Fully Dynamic Secret Sharing Schemes *

C. Blundo,[1] A. Cresti,[2] A. De Santis,[1] and U. Vaccaro[1]

[1] Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84081 Baronissi (SA), Italy

[2] Dipartimento di Scienze dell' Informazione,
Università di Roma "La Sapienza", 00198 Roma, Italy

Abstract. We consider secret sharing schemes in which the dealer has the feature of being able (after a preprocessing stage) to activate a particular access structure out of a given set and/or to allow the participants to reconstruct different secrets (in different time instants) by sending to all participants the same broadcast message. In this paper we establish a formal setting to study such secret sharing schemes. The security of the schemes presented is unconditional, since they are not based on any computational assumption. We give bounds on the size of the shares held by participants and on the size of the broadcast message in such schemes.

1 Introduction

A secret sharing scheme is a method of dividing a secret s among a set $\mathcal{P}$ of participants in such a way that: if the participants in $A \subseteq \mathcal{P}$ are qualified to know the secret then by pooling together their information they can reconstruct the secret s; but any set A of participants not qualified to know s has absolutely no information on the secret. The collection of subsets of participants qualified to reconstruct the secret is usually referred to as the *access structure* of the secret sharing scheme.

Secret sharing schemes are useful in any important action that requires the concurrence of several designed people to be initiated, as launching a missile, opening a bank vault or even opening a safety deposit box. Secret sharing schemes are also used in management of cryptographic keys and multi-party secure protocols (see [7] for example). We refer the reader to the excellent surveys papers [13] and [16] for a detailed discussion of secret sharing schemes and for a complete bibliography on the argument.

Simmons [13] pointed out the practical relevance of secret sharing schemes having the feature of being able (after some preprocessing stage) to activate a particular access structure out of a given set and/or to allow the participants to

* Partially supported by Italian Ministry of University and Research (M.U.R.S.T.) and by National Council for Research (C.N.R.).

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 110-125, 1994.

reconstruct different secrets (in different time instants) simply by sending to all participants the same broadcast message. Harn, Hwang, Laih, and Lee [8] gave an algorithm to set up threshold secret sharing schemes (i.e., characterized by an access structure consisting of all subsets of participants of cardinality not less than some integer k), in which participants could be qualified to recover different secrets in different time instants simply by receiving a broadcast message. However, they assumed that the access structure remained the same in each time instant. Martin [11] presented a technique to realize secret sharing schemes for general access structures in which by sending a broadcast message to all participants, at each time instant a new secret is activated and a participant is disenrolled from the scheme. Blakley, Blakley, Chan, and Massey [1] considered the problem of constructing threshold secret sharing schemes with disenrollment capability. The threshold of the secret sharing schemes is not changed at each disenrollment. They gave a lower bound on the size of the shares held by each participant in such schemes.

In this paper we establish a formal setting to study secret sharing schemes in which different access structures and/or different secrets can be activated in subsequent time instants simply by sending the same broadcast message to all participants. Our approach is information–theoretic based. The security of the schemes presented in this paper is unconditional, since they are not based on any computational assumption. We first study the case in which we have different access structures and we want to enable one of them to reconstruct a predefined secret. In this model we show that the size of shares held by any participant and the size of the broadcast message are bounded from below by the size of the secret. We show that these bounds are optimal if one considers either the share of the participant or the broadcast message (see Theorem 6 and Theorem 7). Motivated by this result we define *Ideal Secret Sharing Schemes with Broadcast* as schemes for which the size of the shares held by participants and the size of the broadcast messages are the same as the size of the secret. We analyze ideal secret sharing schemes with broadcast messages when the family of the access structures that can be activated contains threshold access structures only. In Section 6 we consider the general case in which one wants to activate different access structures to recover possibly different secrets at subsequent time instants. We give sufficient conditions for the existence of a participant whose share size is lower bounded by the sum of the sizes of the secrets. This result generalizes the result of [1].

2 Secret Sharing Schemes with Broadcast Message

In this section we define secret sharing schemes with broadcast message. Let $\mathcal{P}$ be the set of participants. Denote by $\mathcal{A}$ the family of subsets of participants which we desire to be able to recover the secret; hence $\mathcal{A} \subseteq 2^{\mathcal{P}}$. $\mathcal{A}$ is called the *access structure* of the secret sharing scheme. In this section we consider the situation in which we have *more* than one access structure and we want to enable only one of them to be active to recover a predefined secret. In this scheme there

is a special participant called the *dealer*. The dealer is denoted by D and we assume $D \notin \mathcal{P}$. Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of access structures on the set of participants $\mathcal{P}$ and let $\{p_S(s)\}_{s \in S}$ be a probability distribution on the set of secrets S. The dealer in the preprocessing phase, knowing $\{p_S(s)\}_{s \in S}$ (but not knowing the value of the secret) and A, generates and distributes shares to participants in $\mathcal{P}$. The dealer, in the message-generation phase, on input a secret s randomly chosen accordingly to $\{p_S(s)\}_{s \in S}$, the access structures $\mathcal{A}_1, \ldots, \mathcal{A}_m$, the shares of participants $P_1, \ldots, P_n$, and an index $i \in \{1, 2, \ldots, m\}$ (arbitrarily chosen) computes a message b_i and broadcasts it to all participants in $\mathcal{P}$. At the end of the message-generation phase, only the subsets of participants in $\mathcal{A}_i$ are able to recover s. These phases are described in the following algorithms.

Preprocessing-Algorithm

Input: $\{p_S(s)\}_{s \in S}$, $\mathcal{P} = \{P_1, \ldots, P_n\}$, and $\mathcal{A}_1, \ldots, \mathcal{A}_m$.

Output: The shares $a_1, \ldots, a_n$ for participants $P_1, \ldots, P_n$, respectively.

Message-Generation

Input: $s \in S$, $\mathcal{A}_1, \ldots, \mathcal{A}_m$, $a_1, \ldots, a_n$, and $i \in \{1, 2, \ldots, m\}$.

Output: The broadcast message b_i that enables the access structure $\mathcal{A}_i$.

In this section we consider the case in which we want to enable only one access structure among the family A, the case in which we want to enable different access structures at different times will be analyzed in Section 6.

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of participants and let $\mathcal{A}$ be an access structure on $\mathcal{P}$. It is reasonable to require that $\mathcal{A}$ be *monotone*, that is if $A \in \mathcal{A}$ and $A \subseteq A' \subseteq \mathcal{P}$, then $A' \in \mathcal{A}$. In this paper, we assume that the access structures are not trivial, that is, there is always at least a subset of participants who can reconstruct the secret, i.e., $\mathcal{A} \neq \emptyset$, and that not all possible subsets of participants are able to recover the secret, i.e., $\mathcal{A} \neq 2^{\mathcal{P}}$.

