper, we analyze the multiplicativity of two important families of hierarchical secret sharing schemes: threshold schemes based on conjunction and disjunction of conditions. First, we prove necessary conditions for multiplicativity. Then, we look at constructions based on Shamir threshold secret sharing and show that they are always (strongly) multiplicative whenever these necessary conditions are fulfilled. The constructions are not ideal but have a reasonable information rate when the number of levels in the hierarchy is small. Next, we investigate ideal constructions and propose a new conjunctive scheme based on the Tassa scheme [12]. We prove sufficient conditions for (strong) multiplicativity of the modified scheme. The conditions are not tight but we demonstrate that the gap is quite small, i.e, the construction is close to optimal. Finally, we note that our modified scheme actually has better multiplicative properties than the original scheme of Tassa. Thus, as a result of our analysis and our improvements to existing designs, we describe a big class of strongly multiplicative secret sharing schemes that have an efficient ideal construction.

**Road Map.** In Sect. 2 we review the basic theory of linear secret sharing schemes and monotone span programs. In Sect. 3 we introduce hierarchical

threshold access structures and give necessary conditions for (strong) multiplicativity (Sect. 3.1). In Sect. 4, we describe non-ideal constructions and prove their multiplicativity (Theorems 3 and 4). In Sect. 5, we describe two ideal constructions and subsequently propose a modification that improves multiplication properties. The main result of this section is Theorem 6 that gives sufficient conditions for (strong) multiplicativity in the conjunctive case. Finally, in Sect. 6, we discuss some open problems. Technical details of proofs are given in appendices.

## 2 Preliminaries

**Notations.** For a set  $A \subseteq S$ , we denote its complement set by  $A^c = \{b \in S : b \notin A\}$ . The  $i$ th derivative of a polynomial  $P(x)$  is denoted by  $P^{(i)}(x)$ .

**Linear Secret Sharing Schemes.** In a (linear) secret sharing scheme (LSSS), a *dealer* distributes shares of a secret  $s$  amongst  $n$  *participants*. The shares are computed in such a way that *qualified* groups of participants can completely reconstruct the secret (as a linear combination of their shares), while *forbidden* groups obtain no information about the secret whatsoever. An LSSS is *correct* if every qualified group can reconstruct the secret, and *private*, if no forbidden group can learn anything about the secret. In the multi-party computation setting, the scheme is *robust* if honest participants can correctly carry out computations. An LSSS is *ideal* if the share of every participant and the secret are equal in size. The first secret sharing schemes used a  $(t, n)$ -threshold setting, where the number of participants in a group needs to be strictly greater than a threshold  $t$  in order to become qualified. In general, as first put forth by Ito et al. [7], the set of qualified groups may be arbitrary, with the natural restriction that it is monotone: if  $\mathcal{V}$  is qualified, then any  $\mathcal{V}' \supset \mathcal{V}$  is also qualified.

**Access and Adversary Structures.** The set of qualified groups is called the access structure of the LSSS and is denoted by  $\Gamma$ . Conversely, the set of forbidden groups is the privacy structure  $\Delta = \Gamma^c$ . Notice that an adversary can fully corrupt any single set in  $\Delta$  without violating privacy. Sometimes, we distinguish between passive and active corruption and also consider weaker active adversaries  $\Delta_{\mathcal{A}} \subset \Delta$ . In this case, we require privacy w.r.t.  $\Delta$  and robustness w.r.t.  $\Delta_{\mathcal{A}}$ .

**Monotone Span Programs.** LSSS with arbitrary monotone access structures can conveniently be described by the following share dealing mechanism borrowed from linear algebra [8]:

**Definition 1.** 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  $d \geq n$  rows and  $e \leq d$  columns),  $\psi : \{1, \dots, d\} \rightarrow \{1, \dots, n\}$  is a surjective function and  $\varepsilon \in \mathbb{F}^e$  is a target vector. The size of  $\mathcal{M}$  is the number of rows  $d$ .

Function  $\psi$  assigns each row to a participant. An MSP is called ideal if  $d = n$ , 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  $s \in \mathbb{F}$ , the dealer chooses a random

vector  $\mathbf{r} \in \mathbb{F}^{e-1}$ , computes a vector of  $d$  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. For a subset of participants  $\mathcal{V}$ , we denote by  $M_{\mathcal{V}}$  the matrix  $M$  restricted to the rows they hold. Participants in  $\mathcal{V}$  can then reconstruct  $s$  if and only if the rows of  $M_{\mathcal{V}}$  contain the target vector  $\varepsilon$  in their linear span. An MSP  $\mathcal{M}$  computes access structure  $\Gamma$  if  $\varepsilon$  is in the linear span of  $M_{\mathcal{V}}$  precisely if  $\mathcal{V} \in \Gamma$ . In what follows, we identify an LSSS with its underlying MSP. For example, in Shamir's  $(t, n)$ -threshold scheme, the dealer chooses a random degree  $t$  polynomial  $P(x)$  subject to  $P(0) = s$  and gives participant  $u$  a share  $P(\alpha_u)$ , where  $0 \neq \alpha_u \in \mathbb{F}$  is a field element associated with  $u$ . In terms of MSPs, participant  $u$  then holds a row  $(1, \alpha_u, \dots, \alpha_u^t)$ .

The *diamond product* of two matrices  $M_1, M_2$  associated with MSPs  $\mathcal{M}_1, \mathcal{M}_2$  is the matrix

$$M = M_1 \diamond M_2 = \begin{pmatrix} M_1^1 \otimes M_2^1 \\ M_1^2 \otimes M_2^2 \\ \dots \\ M_1^n \otimes M_2^n \end{pmatrix},$$

where  $M_i^j$  is the matrix of rows owned by participant  $j$  in MSP  $\mathcal{M}_i$ ; and  $\otimes$  is the Kronecker product. Given two MSPs  $\mathcal{M}_1 = (\mathbb{F}, M_1, \psi_1, \varepsilon_1)$ ,  $\mathcal{M}_2 = (\mathbb{F}, M_2, \psi_2, \varepsilon_2)$ , we now define the product MSP  $\mathcal{M}_1 \diamond \mathcal{M}_2 = (\mathbb{F}, M_1 \diamond M_2, \psi, \varepsilon_1 \otimes \varepsilon_2)$ , where  $\psi(i, j) = p$  if and only if  $\psi_1(i) = \psi_2(j) = p$ . Product MSPs are useful in investigating the multiplication property of MSPs.

**Multiplicativity.** Informally, an MSP is multiplicative if participants, holding shares of secrets  $s$  and  $s'$ , can compute shares of the product  $ss'$ , using only their local shares. An MSP is strongly multiplicative if honest participants can compute shares of the product. More precisely, we require the product  $ss'$  to be a linear combination of such shares. Given two share-vectors  $\mathbf{s} = M(s, \mathbf{r}) = (s_1, \dots, s_d)$  and  $\mathbf{s}' = M(s', \mathbf{r}') = (s'_1, \dots, s'_d)$ , we define  $\mathbf{s} \diamond \mathbf{s}'$  to be the vector containing all entries  $s_i s'_j$ , where  $\psi(i) = \psi(j)$ . Then  $\mathbf{s} \diamond \mathbf{s}'$  is computed by  $\mathcal{M} \diamond \mathcal{M}$  as  $\mathbf{s} \diamond \mathbf{s}' = M(s, \mathbf{r}) \diamond M(s', \mathbf{r}') = (M \diamond M)((s, \mathbf{r}) \otimes (s', \mathbf{r}'))$ . Each component of  $\mathbf{s} \diamond \mathbf{s}'$  can be computed locally by some participant, and we arrive at the following formal definition:

**Definition 2.** A monotone span program  $\mathcal{M}$  is multiplicative if there exists a recombination vector  $\boldsymbol{\lambda}$  such that for any two secrets  $s$  and  $s'$  and any  $\mathbf{r}, \mathbf{r}'$ , it holds that

$$s \cdot s' = \langle \boldsymbol{\lambda}, M(s, \mathbf{r}) \diamond M(s', \mathbf{r}') \rangle .$$

An MSP  $\mathcal{M}$  is strongly multiplicative with respect to an adversary structure  $\Delta_{\mathcal{A}}$  if for every  $\mathcal{W} \in \Delta_{\mathcal{A}}$ ,  $\mathcal{M}_{\mathcal{W}^c}$  is multiplicative.

