Compounding Secret Sharing Schemes

E. Martínez-Moro, J. Mozo-Fernández and C. Munuera [1]
Departamento de Matemática Aplicada Fundamental
University of Valladolid,
47014 Valladolid, Castilla, Spain
E-mail: edgar.martinez@ieee.org, jmozo@maf. uva.es,
cmunuera@modulor.arq.uva.es

Version: April 1, 2002

In this paper we introduce the class of composite access structures for secret sharing. We also provide secret sharing schemes realizing these structures and study their information rates. As a particular case of this construction, we present the subclass of iterated threshold schemes, a large class of ideal secret sharing schemes.

Key Words: Cryptography, Secret sharing schemes, Threshold schemes.
Subject Classification: (MSC 2000) 94A60

1. INTRODUCTION

Secret sharing schemes are methods for distributing a *secret* K among a set $\mathcal{P}$ of participants. Each participant receives a piece of the secret, or *share*, in such a way that only specified subsets of $\mathcal{P}$ are able to reconstruct the secret by pooling their shares. If non-allowed coalitions cannot obtain any information about the secret then the scheme is said to be *perfect*.

The family of qualified subsets $\Gamma \subseteq 2^{\mathcal{P}}$ is called the *access structure* of the scheme. It is considered to be *monotone*, that is, if $A \subseteq B \subseteq \mathcal{P}$ and $A \in \Gamma$, then also $B \in \Gamma$. Thus the set of minimal elements in Γ, denoted Γ^m, determines the whole structure Γ and it is called the *basis* of Γ.

One of the basic parameters of a secret sharing scheme Σ is its *information rate*, which is the rate between the length (in bits) of the secret and the maximum length of the shares of the participants:

$$\rho(\Sigma,\Gamma,\mathcal{K}) = \rho(\Sigma) = \frac{\log_2|\mathcal{K}|}{\max_{\mathcal{P}}(\log_2|\mathcal{S}(P)|)}.$$

Here $\mathcal{K}$ is the set of all possible secrets for Σ and $\mathcal{S}(P)$ is the set of all possible shares for $P \in \mathcal{P}$. A scheme Σ is called *ideal* if $\rho(\Sigma) = 1$ (notice that always $\rho(\Sigma) \leq 1$). An access structure Γ is called *ideal* if there is an ideal scheme realizing it. More generally we define the *optimal information rate* of the structure Γ as

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

where the supremum is taken over all possible Σ and $\mathcal{K}$ for Γ.

[1]First and third authors research are partially supported by the "Junta de Castilla y León" under Projet VA020/02 and by MCyT under project BFM2001-2251. Second author partially supported by the "Junta de Castilla y León" under Projet VA56/00B.

The problems of characterizing ideal access structures and finding ideal schemes for them are important and they have received great attention in the literature (see for example [3, 4]).

A particular interesting class of secret sharing schemes is the class of *threshold schemes*, which were the first secret sharing schemes introduced independently by Blakley [1] and Shamir [8] in 1979. The access structure of a (t, n)-threshold scheme consists of all subsets of $\mathcal{P}$ with at least t out of n participants. Threshold schemes are ideal and admit a vector space construction (see section 3). In what follows, for short we shall denote a (t, n)-threshold scheme simply by (t, n).

In the case of threshold schemes all the participants have the same opportunity for acceding to the secret. This property does not hold for general access structures: some participants have a great chance than others. This difference among participants is not unsuitable in practice. On the contrary, it can be useful as it reflects that usually in real life participants are, in a natural way, in a hierarchy and not on equal terms. Then, structures in which participants are divided in several classes abound in the literature: Simmons' multilevel/multipart schemes, [9], sums and products, bipartite structures, [7], compartmented schemes, [2], etc. In this paper we present a very general construction of this type. Participants are divided in several groups, each of them having its own family of authorized coalitions. As a particular case of this construction we introduce the class of *iterated threshold schemes*. We show that all schemes in this class are ideal and admit a vector space construction. We also show that many ideal schemes (all ideal schemes in the case of 4 participants and most ideal schemes in the case of 5 participants) in fact belong to this class.

The organization of the paper is as follows: composite access structures are defined in section 2, where some of their main properties are also stated. In section 3 we show how to construct secret sharing schemes for these structures. Section 4 is devoted to study of a particular type of composite structures, the so-called *class-reducible* structures. Finally, in section 5 we study the particular interesting case in which all the structures involved are either threshold or composition of threshold structures.

2. COMPOSITION OF ACCESS STRUCTURES

Let $\mathcal{P}$ be a set of participants and let $\mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_r$, $(r > 1)$ be a partition of $\mathcal{P}$ (that is $\emptyset \neq \mathcal{P}_i \neq \mathcal{P}$ and $\mathcal{P}_i \cap \mathcal{P}_j = \emptyset$ if $i \neq j$). Let us write $\mathcal{P}_i = \{P_1^{(i)}, \ldots, P_{n_i}^{(i)}\}$ and $n = n_1 + \cdots + n_r$. For a set $A \subseteq \mathcal{P}$ we denote $A_i = A \cap \mathcal{P}_i$. Obviously $A = A_1 \cup \cdots \cup A_r$. For $i = 1, \ldots, r$, let Γ_i be an access structure on $\mathcal{P}_i$, and let Γ_0 an access structure on the participant set $\overline{\mathcal{P}} = \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$.