If $\mathcal{A}$ is an access structure on $\mathcal{P}$, then $B \in \mathcal{A}$ is a *minimal* authorized subset if $A \notin \mathcal{A}$ whenever $A \subset B$. The set of minimal authorized subsets of $\mathcal{A}$ is denoted $\mathcal{A}^0$ and is called the *basis* of $\mathcal{A}$. $\mathcal{A}$ is uniquely determined as a function of $\mathcal{A}^0$, as we have $\mathcal{A} = \{B \subseteq \mathcal{P} : A \subseteq B, A \in \mathcal{A}^0\}$. We say that $\mathcal{A}$ is the *closure* of $\mathcal{A}^0$ and write $\mathcal{A} = cl(\mathcal{A}^0)$.

Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m \mid \mathcal{A}_i \subseteq 2^{\mathcal{P}}, 1 \leq i \leq m\}$ be a family of monotone access structures on $\mathcal{P}$. For $1 \leq j \leq m$, define $\mathcal{P}_j = \bigcup_{X \in \mathcal{A}_j} X$; $\mathcal{P}_j$ denotes the set of participants in the scheme with access structure $\mathcal{A}_j$. Let S be the set of secrets, $\{p_S(s)\}_{s \in S}$ be a probability distribution on S, and let a secret sharing scheme with broadcast message for secrets in S be fixed. For any participant $P \in \mathcal{P}$, let us denote by $K(P)$ the set of all possible shares given to participant P. Given a set of participants $A = \{P_{i_1}, \ldots, P_{i_r}\} \subseteq \mathcal{P}$, where $i_1 < i_2 < \ldots < i_r$, denote by $K(A)$ the set $K(P_{i_1}) \times \cdots \times K(P_{i_r})$. A secret sharing scheme with

broadcast message for secrets in S and a probability distribution $\{p_S(s)\}_{s\in S}$ naturally induce a probability distribution on $K(A)$, for any $A \subseteq \mathcal{P}$. Denote such probability distribution by $\{p_{K(A)}(a)\}_{a\in K(A)}$. Finally, denote by $H(S)$ the entropy of $\{p_S(s)\}_{s\in S}$ and by $H(A)$ the entropy of $\{p_{K(A)}(a)\}_{a\in K(A)}$, for any $A \in 2^{\mathcal{P}}$.

For any access structure $\mathcal{A}_i \in \mathsf{A}$, let us denote by b_i a generic broadcast message that enables the access structure $\mathcal{A}_i$ and by B_i the set of all possible broadcast messages enabling $\mathcal{A}_i$. A secret sharing scheme with broadcast message for $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ and a probability distribution $\{p_S(s)\}_{s\in S}$ induce, through the two probabilistic algorithms above, a probability distribution on each B_i. Denote such probability distribution by $\{p_{B_i}(b)\}_{b\in B_i}$. Finally, for all $1 \leq i \leq m$, denote by $H(B_i)$ the entropy of $\{p_{B_i}(b)\}_{b\in B_i}$.

By using the entropy approach, as done in [9] and [6] for usual secret sharing schemes, we define a secret sharing scheme with broadcast message as follows.

Definition 1. Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of monotone, non trivial access structures on $\mathcal{P}$. A *secret sharing scheme with broadcast message* is a sharing of secrets in S among participants in $\mathcal{P}$ such that

1. Before knowing the broadcast message any subset of participants has no information about the value of the secret:
   Formally, for any $X \in 2^{\mathcal{P}}$, *it holds* $H(S|X) = H(S)$.
2. After seeing the broadcast message, we have a perfect secret sharing scheme:
   Formally, for any $\mathcal{A}_i \in \mathsf{A}$ *and for any* $X \in 2^{\mathcal{P}}$, *it holds*

$$H(S|XB_i) = \begin{cases} H(S) & \text{if } X \notin \mathcal{A}_i \\ 0 & \text{if } X \in \mathcal{A}_i \end{cases}$$

Notice that $H(S|X) = H(S)$ is equivalent to state that S and X are statistically independent, i.e., for all $x \in K(X)$ and for all $s \in S$, $p(s|x) = p_S(s)$ and therefore the knowledge of x gives no information about the secret. Equivalently, $H(S|XB_i) = H(S)$ means that S and XB_i are statistically independent. Moreover, $H(S|XB_i) = 0$ means that each set of values of the shares and broadcast message in $K(X) \times K(B_i)$ corresponds to a unique value of the secret. In fact, by definition, $H(S|XB_i) = 0$ is equivalent to the fact that for all $x \in K(X)$ and for all $b \in K(B_i)$ with $p(x, b) > 0$ a unique $s \in S$ exists such that $p(s|x\ b) = 1$.

For any access structure $\mathcal{A}_i \in \mathsf{A}$, let $\mathcal{A}_i^B = \{X \cup \{B_i\} | X \in \mathcal{A}_i\}$, that is, $\mathcal{A}_i^B$ contains all the sets that can reconstruct the secret in the access structure $\mathcal{A}_i$ together with the broadcast message that enables this access structure. Intuitively, in $\mathcal{A}_i^B$ the broadcast message B_i "plays" the role of a participant.

As an example let us consider the following situation. Let $\mathcal{P} = \{P_1, P_2, ..., P_6\}$ be the set of participants. The family A, depicted in Figure 1, contains three access structures $\mathcal{A}_1 = \{P_1P_2, P_2P_3\}$, $\mathcal{A}_2 = \{P_3P_4\}$, and $\mathcal{A}_3 = \{P_4P_5, P_5P_6\}$. The following algorithms realize a secret sharing scheme with broadcast for A when the secret is uniformly chosen in $GF(q)$, where q is a prime power.

Preprocessing-Algorithm

Input: a prime power q, $\mathsf{A} = \{\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3\}$, and $\mathcal{P} = \{P_1, \ldots, P_6\}$.

Randomly select $r_1, r_2, r_3, r_4, r_5, r_6 \in GF(q)$.

Let $a_1 = r_1$ be the share of participant P_1, $a_2 = r_2$ be the share of participant P_2, $a_3 = r_1, r_3$ be the share of participant P_3, $a_4 = r_4, r_5$ be the share of participant P_4, $a_5 = r_6$ be the share of participant P_5, and $a_6 = r_5$ be the share of participant P_6.

Output: The shares $a_1, \ldots, a_6$ for participants $P_1, \ldots, P_6$, respectively.

