On the Dealer's Randomness Required in Secret Sharing Schemes

C. Blundo[1,*], A. Giorgio Gaggia[1], and D.R. Stinson[2]

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

[2] Department of Computer Science and Engineering,
and Center for Communication and Information Sciences,
University of Nebraska-Lincoln, Lincoln, NE-68588, USA

Abstract. The problem we deal with in this paper is the research of upper and lower bounds on the randomness required by the dealer to set up a secret sharing scheme. We give both lower and upper bounds for infinite classes of access structures. Lower bounds are obtained using entropy arguments. Upper bounds derive from a decomposition construction based on combinatorial designs (in particular, t-(v, k, λ) designs). We prove a general result on the randomness needed to construct a scheme for the cycle C_n; when n is odd our bound is tight. We study the access structures on at most four participants and the connected graphs on five vertices, obtaining exact values for the randomness for all them. Also, we analyze the number of random bits required to construct anonymous threshold schemes, giving upper bounds. (Informally, anonymous threshold schemes are schemes in which the secret can be reconstructed without knowledge of which participants hold which shares.)

1 Introduction

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 reducing the number of random bits used by probabilistic algorithms (see for instance [15]) and to analyzing the amount of randomness required in order to achieve a given performance [18].

A secret sharing scheme is a method of distributing a secret s among a set of participants $\mathcal{P}$ in such a way that qualified subsets of $\mathcal{P}$ can reconstruct the value

* This work has been done while the author was visiting the Department of Computer Science and Engineering of the University of Nebraska-Lincoln, NE-68588, U.S.A..

of s, whereas any other (non-qualified) subset of $\mathcal{P}$ cannot determine anything about the value of the s.

Secret sharing schemes are useful in any important action that requires the concurrence of several designated people to be initiated, such 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 [14] for example).

Blundo, De Santis, and Vaccaro [6] introduced the concept of randomness coefficient for secret sharing schemes. The randomness coefficient of a secret sharing scheme is the amount of randomness per bit of the secret required by the dealer to set up such a scheme.

In this paper we analyze the randomness coefficient of secret sharing schemes for access structures which are the closure of the edge set of a graph, that is, access structures for which the set of participants can be identified with the vertex set $V(G)$ of a graph $G = (V(G), E(G))$, and the set of participants qualified to reconstruct the secret are only those containing an edge of G. Secret sharing schemes for such access structures have been extensively studied in several papers, such as [7, 8, 10, 5, 4, 24, 26].

We give both lower and upper bounds for infinite classes of access structures. Lower bounds are obtained using entropy arguments. We prove a general lower bound on the randomness coefficient for access structure based on graphs. As a result we obtain a general bound for the cycle C_n. This bound improves that proposed in [6]; for C_n, when n is odd, our bound is tight. The upper bounds derive from a decomposition construction based on combinatorial designs (in particular, t-(v, k, λ) designs). A decomposition construction can be considered as a recursive technique that uses small schemes to build schemes for larger access structures. The decomposition of a given access structure into smaller ones has been accomplished in several ways; we refer the reader to [8, 5, 25, 19]. Also, we study the access structures on at most five participants, obtaining exact values for the randomness coefficient for all access structures on at most four participants, and for all connected graphs on five vertices. Finally, we analyze the randomness coefficient of anonymous threshold schemes, giving both a lower and an upper bound on it.

Due to the space limit on this extended abstract, all proofs are omitted. The authors will supply a complete version on request.

2 Basic Definitions

In this section we recall some basic definitions of secret sharing schemes and the randomness coefficient for secret sharing schemes. Both secret sharing schemes and the randomness coefficient are defined using the entropy approach.

To formally define the randomness coefficient 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 $H(\mathbf{P}) = -\sum_{i=1}^{n} p_i \log p_i$.

2.1 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, and 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.

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

In this paper, we assume that there is always at least one subset of participants who can reconstruct the secret, i.e. $\mathcal{A} \neq \emptyset$.

