RAIRO-Inf. Theor. Appl. **40** (2006) 559-567
DOI: 10.1051/ita:2006040

THE ACCESSIBILITY OF AN ACCESS STRUCTURE

Francesc Carreras[1], Antonio Magaña[1] and Carlo Munuera[2]

Abstract. In secret sharing, different access structures have different difficulty degrees for acceding to the secret. We give a numerical measure of how easy or how difficult is to recover the secret, depending only on the structure itself and not on the particular scheme used for realizing it. We derive some consequences.

Mathematics Subject Classification. 94A62, 94A60.

1. Introduction

Secret sharing schemes are methods of distributing a secret among a set of participants. Each of these participants receives a piece of the secret, known as the *share*, in such a way that only specified coalitions of participants can reconstruct the secret by pooling the shares of their members. Applications of secret sharing schemes include key management and visual cryptography (see [1,3]). For a general reference on secret sharing, see [4].

A very important part in the theory of secret sharing concerns to security questions. In this way, problems like the determination of the best possible ratio *size of the secret/size of the shares*, the protection against cheating, etc., have received considerable attention. This paper is devoted to introduce another security aspect of secret sharing. In order to motivate our study, let us begin by describing a real example. The formula of a famous refreshing drink is an industrial secret. It is

Keywords and phrases. Cryptography, secret sharing schemes, access structures.

[1] Polytechnic University of Catalonia, Dept. of Applied Mathematics II, School of Industrial Engineering of Terrassa, C. Colón 11, 08222 Terrassa, Barcelona, Spain;
francesc.carreras@upc.edu, antonio.magana@upc.edu.
Their research is supported by Grant BFM 2003-01314 of the Spanish Ministry of Science and Technology and the European Regional Development Fund.
[2] University of Valladolid, Dept. of Applied Mathematics, Avda Salamanca SN, 47014 Valladolid, Castilla, Spain; cmunuera@modulor.arq.uva.es.
Munuera's research is supported by the 'Junta de Castilla y León', Project VA–0399.

shared to three people (three high-level directors of the company) in such a way that it is necessary the cooperation of any two of them to recover the secret. Here, the key point for us is the number (two out of three) of participants necessary for acceding to the secret. The reason of this choice is clear: if this number were one then the secret would became too accessible. Conversely, if this number were three then the secret would be too unaccessible (perhaps impossible to recover).

It appears that the concept of *accessibility* can be useful to consider when sharing a secret. It measures how many ways there exist for acceding to the secret and hence how easy or how difficult is to recover it. So it depends on the access structure itself and not on the particular scheme used for realizing it: the more is the number of authorized coalitions, the more are the ways of getting the secret. The fact that different structures give different difficulty levels for acceding to the secret is not unsuitable in practice. On the contrary, as seen in the example, it can be used to obtain different security levels according to the nature of the secret.

We shall give a numerical measure of chance for acceding to the secret and we shall study some of its properties (Sects. 2–4). Our main result is an axiomatic characterization of the proposed formula (Sect. 4), which also provides us a retrospective justification of it. Finally, in Section 5 we observe that also different participants in the same structure have different chance for acceding to the secret. By using the obtained formula for the accessibility of the structure we can derive a measure of the accessibility of the participants. This measure can be used to estimate the relative importance of each participant in the structure.

2. Definition and first properties

For the convenience of the reader we first recall the basic definitions about secret sharing. A complete treatment can be found in [4].

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n participants. An *access structure* on $\mathcal{P}$ is a set Γ of subsets of $\mathcal{P}$ ($\Gamma \subseteq 2^{\mathcal{P}}$). The subsets in Γ are those subsets of $\mathcal{P}$ that should be able to compute the shared secrets, and are called *authorized coalitions*. For practical applications the access structure Γ must be *monotone*, that is, if $A \subseteq B \subseteq \mathcal{P}$ and $A \in \Gamma$, then $B \in \Gamma$. For a monotone structure Γ, the set of minimal authorized coalitions, denoted by Γ_0, determines the whole structure Γ and it is called the *basis* of Γ. All structures in this paper are assumed to be monotone.