Message-Generation

Input: $s \in GF(q)$, $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$, $a_1, \ldots, a_6$, and $i \in \{1, 2, 3\}$.

Compute $x_1 = r_1 + r_2 \bmod q$, $x_2 = r_3 + r_4 \bmod q$, and $x_3 = r_5 + r_6 \bmod q$.

Output: The broadcast message $b_i = s + x_i \bmod q$ that enables $\mathcal{A}_i$.

It is easy to see that previous algorithms realize a secret sharing scheme with broadcast for A.

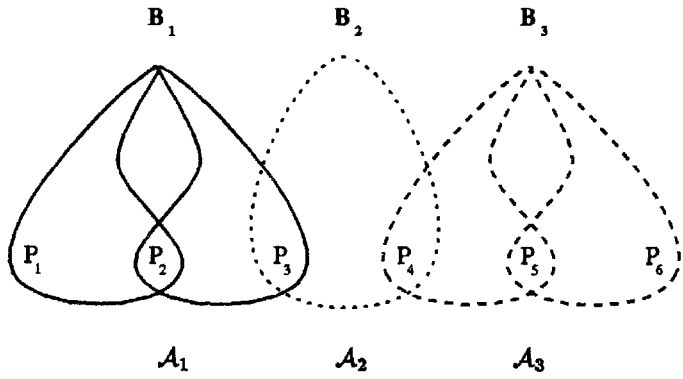

Figure 1.

3 The Size of Shares

An important issue in the implementation of secret sharing schemes is the size of the shares, since the security of a system degrades as the amount of secret information increases. Thus, one of the basic problems is to analyze the amount of information that must be kept secret. Unfortunately, in all secret sharing schemes with broadcast message the size of the shares, as well as the size of the broadcast message, cannot be less than the size of the secret as we will see in the next lemma. Moreover, there are families of access structures for which any corresponding secret sharing scheme with broadcast message must either give

to some participant a share of size strictly bigger than the secret size, or the broadcast message has to have size strictly bigger than the secret size, as we will see in Section 5.

The following lemmas are a generalization to secret sharing schemes with broadcast message of the results proved in [6] for secret sharing schemes with no broadcast message.

Lemma 2. *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of monotone access structures on a set* $\mathcal{P}$ *of participants. Let* $\mathcal{A}_i \in \mathsf{A}$, *if* $Y \in 2^{\mathcal{P} \cup \{B_i\}} \backslash \mathcal{A}_i^B$ *and* $X \cup Y \in \mathcal{A}_i^B$, *then* $H(X|Y) = H(S) + H(X|YS)$.

Proof: If $Y \in 2^{\mathcal{P} \cup \{B_i\}} \backslash \mathcal{A}_i^B$ we distinguish two cases: $B_i \notin Y$ and $B_i \in Y$. If $B_i \notin Y$, then $H(S|Y) = H(S)$ by property 1 of Definition 1. If $B_i \in Y$, then $H(S|Y) = H(S)$ because of property 2 of Definition 1 since $Y \backslash \{B_i\} \notin \mathcal{A}_i$.
Now, consider the conditional mutual information $I(X; S|Y)$, it can be written either as $H(X|Y) - H(X|YS)$ or as $H(S|Y) - H(S|XY)$. Hence, $H(X|Y) = H(X|YS) + H(S|Y) - H(S|XY)$. Because of $H(S|XY) = 0$ for $X \cup Y \in \mathcal{A}_i^B$ and $H(S|Y) = H(S)$, we have $H(X|Y) = H(S) + H(X|YS)$. □

As immediate consequence of the previous lemma we get the following theorem.

Theorem 3. *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of monotone access structures on a set* $\mathcal{P}$ *of participants. For any secret sharing scheme with broadcast message for* A *the following properties hold:*

1. *For any* $P \in \mathcal{P}$, *it holds* $H(P) \geq H(S)$.
2. *For* $i = 1, 2, \ldots, m$, *it holds* $H(B_i) \geq H(S)$.

If the secrets are uniformly chosen in S, that is $H(S) = \log |S|$, then we can bound both the size of the shares distributed to participants and the size of the broadcast messages.

Theorem 4. *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of monotone access structures on a set* $\mathcal{P}$ *of participants. If the secrets are uniformly chosen in* S, *then for any secret sharing scheme with broadcast message for* A *the following properties hold:*

1. *For any* $P \in \mathcal{P}$, *it holds* $\log |K(P)| \geq \log |S|$.
2. *For* $i = 1, 2, \ldots, m$, *it holds* $\log |B_i| \geq \log |S|$.

Next lemma implies that the uncertainty on shares of participants, who cannot recover the secret, it cannot be decreased by the knowledge of the secret.

Lemma 5. *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of monotone access structures on a set* $\mathcal{P}$ *of participants. Let* $\mathcal{A}_i \in \mathsf{A}$, *if* $X \cup Y \in 2^{\mathcal{P} \cup \{B_i\}} \backslash \mathcal{A}_i^B$, *then* $H(Y|X) = H(Y|XS)$.

Proof: The conditional mutual information $I(Y, S|X)$ can be written either as $H(Y|X) - H(Y|XS)$ or as $H(S|X) - H(S|XY)$. Hence, $H(Y|X) = H(Y|XS) + H(S|X) - H(S|XY)$. Because of $H(S|XY) = H(S|X) = H(S)$, for $X \cup Y \notin \mathcal{A}_i^B$, we have $H(Y|X) = H(Y|XS)$. □

Next theorems prove that for any family of monotone access structures there are secret sharing schemes with broadcast message such that the size of the shares given to a predefined participant or the size of the broadcast messages is the same than that of the secret.

The secret sharing schemes with broadcast message presented in this paper are all realized by considering uniform distributions on S. In this case, we suppose that $S = GF(q)$, where q is a prime power.

Theorem 6. *Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of monotone access structures on a set $\mathcal{P}$ of participants and let $P \in \mathcal{P}$ be a fixed participant. If the secret is uniformly chosen then there exists a secret sharing scheme with broadcast message such that*

$$H(P) = H(S).$$

In Section 2 we presented a scheme for the family of monotone access structures $\mathsf{A} = \{\{P_1P_2, P_2P_3\}, \{P_3P_4\}, \{P_4P_5, P_5P_6\}\}$ on the set of participants $\mathcal{P} = \{P_1, P_2, \ldots, P_6\}$. In such scheme participants P_3 and P_4 get a share whose size is twice the size of the secret. By previous theorem there exists a scheme where either P_3 or P_4 can have a share of the same size than that of the secret. A possible scheme, in which P_3 gets a shares whose size is equal to the size of the secret, is the following. In this sheme the secret is uniformly chosen in $GF(q)$, where q is a prime power.

