Journal of Universal Computer Science, vol. 5, no. 7 (1999), 367-389
submitted: 12/2/99, accepted: 15/7/99, appeared: 28/7/99 © Springer Pub. Co.

Randomness in Multi–Secret Sharing Schemes

Carlo Blundo
(Dipartimento di Informatica ed Applicazioni
Università di Salerno
84081 Baronissi (SA), Italy
carblu@dia.unisa.it)

Barbara Masucci
(Dipartimento di Informatica ed Applicazioni
Università di Salerno
84081 Baronissi (SA), Italy
masucci@dia.unisa.it)

Abstract: A multi–secret sharing scheme is a protocol to share a number of (arbitrarily related) secrets among a set of participants in such a way that only qualified sets of participants can recover the secrets, whereas non-qualified sets of participants might have partial information about them.
In this paper we analyze the amount of randomness needed by multi–secret sharing schemes. Given an m-tuple of access structures, we give a lower bound on the number of random bits needed by multi–secret sharing schemes; the lower bound is expressed in terms of a combinatorial parameter that depends only upon the access structures and not on the particular multi–secret sharing scheme used.

Key Words: Data Security, Cryptography, Randomness, Secret Sharing Schemes.
Category: E.3

1 Introduction

There are many situations in cryptography in which it is important to be able to generate random numbers, random bit strings, etc. For example, cryptographic keys are to be generated at random from a specified keyspace, and the use of a natural source of random bits, such as an unbiased coin, a radioactive source or a noise diode, is absolutely essential. Since random bits are a natural computational resource, the amount of randomness used in a computation is an important issue in many applications. Therefore, considerable effort has been devoted to reduce the number of random bits used by probabilistic algorithms [Cohen et al. 89, Impagliazzo et al. 89], to construct different kinds of small probability spaces (which sometimes even allow to eliminate the use of randomness) [Koller et al. 93, Naor et al. 93], and to analyze the amount of randomness required in order to achieve a given performance [Krizanc et al. 88, Kushilevitz et al. 94].
A secret sharing scheme is a method to share a secret s among a set $\mathcal{P}$ of participants in such a way that only qualified subsets of $\mathcal{P}$, pooling together their information, can reconstruct the secret s; whereas any other (non-qualified) subset of $\mathcal{P}$ has no information on it. Secret sharing schemes were introduced by Shamir [Shamir 79] and Blakley [Blakley 79]. They analyzed the case when only subsets of $\mathcal{P}$ of cardinality at least k, for a fixed integer $k \leq |\mathcal{P}|$, can reconstruct the secret. These schemes are called (k, n) threshold schemes, where $n = |\mathcal{P}|$. The

construction of (k, n) threshold schemes, based on polynomial interpolation, is the following: let q_i a prime power greater than n and let $s \in GF(q)$ be the secret to be shared. The dealer independently and uniformly chooses $k-1$ elements $a_1, ..., a_{k-1}$ in $GF(q)$ and constructs the polynomial $f(y) = s + a_1 y + a_2 y^2 + \cdots + a_{k-1} y^{k-1}$. The information distributed to the i-th participant is equal to $f(i)$. It is easy to see that any k participants can perform a Lagrange interpolation on their values to recover $f(y)$, and hence recover the secret s. On the other hand, any $k-1$ participants have no information about the secret. Indeed, for any value $s' \in GF(q)$ there exists one and only one polynomial $g(y)$ of degree $k-1$ such that $g(0) = s'$ and $g(i) = f(i)$ for any participant i.

Subsequently, Ito, Saito, and Nishizeki [Ito et al. 93] and Benaloh and Leichter [Blakley et al. 90] described a more general method of secret sharing. They showed how to realize a secret sharing scheme for any access structure, where the access structure is the family of all subsets of participants that are able to reconstruct the secret. For an updated bibliography on secret sharing schemes we refer the reader to [Stinson], while, for a detailed description of results in the area we recommend the surveys [Simmons 91] and [Stinson 92].

Many secret sharing applications, in particular those associated to key-management, require protection of more than one secret. As an example, consider the following situation, described in [Simmons 91]: There is a missile battery in which each missile has a different launch enable code. The problem is to devise a scheme to protect these codes by using the same pieces of private information. Another scenario, in which the sharing of many secrets is important, was considered by Franklin and Yung [Franklin et al.]. They investigated the communication complexity of unconditionally secure multi–party computation and its relations with various fault–tolerant models. They presented a general technique for parallelizing non–cryptographic computation protocols, at a small cost in fault–tolerance. Their technique replaces polynomial–based (single) secret sharing with a technique allowing multiple secrets to be hidden in a single polynomial.

The problem of sharing more than one secret was also considered by many researchers (see [Blundo et al. 98a], [Blundo et al. 94], [Blundo et al. 93], [De Santis et al. 99], [Ding et al. 97], [Karnin et al. 83], [Jackson et al. 93], [Jackson et al. 94], [Jackson et al. 96], [McEliece et al. 81]). The authors of [Blundo et al. 98a] analyzed different models for sharing many secrets, taking into account both the "level of security" and the degrees of dependence among the secrets to be shared. They formally defined *multi–secret sharing schemes* and gave a systematic analysis for such schemes in information theoretic terms.

The best way to understand multi–secret sharing schemes is by resorting to an example. Suppose that there are two secrets s_1 and s_2 to be shared, with $s_1 \in GF(q_1)$ and $s_2 \in GF(q_2)$, where q_1 and q_2 are prime powers. Suppose that there are two sets $\mathcal{P}_1 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ and $\mathcal{P}_2 = \{P_3, P_4, P_5, P_6, P_7, P_8\}$ of participants. We want to share the secret s_1 among participants in $\mathcal{P}_1$ in such a way that the subsets of $\mathcal{P}_1$ qualified to recover s_1 are $\{P_3\}, \{P_1, P_2\}$ and $\{P_4, P_5, P_6\}$. Besides, we want to share the secret s_2 among participants in $\mathcal{P}_2$ in such a way that the subsets of $\mathcal{P}_2$ qualified to recover s_2 are $\{P_3, P_5, P_6\}$, $\{P_7, P_8\}$ and $\{P_4\}$. Let $q = \max\{q_1, q_2\}$. The dealer uniformly chooses four values $x_1, \ldots, x_4$, where $x_1 \in GF(q_1)$, $x_2 \in GF(q_2)$, and $x_3, x_4 \in GF(q)$, then he distributes the shares as follows:

P_1 gets x_1	P_2 gets $x_1 + s_1 \bmod q_1$	P_3 gets $(s_1, x_4 + s_2 \bmod q)$
P_4 gets $(s_2, x_4 + s_1 \bmod q)$	P_5 gets x_3	P_6 gets $x_3 + x_4 \bmod q$
P_7 gets x_2	P_8 gets $x_2 + s_2 \bmod q_2$.	

It is easy to see that in this scheme only the qualified subsets can recover the secrets.

The quantitative study of the number of random bits needed by secret sharing schemes has been initiated in [Blundo et al. 96], 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 [Blundo et al. 97, Blundo et al 98c, Czirimaz 96].

In this paper we analyze the amount of randomness needed to set up a multi–secret sharing scheme. We measure the randomness by the entropy of the probability space from which the shares, to be given to participants, are taken. For any given m-tuple of access structures (an access structure is the specification of all subsets of participants that can recover the secret), we provide a lower bound on the randomness needed to generate the shares to distribute to participants. The lower bound is expressed in terms of a combinatorial parameter that depends only upon the access structures and not on the particular multi–secret sharing scheme used.

The paper is organized as follows: In Section 2 we recall basic definitions of multi–secret sharing schemes. In Section 3 we present some results that will be useful to prove our limitations. In Section 4 we define and analyze a measure for the amount of randomness needed to realize a multi–secret sharing scheme. Moreover, we present a general lower bound on the amount of randomness in multi–secret sharing schemes. In Sections 5 and 6 we present tight lower bounds on the randomness in multi–secret sharing schemes for pairs of access structures. In particular, in Section 6 we analyze the case in which at least one of the access structures is a (k, n) threshold structure (i.e., an access structure on a set of n participants in which any qualified set of participants has cardinality at least k).

2 Multi–Secret Sharing Schemes

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 about the secret. An access structure $\mathcal{A}$ is the set of all subsets of $\mathcal{P}$ that can recover the secret.

Definition 1. Let $\mathcal{P}$ be a set of participants, a *monotone access structure* $\mathcal{A}$ on $\mathcal{P}$ is a subset $\mathcal{A} \subseteq 2^{\mathcal{P}} \setminus \{\emptyset\}$, such that $A \in \mathcal{A}, A \subseteq A' \subseteq \mathcal{P} \Rightarrow A' \in \mathcal{A}$.

Definition 2. Let $\mathcal{P}$ be a set of participants and $\mathcal{A} \subseteq 2^{\mathcal{P}}$. The *closure* of $\mathcal{A}$, denoted by $\mathsf{cl}(\mathcal{A})$, is the set $\mathsf{cl}(\mathcal{A}) = \{C | \exists B \in \mathcal{A} \text{ and } B \subseteq C \subseteq \mathcal{P}\}$.

For a monotone access structure $\mathcal{A}$ we have $\mathcal{A} = \mathsf{cl}(\mathcal{A})$. From now on we will consider only monotone access structures. Let $\mathcal{A}$ be an access structure, a set $C \in \mathcal{A}$ is a *minimal* set of $\mathcal{A}$ if it does not contain any set in $\mathcal{A} \setminus \{C\}$. A *basis* $\mathcal{A}_0$ of $\mathcal{A}$ is the family of all minimal sets of $\mathcal{A}$. We will refer to a participant $P \in \mathcal{P}$ as an *essential* participant if there exists a set $X \subseteq \mathcal{P}$ such that $X \cup \{P\} \in \mathcal{A}_0$. If a participant P is not essential, then we can construct a secret sharing scheme giving him\her nothing as share. In fact, a non–essential participant does not need to participate "actively" in the reconstruction of the secret, since the information he\she has is not needed by any set in $\mathcal{P}$ in order to recover the shared secret. Therefore, we assume throughout this paper that all participants are essential.

Multi–secret sharing schemes are a natural generalization of single secret sharing schemes: we consider different access structures and in each of them we share a secret. In a multi–secret sharing scheme, an m-tuple of secrets $(s_1,\ldots,s_m) \in S_1 \times \cdots \times S_m$ is shared in an m-tuple $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ of access structures on $\mathcal{P}$, where $\mathcal{P} = \{P_1,\ldots,P_n\}$, in such a way that, for each $i = 1,\ldots,m$, the access structure $\mathcal{A}_i$ is the set of all subsets of $\mathcal{P}$ that can recover the secret $s_i \in S_i$. This means that only the sets $A \in \mathcal{A}_i$ can recover the secret s_i, but any set $A \notin \mathcal{A}_i$, even knowing an arbitrary subset of secrets, has no more information about s_i than that already conveyed by the secrets A knows.

Let $M = \{1,\ldots,m\}$ and let $S_M = S_1 \times \cdots \times S_m$ be the set from where the secrets are chosen. (The i-th secret to be shared is chosen from S_i).

Let $\{Pr_{S_M}(s_1,\ldots,s_m)\}_{(s_1,\ldots,s_m)\in S_M}$ be a probability distribution on S_M. Let a multi–secret sharing scheme for secrets in S_M 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 secrets $(s_1,\ldots,s_m) \in S_M$ 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, not necessarily uniform, probability distribution.