Given a set of secrets $\mathcal{K}$, a *(perfect) secret sharing scheme* for $\mathcal{K}$ *realizing the access structure* Γ is a method of sharing each secret $k \in \mathcal{K}$ among the participants in $\mathcal{P}$, in such a way that

- if an authorized coalition of participants $A \in \Gamma$ pool their shares, then they can determine k;
- if an unauthorized coalition of participants $B \subset \mathcal{P}$ pool their shares, then they can determine nothing about k.

The best known examples of secret sharing schemes are the so-called *threshold schemes*. A (t, n)*-threshold access structure* consists of all subsets of $\mathcal{P} =$

$\{P_1, \ldots, P_n\}$ having at least t out of n participants. For example, in the case of the famous refreshing drink mentioned in the introduction the secret is shared following a $(2, 3)$-threshold access structure.

There are different schemes realizing the same structure. Indeed, schemes realizing a (t, n)-threshold access structure were proposed by Blakley [2] and Shamir [3]. In the Shamir scheme, the set of secrets is a finite field $\mathbb{Z}_p$ (p prime). Firstly, a *dealer* chooses n distinct nonzero elements, $x_1, \ldots, x_n \in \mathbb{Z}_p$ and gives the value x_i to P_i. When sharing a secret $k \in \mathbb{Z}_p$, the dealer secretly chooses a random polynomial of degree $t-1$, $f(x) = k + a_1 x + \cdots + a_{t-1}x^{t-1}$, computes $y_i = f(x_i)$ for $i = 1, \ldots, n$, and gives the share y_i to P_i. It is clear that any authorized coalition can recover $f(x)$ (hence $k = f(0)$) by polynomial interpolation, whereas an unauthorized coalition has no information about k.

Let us already proceed to study the accessibility of an access structure. As above, let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n participants and let $\mathcal{A}_\mathcal{P}$ be the set of all access structures on $\mathcal{P}$.

Definition 2.1. The *accessibility index* on $\mathcal{P}$ is the map $\delta_\mathcal{P} : \mathcal{A}_\mathcal{P} \longrightarrow \mathbb{R}$ given by

$$\delta_\mathcal{P}(\Gamma) = \frac{|\Gamma|}{2^n} \quad \text{for} \quad \Gamma \in \mathcal{A}_\mathcal{P},$$

where $n = |\mathcal{P}|$. The number $\delta_\mathcal{P}(\Gamma)$ will be called the *accessibility degree* of structure Γ.

$\delta_\mathcal{P}(\Gamma)$ may be interpreted as the probability of a random coalition in $\mathcal{P}$ to be authorized when each participant has a probability $1/2$ to belong to it. As it is obvious, $\delta_\mathcal{P}(\Gamma) = 0$ iff $\Gamma = \emptyset$. Otherwise, $0 < \delta_\mathcal{P}(\Gamma) < 1$, and $|\Gamma| < |\Gamma'|$ implies $\delta_\mathcal{P}(\Gamma) < \delta_\mathcal{P}(\Gamma')$.

Example 2.2. The accessibility degree of a (t, n)-threshold access structure Γ is

$$\delta_\mathcal{P}(\Gamma) = \frac{1}{2^n} \sum_{s=t}^{n} \binom{n}{s}.$$

Fixing $\mathcal{P}$, the accessibility is a strictly decreasing function of t in the interval $1 \leq t \leq n$. The extreme cases arise for $t = n$, that gives the *unanimity structure* $U_\mathcal{P}$ of degree $1/2^n$, and for $t = 1$ that gives the *individualistic structure* of degree $1 - 1/2^n$. For unanimity structures the degree decreases with the number of participants.

Let us recall that the dual of an access structure Γ on $\mathcal{P}$ is $\Gamma^* = \{S \subseteq \mathcal{P} : \mathcal{P} \setminus S \notin \Gamma\}$.

Proposition 2.3. *Let Γ be a nonempty structure on $\mathcal{P}$ and let Γ^* be its dual. Then*

1. $\delta_\mathcal{P}(\Gamma^*) + \delta_\mathcal{P}(\Gamma) = 1$.

2. $\delta_\mathcal{P}(\Gamma^*) - \delta_\mathcal{P}(\Gamma) = \dfrac{|Q| - |C|}{2^n}$, *where we define* $Q = \{S \subseteq \mathcal{P} : S \notin \Gamma$ *and* $\mathcal{P} \setminus S \notin \Gamma\}$ *and* $C = \{S \subseteq \mathcal{P} : S \in \Gamma$ *and* $\mathcal{P} \setminus S \in \Gamma\}$.