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

For a monotone access structure $\mathcal{A}$ we have $\mathcal{A} = \mathsf{cl}(\mathcal{A})$. 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 by $\mathcal{A}^0$ and is called the *basis* of $\mathcal{A}$.

Following [17] and [10], by using the entropy approach a secret sharing scheme can be defined as follows.

Definition 3. A *secret sharing scheme* is a distribution of the secrets in S among participants in $\mathcal{P}$ such that

1. *Any qualified subset can reconstruct the secret:*
   Formally, for all $A \in \mathcal{A}$, there holds $H(S|A) = 0$.
2. *Any non-qualified subset has absolutely no information on the secret:*
   Formally, for all $A \notin \mathcal{A}$, there holds $H(S|A) = H(S)$.

2.2 Dealer's Randomness

In this section we recall the definition of the randomness coefficient for a given access structure $\mathcal{A}$. The total randomness present in a secret sharing scheme for an access structure $\mathcal{A}$ on a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n participants is equal to $H(P_1 \ldots P_n)$. This takes into account also the randomness $H(S)$ of the secret. The dealer's randomness is the randomness needed by the dealer to generate the shares, given that the set S and the probability distribution $\{p_S(s)\}_{s \in S}$ are known. Therefore, given an access structure $\mathcal{A}$ and a secret sharing scheme, the dealer's randomness is equal to $H(P_1 \ldots P_n|S)$. This randomness is needed only to generate the shares distributed to participants. The following result relates the total randomness and the dealer's randomness.

Result 4. ([6]) *Let $\mathcal{A}$ be an access structure on the set $\mathcal{P} = \{P_1, \ldots, P_n\}$. For any secret sharing scheme for secrets in S, there holds $H(P_1 \ldots P_n) = H(P_1 \ldots P_n|S) + H(S)$.*

To analyze the randomness required by the dealer we define the *randomness coefficient* of a secret sharing scheme Σ, given that the probability distribution on the set of secrets S is Π_S. This randomness coefficient was defined in [6] to be

$$\mu(\mathcal{A}, \Pi_S, \Sigma) = \frac{H(P_1 \dots P_n|S)}{H(S)}.$$

The value $\mu(\mathcal{A}, \Pi_S, \Sigma)$ represents the amount of randomness per bit of the secret required by the dealer to set up the scheme, when using the scheme Σ and where Π_S is the probability distribution on the secret. Notice that $\mu(\mathcal{A}, \Pi_S, \Sigma)$ also depends on Σ since the probability that participants receive given shares, and therefore the entropy $H(P_1 \dots P_n|S)$, depends both on $\{p_S(s)\}_{s \in S}$ and Σ. Since we are interested in the minimum possible amount of randomness for a given access structure $\mathcal{A}$, we employ the following definition.

Definition 5. *([6])* Let $\mathcal{A}$ be an access structure on a set $\mathcal{P} = \{P_1, \dots, P_n\}$ of n participants. The *randomness coefficient* $\mu(\mathcal{A})$ of $\mathcal{A}$ is defined as

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

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 Σ for the access structure $\mathcal{A}$.

3 Lower Bounds

In this section we analyze access structures which are the closure of the edge set of a given graph, that is, access structures for which the set of participants can be identified with the vertex set $V(G)$ of a graph $G = (V(G), E(G))$, and the sets of participants qualified to reconstruct the secret are precisely those containing an edge of G. Secret sharing schemes for such access structures have been extensively studied in several papers, such as [7, 8, 10, 5, 4, 24, 26]. In this section we will give a general lower bound on the randomness coefficient for access structures based on graphs. We will give a bound for the cycle C_n, $n \geq 5$. The only previous bound known for C_n was given in [6]. We improve on that result; in the case of odd n our bound is tight.

In [6] an *independent sequence* is defined as follows.