Given a set of participants $A = \{P_{i_1},\ldots,P_{i_r}\} \subseteq \mathcal{P}$, where $i_1 < i_2 < \ldots < i_r$, let $K(A) = K(P_{i_1}) \times \cdots \times K(P_{i_r})$. Moreover, for any $A \subseteq \mathcal{P}$, let $\mathcal{I}(A) \subseteq M$ be the set of indices of secrets that can be recovered by A, that is $\mathcal{I}(A) = \{i : A \in \mathcal{A}_i\}$. Given a set of indices $T = \{i_1,\ldots,i_t\} \subseteq M$, where $i_1 < i_2 < \ldots < i_t$, let $S_T = S_{i_1} \times \cdots \times S_{i_t}$. Any multi–secret sharing scheme for secrets in S_M and a probability distribution $\{Pr_{S_M}(s_1,\ldots,s_m)\}_{(s_1,\ldots,s_m)\in S_M}$ naturally induce probability distributions on $K(A)$ and on S_T, for any $A \subseteq \mathcal{P}$ and for any $T \subseteq M$. Denote such probability distributions by $\{Pr_{K(A)}(a)\}_{a\in K(A)}$ and $\{Pr_{S_T}(t)\}_{t\in S_T}$, respectively. For any $A \subseteq \mathcal{P}$, denote by $\mathbf{A}$ the random variable taking values on $K(A)$ according to the probability distribution $\{Pr_{K(A)}(a)\}_{a\in K(A)}$. For any $T \subseteq M$, denote by $\mathbf{S}_T$ the random variable taking values on S_T according to the probability distribution $\{Pr_{S_T}(t)\}_{t\in S_T}$. For $i = 1,\ldots m$, denote by $H(\mathbf{S}_i)$ the entropy (for the basic properties of the entropy used in this paper consult the Appendix) of $\{Pr_{S_i}(s_i)\}_{s_i\in S_i}$, for any $A \subseteq \mathcal{P}$, denote by $H(\mathbf{A})$ the entropy of $\{Pr_{K(A)}(a)\}_{a\in K(A)}$, and for any $T \subseteq M$ denote by $H(\mathbf{S}_T)$ the entropy of $\{Pr_{S_T}(t)\}_{t\in S_T}$. As done in [Blundo et al. 98a], we define multi–secret sharing schemes as follows.

Definition 3. Let $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. A *multi–secret sharing scheme* for $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ with secrets chosen according to $\mathbf{S}_M$ is a sharing of secrets in S_M in such a way that, for $i = 1,\ldots,m$,

1. Any subset $A \subseteq \mathcal{P}$ of participants enabled to recover a secret can compute it.
   For all $A \in \mathcal{A}_i$, *it holds that* $H(\mathbf{S}_i|\mathbf{A}) = 0$.
2. Any subset $A \subseteq \mathcal{P}$ of participants not enabled to recover a secret, even knowing an arbitrary subset of secrets, has no more information on it than

that already conveyed by the known secrets.
For all $A \notin \mathcal{A}_i$, and $T \subseteq M$, it holds that $H(\mathbf{S}_i|\mathbf{A}\mathbf{S}_T) = H(\mathbf{S}_i|\mathbf{S}_{\mathcal{I}(A)}\mathbf{S}_T)$, where $\mathcal{I}(A) = \{i : A \in \mathcal{A}_i\}$.

3 Technical Lemmas

In this section we present some results that will be useful to prove our limitations. Assume a set of participants $Y \subseteq \mathcal{P}$ cannot determine the secret s_i, but they can do so if another participant (or another group of participants) X would be willing to pool its own share. The following technical lemma, proved in [Blundo et al. 98a], gives a lower bound on the entropy of the probability space from where the shares given to X are chosen, when the shares given to Y and a subset of secrets are known.

Lemma 4. *Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. Let $X \subseteq \mathcal{P}$ and $T \subseteq \{1, \ldots, m\}$. If there exists a set of participants $Y \subseteq \mathcal{P}$ such that $Y \notin \mathcal{A}_i$ and $X \cup Y \in \mathcal{A}_i$, then, in any multi–secret sharing scheme for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ with secrets chosen according to $\mathbf{S}_M$, it holds that*

$$H(\mathbf{X}|\mathbf{Y}\mathbf{S}_T) = H(\mathbf{S}_i|\mathbf{S}_{\mathcal{I}(Y)}\mathbf{S}_T) + H(\mathbf{X}|\mathbf{Y}\mathbf{S}_T\mathbf{S}_i).$$

The next lemma shows a useful relation between the entropy of the probability space from where the shares given to any subset of participants are chosen and the size of the secrets they can recover.

Lemma 5. *Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. In any multi–secret sharing scheme for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ with secrets chosen according to $\mathbf{S}_M$, for any $X \subseteq \mathcal{P}$, it holds that*

$$H(\mathbf{X}) = H(\mathbf{X}|\mathbf{S}_M) + H(\mathbf{S}_{\mathcal{I}(X)}).$$

Proof. From (13) of Appendix we have that

$$\begin{aligned} I(\mathbf{X};\mathbf{S}_M) &= H(\mathbf{X}) - H(\mathbf{X}|\mathbf{S}_M) \\ &= H(\mathbf{S}_M) - H(\mathbf{S}_M|\mathbf{X}). \end{aligned} \tag{1}$$

If $\mathcal{I}(X) = \{1, \ldots, m\}$ (i.e., $S_{\mathcal{I}(X)} = S_M$) then, from the above equation, it is immediate to see that

$$H(\mathbf{X}) = H(\mathbf{X}|\mathbf{S}_M) + H(\mathbf{S}_{\mathcal{I}(X)}).$$

Now, without loss of generality, assume that $\mathcal{I}(X) = \{1, \ldots, t\}$, with $t < m$. From (12) of Appendix we obtain

$$\begin{aligned} H(\mathbf{S}_M|\mathbf{X}) &= H(\mathbf{S}_{\mathcal{I}(X)}|\mathbf{X}) + H(\mathbf{S}_{M \setminus \mathcal{I}(X)}|\mathbf{X}\mathbf{S}_{\mathcal{I}(X)}) \\ &= H(\mathbf{S}_{\{1,\ldots,t\}}|\mathbf{X}) + H(\mathbf{S}_{\{t+1,\ldots,m\}}|\mathbf{X}\mathbf{S}_{\{1,\ldots,t\}}) \\ &= H(\mathbf{S}_1|\mathbf{X}) + \sum_{i=2}^{t} H(\mathbf{S}_i|\mathbf{X}\mathbf{S}_{\{1,\ldots,i-1\}}) + H(\mathbf{S}_{t+1}|\mathbf{X}\mathbf{S}_{\{1,\ldots,t\}}) + \end{aligned}$$

$$\begin{aligned}
& \sum_{i=t+2}^{m} H(\mathbf{S}_i|\mathbf{X}\mathbf{S}_{\{1,\ldots,i-1\}}) \;\; \text{(from (12) of Appendix)} \\
&= H(\mathbf{S}_{t+1}|\mathbf{S}_{\{1,\ldots,t\}}) + \sum_{i=t+2}^{m} H(\mathbf{S}_i|\mathbf{S}_{\{1,\ldots,i-1\}}) \;\; \text{(from Definition 3)} \\
&= H(\mathbf{S}_{\{t+1,\ldots,m\}}|\mathbf{S}_{\{1,\ldots,t\}}) \;\; \text{(from (12) of Appendix)} \\
&= H(\mathbf{S}_{M\setminus\mathcal{I}(X)}|\mathbf{S}_{\mathcal{I}(X)}). \qquad (2)
\end{aligned}$$

Therefore, we have that

$$\begin{aligned}
H(\mathbf{X}) &= H(\mathbf{X}|\mathbf{S}_M) + H(\mathbf{S}_M) - H(\mathbf{S}_M|\mathbf{X}) \text{ (from (1))} \\
&= H(\mathbf{X}|\mathbf{S}_M) + H(\mathbf{S}_M) - (\mathbf{S}_{M\setminus\mathcal{I}(X)}|\mathbf{S}_{\mathcal{I}(X)}) \text{ (from (2))} \\
&= H(\mathbf{X}|\mathbf{S}_M) + H(\mathbf{S}_{\mathcal{I}(X)}) \;\; \text{(from (12) of Appendix).}
\end{aligned}$$

Hence, the lemma holds. □

From the next theorem we can easily derive a lower bound on the size of the share given to each participant. The proof of the next theorem is similar to the one of Theorem 3.2 in [Blundo et al. 98a].

Theorem 6. *Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. Assume that there exist a participant P and $m+1$ sets $Y, X_1, X_2, \ldots, X_m \subset \mathcal{P}$ such that, for $1 \le i \le m$: $\{P\} \cup Y \cup X_1 \cup \cdots \cup X_i \in \mathcal{A}_i$, and $Y \cup X_1 \cup \cdots \cup X_i \notin \mathcal{A}_i$. Then, in any multi–secret sharing scheme for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ with secrets chosen according to $\mathbf{S}_M$, the entropy of the share given to P satisfies*

$$H(\mathbf{P}|\mathbf{Y}) \ge H(\mathbf{S}_M) + H(\mathbf{P}|\mathbf{X}_1 \ldots \mathbf{X}_m \mathbf{S}_M).$$

Proof. For $1 \le i \le m$, since $Y \cup X_1 \cup \cdots \cup X_i \notin \mathcal{A}_i$ implies $Y \cup X_1 \cup \cdots \cup X_{i-1} \notin \mathcal{A}_i$, it is easy to see that $\mathcal{I}(Y \cup X_1 \cup \cdots \cup X_i) \subseteq \{1, \ldots, i-1\}$. The proof of the theorem is by induction on m. Assume $m = 1$. We have that

$$\begin{aligned}
H(\mathbf{P}|\mathbf{Y}) &\ge H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1) \text{ (from (14) of Appendix)} \\
&= H(\mathbf{S}_1|\mathbf{S}_{\mathcal{I}(Y\cup X_1)}) + H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1\mathbf{S}_1) \text{ (from Lemma 4)} \\
&= H(\mathbf{S}_1) + H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1\mathbf{S}_1) \text{ (since } \mathcal{I}(Y \cup X_1) = \emptyset).
\end{aligned}$$

Therefore, the lemma is true for $m = 1$.
Now, suppose the lemma true for $m-1$, that is

$$H(\mathbf{P}|\mathbf{Y}) \ge H(\mathbf{S}_{\{1,\ldots,m-1\}}) + H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1 \ldots \mathbf{X}_{m-1}\mathbf{S}_{\{1,\ldots,m-1\}}).$$

From (14) of Appendix we have that

$$\begin{aligned}
H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1 \ldots \mathbf{X}_{m-1}\mathbf{S}_{\{1,\ldots,m-1\}}) &\ge H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1 \ldots \mathbf{X}_m\mathbf{S}_{\{1,\ldots,m-1\}}) \\
&= H(\mathbf{S}_m|\mathbf{S}_{\mathcal{I}(Y\cup X_1\cup\cdots\cup X_m)}\mathbf{S}_{\{1,\ldots,m-1\}}) + \\
&\qquad H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1 \ldots \mathbf{X}_m) \text{ (from Lemma 4)} \\
&= H(\mathbf{S}_m|\mathbf{S}_{\{1,\ldots,m-1\}}) + H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1 \ldots \mathbf{X}_m\mathbf{S}_M). \\
&\qquad \text{(since } \mathcal{I}(Y \cup X_1 \cup \cdots \cup X_m) \subseteq \{1, \ldots, m-1\}).
\end{aligned}$$

From the above inequalities applied to the inductive hypothesis we obtain

$$\begin{aligned} H(\mathbf{P}|\mathbf{Y}) &\geq H(\mathbf{S}_{\{1,\ldots,m-1\}}) + H(\mathbf{S}_m|\mathbf{S}_{\{1,\ldots,m-1\}}) + H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1\ldots\mathbf{X}_m\mathbf{S}_{M}) \\ &= H(\mathbf{S}_{M}) + H(\mathbf{P}|\mathbf{Y}\mathbf{X}_1\ldots\mathbf{X}_m\mathbf{S}_{M}) \text{ (from (11) of Appendix).} \end{aligned}$$

Thus, the theorem holds. □

Since the entropy of the random variable $\mathbf{P}$ satisfies the property $0 \leq H(\mathbf{P}) \leq \log|K(P)|$, Theorem 6 gives a lower bound on the size of the shares given to each participant.