TABLE 1. Accessibility characteristics of structures with four participants.

Number	Γ_0	Dual	Total degree	Participant degrees
1	$\{1;2;3;4\}$	20	0.9375	1 : 1 : 1 : 1
2	$\{1;2;34\}$	19	0.8125	3 : 3 : 1 : 1
3	$\{1;23;24;34\}$	18	0.7500	4 : 2 : 2 : 2
4	$\{12;13;14;23;24;34\}$	17	0.6875	3 : 3 : 3 : 3
5	$\{1;23;24\}$	16	0.6875	5 : 3 : 1 : 1
6	$\{12;13;14;23;24\}$	15	0.6250	4 : 4 : 2 : 2
7	$\{12;13;14;23\}$	14	0.5625	5 : 3 : 3 : 1
8	$\{12;13;24;34\}$	13	0.5625	3 : 3 : 3 : 3
9	$\{1;234\}$	12	0.5625	7 : 1 : 1 : 1
10	$\{12;13;24\}$	10	0.5000	4 : 4 : 2 : 2
11	$\{12;13;14;234\}$	11	0.5000	6 : 2 : 2 : 2
12	$\{12;13;14\}$	9	0.4375	7 : 1 : 1 : 1
13	$\{12;34\}$	8	0.4375	3 : 3 : 3 : 3
14	$\{12;13;234\}$	7	0.4375	5 : 3 : 3 : 1
15	$\{12;134;234\}$	6	0.3750	4 : 4 : 2 : 2
16	$\{12;134\}$	5	0.3125	5 : 3 : 1 : 1
17	$\{123;124;134;234\}$	4	0.3125	3 : 3 : 3 : 3
18	$\{123;124;134\}$	3	0.2500	4 : 2 : 2 : 2
19	$\{123;124\}$	2	0.1875	3 : 3 : 1 : 1
20	$\{1234\}$	1	0.0625	1 : 1 : 1 : 1

Proof. (1) Let us consider the sets D and T given by $D = \{S \subseteq \mathcal{P} : S \in \Gamma \text{ and } \mathcal{P} \setminus S \notin \Gamma\}$ and $T = \{S \subseteq \mathcal{P} : S \notin \Gamma \text{ and } \mathcal{P} \setminus S \in \Gamma\}$. Then $2^{\mathcal{P}} = D \cup C \cup Q \cup T$ and $|D| = |T|$, hence $2|D| + |C| + |Q| = 2^n$ and $|\Gamma| + |\Gamma^*| = 2^n$. (2) Here we use $|\Gamma^*| - |\Gamma| = |Q| - |C|$ and the identities $D^* = D$, $C^* = Q$, $Q^* = C$, $P^* = P$. □

Example 2.4. Table 1 above shows all structures with 4 participants (up to isomorphism) and their main characteristics. They are ranked by decreasing accessibility degree. The second column describes the basis of the structure (for simplicity, here we write i instead of P_i). The third column gives the dual structure. The fourth column gives the accessibility of each structure in decimal form. Finally, the fifth column gives $2^4 = 16$ times the accessibility of the participants (see Sect. 5).

3. Composed structures

As it is well known, many structures can be obtained from other simpler ones by composing them following some rules. In this section we show how to obtain the accessibility degree of some composed structures in terms of the degrees of the structures we are composing.

Definition 3.1. Let $\mathcal{P}$ be a set of participants.

(1) Given two access structures Γ and Γ' on $\mathcal{P}$, we define the structures *union* and *intersection* as $\Gamma \cup \Gamma' = \{S \subseteq \mathcal{P} : S \in \Gamma \text{ or } S \in \Gamma'\}$ and $\Gamma \cap \Gamma' = \{S \subseteq \mathcal{P} : S \in \Gamma \text{ and } S \in \Gamma'\}$.