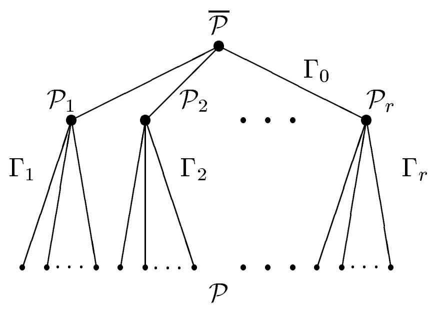
DEFINITION 1. With the notation as above, we define the **composite access structure** of $\Gamma_1, \Gamma_2, \ldots, \Gamma_r$, **following** Γ_0, denoted $\Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r]$, as

$$\begin{aligned}\Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r] &= \{A \subseteq \mathcal{P} \mid \exists B \in \Gamma_0 \text{ such that } A_i \in \Gamma_i \text{ for all } \mathcal{P}_i \in B\} \\ &= \bigcup_{B \in \Gamma_0} \{A \subseteq \mathcal{P} \mid A_i \in \Gamma_i \text{ for all } \mathcal{P}_i \in B\}.\end{aligned}$$

That is, each of the sets $\mathcal{P}_i$ plays the role of a participant for Γ_0. A coalition $A \subseteq \mathcal{P}$ is authorized if and only if it includes, as subsets, authorized coalitions in enough of the components $\Gamma_1, \Gamma_2, \ldots, \Gamma_r$ to constitute an authorized subset for Γ_0.

We have a pictorial representation of the scheme as given in Figure 1.

FIG. 1 Pictorial representation of composite structures



Composite secret sharing schemes can be useful for sharing secrets when the set of participants is divided into several groups, each of them with its own family of authorized coalitions. The relation among these groups is given by the structure Γ_0. It is not so difficult to imagine a situation requiring a model of this type.

EXAMPLE 1.

(a) Sums and products. Two typical compositions of access structures are sums and products, defined as follows: given a partition $\mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_r$, and access structures $\Gamma_1, \ldots, \Gamma_r$, the *sum* of $\Gamma_1, \ldots, \Gamma_r$ is

$$\Gamma_1 + \cdots + \Gamma_r = \{A \subseteq \mathcal{P} \mid A_i \in \Gamma_i \text{ for some } i\}$$

and the *product*

$$\Gamma_1 \times \cdots \times \Gamma_r = \{A \subseteq \mathcal{P} \mid A_i \in \Gamma_i \text{ for all } i\}.$$

Since $\Gamma_1 + \cdots + \Gamma_r = (1,r)[\Gamma_1, \ldots, \Gamma_r]$ and $\Gamma_1 \times \cdots \times \Gamma_r = (r,r)[\Gamma_1, \ldots, \Gamma_r]$, both are particular cases of our construction.

(b) Insertions. Let Γ_1, Γ_2 be two structures defined on the sets $\mathcal{P}_1$ and $\mathcal{P}_2$, and let $P \in \mathcal{P}_1$. The *insertion* of Γ_2 at P in Γ_1, denoted $\Gamma_1(P \mapsto \Gamma_2)$, is defined to be the structure on the set $\mathcal{P}_1 \setminus \{P\} \cup \mathcal{P}_2$ such that for $A \subseteq (\mathcal{P}_1 \setminus \{P\}) \cup \mathcal{P}_2$, we have $A \in \Gamma_1(P \mapsto \Gamma_2)$ if and only if $A \cap \mathcal{P}_1 \in \Gamma_1$, or $(A \cap \mathcal{P}_1) \cup \{P\} \in \Gamma_1$ and $A \cap \mathcal{P}_2 \in \Gamma_2$ (see Martin [6]). It is clear that $\Gamma_1(P_1 \mapsto \Gamma_2) = \Gamma_1[\Gamma_2, (1,1), \ldots, (1,1)]$.

Let us see some first properties of composite structures.

PROPOSITION 1. $(\Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r])^m = \Gamma_0^m[\Gamma_1^m, \Gamma_2^m, \ldots, \Gamma_r^m]$.

Proof. Let $\Gamma = \Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r]$ and $A \in \Gamma^m$. Let $C = \{\mathcal{P}_i \mid A_i \in \Gamma_i, i \neq 0\} \in \Gamma_0$. Let us assume that $C \notin {\Gamma_0}^m$. Then there exists $C' \in {\Gamma_0}^m$ such that $C' \subsetneq C$. Let us consider the set

$$A' = A \cap \bigcup_{\mathcal{P}_i \in C'} \mathcal{P}_i.$$

Then $A' \subset A$ and $A' \in \Gamma^m$ which contradicts the fact $A \in \Gamma^m$. Hence $C \in {\Gamma_0}^m$. Let fix i such that $\mathcal{P}_i \in C$ and let us suppose $A_i \notin \Gamma_i^m$. Then there exists $A_i' \subsetneq A_i$ such that $A_i' \in \Gamma_i^m$. Let $D = A_i \setminus A_i' \subset \mathcal{P}_i$. Then $A \setminus D \subset A$ and, since the $\mathcal{P}_i$'s are a partition on $\mathcal{P}$, $A \setminus D \in \Gamma^m$. This contradicts that $A \in \Gamma^m$. Thus we have $\Gamma^m \subseteq \Gamma_0^m[\Gamma_1^m, \Gamma_2^m, \ldots, \Gamma_r^m]$. The other inclusion is straightforward. ∎

Next we shall show that composition behaves well by duality. Let us remember that for a given access structure Γ on $\mathcal{P}$, the *dual* structure of Γ is defined as the set of coalitions whose complement is not authorized,

$$\Gamma^\star = \{A \subseteq \mathcal{P} \mid \mathcal{P} \setminus A \notin \Gamma\}.$$

PROPOSITION 2. $(\Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r])^\star = \Gamma_0^\star[\Gamma_1^\star, \Gamma_2^\star, \ldots, \Gamma_r^\star]$.