4 Dealer's Randomness in Multi–Secret Sharing Schemes

In this section we define and analyze a measure for the amount of randomness needed to realize a multi–secret sharing scheme.

The Shannon entropy of the random source generating the random bits represents the most general and natural measure of randomness. Indeed, it has been shown (see [Knuth et al. 76]) that the entropy of a random variable $\mathbf{X}$ (i.e., of a memoryless random source) is approximatively equal to the average number of tosses of an unbiased coin to simulate the outcomes of $\mathbf{X}$. Let A be an algorithm that generates the probability distribution $\{Pr_{\mathbf{X}}(x)\}_{x\in X}$ 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 $T(\mathbf{X}) = \min_A T(A)$. Knuth and Yao [Knuth et al. 76] proved the following inequalities:

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

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

The *total randomness* present in a multi–secret sharing scheme Σ for an m-tuple of access structures $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ on a set $\mathcal{P} = \{P_1,\ldots,P_n\}$ of n participants is equal to the entropy $H(\mathbf{P}_1\ldots\mathbf{P}_n)$. This takes into account also the randomness $H(\mathbf{S}_{M})$ of the secrets, as we will see later. The *dealer's randomness* is the randomness needed by the dealer to set up a multi–secret sharing scheme for secrets chosen according to $\mathbf{S}_{M}$, that is, the randomness he uses to generate the shares, given that the probability distribution $\Pi_{S_M} \triangleq \{Pr_{S_M}(s_1,\ldots,s_m)\}_{(s_1,\ldots,s_m)\in S_M}$ on the secrets is known. Therefore, for an m-tuple of access structures $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ and a multi–secret sharing scheme, the amount of randomness used by the dealer is equal to $H(\mathbf{P}_1\ldots\mathbf{P}_n|\mathbf{S}_{M})$. This randomness is needed only to generate the shares distributed to participants.

Extending Lemma 2.7 in [Blundo et al. 96] we obtain the following result, that relates the total randomness and the dealer's randomness in multi–secret sharing schemes.

Lemma 7. *Let $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. Then, in any multi–secret sharing scheme for $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ with secrets chosen according to $\mathbf{S}_{M}$, it holds that*

$$H(\mathbf{P}_1\ldots\mathbf{P}_n) = H(\mathbf{P}_1\ldots\mathbf{P}_n|\mathbf{S}_{M}) + H(\mathbf{S}_{M}).$$

Extending the definition of dealer's randomness in single secret sharing schemes given in [Blundo et al. 96], we define the *dealer's randomness* in a multi–secret sharing scheme Σ for the m-tuple of access structures $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$, when the secrets to be shared are chosen in $S_{\scriptscriptstyle M}$ according to the probability distribution $\Pi_{S_{\scriptscriptstyle M}}$, as

$$\mu[(\mathcal{A}_1,\ldots,\mathcal{A}_m),\Pi_{S_{\scriptscriptstyle M}},\Sigma] = H(\mathbf{P}_1\ldots\mathbf{P}_n|\mathbf{S}_{\scriptscriptstyle M}).$$

Notice that $\mu[(\mathcal{A}_1,\ldots,\mathcal{A}_m),\Pi_{S_{\scriptscriptstyle M}},\Sigma]$ depends also on Σ, since the probability that participants receive given shares depends both on $\Pi_{S_{\scriptscriptstyle M}}$ and on the distribution scheme Σ. Since we are interested in the minimum amount possible of randomness for an m-tuple of access structures $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$, we give the following definition:

Definition 8. Let $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. Let $S_{\scriptscriptstyle M} = S_1\times\cdots\times S_m$ and let $q_i = |S_i|$, for $i = 1,\ldots,m$. The *dealer's randomness* $\mu[(\mathcal{A}_1,\ldots,\mathcal{A}_m),(q_1,\ldots,q_m)]$ of a multi–secret sharing scheme for $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ with secrets chosen in $S_{\scriptscriptstyle M}$, is defined as

$$\mu[(\mathcal{A}_1,\ldots,\mathcal{A}_m),(q_1,\ldots,q_m)] = \inf_{\mathcal{Q},\mathcal{T}} \mu[(\mathcal{A}_1,\ldots,\mathcal{A}_m),\Pi_{S_{\scriptscriptstyle M}},\Sigma]$$

where $\mathcal{Q}$ is the space of all probability distributions $\Pi_{S_{\scriptscriptstyle M}}$ on the sets of secrets $S_{\scriptscriptstyle M}$ and $\mathcal{T}$ is the space of all multi–secret sharing schemes Σ for the m-tuple of access structures $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$.

We recall here the definition of *independent sequence* given in [Blundo et al. 96]. The independent sequence has been used to derive lower bounds on the randomness needed in single secret sharing schemes.

Definition 9. Let $\mathcal{A}$ be an access structure on the set of participants $\mathcal{P}$. A sequence $P_{r_1}\ldots P_{r_\ell}$ of participants is called independent for $\mathcal{A}$ if the following two properties are satisfied:

1. $\{P_{r_1},\ldots,P_{r_\ell}\}\notin\mathcal{A}$,
2. For all $j<\ell$ there exists a subset $X_j\subset\mathcal{P}$ such that
   (a) $\{P_{r_1},\ldots,P_{r_j}\}\cup X_j\notin\mathcal{A}$,
   (b) $\{P_{r_1},\ldots,P_{r_j}\}\cup X_j\cup\{P_{r_{j+1}}\}\in\mathcal{A}$.

We generalize the definition of *independent sequence* to the case of multi–secret sharing schemes. The independent sequence will be a useful tool to derive lower bounds on the amount of randomness needed by the dealer to realize a multi–secret sharing scheme.

Definition 10. Let $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. A sequence $P_{r_1}\ldots P_{r_\ell}$ of participants is an $(a_1,\ldots,a_m,b)$-sequence for $(\mathcal{A}_1,\ldots,\mathcal{A}_m)$ if the following three properties are satisfied:

1. $\{P_{r_1}\ldots P_{r_\ell}\}\notin\mathcal{A}_1\cap\cdots\cap\mathcal{A}_m$,
2. For all $j<\ell$:
   There exist a subset $X_j\subset\mathcal{P}$ and an index $k_{j+1}\in\{1,\ldots,m\}$ such that
   a.1) $\{P_{r_1},\ldots,P_{r_j}\}\cup X_j\notin\mathcal{A}_{k_{j+1}}$,
   a.2) $\{P_{r_1},\ldots,P_{r_j}\}\cup X_j\cup\{P_{r_{j+1}}\}\in\mathcal{A}_{k_{j+1}}$,
   or there exist m subsets $X_j^1,\ldots,X_j^m\subset\mathcal{P}$ such that, for any $h\in\{1,\ldots,m\}$
   b.1) $\{P_{r_1},\ldots,P_{r_j}\}\cup X_j^1\cup\cdots\cup X_j^h\notin\mathcal{A}_h$,
   b.2) $\{P_{r_1},\ldots,P_{r_j}\}\cup X_j^1\cup\cdots\cup X_j^h\cup\{P_{r_{j+1}}\}\in\mathcal{A}_h$,

3. For any i, $1 \leq i \leq m$, $a_i = |\{j : 1 < j \leq \ell : k_j = i\}|$ and $b = \ell - \sum_{i=1}^{m} a_i$.

To avoid overburdening the notation, we will refer to an independent sequence (or to an $(a_1, \ldots, a_m, b)$-sequence) as to a set of participants, and thus we will apply the usual set operators to it. Hence, if $Z_1 = P_1 \ldots P_h$ and $Z_2 = Q_1 \ldots Q_k$ are such sequences, we will denote with $Z_1 \cap Z_2$ the set $\{P_1, \ldots, P_h\} \cap \{Q_1, \ldots, Q_k\}$ and with $\mathcal{P} \setminus Z_1$ the set $\mathcal{P} \setminus \{P_1, \ldots, P_h\}$. Moreover, we often will write $P_1 \ldots P_h$ rather than $\{P_1, \ldots, P_h\}$, and also XY rather than $X \cup Y$.
The next theorem gives a lower bound on $\mu[(\mathcal{A}_1, \ldots, \mathcal{A}_m), (q_1, \ldots, q_m)]$ when an $(a_1, \ldots, a_m, b)$-sequence for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ is known.

Theorem 11. *Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. If there exists an $(a_1, \ldots, a_m, b)$-sequence Z for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$, then it holds that*

$$\mu[(\mathcal{A}_1, \ldots, \mathcal{A}_m), (q_1, \ldots, q_m)] \geq \sum_{i=1}^{m} a_i H(\mathbf{S}_i | \mathbf{S}_{M \setminus \{i\}}) + bH(\mathbf{S}_M) - H(\mathbf{S}_{\mathcal{I}(Z)}).$$

Proof. For the sake of simplicity assume that $Z = P_1 \ldots P_\ell$ is an $(a_1, \ldots, a_m, b)$-sequence for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$. For $1 \leq i \leq m$, let $Z_{A_i} = \{P_j \in Z : k_j = i\}$ and $Z_B = Z \setminus \bigcup_{i=1}^{m} Z_{A_i}$. From Definition 10 it follows that $|Z_{A_i}| = a_i$ and $|Z_B| = \ell - \sum_{i=1}^{m} a_i$. Consider the participant $P_j \in Z$, for any $j = 1, \ldots, \ell$. We distinguish two cases:

1. If $P_j \in Z_{A_i}$, where $i \in M$, then there exists a subset of participants X_{j-1} such that $P_1 \ldots P_{j-1} X_{j-1} \notin \mathcal{A}_i$ and $P_1 \ldots P_{j-1} X_{j-1} P_j \in \mathcal{A}_i$. Therefore, we have that
$$\begin{aligned} H(\mathbf{P}_j | \mathbf{P}_1 \ldots \mathbf{P}_{j-1}) &\geq H(\mathbf{P}_j | \mathbf{P}_1 \ldots \mathbf{P}_{j-1} \mathbf{X}_{j-1}) \text{ (from (14) of Appendix)} \\ &\geq H(\mathbf{S}_i | \mathbf{S}_{\mathcal{I}(P_1 \ldots P_{j-1} X_{j-1})})) \text{ (from Lemma 4).} \end{aligned}$$
Since $P_1 \ldots P_{j-1} X_{j-1} \notin \mathcal{A}_i$, we have that $\mathcal{I}(P_1 \ldots P_{j-1} X_{j-1}) \subseteq M \setminus \{i\}$. Therefore, from (14) of Appendix it follows that
$$H(\mathbf{S}_i | \mathbf{S}_{\mathcal{I}(P_1 \ldots P_{j-1} X_{j-1})})) \geq H(\mathbf{S}_i | \mathbf{S}_{M \setminus \{i\}}).$$
Hence, for any participant $P_j \in Z_{A_i}$, it holds that
$$H(\mathbf{P}_j | \mathbf{P}_1 \ldots \mathbf{P}_{j-1}) \geq H(\mathbf{S}_i | \mathbf{S}_{M \setminus \{i\}}). \tag{3}$$
2. If $P_j \in Z_B$, then there exist m subsets of participants $X_j^1, \ldots, X_j^m$ such that, for any $i \in M$, it holds $P_1 \ldots P_{j-1} X_j^1 \ldots X_j^i \notin \mathcal{A}_i$ and $P_1 \ldots P_{j-1} X_j^1 \ldots X_j^i P_j \in \mathcal{A}_i$. Then, from Theorem 6 we have that
$$H(\mathbf{P}_j | \mathbf{P}_1 \ldots \mathbf{P}_{j-1}) \geq H(\mathbf{S}_M). \tag{4}$$