If  $\mathcal{M}$  is strongly multiplicative with respect to its privacy structure  $\Delta = \Gamma^c$ , then we say simply that  $\mathcal{M}$  is strongly multiplicative. Shamir's  $(t, n)$ -scheme tolerates the corruption of  $t$  parties and requires an additional  $2t + 1$  honest participants for multiplication, so it is strongly multiplicative for  $n > 3t$ . In general, multiplicativity is strongly related to the  $\mathcal{Q}_\ell$  property of access structures:

**Definition 3.** An adversary structure  $\Delta_{\mathcal{A}}$  is  $\mathcal{Q}_\ell$  if no  $\ell$  sets in  $\Delta_{\mathcal{A}}$  cover the full set of participants. An access structure  $\Gamma$  is  $\mathcal{Q}_\ell$  if the corresponding privacy structure  $\Delta = \Gamma^c$  is  $\mathcal{Q}_\ell$ .

It is well known that multiplicative MSPs only exist for  $\mathcal{Q}_2$  access structures and strongly multiplicative MSPs only exist for  $\mathcal{Q}_3$  access structures [3].

### 3 Hierarchical Threshold Secret Sharing

In this section, we define two important families of hierarchical threshold access structures (HTAccS): the disjunctive HTAccS and the conjunctive HTAccS. We then give *necessary* conditions for schemes realizing these access structures to be (strongly) multiplicative. These conditions depend only on the underlying access structures and not on the specific construction of the LSSS. In Section 5, we analyze explicit constructions of schemes having such access structures and give *sufficient* conditions for those schemes to have the (strong) multiplicativity property.

The first family of access structures corresponds to the setting where at least one threshold must be met, so we call this the disjunctive access structure. The second definition captures our “nuclear button” example where all thresholds must be met, so this is the conjunctive access structure. We also define two adversary structures.

**Definition 4.** Let  $\mathcal{U}$  be a set of  $n$  participants divided into  $m$  disjoint levels, i.e.,  $\mathcal{U} = \bigcup_{i=1}^m \mathcal{U}_i$  where  $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$  for all  $1 \leq i < j \leq m$ . Let  $\mathbf{t} = \{t_i\}_{i=1}^m$  be a monotonically increasing sequence of integers,  $0 \leq t_1 < \dots < t_m$ . Then the  $(\mathbf{t}, n)$ -disjunctive hierarchical threshold access structure (HTAccS) is

$$\Gamma^\exists = \{ \mathcal{V} \subseteq \mathcal{U} : \exists i \in \{1, \dots, m\} \mid |\mathcal{V} \cap (\bigcup_{j=1}^i \mathcal{U}_j)| > t_i \} \quad (1)$$

and the  $(\mathbf{t}, n)$ -conjunctive hierarchical threshold access structure is

$$\Gamma^\forall = \{ \mathcal{V} \subseteq \mathcal{U} : \forall i \in \{1, \dots, m\} \mid |\mathcal{V} \cap (\bigcup_{j=1}^i \mathcal{U}_j)| > t_i \}. \quad (2)$$

The  $(\mathbf{t}, n)$ -disjunctive hierarchical threshold adversary structure (HTAdS) is

$$\Delta^\exists = \{ \mathcal{W} \subseteq \mathcal{U} : \exists i \in \{1, \dots, m\} \mid |\mathcal{W} \cap (\bigcup_{j=1}^i \mathcal{U}_j)| \leq t_i \} \quad (3)$$

and the  $(\mathbf{t}, n)$ -conjunctive hierarchical threshold adversary structure is

$$\Delta^\forall = \{ \mathcal{W} \subseteq \mathcal{U} : \forall i \in \{1, \dots, m\} \mid |\mathcal{W} \cap (\bigcup_{j=1}^i \mathcal{U}_j)| \leq t_i \}. \quad (4)$$

The choice of adversary structures is not arbitrary: a  $(\mathbf{t}, n)$ -disjunctive HTAdS coincides with the privacy structure of a  $(\mathbf{t}, n)$ -conjunctive HTAccS and, vice versa, a  $(\mathbf{t}, n)$ -conjunctive HTAdS coincides with the privacy structure of a  $(\mathbf{t}, n)$ -disjunctive HTAccS. In other words, in the above definition,  $\Delta^\exists = (\Gamma^\forall)^c$  and  $\Delta^\forall = (\Gamma^\exists)^c$ . Notice that for the same threshold vector  $\mathbf{t}$  and the same set of participants  $\mathcal{U}$ , the conjunctive access structure is contained in the disjunctive structure. Conversely, the conjunctive adversary is weaker than the disjunctive adversary:  $\Delta^\forall \subseteq \Delta^\exists$ . A duality relation exists between conjunctive and disjunctive HTAccS [12].

### 3.1 Necessary Conditions for (Strong) Multiplicativity

Recall that an access structure is  $\mathcal{Q}_\ell$  if no  $\ell$  forbidden subsets cover the whole set of participants. It is well known that if an LSSS is multiplicative, then the corresponding access structure must be  $\mathcal{Q}_2$ , and if it is strongly multiplicative, then the access structure must be  $\mathcal{Q}_3$ . In the following, we give necessary and sufficient conditions for the two types of hierarchical access structures to be  $\mathcal{Q}_2$  and  $\mathcal{Q}_3$ . Thus, we immediately obtain necessary conditions for (strong) multiplicativity. However, sufficient conditions for multiplicativity depend on the LSSS rather than just the access structure. In the Shamir setting, every scheme with a  $\mathcal{Q}_2$  ( $\mathcal{Q}_3$ ) access structure is also (strongly) multiplicative, but this is not the case in general. In particular, we can give counterexamples for the ideal hierarchical threshold constructions proposed by Tassa. Thus, we shall later look for stronger conditions that are sufficient for these particular schemes to have multiplication.

In order to be able to distinguish the possibly smaller (active) adversary structure from the privacy structure, we give all our results in terms of general adversary structures (for proofs of theorems in this section, see Appendix A). We begin with the conjunctive adversary that corresponds to the disjunctive access structure. From now on, we denote by  $u_i = |\bigcup_{j=1}^i \mathcal{U}_j|$  the number of participants at levels  $\mathcal{U}_1, \dots, \mathcal{U}_i$  in a hierarchical threshold secret sharing scheme (HTSSS).

**Theorem 1.** *A  $(t, n)$ -conjunctive HTAdS  $\Delta^\vee$  is  $\mathcal{Q}_\ell$  if and only if*

$$\exists i \in \{1, \dots, m\} \quad \text{such that} \quad u_i > \ell t_i . \quad (5)$$

Recalling that a disjunctive access structure  $\Gamma^\exists$  is  $\mathcal{Q}_\ell$  if its corresponding privacy structure  $\Delta^\vee$  is  $\mathcal{Q}_\ell$ , we immediately conclude a necessary condition for multiplicativity.

**Corollary 1.** *If an HTSSS realizing a  $(t, n)$ -disjunctive HTAccS  $\Gamma^\exists$  is multiplicative, then*

$$\exists i \in \{1, \dots, m\} \quad \text{such that} \quad u_i > 2t_i . \quad (6)$$

*If an HTSSS realizing  $\Gamma^\exists$  is strongly multiplicative, then*

$$\exists i \in \{1, \dots, m\} \quad \text{such that} \quad u_i > 3t_i . \quad (7)$$

The result for the conjunctive case is slightly more complicated.

**Theorem 2.** *A  $(t, n)$ -disjunctive HTAdS  $\Delta^\exists$  is  $\mathcal{Q}_\ell$  if and only if*

$$\forall i \in \{1, \dots, m\} \quad u_i > t_i + (\ell - 1)t_m . \quad (8)$$

**Corollary 2.** *If an HTSSS realizing a  $(t, n)$ -conjunctive HTAccS  $\Gamma^\vee$  is multiplicative, then*

$$\forall i \in \{1, \dots, m\} \quad u_i > t_i + t_m . \quad (9)$$

*If an HTSSS realizing  $\Gamma^\vee$  is strongly multiplicative, then*

$$\forall i \in \{1, \dots, m\} \quad u_i > t_i + 2t_m . \quad (10)$$

Notice that if for some  $i > 1$  we have  $u_i - u_{i-1} = |\mathcal{U}_i| \leq t_i - t_{i-1}$ , then for any allowed set  $\mathcal{V}$  in the conjunctive setting, condition  $\mathcal{V} \cap \bigcup_{j=1}^i \mathcal{U}_j > t_i$  implies  $\mathcal{V} \cap \bigcup_{j=1}^{i-1} \mathcal{U}_j > t_{i-1}$ , so the latter threshold is obsolete. Thus, we can collapse levels: the  $(\mathbf{t}, n)$ -conjunctive HTSSS with sets  $\mathcal{U}_1, \dots, \mathcal{U}_m$  has the same access structure as the  $(\mathbf{t}', n)$ -conjunctive HTSSS with  $\mathbf{t}' = (t_1, \dots, t_{i-2}, t_i, t_{i+1}, \dots, t_m)$  and sets  $\mathcal{U}_1, \dots, \mathcal{U}_{i-2}, \mathcal{U}_{i-1} \cup \mathcal{U}_i, \mathcal{U}_{i+1}, \dots, \mathcal{U}_m$ . Assuming now that  $u_i - u_{i-1} > t_i - t_{i-1}$ ,  $i \in \{2, \dots, m\}$ , we see that the first condition of (8)  $u_1 > t_1 + (\ell - 1)t_m$  implies all the remaining conditions  $u_i > t_i + (\ell - 1)t_m$ .