Proof. Let $\Gamma = \Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r]$, $\tilde{\Gamma} = \Gamma_0^\star[\Gamma_1^\star, \Gamma_2^\star, \ldots, \Gamma_r^\star]$ and let $A \in \tilde{\Gamma}$. There is $B \in \Gamma_0^\star$ such that if $\mathcal{P}_i \in B$ then $A_i \in \Gamma_i^\star$ $(i \neq 0)$. By definition, for this B, if $\mathcal{P}_i \in B$ then $\mathcal{P}_i \setminus A_i \notin \Gamma_i$, $i \neq 0$. If $A \notin \Gamma^\star$ then $\mathcal{P} \setminus A \in \Gamma$. This means that there exists $B' \in \Gamma_0$ such that if $\mathcal{P}_i \in B'$ then $(\mathcal{P} \setminus A) \cap \mathcal{P}_i = \mathcal{P}_i \setminus A_i \in \Gamma_i$ for $i \neq 0$. Hence $B \cap B' = \emptyset$ and so $B' \subseteq \overline{\mathcal{P}} \setminus B$ and $\overline{\mathcal{P}} \setminus B \in \Gamma_0$. We arrive to a contradiction, and therefore $\tilde{\Gamma} \subseteq \Gamma^\star$.

Conversely, consider now $A \in \Gamma^\star$, that is, $\mathcal{P} \setminus A \notin \Gamma$. By definition, for every $B \in \Gamma_0$ there exists $\mathcal{P}_i \in B$ such that $\mathcal{P}_i \setminus A_i \notin \Gamma_i$. If $A \notin \tilde{\Gamma}$ then for every $B' \in \Gamma_0^\star$ there exists $\mathcal{P}_i \in B'$ such that $\mathcal{P}_i \setminus A_i \in \Gamma_i$. Let $\Gamma_0^m = \{B_j\}_{j \in J}$ be the basis of Γ_0. For each $j \in J$ there exists $\mathcal{P}_{i_j} \in B_j$ such that $\mathcal{P}_{i_j} \setminus A_{i_j} \notin \Gamma_i$. Let $B' = \{\mathcal{P}_{i_j}\}_{j \in J}$. Then B_j is not contained in $\overline{\mathcal{P}} \setminus B'$ because $B' \cap B_j \neq \emptyset$ for all $j \in J$. Therefore, $B' \in \Gamma_0^\star$. On the other hand, for all $\mathcal{P}_i \in B'$ we have $\mathcal{P}_i \setminus A_i \notin \Gamma_i$ which is a contradiction. Hence $\tilde{\Gamma} \supseteq \Gamma^\star$. ∎

From this result, in particular we have that the dual of the sum is the product of the duals, and the dual of the product is the sum of the duals.

COROLLARY 1. *The dual of a composite access structure is also a composite access structure.*

Obviously, every structure Γ can be expressed as a composition in the ways $\Gamma = \Gamma[(1,1), \cdots, (1,1)]$ and $\Gamma = (1,1)[\Gamma]$. These compositions are called *trivial*. We shall not consider trivial compositions any more. A structure that cannot be expressed as a nontrivial composition is called *indecomposable*. For example, it is easy to see that threshold access structures (t, n) are indecomposable whenever $1 < t < n$.

On the other hand, the expression $\Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r]$ of a structure as a composition is in general not unique, because the Γ_i, $i = 1, \ldots, r$, can be, themselves, decomposable. We have the following result.

PROPOSITION 3. *Let* $\Gamma = \Gamma_0[\Gamma_1, \Gamma_2, \cdots, \Gamma_r]$. *Assume that for* $i = 1, \ldots, r$, *we have* $\Gamma_i = \Delta_0^{(i)}[\Delta_1^{(i)}, \Delta_2^{(i)}, \ldots, \Delta_{j_i}^{(i)}]$. *Then*

$$\begin{aligned} \Gamma &= \Gamma_0[\Delta_0^{(1)}[\Delta_1^{(1)}, \Delta_2^{(1)}, \ldots, \Delta_{j_1}^{(1)}], \ldots, \Delta_0^{(r)}[\Delta_1^{(r)}, \Delta_2^{(r)}, \ldots, \Delta_{j_r}^{(r)}]] \\ &= (\Gamma_0[\Delta_0^{(1)}, \Delta_0^{(2)}, \ldots, \Delta_0^{(r)}])\,[\Delta_1^{(1)}, \ldots, \Delta_{j_1}^{(1)}, \ldots, \Delta_1^{(r)}, \ldots, \Delta_{j_r}^{(r)}]. \end{aligned}$$

The proof is straightforward. The iterative application of this result yields the following corollary.

COROLLARY 2. *Let* Γ *be a decomposable structure. Then* Γ *can be written as* $\Gamma = \Gamma_0[\Gamma_1, \ldots, \Gamma_r]$ *where all the structures* $\Gamma_1, \ldots, \Gamma_r$ *are indecomposable.*

3. COMPOSITE SCHEMES FOR COMPOSITE STRUCTURES

Let $\Gamma = \Gamma_0[\Gamma_1, \ldots, \Gamma_r]$ be a composite access structure on $\mathcal{P}$. In order to construct a secret sharing scheme for Γ, we can compose secret sharing schemes for each Γ_i, $i = 0, \ldots, r$. Following Martin, [6], if the set $\mathcal{K}$ of secrets to share has cardinality q, then a perfect secret sharing scheme for Γ will be denoted $PS(\Gamma, q)$. Let us remember that for a participant $P \in \mathcal{P}$, $\mathcal{S}(P)$ denotes the set of all possible shares for P, and that the insertion schemes were introduced in Example 1. The following result can be found in [6].