Hence, we have that

$$\begin{aligned} H(\mathbf{Z}) &= H(\mathbf{P}_1 \ldots \mathbf{P}_\ell) \\ &= H(\mathbf{P}_1) + H(\mathbf{P}_2 | \mathbf{P}_1) + \ldots + H(\mathbf{P}_\ell | \mathbf{P}_1 \ldots \mathbf{P}_{\ell-1}) \text{ (from (11) of Appendix)} \\ &\geq \sum_{i=1}^{m} a_i H(\mathbf{S}_i | \mathbf{S}_{M \setminus \{i\}}) + bH(\mathbf{S}_M) \text{ (from (3) and (4)).} \end{aligned} \tag{5}$$

Moreover, from Lemma 5 we obtain

$$H(\mathbf{Z}|\mathbf{S}_M) = H(\mathbf{Z}) - H(\mathbf{S}_{\mathcal{I}(Z)}). \qquad (6)$$

Hence, we have that

$$\begin{aligned} H(\mathbf{P}_1 \dots \mathbf{P}_n|\mathbf{S}_M) &\geq H(\mathbf{P}_1 \dots \mathbf{P}_\ell|\mathbf{S}_M) \\ &= H(\mathbf{Z}|\mathbf{S}_M) \\ &= H(\mathbf{Z}) - H(\mathbf{S}_{\mathcal{I}(Z)}) \text{ (from (6))} \\ &\geq \sum_{i=1}^{m} a_i H(\mathbf{S}_i|\mathbf{S}_{M\setminus\{i\}}) + bH(\mathbf{S}_M) - H(\mathbf{S}_{\mathcal{I}(Z)}) \text{ (from (5))}. \end{aligned}$$

Thus, the theorem holds. □

Notice that if the access structures $\mathcal{A}_1, \dots, A_m$ are equal to the same access structure $\mathcal{A}$ and there exists an independent sequence $Z = P_{r_1} \dots P_{r_\ell}$ of length ℓ for $\mathcal{A}$, then Z is also a $(\underbrace{0, \dots, 0}_{m}, \ell)$-sequence for $(\mathcal{A}_1, \dots, \mathcal{A}_m)$. Indeed, $Z \notin \mathcal{A}_1 \cap \dots \cap A_m$, (i.e., $\mathcal{I}(Z) = \emptyset$) and for $j < \ell$, it is possible to construct the sets $X_j^1, \dots, X_j^m$ as follows: $X_j^1 = X_j$, where X_j is the set satisfying Property *2* of Definition 9 for Z, and let $X_j^h = \emptyset$, for $h = 2, \dots, m$. Therefore, for any $j < \ell$ and any $h = 1, \dots, m$, it holds that $\{P_{r_1}, \dots, P_{r_j}\} \cup X_j^1 \cup \dots \cup X_j^h \notin \mathcal{A}_h$ and $\{P_{r_1}, \dots, P_{r_j}\} \cup X_j^1 \cup \dots \cup X_j^h \cup \{P_{r_{j+1}}\} \in \mathcal{A}_h$. Hence, from Theorem 11 we get $\mu[(\mathcal{A}_1, \dots, \mathcal{A}_m), (q_1, \dots, q_m)] \geq \ell H(\mathbf{S}_M)$.

Definition 10 can be slightly modified with a stronger assumption.

Definition 12. Let $(\mathcal{A}_1, \dots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. A sequence $P_{r_1} \dots P_{r_\ell}$ of participants is an $[a_1, \dots, a_m, b]$-sequence for $(\mathcal{A}_1, \dots, \mathcal{A}_m)$ if it is an $(a_1, \dots, a_m, b)$ sequence and if Property a.1 of Definition 10 is substituted by the following property: For all $j < \ell$ there exists a subset $X_j \subset \mathcal{P}$, such that $\{P_{r_1} \dots P_{r_j}\} \cup X_j \notin \mathcal{A}_1 \cup \dots \cup \mathcal{A}_m$.

The next theorem gives a lower bound on $\mu[(\mathcal{A}_1, \dots, \mathcal{A}_m), (q_1, \dots, q_m)]$ when an $[a_1, \dots, a_m, b]$-sequence for $(\mathcal{A}_1, \dots, \mathcal{A}_m)$ is known. The proof of the next theorem goes along the lines of the proof of Theorem 11, so we omit it.

Theorem 13. *Let $(\mathcal{A}_1, \dots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. If there exists an $[a_1, \dots, a_m, b]$-sequence Z for $(\mathcal{A}_1, \dots, \mathcal{A}_m)$, then, it holds that*

$$\mu[(\mathcal{A}_1, \dots, \mathcal{A}_m), (q_1, \dots, q_m)] \geq \sum_{i=1}^{m} a_i H(\mathbf{S}_i) + bH(\mathbf{S}_M) - H(\mathbf{S}_{\mathcal{I}(Z)}).$$

Notice that if the secrets are statistically independent, i.e., $H(\mathbf{S}_M) = \sum_{i=1}^{m} H(\mathbf{S}_i)$, then Theorems 11 and 13 lead to the same lower bound.

4.1 Threshold Structures

In this section we consider the problem of sharing many secrets in different threshold structures. More precisely, we analyze the case in which the secret s_i, where $i \in M$, is shared according to the access structure $\mathcal{A}_{(k_i,\mathcal{P}_i)}$, consisting of all subsets of participants in $\mathcal{P}_i \subseteq \mathcal{P}$ of cardinality at least k_i. The access structure $\mathcal{A}_{(k_i,\mathcal{P}_i)}$ is referred to as *threshold structure.* We prove tight lower bounds on the dealer's randomness needed by multi–secret sharing schemes for threshold structures. [De Santis et al. 99] considered the case $\mathcal{P}_1 = \mathcal{P}_2 = \cdots = \mathcal{P}_m$ and $k_1 \le k_2 \le \cdots \le k_m$.

Theorem 14. *Let $(\mathcal{A}_{(k,\mathcal{P}_1)}, \ldots, \mathcal{A}_{(k,\mathcal{P}_m)})$ be an m-tuple of threshold structures. In any multi–secret sharing scheme for $(\mathcal{A}_{(k,\mathcal{P}_1)}, \ldots, \mathcal{A}_{(k,\mathcal{P}_m)})$ with secrets chosen according to $\mathbf{S}_M$, if $\mathcal{P}_1 \subseteq \mathcal{P}_2 \subseteq \ldots \subseteq \mathcal{P}_m$, then it holds that*

$$\mu[(\mathcal{A}_{(k,\mathcal{P}_1)}, \ldots, \mathcal{A}_{(k,\mathcal{P}_m)}), (q_1, \ldots, q_m)] \ge (k-1)H(\mathbf{S}_M).$$

Proof. Let $X = \{P_{j_1}, \ldots, P_{j_k}\}$ be a set of k participants in $\mathcal{P}_1$. It is easy to see that $Z = P_{j_1} \ldots P_{j_{k-1}}$ is a $(\underbrace{0, \ldots, 0}_{m}, k-1)$-sequence for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$. Indeed, for $i = 1, \ldots, k-2$, the m sets $X_i^1, \ldots, X_i^m$ satisfying Definition 10 are all equal to $\{P_{j_{i+2}}, \ldots, P_{j_k}\}$. Since $\mathcal{I}(Z) = \emptyset$, the bound follows from Theorem 11. $\square$

If each secret s_i is uniformly chosen in $S_i = GF(q_i)$, with q_i a prime power greater than n, then it is possible to realize a multi–secret sharing scheme meeting the above bound. To accomplish this it is enough to combine m independent threshold schemes, say Shamir's schemes [Shamir 79], one for each threshold structure.

Multi-Threshold Algorithm

Input: $s_1 \in GF(q_1), \ldots, s_m \in GF(q_m)$, k, and $\mathcal{P}_1 \subseteq \mathcal{P}_2 \subseteq \cdots \subseteq \mathcal{P}_m \subseteq \{P_1, \ldots, P_n\}$.

For $1 \le i \le m$
- Let $F_{k-1}^i[x]$ be the set of all $k-1$ degree polynomials with coefficients in $GF(q_i)$.
- Choose randomly a polynomial $f_i(x) \in F_{k-1}^i[x]$ such that $f_i(0) = s_i$.
- For any $P_j \in \mathcal{P}_i$
  - Let $y_{i,j} = f_i(j)$ be the share of P_j when the secret s_i is shared in $\mathcal{A}_{(k,\mathcal{P}_i)}$.

For $1 \le j \le n$
- Let $\mathcal{I}(P_j) = \{i \in [1, \ldots, m] : P_j \in \mathcal{P}_i\} = \{h_1 \ldots, h_r\}$ and let $\mathbf{w}_j = (y_{h_1,j}, \ldots, y_{h_r,j})$ be the share of participant P_j.

Output: The shares $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n$ of participants $P_1, P_2, \ldots, P_n$ respectively.

It is easy to see that the previous protocol realizes a multi–secret sharing scheme for the m-tuple of threshold structures $(\mathcal{A}_{(k,\mathcal{P}_1)}, \ldots, \mathcal{A}_{(k,\mathcal{P}_m)})$. The protocol is optimal with respect to the number of random bits needed by the dealer to set up the scheme.

5 Randomness for Pairs of Access Structures

In this section we consider multi–secret sharing schemes for pairs of access structures. More precisely, we prove tight lower bounds on the dealer's randomness for any pair of access structures $(\mathcal{A}_1, \mathcal{A}_2)$ when two independent sequences Z_1 and Z_2, for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively, are known. This assumption is not restrictive at all, since it is easy to find an independent sequence for any access structure. Indeed, let $X \in \mathcal{A}_0$ be a minimal set for the access structure $\mathcal{A}$. It is easy to see that any subset $Y \subset X$ is an independent sequence for $\mathcal{A}$. On the other hand, computing the length of the longest independent sequence for an access structure is a hard computational problem. In [Blundo et al. 96] the authors proved that even computing an *approximation* to it is hard.

Theorem 15. *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. Let Z_1 (resp., Z_2) be an independent sequence of length α (resp., β) for $\mathcal{A}_1$ (resp., $\mathcal{A}_2$). Finally, assume that $Z_1 \cap \mathcal{P}_2 = \emptyset$ and $Z_2 \cap \mathcal{P}_1 \neq \emptyset$. Then, it holds that*

$$\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq \alpha H(\mathbf{S}_1 | \mathbf{S}_2) + \beta H(\mathbf{S}_2 | \mathbf{S}_1). \tag{7}$$

Moreover, if the secrets are statistically independent, or if $Z_1 \cup (\mathcal{P}_1 \cap \mathcal{P}_2) \notin \mathcal{A}_1 \cup \mathcal{A}_2$, then it holds that

$$\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq \alpha H(\mathbf{S}_1) + \beta H(\mathbf{S}_2). \tag{8}$$

Proof. For the sake of simplicity, assume that $Z_1 = P_1 \ldots P_\alpha$ and $Z_2 = Q_1 \ldots Q_\beta$, where $P_1, \ldots, P_\alpha \in \mathcal{P}_1$ and $Q_1, \ldots, Q_\beta \in \mathcal{P}_2$, are two independent sequences for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. From Definition 9 we have that $Z_1 \notin \mathcal{A}_1$, and that for all $i < \alpha$ there exists a subset $U_i \subset \mathcal{P}_1$ such that

$$P_1 \ldots P_i U_i \notin \mathcal{A}_1 \text{ and } P_1 \ldots P_i U_i P_{i+1} \in \mathcal{A}_1.$$

Similarly, we have that $Z_2 \notin \mathcal{A}_2$, and that for all $i < \beta$ there exists a subset $V_i \subset \mathcal{P}_2$ such that

$$Q_1 \ldots Q_i V_i \notin \mathcal{A}_2 \text{ and } Q_1 \ldots Q_i V_i Q_{i+1} \in \mathcal{A}_2.$$

Consider the sequence $Z_1 Z_2 = R_1 \ldots R_{\alpha+\beta}$, where $R_i = P_i$, for $i = 1, \ldots, \alpha$, and $R_i = Q_{i-\alpha}$, for $i = \alpha+1, \ldots, \alpha+\beta$. Since $Z_2 \notin \mathcal{A}_2$ and $Z_1 \subseteq \mathcal{P}_1 \setminus \mathcal{P}_2$, it holds that $Z_1 Z_2 \notin \mathcal{A}_2$. We distinguish two cases: $Z_1 Z_2 \notin \mathcal{A}_1$ and $Z_1 Z_2 \in \mathcal{A}_1$.

