Fully Dynamic Secret Sharing Schemes *

Carlo Blundo,[1] Antonella Cresti,[2] Alfredo De Santis,[1] and Ugo 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 is 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 them the same broadcast message. In this paper we establish a formal setting to study secret sharing schemes of this kind. 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, on the size of the broadcast message, and on the randomness needed 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 [11] for example). We refer the reader to the excellent survey papers [21] and [24] for a detailed discussion of secret sharing schemes and for a complete bibliography on the argument.

Simmons [21] first 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 reconstruct different secrets (in different time instants) simply by sending to all participants the same broadcast message. Harn, Hwang, Laih, and Lee [12] gave an algorithm to construct 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 the dealer could enable participants

*Partially supported by Italian Ministry of University and Research (M.U.R.S.T.) and by National Council for Research (C.N.R.). A preliminary version of this paper has been presented at Crypto '93.

to recover different secrets in different time instants simply by sending the same broadcast message to all of them. However, the authors of [12] assumed that the access structure remained the same in each time instant. Martin [19] presented a technique to realize secret sharing schemes for general access structures in which, by sending a broadcast message to all participants, a new secret is activated and a participant is disenrolled from the scheme. Blakley, Blakley, Chan, and Massey [2] considered the problem of constructing threshold secret sharing schemes with disenrollment capability, but the value of the threshold of the secret sharing schemes is not changed at each disenrollment. Moreover, they gave a lower bound on the size of the shares held by each participant in such schemes.

The problem of evaluating the size of the shares to be given to participants is among the most important problems in the area of secret sharing schemes. Recently, the problem of estimating the amount of random bits necessary to set up the schemes has received considerably attention. The first problem is strictly related to the security of the schemes, since the security of any system degrades as the amount of secret information increases. The problem of estimating the number of random bits necessary to implement randomized algorithms is receiving considerable interest (see [13], [17], for example). This is due to the fact that the amount of randomness needed by an algorithm is to be considered a computational resource, analogously to the amount of time and space needed. The quantitative study of the number of random bits needed by secret sharing schemes has been initiated in [6], where the optimality of several secret sharing schemes according to this measure has been proved. Some other results on this topic can be found in [3].

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 separately the problem of bounding the size of the share of the participant and that of the broadcast message (see Theorem 4.5 and Theorem 4.6). Motivated by this result we define *Ideal Secret Sharing Schemes with Broadcast Message* 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 7 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 [2]. In Section 8 we analyze the randomness needed to set up secret sharing schemes with broadcast message and we give protocols that are optimal to this respect.

2 Secret Sharing

A secret sharing scheme permits a secret to be shared among a set $\mathcal{P}$ of n participants in such a way that only qualified subsets of $\mathcal{P}$ can recover the secret, but any non-qualified subset has absolutely no information on the secret. An access structure $\mathcal{A}$ is the set of all subsets of $\mathcal{P}$ that can recover the secret. In this paper we require that any considered access structure $\mathcal{A}$ be *monotone*, that is if $A \in \mathcal{A}$ and $A \subseteq A' \subseteq \mathcal{P}$, then $A' \in \mathcal{A}$.

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 Σ 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. Suppose a *dealer* D wants to share the secret $s \in S$ among the participants in $\mathcal{P}$ (we will assume that $D \notin \mathcal{P}$). He does this by giving each participant $P \in \mathcal{P}$ a share from $K(P)$ chosen according to some, non necessarily uniform, probability distribution. Given a set of participants $A = \{P_{i_1}, \ldots, P_{i_r}\} \subseteq \mathcal{P}$, where $i_1 < i_2 < \cdots < i_r$, denote by $K(A) = K(P_{i_1}) \times \cdots \times K(P_{i_r})$.

We represent, as in [25], a *perfect* secret sharing scheme, or simply a secret sharing scheme, Σ by a collection of distribution rules. A *distribution rule* is a function

$$f : \mathcal{P} \cup \{D\} \to K(\mathcal{P}) \cup S$$

which satisfies the conditions $f(D) \in S$ and $f(P_i) \in K(P_i)$, for $i = 1, 2, \ldots, n$. A distribution rule f represents a possible distribution of shares to the participants, where $f(D)$ is the secret being shared, and $f(P_i)$ is the share given to P_i. If $s \in S$ is the value of the secret that D wants to share, then D will randomly choose a distribution rule f among all distribution rules having s as the secret, that is $f \in \{f \in \mathcal{F} \ : \ f(D) = s\}$, according to some probability distribution, and use f to distribute shares to the participants.

The family of distribution rules $\mathcal{F}$ can also be depicted as a matrix M, each row of which corresponds to one distribution rule. One column of M will be indexed by D, and the remaining columns are indexed by the members of $\mathcal{P}$.

Any secret sharing scheme 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 $H(S) = -\sum_{s\in S} p_S(s) \log p_S(s)$ the entropy[1] of $\{p_S(s)\}_{s\in S}$ and by $H(A) = -\sum_{a\in K(A)} p_{K(A)}(a) \log p_{K(A)}(a)$ the entropy of $\{p_{K(A)}(a)\}_{a\in K(A)}$, for any $A \subseteq \mathcal{P}$.

Following the approach of [14], [16], and [8] we define secret sharing schemes using the information measures listed in Appendix A. Therefore, we say that a perfect secret sharing scheme, or simply a secret sharing scheme, is a sharing of the secrets in S among participants in $\mathcal{P}$ such that

1. *Any subset $A \subseteq \mathcal{P}$ of participants enabled to recover the secret can compute the secret:* Formally, for all $A \in \mathcal{A}$, it holds that $H(S|A) = 0$.

2. *Any subset $A \subseteq \mathcal{P}$ of participants not enabled to recover the secret has no information on the secret value:*
   Formally, for all $A \notin \mathcal{A}$, it holds that $H(S|A) = H(S)$.

3 Secret Sharing Schemes with Broadcast Message

In this section we define secret sharing schemes with broadcast message. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of participants. Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of monotone access structures

[1] For definition and properties of information theoretic quantities that we will use in this paper see Appendix A.

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 $\mathcal{P}$. Afterward, in the message-generation phase, the dealer having in 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: S, $\{p_S(s)\}_{s\in S}$, $\mathcal{P} = \{P_1, \ldots, P_n\}$, 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 once for all 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 7.

We assume that the considered 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., $\emptyset \notin \mathcal{A}$.

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 $\mathcal{A}$. The access structure $\mathcal{A}$ is uniquely determined as a function of $\mathcal{A}^0$, since 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 $\mathcal{A} = \mathsf{cl}(\mathcal{A}^0)$.

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 distinct access structures on $\mathcal{P}$. For $1 \leq j \leq m$, let $\mathcal{P}_j = \bigcup_{X\in\mathcal{A}_j^0} X$. We will refer to a participant $P \in \mathcal{P}$ as an *essential* participant if there exist a set $X \subseteq \mathcal{P}$ and an index i such that $X \cup \{P\} \in \mathcal{A}_i^0$. If a participant P in not essential then we can construct a secret sharing scheme with broadcast message giving him nothing as share. In this paper we assume that the set of participants $\mathcal{P}$ consists only of essential participants. Moreover, we suppose that the family of access structures A is different from the trivial one, i.e., $\mathsf{A} \neq \{\mathsf{cl}(\{\{P_1\}, \ldots, \{P_n\}\})\}$. Indeed, to realize a secret sharing scheme with broadcast message for A the dealer hands out to participants nothing as share and, in the Message-Generation phase, he distributes the secret itself as broadcast message.

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. Analogously to the case of secret sharing scheme without broadcast message, for any participant $P \in \mathcal{P}$, we 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 with $K(A)$ 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 $\{p_S(s)\}_{s\in S}$ induce a probability distribution on $K(A)$, for any $A \subseteq \mathcal{P}$. Denote such a 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 $\mathcal{E}(B_i)$ 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 $\mathcal{E}(B_i)$. Denote such a probability distribution by $\{p_{\mathcal{E}(B_i)}(b)\}_{b \in \mathcal{E}(B_i)}$. Finally, for all $1 \leq i \leq m$, denote by $H(B_i)$ the entropy of $\{p_{\mathcal{E}(B_i)}(b)\}_{b \in \mathcal{E}(B_i)}$.

By using the entropy approach, as done in [14], [16], and [8] for usual secret sharing schemes, we define a secret sharing scheme with broadcast message as follows.

Definition 3.1 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of access structures on* $\mathcal{P}$. *A* secret sharing scheme with broadcast message *is a distribution 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 that $H(S|X) = H(S)$.

2. *After seeing a broadcast message in* $\mathcal{E}(B_i)$, *we have a secret sharing scheme for the access structure* $\mathcal{A}_i$*:*
   Formally, for any $\mathcal{A}_i \in \mathsf{A}$ and for any $X \in 2^{\mathcal{P}}$, it holds that

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

Notice that the condition $H(S|X) = H(S)$ is equivalent to state that S and X are statistically independent, i.e., for all $x \in K(X)$ and for all $s \in S$, it results $p(s|x) = p_S(s)$ and therefore the knowledge of x gives no information about the secret. Equivalently, the condition $H(S|XB_i) = H(S)$ means that S and XB_i are statistically independent. Moreover, the condition $H(S|XB_i) = 0$ means that each set of values of the shares and broadcast message in $K(X) \times \mathcal{E}(B_i)$ 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 $b \in \mathcal{E}(B_i)$ 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 us denote with $\mathcal{A}_i^B$ the family $\mathcal{A}_i^B = \{X \cup \{B_i\} | X \in \mathcal{A}_i\}$, that is, $\mathcal{A}_i^B$ contains all the sets in the access structure $\mathcal{A}_i$ that can reconstruct the secret once they know the broadcast message b_i that enables $\mathcal{A}_i$. 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 $\mathcal{P} = \{P_1, P_2, \ldots, P_6\}$ be the set of participants. Suppose the family A contains three access structures $\mathcal{A}_1 = \mathsf{cl}(\{\{P_1, P_2\}, \{P_2, P_3\}\})$, $\mathcal{A}_2 = \mathsf{cl}(\{\{P_3, P_4\}\})$, and $\mathcal{A}_3 = \mathsf{cl}(\{\{P_4, P_5\}, \{P_5, P_6\}\})$. The family of all bases is depicted in Figure 1. The following algorithms realize a secret sharing scheme with broadcast message for A when the secret is uniformly chosen in $\mathbf{Z}_q$, with U_q we denote the uniform probability distribution on $\mathbf{Z}_q$.