THEOREM 1. *Let Γ_1, Γ_2 be access structures defined on participant sets $\mathcal{P}_1$ and $\mathcal{P}_2$, and let $P \in \mathcal{P}_1$. If there is a $PS(\Gamma_1, q)$ and a $PS(\Gamma_2, |\mathcal{S}(P)|)$, then there exist a $PS(\Gamma_1(P \mapsto \Gamma_2), q)$.*

Let $\Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_r]$. It is clear that Γ can be obtained from Γ_0 after r insertions at the participants $\mathcal{P}_1, \ldots, \mathcal{P}_r$. Thus, the above Theorem can be generalized to the following.

PROPOSITION 4. *Let $\Gamma = \Gamma_0[\Gamma_1, \ldots, \Gamma_r]$ be as above. If there exist a $PS(\Gamma_0, q)$ and for $i = 1, \ldots, r$, a $PS(\Gamma_i, |\mathcal{S}(P_i)|)$, then there exists a $PS(\Gamma, q)$.*

The proof is obvious from Theorem 1. Furthermore, since the proof of the Theorem in [6] is constructive, we can effectively give the $PS(\Gamma, q)$. For the convenience of the reader let us present the idea of this construction: we want to share $K \in \mathcal{K}$ among the participants in $\mathcal{P}$. By using the $PS(\Gamma_0, q)$ we compute the shares $s_1, \ldots, s_r$ of $\mathcal{P}_1, \cdots, \mathcal{P}_r$. Now, by using the $PS(\Gamma_i, |\mathcal{S}(P_i)|)$ we share each s_i among the participants in $\mathcal{P}_i$: $s_1^{(i)}, \cdots, s_{n_i}^{(i)}$. Then the shares given by $PS(\Gamma, q)$ are $s_1^{(1)}, \ldots, s_{n_1}^{(1)}, \ldots, s_1^{(r)}, \ldots, s_{n_r}^{(r)}$.

By studying the proof of the Theorem, we also conclude the following.

COROLLARY 3. *Let $\Gamma = \Gamma_0[\Gamma_1, \cdots, \Gamma_r]$. With the notations above, we have*

$$\rho(PS(\Gamma, q)) = \min\{\rho(PS(\Gamma_0, q)) \cdot \rho(PS(\Gamma_i, |\mathcal{S}(P_i)|)) \mid 1 \leq i \leq r\}.$$

Thus $\rho^*(\Gamma) \geq \min\{\rho^*(\Gamma_0) \cdot \rho^*(\Gamma_i) \mid 1 \leq i \leq r\}$.

In particular, if all the structures Γ_i, $i = 0, \ldots, r$, are ideal, then Γ is ideal.

A particular interesting kind of access structures is formed by those admitting a *Brickell's vector space construction*. Let us remember that a structure Γ on $\mathcal{P}$ admits a vector space construction over the finite field $\mathbb{F}_p$ if there is a map $\Phi : \mathcal{P} \longrightarrow \mathbb{F}_p^d$ (d large enough) and a vector $\vec{v} \in \mathbb{F}_p^d$, $\vec{v} \neq \vec{0}$, such that for all $A \subseteq \mathcal{P}$ we have $\vec{v} \in \langle \Phi(P_i) \mid P_i \in A \rangle$ if and only if $A \in \Gamma$ (see [2, 11]). Such a construction directly provides an ideal $PS(\Gamma, p)$. Unfortunately no criteria is known to decide when a structure Γ admits a vector space construction.

In the above construction usually one takes $\vec{v} = \vec{e_1} = (1, 0, \ldots, 0)$. However it is clear that the particular choice of $\vec{v}$ is not relevant whenever $\vec{v} \neq 0$.

It is well known that every (t, n)-threshold scheme admits a vector space construction. Just take n different non-zero elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$ and define

$$\Phi(P_i) = (1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{t-1}) \in \mathbb{F}_p^t$$

for all $i, 1 \leq i \leq n$.

It is not clear when the composition of structures admitting a vector space constructions admits a vector space construction. At the moment we simply state the following result.

PROPOSITION 5. *Let $\Gamma = \Gamma_0[\Gamma_1, \Gamma_2, \cdots, \Gamma_r]$ be a composite access structure such that Γ_i is a (t_i, n_i)-threshold structure for $1 \leq i \leq r$. If Γ_0 admits a vector space construction, then also Γ admits a vector space construction.*

Proof. For $1 \leq i \leq r$, we shall consider the map $\Phi_i : \mathcal{P}_i \longrightarrow \mathbb{F}_p^{t_i}$ defined by

$$\Phi_i(P_j^{(i)}) = (1, \alpha_{ij}, \alpha_{ij}^2, \ldots, \alpha_{ij}^{t_i - 1})$$

where $\mathcal{P}_i = \{P_1^{(i)}, \ldots, P_{n_i}^{(i)}\}$. For Γ_0 we have a map $\Phi_0 : \{\mathcal{P}_1, \ldots, \mathcal{P}_r\} \longrightarrow \mathbb{F}_p^d$ that defines its vector space construction. Consider the maps $\Psi_i : \mathcal{P}_i \longrightarrow \mathbb{F}_p^{t_i - 1}$,

$$\Psi_i(P_j^{(i)}) = (\alpha_{ij}, \alpha_{ij}^2, \ldots, \alpha_{ij}^{t_i - 1})$$

and let $\Phi_i : \longrightarrow \mathbb{F}_p^{d + t_1 + \cdots + t_r - r}$ defined by

$$\Phi(P_j^{(i)}) = (\Phi_0(\mathcal{P}_i), \vec{0}, \cdots, \Psi_i(P_j^{(i)}), \ldots, \vec{0}).$$