`Case` $Z_1 Z_2 \notin \mathcal{A}_1$, i.e., $\mathcal{I}(Z_1 Z_2) = \emptyset$. We prove that $Z_1 Z_2$ is an $(\alpha, \beta, 0)$-sequence for the pair of access structures $(\mathcal{A}_1, \mathcal{A}_2)$. It is easy to see that, for $i = 1, \ldots, \alpha-1$, the set $X_i = U_i$ satisfies

$$R_1 \ldots R_i X_i \notin \mathcal{A}_1 \text{ and } R_1 \ldots R_i X_i R_{i+1} \in \mathcal{A}_1$$

and, for $i = \alpha, \ldots, \alpha+\beta-1$, the set $Y_i = V_{i-\alpha+1}$ satisfies

$$R_1 \ldots R_i Y_i \notin \mathcal{A}_2 \text{ and } R_1 \ldots R_i Y_i R_{i+1} \in \mathcal{A}_2.$$

Therefore, from Definition 10 we have that $Z_1 Z_2$ is an $(\alpha, \beta, 0)$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$. Since $\mathcal{I}(Z_1 Z_2) = \emptyset$, the bound follows from Theorem 11.

`Case` $Z_1Z_2 \in \mathcal{A}_1$, i.e., $\mathcal{I}(Z_1Z_2) = \{1\}$. We prove that Z_1Z_2 is an $(\alpha, \beta-1, 1)$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$. Since $Z_1 \notin \mathcal{A}_1$, then there exists an index $i \in [\alpha, \ldots, \alpha+\beta]$ such that $R_1 \ldots R_i \notin \mathcal{A}_1$ and $R_1 \ldots R_{i+1} \in \mathcal{A}_1$. Hence, there exist two subsets $X_i^1 = \emptyset$ and $X_i^2 = V_{i-\alpha+1}$ such that

$$R_1 \ldots R_i X_i^1 \notin \mathcal{A}_1, \; R_1 \ldots R_i X_i^1 R_{i+1} \in \mathcal{A}_1,$$

$$R_1 \ldots R_i X_i^1 X_i^2 \notin \mathcal{A}_2, \text{ and } R_1 \ldots R_i X_i^1 X_i^2 R_{i+1} \in \mathcal{A}_2.$$

Therefore, Z_1Z_2 is an $(\alpha, \beta-1, 1)$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$. Hence, from Theorem 11, we get

$$\begin{aligned}\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] &\geq \alpha H(\mathbf{S}_1|\mathbf{S}_2) + (\beta-1)H(\mathbf{S}_2|\mathbf{S}_1) + H(\mathbf{S}_1\mathbf{S}_2) - H(\mathbf{S}_{\mathcal{I}(Z_1Z_2)}) \\ &= \alpha H(\mathbf{S}_1|\mathbf{S}_2) + \beta H(\mathbf{S}_2|\mathbf{S}_1) - H(\mathbf{S}_2|\mathbf{S}_1) + H(\mathbf{S}_1\mathbf{S}_2) - H(\mathbf{S}_1) \\ &\qquad\qquad\qquad\qquad\qquad\qquad (\text{since } \mathcal{I}(Z_1Z_2) = \{1\}) \\ &= \alpha H(\mathbf{S}_1|\mathbf{S}_2) + \beta H(\mathbf{S}_2|\mathbf{S}_1) \text{ (from (11) of Appendix).}\end{aligned}$$

Thus, inequality (7) is satisfied. If the secrets are independent, then inequality (8) directly follows from inequality (7). Inequality (8) is satisfied also when $Z_1 \cup (\mathcal{P}_1 \cap \mathcal{P}_2) \notin \mathcal{A}_1 \cup \mathcal{A}_2$. Indeed since, for $i = 1, \ldots, \alpha-1$, it holds that $(R_1 \ldots R_i U_i) \cap \mathcal{P}_2 = U_i \cap \mathcal{P}_2 = \mathcal{P}_1 \cap \mathcal{P}_2 \subset Z_1 \cup (\mathcal{P}_1 \cap \mathcal{P}_2)$, we have

$$R_1 \ldots R_i U_i \notin \mathcal{A}_1 \cup \mathcal{A}_2 \text{ and } R_1 \ldots R_i U_i R_{i+1} \in \mathcal{A}_1.$$

For $i = \alpha, \ldots, \alpha+\beta-1$, we get $(R_1 \ldots R_i V_{i-\alpha+1}) \cap \mathcal{P}_1 = Z_1 \cup (R_{\alpha+1} \ldots R_i V_{i-\alpha+1} \cap \mathcal{P}_1) = Z_1 \cup (\mathcal{P}_1 \cap \mathcal{P}_2)$ and it holds that

$$R_1 \ldots R_i V_{i-\alpha+1} \notin \mathcal{A}_1 \cup \mathcal{A}_2 \text{ and } R_1 \ldots R_i V_{i-\alpha+1} R_{i+1} \in \mathcal{A}_2.$$

Therefore, Z_1Z_2 is an $[\alpha, \beta, 0]$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$ and since $\mathcal{I}(Z_1Z_2) = \emptyset$, the inequality (8) follows from Theorem 13. □

Notice that if $Z_1 \cap \mathcal{P}_2 = \emptyset$ and $Z_2 \cap \mathcal{P}_2 = \emptyset$, then we have that $Z_1Z_2 \notin \mathcal{A}_1$ and $Z_1Z_2 \notin \mathcal{A}_2$, and, analogously to Theorem 15, we can prove that

$$\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq \alpha H(\mathbf{S}_1|\mathbf{S}_2) + \beta H(\mathbf{S}_2|\mathbf{S}_1).$$

Example 1. Let $\mathcal{P}_1 = \{P_1, P_2, P_3, P_5\}$ and $\mathcal{P}_2 = \{P_4, P_5, P_6, P_7\}$ be two sets of participants. Let $\mathcal{A}_1 = \{P_1P_2P_3, P_3P_5\}$ and $\mathcal{A}_2 = \{P_4P_5P_6, P_6P_7\}$ be two access structures on $\mathcal{P}_1$ and $\mathcal{P}_2$, respectively. It is easy to see that $Z_1 = P_1P_2$ and $Z_2 = P_4P_5$ are independent sequences for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. From Theorem 15, it holds that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq 2H(\mathbf{S}_1) + 2H(\mathbf{S}_2)$. This bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound it is enough to combine two independent single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, as follows: To share the secret $s_1 \in GF(q_1)$ the dealer randomly chooses two values x_1 and x_3 in $GF(q_1)$, then he distributes the shares as follows:

$$\begin{array}{ll} P_1 \text{ gets } x_1 & P_2 \text{ gets } x_1 + x_3 + s_1 \bmod q_1 \\ P_3 \text{ gets } x_3 & P_5 \text{ gets } s_1 + x_3 \bmod q_1. \end{array}$$

The number of random bits needed by the dealer to set up this scheme is $2\log q_1$. To share the secret $s_2 \in GF(q_2)$ the dealer randomly chooses two values x_4 and x_6 in $GF(q_2)$, then he distributes the shares as follows:

$$\begin{array}{ll} P_4 \text{ gets } x_4 & P_5 \text{ gets } x_4 + x_5 + s_2 \bmod q_2 \\ P_6 \text{ gets } x_6 & P_7 \text{ gets } s_2 + x_6 \bmod q_2. \end{array}$$

The number of random bits needed by the dealer to set up this scheme is $2\log q_2$. Hence, if we combine two independent copies of these single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, the number of random bits needed by the dealer is $2\log q_1 + 2\log q_2$. Therefore, the bound provided by Theorem 16 is tight. △

Theorem 16. *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. Let Z_1 (resp., Z_2) be an independent sequence of length α (resp., β) for $\mathcal{A}_1$ (resp., $\mathcal{A}_2$). Finally, assume that $|Z_1 \cap \mathcal{P}_2| = a$ and $|Z_2 \cap \mathcal{P}_1| = b$. If the secrets are independent, then it holds that*

$$\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq \alpha H(\mathbf{S}_1) + \beta H(\mathbf{S}_2) - \min\{aH(\mathbf{S}_1), bH(\mathbf{S}_2)\}.$$

Proof. Let $Z_1' = Z_1 \setminus \mathcal{P}_2$ and let $Z_2' = Z_2 \setminus \mathcal{P}_1$. It is easy to see that Z_1' (resp., Z_2') is an independent sequence of length $\alpha - a$ (resp., $\beta - b$) for $\mathcal{A}_1$ (resp., $\mathcal{A}_2$). Since the secrets are independent, applying Theorem 15 twice with (Z_1', Z_2) and (Z_1, Z_2'), respectively, we get $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq (\alpha - a)H(\mathbf{S}_1) + \beta H(\mathbf{S}_2)$ and $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq \alpha H(\mathbf{S}_1) + (\beta - b)H(\mathbf{S}_2)$. Thus, the theorem holds. □

Example 2. Let $\mathcal{P}_1 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ and $\mathcal{P}_2 = \{P_3, P_4, P_5, P_6, P_7, P_8\}$ be two sets of participants. Let $\mathcal{A}_1 = \{P_3, P_1P_2, P_4P_5P_6\}$ and $\mathcal{A}_2 = \{P_3P_5P_6, P_7P_8, P_4\}$ be two access structures on $\mathcal{P}_1$ and $\mathcal{P}_2$, respectively. It is easy to see that $Z_1 = P_4P_5P_1$ and $Z_2 = P_3P_5P_7$ are independent sequences for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. From Theorem 16, it holds that

$$\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq 3H(\mathbf{S}_1) + 3H(\mathbf{S}_2) - 2\min\{H(\mathbf{S}_1), H(\mathbf{S}_2)\}.$$

This bound is tight. Indeed, the scheme presented on page 2 uses exactly $\log q_1 + \log q_2 + 2\log q$ random bits. △

Corollary 17. *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. Let Z_1 (resp., Z_2) be an independent sequence of length α (resp., β) for $\mathcal{A}_1$ (resp., $\mathcal{A}_2$). Finally, assume that $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$. Then, it holds that*

$$\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq \alpha H(\mathbf{S}_1) + \beta H(\mathbf{S}_2).$$

Proof. The corollary follows from Theorem 15, as $Z_1 \cup (\mathcal{P}_1 \cap \mathcal{P}_2) = Z_1$ and $Z_1 \notin \mathcal{A}_1 \cup \mathcal{A}_2$. □

Example 3. Let $\mathcal{P}_1 = \{P_1, P_2, P_3, P_4, P_5\}$ and $\mathcal{P}_2 = \{P_6, P_7, P_8, P_9\}$ be two sets of participants. Let $\mathcal{A}_1 = \{P_1P_4, P_2P_5, P_3P_5\}$ and $\mathcal{A}_2 = \{P_6P_7P_8, P_6P_7P_9\}$ be two access structures on $\mathcal{P}_1$ and $\mathcal{P}_2$, respectively. It is easy to see that $Z_1 = P_1P_2$ and $Z_2 = P_7P_8$ are independent sequences for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. From Corollary 17, it holds that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq 2H(\mathbf{S}_1) + 2H(\mathbf{S}_2)$. This bound is tight.