(2) Let $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \cdots \cup \mathcal{P}_r$ be a partition of $\mathcal{P}$, and let Γ_i be an access structure on $\mathcal{P}_i$ for $i = 1, \ldots, r$. The *product* of $\Gamma_1, \ldots, \Gamma_r$ is the structure on $\mathcal{P}$ given by $\Gamma_1 \times \cdots \times \Gamma_r = \{S \subseteq \mathcal{P} : S \cap \mathcal{P}_i \in \Gamma_i \text{ for all } i = 1, 2, \ldots, r\}$.

Definition 3.2. Let $\mathcal{P}, \mathcal{Q}, \mathcal{R}$ be sets of participants such that $\mathcal{Q} \subset \mathcal{P} \subset \mathcal{R}$ and let Γ be an access structure on $\mathcal{P}$.

(1) A participant $P_i \in \mathcal{P}$ such that $P_i \notin S$ for all $S \in \Gamma_0$ will be called a *null* participant.

(2) The structure on $\mathcal{R}$ given by $\Gamma^{\mathcal{R}} = \{T \subseteq \mathcal{R} : T \cap \mathcal{P} \in \Gamma\}$ is called the *null extension* of Γ *to* $\mathcal{R}$.

(3) The structure on $\mathcal{Q}$ given by $\Gamma_{\mathcal{Q}} = \{S \subseteq \mathcal{Q} : S \in \Gamma\}$ is the *restriction* of Γ to $\mathcal{Q}$ (or, simply, a *substructure* of Γ). When it is $\mathcal{Q}$ that leaves the structure, then $\Gamma_{\mathcal{P}\setminus\mathcal{Q}}$ is denoted $\Gamma_{-\mathcal{Q}}$ and called *residual structure*. In this case, if $\mathcal{Q} = \{P_i\}$ we simply write Γ_{-i}.

Theorem 3.3. *Let $\mathcal{P}$ be a set of participants and let Γ be an access structure on $\mathcal{P}$. With the notations as above we have the following.*

1. *If $\mathcal{P} \subset \mathcal{R}$ then $\delta_{\mathcal{R}}(\Gamma^{\mathcal{R}}) = \delta_{\mathcal{P}}(\Gamma)$.*
2. *If $\mathcal{Q} \subset \mathcal{P}$ then $\delta_{\mathcal{P}\setminus\mathcal{Q}}(\Gamma_{-\mathcal{Q}}) \leq \delta_{\mathcal{P}}(\Gamma)$, with equality iff all participants in $\mathcal{Q}$ are null in Γ.*
3. *If $\Gamma = \Gamma_1 \times \cdots \times \Gamma_r$ then $\delta_{\mathcal{P}}(\Gamma) = \prod_{i=1}^{r} \delta_{\mathcal{P}_i}(\Gamma_i)$.*
4. *$\delta_{\mathcal{P}}(\Gamma \cup \Gamma') = \delta_{\mathcal{P}}(\Gamma) + \delta_{\mathcal{P}}(\Gamma') - \delta_{\mathcal{P}}(\Gamma \cap \Gamma')$. Moreover, if the sets $\mathcal{E}$ and $\mathcal{E}'$ of non-null participants of Γ and Γ' (respectively) are disjoint, then $\delta_{\mathcal{P}}(\Gamma \cap \Gamma') = \delta_{\mathcal{P}}(\Gamma)\delta_{\mathcal{P}}(\Gamma')$.*

Proof. (1) It suffices to consider the case where $\mathcal{R} = \mathcal{P} \cup \{P_i\}$. Then every coalition $S \in \Gamma$ gives rise to exactly two coalitions in $\Gamma^{\mathcal{R}}$, namely S and $S \cup \{P_i\}$. Thus $\delta_{\mathcal{R}}(\Gamma^{\mathcal{R}}) = 2|\Gamma|/2^{n+1} = \delta_{\mathcal{P}}(\Gamma)$. (2) It suffices again to deal with the case $\mathcal{Q} = \{P_i\}$. Then each coalition $T \in \Gamma_{-i}$ gives rise to at least two coalitions in Γ: T and $T \cup \{P_i\}$. Then $|\Gamma| \geq 2|\Gamma_{-i}|$ and

$$\delta_{\mathcal{P}\setminus\{P_i\}}(\Gamma_{-i}) = \frac{|\Gamma_{-i}|}{2^{n-1}} \leq \frac{|\Gamma|}{2^n} = \delta_{\mathcal{P}}(\Gamma).$$