Definition 6. *([6])* Let $\mathcal{A}$ be an access structure on a set $\mathcal{P} = \{P_1, \dots, P_n\}$ of participants. A sequence $P_{j_1}, \dots, P_{j_m}$ of participants is called *independent* if

1. $\{P_{j_1}, \dots, P_{j_m}\} \notin \mathcal{A}$,
2. for all $i < m$ a subset $X_i \in 2^{\mathcal{P}}$ of participants exists such that
   (a) $\{P_{j_1}, \dots, P_{j_i}\} \cup X_i \notin \mathcal{A}$,
   (b) $\{P_{j_1}, \dots, P_{j_i}, P_{j_{i+1}}\} \cup X_i \in \mathcal{A}$.

The following result gives a lower bound on the randomness coefficient of any access structure $\mathcal{A}$ when an independent sequence of $\mathcal{A}$ is known.

Result 7. ([6]) *Let $\mathcal{A}$ be an access structure on a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of participants. If there exists an independent sequence of length m then $\mu(\mathcal{A}) \geq m$.*

For an access structure $\mathcal{A}$ which consists of the closure of the edge-set of a graph G we denote the randomness coefficient by $\mu(G) = \mu(\mathcal{A})$. Before we state our main theorem of this section we need some definitions.

Let P and H be the graphs with vertex set $V(P) = V(H) = \{P_1, P_2, P_3, P_4\}$ and edge set, $E(P) = \{(P_1, P_2), (P_2, P_3), (P_3, P_4)\}$ and $E(H) = \{(P_1, P_2), (P_2, P_3), (P_2, P_4), (P_3, P_4)\}$, respectively. In [10] it was proved that $H(P_2P_3) \geq 3H(S)$ for both P and H.

Let G be a graph. If $V_1 \subseteq V(G)$, then we define the graph $G[V_1]$ to have vertex set V_1 and edge set $\{(U, V) \in E(G) : U, V \in V_1\}$. We say that $G[V_1]$ is an *induced subgraph* of G.

Definition 8. Let G be a graph. G is said to be k-$\{H, P\}$-*induced* if there exist k sets $X_1, ..., X_k$ such that

1. For $i = 1, 2, \ldots, k$, $X_i = \{P_{i_1}, P_{i_2}, P_{i_3}, P_{i_4}\} \subseteq V(G)$.
2. For all $i \neq j$, $X_i \cap X_j = \emptyset$.
3. For $i = 1, 2, \ldots, k$, $G[X_i]$ is isomorphic either to P or to H.

It is clear that a k-$\{H, P\}$-induced graph G is also a $(k-1)$-$\{H, P\}$-induced. Moreover if each $G[X_i]$ is isomorphic either to P or to H then, there exist two participants $P', P'' \in X_i$ such that $H(P'P'') \geq 3H(S)$. Suppose, wlog, that for $i = 1, 2, \ldots, k$, $H(P_{i_2}P_{i_3}) \geq 3H(S)$. Then we have the following definition.

Definition 9. Let G be a graph. G is said to be *strong* k-$\{H, P\}$-*induced* if G is k-$\{H, P\}$-induced and for any $l \in \{i_2, i_3\}$ and $r \in \{j_1, j_2, j_3, j_4\}$, where $i, j = 1, 2, \ldots, k$ and $i \neq j$, the edge $(l, r) \notin E(G)$.

One can easily prove, by adapting the proof of Theorem 4.1 in [10], that in any strong k-$\{H, P\}$-induced graph G there exist k participants, say $P_{j_1}, \ldots, P_{j_k}$, such that

$$H(P_{j_1} \ldots P_{j_k}) \geq \frac{3k}{2} H(S). \tag{1}$$

Moreover, the participants $P_{j_1}, \ldots, P_{j_k}$ constitute an independent sequence in G. The following theorem holds.