Preprocessing-Algorithm

Input: a prime power q, $\mathsf{A} = \{\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3\}$, and $\mathcal{P} = \{P_1, \ldots, P_6\}$.

Randomly select $r_1, r_2, \ldots, r_9 \in GF(q)$.

Let $a_1 = r_1$ be the share of participant P_1, $a_2 = r_2, r_3$ be the share of participant P_2, $a_3 = r_4$ be the share of participant P_3, $a_4 = r_5, r_6$ be the share of participant P_4, $a_5 = r_7, r_8$ be the share of participant P_5, and $a_6 = r_9$ be the share of participant P_6.

Output: The shares $a_1, \ldots, a_6$ for participants $P_1, \ldots, P_6$, respectively.

Message-Generation

Input: $s \in S = GF(q)$, $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$, $a_1, \ldots, a_6$, and $i \in \{1, 2, 3\}$.

Compute $b_1 = s + r_1 + r_2 \bmod q$, $s + r_3 + r_4 \bmod q$, $b_2 = s + r_4 + r_5 \bmod q$, and $b_3 = r_8 + r_7 \bmod q$, $s + r_8 + r_9 \bmod q$.

Output: The broadcast message b_i that enables the access structure $\mathcal{A}_i$.

It is easy to see that previous algorithms realize a secret sharing scheme with broadcast for A, in which the participant P_3 gets a shares whose size is equal to the size of the secret.

Next theorem states that for any family of monotone access structures there are secret sharing schemes with broadcast message such that the size of the broadcast messages is the same than that of the secret.

Theorem 7. *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of monotone access structures on a set* $\mathcal{P}$ *of participants. If the secret is uniformly chosen then there exists a secret sharing scheme with broadcast message such that, for all* $i \in \{1, 2, \ldots, m\}$, *it holds*

$$H(B_i) = H(S).$$

4 Ideal Schemes

In the previous section we have seen that for any family of access structures A either the shares given to a participant in $\mathcal{P}$, or the broadcast messages can be of the same dimension than that of the secret. In this section we give a sufficient condition for which there exists a secret sharing scheme with broadcast message for a family of access structures $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ such that for any $P \in \mathcal{P}$ and for any $i \in \{1, 2, \ldots, m\}$, it holds $H(P) = H(B_i) = H(S)$. That is, we consider schemes in which both the broadcast messages and the shares of participants have the same dimension than the secret. We will use the following lemma that is an extension of a lemma proved in [6].

Lemma 8. *Let be* A, B, C, D, F, S *six random variables such that*

1. $H(S|ABF) = H(S|BCF) = H(S|ACDF) = 0$,
2. $H(S|BF) = H(S|ACF) = H(S|ADF) = H(S|F)$.

Then $H(BC|F) \geq 3H(S|F)$.

An ideal secret sharing scheme with broadcast message is defined as follows.

Definition 9. Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of monotone access structures on a set $\mathcal{P}$ of participants. A secret sharing scheme with broadcast message for A is said *ideal* if for any $P \in \mathcal{P}$ and for any $i \in \{1, 2, \ldots, m\}$, we have $H(P) = H(B_i) = H(S)$.

We first consider the simple case in which $\mathsf{A} = \{\mathcal{A}_1\}$.

Theorem 10. *Assume that the secret is uniformly chosen. An ideal secret sharing scheme with broadcast message for* $\mathsf{A} = \{\mathcal{A}_1\}$ *exists if and only if there exists an ideal secret sharing scheme for the access structure* $\mathcal{A}_1$.

Therefore, in such a case the classification of ideal secret sharing schemes with no broadcast messages given in [5] applies.

Definition 11. Two access structures $\mathcal{A}_1$ and $\mathcal{A}_2$, on the sets of participants $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, are *compatible* if and only if

$$P \in \mathcal{P}_1 \cap \mathcal{P}_2 \Rightarrow P \in \bigcap_{X \in \mathcal{A}_1^0} X \cap \bigcap_{Y \in \mathcal{A}_2^0} Y.$$

Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be two access structures on the sets of participants $\mathcal{P}_1$ and $\mathcal{P}_2$, respectively. If $\mathcal{P}_1 \cap \mathcal{P}_2 \neq \emptyset$ we say that the two access structures are *connected*. If $\mathcal{A}_1$ and $\mathcal{A}_2$ are not connected, then for $\mathsf{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$ there exists an ideal secret sharing scheme with broadcast message if and only if it exists an ideal secret sharing scheme with broadcast message for both $\mathsf{A}_1 = \{\mathcal{A}_1\}$ and $\mathsf{A}_2 = \{\mathcal{A}_2\}$. We say that m access structures $\mathcal{A}_1, \ldots, \mathcal{A}_m$ are *connected* if the set $\cup_{i=1}^{m} \mathcal{P}_i$ cannot be partitioned into two nonempty sets X and Y such that each $\mathcal{P}_i$, for $i = 1, \ldots, m$, is all contained either in X or in Y. When $\mathcal{A}_1, \ldots, \mathcal{A}_m$ are not connected, we can study separately each connected part.

Theorem 12. *Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of m connected access structures pairwise compatible such that there exists an ideal secret sharing scheme with broadcast message for each $\mathcal{A}_i$, $i = 1, \ldots, m$. If the secret is uniformly chosen, then there exists an ideal secret sharing scheme with broadcast message for* A.

5 Threshold Schemes with Broadcast Message

In this section we analyze the case in which all access structures in A are distinct threshold structures. That is, $\mathsf{A} = \{\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}, \ldots, \mathcal{A}_{(k_t,\mathcal{P}_t)}\}$, where $\mathcal{A}_{(k_i,\mathcal{P}_i)}$ is the set of all subsets consisting of at least k_i participants in $\mathcal{P}_i$. In previous section we gave a sufficient condition for which ideal secret sharing schemes with broadcast message exist. Each access structure in the scheme must admit an ideal secret sharing scheme. This condition is necessary but not sufficient. In fact, threshold schemes that admit ideal secret sharing schemes not always have ideal secret sharing schemes with broadcast message as we will see in the following. If $t = 1$, then by Theorem 10 and [12] there exists an ideal secret sharing scheme with broadcast message for A. We observe that for a threshold structure $\mathcal{A}_{(k_i,\mathcal{P}_i)}$ a participant P belongs to $\bigcap_{X \in \mathcal{A}^0_{(k_i,\mathcal{P}_i)}} X$ if and only if $k_i = |\mathcal{P}_i|$, that is $|\mathcal{A}^0_{(k_i,\mathcal{P}_i)}| = 1$. Thus, two connected access structures $\mathcal{A}_{(k_1,\mathcal{P}_1)}$ and $\mathcal{A}_{(k_2,\mathcal{P}_2)}$ are compatible if and only if $k_1 = |\mathcal{P}_1|$ and $k_2 = |\mathcal{P}_2|$.