Preprocessing-Algorithm

Input: $\mathbf{Z}_q$, U_q, $\mathcal{P} = \{P_1, \ldots, P_6\}$, and $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$.

Randomly select $r_1, r_2, r_3, r_4, r_5, r_6 \in \mathbf{Z}_q$.
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: $s \in \mathbf{Z}_q$, $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$, $a_1, \ldots, a_6$, and $i \in \{1, 2, 3\}$.

Let $a_1 = r_1$, $a_2 = r_2$, $a_3 = (r_1, r_3)$, $a_4 = (r_4, r_5)$, $a_5 = r_6$, and $a_6 = r_5$.
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 the access structure $\mathcal{A}_i$.

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

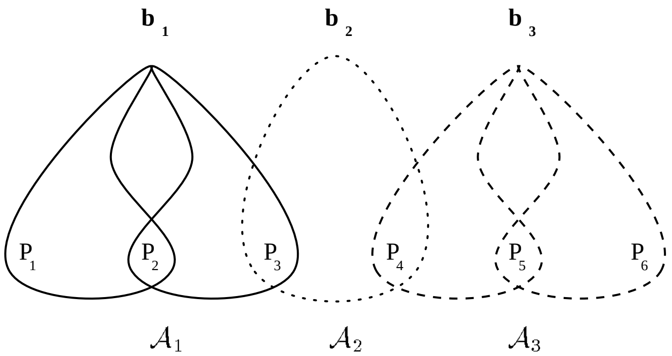

Figure 1.

4 The Size of Shares

The problem of establishing bounds on the size of the shares to be given to participants in secret sharing schemes is one of the basic problem in the area and has received considerable attention by several researchers. The practical relevance of this issue is based on the following observations: Firstly, the security of any system tends to degrade as the amount of information that must be kept secret, i.e., the shares of the participants, increases. Secondly, if the shares given to participants are too long, the memory requirements for the participants will be too severe and, at the same time, the shares distribution algorithms will become inefficient. Therefore, one important problem is to analyze the amount of information that each participant must keep secret. We will prove a basic bound stating that in any secret sharing scheme 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.[2] 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 that of the secret, as we will see in Section 6.

The following lemmas are a generalization to secret sharing schemes with broadcast message of the results proved in [8] for secret sharing schemes with no broadcast message.

Lemma 4.1 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of access structures on a set* $\mathcal{P}$ *of participants. Let* $i \in [1, \ldots, m]$*, 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: Let $Y \in 2^{\mathcal{P}\cup\{B_i\}} \backslash \mathcal{A}_i^B$, 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 3.1. If $B_i \in Y$, then $H(S|Y) = H(S)$ because of property 2 of Definition 3.1 since $Y \backslash \{B_i\} \notin \mathcal{A}_i$. Now, consider the conditional mutual information $I(X; S|Y)$, that 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 and property (4) (see Appendix *A*) we get the following theorem.

Theorem 4.2 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of 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 participant* $P \in \mathcal{P}$*, it holds that* $H(P) \geq H(S)$*.*
2. *For* $i = 1, 2, \ldots, m$*, it holds that* $H(B_i) \geq H(S)$*.*

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

Theorem 4.3 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of access structures on a set* $\mathcal{P}$ *of participants. If the secret is 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 that* $\log |K(P)| \geq \log |S|$*.*
2. *For* $i = 1, 2, \ldots, m$*, it holds that* $\log |\mathcal{E}(B_i)| \geq \log |S|$*.*

Next lemma implies that the uncertainty on shares of participants in $X \notin \mathcal{A}_i$ cannot be decreased by the knowledge of the secret.

[2] As customarily, we measure both the size of the shares and the size of the broadcast message with the logarithm of the size of the sets from which they are taken, that is, by the number of bits necessary to their representation.

Lemma 4.4 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of access structures on a set* $\mathcal{P}$ *of participants. Let* $i \in [1, \ldots, m]$, *if* $X \cup Y \in 2^{\mathcal{P} \cup \{B_i\}} \setminus \mathcal{A}_i^B$, *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, $H(Y|X) = H(Y|XS) + H(S|X) - H(S|XY)$. Since $X \cup Y \notin \mathcal{A}_i^B$ we have $H(S|XY) = H(S|X) = H(S)$. Hence, $H(Y|X) = H(Y|XS)$. $\square$

Next theorems prove that the bounds given in Theorem 4.3 are optimal if considered separately. More precisely, we will prove that for any family of access structures there exist 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 section are all realized by considering uniform distributions on $S = \mathbf{Z}_q$, where $q \geq 2$.

Theorem 4.5 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of access structures on a set of participants* $\mathcal{P}$ *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 the entropy of the shares given to participant* P *satisfies*

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

Proof: We describe a secret sharing scheme with broadcast message that satisfies the property above for a participant $P_k \in \mathcal{P}$.

Preprocessing-Algorithm

Input: $\mathbf{Z}_q$, U_q, $\mathcal{P} = \{P_1, \ldots, P_n\}$, $P_k \in \mathcal{P}$, and $\mathcal{A}_1, \ldots, \mathcal{A}_m$. Randomly select $r \in \mathbf{Z}_q$.
Let $a_k = r$ be the share of P_k.
For $1 \leq i \leq m$, for any $Y \in \mathcal{A}_i$, and for any $P_j \in Y \setminus \{P_k\}$ randomly select $y_{i,Y,j} \in \mathbf{Z}_q$.
For all $P_j \in \mathcal{P} \setminus \{P_k\}$ compute

$$a_j = \bigcup_{i=1}^{m} \bigcup_{Y \in \mathcal{A}_i^0} \{y_{i,Y,j}\}.$$

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

Message-Generation

Input: $s \in S = \mathbf{Z}_q$, $\mathcal{A}_1, \ldots, \mathcal{A}_m$, $a_1, \ldots, a_n$, and $i \in \{1, 2, \ldots, m\}$.
For the access structure $\mathcal{A}_i$ compute

$$b_i = \bigcup_{Y \in \mathcal{A}_i^0} \{s + \sum_{j \,:\, P_j \in Y} y_{i,Y,j} \mod q\}$$

where $y_{i,Y,k} = a_k$ if $P_k \in Y$ and $Y \in \mathcal{A}_i^0$.
Output: The broadcast message b_i enabling the access structures $\mathcal{A}_i$.

It is not difficult to see that the previous protocols realize a secret sharing scheme with broadcast message. Indeed, before knowing the broadcast message any subset of participants has no information about the value of the secret; once the dealer distributes the broadcast message b_i only the participants in $Y \in \mathcal{A}_i^0$ can recover the secret s. Given the broadcast message b_i, the participants in $Y \in \mathcal{A}_i^0$ can first obtain $s + \sum_{P_j \in Y} y_{i,Y,j} \mod q$. From the preprocessing phase they can compute $\sum_{P_j \in Y} y_{i,Y,j} \mod q$ from which they get the secret $s \in S$. $\square$

In Section 3 we presented a scheme for the family of access structures $\mathsf{A} = \{\mathsf{cl}(\{\{P_1, P_2\}, \{P_2, P_3\}\}), \mathsf{cl}(\{\{P_3, P_4\}\}), \mathsf{cl}(\{\{P_4, P_5\}, \{P_5, P_6\}\})\}$ on the set of participants $\mathcal{P} = \{P_1, ..., P_6\}$. In such a scheme participants P_3 and P_4 get a share whose size is twice the size of the secret. By using the algorithms presented in the previous theorem 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 share whose size is equal to the size of the secret is the following, when it is assumed that the secret is uniformly chosen in $\mathbf{Z}_q$, where $q \geq 2$.

Preprocessing-Algorithm

Input: $\mathbf{Z}_q$, U_q, $\mathcal{P} = \{P_1, \ldots, P_6\}$, and $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$.

Randomly select $r_1, r_2, \ldots, r_9 \in \mathbf{Z}_q$.
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: $s \in S = \mathbf{Z}_q$, $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$, $a_1, \ldots, a_6$, and $i \in \{1, 2, 3\}$.

Let $a_1 = r_1$, $a_2 = (r_2, r_3)$, $a_3 = r_4$, $a_4 = (r_5, r_6)$, $a_5 = (r_7, r_8)$, and $a_6 = r_9$.
Compute $b_1 = (s + r_1 + r_2 \mod q,\ s + r_3 + r_4 \mod q)$, $b_2 = s + r_4 + r_5 \mod q$, and

$b_3 = (r_6 + r_7 \mod q,\ s + r_8 + r_9 \mod q)$.

Output: The broadcast message b_i enabling 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 proves that for any family of access structures there exists a secret sharing scheme with broadcast message such that the size of the broadcast messages is the same than that of the secret.