If P_i is null in Γ then $\Gamma = (\Gamma_{-i})^{\mathcal{P}}$ so, according to item (1), we have $\delta_{\mathcal{P}\setminus\{P_i\}}(\Gamma_{-i}) = \delta_{\mathcal{P}}(\Gamma)$. Conversely, if the degrees coincide then $|\Gamma| = 2|\Gamma_{-i}|$. This means that P_i is null in Γ. (3) We need only to work out the case $r = 2$. Thus $S \in \Gamma$ iff $S = S_1 \cup S_2$, with $S_1 \in \Gamma_1$ and $S_2 \in \Gamma_2$. Then $|\Gamma| = |\Gamma_1||\Gamma_2|$ and

$$\delta_{\mathcal{P}}(\Gamma) = \frac{|\Gamma|}{2^n} = \frac{|\Gamma_1|}{2^{n_1}} \frac{|\Gamma_2|}{2^{n_2}} = \delta_{\mathcal{P}_1}(\Gamma_1)\delta_{\mathcal{P}_2}(\Gamma_2).$$

(4) The first property follows at once from the relation $|\Gamma \cup \Gamma'| = |\Gamma| + |\Gamma'| - |\Gamma \cap \Gamma'|$. To see the second one note that, under the hypotheses made, $\Gamma \cap \Gamma'$ is isomorphic

to the null extension to $\mathcal{P}$ of the product structure $\Gamma_{\mathcal{E}} \times \Gamma_{\mathcal{E}'}$. Then, by applying (1) and (3) we obtain $\delta_{\mathcal{P}}(\Gamma \cap \Gamma') = \delta_{\mathcal{E}}(\Gamma_{\mathcal{E}})\delta_{\mathcal{E}'}(\Gamma_{\mathcal{E}'}) = \delta_{\mathcal{P}}(\Gamma)\delta_{\mathcal{P}}(\Gamma')$. □

Remark 3.4. When an access structure Γ is defined by its basis Γ_0, we have also to specify the set of participants $\mathcal{P}$, because we can add as many null participants as we want. However, in view of properties (1) and (2) of the preceding theorem, these possible variations in the set of participants do not affect the accessibility degree. Thus, we can consider the accessibility index as a map $\delta : \mathcal{A} = \cup_{\mathcal{P}} \mathcal{A}_{\mathcal{P}} \longrightarrow \mathbb{R}$ given by $\delta(\Gamma) = \delta_{\mathcal{P}}(\Gamma)$ if $\cup_{S \in \Gamma_0} S \subseteq \mathcal{P}$.

4. Axiomatic characterization

We shall provide an axiomatic characterization of the accessibility index we have introduced. We begin by setting a set of independent properties that we want the index satisfies.

(A0) *The Empty Structure property*: $\delta_{\mathcal{P}}(\emptyset) = 0$.
(A1) *The Transfer property*: $\delta_{\mathcal{P}}(\Gamma \cup \Gamma') = \delta_{\mathcal{P}}(\Gamma) + \delta_{\mathcal{P}}(\Gamma') - \delta_{\mathcal{P}}(\Gamma \cap \Gamma')$. The aggregate accessibility arising from Γ and Γ' is exactly shared among $\Gamma \cup \Gamma'$ and $\Gamma \cap \Gamma'$.
(A2) *The Null Participant property*: If $P \notin \mathcal{P}$ and $\mathcal{R} = \mathcal{P} \cup \{P\}$, then $\delta_{\mathcal{P}}(\Gamma) = \delta_{\mathcal{R}}(\Gamma^{\mathcal{R}})$. Neither the adjunction nor the suppression of null participants will affect the accessibility.
(A3) *The Unanimity property*: $\delta_{\mathcal{P}}(U_{\mathcal{P}}) = 1/2^n$, where $n = |\mathcal{P}|$ and $U_{\mathcal{P}}$ stands for the unanimity structure (that is, the (n, n)-threshold access structure).