Let us show that Φ is a vector space construction for Γ. If $A \in \Gamma$, let $B = \{\mathcal{P}_i \mid A \cap \mathcal{P}_i \in \Gamma_i\}$ be an element of Γ_0. If $\mathcal{P}_i \in B$, take $\{P_{j_1}^{(i)}, \cdots, P_{j_{t_i}}^{(i)}\}$, t_i different elements of $A \cap \mathcal{P}_i$. There exists a linear combination in $\mathbb{F}_p^{t_i}$

$$\overrightarrow{e_1} = \sum_{k=1}^{t_i} \lambda_k \cdot \Phi_i(P_{j_k}^{(i)})$$

such that $\sum_{k=1}^{t_i} \lambda_k = 1$. Then we have

$$\sum_{k=1}^{t_i} \lambda_k \cdot \Phi(P_{j_k}^{(i)}) = (\Phi_0(\mathcal{P}_i), \vec{0}, \ldots, \vec{0}).$$

As $\overrightarrow{e_1} \in \langle \Phi_0(B) \rangle$, it follows that $\overrightarrow{e_1} \in \langle \Phi(A) \rangle$. Conversely, let $A \subseteq \mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_r$ be such that $\overrightarrow{e_1} \in \langle \Phi(A) \rangle$. Assume that all the coefficients in the linear combination that gives $\overrightarrow{e_1}$ are non-zero. Take $A_i = A \cap \mathcal{P}_i$. If $A_i \neq \emptyset$, then $\Psi_i(A_i)$ is a set of linearly dependent vectors. Thus there exist a linear combination

$$\overrightarrow{0} = \sum_j \lambda_{ij} \cdot \Psi_i(P_j^{(i)})$$

with every $\lambda_{ij} \neq 0$. This means that $t_i \leq |A_i|$, and hence the vectors $\Phi_i(P_j^{(i)})$ span $\overrightarrow{e_1}$. So $A_i \in \Gamma_i$. Moreover $\overrightarrow{e_1}$ must be generated by $B = \{\Phi_0(\mathcal{P}_i) \mid A_i \neq \emptyset\}$ and then $B \in \Gamma_0$. This ends the proof. ∎

Let us note that the above proof is constructive. Thus, if we have a scheme for Γ_0, then we can effectively construct a secret sharing scheme for Γ.

4. REDUCIBLE STRUCTURES

In this section we briefly study a type of decomposable structures which will be useful for us in the sequel.

DEFINITION 2. Let Γ be an access structure on the set of participants $\mathcal{P}$. We say that two participants P_i, P_j are *related*, denoted $P_i \sim P_j$, if for every $A \in \Gamma^m$ we have:
a) if $P_i \in A$ then $(A \setminus \{P_i\}) \cup P_j \in \Gamma$; and conversely
b) if $P_j \in A$ then $(A \setminus \{P_j\}) \cup P_i \in \Gamma$.

Let us note that $\sim$ is an equivalence relation on $\mathcal{P}$. We say that the structure Γ admits a *class reduction* (or shortly that it is *reducible*) if at least one of the equivalence classes of $\sim$ has more than one participant. In this case, the class reduction allows us to define a new access structure on the set of participants $\mathcal{P}_\sim = \mathcal{P}/\sim$ given by $\Gamma_\sim = \Gamma/\sim$.

Remark 1. If two participants P_i, P_j are related, then the set $\{P_i, P_j\}$ cannot be extended to a minimal coalition $A \in \Gamma$. In fact, if $A = \{P_i, P_j\} \cup B \in \Gamma^m$ then, by definition, $\{P_i, P_j\} \cup B = \{P_i\} \cup B \in \Gamma^m$, which contradicts the fact of A being minimal. Conversely, if $P_i \sim P_j$ it is easy to see that $\{P_i, P_j\} \subseteq A$ for all $A \in \Gamma^\star$ such that $P_i \in A$ or $P_j \in A$.

The relationship between reducibility and decomposability is given by the following result.

PROPOSITION 6. *Let $\mathcal{P} = \{P_1, \cdots, P_n\}$. For every equivalence class $[P] \in \mathcal{P}_\sim$, fix a representative $Q \in [P]$ so that $\mathcal{P}_\sim = \{Q_1, \ldots, Q_r\}$. If $n_i = |[Q_i]|$, then*

$$\Gamma = \Gamma_\sim[(1, n_1), (1, n_2), \ldots, (1, n_r)].$$

In particular, all reducible structures on $n \geq 3$ participants are decomposable.

Proof. It is a direct consequence of Proposition 1, the definition of related participants and the above Remark. ∎

The converse of Proposition 6 is not true in general, that is, there exist decomposable structures which are irreducible.

The structures Γ and $\Gamma_\sim$ have similar properties. Let us see some of them. To that end we shall use the following notation: for a participant P_i, we shall denote by $[P_i]$ its equivalence class in $\mathcal{P}_\sim$ and by $\Sigma(P_i)$ its share given by the secret sharing scheme Σ that realizes Γ.

LEMMA 1. *Let Γ be an access structure on the set $\mathcal{P}$. There is a secret sharing scheme Σ realizing Γ, such that:*
a) $\rho(\Sigma) = \rho^*(\Gamma)$; and
b) if $P_i \sim P_j$ then $\Sigma(P_i) = \Sigma(P_j)$.