Thus, we see that the necessary condition for the conjunctive hierarchical threshold access structure to be (strongly) multiplicative is essentially a lower bound on the number of participants of highest priority. This is unavoidable, since the adversary can by definition corrupt all participants at levels  $2, \dots, m$  without violating privacy. On the other hand, the strength of the bound is somewhat unnatural in real-life scenarios, where there are usually few top-level participants, be it company directors, ministers or program committee chairs.

An interesting question is to what extent the situation changes if we distinguish the passive adversary from the active adversary. That is, while the conjunctive HTAccS  $\Gamma^\forall$  has privacy w.r.t. the disjunctive HTAdS  $\Delta^\exists$ , we only require that multiplication is robust w.r.t. a weaker adversary  $\Delta_{\mathcal{A}} \subset \Delta^\exists$ . A natural candidate for a weaker active adversary is the conjunctive adversary  $\Delta_{\mathcal{A}} = \Delta^\forall$  from Eq. (4) of Definition 4. Consider a  $(\mathbf{t}', n)$ -conjunctive adversary that can actively corrupt at most  $t'_i$  participants from any subset  $\bigcup_{j=1}^i \mathcal{U}_j$ . The next result gives necessary conditions on participant set sizes in order to preserve robustness of multiplication.

**Corollary 3.** *If an HTSSS realizing a  $(\mathbf{t}, n)$ -conjunctive HTAccS  $\Gamma^\forall$  is strongly multiplicative with respect to a  $(\mathbf{t}', n)$ -conjunctive HTAdS  $\Delta^\forall$ , then*

$$\forall i \in \{1, \dots, m\} \quad u_i > t_i + t'_i + t_m . \quad (11)$$

*Proof.* If the scheme is strongly multiplicative w.r.t.  $\Delta^\forall$ , then for all  $\mathcal{W} \in \Delta^\forall$ ,  $\Gamma_{\mathcal{U} \setminus \mathcal{W}}^\forall$  is multiplicative and thus  $\mathcal{Q}_2$ . Assume now that for some  $k$ ,  $u_k \leq t_k + t'_k + t_m$ . As in the proof of Theorem 1, we can construct a set  $\mathcal{W}$  such that  $\forall i \in \{1, \dots, m\}$   $|\mathcal{W} \cap \bigcup_{j=1}^i \mathcal{U}_j| \leq t'_i$  and in particular,  $|\mathcal{W} \cap \bigcup_{j=1}^k \mathcal{U}_j| = \min\{t'_k, u_k\}$ . But then,  $|\bigcup_{j=1}^k \mathcal{U}_j \setminus \mathcal{W}| \leq u_k - t'_k \leq t_k + t_m$ , so by Theorem 2,  $\Gamma_{\mathcal{U} \setminus \mathcal{W}}^\forall$  is not  $\mathcal{Q}_2$ , contradiction.  $\square$

Notice that the threshold vectors may differ for the access structure and the adversary structure. In the simple case when they coincide, we require  $u_i > 2t_i + t_m$ . More than  $t_i$  participants from  $\bigcup_{j=1}^i \mathcal{U}_j$  are then required to reconstruct the secret, while multiplication is possible when at most  $t_i$  participants from these levels are corrupt.

**Example.** If a  $((1, 3), n)$ -conjunctive scheme is used, then the total number of top-level participants must be at least 5 to allow multiplication; on the other hand, it must be at least as much as 8 to allow multiplication in the presence of an adversary. At the same time, with 6 top-level participants, we can already hope to

assure robustness of multiplication against the weaker, conjunctive adversary. In the next section, we look at constructions with optimal multiplication properties.

## 4 Non-Ideal Constructions

In this section we analyze two simple explicit constructions, one for the conjunctive and one for the disjunctive HTAccS. Although these constructions are not ideal, they have the advantage that they are (strongly) multiplicative whenever the access structure permits multiplication at all. Since both constructions use Shamir secret sharing as the basic building-block, the results are not surprising. Note though that in the conjunctive case, usual care must be taken to assure compatibility of shares: every participant  $u$  must be associated with the same field element  $\alpha_u$  in every Shamir block used to construct the scheme.

The notion of sum and product access structures is helpful in formalizing our results [9]:

**Definition 5.** *If  $\Gamma_1$  and  $\Gamma_2$  are access structures defined on sets  $\mathcal{U}_1$  and  $\mathcal{U}_2$ , respectively, then the sum  $\Gamma_1 + \Gamma_2$  and product  $\Gamma_1 \times \Gamma_2$  access structures are defined on  $\mathcal{U}_1 \cup \mathcal{U}_2$  such that for  $\mathcal{V} \subseteq \mathcal{U}_1 \cup \mathcal{U}_2$ ,*

$$\begin{aligned} \mathcal{V} \in \Gamma_1 + \Gamma_2 &\iff (\mathcal{V} \cap \mathcal{U}_1 \in \Gamma_1 \text{ or } \mathcal{V} \cap \mathcal{U}_2 \in \Gamma_2) \text{ ,} \\ \mathcal{V} \in \Gamma_1 \times \Gamma_2 &\iff (\mathcal{V} \cap \mathcal{U}_1 \in \Gamma_1 \text{ and } \mathcal{V} \cap \mathcal{U}_2 \in \Gamma_2) \text{ .} \end{aligned}$$

Now, let  $\Gamma_i$  be a  $(t_i, u_i)$ -threshold access structure on the set  $\bigcup_{j=1}^i \mathcal{U}_j$ . Clearly, every  $(t, n)$ -disjunctive HTAccS is a sum access structure:  $\Gamma = \Gamma_1 + \dots + \Gamma_m$ . Similarly, every  $(t, n)$ -conjunctive HTAccS is a product access structure:  $\Gamma = \Gamma_1 \times \dots \times \Gamma_m$ . We use the following well-known result to construct MSPs for the disjunctive and conjunctive HTAccS:

**Lemma 1.** *If MSPs  $\mathcal{M}_1$  and  $\mathcal{M}_2$  with matrices  $M_1 = (\mathbf{v}_1 \ \overline{M}_1)$  and  $M_2 = (\mathbf{v}_2 \ \overline{M}_2)$  (where  $\mathbf{v}_1$  and  $\mathbf{v}_2$  are the first columns of the matrices) and target vectors  $(1, 0, \dots, 0)$  compute access structures  $\Gamma_1$  and  $\Gamma_2$ , then MSPs  $\mathcal{M}_1 + \mathcal{M}_2$  and  $\mathcal{M}_1 \times \mathcal{M}_2$  defined by*

$$M_1 + M_2 = \begin{pmatrix} \mathbf{v}_1 & \overline{M}_1 & \mathbf{0} \\ \mathbf{v}_2 & \mathbf{0} & \overline{M}_2 \end{pmatrix} \quad \text{and} \quad M_1 \times M_2 = \begin{pmatrix} \mathbf{v}_1 & \mathbf{0} & \overline{M}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{v}_2 & \mathbf{0} & \overline{M}_2 \end{pmatrix} \quad (12)$$

compute  $\Gamma_1 + \Gamma_2$  and  $\Gamma_1 \times \Gamma_2$ , respectively.<sup>1</sup>

The first construction formalizes the situation where the same secret is shared twice using two different access structures; the second corresponds to the case where a secret is split into two parts and each part is shared according to a different access structure. Using this construction with Shamir secret sharing as the basic building block, we can give strongly multiplicative MSPs for the disjunctive and the conjunctive HTAccS. The corresponding schemes have information rate  $1/m$ .