Theorem 4.6 *Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of access structures on a set of participants $\mathcal{P}$. If the secret is uniformly chosen then there exists a secret sharing scheme with broadcast message such that, for all $j \in \{1, 2, \ldots, m\}$, the entropy of B_j satisfies*

$$H(B_j) = H(S).$$

Proof: We describe a secret sharing scheme with broadcast message that satisfies the property above. For each $j = 1, 2, \ldots, m$, let Σ_j be a secret sharing scheme for the access structure $\mathcal{A}_j$ for secrets chosen in $\mathbf{Z}_q$.

Preprocessing-Algorithm

Input: $\mathbf{Z}_q$, U_q, $\mathcal{P} = \{P_1, \ldots, P_n\}$, and $\mathcal{A}_1, \ldots, \mathcal{A}_m$.
Randomly select $x_1, x_2, \ldots, x_m \in \mathbf{Z}_q$.
For each access structure $\mathcal{A}_i$, with $i = 1, 2, \ldots, m$, let $y_{i,j}$ be the share given to the participant $P_j \in \mathcal{P}_i$, when we share the value x_i by using the scheme Σ_i.
For all $P_j \in \mathcal{P}$ compute

$$a_j = \bigcup_{i\,:\,P_j \in \mathcal{P}_i} \{y_{i,j}\}.$$

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

Message-Generation

Input: $s \in S = \mathbf{Z}_q$, $\mathcal{A}_1, \ldots, \mathcal{A}_m$, $a_1, \ldots, a_n$, and $i \in \{1, 2, \ldots, m\}$.
Let $a_j = \bigcup_{i\,:\,P_j \in \mathcal{P}_i} \{y_{i,j}\}$, for $j = 1, 2, \ldots, n$.
Let x_i be secret corresponding to the shares $y_{i,1}, y_{i,2}, \ldots, y_{i,n}$ in the scheme Σ_i.
Let $b_i = s + x_i \bmod q$.
Output: The broadcast message b_i that enables the access structures $\mathcal{A}_i$.

It is not difficult to see that the previous protocols realize a secret sharing scheme with broadcast message. Moreover, in the previous protocols we have that $H(B_j) = H(S)$, where $j = 1, 2, \ldots, m$. $\square$

5 Ideal Schemes

In the previous section we have seen that for any family of access structures A either the share 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 that $H(P) = H(B_i) = H(S)$. That is, we consider schemes in which both the broadcast messages and the shares of participants have the same dimension than that of the secret. We will use the following lemma that is a slight extension of Theorem 4.1 proved in [8], we omit the proof since it is completely similar to that given in [8].

Lemma 5.1 *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 $H(BC|F) \geq 3H(S|F)$.

In analogy with secret sharing schemes without broadcast message [7], we define *ideal*[3] secret sharing schemes with broadcast message as follows.

[3] From Theorem 4.2 it turns out that we get an optimal situation when $H(P) = H(B) = H(S)$, for any participant P and broadcast message B, hence the term ideal.

Definition 5.2 *Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of 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 $\mathsf{A} = \{\mathcal{A}_1\}$.

Theorem 5.3 *Assume that the secret is uniformly chosen in $S = \mathbf{Z}_q$, $q \geq 2$. An ideal secret sharing scheme with broadcast message for $\mathsf{A} = \{\mathcal{A}_1\}$, where $S = \mathbf{Z}_q$, exists if and only if there exists an ideal secret sharing scheme for the access structure $\mathcal{A}_1$, where $S = \mathbf{Z}_q$.*

Proof: Suppose that there exists an ideal secret sharing scheme Σ with broadcast message for A. Given a non-zero probability broadcast message $b \in \mathcal{E}(B_1)$, consider the following scheme Σ^b for $\mathcal{A}_1$ when the probability distribution on S is uniform. For any possible broadcast message b consider the scheme Σ^b obtained by considering only the distribution rules dealing with b as broadcast message. In the scheme Σ^b the dealer hands out to the participants of $\mathcal{A}_1$ the same shares as he would distributed in Σ conditioned on the fact that the the broadcast message is b. The scheme Σ^b is a secret sharing scheme for $\mathcal{A}_1$, in fact since b is a broadcast message, if $X \notin \mathcal{A}_1$ then $H(S|X) = H(S)$ and if $X \in \mathcal{A}_1$ then $H(S|X) = 0$. Is is immediate to see that for any value b the secret sharing scheme Σ^b is ideal. Suppose, on the other hand, that an ideal secret sharing scheme Σ', with secrets in $\mathbf{Z}_q$, for $\mathcal{A}_1$ exists. Then, use it to distribute among the participants in $\mathcal{P}$ a value x randomly chosen in $\mathbf{Z}_q$. The broadcast message will be $b_1 = s + x \bmod q$. The shares of participants in the scheme for A will be the shares distributed to participant by using the ideal scheme Σ'. Clearly this is an ideal secret sharing scheme with broadcast message for A. $\square$

Therefore, the classification of ideal secret sharing schemes with no broadcast messages given in [7] applies also to secret sharing schemes with broadcast message.

Recall that, for $1 \leq j \leq m$, $\mathcal{P}_j = \bigcup_{X \in \mathcal{A}_j^0} X$.

Definition 5.4 *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*

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

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*. Suppose that $\mathcal{A}_1$ and $\mathcal{A}_2$ are not connected. If $\mathcal{A}_l \neq \mathsf{cl}(\{\{P_i\} : P_i \in \mathcal{P}_l\})$, for $l = 1, 2$, then there exists an ideal secret sharing scheme with broadcast message for $\mathsf{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$, where $S = \mathbf{Z}_q$, if and only if it exists an ideal secret sharing scheme with broadcast message for both $\mathsf{A}_1 = \{\mathcal{A}_1\}$ and $\mathsf{A}_2 = \{\mathcal{A}_2\}$, where $S = \mathbf{Z}_q$. If $\mathcal{A}_1 = \mathsf{cl}(\{\{P_i\} : P_i \in \mathcal{P}_1\})$ and $\mathcal{A}_2 \neq \mathsf{cl}(\{\{P_i\} : P_i \in \mathcal{P}_2\})$, then it is easy to see that there exists an ideal secret sharing scheme with broadcast message for $\mathsf{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$, where $S = \mathbf{Z}_q$, if and only if there exists an ideal secret sharing scheme with broadcast message for $\mathsf{A}_2 = \{\mathcal{A}_2\}$, where $S = \mathbf{Z}_q$. (To the participants $P_i \in \mathcal{P}_1$ the dealer distributes a randomly chosen value $x \in \mathbf{Z}_q$, and when he wants to share a secret s he distributes the broadcast message $x + s \bmod q$.) Finally, if $\mathcal{A}_l = \mathsf{cl}(\{\{P_i\} : P_i \in \mathcal{P}_l\})$, for $l = 1, 2$, and $\mathcal{A}_l \neq \mathcal{A}_2$ then there exists an ideal secret sharing scheme with broadcast message for $\mathsf{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$, where $S = \mathbf{Z}_q$.

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.

The following lemma, due to Brickell and Davenport [7], holds for any ideal secret sharing scheme. We will use it in the next theorem.

Lemma 5.5 *Let $\mathcal{A}$ be an access structure. If there exists an ideal secret sharing scheme for $\mathcal{A}$, where S is the set of the secrets, then for any $A \in \mathcal{A}_0$, the set $K(A)$ of the possible shares for A is $S^{|A|}$.*

The following corollary is an immediate consequence.

Corollary 5.6 *Let $\mathcal{A}$ be an access structure. Suppose there exists an ideal secret sharing scheme for $\mathcal{A}$, where $S = \mathbf{Z}_q$. Then, for any $B \subseteq A$, where $A \in \mathcal{A}_0$, the set $K(B)$ of the possible shares for B is $\mathbf{Z}_q^{|B|}$.*

Theorem 5.7 *Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of m connected access structures pairwise compatible. Suppose that, for each $\mathcal{A}_i$, with $i = 1, \ldots, m$, there exists an ideal secret sharing scheme with broadcast message where $S = \mathbf{Z}_q$, $q \geq 2$. If the secret is uniformly chosen, then there exists an ideal secret sharing scheme with broadcast message for A where $S = \mathbf{Z}_q$.*

Proof: Consider an access structure $\mathcal{A}$ on the set of participants $\mathcal{P}'$ and suppose that there exists an ideal scheme Σ, represented by a family of distribution rules $\mathcal{F}$, when the secrets are randomly chosen in $\mathbf{Z}_q$. If we randomly choose the shares of the participants in $I = \cap_{X \in \mathcal{A}^0} X$, say the participant $P_{i_j} \in I$ receives the share y_{i_j}, then, from Corollary 5.6 there exists at least one distribution rule $f \in \mathcal{F}$ such that $f(P_{i_j}) = y_{i_j}$, for $j = 1, 2, \ldots, |I|$. The following Preprocessing-Algorithm is based on the previous observation. Hence, we randomly choose the share of any participant belonging to at least two access structures in A (remember that the access structures in A are pairwise compatible), then we distribute the shares to the remaining participants accordingly to the distribution rules that agree on the shares previously distributed. The Message-Generation algorithm is realized accordingly. The algorithms realizing a secret sharing scheme with broadcast message for A, with secrets in $\mathbf{Z}_q$, are the following.