Theorem 13. *Let $\mathsf{A} = \{\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}, \ldots, \mathcal{A}_{(k_t,\mathcal{P}_t)}\}$ be a family of $t \geq 2$ (distinct) connected access structures. There exists an ideal secret sharing scheme with broadcast message for* A *if and only if the access structures composing* A *are pairwise compatible.*
If an ideal secret sharing scheme with broadcast message does not exist then, for each participant $P \in \mathcal{P}_{i_1} \cap \mathcal{P}_{i_2}$ there is an index $j \in \{1, 2\}$, such that for any secret sharing scheme with broadcast message it holds $H(P) + H(B_{i_j}) \geq 3H(S)$.

The previous theorem proves a gap for the dimension of the shares of participants and of the broadcast message. Either there is an ideal scheme (and thus they all have the same size than the secret) or the size of at least one of them is 50% bigger the the secret size. Thus, we have proved that there are families of access

structures for which any corresponding secret sharing scheme with broadcast message must either give to some participant a share of size strictly bigger than the secret size, or the broadcast message has to have size strictly bigger than the secret size even though each access structure belonging to these families admits an ideal secret sharing scheme.

Next corollary is a consequence of Theorem 13.

Corollary 14. *Let* $\mathsf{A} = \{\mathcal{A}_{(1,\mathcal{P}_1)}, \ldots, \mathcal{A}_{(1,\mathcal{P}_t)}\}$ *be a family of* $t \geq 2$ *(distinct) access structures. There exists an ideal secret sharing scheme with broadcast message for* A *if and only if the access structures composing* A *are not connected, that is,* $\mathcal{P}_i \cap \mathcal{P}_j = \emptyset$, *for all* $i \neq j$.

In some cases a better bound on the size of the shares distributed to participants holds. Consider the set of participants $\mathcal{P} = \{X_0, X_1, X_2, \cdots, X_n\}$ and the $\mathcal{M}_n$ be the closure of $\{X_1X_2 \ldots X_n\} \cup \{X_0X_1, X_0X_2, \ldots, X_0X_{n-1}\}$. In a similar way of Theorem 4.1 in [3] one can easily prove that for any $n-2$ indices $i_1, i_2, \ldots, i_{n-2} \in \{1, 2, \ldots, n-1\}$, it holds

$$H(X_0) + H(X_{i_1}) + \ldots + H(X_{i_{n-2}}) \geq (2n-3)H(S). \tag{1}$$

The following theorem holds.

Theorem 15. *Let* $\mathsf{A} = \{\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}\}$, *with* $k_1 \leq k_2$, *be a family of two distinct connected access structures. Let* $r = |\mathcal{P}_1 \cap \mathcal{P}_2|$.
If $k_1 < r$ *then*

1. *If* $k_1 < k_2$, *then for any* $P_{l_1}, \ldots, P_{l_{t-k_1}} \in \mathcal{P}_1 \cap \mathcal{P}_2$ *where* $t = \min\{k_2, r\}$, *it holds*
   $H(B_1) + \sum_{j=1}^{t-k_1} H(P_{l_j}) \geq (2(t-k_1)+1)H(S)$.
2. *If* $k_1 = k_2 = k$ *and* $r = t_2$, *then for any* $P_{l_1}, \ldots, P_{l_\ell} \in \mathcal{P}_1 \cap \mathcal{P}_2$, *where* $\ell = \min\{k-1, t_1 - r\}$, *it holds* $H(B_1) + \sum_{j=1}^{\ell} H(P_{l_j}) \geq (2\ell+1)H(S)$.
3. *If* $k_1 = k_2 = k$ *and* $r < t_2$, *then for any* $P_{l_1}, \ldots, P_{l_\ell} \in \mathcal{P}_1 \cap \mathcal{P}_2$, *where* $\ell = \min\{k-1, t_2 - r\}$, *it holds* $H(B_2) + \sum_{j=1}^{\ell} H(P_{l_j}) \geq (2\ell+1)H(S)$.

If $r \leq k_1$ *then*

1. *If* $k_2 < t_2$, *then for any* $P_{l_1}, \ldots, P_{l_{t-1}} \in \mathcal{P}_1 \cap \mathcal{P}_2$, *where* $t = \min\{r, t_2 - k_2 + 1\}$, *it holds*
   $H(B_2) + \sum_{j=1}^{t-1} H(P_{l_j}) \geq (2(t-1)+1)H(S)$.
2. *If* $k_2 = t_2$, *then for any* $P_{l_1}, \ldots, P_{l_{t-1}} \in \mathcal{P}_1 \cap \mathcal{P}_2$, *where* $t = \min\{r, t_1 - k_1 + 1\}$, *it holds*
   $H(B_1) + \sum_{j=1}^{t-1} H(P_{l_j}) \geq (2(t-1)+1)H(S)$.

We now analyze the case in which the access structures in A consist of all possible distinct threshold structures on $\mathcal{P}$, that is, $\mathsf{A} = \{\mathcal{A}_{(k,\mathcal{P}')} \mid 1 \leq k \leq |\mathcal{P}'| \leq n \text{ and } \mathcal{P}' \subseteq \mathcal{P}\} \backslash \{\mathcal{A}_{(1,\mathcal{P})}\}$. From Theorem 13 there is no ideal secret sharing

scheme with broadcast message for A. A scheme based on a geometric construction (for an overview of geometric constructions for secret sharing schemes, the reader is advised to consult [13], see also [15] and [14]) is the following: Let q be a prime power, consider the $(n+1)$-dimensional vector space over $GF(q)$. Consider the $(n+1)$-dimensional affine geometry $AG(n+1,q)$. Let V_D be a fixed line in $AG(n+1,q)$ and let V_I be a hyperplane such that $|V_D \cap V_I| = 1$. The secret will be the point $s \in V_D \cap V_I$. Choose $2n$ points $y_1, y_2, \ldots, y_{2n} \in V_I$ such that no $n+1$ of the $2n+1$ points $y_1, y_2, \ldots, y_{2n}, s$ are collinear. For $i = 1, 2, \ldots, n$, give the point y_i to the participant P_i. The broadcast message $b_{k,\mathcal{P}'}$ that enables the access structure $\mathcal{A}_{(k,\mathcal{P}')}$ will be equal to

$$b_{k,\mathcal{P}'} = \Big(\bigcup_{1 \le i \le |\mathcal{P}'|-k+1} \{y_{n+i}\} \Big) \cup \Big(\bigcup_{P_i \notin \mathcal{P}'} \{y_i\} \Big).$$