Indeed, to realize a multi–secret sharing scheme meeting this bound it is enough to combine two independent single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, as follows: To share the secret $s_1 \in GF(q_1)$ the dealer randomly chooses three values x_1, x_4 and x_5 in $GF(q_1)$, then he distributes the shares as follows:

$$\begin{array}{lll} P_1 \text{ gets } x_1 & P_2 \text{ gets } x_1 + s_1 \bmod q_1 & P_3 \text{ gets } s_1 \\ P_4 \text{ gets } x_4 & P_5 \text{ gets } x_5 & P_6 \text{ gets } x_4 + x_5 + s_1 \bmod q_1. \end{array}$$

The number of random bits needed by the dealer to set up this scheme is $3 \log q_1$. To share the secret $s_2 \in GF(q_2)$ the dealer randomly chooses three values x_3, x_5 and x_7 in $GF(q_2)$, then he distributes the shares as follows:

$$\begin{array}{lll} P_3 \text{ gets } x_3 & P_4 \text{ gets } s_2 & P_5 \text{ gets } x_5 \\ P_6 \text{ gets } x_3 + x_5 + s_2 \bmod q_2 & P_7 \text{ gets } x_7 & P_8 \text{ gets } x_7 + s_2. \end{array}$$

The number of random bits needed by the dealer to set up this scheme is $3 \log q_2$. Hence, if we combine two independent copies of these single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, the number of random bits needed by the dealer is $3 \log q_1 + 3 \log q_2$. Therefore, the bound provided by Corollary 17 is tight.

$\triangle$

6 Randomness for Threshold Structures

In this section we derive bounds on the dealer's randomness for pairs of access structures. More precisely, we analyze the case in which at least one of the access structures $\mathcal{A}_1$ and $\mathcal{A}_2$ is a threshold structure. We denote by $\mathcal{A}_{(k_i, \mathcal{P}_i)}$ the access structure consisting of all subsets of participants in $\mathcal{P}_i$ of cardinality at least k_i.

Theorem 18. *Let $\mathcal{A}_{(k,\mathcal{P}_1)}$ be a threshold structure on the set of participants $\mathcal{P}_1$ and let $\mathcal{A}_2$ be an access structure on the set of participants $\mathcal{P}_2$. Let Z be an independent sequence of length β for $\mathcal{A}_2$. Finally, assume that the secrets are independent. Then, it holds that*

$$\mu[(\mathcal{A}_{(k,\mathcal{P}_1)}, \mathcal{A}_2), (q_1, q_2)] \geq (k-1)H(\mathbf{S}_1) + \beta H(\mathbf{S}_2).$$

Proof. Assume that $Z = Q_1 \ldots Q_\beta$, where $Q_1, \ldots, Q_\beta \in \mathcal{P}_2$, is an independent sequence for $\mathcal{A}_2$ and let $|Z \cap \mathcal{P}_1| = t$. For the sake of simplicity assume that $Z \cap \mathcal{P}_1 = Q_1 \ldots Q_t$. We distinguish two cases: $t < k$ and $t \geq k$.

`Case` $t < k$.
Let $P_1, \ldots, P_{k-t-1} \in \mathcal{P}_1 \backslash Z$. Consider the sequence $W = R_1 \ldots R_{\beta+k-t-1}$, where $R_i = Q_i$, for $i = 1, \ldots, \beta$, and $R_i = P_{i-\beta}$, for $i = \beta+1, \ldots, \beta+k-t-1$. Since $|W \cap \mathcal{P}_1| = k-1$, we have that $W \notin \mathcal{A}_1$. Since Z is an independent sequence for $\mathcal{A}_2$, from Definition 9 it holds that, for all $i = 1, \ldots, \beta-1$, there exists a set $V_i \subset \mathcal{P}_2$, such that

$$Q_1 \ldots Q_i V_i \notin \mathcal{A}_2 \text{ and } Q_1 \ldots Q_i V_i Q_{i+1} \in \mathcal{A}_2.$$

For $i = 1, \ldots, t-1$, let $T_i = \{Q_1, \ldots, Q_i\} \cup V_i$, and let $\lambda_i = |T_i \cap \mathcal{P}_1|$. We distinguish two cases: $\lambda_i < k$ and $\lambda_i \geq k$.

If $\lambda_i < k$, then there exists a subset $X_i \subset \mathcal{P}_1 \setminus Z$ such that $|(T_i X_i) \cap \mathcal{P}_1| = k-1$. This implies that

$$\begin{array}{l} R_1 \ldots R_i V_i \notin \mathcal{A}_2, \\ R_1 \ldots R_i V_i R_{i+1} \in \mathcal{A}_2, \\ R_1 \ldots R_i V_i X_i \notin \mathcal{A}_1, \\ R_1 \ldots R_i V_i X_i R_{i+1} \in \mathcal{A}_1. \end{array} \tag{9}$$

On the other hand, if $\lambda_i \geq k$, then there exists a subset $W_i \subset V_i \cap \mathcal{P}_1$, such that $|(Q_1 \ldots Q_i W_i) \cap \mathcal{P}_1| = k-1$. This implies that

$$\begin{array}{l} R_1 \ldots R_i W_i \notin \mathcal{A}_1, \\ R_1 \ldots R_i W_i R_{i+1} \in \mathcal{A}_1, \\ R_1 \ldots R_i W_i V_i X_i \notin \mathcal{A}_2, \\ R_1 \ldots R_i W_i V_i X_i R_{i+1} \in \mathcal{A}_2. \end{array} \tag{10}$$

Moreover, for $i = t, \ldots, \beta - 1$, it holds that

$$R_1 \ldots R_i V_i \notin \mathcal{A}_2 \text{ and } R_1 \ldots R_i V_i R_{i+1} \in \mathcal{A}_2.$$

Finally, if $W \notin \mathcal{A}_2$, (i.e., $\mathcal{I}(W) = \emptyset$), then, for $i = \beta, \ldots, \beta + k - t - 2$, there exists the set $Y_i = R_{i+2} \ldots R_{\beta+k-t} \subset \mathcal{P}_1 \setminus Z$ such that

$$R_1 \ldots R_i Y_i \notin \mathcal{A}_1 \text{ and } R_1 \ldots R_i Y_i R_{i+1} \in \mathcal{A}_1.$$

Hence, W is a $(k-t-1, \beta-t, t)$-sequence for $(\mathcal{A}_{(k,\mathcal{P}_1)}, \mathcal{A}_2)$. Since $\mathcal{I}(W) = \emptyset$, the bound follows from Theorem 11.
If $W \in \mathcal{A}_2$ (i.e., $\mathcal{I}(W) = \{2\}$), then, for $i = \beta, \ldots, \beta + k - t - 2$, there exists the set $Y_i = R_{i+2} \ldots R_{\beta+k-t} \subset \mathcal{P}_1 \setminus Z$ such that

$$R_1 \ldots R_i \notin \mathcal{A}_2, \; R_1 \ldots R_i R_{i+1} \in \mathcal{A}_2,$$

$$R_1 \ldots R_i Y_i \notin \mathcal{A}_1 \text{ and } R_1 \ldots R_i Y_i R_{i+1} \in \mathcal{A}_1.$$

Hence, W is a $(k-t-2, \beta-t, t+1)$-sequence for $(\mathcal{A}_{(k,\mathcal{P}_1)}, \mathcal{A}_2)$. Since $\mathcal{I}(W) = \{2\}$, the bound follows from Theorem 11.

`Case` $t \geq k$.
Since $Z \in \mathcal{A}_1 \setminus \mathcal{A}_2$ (i.e, $\mathcal{I}(Z) = \{1\}$), for $i = 1, \ldots, t$, the participant R_{i+1} satisfies either (9) or (10). Hence, Z is a $(0, \beta - k, k)$-sequence for $(\mathcal{A}_{(k,\mathcal{P}_1)}, \mathcal{A}_2)$. Since $\mathcal{I}(W) = \{1\}$, the theorem follows from Theorem 11. □

Example 4. Let $\mathcal{A}_1$ be the access structure of a $(4,5)$-threshold scheme on $\mathcal{P}_1 = \{P_1, P_2, P_3, P_4, P_5\}$ and let $\mathcal{A}_2 = \{P_4P_5P_6, P_6P_7\}$ be an access structure on $\mathcal{P}_2 = \{P_4, P_5, P_6, P_7\}$. It is easy to see that $Z_1 = P_1P_2P_3$ and $Z_2 = P_4P_5$ are independent sequences for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. From Theorem 18, it holds that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq 3H(\mathbf{S}_1) + 2H(\mathbf{S}_2)$. This bound is tight.
Indeed, to realize a multi–secret sharing scheme meeting this bound it is enough to combine two independent single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, as follows: To share the secret $s_1 \in GF(q_1)$ the dealer uses a $(4,5)$ Shamir's threshold scheme, so the number of random bits he uses is $3 \log q_1$. To share the secret $s_2 \in GF(q_2)$ the dealer randomly chooses two values x_4 and x_6 in $GF(q_2)$, then he distributes the shares as follows:

$$P_4 \text{ gets } x_4 \quad P_5 \text{ gets } x_4 + x_6 + s_2 \bmod q_2$$
$$P_6 \text{ gets } x_6 \quad P_7 \text{ gets } x_6 + s_2 \bmod q_2.$$

The number of random bits needed by the dealer to set up this scheme is $2 \log q_2$. Hence, if we combine two independent copies of these single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, the number of random bits needed by the dealer is $3 \log q_1 + 2 \log q_2$. Therefore, the bound provided by Theorem 18 is tight. $\triangle$

In the following theorem we consider a pair of threshold structures on different sets of participants. Notice that this situation is different from that considered in Section 4.1, in which we analyze many threshold structures with the same threshold where the sets of participants are such that $\mathcal{P}_i \subseteq P_{i+1}$ for $i = 1, \ldots, m-1$.

Theorem 19. *Let $\mathcal{A}_{(k_1,\mathcal{P}_1)}$ and $\mathcal{A}_{(k_2,\mathcal{P}_2)}$ be two threshold structures on the sets of participants $\mathcal{P}_1$ and $\mathcal{P}_2$, respectively. Assume $k_1 \leq k_2$ and let $|\mathcal{P}_1 \cap \mathcal{P}_2| = t$. If $t < k_1$, then it holds that*

$$\mu[(\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}), (q_1, q_2)] \geq (k_1-t-1)H(\mathbf{S}_1)+(k_2-t-1)H(\mathbf{S}_2)+tH(\mathbf{S}_1\mathbf{S}_2);$$

if $k_1 \leq t < k_2$ or, $t \geq k_2$ and $k_1 \neq k_2$, then it holds that

$$\mu[(\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}), (q_1, q_2)] \geq (k_1 - 1)H(\mathbf{S}_1\mathbf{S}_2) + (k_2 - k_1)H(\mathbf{S}_2|\mathbf{S}_1);$$

otherwise, it holds that

$$\mu[(\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}), (q_1, q_2)] \geq (k_2 - 1)H(\mathbf{S}_1\mathbf{S}_2).$$

Finally, if the secrets are independent, then it holds that

$$\mu[(\mathcal{A}_{(k_1,\mathcal{P}_1)}, \mathcal{A}_{(k_2,\mathcal{P}_2)}), (q_1, q_2)] \geq (k_1 - 1)H(\mathbf{S}_1) + (k_2 - 1)H(\mathbf{S}_2).$$