<sup>1</sup> the target vector of  $\mathcal{M} \times \mathcal{M}$  is  $(1, 1, 0, \dots, 0)$

The disjunctive construction is obtained by sharing the same secret in  $m$  different ways using  $m$  different thresholds  $t_1, \dots, t_m$ . The multiplication property then follows from the multiplicativity of the underlying Shamir scheme. For the conjunctive case, we choose randomly  $m$  different secrets  $s_1, \dots, s_m$  such that they add up to the secret:  $s = s_1 + \dots + s_m$ . Each  $s_i$  is then shared using a different threshold  $t_i$ . We give constructive proofs of the following results in Appendix B.

**Theorem 3.** *If  $\Gamma^\exists$  is a  $\mathcal{Q}_2$  ( $\mathcal{Q}_3$ ) disjunctive HTAccS, then there exists a (strongly) multiplicative MSP of size  $u_1 + \dots + u_m$  computing  $\Gamma^\exists$ .*

**Theorem 4.** *If  $\Gamma^\forall$  is a  $\mathcal{Q}_2$  ( $\mathcal{Q}_3$ ) conjunctive HTAccS, then there exists a (strongly) multiplicative MSP of size  $u_1 + \dots + u_m$  computing  $\Gamma^\forall$ . If  $\Gamma^\forall$  is a conjunctive HTAccS that satisfies condition (11) of Corollary 3, then there exists an MSP of size  $u_1 + \dots + u_m$  computing  $\Gamma^\forall$  that is strongly multiplicative with respect to the conjunctive adversary  $\Delta^\forall$  of Corollary 3.*

**Example.** Suppose that a secure computation is carried out by 5 servers, and 3 of them are trusted more than the remaining two. If a (1, 5)-threshold scheme is used, then the two semi-trusted servers can jointly recover all secrets. If a (2, 5)-threshold scheme is used, then no errors are tolerated in multiplication. But if we use a two-level ((0, 1), 5)-conjunctive scheme, then the presence of one trusted server is always required, while the failure of one trusted server is also tolerated. The maximum share size is still reasonable—it is double the size of the secret. However, when the hierarchy has more levels, it becomes important to look for ideal constructions.

## 5 Ideal Constructions

We proceed to analyze the multiplicativity of two ideal constructions proposed by Tassa [12]. Both schemes, one for the conjunctive and one for the disjunctive hierarchical threshold access structure, draw ideas from polynomial interpolation.

### 5.1 The Conjunctive Construction

Tassa’s key idea is to give participants in the top level of the hierarchy points on a polynomial, and participants in lower levels points on derivatives of the same polynomial. This way, shares of lower levels contain less information; in particular, when the secret is the free coefficient, points on derivatives contain no information about the secret, so a number of participants from the top level is always required to recover the secret. More precisely, in order to share a secret  $s$  according to a  $(t, n)$ -conjunctive HTAccS, the dealer (1) selects a random polynomial  $P(x) = \sum_{i=0}^{t_m} a_i x^i$  subject to  $a_0 = s$ , where  $t_m$  is the highest threshold; and (2) gives participant  $u \in \mathcal{U}_i$  a share  $P^{(t_{i-1}+1)}(\alpha_u)$ , i.e., the  $(t_{i-1} + 1)$ th

derivative of  $P(x)$  at  $x = \alpha_u$ , where  $t_0 = -1$  and  $\alpha_u$  is the field element associated with participant  $u$ . Thus, in the corresponding MSP, participant  $u \in \mathcal{U}_i$  holds a row

$$(0, \dots, 0, c_0, c_1\alpha_u, c_2\alpha_u^2, \dots, c_{t_m-t_{i-1}-1}\alpha_u^{t_m-t_{i-1}-1}) \quad (13)$$

with  $t_{i-1} + 1$  leading zeroes (where  $c_i = (t_{i-1} + i + 1)!/i!$ ).

**Example.** Consider a two-level scheme with thresholds  $t_1 = 0$ ,  $t_2 = 2$  and suppose that there are 4 participants at level  $\mathcal{U}_1$  and 1 participant at level  $\mathcal{U}_2$ . The matrix of the MSP is then

$$M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \\ 1 & \alpha_4 & \alpha_4^2 \\ 0 & 1 & 2\alpha_5 \end{pmatrix}, \quad (14)$$

where  $\alpha_i$  are some distinct non-zero field elements. The first question that we need to ask is: does this construction indeed yield the desired hierarchical access structure? It turns out that some care must be taken in assigning field elements to participants, but that even a random allocation strategy is successful with an overwhelming probability [12]:

**Theorem 5.** *Assume a random allocation of participant identities in a field  $\mathbb{F}_q$ . Then the ideal HTSSS of (13) computes a  $(t, n)$ -conjunctive HTAccS with probability*

$$p \geq 1 - \frac{\binom{n+1}{t_m+1} t_m (t_m - 1)}{2(q - t_m - 1)}.$$

The secret space is normally very large compared to the threshold  $t_m$  and the number of participants  $n$ , hence the success probability  $p = 1 - \Theta(1/q)$  is indeed overwhelming.

Next, we look at multiplication. While secret sharing based on polynomials is “naturally” multiplicative, derivatives bring trouble. Indeed, when participants from the top level multiply their shares of  $P(x)$  and  $Q(x)$ , they obtain shares of  $(P \cdot Q)(x)$ , but participants holding points on  $P^{(i)}(x)$  and  $Q^{(i)}(x)$  obtain shares of  $(P^{(i)} \cdot Q^{(i)})(x) \neq (P \cdot Q)^{(j)}(x)$  for any  $j$ . Returning to Example (14), we see that the scheme is not multiplicative, even though the access structure is  $\mathcal{Q}_2$ . We get

$$M \diamond M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^2 & \alpha_1^3 & \alpha_1^4 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^2 & \alpha_2^3 & \alpha_2^4 \\ 1 & \alpha_3 & \alpha_3^2 & \alpha_3^2 & \alpha_3^3 & \alpha_3^4 \\ 1 & \alpha_4 & \alpha_4^2 & \alpha_4^2 & \alpha_4^3 & \alpha_4^4 \\ 0 & 0 & 0 & 1 & 2\alpha_5 & 4\alpha_5^2 \end{pmatrix}.$$

Clearly, the five participants in  $\mathcal{U}_1 \cup \mathcal{U}_2$  can recover the secret only if the five last columns of the matrix are linearly dependent. However, expanding by the last

row, we see that the corresponding determinant is a Vandermonde determinant (multiplied by  $\alpha_1\alpha_2\alpha_3\alpha_4$ ), so it is always non-zero, regardless of the choice of field elements.

Before analyzing further the multiplicativity of the scheme, we modify the distribution of shares. Namely, we ignore the leading coefficients  $c_i$  in (13) and let participant  $u \in \mathcal{U}_i$  hold a row

$$(0, 0, \dots, 0, 1, \alpha_u, \dots, \alpha_u^{t_m - t_{i-1} - 1}) \quad (15)$$

with  $t_{i-1} + 1$  leading zeroes. In the example above, we let the fifth participant hold  $(0, 1, \alpha_5)$  instead of  $(0, 1, 2\alpha_5)$ . This tweak simplifies the analysis and in fact even improves the multiplication property of the scheme. Since all arguments in the proof of Theorem 5 apply equally for the modified scheme, random allocation yields the correct access structure with an overwhelming probability. For completeness, we give the proof of Theorem 5 for the modified case in Appendix C.

Denote by  $p_i$  the number of participants at level  $\mathcal{U}_i$ , i.e.,  $p_i = |\mathcal{U}_i| = u_i - u_{i-1}$ . The next theorem gives sufficient conditions for having an ideal HTSSS with multiplication for a conjunctive HTAccS:

**Theorem 6.** *If the  $(\mathbf{t}, n)$ -conjunctive HTAccS computed by the HTSSS of (15) satisfies*

$$\begin{aligned} &\exists s, 0 = i_1 < i_2 < \dots < i_s = m \quad \text{such that} \\ &\forall j \in \{1, \dots, s-1\} \quad p_{i_{j+1}} > t_{i_{j+1}} + t_m - 2(t_{i_j} + 1) , \end{aligned} \quad (16)$$

where  $t_0 = -1$ , then the scheme is multiplicative.