Proof. Keeping the notations as above, for every equivalence class $[P] \in \mathcal{P}_\sim$, fix a representative $Q \in [P]$ so that $\mathcal{P}_\sim = \{Q_1, \cdots, Q_r\}$. Let Σ' be a secret sharing scheme that realizes Γ and such that $\rho(\Sigma') = \rho^*(\Gamma)$. We define $\Sigma(P_1), \cdots, \Sigma(P_n)$, as $\Sigma(P_i) = \Sigma'(Q_j)$ if $[P_i] = [Q_j]$. Let us consider the projection map $\pi : \mathcal{P} \to \mathcal{P}_\sim$, $\pi(P_i) = Q_j$ if $[P_i] = [Q_j]$. If $A \in \Gamma^m$ then A does not contain related participants, hence $\pi(A) \in \Gamma^m$. Furthermore the shares given by Σ to the participants in A are the same as the shares given by Σ' to the participants in $\pi(A)$. Thus Σ is a sharing scheme realizing Γ. Clearly Σ verifies b). Moreover $\rho(\Sigma) \leq \rho(\Sigma')$ hence we get equality here because $\rho(\Sigma') = \rho^*(\Gamma)$. ∎

Remark 2. The above Lemma show the following nice characterization of related participants: Let Γ be an access structure on $\mathcal{P}$; two participants, P_i and P_j, are related if and only if there is a secret sharing scheme Σ realizing Γ such that $\Sigma(P_i) = \Sigma(P_j)$.

A secret sharing scheme is said to be *regular* if it is optimal and gives equal shares to related participants. From Proposition 6 and Lemma 1, given an access structure Γ, there is a one-to-one correspondence between regular sharing schemes realizing Γ and optimal sharing schemes realizing $\Gamma_\sim$.

PROPOSITION 7. *Let Γ be an access structure on the set $\mathcal{P}$. Then*
a) $\rho^*(\Gamma) = \rho^*(\Gamma_\sim)$.
b) Γ *admits a vector space construction iff* $\Gamma_\sim$ *admits a vector space construction.*

Proof. a) Let Σ be a regular secret sharing scheme for Γ. Then we define a secret sharing scheme on $\mathcal{P}_\sim$ as

$$\Sigma_\sim([P_i]) = \Sigma(P_i),\ i = 1, \dots, n.$$

$\Sigma_\sim$ is well defined, realizes $\Gamma_\sim$ and, obviously, has the same information rate as Σ. Conversely, for a secret sharing scheme Π realizing $\Gamma_\sim$, we define the scheme $\Pi^\sim$ on $\mathcal{P}$ as

$$\Pi^\sim(P_i) = \Pi([P_i]),\ i = 1, \dots, n.$$

In the same way, $\Pi^\sim$ realizes Γ and has the same information rate as Π. Then $\rho^*(\Gamma) = \rho^*(\Gamma_\sim)$. The same argument proves b). (Furthermore, note that one implication also follows from Proposition 5). ∎

5. ITERATED THRESHOLD SCHEMES

In this section we introduce an interesting class of composite secret sharing schemes. This class is formed by composing threshold schemes or compositions of threshold schemes. More formally, we define the class of *iterated threshold access structures* as the smallest class $\mathcal{C}$ of access structures such that:

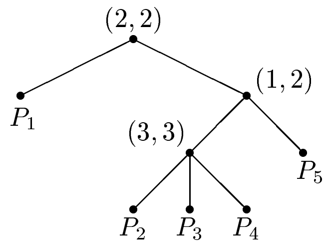
1. All threshold access structures are in $\mathcal{C}$.
2. The composition of elements in $\mathcal{C}$ is also in $\mathcal{C}$; that is, if $\Gamma_0, \Gamma_1, \cdots, \Gamma_r \in \mathcal{C}$, then $\Gamma_0[\Gamma_1, \Gamma_2, \dots, \Gamma_r] \in \mathcal{C}$ (when this composition makes sense).

Schemes realizing iterated threshold access structures are called *iterated threshold schemes*. As we shall see below, iterated threshold schemes can be also found by composition of threshold schemes.

As composite structures, iterated threshold access structures have a pictorial representation. In this case they can also be represented as labeled trees in the obvious way. For example consider the structure on a set of 5 participants given by $\Gamma^m = \{P_1P_2P_3P_4, P_1P_5\}$. It can also be realized as the labeled tree shown in Figure 2, where as usual (t, n) means a t-threshold scheme on n participants. We will denote this iterated threshold scheme as $(2,2)[(1,1),(1,2)[(3,3),(1,1)]]$. Observe that this representation is not unique. For example the schemes $(2,2)[(2,2),(1,2)[(2,2),(1,1)]]$ and $(3,3)[(1,1),(1,1), (1,2)[(2,2),(1,1)]]$ realize the same structure. In general we have $(j,j)[(t,t),\Delta] = (j+t-1, j+t-1)[(1,1), \cdots_{(t)}, (1,1), \Delta]$ and $(1,j)[(1,t),\Delta] = (1, j+t-1)[(1,1), \cdots_{(t)}, (1,1), \Delta]$.

Iterated threshold schemes have some nice properties. Let us study some of them.

FIG. 2 Labeled tree for an iterated access structure.



PROPOSITION 8. *The dual of an iterated threshold access structure is an iterated threshold access structure.*

Proof. It follows from Proposition 2 and the fact that the dual of a threshold access structure is also a threshold access structure. ∎

PROPOSITION 9. *Every iterated threshold access structure admits a vector space construction. In particular every iterated threshold access structure is ideal.*

Proof. It suffices to prove the first fact. Let $\Gamma = \Gamma_0[\Gamma_1, \ldots, \Gamma_r]$ be an iterated threshold access structure. According to Corollary 2, Γ admits a representation $\Gamma_0^{(1)}[\Gamma_1^{(1)}, \cdots, \Gamma_{r_1}^{(1)}]$, where $\Gamma_1^{(1)}, \cdots, \Gamma_{r_1}^{(1)}$ are indecomposable, and hence threshold access structures. Then, according to Proposition 5, it suffices to prove that $\Gamma_0^{(1)}$ admits a vector space construction. But $\Gamma_0^{(1)}$ is again an iterated threshold access structure. Thus we can apply again the above argument to $\Gamma_0^{(1)}$. By iterating this reasoning a number of times, we shall arrive to an expression $\Gamma_0^{(m-1)} = \Gamma_0^{(m)}[\Gamma_1^{(m)}, \cdots, \Gamma_{r_m}^{(m)}]$, where $\Gamma_1^{(m)}, \cdots, \Gamma_{r_m}^{(m)}$ are threshold access structures and $\Gamma_0^{(m)}$ is an indecomposable iterated threshold access structures, that is, also a threshold access structure. Since (classical) threshold structures admit a vector space construction (as the one seen in section 3) then, according to Proposition 5, $\Gamma_0^{(m-1)}$ also admits a vector space construction, and so, the same happens for Γ. ∎

Let us note that, as in the case of Proposition 5, the above proof is constructive. Thus, we can effectively give vector space constructions for all iterated threshold schemes.