Proof. For the sake of simplicity, denote by $\mathcal{A}_1$ and $\mathcal{A}_2$ the threshold structures $\mathcal{A}_{(k_1,\mathcal{P}_1)}$ and $\mathcal{A}_{(k_2,\mathcal{P}_2)}$, respectively. Let $\mathcal{P}_1 = \{R_1, \ldots, R_t, P_{t+1}, \ldots, P_{|\mathcal{P}_1|}\}$ and $\mathcal{P}_2 = \{R_1, \ldots, R_t, Q_{t+1}, \ldots, Q_{|\mathcal{P}_2|}\}$, and recall that $k_1 \leq k_2$.
If $t < k_1$, then consider the sequence $Z = Z_1 \ldots Z_{k_1+k_2-t-2}$ where $Z_i = R_i$, for $i = 1, \ldots, t$, $Z_i = P_i$, for $i = t+1, \ldots, k_1 - 1$, and $Z_i = Q_{i+t-k_1+1}$, for $i = k_1, \ldots, k_1 + k_2 - t - 2$. It is easy to see that $Z \notin \mathcal{A}_1 \cup \mathcal{A}_2$ (i.e., $\mathcal{I}(Z) = \emptyset$).
For $i = 1, \ldots, t-1$, we have that

$$Z_1 \ldots Z_i X_i \notin \mathcal{A}_1, \; Z_1 \ldots Z_i X_i Z_{i+1} \in \mathcal{A}_1,$$

$$Z_1 \ldots Z_i X_i Y_i \notin \mathcal{A}_2, \text{ and } Z_1 \ldots Z_i X_i Y_i Z_{i+1} \in \mathcal{A}_2,$$

where $X_i = Z_{i+2} \ldots Z_{k_1}$ and $Y_i = Z_{k_1+1} \ldots Z_{k_2}$.
For $i = t, \ldots, k_1 - 2$, we have that

$$Z_1 \ldots Z_i V_i \notin \mathcal{A}_1 \cup \mathcal{A}_2, \text{ and } Z_1 \ldots Z_i V_i Z_{i+1} \in \mathcal{A}_1,$$

where $V_i = Z_{i+2} \ldots Z_{k_1}$.
Finally, for $i = k_1 - 1, \ldots, k_1 + k_2 - t - 3$, we have that

$$Z_1 \ldots Z_i W_i \notin \mathcal{A}_1 \cup \mathcal{A}_2 \text{ and } Z_1 \ldots Z_i W_i Z_{i+1} \in \mathcal{A}_2,$$

where $W_i = Z_{i+2} \ldots Z_{k_1+k_2-t-1}$.

Therefore, Z is a $[k_1-t-1, k_2-t-1, t]$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$. Since $\mathcal{I}(Z)=\emptyset$, the bound follows from Theorem 13.

Assume now that $k_1 \le t < k_2$ and consider the sequence $Z = Z_1 \ldots Z_{k_2-1}$, where $Z_i = R_i$, for $i=1,\ldots,t$, and $Z_i = Q_i$, for $i=t+1,\ldots,k_2-1$. Since $k_1 \le t$, we have that $\mathcal{I}(Z)=\{1\}$.
For $i=1,\ldots,k_1-1$, we have that

$$Z_1 \ldots Z_i X_i \notin \mathcal{A}_1,\ Z_1 \ldots Z_i X_i Z_{i+1} \in \mathcal{A}_1,$$

$$Z_1 \ldots Z_i X_i Y_i \notin \mathcal{A}_2,\ \text{and } Z_1 \ldots Z_i X_i Y_i Z_{i+1} \in \mathcal{A}_2,$$

where $X_i = Z_{i+2} \ldots Z_{k_1}$ and $Y_i = Z_{k_1+1} \ldots Z_{k_2-1} Q_{k_2}$.
For $i=k_1,\ldots,t-1$, we have that

$$Z_1 \ldots Z_i U_i \notin \mathcal{A}_2 \text{ and } Z_1 \ldots Z_i U_i Z_{i+1} \in \mathcal{A}_2,$$

where $U_i = Z_{i+2} \ldots Z_{k_2-1} Q_{k_2}$.
Finally, for $i=t,\ldots,k_2-1$, we have that

$$Z_1 \ldots Z_i V_i \notin \mathcal{A}_2 \text{ and } Z_1 \ldots Z_i V_i Z_{i+1} \in \mathcal{A}_2,$$

where $V_i = Z_{i+2} \ldots Z_{k_2-1} Q_{k_2}$.
Hence, Z is a $(0, k_2-k_1-1, k_1)$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$. Since $\mathcal{I}(Z)=\{1\}$, the bound follows from Theorem 11.

Assume now that $t \ge k_2$ and $k_1 \ne k_2$. Consider the sequence $Z = R_1 \ldots R_{k_2-1}$. Since $|Z| \ge k_1$, we have that $\mathcal{I}(Z)=\{1\}$.
For $i=1,\ldots,k_1-1$, we have that

$$R_1 \ldots R_i X_i \notin \mathcal{A}_1,\ R_1 \ldots R_i X_i R_{i+1} \in \mathcal{A}_1,$$

$$R_1 \ldots R_i X_i Y_i \notin \mathcal{A}_2,\ \text{and } R_1 \ldots R_i X_i Y_i R_{i+1} \in \mathcal{A}_2,$$

where $X_i = R_{i+2} \ldots R_{k_1}$ and $Y_i = R_{k_1+1} \ldots R_{k_2}$.
For $i=k_1,\ldots,k_2-1$, it holds that

$$R_1 \ldots R_i U_i \notin \mathcal{A}_2 \text{ and } R_1 \ldots R_i U_i R_{i+1} \in \mathcal{A}_2,$$

where $U_i = R_{i+2} \ldots R_{k_2}$.
Hence, Z is a $(0, k_2-k_1-1, k_1)$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$. Since $\mathcal{I}(Z)=\{1\}$, the bound follows from Theorem 11.

Assume now that $t \ge k_2$ and $k_1 = k_2$. Consider the sequence $Z = R_1 \ldots R_{k_2-1}$. Notice that $\mathcal{I}(Z)=\emptyset$.
For $i=1,\ldots,k_2-1$, we have that

$$R_1 \ldots R_i V_i \notin \mathcal{A}_1,\ R_1 \ldots R_i V_i R_{i+1} \in \mathcal{A}_1,$$

$$R_1 \ldots R_i V_i \notin \mathcal{A}_2,\ \text{and } R_1 \ldots R_i V_i R_{i+1} \in \mathcal{A}_2,$$

where $V_i = R_{i+2} \ldots R_{k_2}$.
Hence, Z is a $(0, 0, k_2-1)$-sequence for $(\mathcal{A}_1, \mathcal{A}_2)$. Since $\mathcal{I}(Z)=\emptyset$, the bound follows from Theorem 11.

Finally, if the secrets are independent, then the bound follows from Theorem 18. $\square$

The bounds provided by Theorem 19 are tight, as shown in the following examples. The following setting is common to all examples: Suppose that the secrets s_1 and s_2 are chosen from S_1 and S_2, respectively, where $S_1 = S_2 = GF(q^2)$ and q is a prime power. We first consider the case of independent secrets. Moreover, we consider the case $s_1 = u \circ v$ and $s_2 = u \circ w$, where $x \circ y$ denotes the concatenation of x and y, and u, v and w are uniformly chosen from $GF(q)$. It is easy to see that $H(\mathbf{S}_1|\mathbf{S}_2) = H(\mathbf{S}_2|\mathbf{S}_1) = 0.5H(\mathbf{S}_1) = 0.5H(\mathbf{S}_2) = \log q$.

Example 5 (Case $t < k_1$). Let $\mathcal{P}_1 = \{P_1, P_2\}$ and $\mathcal{P}_2 = \{P_1, P_3\}$ be two sets of participants. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be the access structures of a $(2,2)$ threshold scheme on $\mathcal{P}_1$ and on $\mathcal{P}_2$, respectively. If the secrets are independent, then from Theorem 19 we get $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1) + H(\mathbf{S}_2)$. This bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound it is enough to combine two independent single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$. If the secrets are dependent, then from Theorem 19 it holds that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1\mathbf{S}_2)$. If $H(\mathbf{S}_1|\mathbf{S}_2) = H(\mathbf{S}_2|\mathbf{S}_1) = 0.5H(\mathbf{S}_1) = 0.5H(\mathbf{S}_2)$, then this bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound we share the value v among participants in $\mathcal{P}_1$ by using a $(2,2)$ threshold scheme; whereas, we share the value w among participants in $\mathcal{P}_2$ by using a $(2,2)$ threshold scheme. Finally, we share the value u according to the access structure $\mathcal{A} = \{P_1P_2, P_1P_3\}$. It is easy to see that the number of random bits needed by the dealer to set up the scheme is $3 \log q = H(\mathbf{S}_1\mathbf{S}_2)$. Therefore, the bound provided by Theorem 19 is tight. $\triangle$

Example 6 (Case $k_1 \leq t < k_2$). Let $\mathcal{A}_1$ be the access structure of a $(2,3)$ threshold scheme on $\mathcal{P}_1 = \{P_1, P_2, P_3\}$ and let $\mathcal{A}_2$ be the access structure of a $(5,6)$ threshold scheme on $\mathcal{P}_2 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. If the secrets are independent, then from Theorem 19 we have that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1) + 4H(\mathbf{S}_2)$. This bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound it is enough to combine two independent single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. If the secrets are dependent, then from Theorem 19 it holds that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1\mathbf{S}_2) + 3H(\mathbf{S}_2|\mathbf{S}_1)$. If $H(\mathbf{S}_1|\mathbf{S}_2) = H(\mathbf{S}_2|\mathbf{S}_1) = 0.5H(\mathbf{S}_1) = 0.5H(\mathbf{S}_2)$, then this bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound we share the value u among participants in $\mathcal{P}_1$ by using a $(2,3)$ threshold scheme; whereas, we share the value v among participants in $\mathcal{P}_1$ by using a $(2,3)$ threshold scheme. Finally, we share the value w among participants in $\mathcal{P}_2$ by using a $(5,6)$ threshold scheme. It is easy to see that the number of random bits needed by the dealer to set up the scheme is $6 \log q = H(\mathbf{S}_1\mathbf{S}_2) + 3H(\mathbf{S}_2|\mathbf{S}_1)$. Therefore, the bound provided by Theorem 19 is tight. $\triangle$

Example 7 (Case $t \geq k_2$ and $k_1 \neq k_2$). Let $\mathcal{A}_1$ be the access structure of a $(2,3)$ threshold scheme on $\mathcal{P}_1 = \{P_1, P_2, P_3\}$ and let $\mathcal{A}_2$ be the access structure of a $(3,4)$ threshold scheme on $\mathcal{P}_2 = \{P_1, P_2, P_3, P_4\}$. If the secrets are independent, then from Theorem 19 we have that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1) + 2H(\mathbf{S}_2)$. This bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound it is enough to combine two independent single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. If the secrets are dependent, then from Theorem 19 it holds that $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1\mathbf{S}_2) + H(\mathbf{S}_2|\mathbf{S}_1)$. If $H(\mathbf{S}_1|\mathbf{S}_2) = H(\mathbf{S}_2|\mathbf{S}_1) = 0.5H(\mathbf{S}_1) = 0.5H(\mathbf{S}_2)$, then this bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound we share the value u among participants in $\mathcal{P}_1$ by using a $(2,3)$ threshold scheme; whereas, we share the value v among participants in $\mathcal{P}_1$ by using a $(2,3)$ threshold scheme. Finally, we share the value w among participants in $\mathcal{P}_2$ by using a $(3,4)$ threshold scheme. It is easy to see that the number of random bits needed by the dealer to set up the scheme is $4\log q = H(\mathbf{S}_1\mathbf{S}_2) + H(\mathbf{S}_2|\mathbf{S}_1)$. Therefore, the bound provided by Theorem 19 is tight. $\triangle$

Example 8 (Case $t \geq k_2$ and $k_1 = k_2$). Let $\mathcal{A}_1$ be the access structure of a $(2,4)$ threshold scheme on $\mathcal{P}_1 = \{P_1, P_2, P_3, P_4\}$ and let $\mathcal{A}_2$ be the access structure of a $(2,5)$ threshold scheme on $\mathcal{P}_2 = \{P_1, P_2, P_3, P_4, P_5\}$. If the secrets are independent, then from Theorem 19 we get $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1) + H(\mathbf{S}_2)$. This bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound it is enough to combine two independent single secret sharing schemes for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. If the secrets are dependent, then from Theorem 19 we get $\mu[(\mathcal{A}_1, \mathcal{A}_2), (q_1, q_2)] \geq H(\mathbf{S}_1\mathbf{S}_2)$. If $H(\mathbf{S}_1|\mathbf{S}_2) = H(\mathbf{S}_2|\mathbf{S}_1) = 0.5H(\mathbf{S}_1) = 0.5H(\mathbf{S}_2)$, then this bound is tight. Indeed, to realize a multi–secret sharing scheme meeting this bound we share the value u among participants in $\mathcal{P}_1$ by using a $(2,4)$ threshold scheme; whereas, we share the value v among participants in $\mathcal{P}_1$ by using a $(2,4)$ threshold scheme. Finally, we share the value w among participants in $\mathcal{P}_2$ by using a $(2,5)$ threshold scheme. It is easy to see that the number of random bits needed by the dealer to set up the scheme is $3\log q = H(\mathbf{S}_1\mathbf{S}_2)$. Therefore, the bound provided by Theorem 19 is tight. $\triangle$

Acknowledgements

We would like to thank the anonymous referees for their careful reading and useful comments.