In order to understand condition (16), we note that taking  $i_j = j - 1$  and  $s = m + 1$  yields

$$\forall i \in \{1, \dots, m\} \quad p_i > t_i + t_m - 2(t_{i-1} + 1) .$$

*Proof.* We prove the theorem for the general condition (16). The key idea is to prove that (1) there exists a set of participants  $\mathcal{V}$  such that the corresponding product MSP  $\mathcal{M}_{\mathcal{V}} \diamond \mathcal{M}_{\mathcal{V}}$  has a block-triangular matrix; and (2) the blocks on the diagonal of  $\mathcal{M}_{\mathcal{V}} \diamond \mathcal{M}_{\mathcal{V}}$  are Vandermonde blocks, and its determinant is thus non-zero. Technical details of the proof are presented in Appendix D.  $\square$

**Example.** Consider a  $((1, 2, 4), n)$ -scheme. Then, any one of the following sets of conditions is sufficient for the scheme to be multiplicative:

$$p_1 > 8 \text{ or } p_1 > 6 \ \& \ p_3 > 2 \text{ or } p_1 > 5 \ \& \ p_2 > 2 \ \& \ p_3 > 2 \text{ or } p_1 > 5 \ \& \ p_2 > 4 . \quad (17)$$

For example, a set  $\mathcal{V}$  with 6 participants from level  $\mathcal{U}_1$  and 5 participants from level  $\mathcal{U}_2$  is allowed. In comparison, if we were using the original Tassa scheme, the same set  $\mathcal{V}$  would always be forbidden. Thus, by deleting the leading coefficients

in the lower-order shares, we have actually improved the multiplication property of the scheme (see Appendix D for details).

Finally, we also give sufficient conditions for strong multiplicativity. For simplicity, we consider only the case where participants from all levels are engaged.

**Corollary 4.** *If the  $(t, n)$ -conjunctive HTAccS computed by the HTSSS described above satisfies*

$$\forall i \in \{1, \dots, m\} \quad p_i > t_i + 2t_m - 2(t_{i-1} + 1) \quad , \quad (18)$$

where  $t_0 = -1$ , then the scheme is strongly multiplicative. If it satisfies

$$\forall i \in \{1, \dots, m\} \quad p_i > t_i + t'_i + t_m - 2(t_{i-1} + 1) \quad , \quad (19)$$

then it is strongly multiplicative with respect to a  $(t', n)$ -conjunctive HTAdS  $\Delta^\forall$ .

*Proof.* We prove only the first claim. Let  $\mathcal{W}$  be a corrupted set and assume (18). Again, there must exist an index for which  $\mathcal{W}$  does not cross the threshold, i.e.,  $\exists k : |\mathcal{W} \cap \bigcup_{j=1}^k \mathcal{U}_j| \leq t_k \leq t_m$ . But then

$$\begin{aligned} \forall i < k \quad & |(\mathcal{U} \setminus \mathcal{W}) \cap \mathcal{U}_i| = |\mathcal{U}_i| - |\mathcal{W} \cap \mathcal{U}_i| \geq p_i - t_m > t_i + t_m - 2(t_{i-1} + 1) \quad , \\ & |(\mathcal{U} \setminus \mathcal{W}) \cap \mathcal{U}_k| = |\mathcal{U}_k| - |\mathcal{W} \cap \mathcal{U}_k| \geq p_k - t_k > 2t_m - 2(t_{k-1} + 1) \quad , \end{aligned}$$

so  $s = k + 1$  with index set  $i_j = j - 1$ ,  $j = 1, \dots, k$  satisfies the assumptions of Theorem 6 and the participants in  $\bigcup_{j=1}^k \mathcal{U}_j \setminus \mathcal{W}$  can compute shares of the product.  $\square$

Although there is a gap between necessary and sufficient conditions for (strong) multiplicativity, the positive implication of our results is the following: it is possible to achieve (strong) multiplicativity while keeping the number of top-level participants at the minimum required threshold. That is, if there are sufficiently many lower-level participants, then the scheme is multiplicative for  $u_1 > t_1 + t_m$  and strongly multiplicative for  $u_1 > t_1 + 2t_m$ . Returning to Example (17) above, the minimum requirement for multiplicativity is  $u_1 > 5$ . Additionally, we require  $u_2 > 6$  and  $u_3 > 8$  (see Corollary 2). On the other hand, as we have seen,  $p_1 > 5$ ,  $p_2 > 2$  and  $p_3 > 2$  is sufficient. Thus, we only need 3 extra participants from lower levels to fill the gap.

## 5.2 The Disjunctive Construction

Tassa's construction is again based on polynomial interpolation, only this time, participants from higher levels get lower-order derivatives. Also, the secret is the set to be the highest-power coefficient  $a_{t_m}$ , instead of the free coefficient  $a_0$ . So, to share a secret according to a  $(t, n)$ -disjunctive HTAccS, the dealer (1) selects a random polynomial  $P(x) = \sum_{i=0}^{t_m} a_i x^i$ , where  $t_m$  is the highest threshold and the secret is  $s = a_{t_m}$ ; and (2) gives participant  $u \in \mathcal{U}_i$  a share  $P^{(t_m - t_i)}(\alpha_u)$ . An analog of Theorem 5 again guarantees the desired access structure.

Recall from Corollary 1 that if the disjunctive scheme is (strongly) multiplicative, then there exists an index  $i$  for which  $u_i > 2t_i$  ( $u_i > 3t_i$ ). On the other hand, it is easy to see that if the number of participants at some single level  $i$  is  $p_i > 2t_i$  ( $p_i > 3t_i$ ), then the scheme is (strongly) multiplicative. However, if these conditions hold, then participants in  $\mathcal{U}_i$  can compute shares of the product without engaging participants in other sets at all. In the following we show that strong multiplicativity is possible even if such an index  $i$  does not exist.

**Theorem 7.** *If the  $(\mathbf{t}, n)$ -disjunctive HTAccS computed by the HTSSS described above satisfies*

$$\exists i \text{ such that } u_i > 3t_i + 2 \sum_{j=1}^{i-1} t_j, \quad (20)$$

*then the scheme is strongly multiplicative.*

*Proof.* Assume that (20) holds. The  $(\mathbf{t}, n)$ -conjunctive hierarchical threshold adversary  $\Delta^\forall$  can corrupt at most  $t_i$  participants from  $\bigcup_{j=1}^i \mathcal{U}_j$ . Consequently, there are more than  $2 \sum_{j=1}^i t_j$  honest participants in this set. But then at least one of the sets  $\mathcal{U}_j$ ,  $j \in \{1, \dots, i\}$  must have more than  $2t_j$  honest participants, and they can compute shares of the product.  $\square$

**Example.** Consider a  $((1, 2, 4), n)$ -disjunctive HTAccS and let  $p_1 = 3$ ,  $p_2 = 5$  and  $p_3 = 11$ . Then the HTSSS computing the HTAccS is strongly multiplicative, even though  $p_i \leq 3t_i$  for  $i \in \{1, 2, 3\}$ .

## 6 Concluding Remarks

Strongly multiplicative secret sharing schemes are used in multi-party computation to obtain error-free multiplication unconditionally secure against an active adversary. However, enforcing the multiplication property is in general expensive and few efficient non-threshold examples are known.

We have proposed two different solutions for obtaining strong multiplication in the hierarchical threshold setting. The constructions of Section 4 achieve robustness against the strongest possible adversary. These schemes are not ideal but have a reasonable information rate for hierarchies with few levels. The ideal constructions of Section 5 are strongly multiplicative under somewhat stronger, but still feasible assumptions. In particular, we have proposed a modification that improves the multiplication properties of the scheme. Our results are not tight and it is possible that better bounds can be obtained by more careful analysis. However, we have proven the modified scheme to be optimal with respect to the most crucial property—the number of required top-level participants.

The modified ideal scheme has a randomized identity allocation strategy with failure probability  $p = \Theta(1/q)$ , which is a safe bet for large field sizes  $q$ . Still, for the original conjunctive and disjunctive constructions, the author also

proposed a deterministic allocation strategy, which has zero failure probability if the field is sufficiently large. The strategy allocates identities in a monotone fashion, so participants from higher levels get “smaller” field elements. It would be interesting to verify if the deterministic strategy also applies for the new scheme.

**Acknowledgements.** The authors thank Sven Laur and George Danezis for helpful comments. This work 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. Svetla Nikova was also partially supported by the Flemish IWT SBO project ADAPID and Emilia Käsper by the FWO-Flanders project nr. G.0317.06 *Linear Codes and Cryptography*.