Many ideal secret sharing schemes (all of them admitting a vector space construction) are in fact iterated threshold schemes. These include all ideal schemes on participant set with $n \leq 4$ participants and most ideal schemes on $n = 5$ participants. To see this we shall use the results developed in section 4.

PROPOSITION 10. *Let Γ be an access structure on the set $\mathcal{P}$. If $\Gamma_\sim$ is an iterated threshold access structure, then Γ is also an iterated threshold access structure.*

Proof. It is a direct consequence of 6. ∎

Remark 3. Let Γ be an access structure. If $\Gamma^\star$ is class reducible and it reduces to an iterated threshold structure, then, in light of Propositions 8 and 10, we have that Γ is also an iterated threshold structure.

TABLE 1
Ideal access structures on at most 4 participants.

n	Γ^m	Realization	Dual
1	1	1	selfdual
2	12	(2,2)	(1,2)
3	123	(3,3)	(1,3)
	12,23	(2,2)[(1,2),1]	(1,2)[(2,2),1]
	12,23,13	(2,3)	selfdual
4	12,13,14	(2,2)[1,(1,3)]	(1,2)[1,(3,3)]
	12,14,23,34	(2,2)[(1,2),(1,2)]	(1,2)[(2,2),(2,2)]
	12,13,14,23,24	(2,3)[1,1,(1,2)]	(2,3)[1,1,(2,2)]
	12,13,14,23,24,34	(2,4)	(3,4)
	123,14	(2,2)[1,(1,2)[(2,2),1]]	(1,2)[1,(2,2)[(1,2),1]]
	123,124	(3,3)[1,1,(1,2)]	(1,3)[1,1,(2,2)]
	123,124,134	(2,2)[1,(2,3)]	(1,2)[1,(2,3)]
	1234	(4,4)	(1,4)

Let us study now how many iterated threshold access structures exist on a set $\mathcal{P}$ with at most five participants.

PROPOSITION 11. *All ideal access structures on a participant set with at most 4 participants are iterated threshold access structures.*

Proof. For a list of all ideal access structures on at most 4 participants we refer to [11]. Clearly all ideal access structures on 1 or 2 participants are threshold structures. All ideal structures on 3 participants except the one having basis P_1P_2, P_2P_3, P_3P_1, are class reducible and therefore can be realized as iterated threshold structures. P_1P_2, P_2P_3, P_3P_1 is just $(2,3)$. On 4 participants we find again that all ideal structures are class reducible except $P_1P_2, P_1P_3, P_1P_4, P_2P_3, P_2P_4, P_3P_4$ and its dual, that are $(2,4)$ and $(3,4)$. ∎

Table 1 contains all ideal access structures on $n \leq 4$ participants and their realizations as iterated threshold schemes. For short, in the second column participant P_i is simply denoted by i. Furthermore, the threshold scheme (1,1) is denoted by 1.

Let us examine now the case of $n = 5$ participants. For a list of all access structures in this case to refer to [5]. There are 61 ideal structures, 49 of them being reducible.

PROPOSITION 12. *On five participants there are 53 iterated threshold access structures out of 61 ideal structures. These 53 structures are all the reducible ideal access structures, the three threshold structures* $(2,5), (3,5), (4,5)$*, and the selfdual structure* $(2,3)[(1,1),(1,1),(2,3)]$.

Proof. In view of Propositions 7, 10 and 11, clearly all threshold and class reducible ideal access structures are iterated threshold. The selfdual structure with basis 124,125,134,135,234,235,45 is realized as $(2,3)[(1,1),(1,1),(2,3)]$. An exhaustive search shows that there are no more iterated threshold structures. ∎

TABLE 2
Iterated threshold schemes on 5 participants (up to equivalence).