Theorem 4.1. *A function $\vartheta : \mathcal{A} \longrightarrow \mathbb{R}$ satisfies the properties A0, A1, A2 and A3 if and only if it is the accessibility index.*

Proof. As shown in Theorem 3.3 and Example 2.2, the accessibility index satisfies A0, A1, A2 and A3. Conversely, let ϑ be a function satisfying A0, A1, A2 and A3. Let us see that $\vartheta = \delta$. Given structures $\Gamma_1, \ldots, \Gamma_r$ on $\mathcal{P}$, from A1 it follows by recurrence that

$$\vartheta_{\mathcal{P}}(\cup_{i=1}^{r} \Gamma_i) = \sum_{j=1}^{r} (-1)^{j+1} \sum_{1 \le i_1 < \cdots < i_j \le r} \vartheta_{\mathcal{P}}(\Gamma_{i_1} \cap \Gamma_{i_2} \cap \cdots \cap \Gamma_{i_j}).$$

If Γ is an access structure on $\mathcal{P}$ and $\Gamma_0 = \{S_1, S_2, \ldots, S_r\}$, then Γ can be written as the union of the unanimity structures: $\Gamma = U^{\mathcal{P}}_{S_1} \cup U^{\mathcal{P}}_{S_2} \cup \cdots \cup U^{\mathcal{P}}_{S_r}$. Moreover, $U^{\mathcal{P}}_{S_{i_1}} \cap U^{\mathcal{P}}_{S_{i_2}} \cap \cdots \cap U^{\mathcal{P}}_{S_{i_k}} = U^{\mathcal{P}}_{S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_k}}$. By A3, ϑ coincides with δ on unanimity structures $U_{\mathcal{P}}$: $\delta_{\mathcal{P}}(U_{\mathcal{P}}) = \vartheta_{\mathcal{P}}(U_{\mathcal{P}})$. By A2, they also coincide on extensions of unanimity structures, that is, if $\mathcal{Q} \subset \mathcal{P}$ then $\delta_{\mathcal{P}}(U^{\mathcal{P}}_{\mathcal{Q}}) = \vartheta_{\mathcal{P}}(U^{\mathcal{P}}_{\mathcal{Q}})$. From the formula derived before we conclude that $\vartheta = \delta$ on $\mathcal{A}$. □

5. The accessibility of the participants

In the former sections we have studied the accessibility to the secret of the *whole* structure. However, if we look at the participants, it is clear that each of them have also a different opportunity for acceding to the secret: some of them belong to many authorized subsets, and some others do not; some of them are with small authorized subsets, etc. Look for instance at the structure having basis $\Gamma_0 = \{P_1, P_2P_3P_4\}$. It is clear that the chance of P_1 for acceding to the secret is much bigger than the chance of the others. Then, we can say that, when we are sharing a secret among a set of participants $\mathcal{P}$ following an access structure, we are also sharing some amount of power to them. This is not unsuitable in practice; on the contrary, it can be often useful when the participants are, in a natural way, in a hierarchy and hence they are not on equal terms. In this situation, it should be even convenient that different participants have different chance for acceding to the secret, relating the power shared with the access structure and their real power in the corporation of participants.

The accessibility index we have introduced (to which we may call *total accessibility index*) provide a natural tool to measure the accessibility of the participants.

Definition 5.1. Let $\mathcal{P}$ be a set of n participants and let Γ be an access structure on $\mathcal{P}$. For $i = 1, \ldots, n$, the *accessibility degree of participant* P_i *in* Γ is $\delta_{\mathcal{P}}(P_i, \Gamma) = \delta_{\mathcal{P}}(\Gamma) - \delta_{\mathcal{P}\setminus\{P_i\}}(\Gamma_{-i})$.

That is, $\delta_{\mathcal{P}}(P_i, \Gamma)$ is the fall in the accessibility degree of the structure when participant P_i leaves it. The following proposition collects some of its properties. Before that, let us state a new concept. Given two participants, P_i, P_j, we say that P_i is *over* P_j if for every $S \subset \mathcal{P}$ such that $P_i, P_j \notin S$, we have $S \cup \{P_i\} \in \Gamma$ whenever $S \cup \{P_j\} \in \Gamma$. Given two participants P_i, P_j, it can happen that none of them is over the other, or conversely that both P_i, P_j are simultaneously over the other. In this last case we say that P_i and P_j are *equivalent* participants. For weighted structures (see Ex. 5.5) it is clear that $w_i \geq w_j$ implies that P_i is over P_j and $w_i = w_j$ implies that they are equivalent.