## References

1. Ernest F. Brickell. Some ideal secret sharing schemes. In *Advances in Cryptology - EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 468–475. Springer, 1989.
2. Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In *Advances in Cryptology - CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 521–536. Springer, 2006.
3. Ronald Cramer, Ivan Damgård, and Ueli M. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer, 2000.
4. Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, and Carles Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. In *Advances in Cryptology - CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 327–343. Springer, 2005.
5. Oriol Farràs, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. In *Advances in Cryptology - EUROCRYPT 2007*, 2007. To appear.
6. Rosario Gennaro, Michael O. Rabin, and Tal Rabin. Simplified VSS and fact-track multiparty computations with applications to threshold cryptography. In *ACM Symposium on Principles of Distributed Computing*, pages 101–111, 1998.
7. M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *IEEE Goblecom '87*, 1987.
8. Mauricio Karchmer and Avi Wigderson. On span programs. In *Structure in Complexity Theory Conference*, pages 102–111, 1993.
9. Keith M. Martin. New secret sharing schemes from old. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 14:65–77, 1993.
10. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
11. Gustavus J. Simmons. How to (really) share a secret. In *Advances in Cryptology - CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 390–448. Springer, 1990.

12. Tamir Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology*, 20(2):237–264, 2007.

## A $\mathcal{Q}_\ell$ Conditions (Theorems 1 and 2)

*Proof (of Theorem 1).* If (5) holds for some  $i$ , then no  $\ell$  adversarial sets can cover all participants in  $\bigcup_{j=1}^i \mathcal{U}_j$ , so  $\Delta^\forall$  is  $\mathcal{Q}_\ell$ . Assume now that (5) does not hold, so  $\forall i \quad u_i \leq \ell t_i$ . Clearly, it is possible to divide the  $u_1$  participants of level  $\mathcal{U}_1$  into  $\ell$  sets  $\mathcal{W}_1, \dots, \mathcal{W}_\ell$  such that  $|\mathcal{W}_k \cap \mathcal{U}_1| \leq t_1$  for  $k \in \{1, \dots, \ell\}$ . We complete the proof by induction on levels. Suppose that all  $u_i$  participants from  $\bigcup_{j=1}^i \mathcal{U}_j$  have been divided into  $\ell$  sets such that  $|\mathcal{W}_k \cap \bigcup_{j=1}^i \mathcal{U}_j| = w_k \leq t_i$  for  $k \in \{1, \dots, \ell\}$ . Then, we can add  $t_{i+1} - w_k$  participants from  $\mathcal{U}_{i+1}$  into  $\mathcal{W}_k$  without violating  $|\mathcal{W}_k \cap \bigcup_{j=1}^{i+1} \mathcal{U}_j| \leq t_{i+1}$ . On the other hand,

$$|\mathcal{U}_{i+1}| = u_{i+1} - u_i = u_{i+1} - \sum_{k=1}^{\ell} w_k \leq \ell t_{i+1} - \sum_{k=1}^{\ell} w_k = \sum_{k=1}^{\ell} (t_{i+1} - w_k) ,$$

so all  $u_{i+1}$  participants from  $\bigcup_{j=1}^{i+1} \mathcal{U}_j$  can also be allocated.  $\square$

*Proof (of Theorem 2).* Assume first that (8) holds and consider any  $\ell$  corrupt sets  $\mathcal{W}_1, \mathcal{W}_2, \dots, \mathcal{W}_\ell \in \Delta^\exists$ . For  $k \in \{1, \dots, \ell\}$ , let  $i_k$  be the smallest index such that  $|\mathcal{W}_k \cap (\bigcup_{j=1}^{i_k} \mathcal{U}_j)| \leq t_{i_k}$  and assume w.l.o.g. that  $i_1 \leq i_2 \leq \dots \leq i_\ell$ . Then

$$\begin{aligned} |(\bigcup_{k=1}^{\ell} \mathcal{W}_k) \cap (\bigcup_{j=1}^{i_1} \mathcal{U}_j)| &\leq \sum_{k=1}^{\ell} |\mathcal{W}_k \cap (\bigcup_{j=1}^{i_1} \mathcal{U}_j)| \leq \sum_{k=1}^{\ell} |\mathcal{W}_k \cap (\bigcup_{j=1}^{i_k} \mathcal{U}_j)| \\ &\leq \sum_{k=1}^{\ell} t_{i_k} \leq t_{i_1} + (\ell - 1)t_m < u_{i_1} , \end{aligned}$$

implying that  $\mathcal{W}_1, \mathcal{W}_2, \dots, \mathcal{W}_\ell$  cannot cover all players in  $\bigcup_{j=1}^{i_1} \mathcal{U}_j$ , so  $\Delta^\exists$  is  $\mathcal{Q}_\ell$ .

Assume now that condition (8) does not hold and let  $i$  be the smallest index such that  $u_i \leq t_i + (\ell - 1)t_m$ . Construct  $\ell$  sets as follows. Let  $\mathcal{W}_1, \dots, \mathcal{W}_{\ell-1}$  be pairwise disjoint sets that each consist of some  $t_m$  participants from  $\bigcup_{j=1}^i \mathcal{U}_j$ . Clearly,  $\mathcal{W}_k \in \Delta^\exists$ ,  $k \in \{1, \dots, \ell - 1\}$ . Finally, let  $\mathcal{W}_\ell$  consist of the remaining  $u_i - (\ell - 1)t_m$  participants in  $\bigcup_{j=1}^i \mathcal{U}_j$  and all the participants in  $\bigcup_{j=i+1}^m \mathcal{U}_j$ . Then  $|\mathcal{W}_\ell \cap (\bigcup_{j=1}^i \mathcal{U}_j)| = u_i - (\ell - 1)t_m \leq t_i$ , implying that  $\mathcal{W}_\ell \in \Delta^\exists$ . On the other hand,  $\bigcup_{k=1}^{\ell} \mathcal{W}_k = \mathcal{U}$ , so  $\Delta^\exists$  is not  $\mathcal{Q}_\ell$ .  $\square$

## B Non-Ideal Constructions (Theorems 3 and 4)

*Proof (of Theorem 3).* We prove only the multiplicative case. Let  $\mathcal{M}_i$  with  $M_i = (\mathbf{1} \overline{M}_i)$  be an MSP realizing the  $(t_i, u_i)$ -threshold access structure. Consider the

MSP  $\mathcal{M} = \mathcal{M}_1 + \dots + \mathcal{M}_m$  with matrix

$$M = \begin{pmatrix} \mathbf{1} & \overline{M}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \overline{M}_1 & \dots & \mathbf{0} \\ \vdots & & & \ddots & \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \dots & \overline{M}_m \end{pmatrix},$$

where participants in  $\bigcup_{j=1}^i \mathcal{U}_j$  hold rows from  $(\mathbf{1}, \mathbf{0}, \dots, \mathbf{0}, \overline{M}_i, \mathbf{0}, \dots, \mathbf{0})$ . By Lemma 1,  $\mathcal{M}$  computes the  $(\mathbf{t}, n)$ -disjunctive HTAccS  $\Gamma^\exists$ . Now, if  $\Gamma^\exists$  is  $\mathcal{Q}_2$ , then by Theorem 1, there exists an index  $i$  s.t.  $u_i > 2t_i$ . But then participants from  $\mathcal{U}_{j=1}^i$  can clearly compute the product by using a recombination vector  $(0, \dots, 0, \lambda_i, 0, \dots, 0)$ , where  $\lambda_i$  is a suitable recombination vector for the MSP  $\mathcal{M}_i \diamond \mathcal{M}_i$ .  $\square$