Appendix
Information Theory Background

In this Appendix we review the basic concepts of Information Theory used in our definitions and proofs. For a complete treatment of the subject the reader is advised to consult [Cover et al. 91].

Given a probability distribution $\{Pr_X(x)\}_{x\in X}$ on a set X, the Shannon *entropy* of $\mathbf{X}$, denoted by $H(\mathbf{X})$, is defined as

$$H(\mathbf{X}) = -\sum_{x\in X} Pr_X(x)\log Pr_X(x)$$

(all logarithms in this paper are to the base 2). Given two sets X and Y and a joint probability distribution on their cartesian product, the *conditional entropy* $H(\mathbf{X}|\mathbf{Y})$, is defined as

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y\in Y}\sum_{x\in X} Pr_Y(y)Pr(x|y)\log Pr(x|y).$$

From the definition of conditional entropy it is easy to see that $H(\mathbf{X}|\mathbf{Y}) \geq 0$.

Given $n+1$ sets $X_1,\ldots,X_n,Y$ and a joint probability distribution on their cartesian product, the entropy of $\mathbf{X}_1\ldots\mathbf{X}_n$ satisfies

$$H(\mathbf{X}_1\ldots\mathbf{X}_n) = H(\mathbf{X}_1) + H(\mathbf{X}_2|\mathbf{X}_1) + \cdots + H(\mathbf{X}_n|\mathbf{X}_1\ldots\mathbf{X}_{n-1}); \qquad (11)$$

whereas, the entropy of $\mathbf{X}_1\ldots\mathbf{X}_n$ given $\mathbf{Y}$ can be expressed as

$$H(\mathbf{X}_1\ldots\mathbf{X}_n|\mathbf{Y}) = H(\mathbf{X}_1|\mathbf{Y}) + \sum_{i=2}^{n} H(\mathbf{X}_i|\mathbf{X}_1\ldots\mathbf{X}_{i-1}\mathbf{Y}). \qquad (12)$$

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

$$I(\mathbf{X};\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{Y}) - H(\mathbf{Y}|\mathbf{X})$$

and satisfies $I(\mathbf{X};\mathbf{Y}) \geq 0$, from which one gets $H(\mathbf{X}) \geq H(\mathbf{X}|\mathbf{Y})$.

Given $n+2$ sets $X,Y,Z_1,\ldots,Z_n$ and a joint probability distribution on their cartesian product, the *conditional mutual information* $I(\mathbf{X};\mathbf{Y}|\mathbf{Z}_1\ldots\mathbf{Z}_n)$ between $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{Z}_1,\ldots,\mathbf{Z}_n$ can be written as

$$\begin{aligned} I(\mathbf{X};\mathbf{Y}|\mathbf{Z}_1\ldots\mathbf{Z}_n) &= H(\mathbf{X}|\mathbf{Z}_1\ldots\mathbf{Z}_n) - H(\mathbf{X}|\mathbf{Z}_1\ldots\mathbf{Z}_n\mathbf{Y}) \qquad (13)\\ &= H(\mathbf{Y}|\mathbf{Z}_1\ldots\mathbf{Z}_n) - H(\mathbf{Y}|\mathbf{Z}_1\ldots\mathbf{Z}_n\mathbf{X}). \end{aligned}$$

Since the conditional mutual information is always non negative we get

$$H(\mathbf{X}|\mathbf{Z}_1\ldots\mathbf{Z}_n) \geq H(\mathbf{X}|\mathbf{Z}_1\ldots\mathbf{Z}_n\mathbf{Y}). \qquad (14)$$

References

[Blakley 79] Blakley, G. R.: *"Safeguarding Cryptographic Keys"*; Proc. AFIPS 1979 National Computer Conference (1979), 313–317.

[Blakley et al. 90] Benaloh, J. C., Leichter, J.: *Generalized Secret Sharing and Monotone Functions*; Proc. Advances in Cryptology - CRYPTO '88, LNCS 403 (1990), 27–35.

[Blundo et al. 98a] Blundo, C., De Santis, A., Di Crescenzo, G., Giorgio Gaggia, A., Masucci, B., Vaccaro, U.: *"Secret Sharing of Many Secrets"*; submitted for publication (1998). Avalaible on line at `http://www.unisa.it/~masucci`

[Blundo et al. 94] Blundo, C., De Santis, A., Di Crescenzo, G., Giorgio Gaggia, A., Vaccaro, U.: *"Multi–Secret Sharing Schemes"*; Proc. Advances in Cryptology - CRYPTO '94, LNCS 839 (1994), 150–163.

[Blundo et al. 93] Blundo, C., De Santis, A., Vaccaro, U.: *"Efficient Sharing of Many Secrets"*; Proc. 10*th* Symp. on Theoretical Aspects of Computer Science - STACS '93, LNCS 665 (1993), 692–703.

[Blundo et al. 98b] Blundo, C., De Santis, A., Vaccaro, U.: *"On Secret Sharing Schemes"*; Information Processing Letters, 65, 1 (1998), 25–32.

[Blundo et al. 96] Blundo, C., De Santis, A., Vaccaro, U.: *"Randomness in Distribution Protocols"*; Information and Computation, 131 (1996), 111–139.

[Blundo et al. 97] Blundo, C., Giorgio Gaggia, A., Stinson, D. R.: *"On the Dealer's Randomness Required in Secret Sharing Schemes"*; Design, Codes, and Cryptography, 11, 2 (1997), 107–122.

[Blundo et al 98c] Blundo, C., Masucci, B., *"A Note on the Randomness in Dynamic Threshold Schemes"*; Journal of Computer Security, to appear.

[Capocelli et al. 93] Capocelli, R. M., De Santis, A., Gargano, L., Vaccaro, U.: *"On the Size of Shares for Secret Sharing Schemes"*; Journal of Cryptology, 6 (1993), 57–167.

[Cohen et al. 89] Cohen, A., Wigderson, A.: *"Dispersers, Deterministic Amplification and Weak Random Sources"*;, Proc. 30th IEEE Symposium on Foundations of Computer Science (1989), 14–19.

[Cover et al. 91] Cover, T. M., Thomas, J. A.: *"Elements of Information Theory"*; John Wiley & Sons (1991).

[Czirimaz 96] Czirimaz, L.: *"The Dealer's Random Bits in Secret Sharing Schemes"*; Studia Sci. Math. Hungar., 32 (1996), 429–437.

[De Santis et al. 99] De Santis, A., Masucci, B.: *"Multiple Ramp Schemes"*, IEEE Transactions on Information Theory, 45, 5 (1999), 1720–1728.

[Ding et al. 97] Ding, C., Laihonen, T., Renvall, A.: *"Linear Multisecret-Sharing Schemes and Error-Correcting Codes"*; Journal of Universal Computer Science, 3, 9 (1997), 1023–1036.

[Franklin et al.] Franklin M., Yung, M.: *"Communication Complexity of Secure Computation"*; Proc. 24th Annual ACM Symposium on Theory of Computing (1992), 699–710.

[Impagliazzo et al. 89] Impagliazzo, R., Zuckerman, D.: *"How to Recycle Random Bits"*; Proc. 30th IEEE Symposium on Foundations of Computer Science (1989), 248–255.

[Ito et al. 93] Ito, M., Saito, A., Nishizeki, T.: *Multiple Assignment Scheme for Sharing Secret*; Journal of Cryptology, 6 (1993), 15–20.

[Karnin et al. 83] Karnin, E. D., Greene, J. W., Hellman, M. E.: *"On Secret Sharing Systems"*; IEEE Transactions on Information Theory, 29, 1 (1983), 35–41.

[Knuth et al. 76] Knuth, D. E., Yao, A. C.: *"The Complexity of Nonuniform Random Number Generation"*; in Algorithms and Complexity, Academic Press (1976), 357–428.

[Koller et al. 93] Koller, D., Megiddo, N.: *"Constructing Small Sample Spaces Satisfying Given Constraints"*; Proc. 25th Annual ACM Symposium on Theory of Computing (1993), 268–277.

[Krizanc et al. 88] Krizanc, D., Peleg, D., Upfal, E.: *"A Time–Randomness Tradeoff for Oblivious Routing"*; Proc. 20th Annual ACM Symposium on Theory of Computing (1988), 93–102.

[Kushilevitz et al. 94] Kushilevitz, E., Rosen, A.: *"A Randomness-Rounds Tradeoff in Private Computation"*; Proc. Advances in Cryptology - CRYPTO 94, LNCS 839 (1994), 397–410.

[Jackson et al. 93] Jackson, W.-A., Martin, K. M., O'Keefe, C. M.: *"Multisecret Threshold Schemes"*; Proc. Advances in Cryptology - CRYPTO '93, LNCS 773 (1994), 126–135.

[Jackson et al. 94] Jackson, W.-A., Martin, K. M., O'Keefe, C. M.: *"On Sharing Many Secrets"*; Proc. Advances in Cryptology – ASIACRYPT '94, LNCS 917 (1995), 42–54.

[Jackson et al. 96] Jackson, W.-A., Martin, K. M., O'Keefe, C. M.: *"Ideal Secret Sharing Schemes with Multiple Secrets"*; Journal of Cryptology, 9 (1996), 233–250.

[McEliece et al. 81] McEliece, R. J., Sarwate, D.: *"On Sharing Secrets and Reed–Solomon Codes"*; Communications of the ACM, 24, 9 (1981), 583–584.

[Naor et al. 93] Naor, J., Naor, M.: *"Small-Bias Probability Spaces: Efficient Constructions and Applications"*; SIAM Journal of Computing, 22, 4 (1993), 838–856.

[Nisan 90] Nisan, N.: *"Pseudorandom Generator for Space Bounded Computation"*, Proc. 22nd Annual ACM Symposium on Theory of Computing (1990), 204–212.

[Shamir 79] Shamir, A.: *"How to Share a Secret"*; Communications of the ACM, 22, 11 (1979), 612–613.

[Simmons 91] Simmons, G. J.: *"An Introduction to Shared Secret and/or Shared Control Schemes and Their Applications"*; Contemporary Cryptology, IEEE Press (1991), 441–497.

[Stinson 92] Stinson, D. R.: *"An Explication of Secret Sharing Schemes"*; Design, Codes, and Cryptography, 2 (1992), 357–390.

[Stinson] Stinson, D. R.: *Bibliography on Secret Sharing*, Available on-line as `http://cacr.math.uwaterloo.ca/~dstinson/ssbib.html`