Proposition 5.2. *Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n participants and let Γ be an access structure on $\mathcal{P}$. For $i = 1, \ldots, n$, we have*

1. $0 \leq \delta_{\mathcal{P}}(P_i, \Gamma) \leq \delta_{\mathcal{P}}(\Gamma)$.
2. $\delta_{\mathcal{P}}(P_i, \Gamma) = 0$ *if and only if* P_i *is a null participant.*
3. $\delta_{\mathcal{P}}(P_i, \Gamma) = \delta_{\mathcal{P}}(\Gamma)$ *if and only if* $P_i \in \cap_{S\in\Gamma} S$.
4. *If* P_i *is over* P_j, *then* $\delta_{\mathcal{P}}(P_i, \Gamma) \geq \delta_{\mathcal{P}}(P_j, \Gamma)$. *If* P_i, P_j *are equivalent then equality holds.*
5. $\delta_{\mathcal{P}}(P_i, \Gamma) = \delta_{\mathcal{P}}(P_i, \Gamma^*)$.

Proof. (1) and (2) follow from Theorem 3.3. (3) follows from the fact that $\delta_{\mathcal{P}\setminus\{P_i\}}(\Gamma_{-i}) = 0$ iff $\Gamma_{-i} = \emptyset$, hence iff $P_i \in \cap_{S\in\Gamma} S$. (4) If P_i is over P_j, let us consider the map $f : \Gamma_{-i} \longrightarrow \Gamma_{-j}$ given by $f(S) = S$ if $P_j \notin S$ and $f(S) = S \setminus \{P_j\} \cup \{P_i\}$ if $P_j \in S$. f is injective, hence $|\Gamma_{-i}| \leq |\Gamma_{-j}|$. (5) Write $\Gamma_i = \{S \in \Gamma : S \setminus \{P_i\} \notin \Gamma\}$ and $\Gamma^i = \{S \in \Gamma : P_i \in S, S \setminus \{P_i\} \in \Gamma\}$. We have a decomposition of Γ in pairwise

disjoint sets, $\Gamma = \Gamma_i \cup \Gamma_{-i} \cup \Gamma^i$. Therefore

$$\delta_{\mathcal{P}}(\Gamma) = \frac{|\Gamma_i| + |\Gamma_{-i}| + |\Gamma^i|}{2^n}.$$

The map $f : \Gamma_{-i} \longrightarrow \Gamma^i$ given by $f(S) = S \cup \{P_i\}$ is bijective. Thus $|\Gamma_{-i}| = |\Gamma^i|$ and

$$\delta_{\mathcal{P}}(P_i, \Gamma) = \delta_{\mathcal{P}}(\Gamma) - \delta_{\mathcal{P}\setminus\{P_i\}}(\Gamma_{-i}) = \frac{|\Gamma_i| + 2|\Gamma_{-i}|}{2^n} - \frac{|\Gamma_{-i}|}{2^{n-1}} = \frac{|\Gamma_i|}{2^n}.$$

As $\Gamma_i^* = \{S \in \Gamma^* : S \setminus \{P_i\} \notin \Gamma^*\} = \{\mathcal{P} \setminus S \notin \Gamma : \mathcal{P} \setminus S \cup \{P_i\} \in \Gamma\}$, we have $\delta_{\mathcal{P}}(P_i, \Gamma^*) = \frac{|\Gamma_i^*|}{2^n}$. Hence, it is clear that $S \in \Gamma_i^*$ iff $\mathcal{P} \setminus S \cup \{P_i\} \in \Gamma_i$. Once again it is possible to define a bijective map between Γ_i and Γ_i^* and then $|\Gamma_i| = |\Gamma_i^*|$. □

Example 5.3. Table 1 (the fifth column) contains the accessibility of the participants on all structures with four participants. For simplicity these numbers are multiplied by $2^4 = 16$.

In the proof of the above Proposition (item (5)), we have found an alternative formula for computing $\delta_{\mathcal{P}}(P_i, \Gamma)$: $\delta_{\mathcal{P}}(P_i, \Gamma) = \frac{|\Gamma_i|}{2^n}$. Furthermore, once these numbers $\delta_{\mathcal{P}}(P_i, \Gamma)$ are known we can use them for computing the total accessibility degree $\delta_{\mathcal{P}}(\Gamma)$ in a more efficient way than just its definition, as the following Proposition shows.