*Proof (of Theorem 4).* We prove only the strongly multiplicative case. As before, let  $\mathcal{M}_i$  with  $M_i = (\mathbf{1} \ \overline{M}_i)$  be the  $(t_i, u_i)$ -threshold MSP. Consider the MSP  $\mathcal{M} = \mathcal{M}_1 \times \dots \times \mathcal{M}_m$ , where

$$M = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \dots & \mathbf{0} & \overline{M}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \dots & \mathbf{0} & \mathbf{0} & \overline{M}_1 & \dots & \mathbf{0} \\ \vdots & & & & & & \ddots & \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{1} & \mathbf{0} & \mathbf{0} & \dots & \overline{M}_m \end{pmatrix},$$

where participants in  $\bigcup_{j=1}^i \mathcal{U}_j$  hold rows from  $(\mathbf{0}, \dots, \mathbf{0}, \mathbf{1}, \mathbf{0}, \dots, \mathbf{0}, \overline{M}_i, \mathbf{0}, \dots, \mathbf{0})$ . By Lemma 1,  $\mathcal{M}$  computes the  $(\mathbf{t}, n)$ -conjunctive HTAccS  $\Gamma^\forall$  with a target vector  $(1, \dots, 1, 0, \dots, 0)$  that has  $m$  leading 1-entries. Note that if the secret  $s = s_1 + \dots + s_m$  is shared using a vector  $(s_1, \dots, s_m, \mathbf{r})$ , then the target vector corresponds to  $s$ . Next, it is easy to verify that for Shamir MSPs  $\mathcal{M}_i$ ,

$$\begin{aligned} \mathcal{M} \diamond \mathcal{M} &= (\mathcal{M}_1 \times \dots \times \mathcal{M}_m) \diamond (\mathcal{M}_1 \times \dots \times \mathcal{M}_m) \\ &\equiv (\mathcal{M}_1 \diamond \mathcal{M}_1) \times \dots \times (\mathcal{M}_1 \diamond \mathcal{M}_m) \times \dots \times (\mathcal{M}_m \diamond \mathcal{M}_m), \end{aligned}$$

where  $\mathcal{M}_i \diamond \mathcal{M}_k$  is computed on  $\bigcup_{j=1}^i \mathcal{U}_j$  for  $i \leq k$ . By basic properties of Shamir secret sharing,  $\mathcal{M}_i \diamond \mathcal{M}_k$  computes a  $(t_i + t_k, u_i)$ -threshold access structure. Thus, by Lemma 1,  $\mathcal{M} \diamond \mathcal{M}$  computes a  $(\bar{\mathbf{t}}, n)$ -conjunctive HTAccS  $\bar{\Gamma}^\forall$ , where  $\bar{\mathbf{t}} = (t_1 + t_m, \dots, t_m + t_m)$ . The target vector  $(1, \dots, 1, 0, \dots, 0)$  of  $\mathcal{M} \diamond \mathcal{M}$  has (after suitable reordering of columns)  $m^2$  leading 1-entries and it corresponds to  $ss' = s_1 s'_1 + \dots + s_1 s'_m + \dots + s_m s'_1 + \dots + s_m s'_m$ .

It only remains to show that if  $\bar{\Gamma}^\forall$  is  $\mathcal{Q}_3$ , then the number of honest participants at every level  $\bigcup_{j=1}^i \mathcal{U}_i$ ,  $i \in \{1, \dots, m\}$ , always exceeds the threshold  $t_i + t_m$ . Let  $\mathcal{W} \in \Delta^\exists$  be the set of corrupted participants. Then there must exist an index  $k$  for which  $\mathcal{W}$  does not cross the threshold, i.e.,  $\exists k : |\mathcal{W} \cap \bigcup_{j=1}^k \mathcal{U}_j| \leq t_k$ . Next,

$$\begin{aligned} \forall i \geq k \quad & |(\bigcup_{j=1}^i \mathcal{U}_j) \setminus \mathcal{W}| \geq |(\bigcup_{j=1}^k \mathcal{U}_j) \setminus \mathcal{W}| \geq u_k - t_k > 2t_m \geq t_i + t_m, \\ \forall i < k \quad & |(\bigcup_{j=1}^i \mathcal{U}_j) \setminus \mathcal{W}| \geq u_i - t_k \geq u_i - t_m > t_i + t_m, \end{aligned}$$

where strict inequalities follow from condition (8).  $\square$

## C Allocation of Participant Identities (Theorem 5)

*Proof.* Let  $D$  be the dealer holding the row  $(1, 0, \dots, 0)$  corresponding to the secret. Call a qualified subset  $\mathcal{V}$  minimal if no proper subset  $\mathcal{V}' \subset \mathcal{V}$  is qualified, and call a forbidden subset  $\mathcal{W}$  maximal, if it has size  $|\mathcal{W}| = t_m$  and is missing a single participant to become qualified. We divide the proof into two steps:

*Claim 1.* If for every minimal qualified subset  $\mathcal{V}$  and for every maximal forbidden subset  $\mathcal{W}$ , matrices  $M_{\mathcal{V}}$  and  $M_{\mathcal{W} \cup \{D\}}$  are regular, then the scheme is correct and private.

*Claim 2.* When participant identities are allocated at random, then the probability that all such matrices  $M_{\mathcal{V}}$  and  $M_{\mathcal{W} \cup \{D\}}$  are regular is at least

$$p \geq 1 - \frac{\binom{n+1}{t_m+1} t_m (t_m - 1)}{2(q - t_m - 1)}.$$

*Proof of Claim 1.* If the matrix of every minimal qualified subset  $\mathcal{V}$  is regular, then the scheme is clearly correct. If the matrix  $M_{\mathcal{W} \cup \{D\}}$  of a maximal forbidden subset  $\mathcal{W}$  is regular, then the row  $(1, 0, \dots, 0)$  corresponding to the dealer is independent of the rows of  $\mathcal{W}$  and the linear span of the rows of  $\mathcal{W}$  does not contain the target vector, so  $\mathcal{W}$  can indeed learn nothing about the secret.

Consider now any forbidden set  $\mathcal{W}$  of size  $|\mathcal{W}| > t_m$ . W.l.o.g. we may assume that  $\mathcal{W}$  is missing a single participant from a level  $\mathcal{U}_i$ , i.e.,  $|\mathcal{W} \cap \cup_{j=1}^i \mathcal{U}_j| = t_i$ . Consider the set  $\mathcal{W} \cap \cup_{j=i+1}^m \mathcal{U}_j$ . The rows belonging to participants in these levels begin with at least  $t_i + 1$  leading zeroes, so we may select  $t_m - t_i$  participants whose rows span the same space. Thus, these  $t_m - t_i$  participants together with the  $t_i$  participants from  $\mathcal{W} \cap \cup_{j=1}^i \mathcal{U}_j$  have the same information about the secret as  $\mathcal{W}$ . But the former set is a maximal forbidden subset, so we can repeat the above argument to conclude that they can learn nothing about the secret.

*Proof of Claim 2.* We prove that the probability of a single matrix  $M$  being singular is bounded by  $\Pr[|M| = 0] \leq \frac{t_m(t_m-1)}{2(q-t_m-1)}$ . Since there are altogether at most  $\binom{n}{t_m+1} + \binom{n}{t_m} = \binom{n+1}{t_m+1}$  such matrices, the claim follows.

The proof is by induction on  $t_m$ . Notice that when we delete the last column of the matrix of a  $(\mathbf{t}, n)$ -scheme, the dealer and the participants are holding rows according to a  $(\mathbf{t}', n)$ -scheme, where  $\mathbf{t}' = (t_1, \dots, t_{m-1}, t_m - 1)$ . The matrices are clearly regular for  $t_m = 0$ . Assume now that  $t_m > 0$  and let the rows in the matrix be ordered according to the hierarchy (the dealer having the highest priority). Let  $\mathbf{r}$  be the last row in a matrix  $M$ . There are two cases to consider:

1.  $\mathbf{r} = (0, \dots, 0, 1)$ ;
2.  $\mathbf{r} = (0, \dots, 0, 1, \alpha_u, \dots, \alpha_u^{t_m-t_i-1})$ .

The first case happens when  $t_{m-1} = t_m - 1$ . Clearly, in a minimal qualified subset or a maximal forbidden subset, there can be only one such row. Thus, we can solve for the last unknown  $\alpha_{t_m}$ , delete the last row and the last column of the matrix and conclude by induction that  $\Pr[|M| = 0] \leq \frac{(t_m-1)(t_m-2)}{2(q-t_m)} < \frac{t_m(t_m-1)}{2(q-t_m-1)}$ .