Preprocessing-Algorithm

Input: $S = \mathbf{Z}_q$, U_q, $\{P_1, P_2, \ldots, P_n\}$, and $\mathcal{A}_1, \ldots, \mathcal{A}_m$.
Let, w.l.o.g., $P_1, \ldots, P_r$ be all participants in at least two access structures in A.
For $1 \leq j \leq m$, let Σ_j an ideal secret sharing scheme for the access structure $\mathcal{A}_j$ represented by the family of distribution rules $\mathcal{F}_j$.

For $1 \leq j \leq r$

randomly select $r_j \in \mathbf{Z}_q$

let $a_j = r_j$ be the share of participant P_j.

For $1 \leq j \leq m$

if $\mathcal{P}_j \not\subseteq \{P_1, \ldots, P_r\}$ then

Randomly choose $f \in \mathcal{F}_j$ such that $f(P_i) = r_i$, for all $P_i \in \mathcal{P}_j$ and $1 \leq i \leq r$.

Let $x_j = f(D)$.

For all $P_i \in \mathcal{P}_j \setminus \{P_1, \ldots, P_r\}$, let $a_i = f(P_i)$.

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

Message-Generation

Input: $s \in S = \mathbf{Z}_q$, $\mathcal{A}_1, \ldots, \mathcal{A}_m$, $a_1, \ldots, a_n$, $x_1, \ldots, x_r$, $P_1, \ldots, P_r$, and $i \in \{1, 2, \ldots, m\}$.
For $1 \leq j \leq m$

If $\mathcal{P}_j \not\subseteq \{P_1, \ldots, P_r\}$ then

Let $b_j = s + x_j \bmod q$ be the broadcast message for $\mathcal{A}_j \in \mathsf{A}$.

else

Let $b_j = s + \sum_{P_i \in \mathcal{P}_j} a_j \bmod q$ be the broadcast message for $\mathcal{A}_j \in \mathsf{A}$.

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

These algorithms realize an ideal secret sharing scheme with broadcast message for A. In fact, if $\mathcal{P}_j \not\subseteq \{P_1, \ldots, P_r\}$, then the participants in $Y \in \mathcal{A}_i^0$ know $b_j = s + x_j \bmod q$. They can compute x_j from their shares and thus get $s \in S$. The same arguments apply in case of $\mathcal{P}_j \subseteq \{P_1, \ldots, P_r\}$. Moreover, both the size of the shares given to participants and the size of the broadcast message are the same than the size of the secret. $\square$

6 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 $\mathcal{P}_i$, i.e., $\mathcal{A}_{(k_i,\mathcal{P}_i)} = \{X \subseteq \mathcal{P}_i : |X| \geq k_i\}$. In the 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 5.3 and [20] 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 $k_2 = |\mathcal{P}_2|$.

From Theorem 5.7 we know that if the access structures in $\mathsf{A} = \{\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}, \ldots, \mathcal{A}_{(k_t,\mathcal{P}_t)}\}$ are pairwise compatible, then there exists an ideal secret sharing scheme with broadcast message for A. The following theorem establishes that if there exists an ideal secret sharing scheme with broadcast message for the family A of threshold structures, then the access structures in A are pairwise compatible. Moreover, if an ideal scheme for A does not exist, then the following theorem proves a gap for the dimension of the shares of participants and of the broadcast message. Either there is an ideal scheme or the size of at least one of them is 50% bigger than the secret size.

Theorem 6.1 *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. If an ideal secret sharing scheme with broadcast message for A exists then, the access structures in 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 that $H(P) + H(B_{i_j}) \geq 3H(S)$.

Proof: We first consider the case $t = 2$. If $\mathcal{A}_1$ and $\mathcal{A}_2$ are compatible, then there exists an ideal secret sharing scheme with broadcast messages for A from Theorem 5.7. Suppose now that $\mathcal{A}_1$ and $\mathcal{A}_2$ are not compatible. Let be $r = |\mathcal{P}_1 \cap \mathcal{P}_2|$. Notice that r is always greater than zero since the access structures are connected. We distinguish two cases:
Case **a.** There exists a threshold $k_i,\ i \in \{1,2\}$ such that $k_i < r$.
Case **b.** Each threshold $k_i,\ i \in \{1,2\}$ is not less than r.

Case **a.** We assume, w.l.o.g., that $k_1 < r$. Let $\mathcal{P}'_1 = \mathcal{P}_1 \cap \mathcal{P}_2 = \{P_1, \ldots, P_r\}$ and $\mathcal{P}_2 = \{P_1, \ldots, P_{t_2}\}$. We further distinguish 2 subcases.
Case a.1. $k_1 \neq k_2$. Let be $k_i = \min\{k_1, k_2\}$ and $k_j = \max\{k_1, k_2\}$. Consider the five random variables:

$$\begin{aligned} F &= P_1 \cdots P_{k_i-1} \\ A &= P_{k_i+1} \cdots P_{k_j} \\ B &= B_i \\ C &= P_{k_i} \\ D &= B_j. \end{aligned}$$

Random variables A, B, C, D, F, S satisfy the hypothesis of Lemma 5.1. Indeed, $H(S|ABF) = 0$ as the participants in A together with the participants in F are $k_j - 1 \geq k_i$ and so with the broadcast message B_i they can recover the secret. Analogously, one can verify that $H(S|BCF) = 0$ and $H(S|ACDF) = 0$. Moreover, $H(S|ADF) = H(S|F) = H(S)$, as the participants in AF are $k_j - 1$ and they are not sufficient to recover the secret with B_j. $H(S|BF) = H(S|F) = H(S)$ as the $k_i - 1$ shares of participants in F are not sufficient to get any information on S even after seeing B_i. Finally, $H(S|ACF) = H(S|F) = H(S)$ as there is no broadcast message in ACF. From Lemma 5.1, we have $H(BC) \geq H(BC|F) \geq 3H(S|F) = 3H(S)$ and there is no ideal secret sharing scheme with broadcast messages.

CASE a.2. $k_1 = k_2 = k$. If $r = t_2$ as we suppose that the two access structures are distinct there exists a participant $P_j \in \mathcal{P}_1 \backslash \mathcal{P}'_1$. Consider the following random variables:

$$\begin{aligned} F &= P_1 \cdots P_{k-2} P_j \\ A &= P_{k-1} \\ B &= B_1 \\ C &= P_k \\ D &= B_2, \end{aligned}$$

together with S they satisfy the hypothesis of Lemma 5.1.
If $r < t_2$ consider the following random variables:

$$\begin{aligned} F &= P_1 \cdots P_{k-2} P_{t_2} \\ A &= P_{k-1} \\ B &= B_2 \\ C &= P_k \\ D &= B_1, \end{aligned}$$

together with S they satisfy the hypothesis of Lemma 5.1.

CASE **b.** Assume, for simplicity, that $k_1 \leq k_2$ and that $\mathcal{P}_1 \backslash \mathcal{P}_2 = \{P_1, \ldots, P_{t_1-r}\}$, $\mathcal{P}_1 \cap \mathcal{P}_2 = \{P_{t_1-r+1}, \ldots, P_{t_1}\}$ and $\mathcal{P}_2 \backslash \mathcal{P}_1 = \{P_{t_1+1}, \ldots, P_{t_1+t_2-r}\}$.
If $k_2 < t_2$, then consider the following random variables:

$$\begin{aligned} F &= P_1 \cdots P_{k_1-r} P_{t_1-r+1} \cdots P_{t_1-1} P_{t_1+1} \cdots P_{t_1+k_2-r} \\ A &= P_{t_1+t_2-r} \\ B &= B_2 \\ C &= P_{t_1} \\ D &= B_1, \end{aligned}$$

together with S they satisfy the hypothesis of Lemma 5.1 and thus there is no ideal secret sharing scheme for A.
Else, if $k_2 = t_2$, as the two structures are not compatible, we have $k_1 < t_1$. Then consider the following random variables:

$$\begin{aligned} F &= P_1 \cdots P_{k_1-r} P_{t_1-r+1} \cdots P_{t_1-1} P_{t_1+1} \cdots P_{t_1+t_2-r} \\ A &= P_{t_1-r} \\ B &= B_1 \\ C &= P_{t_1} \\ D &= B_2. \end{aligned}$$

We can see that those random variables, together with S, satisfy the hypothesis of Lemma 5.1 and thus there is no ideal secret sharing scheme for A.

Hence, if $\mathcal{A}_1$ and $\mathcal{A}_2$ are not compatible, it is always possible to find five random variables F, A, B, C, D such that $C = P_i$, for some $P_i \in \mathcal{P}_1 \cap \mathcal{P}_2$ and $B = B_j$, where $j \in \{1, 2\}$, that verify the hypothesis of Lemma 5.1. Moreover, our constructions does not depend on the particular $P_i \in \mathcal{P}_1 \cap \mathcal{P}_2$. We conclude that, if $\mathcal{A}_1$ and $\mathcal{A}_2$ are not compatible, for all $P_i \in \mathcal{P}_1 \cap \mathcal{P}_2$ there exist a broadcast message B_j, $j = 1, 2$ such that $H(P_i B_j) \geq 3H(S)$, and, consequently, there is no ideal secret sharing scheme for A.

We now consider the case $t \geq 3$. If there exists a pair of access structures in A that are not compatible then, from the previous discussion there is no ideal secret sharing scheme with broadcast message for A. On the other hand, if the t access structures are pairwise compatible, then for Theorem 5.7 there exists an ideal secret sharing scheme with broadcast message for A. □

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 than 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 6.1.

Corollary 6.2 *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* $\mathcal{P}_i \cap \mathcal{P}_j = \emptyset$*, for all* $i \neq j$.