Γ^m	Realization	Dual
12,13,14,15	(2,2)[1,(1,4)]	(1,2)[1,(4,4)]
12,23,34,45,14,25	(2,2)[(1,2),(1,3)]	(1,2)[(2,2),(3,3)]
12,14,23,24,25,34,45	(2,3)[1,1,(1,3)]	(1,3)[1,1,(3,3)]
12,13,14,15,23,25,34,45	(2,3)[1,(1,2),(1,2)]	(2,3)[1,(2,2),(2,2)]
12,13,14,15,23,24,25,34,35	(2,4)[1,1,1,(1,2)]	(3,4)[1,1,1,(2,2)]
$\binom{5}{2}$	(2,5)	(4,5)
123,14,15	(2,2)[1,(1,3)[(2,2),1,1]]	(1,2)[1,(3,3)[(1,2),1,1]]
123,145	(2,2)[1,(1,2)[(2,2),(2,2)]]	(1,2)[1,(2,2)[(1,2),(1,2)]]
123,124,15	(2,2)[1,(1,2)[(2,2),1]]	(1,2)[1,(2,2)[(1,2),1]]
123,124,35,45	(2,2)[(1,2),(1,2)[1,(2,2)]]	(1,2)[(2,2),(2,2)[1,(1,2)]]
123,124,34,35,45	(2,3)[(1,2)[(2,2),1],1,1]	(2,3)[(2,2)[(1,2),1],1,1]
123,124,125	(3,3)[1,(1,3)]	(1,3)[1,(3,3)]
123,124,134,15	(2,2)[1,(1,2)[(2,3),1]]	(1,2)[1,(2,2)[(2,3),1]]
123,124,125,34,35	(2,3)[(2,2),1,(1,2)]	selfdual
123,124,125,34,35,45	(2,4)[(2,2),1,1,1]	(3,4)[(1,2),1,1,1]
123,124,135,145	(3,3)[1,(1,2),(1,2)]	(1,3)[1,(2,2),(2,2)]
123,124,134,125,135	(2,2)[1,(2,3)[1,1,(1,2)]]	(1,2)[1,(2,3)[1,1,(2,2)]]
123,124,125,134,135,145	(2,2)[1,(2,4)]	(1,2)[1,(3,4)]
124,125,135,134,234,235	(2,2)[(2,3),(1,2)]	(1,2)[(2,3),(2,2)]
124,125,135,134,234,235,45	(2,3)[1,1,(2,3)]	selfdual
$\binom{5}{3}$	(3,5)	selfdual
1234,15	(2,2)[1,(1,2)[(3,3),1]]	(1,2)[1,(2,2)[(1,3),1]]
1234,125	(3,3)[1,1,(1,2)[(2,2),1]]	(1,3)[1,1,(2,2)[(1,2),1]]
1234,1235	(4,4)[1,1,1,(1,2)]	(1,4)[1,1,1,(2,2)]
1234,1235,145	(2,2)[1,(2,3)[(2,2),1,1]]	(1,2)[1,(3,2)[(2,1),1,1]]
1234,1235,1345	(3,3)[1,1,(2,3)]	(1,3)[1,1,(3,2)]
1234,1235,1245,1345	(2,2)[1,(3,4)]	(1,2)[1,(2,4)]
$\binom{5}{5}$	(5,5)	(1,5)

Remark 4. Let us see with some detail how to find all iterated threshold access structures on five participants. To that end we follow all possible partitions of $\mathcal{P}$.

<u>1,4 :</u> $(i,2)[1,\Delta]$, $\quad i = 1,2$. Clearly either the structure or its dual begins $(1,2)$ and therefore has an isolated participant an is reducible to one with 4 participants.

<u>2,3 :</u> $(i,2)[(i,2),\Delta]$, $\quad i = 1,2$. The structure has a final branch $(i,2)$, hence is reducible.

<u>1,1,3:</u> $(i,3)[1,1,\Delta]$, $\quad i = 1,2,3$. where Δ is an iterated threshold scheme with 3 participants. There are 5 of such structures (see Table 1 in the appendix). If $i = 1,3$ we can rewrite it as $(i,2)[(i,2),\Delta]$ and therefore they are reducible. Suppose $i = 2$:

(a) $(2,3)[1,1,(1,3)]$ is reducible.

(b) $(2,3)[1,1,(1,2)[(2,2)(2,2)]$ is reducible.

(c) $(2,3)[1,1,(2,3)]$ realizes the irreducible ideal structure $124, 125, 135, 134, 234, 235, 45$.

<u>1,2,2 :</u> $(i,3)[1,(j,2),(t,2)]$, $\quad i = 1,2,3$. They are reducible.

<u>1,1,1,2 :</u> $(i,4)[1,1,1,(t,2)]$, $\quad i = 1,\dots,4$. They are reducible.

<u>5 :</u> They are ideal since they are threshold schemes.

On the other hand, the 8 structures on 5 participants that are not realizable as iterated treshold schemes are the following:

$123, 145, 24, 35$ (Selfdual)

$123, 124, 135, 25, 34$ and its dual.

$123, 134, 135, 145, 25, 34$ and its dual.

$123, 124, 125, 134, 135, 234, 45$ (Selfdual)

$123, 124, 125, 134, 135, 234, 235, 45$ and its dual.

Table 2 contains all ideal access structures on $n = 5$ participants that are realizable as iterated threshold schemes and their realizations.

REFERENCES

[1] G. Blakley, Safeguarding Cryptographic Keys. AFIPS Conference Proceedings 1979, **48**, 313–317.

[2] E.F. Brickell, Some Ideal Secret Sharing Schemes, Lecture Notes in Computer Science: Eurocrypt'89, (Springer Verlag, 1989), 468–475.

[3] E.F. Brickell, Some Ideal Secret Sharing Schemes, Journal of Combinatorial Mathematics and Combinatorial Computing, **9** (1989), 105–113.

[4] E.F. Brickell, D.M. Davenport, On the Classification of Ideal Secret Sharing Schemes. Journal of Cryptology, **4** (1991), 123–134.

[5] W.-A. Jackson, K.M. Martin, Perfect Secret Sharing Schemes on Five Participants, Designs, Codes and Cryptography **9** (1996), 267–286.

[6] K.M.Martin, New secret sharing schemes from old, Journal of Combinatorial Mathematics and Combinatorial Computing, **14**(1993), 65–77.

[7] C. Padro, G. Saez Secret sharing schemes with bipartite access structure, Lecture Notes in Computer Science: Eurocrypt'98, (Springer Verlag, 1998), 500–511.

[8] A. Shamir, How to share a secret, Comm. ACM **22** (11) (1979), 612–613.

[9] G.J.Simmons (Ed.) Contemporary Cryptology, (IEEE Press, New York 1992).

[10] D.R. Stinson, Decomposition Constructions for Secret Sharing Schemes, IEEE Trans. Inform. Theory, vol. IT-40 (1994), 118–125.

[11] D.R. Stinson, Cryptography: Theory and Practice. (CRC Press, New York, 1995).