In the second case, we write the determinant of  $M$  as a polynomial in  $\alpha_u$ :

$$|M| = P(\alpha_u) = \sum_{j=0}^{t_m - t_i - 2} c_j \alpha_u^j + \mu \alpha_u^{t_m - t_i - 1} ,$$

where  $c_i$  are some coefficients and  $\mu$  is the determinant of the upper-left  $t_m \times t_m$  minor. Then

$$\Pr[|M| = 0] = \Pr[P(\alpha_u) = 0] \leq \Pr[\mu = 0] + \Pr[P(\alpha_u) = 0 | \mu \neq 0] .$$

In the first case, we can apply the induction argument to conclude that  $\Pr[\mu = 0] \leq \frac{(t_m - 1)(t_m - 2)}{2(q - t_m)}$ . In the second case when  $\mu \neq 0$ ,  $P(\alpha_u)$  vanishes for at most  $t_m - t_i - 1$  of the  $(q - 1) - t_m$  possible values of  $\alpha_u$  (there are  $q - 1$  nonzero elements in  $\mathbb{F}_q$ , and  $t_m$  of them are reserved for other rows of the matrix). Thus  $\Pr[P(\alpha_u) = 0 | \mu \neq 0] \leq \frac{(t_m - t_i - 1)}{(q - 1 - t_m)}$ . If  $i = 0$  ( $t_0 = -1$ ), then all participants belong to the highest level, so the matrix is a Vandermonde matrix and is regular. Thus, the worst case is  $t_i = 0$  and we get

$$\Pr[|M| = 0] = \Pr[P(\alpha_u) = 0] \leq \frac{(t_m - 1)(t_m - 2)}{2(q - t_m)} + \frac{t_m - 1}{q - 1 - t_m} \leq \frac{t_m(t_m - 1)}{2(q - 1 - t_m)} ,$$

completing the induction step.  $\square$

## D Multiplicativity of the Ideal Scheme (Theorem 6)

*Proof.* First, notice that if we multiply each row  $(0, \dots, 0, 1, \alpha_u, \dots, \alpha_u^{t_m - t_i - 1})$  by  $\alpha_u^{t_i + 1}$ , then each column of  $M$  has the form  $(\alpha_1^i, \alpha_2^i, \dots, \alpha_k^i, 0, \dots, 0)^T$  for some  $i$  and  $k$ . It then follows that also each column in  $M \diamond M$  has the same form. We conclude that if lowest-level participants in some set  $\mathcal{V}$  hold rows  $(0, 0, \dots, 1, \alpha_u, \dots, \alpha_u^i, \dots, \alpha_u^i, \dots, \alpha_u^{t_m - t_i - 1})$  in  $M_{\mathcal{V}} \diamond M_{\mathcal{V}}$ , then the two columns containing the  $i$ th powers are linearly dependent in the whole matrix  $M_{\mathcal{V}} \diamond M_{\mathcal{V}}$ . We will use this observation to delete linearly dependent columns in  $M_{\mathcal{V}} \diamond M_{\mathcal{V}}$ .

Assume now that (16) holds and let  $\mathcal{V} = \bigcup_{j=1}^{s-1} \mathcal{U}_{i_j+1}$ . We finish the proof by induction on  $j$ . Let  $j = s - 1$  and let  $i_{s-1}$  be such that  $p_{i_{s-1}+1} > t_{i_s} + t_m - 2(t_{i_{s-1}} + 1) = 2(t_m - t_{i_{s-1}} - 1)$  (recall that  $i_s = m$  by definition).

Each player  $u \in \mathcal{U}_{i_{s-1}+1}$  holds a row  $(0, \dots, 0, 1, \alpha_u, \dots, \alpha_u^{t_m - t_{i_{s-1}} - 1})$  in  $M$  and a row  $(0, \dots, 0, 1, \alpha_u, \dots, \alpha_u^{2(t_m - t_{i_{s-1}} - 1)})$  in  $M \diamond M$ . In particular, since  $\mathcal{U}_{i_{s-1}+1}$  is the lowest level present in  $\mathcal{V}$ , we can delete linearly dependent columns in  $M_{\mathcal{V}} \diamond M_{\mathcal{V}}$  and assume that each power  $\alpha_u^i$  is present only once in the row. But then the block formed by any  $2(t_m - t_{i_{s-1}} - 1) + 1$  participants from the lowest level is a Vandermonde block and its determinant is non-zero.

Let now  $j < s - 1$  and assume that the lower-right minor obtained from the non-zero columns of lower levels in  $\mathcal{V}$  is non-zero. In the original matrix  $M_{\mathcal{V}}$ ,

participant  $u \in \mathcal{U}_{i_j+1}$  and participant  $v \in \mathcal{U}_{i_{j+1}+1}$  hold rows

$$\begin{aligned} & (0, \dots, 0, 1, \alpha_u, \dots, \alpha_u^{t_{i_j+1}-t_{i_j}-1}, \alpha_u^{t_{i_j+1}-t_{i_j}}, \dots, \dots, \alpha_u^{t_m-t_{i_j}-1}) , \\ & (0, \dots, 0, 0, 0, \dots, 0, 1, \alpha_v, \dots, \alpha_v^{t_m-t_{i_j+1}-1}) , \end{aligned}$$

respectively. Thus, in  $M_{\mathcal{V}} \diamond M_{\mathcal{V}}$ , they hold rows

$$\begin{aligned} & (0, \dots, 0, 1, \alpha_u, \dots, \alpha_u^{t_m+t_{i_j+1}-2t_{i_j}-2}, \alpha_u^{2(t_{i_j+1}-t_{i_j})}, \dots, \dots, \alpha_u^{2(t_m-t_{i_j}-1)}) , \\ & (0, \dots, 0, 0, 0, \dots, 0, 1, \alpha_v, \dots, \alpha_v^{2(t_m-t_{i_j+1}-1)}) . \end{aligned}$$

By the induction assumption, the lower-right minor obtained from the  $2(t_m - t_{j+1})$  non-zero columns of lower levels is non-zero. By applying our observation about deleting linearly dependent columns on the upper-left minor, we see that the next block on the diagonal contains rows  $(1, \alpha_u, \dots, \alpha_u^{t_m+t_{i_j+1}-2t_{i_j}-2})$ . Since the number of participants at level  $\mathcal{U}_{i_j+1}$  is indeed  $p_{i_j+1} > t_{i_j+1} + t_m - 2(t_{i_j} + 1)$ , we obtain another Vandermonde block. This completes the induction step.  $\square$

**Example.** Consider a  $((1, 2, 4), n)$ -scheme. For a set  $\mathcal{V}$  with 6 participants from level  $\mathcal{U}_1$  and 5 participants from level  $\mathcal{U}_2$ , we get

$$M_{\mathcal{V}} \diamond M_{\mathcal{V}} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 & \alpha_1^4 & \alpha_1^5 & \alpha_1^4 & \alpha_1^5 & \alpha_1^6 & \alpha_1^7 & \alpha_1^8 \\ \vdots & & & & & & & & & & \\ 1 & \alpha_6 & \alpha_6^2 & \alpha_6^3 & \alpha_6^4 & \alpha_6^5 & \alpha_6^4 & \alpha_6^5 & \alpha_6^6 & \alpha_6^7 & \alpha_6^8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha_7 & \alpha_7^2 & \alpha_7^3 & \alpha_7^4 \\ \vdots & & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha_{11} & \alpha_{11}^2 & \alpha_{11}^3 & \alpha_{11}^4 \end{pmatrix} ,$$

so the determinant is the product of two Vandermonde determinants and the set  $\mathcal{V}$  is allowed. In comparison, if we were using the original Tassa scheme, we would have

$$M_{\mathcal{V}} \diamond M_{\mathcal{V}} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 & \alpha_1^4 & \alpha_1^5 & \alpha_1^4 & \alpha_1^5 & \alpha_1^6 & \alpha_1^6 & \alpha_1^7 & \alpha_1^8 \\ \vdots & & & & & & & & & & & \\ 1 & \alpha_6 & \alpha_6^2 & \alpha_6^3 & \alpha_6^4 & \alpha_6^5 & \alpha_6^4 & \alpha_6^5 & \alpha_6^6 & \alpha_6^6 & \alpha_6^7 & \alpha_6^8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 12\alpha_7 & 24\alpha_7^2 & 36\alpha_7^2 & 72\alpha_7^3 & 144\alpha_7^4 \\ \vdots & & & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 12\alpha_{11} & 24\alpha_{11}^2 & 36\alpha_{11}^2 & 72\alpha_{11}^3 & 144\alpha_{11}^4 \end{pmatrix} .$$

It is easy to verify that the determinant of the matrix formed by the last 11 columns of  $M_{\mathcal{V}} \diamond M_{\mathcal{V}}$  is non-zero, so the set  $\mathcal{V}$  is forbidden in the original scheme. In general, by modifying the scheme, we introduce new linear dependencies in the columns of  $M \diamond M$  and thus improve the multiplicative properties.