Proof: If $\mathcal{P}_i \cap \mathcal{P}_j = \emptyset$, for all $i \neq j$, then the access structures $\mathcal{A}_{(1,\mathcal{P}_1)}, \ldots, \mathcal{A}_{(1,\mathcal{P}_t)}$ are pairwise compatible. Thus, from Theorem 6.1 there exists an ideal secret sharing scheme with broadcast message for A. On the other hand, suppose that there exist two indices i and j, $1 \leq i < j \leq t$ such that $\mathcal{P}_i \cap \mathcal{P}_j \neq \emptyset$. Then $\mathcal{A}_{(1,\mathcal{P}_i)}$ and $\mathcal{A}_{(1,\mathcal{P}_j)}$ are not compatible, as we suppose that the access structures in A are distinct. Hence, for Theorem 6.1, an ideal secret sharing scheme with broadcast message for A does not exist and thus, the corollary is proved. $\square$

In some cases a better bound on the size of the shares distributed to participants holds. Consider the set of participants $\mathcal{P} = \{X_0, X_1, X_2, \ldots, X_n\}$ and the access structure $\mathcal{M}_n$ which is the closure of $\{\{X_1, X_2, \ldots, X_n\}, \{X_0, X_1\}, \{X_0, X_2\}, \ldots, \{X_0, X_{n-1}\}\}$. In a similar way of Theorem 4.1 in [4] 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 that

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

The following theorem holds.

Theorem 6.3 *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 that* $H(B_1) + \sum_{j=1}^{t-k_1} H(P_{l_j}) \geq (2(t-k_1)+1)H(S)$.
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 that* $H(B_1) + \sum_{j=1}^{\ell} H(P_{l_j}) \geq (2\ell+1)H(S)$.
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 that* $H(B_2) + \sum_{j=1}^{\ell} H(P_{l_j}) \geq (2\ell+1)H(S)$.

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 that*
$H(B_2) + \sum_{j=1}^{t-1} H(P_{l_j}) \geq (2(t-1)+1)H(S)$.
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 that*
$H(B_1) + \sum_{j=1}^{t-1} H(P_{l_j}) \geq (2(t-1)+1)H(S)$.

Proof: In this proof we use the same distinction of cases than that of Theorem 6.1. With F we denote the set of participants whose shares will be revealed, this enables us to use directly the lower bound (1). By using the same technique employed in Theorem 5.3 on the participants in F (i.e., from a scheme for A we construct a scheme where the shares of participants in F are fixed), we lower both the number of participants in the scheme and the threshold of the scheme.
Suppose that $k_1 < r$, then we have
CASE **1.** If $k_1 < k_2$, then let $t = \min\{k_2, r\}$. Let $X_0 = B_1$, for $i = 1, 2, \ldots, t-k_1+1$, let $X_i = P_{l_i}$, with $P_{l_i} \in \mathcal{P}_1 \cap \mathcal{P}_2$, let $X_{t-k_1+2} = B_2$, finally let $F = \{P_{j_1}, \ldots, P_{j_{k_1-1}}\} \cup \{P_{\ell_1}, \ldots, P_{\ell_{k_2-t}}\}$, where $\{P_{j_1}, \ldots, P_{j_{k_1-1}}\} \subseteq \mathcal{P}_1 \cap \mathcal{P}_2 \backslash \{P_{l_1}, \ldots, P_{l_{t-k_1+1}}\}$, and $\{P_{\ell_1}, \ldots, P_{\ell_{k_2-t}}\} \subseteq \mathcal{P}_2 \backslash \mathcal{P}_1$ (this last set there is only when $k_2 - t > 0$). It is easy to see that those participants satisfy the hypothesis of lower bound (1).
CASE **2.** If $k_1 = k_2 = k$ and $r = t_2$, then let $\ell = \min\{k-1, t_1 - r\}$. If $r = t_2$ as we suppose that the two access structures are distinct there exists at least participant $P_j \in \mathcal{P}_1 \backslash \mathcal{P}_2$. Let $X_0 = B_1$, for $i = 1, 2, \ldots, \ell+1$, let $X_i = P_{l_i}$, with $P_{l_i} \in \mathcal{P}_1 \cap \mathcal{P}_2$, let $X_{\ell+2} = B_2$, finally let $F = \{P_{j_1}, \ldots, P_{j_{k-1}}\} \subseteq \mathcal{P}_1 \backslash \{P_{l_1}, \ldots, P_{l_{\ell+1}}\}$ such that $\{P_{j_1}, \ldots, P_{j_\ell}\} \subseteq \mathcal{P}_1 \backslash \mathcal{P}_2$. It is easy to see that those participants satisfy the hypothesis of lower bound (1).
CASE **3.** If $k_1 = k_2 = k$ and $r < t_2$, then let $\ell = \min\{k-1, t_2 - r\}$. Let $X_0 = B_2$, for $i = 1, 2, \ldots, \ell+1$, let $X_i = P_{l_i}$, with $P_{l_i} \in \mathcal{P}_1 \cap \mathcal{P}_2$, let $X_{\ell+2} = B_1$, finally let $F = \{P_{j_1}, \ldots, P_{j_{k-1}}\} \subseteq \mathcal{P}_2 \backslash \{P_{l_1}, \ldots, P_{l_{\ell+1}}\}$ such that $\{P_{j_1}, \ldots, P_{j_\ell}\} \subseteq \mathcal{P}_2 \backslash \mathcal{P}_1$. It is easy to see that those participants satisfy the hypothesis of lower bound (1).
On the other hand if $r \leq k_1$ we have
CASE **1.** If $k_2 < t_2$, then let $t = \min\{r, t_2 - k_2 + 1\}$. Let $X_0 = B_2$, for $i = 1, 2, \ldots, t$, let $X_i = P_{l_i}$, with $P_{l_i} \in \mathcal{P}_1 \cap \mathcal{P}_2$, let $X_{t+1} = B_1$, finally let $F = \{P_{s_1}, \ldots, P_{s_{k_2-1}}\} \cup \{P_{j_1}, \ldots, P_{j_{k_1-r}}\}$, with $\{P_{s_1}, \ldots, P_{s_{k_2-1}}\} \subseteq \mathcal{P}_2 \backslash \{P_{l_1}, \ldots, P_{l_t}\}$ and $\{P_{j_1}, \ldots, P_{j_{k_1-r}}\} \subseteq \mathcal{P}_1 \backslash \mathcal{P}_2$. It is easy to see that those participants satisfy the hypothesis of lower bound (1).
CASE **2.** If $k_2 = t_2$, then let $t = \min\{r, t_1 - k_1 + 1\}$. Let $X_0 = B_1$, for $i = 1, 2, \ldots, t$, let $X_i = P_{l_i}$, with $P_{l_i} \in \mathcal{P}_1 \cap \mathcal{P}_2$, let $X_{t+1} = B_2$, finally let $F = \{P_{s_1}, \ldots, P_{s_{k_1-1}}\} \cup \{P_{j_1}, \ldots, P_{j_{k_2-r}}\}$, with $\{P_{s_1}, \ldots, P_{s_{k_1-1}}\} \subseteq \mathcal{P}_1 \backslash \{P_{l_1}, \ldots, P_{l_t}\}$ and $\{P_{j_1}, \ldots, P_{j_{k_2-r}}\} \subseteq \mathcal{P}_2 \backslash \mathcal{P}_1$. It is easy to see that those participants satisfy the hypothesis of lower bound (1). Thus, the theorem holds.
□

We now analyze the case in which the access structures in A consist of all possible distinct threshold structures on $\mathcal{P}$, that is, $\mathsf{A} = \{\mathcal{A}_{(k,\mathcal{P}')} \mid 1 \leq k \leq |\mathcal{P}'| \leq n \text{ and } \mathcal{P}' \subseteq \mathcal{P}\}$. From Theorem 6.1 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 [21], [22], and [23]) 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 $s \in V_D \cap V_I$. Uniformly 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

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

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 techniques described in [24] and [18]), we can obtain a geometric scheme in which $H(P) = H(S)$ and $H(B_{k,\mathcal{P}'}) = (n-k+1)H(S)$.
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 $q \geq \max\{2n, m\}+1$ is a prime power.

Threshold Preprocessing-Algorithm

Input: $S = GF(q)$, U_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 $a_i = r_i$.

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 $1 \leq k \leq |\mathcal{P}'| \leq n$

Use a $(n+1, 2n)$ threshold scheme 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

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

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 [20]. We have to construct a polynomial $f(x)$ over $GF(q)$ of degree n such that $f(i) = y_i$, for $i = 1, 2, \ldots, n$, and $f(0) = s$. This can be done by using the Lagrange interpolation. Thus, we set $y_i = f(i)$, for $i = n+1, \ldots, 2n$. 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 share of each participant $P_i \in \mathcal{P}$ is equal to $H(P_i) = H(S)$. Since each broadcast message $b_{k,\mathcal{P}'}$ consists of $n-k+1$ values of $f(x)$, every k participants in the threshold structure $\mathcal{A}_{(k,\mathcal{P}')}$ know $n+1$ values of $f(x)$ 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.