It is easy to see that in the previous scheme for any P in $\mathcal{P}$ we have, $H(P) = (n+1)H(S)$. Moreover, the broadcast message $b_{k,\mathcal{P}'}$ that enables the access structure $\mathcal{A}_{(k,\mathcal{P}')}$ has entropy equal to $H(B_{k,\mathcal{P}'}) = (n-k+1)(n+1)H(S)$. With a slight modification of the previous scheme (using tecniques described in [16] and [10]), we can obtain a geometric scheme in which $H(P) = H(S)$.
The following algorithms describe a secret sharing scheme with broadcast message such that for all P in $\mathcal{P}$, $H(P) = H(S)$. We suppose that $S = GF(q)$, where $q \ge \max\{2n, m\} + 1$ is a prime power.

Threshold Preprocessing-Algorithm

Input: a prime power q and $\mathcal{P} = \{P_1, \ldots, P_n\}$.

For all $P_i \in \mathcal{P}$, randomly select $r_i \in GF(q)$ and set $a_i = r_i$ to be the share of $P_i \in \mathcal{P}$.

Output: The shares $a_1, \ldots, a_n$ for participants $P_1, \ldots, P_n$, respectively.

Threshold Message-Generation

Input: $s \in S = GF(q)$, $a_1, \ldots, a_n$, k, and $\mathcal{P}'$, such that $1 \le k \le |\mathcal{P}'| \le n$

Use a threshold scheme $(n+1, 2n)$ for the secret s to generate the shares $y_1, \ldots, y_{2n}$ in such a way that $y_i = a_i$, for $i = 1, \ldots, n$.
Compute

$$b_{k,\mathcal{P}'} = \Big(\bigcup_{1 \le i \le |\mathcal{P}'|-k+1} \{y_{n+i}\} \Big) \cup \Big(\bigcup_{P_i \notin \mathcal{P}'} \{a_i\} \Big).$$

Output: The broadcast message $b_{k,\mathcal{P}'}$ that enables the access structure $\mathcal{A}_{(k,\mathcal{P}')}$.

Notice that we can always construct the threshold scheme $(n+1, 2n)$ used in the *Message-Generation* algorithm. Indeed, we can use the threshold scheme proposed by Shamir [12]. We have to construct a polynomial $f(x)$ over $GF(q)$ of degree n such that $f(i) = y_i$, $i = 1, 2, \ldots, n$, and $f(0) = s$. This can be done by using the Lagrange interpolation. Thus, $f(i) = y_i$, $i = n+1, \ldots, 2n$. The broadcast message $b_{k,\mathcal{P}'}$ that enables the access structure $\mathcal{A}_{(k,\mathcal{P}')}$ has entropy

equal to $H(B_{k,\mathcal{P}'}) = (n-k+1)H(S)$. Moreover, the entropy of the shares of each participant $P \in \mathcal{P}$ is equal to $H(P) = H(S)$. Since each broadcast message $b_{k,\mathcal{P}'}$ consists of $n-k+1$ shares, every k participants in the threshold structure $\mathcal{A}_{(k,\mathcal{P}')}$ know $n+1$ shares and can reconstruct the secret s. But $k-1$, or less, participants are not able to recover the secret.
It is clear that the previous algorithm can be easily adapted to handle the case in which only a subset of all threshold structures can be activated by the broadcast message.

6 Fully Dynamic Secret Sharing Schemes

In previous sections we have analyzed the situation in which we have various access structures and by using a public message we enable one of them to recover the secret. A more interesting situation arises when we want to activate different access structures at subsequent times. At time i we want to enable an access structure $\mathcal{A}_{j_i}^{(i)}$, chosen in a fixed family $\mathsf{A}^{(i)}$, to recover the i-*th* secret s_i. The family $\mathsf{A}^{(i)}$ of access structures that can be enabled at time i may depend on the access structures activated at previous times. If $b_{j_1}^{(1)} \ldots b_{j_{i-1}}^{(i-1)}$ are the broadcast messages sent by the dealer from time 1 up to time $i-1$, then we should denote the family of access structures that can be enabled at time i by $\mathsf{A}_{j_1,\ldots,j_{i-1}}^{(i)}$ but to avoid overburdening the notation we will denote this family by $\mathsf{A}^{(i)}$.

Suppose that at time i the dealer enables the access structure $\mathcal{A}_{j_i}^{(i)}$. Thus, after the publication of all $i-1$ previous broadcast messages, the subsets of participants in $\mathcal{A}_{j_i}^{(i)}$ will recover the i-*th* secret after seeing the i-*th* broadcast message. Moreover, at time i each subset of participants knowing only the $i-1$ previous broadcast messages have no information on the secret s_i.

Suppose that we want to enable different access structures to reconstruct a secret a number of times, say T. Let $S^{(i)}$ be the set from which we choose the i-*th* secret, and $\mathsf{A}^{(i)} = \{\mathcal{A}_1^{(i)}, \ldots, \mathcal{A}_{m_i}^{(i)}\}$ be the family of possible access structures at time i, for $i = 1, 2, \ldots, T$. Denote by $\mathcal{P}^{(i)}$ the set of participants involved at time i and let $\mathcal{P} = \bigcup_{i=1}^{T} \mathcal{P}^{(i)}$. Denote by $\mathsf{B}^{(i)} = \{B_1^{(i)}, \ldots, B_{m_i}^{(i)}\}$ the family of all sets of broadcast messages for all possible access structures at time i. A fully dynamic secret sharing scheme is defined as follows.

Definition 16. Let $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ be families of monotone, non trivial access structures on $\mathcal{P}$. A *fully dynamic secret sharing scheme* is a sharing of secrets in $S^{(1)}, \ldots, S^{(T)}$ among participants in $\mathcal{P}$ such that

1. Before knowing the new broadcast message any subset of participants has no information about the new secret:
   Formally, for all $X \in 2^{\mathcal{P}}$, *for all* $i = 1, \ldots, T$, *and for all* $j_1, \ldots, j_{i-1}$, *where* $1 \le j_t \le m_t$, *it holds* $H(S^{(i)} | X B_{j_1}^{(1)} \ldots B_{j_{i-1}}^{(i-1)}) = H(S^{(i)})$.