Proposition 5.4. *Let $\mathcal{P}$ be a set of n participants and let Γ be an access structure on $\mathcal{P}$. For $i = 1, \ldots, n-1$, let us consider the residual structures obtained by successive elimination of participants, $\Gamma^{-i} = \Gamma_{-\{1,2,\cdots,i\}}$, defined on $\mathcal{P}^{-i} = \{P_{i+1}, \ldots, P_n\}$. Let $\delta^{(i)} = \delta_{\mathcal{P}^{-(i-1)}}(P_i, \Gamma^{-(i-1)})$. Then $\delta_{\mathcal{P}}(\Gamma) = \delta^{(1)} + \cdots + \delta^{(n)}$.*

Proof. For $i = 1, \ldots, n$, we have $\delta^{(i)} = \delta_{\mathcal{P}^{-(i-1)}}(P_i, \Gamma^{-(i-1)}) = \delta_{\mathcal{P}^{-(i-1)}}(\Gamma^{-(i-1)}) - \delta_{\mathcal{P}^{-i}}(\Gamma^{-i})$. Adding up these equalities from $i = 1$ to n, it follows that $\delta_{\mathcal{P}}(\Gamma) = \delta^{(1)} + \cdots + \delta^{(n)}$. □

In practice, by using this method, it is convenient to eliminate participants according to a ranking of decreasing importance. When a first empty residual structure Γ^{-i} arises, then $\delta_{\mathcal{P}}(\Gamma) = \delta^{(1)} + \cdots + \delta^{(i)}$.

Example 5.5. Let $\mathcal{P}$ be a set of n participants. Let $w = (w_1, \ldots, w_n)$ be a n-tuple of nonnegative integers, called *weights* (w_i is the weight of participant P_i), and let t be a positive integer, called the *threshold*. The *weighted threshold access structure* $[t; w_1, \cdots, w_n]$ is the structure $[t; w_1, \cdots, w_n] = \{\{P_{i_1}, \cdots, P_{i_h}\} \subseteq \mathcal{P} : w_{i_1} + \cdots + w_{i_h} \geq t\}$. These structures were introduced by Shamir [3] and generalize the usual threshold structures: a (t, n)-threshold access structure is just $[t; 1, \cdots, 1]$.

We will apply the above procedure to compute the accessibility degree of the weighted structure $\Gamma = [62; 10, 10, 10, 10, 8, 5, 5, 5, 5, 4, 4, 3, 3, 3, 2]$, defined on 15 participants. If we denote $w = \sum_{i \in \mathcal{P}} w_i$, as $w - (w_1 + w_2 + w_3) = 57 < t = 62$,

it follows that Γ^{-3} is the empty structure. Thus, after computing $\delta^{(1)} = 0.05645$, $\delta^{(2)} = 0.01965$ and $\delta^{(3)} = 0.0017$, we have $\delta_{\mathcal{P}}(\Gamma) = \delta^{(1)} + \delta^{(2)} + \delta^{(3)} = 0.0778$.

This example clearly illustrates the convenience of suppressing the most important participants at first. The accessibility degree also gives us a way to estimate $|\Gamma|$, $|C|$ and $|Q|$. In our example $|\Gamma| = 2^n \delta_{\mathcal{P}}(\Gamma) = 2549$. And since $\delta(\Gamma^*) = 1 - \delta(\Gamma) = 0.9222$, from Proposition 2.3 it follows that $|C| = 0$ and $|Q| = 2^n[\delta(\Gamma^*) - \delta_{\mathcal{P}}(\Gamma)] = 27669$.

References

[1] G. Ateniese, C. Blundo, A. De Santis and D. Stinson, Extended Capabilities for visual cryptography. *Theoretical Comput. Sci.* **250** (2001) 143–162.
[2] G.R. Blakley, Safeguarding cryptographic keys. *AFIPS Conference Proceedings* **48** (1979) 313–317.
[3] A. Shamir, How to share a secret. *Commun. ACM*, **22** (1979) 612–613.
[4] D.R. Stinson, *Cryptography: Theory and Practice*. CRC Press (1995).

Communicated by C. Choffrut.
Received September 1st, 2003. Accepted November 7, 2005.