7 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 $\mathcal{A}^{(i)}_{j_i}$, 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 $b^{(1)}_{j_1} \ldots b^{(i-1)}_{j_{i-1}}$ 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 $\mathsf{A}^{(i)}_{j_1,\ldots,j_{i-1}}$ 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 $\mathcal{A}^{(i)}_{j_i}$. Thus, after the publication of all $i-1$ previous broadcast messages, the subsets of participants in $\mathcal{A}^{(i)}_{j_i}$ 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 let $\mathsf{A}^{(i)} = \{\mathcal{A}^{(i)}_1, \ldots, \mathcal{A}^{(i)}_{m_i}\}$ be the family of possible access structures at time i, where $i = 1, 2, \ldots, T$. Denote with $\mathcal{P}^{(i)}$ the set of participants involved at time i and let $\mathcal{P} = \bigcup_{i=1}^{T} \mathcal{P}^{(i)}$. Finally, denote with $\mathsf{B}^{(i)} = \{B^{(i)}_1, \ldots, B^{(i)}_{m_i}\}$ 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 7.1 *Let $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$, where $\mathsf{A}^{(i)} = \{\mathcal{A}^{(i)}_1, \ldots, \mathcal{A}^{(i)}_{m_i}\}$, be families of access structures on $\mathcal{P}$. A* fully dynamic secret sharing scheme *is a distribution 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 $1 \le j_\ell \le m_\ell$, it holds that $H(S^{(i)}|XB^{(1)}_{j_1} \ldots B^{(i-1)}_{j_{i-1}}) = H(S^{(i)})$.

2. *After seeing the new broadcast message, we have a new 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 $1 \le j_\ell \le m_\ell$, it holds that
$$H(S^{(i)}|XB^{(1)}_{j_1} \ldots B^{(i)}_{j_i}) = \begin{cases} H(S^{(i)}) & \text{if } X \notin \mathcal{A}^{(i)}_{j_i} \\ 0 & \text{if } X \in \mathcal{A}^{(i)}_{j_i} \end{cases}$$

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

The following theorem is a generalization to fully dynamic secret sharing schemes of Theorem 4.2. We omit the proof since it is similar to the proof of Theorem 4.2.

Theorem 7.2 *Let $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$, where $\mathsf{A}^{(i)} = \{\mathcal{A}^{(i)}_1, \ldots, \mathcal{A}^{(i)}_{m_i}\}$ be families of 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 that $H(P) \ge H(S^{(i)})$.*

2. *For $j = 1, 2, \ldots, m_i$, it holds that $H(B^{(i)}_j) \ge H(S^{(i)})$.*

Definition 7.1 says nothing on the sets X of participants such that $X \notin \mathcal{A}^{(i)}_{j_i}$ and that know all secrets $s_1, \ldots, s_{i-1}$ previously recovered. A natural requirement is that the information that those 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 7.3 *Let* $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ *be families of 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 $1 \leq j_\ell \leq m_\ell$, and for all $X \notin \mathcal{A}_{j_i}^{(i)}$, it holds that

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

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 fact, for all $i = 1, \ldots, T$, for all $j_1, \ldots, j_i$, where $1 \leq j_\ell \leq m_\ell$, and for all $X \notin \mathcal{A}_{j_i}^{(i)}$ it holds that

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

Hence, any fully dynamic secret sharing scheme can be seen as a strong one.

The following lemma is a generalization to strong fully dynamic secret sharing schemes of Lemma 4.1. We omit the proof since it is similar to the proof of Lemma 4.1.

Lemma 7.4 *Let* $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ *be families of access structures on a set* $\mathcal{P}$ *of participants. Let* $\mathcal{A}_{j_i}^{(i)} \in \mathsf{A}^{(i)}$, *if* $Y \in 2^{\mathcal{P}^{(i)} \cup \{B_{j_i}^{(i)}\}} \setminus \mathcal{A}_{j_i}^{(i)B}$ *and* $X \cup Y \in \mathcal{A}_{j_i}^{(i)B}$, *then*

$$H(X|YB_{j_1}^{(1)} \ldots B_{j_{(i-1)}}^{(i-1)} S^{(1)} \ldots S^{(i-1)}) = H(S^{(i)}) + H(X|YB_{j_1}^{(1)} \ldots B_{j_{(i-1)}}^{(i)} S^{(1)} \ldots S^{(i)}).$$

The following theorem proves a lower bound on the size of shares held by a fixed participant.

Theorem 7.5 *Let* $\mathcal{P}$ *be a set of participants,* $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ *be families of 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* $X_i \subseteq \mathcal{P}$, *where* $i = 1, \ldots, T$, *such that*

- $X_i \notin \mathcal{A}_{j_i}^{(i)}$, *but* $X_i \cup \{P\} \in \mathcal{A}_{j_i}^{(i)}$, *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 the shares given to participant* P *satisfies*

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

Proof: Consider the entropy $H(P)$. We have

$$
\begin{aligned}
H(P) &\geq H(P|X_1B^{(1)}_{j_1}) \quad \text{(from (4) and (5), Appendix A)}\\
&= H(S^{(1)}) + H(P|X_1B^{(1)}_{j_1}S^{(1)}) \quad \text{(from Lemma 7.4)}\\
&\geq H(S^{(1)}) + H(P|X_2B^{(1)}_{j_1}B^{(2)}_{j_2}S^{(1)}) \quad \text{(from (5), Appendix A)}\\
&= H(S^{(1)}) + H(S^{(2)}) + H(P|X_2B^{(1)}_{j_1}B^{(2)}_{j_2}S^{(1)}S^{(2)}) \quad \text{(from Lemma 7.4)}\\
&\vdots \quad \dots\\
&\geq H(S^{(1)}) + \cdots + H(S^{(i)}) + H(P|X_iB^{(1)}_{j_1}\dots B^{(i)}_{j_i}S^{(1)}\dots S^{(i)})\\
&\vdots \quad \dots\\
&\geq H(S^{(1)}) + \cdots + H(S^{(T)}) + H(P|X_TB^{(1)}_{j_1}\dots B^{(T)}_{j_T}S^{(1)}\dots S^{(T)})\\
&\geq H(S^{(1)}) + \cdots + H(S^{(T)}) \quad \text{(from (2), Appendix A)}
\end{aligned}
$$

$\square$

We point out that Theorem 7.5 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 access structures on the set of participants $\mathcal{P} = \{P_1, P_2, P_3\}$, where $\mathcal{A}^{(1)}_1 = \mathsf{cl}(\{\{P_1P_2\}\})$ and $\mathcal{A}^{(2)}_1 = \mathsf{cl}(\{\{P_2P_3\}\})$. 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: $\mathbf{Z}_q$, U_q, $\mathcal{P} = \{P_1, P_2, P_3\}$ and $\mathsf{A}^{(1)}$, $\mathsf{A}^{(2)}$.

For $i = 1, 2, 3$, randomly select $r_i \in \mathbf{Z}_q$ 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: $s^{(1)}, s^{(2)} \in \mathbf{Z}_q$, $\mathsf{A}^{(1)}$, $\mathsf{A}^{(2)}$, and a_1, a_2, a_3.

Compute
$$b^{(1)}_1 = a_1 + a_2 + s^{(1)} \mod q$$
and
$$b^{(2)}_1 = a_2 + a_3 + s^{(2)} \mod q,$$
that are the broadcast messages for the two access structures $\mathcal{A}^{(1)}_1$ and $\mathcal{A}^{(2)}_1$, respectively.

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

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

$$H(S^{(2)}|P_1P_3B^{(1)}_1B^{(2)}_1S^{(1)}) = 0, \text{ but } \{P_1P_3\} \notin \mathcal{A}^{(2)}_1.$$

The scheme above satisfies the remaining hypothesis of Theorem 7.5 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 to Theorem 7.5 hold.

Corollary 7.6 *Let $\mathcal{P}$ be a set of participants and let $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(T)}$ be families of 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 the share given to any participant $P \in \mathcal{P}_1$ satisfies*

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

Proof: Suppose that at time i the dealer enables the access structure $\mathcal{A}_{(k_i,\mathcal{P}_i)}$ to recover the i-*th* secret. Let P be a participant in $\mathcal{P}_1$. Construct the sets $X_1, \ldots, X_T$ as follows. Let the set X_1 be equal to $X_1 = \{P_{i_1}, \ldots, P_{i_{k_1-1}}\}$, where each P_{i_t}, with $t = 1, 2, \ldots, k_1 - 1$, belongs to $\mathcal{P}_1 \backslash \{P\}$. For $j = 2, 3, \ldots, T$, if $k_j = k_{j-1}$ then the set X_j will be equal to X_{j-1}, otherwise the set X_j will be equal to $X_j = X_{j-1} \cup \{P_{i_{k_{j-1}+1}}, \ldots, P_{i_{k_j}}\}$, where each P_{i_t}, with $t = k_{j-1} + 1, \ldots, k_j$, belongs to $\mathcal{P}_j \backslash (\{P\} \cup X_{j-1})$. It is easy to see that the participants P and the sets $X_1, \ldots, X_T$ satisfies the hypothesis of Theorem 7.5, thus the corollary is proved. □

Corollary 7.7 *Let $\mathcal{P}$ be a set of n participants and let k and T be positive integers, with $1 \leq k \leq n$ and $T \leq n - k$. Let $\mathsf{A}^{(0)}, \ldots, \mathsf{A}^{(T)}$ be families of 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 the share given to any participant $P \in \mathcal{P}_T$ satisfies*

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

Proof: For any $P \in \mathcal{P}_T$ consider a set $A \in \mathcal{A}_{(k,\mathcal{P}_T)}$ such that $P \in A$. For $i = 0, 1, \ldots, T$, let $X_i = A \backslash \{P\}$. The corollary follow from Theorem 7.5. □

A particular class of strong fully dynamic secret sharing scheme which satisfies the hypothesis of Corollary 7.7 are (k, n) threshold schemes with disenrollment [2]. 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 [2]), with $0 \leq L \leq n - k$, for any participant $P \in \mathcal{P}$, it holds that $H(P) \geq \sum_{i=0}^{L} H(S^{(i)})$, obtaining in this way the main theorem of [2].