2. After seeing the new broadcast message, we have a new perfect secret sharing scheme:
Formally, for all $i = 1, \ldots, T$, *for all* $X \in 2^{\mathcal{P}}$, *and for all* $j_1, \ldots, j_i$, *where* $1 \leq j_t \leq m_t$, *it holds*

$$H(S^{(i)}|XB_{j_1}^{(1)} \ldots B_{j_i}^{(i)}) = \begin{cases} H(S^{(i)}) & \text{if } X \notin \mathcal{A}_{j_i}^{(i)} \\ 0 & \text{if } X \in \mathcal{A}_{j_i}^{(i)} \end{cases}$$

The following theorem is a generalization to fully dynamic secret sharing schemes of Theorem 3

Theorem 17. *Let* $\Gamma^{(1)}, \ldots, \Gamma^{(T)}$ *be families of monotone access structures on a set* $\mathcal{P}$ *of participants. In any fully dynamic secret sharing scheme for* $i = 1, 2, \ldots, T$ *the following properties hold:*

1. *For any* $P \in \mathcal{P}^{(i)}$, *it holds* $H(P) \geq H(S^{(i)})$.
2. *For* $j = 1, 2, \ldots, m_i$, *it holds* $H(B_j^{(i)}) \geq H(S^{(i)})$.

Definition 16 says nothing on the sets X of participants such that $X \notin \mathcal{A}_{j_i}^{(i)}$ and that know all secrets $s_1, \ldots, s_{i-1}$ previously recovered. A natural requirement is that the information of these sets of participants have on the i-*th* secret s_i given the secrets $s_1, \ldots, s_{i-1}$, is equal to zero. That is, the knowledge of previous secrets does not give information about the i-*th* secret to all sets of participants not in $\mathcal{A}_j^{(i)}$. Next we define a *strong fully dynamic secret sharing scheme*, that is a fully dynamic secret sharing scheme with an additional property.

Definition 18. Let $\Gamma^{(1)}, \ldots, \Gamma^{(T)}$ be families of monotone, non trivial access structures on $\mathcal{P}$. A *strong fully dynamic secret sharing scheme* is a fully dynamic secret sharing scheme such that after seeing the new broadcast message, any subset of participants that is not in the new access structure, even knowing all the previous secrets, has no information about new secret:
Formally, for all $i = 1, \ldots, T$, for all $j_1, \ldots, j_i$, where $1 \leq j_t \leq m_t$, and for all $X \notin \mathcal{A}_{j_i}^{(i)}$, it holds

$$H(S^{(i)}|XB_{j_1}^{(1)} \ldots B_{j_i}^{(i)} S^{(1)} \ldots S^{(i-1)}) = H(S^{(i)}).$$

Notice that the property $H(S^{(i)}|XB_{j_1}^{(1)} \ldots B_{j_i}^{(i)} S^{(1)} \ldots S^{(i-1)}) = H(S^{(i)})$ in the above definition implies that $H(S^{(i)}|XB_{j_1}^{(1)} \ldots B_{j_i}^{(i)}) = H(S^{(i)})$ if $X \notin \mathcal{A}_{j_i}^{(i)}$ in Definition 16. In fact, for all $i = 1, \ldots, T$, for all $j_1, \ldots, j_i$, where $1 \leq j_t \leq m_t$, and for all $X \notin \mathcal{A}_{j_i}^{(i)}$ it holds

$$\begin{aligned} H(S^{(i)}) &\geq H(S^{(i)}|XB_{j_1}^{(1)} \ldots B_{j_i}^{(i)}) \\ &\geq H(S^{(i)}|XB_{j_1}^{(1)} \ldots B_{j_i}^{(i)} S^{(1)} \ldots S^{(i-1)}) \\ &= H(S^{(i)}). \end{aligned}$$

If the families of monotone access structures $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ satisfy some condition, then we can prove a lower bound on the size of shares held by a fixed participant. Next theorem holds.

Theorem 19. *Let $\mathcal{P}$ be a set of participants, $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ be families of monotone, non trivial access structures on $\mathcal{P}$. If there exist T indices $j_1, \ldots, j_T$, a participant $P \in \mathcal{P}$, and subsets of participants $X_i \subseteq \mathcal{P}$, $i = 1, \ldots, T$, such that*

- *$X_i \notin \mathcal{A}^{(i)}_{j_i}$, but $X_i \cup \{P\} \in \mathcal{A}^{(i)}_{j_i}$, for $i = 1, \ldots, T$,*
- *$X_i \subseteq X_{i+1}$, for $i = 1, \ldots, T-1$,*

then, in any strong fully dynamic secret sharing scheme for $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ the entropy of P satisfies

$$H(P) \geq \sum_{i=1}^{T} H(S^{(i)}).$$

We point out that Theorem 19 does not hold if we assume fully dynamic secret sharing schemes instead of strong fully dynamic secret sharing schemes.
As an example, consider the following situation. Let $\mathsf{A}^{(1)} = \{\mathcal{A}^{(1)}_1\}$ and $\mathsf{A}^{(2)} = \{\mathcal{A}^{(2)}_1\}$, be two families of monotone access structures on the set of participants $\mathcal{P} = \{P_1, P_2, P_3\}$, where $\mathcal{A}^{(1)}_1 = \{\{P_1P_2\}\}$ and $\mathcal{A}^{(2)}_1 = \{\{P_2P_3\}\}$. Suppose that at time 1 the dealer enables $\mathcal{A}^{(1)}_1$ to reconstruct the secret $s^{(1)}$ and at time 2 the dealer enables $\mathcal{A}^{(2)}_1$ to reconstruct the secret $s^{(2)}$. The following algorithms describe a fully dynamic secret sharing scheme for $\mathsf{A}^{(1)}$ and $\mathsf{A}^{(2)}$.

Preprocessing-Algorithm

Input: a prime power q, $\mathsf{A}^{(1)}$, $\mathsf{A}^{(2)}$, and $\mathcal{P} = \{P_1, P_2, P_3\}$.

For $i = 1, 2, 3$, randomly select $r_i \in GF(q)$ and set $a_i = r_i$ to be the share of $P_i \in \mathcal{P}$.

Output: The shares a_1, a_2, a_3 for participants P_1, P_2, P_3, respectively.

Message-Generation

Input: $s^{(1)}, s^{(2)} \in GF(q)$, $\mathsf{A}^{(1)}$, $\mathsf{A}^{(2)}$, and a_1, a_2, a_3.