8 Randomness in Secret Sharing Schemes with Broadcast

Randomness plays an important role in several areas of theoretical computer science, most notably algorithm design, complexity and cryptography. Since random bits are a natural computational resource, the amount of randomness used in computation is an important issue in many applications. Therefore, considerable effort has been devoted both to reduce the number of random bits used by probabilistic algorithms (see for instance [13]) and to analyze the amount of randomness required in order to achieve a given performance [17]. The Shannon entropy of the random source generating the random bits represents the most general and natural measure of randomness.

In this section we define the dealer's randomness for secret sharing schemes with broadcast message. We present a lower bound on the dealer's randomness $\mathcal{R}(\mathsf{A})$ of any distribution protocol realizing a secret sharing scheme with broadcast message for a given family of access structures $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$.

To formally define the dealer's randomness we use the Shannon entropy of the random variables generating the secret and the shares. Given a probability distribution $\mathbf{P} = (p_1, \ldots, p_n)$, the Shannon entropy of $\mathbf{P}$ is $H(\mathbf{P}) = -\sum_{i=1}^{n} p_i \log p_i$. The entropy is strictly related to the measure of randomness introduced by Knuth and Yao [15]. Let A be an algorithm that generates the probability distribution $\mathbf{P} = (p_1, \ldots, p_n)$, using only independent and unbiased random bits in inputs. Denote by $T(A)$ the average number of random bits used by the algorithm A and let $T(\mathbf{P}) = \min_A T(A)$. Knuth and Yao proved that

Theorem 8.1 ([15])

$$H(\mathbf{P}) \leq T(\mathbf{P}) < H(\mathbf{P}) + 2.$$

Thus, the entropy of a random source is very close to the average number of independent unbiased random bits necessary to simulate the source.

To analyze the randomness needed by the dealer we define the *dealer's randomness* of a secret sharing scheme with broadcast message Σ, when the probability distribution on the set of secrets S is Π_S, as

$$\mathcal{R}(\mathsf{A}, \Pi_S, \Sigma) = H(P_1 \ldots P_n B_1 \ldots B_m | S).$$

The value $\mathcal{R}(\mathsf{A}, \Pi_S, \Sigma)$ represents a lower bound on the amount of randomness required by the dealer to set up the scheme when using the scheme Σ and when Π_S is the probability distribution on the secret. Notice that $\mathcal{R}(\mathcal{A}, \Pi_S, \Sigma)$ depends also on Σ since the probability that participants receive given shares depends both on $\{p_S(s)\}_{s \in S}$ and Σ.

Definition 8.2 *Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of access structures on a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of participants. The* dealer's randomness *$\mathcal{R}(\mathsf{A})$ of A is defined as*

$$\mathcal{R}(\mathsf{A}) = \inf_{\mathcal{Q}, \mathcal{T}} \mathcal{R}(\mathsf{A}, \Pi_S, \Sigma)$$

where $\mathcal{Q}$ is the space of all non-trivial probability distributions Π_S on the set of secrets S and $\mathcal{T}$ is the space of all secret sharing schemes with broadcast message Σ for the family of access structures A.

The dealer's randomness represents the minimum amount possible of randomness for a given family A of access structures.

The definition of independent sequence given in [6] can be easily modified to handle the more general case of secret sharing schemes with broadcast message as follows.

Definition 8.3 *Let $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be a family of access structures on a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of participants. A sequence $P_{j_1}, \ldots, P_{j_\ell}$ of participants is called* independent *if for all $i < \ell$ a subset $X_i \in 2^{\mathcal{P} \cup \{B_1, \ldots, B_m\}}$ and an access structure $\mathcal{A}_{r_i} \in \mathsf{A}$ exist such that*

1. *$\{P_{j_1}, \ldots, P_{j_i}\} \cup X_i \notin \mathcal{A}^B_{r_i}$, and*
2. *$\{P_{j_1}, \ldots, P_{j_i} P_{j_{i+1}}\} \cup X_i \in \mathcal{A}^B_{r_i}$.*

In a similar way of Theorem 2.1 in [6] we can prove the following theorem that represents our main tool to derive lower bounds on the the amount of randomness required by the dealer to set up a secret sharing scheme with broadcast message. We repeat it here for the reader's convenience.

Theorem 8.4 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of access structures on a set* $\mathcal{P} = \{P_1, \ldots, P_n\}$ *of participants. If there exists an independent sequence of length* ℓ *then*

$$\mathcal{R}(\mathsf{A}) \geq \ell H(S).$$

Proof: Let $P_{i_1}, \ldots, P_{i_\ell}$ be an independent sequence of participants. From (3) and (2) (see Appendix A) we get

$$H(P_1 P_2 ... P_n B_1 \ldots B_m | S) \geq H(P_{i_1} ... P_{i_\ell} | S).$$

Since $P_{i_1} \cdots P_{i_\ell} \notin \mathcal{A}^B_{r_i}$, from Lemma 4.4 we have $H(P_{i_1} ... P_{i_\ell}) = H(P_{i_1} ... P_{i_\ell} | S)$ and thus

$$\begin{aligned}
H(P_1 P_2 ... P_n B_1 \ldots B_m | S) &\geq H(P_{i_1} ... P_{i_\ell}) \\
&= H(P_{i_1}) + H(P_{i_2} | P_{i_1}) + \ldots + H(P_{i_\ell} | P_{i_1} ... P_{i_{\ell-1}}) \\
&\qquad \text{(from (3), Appendix A)} \\
&\geq H(P_{i_1}) + H(P_{i_2} | P_{i_1} X_1) + \ldots + H(P_{i_\ell} | P_{i_1} \ldots P_{i_{\ell-1}} X_{\ell-1}) \\
&\qquad \text{(from (5), Appendix A)} \\
&\geq \ell H(S) \text{ (from Lemma 4.1)}
\end{aligned}$$

Hence, for any secret sharing scheme it holds that

$$H(P_1 P_2 ... P_n B_1 \ldots B_m | S) \geq \ell H(S),$$

and the theorem follows. □

Next corollary is an immediate consequence of Theorem 8.4.

Corollary 8.5 *Let* $\mathsf{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ *be a family of access structures on a set* $\mathcal{P} = \{P_1, \ldots, P_n\}$ *of participants. The dealer's randomness* $\mathcal{R}(\mathsf{A})$ *satisfies,*

$$\mathcal{R}(\mathsf{A}) \geq \max_{X \in \mathcal{A}_i^0,\ \mathcal{A}_i \in \mathsf{A}} |X| H(S).$$

Proof: Let $X = \{P_{j_1}, P_{j_2}, \ldots, P_{j_l}\}$ be a minimal qualified set, that is $X \in \mathcal{A}_r^0$ and $\mathcal{A}_r \in \mathsf{A}$, for some $r \in \{1, 2, \ldots, m\}$. The sequence of participants $P_{j_1}, P_{j_2}, \ldots, P_{j_l}$ is an independent sequence. Indeed, the sets $X_i = \{P_{j_{i+2}}, \ldots, P_{j_l} B_r\}$, for $i < l - 1$, and the set $X_{l-1} = \{B_r\}$ satisfy the properties of Definition 8.3. Thus, from Theorem 8.4 we have $\mathcal{R}(\mathsf{A}) \geq |X| H(S)$ and the corollary holds. □

For threshold schemes with broadcast message the following bound holds.

Corollary 8.6 *Let* $\mathsf{A} = \{\mathcal{A}_{(k_1, \mathcal{P}_1)}, \ldots, \mathcal{A}_{(k_m, \mathcal{P}_m)}\}$ *be a family of threshold access structures on a set* $\mathcal{P} = \{P_1, \ldots, P_n\}$ *of participants. Then, the dealer's randomness* $\mathcal{R}(\mathsf{A})$ *satisfies*

$$\mathcal{R}(\mathsf{A}) \geq \max\{k_1, \ldots, k_m\} H(S).$$

In Section 6 we presented a protocol to realize secret sharing schemes with broadcast message for the access structures in A consisting of all possible distinct threshold structures on $\mathcal{P}$. The previous corollary proves that the protocol is optimal with respect to the randomness used to construct such schemes when both the uniform probability distribution on the set S of the secret is assumed and $q = 2^t$. Recall that in such a case $H(S) = t$.

We can improve on the lower bound provided by Corollary 8.6 when A consists of two threshold access structures.