Compute

$$b^{(1)}_1 = a_1 + a_2 + s^{(1)} \bmod q$$

and

$$b^{(2)}_1 = a_2 + a_3 + s^{(2)} \bmod q,$$

that are the broadcast messages for the two access structures $\mathcal{A}^{(1)}_1$ and $\mathcal{A}^{(2)}_1$.

Output: The broadcast messages $b^{(1)}_1$ and $b^{(2)}_1$.

The scheme above is a fully dynamic secret sharing scheme, but it is not a strong one. In fact, it is easy to see that

$$H(S^{(2)} | P_1 P_3 B^{(1)}_1 B^{(2)}_1 S^{(1)}) = 0, \text{ but } \{P_1P_3\} \notin \mathcal{A}^{(2)}_1.$$

The scheme above satisfies the remaining hypothesis of Theorem 19 by setting $P = P_2$, $X_1 = \{P_1\}$ and $X_2 = \{P_1, P_3\}$. On the other hand, we have $H(P_2) = H(S^{(1)}) = H(S^{(2)})$, thus

$$H(P_2) < H(S^{(1)}) + H(S^{(2)}).$$

The following corollaries hold.

Corollary 20. *Let $\mathcal{P}$ be a set of participants and let $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ be families of monotone, non trivial access structures on $\mathcal{P}$ such that $\mathcal{A}_{(k_i, \mathcal{P}_i)} \in \mathsf{A}^{(i)}$, for $i = 1, 2, \ldots, T$. If $k_1 \leq k_2 \leq \cdots \leq k_T$ and $\mathcal{P}_1 \subseteq \mathcal{P}_2 \subseteq \cdots \subseteq \mathcal{P}_T$ then the entropy of any participant $P \in \mathcal{P}_1$ satisfies*

$$H(P) \geq \sum_{i=1}^{T} H(S^{(i)}).$$

Corollary 21. *Let $\mathcal{P}$ be a set of n participants and k an integer, $1 \leq k \leq n$. Let $\mathsf{A}^{(0)}, \ldots, \mathsf{A}^{(T)}$, $1 \leq T \leq n - k$ be families of monotone, non trivial access structures on $\mathcal{P}$ such that $\mathcal{A}_{(k, \mathcal{P}_\ell)} \in \mathsf{A}^{(\ell)}$, for $\ell = 0, 1, \ldots, T$, where $\mathcal{P} = \mathcal{P}_0 \supseteq \mathcal{P}_1 \supseteq \cdots \supseteq \mathcal{P}_T$, and $|\mathcal{P}_\ell| = |\mathcal{P}_{\ell-1}| - 1$ for $\ell = 1, \ldots, T$. Then, in any strong fully dynamic secret sharing scheme for $\mathsf{A}^{(0)}, \ldots, \mathsf{A}^{(T)}$ the entropy of any participant $P \in \mathcal{P}_T$ satisfies*

$$H(P) \geq \sum_{i=0}^{T} H(S^{(i)}).$$

A particular class of strong fully dynamic secret sharing scheme which satisfies the hypothesis of Corollary 21 are (k, n) threshold schemes with disenrollment [1]. At each subsequent time instant we disenroll a participant from the scheme, but the threshold of the new scheme remains unchanged. Thus, in any (k, n) threshold scheme with L-fold disenrollment capability (as defined in [1]), with $0 \leq L \leq n - k$, for any participant $P \in \mathcal{P}$, it holds $H(P) \geq \sum_{i=0}^{L} H(S^{(i)})$.

References

1. B. Blakley, G. R. Blakley, A. H. Chan, and J. Massey, *Threshold Schemes with Disenrollment*, in "Advances in Cryptology - CRYPTO '92", Ed. E. Brickell, "Lecture Notes in Computer Science", Springer-Verlag.
2. G. R. Blakley, *Safeguarding Cryptographic Keys*, Proceedings AFIPS 1979 National Computer Conference, pp.313–317, June 1979.
3. C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, *On the Information Rate of Secret Sharing Schemes*, in "Advances in Cryptology - CRYPTO '92", Ed. E. Brickell, "Lecture Notes in Computer Science", Springer-Verlag.

4. C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, *Graph Decomposition and Secret Sharing Schemes*, in "Advances in Cryptology – Eurocrypt '92", Lecture Notes in Computer Science, Vol. 658, R. Rueppel Ed., Springer-Verlag, pp. 1–24, 1993.
5. E. F. Brickell and D. M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, J. Cryptology, Vol. 4, No. 2, pp. 123–134, 1991.
6. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, *On the Size of Shares for Secret Sharing Schemes*, Journal of Cryptology, Vol. 6, No. 3, pp. 157-169, 1993.
7. O. Goldreich, S. Micali, and A. Wigderson, *How to Play any Mental Game*, Proceedings of 19th ACM Symp. on Theory of Computing, pp. 218–229, 1987.
8. L. Harn, T. Hwang, C. Laih, and J. Lee, *Dynamic Threshold Scheme based on the definition of Cross-Product in a N-dimensional Linear Space* in "Advances in Cryptology - Eurocrypt '89", Lecture Notes in Computer Science, Vol. 435, J. Brassard Ed., Springer-Verlag, pp. 286–298.
9. E. D. Karnin, J. W. Greene, and M. E. Hellman, *On Secret Sharing Systems*, IEEE Trans. on Inform. Theory, Vol. IT-29, no. 1, pp. 35–41, Jan. 1983.
10. K. Martin, *Discrete Structures in the Theory of Secret Sharing*, PhD Thesis, University of London, 1991.
11. K. Martin, *Untrustworthy Participants in Perfect Secret Sharing Schemes*, Proceedings of the 3rd IMA Conference on Coding and Cryptology, 1992.
12. A. Shamir, *How to Share a Secret*, Communications of the ACM, Vol. 22, n. 11, pp. 612–613, Nov. 1979.
13. G. J. Simmons, *An Introduction to Shared Secret and/or Shared Control Schemes and Their Application*, Contemporary Cryptology, IEEE Press, pp. 441–497, 1991.
14. G. J. Simmons, *How to (Really) Share a Secret*, in "Advances in Cryptology - CRYPTO 88", Ed. S. Goldwasser, "Lecture Notes in Computer Science", Springer-Verlag.
15. G. J. Simmons, W. Jackson, and K. Martin, *The Geometry of Shared Secret Schemes*, Bulletin of the ICA, Vol. 1, pp. 71–88, 1991.
16. D. R. Stinson, *An Explication of Secret Sharing Schemes*, Design, Codes and Cryptography, Vol. 2, pp. 357–390, 1992.
17. D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, Technical Report UNL-CSE-92-020, Department of Computer Science and Engineering, University of Nebraska, September 1992.