Theorem 8.7 *Let* $\mathsf{A} = \{\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}\}$ *be a family of two threshold access structures on a set* $\mathcal{P} = \{P_1, \ldots, P_n\}$ *of participants. Let* $t_i = |\mathcal{P}_i|$, *where* $i = 1, 2$, *and* $r = |\mathcal{P}_1 \cap \mathcal{P}_2|$. *If* $\max_{i=1,2} t_i - k_i \geq r$, *then*

$$\mathcal{R}(\mathsf{A}) \geq (k_1 + k_2)H(S).$$

Else, if $t_i - r < k_i$, *for* $i = 1, 2$, *then the dealer's randomness* $\mathcal{R}(\mathsf{A})$ *satisfies*

$$\mathcal{R}(\mathsf{A}) \geq \max\{k_2 + t_1 - r, k_1 + t_2 - r\}H(S).$$

Proof: Suppose, w.l.o.g., that $t_1 - r \geq k_1$. Then, the sequence of participants $P_{i_1}, \ldots, P_{i_{k_1+k_2}}$, where $P_{i_1}, \ldots, P_{i_{k_1}} \in \mathcal{P}_1 \backslash \mathcal{P}_2$ and $P_{i_{k_1+1}} \ldots P_{i_{k_1+k_2}} \in \mathcal{P}_2$, is an independent sequence. On the other hand, suppose that $t_i - r < k_i$, for $i = 1, 2$. Then, $\mathcal{R}(\mathsf{A}) \geq \max\{k_2 + t_1 - r, k_1 + t_2 - r\}H(S)$. In fact, if $k_2 + t_1 - r \geq k_1 + t_2 - r$ then the sequence of participants $P_{i_1}, \ldots, P_{i_{k_2+t_1-r}}$, where $P_{i_1}, \ldots, P_{i_{t_1-r}} \in \mathcal{P}_1 \backslash \mathcal{P}_2$, $P_{i_{t_1-r+1}}, \ldots, P_{i_{t_1+k_2-t_2}} \in \mathcal{P}_1 \cap \mathcal{P}_2$ and $P_{i_{t_1+k_2-t_2+1}}, \ldots, P_{i_{k_2+t_1-r}} \in \mathcal{P}_2 \backslash \mathcal{P}_1$, is an independent sequence. Else if $k_1 + t_2 - r > k_2 + t_1 - r$ then the sequence of participants $P_{i_1}, \ldots, P_{i_{k_1+t_2-r}}$ where $P_{i_1}, \ldots, P_{i_{t_2-r}} \in \mathcal{P}_2 \backslash \mathcal{P}_1$, $P_{i_{t_2-r+1}}, \ldots, P_{i_{t_2+k_1-t_1}} \in \mathcal{P}_1 \cap \mathcal{P}_2$ and $P_{i_{t_2+k_1-t_1+1}}, \ldots, P_{i_{k_1+t_2-r}} \in \mathcal{P}_1 \backslash \mathcal{P}_2$, is an independent sequence. $\square$

It is easy to see that $\max\{k_2 + t_1 - r, k_1 + t_2 - r\} \geq \max\{k_1, k_2\}$ and so above theorem improves on Corollary 8.6.

References

[1] G. R. Blakley, *Safeguarding Cryptographic Keys,* Proceedings AFIPS 1979 National Computer Conference, pp. 313–317, June 1979.

[2] B. Blakley, G. R. Blakley, A. H. Chan, and J. Massey, *Threshold Schemes with Disenrollment,* in "Advances in Cryptology - CRYPTO '92", "Lecture Notes in Computer Science", Vol. 740, E. Brickell Ed., Springer-Verlag, pp. 546–554, 1993.

[3] C. Blundo, A. Giorgio Gaggia, and D.R. Stinson, *On the Dealer's Randomness Required in Secret Sharing Schemes,* to appear in "Advances in Cryptology - Eurocrypt '94", "Lecture Notes in Computer Science", Springer-Verlag, Berlin.

[4] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, *On the Information Rate of Secret Sharing Schemes,* in "Advances in Cryptology - CRYPTO '92", "Lecture Notes in Computer Science", Vol. 740, E. Brickell Ed., Springer-Verlag, pp. 149–169, 1993. To appear in *Theoretical Computer Science.*

[5] 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. To appear in *Journal of Cryptology.*

[6] C. Blundo, A. De Santis, and U. Vaccaro, *Randomness in Distribution Protocols,* "21st International Colloquium on Automata, Languages and Programming" (ICALP '94), Serge Abiteboul and Eli Shamir Eds., Vol. 820 of "Lecture Notes in Computer Science", Springer–Verlag, Berlin, pp. 568–579, 1994.

[7] E. F. Brickell and D. M. Davenport, *On the Classification of Ideal Secret Sharing Schemes,* Journal of Cryptology, Vol. 4, No. 2, pp. 123–134, 1991.

[8] 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.

[9] I. Csiszár and J. Körner, *Information Theory. Coding Theorems for Discrete Memoryless Systems,* Academic Press, 1981.

[10] R. G. Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, New York, NY, 1968.

[11] O. Goldreich, S. Micali, and A. Wigderson, *How to Play any Mental Game*, Proceedings of 19th Annual ACM Symposium on Theory of Computing, pp. 218–229, 1987.

[12] 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, 1990.

[13] R. Impagliazzo and D. Zuckerman, *How to Recycle Random Bits*, in Proc. 30th IEEE Symp. on Foundations of Comput. Sci., pp. 248–255, 1989.

[14] 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.

[15] D.E. Knuth and A.C. Yao, *The Complexity of Nonuniform Random Number Generation*, in: "Algorithms and Complexity", J.F. Traub (Ed.), Academic Press, pp. 357–428, 1976.

[16] S. C. Kothari, *Generalized Linear Threshold Schemes*, in "Advances in Cryptology - CRYPTO '84", G. R. Blakley and D. Chaum Eds., Vol. 196 of "Lecture Notes in Computer Science", Springer-Verlag, pp. 231–241.

[17] D. Krizanc, D. Peleg, and E. Upfal, *A Time–Randomness Tradeoff for Oblivious Routing*, Proceedings of 20th Annual ACM Symposium on Theory of Computing, pp. 93–102, 1988.

[18] K. M. Martin, *Discrete Structures in the Theory of Secret Sharing*, PhD Thesis, University of London, 1991.

[19] K. M. Martin, *Untrustworthy Participants in Perfect Secret Sharing Schemes*, Proceedings of the 3rd IMA Conference on Coding and Cryptology, Cirencester, 1991.

[20] A. Shamir, *How to Share a Secret,* Communications of the ACM, Vol. 22, n. 11, pp. 612–613, Nov. 1979.

[21] G. J. Simmons, *An Introduction to Shared Secret and/or Shared Control Schemes and Their Application*, Contemporary Cryptology, IEEE Press, pp. 441–497, 1991.

[22] G. J. Simmons, *How to (Really) Share a Secret*, in "Advances in Cryptology - CRYPTO 88", Ed. S. Goldwasser, Vol. 403 "Lecture Notes in Computer Science", Springer-Verlag, pp. 390–448, 1989.

[23] G. J. Simmons, W. Jackson, and K. M. Martin, *The Geometry of Shared Secret Schemes,* Bulletin of the ICA, Vol. 1, pp. 71–88, 1991.

[24] D. R. Stinson, *An Explication of Secret Sharing Schemes*, Design, Codes and Cryptography, Vol. 2, pp. 357–390, 1992.

[25] D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, IEEE Trans. on Inform. Theory, Vol. IT-40, pp. 118–125, 1994.

Appendix A

Information Theory Background

In this Appendix we review the basic concepts of Information Theory used in our definitions and proof. For a complete treatment of the subject the reader is advised to consult [9] and [10].

Given a probability distribution $\{p(x)\}_{x \epsilon X}$ on a set X, we define the *entropy* of X, $H(X)$, as

$$H(X) = -\sum_{x \epsilon X} p(x) \log p(x)^4.$$

The entropy $H(X)$ is a measure of the average uncertainty one has about which element of the set X has been chosen when the choices of the elements from X are made according to the probability distribution $\{p(x)\}_{x \epsilon X}$. The entropy enjoys the following property

$$0 \leq H(X) \leq \log |X|,$$

where $H(X) = 0$ if and only if there exists $x_0 \in X$ such that $p(x_0) = 1$; $H(X) = \log |X|$ if and only if $p(x) = 1/|X|$, for all $x \in X$.

Given two sets X and Y and a joint probability distribution $\{p(x, y)\}_{x \epsilon X, y \epsilon Y}$ on their cartesian product, the *conditional entropy* $H(X|Y)$, also called the equivocation of X given Y, is defined as

$$H(X|Y) = -\sum_{y \epsilon Y} \sum_{x \epsilon X} p(y) p(x|y) \log p(x|y).$$

From the definition of conditional entropy it is easy to see that

$$H(X|Y) \geq 0. \tag{2}$$

If we have $n+1$ sets $X_1, \ldots, X_n, Y$, the entropy of $X_1 \ldots X_n$ given Y can be expressed as

$$H(X_1 \ldots X_n|Y) = H(X_1|Y) + H(X_2|X_1Y) + \cdots + H(X_n|X_1 \ldots X_{n-1}Y) \tag{3}$$

The *mutual information* $I(X;Y)$ between X and Y is defined by

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

and enjoys the following properties:

$$I(X;Y) = I(Y;X),$$

and

$$I(X;Y) \geq 0,$$

from which one gets

$$H(X) \geq H(X|Y). \tag{4}$$

Given $n+2$ sets $X, Y, Z_1, \ldots, Z_n$ and a joint probability distribution on their cartesian product, the *conditional mutual information* $I(X;Y|Z_1, \ldots, Z_n)$ between X and Y given $Z_1, \ldots, Z_n$ can be written as

$$\begin{aligned} I(X;Y|Z_1, \ldots, Z_n) &= H(X|Z_1, \ldots, Z_n) - H(X|Z_1, \ldots, Z_nY) \\ &= H(Y|Z_1, \ldots, Z_n) - H(Y|Z_1, \ldots, Z_nX). \end{aligned}$$

[4] All logarithms in this paper are of base 2

Since the conditional mutual information is always non negative we get

$$H(X|Z_1, \ldots, Z_n) \geq H(X|Z_1, \ldots, Z_n Y). \tag{5}$$

From (3) and (5) one easily gets that for any sets $Y, X_1, \ldots, X_n$ and a joint probability distribution on their cartesian product it holds that

$$\sum_{i=1}^{n} H(X_i|Y) \geq H(X_1 X_2 \ldots X_n|Y). \tag{6}$$