Theorem 10. *Let G be a strong k-$\{H, P\}$-induced graph. Let $P_{j_1}, \ldots, P_{j_k}$ be the participants for which $H(P_{j_1} \ldots P_{j_k}) \geq (3k)/2H(S)$. Finally, let $P_{j_1}, \ldots, P_{j_k}$, $P_{j_{k+1}}, \ldots, P_{j_t}$ be the longest independent sequence in G having $P_{j_1}, \ldots, P_{j_k}$ as first k participants. The randomness coefficient $\mu(G)$ satisfies*

$$\mu(G) \geq t + \frac{k}{2}.$$

With C_n we denote the cycle on n vertices, that is, the graph with edges $P_0P_1, ..., P_{n-1}P_0$. The following corollary holds.

Corollary 11. *Let C_n be the cycle on $n \geq 5$ vertices. The randomness coefficient $\mu(C_n)$ satisfies $\mu(C_n) = n/2$ if n is odd and $(n-1)/2 \leq \mu(C_n) \leq n/2$ if n is even.*

If we consider n=6, then from previous corollary we get that $2.5 \leq \mu(C_6) \leq 3$. Brickell and Stinson [8] gave a secret sharing scheme for C_6 which shows that $\mu(C_6) \leq \log_2 6 < 2.58497$. Thus, in the case of the cycle C_6 we have the following theorem.

Theorem 12. *Let C_6 be the cycle on 6 vertices. The randomness coefficient $\mu(C_6)$ satisfies $2.5 \leq \mu(C_6) \leq \log_2 6$.*

A lower bound on the randomness coefficient for graphs is the following.

Result 13. ([6]) *Let G be a connected graph. If G is a complete multipartite graph then $\mu(G) = 1$; otherwise $\mu(G) \geq 2$.*

The following theorem exhibits the existence of a large class of graphs having randomness coefficient greater than 2.

Theorem 14. *Let G be a connected graph with girth at least $t \geq 5$. Then the randomness coefficient $\mu(G)$ satisfies*

$$\mu(G) \geq \begin{cases} t/2 & \text{if } t \text{ is odd} \\ (t-1)/2 & \text{if } t \text{ is even.} \end{cases}$$

3.1 Connected Graphs on at Most Five Vertices

In this section we give some results on the randomness coefficient for access structures based on graphs with 4 and 5 vertices. Before we state our bounds we need the following result.

Result 15. ([6]) *Let G be a graph. If $\eta(G)$ is the smallest number of complete multipartite subgraphs needed to cover all edges of G then the randomness coefficient $\mu(G)$ satisfies $\mu(G) \leq \eta(G)$.*

The next theorem is a consequence.

Theorem 16. *Let G be a graph with $|V(G)| \leq 4$. If G is complete multipartite graph, then $\mu(G) = 1$, otherwise $\mu(G) = 2$.*

Theorem 17. *Let G be a graph with $|V(G)| = 5$. If G is complete multipartite, then $\mu(G) = 1$; if G is the cycle C_5, then $\mu(C_5) = 2.5$; otherwise $\mu(G) = 2$.*

4 Upper Bounds

In this section we present a combinatorial technique to obtain a general upper bound on the randomness coefficient for an infinite class of access structures. We will use an extension of the decomposition construction presented in [24]. Stinson [24] used this decomposition construction, based on Steiner systems $S(t,k,v)$, to obtain general lower bounds on the information rate and average information rate of certain classes of access structures. A decomposition construction can be considered as a recursive technique that uses small schemes to build secret sharing schemes for larger access structures. The decomposition of a given access structure into smaller ones has been accomplished in several ways; we refer the reader to [8, 5, 25, 19].

Stinson [24] defined the *rank* of an access structure to be the maximum cardinality of a minimal authorized subset. An access structure is *uniform* if every minimal authorized subset has the same cardinality.

Blundo, De Santis, and Vaccaro [6], by using a decomposition technique, gave an upper bound on the randomness coefficient for general access structures. To state their bound we need the following definition.

Definition 18. *([6])* Let $\mathcal{A}$ be an access structure and let $\mathcal{A}_1, \ldots, \mathcal{A}_a$ be access structures such that $\mathcal{A}_i \subseteq \mathcal{A}$, for $i = 1, 2, \ldots, a$. If each qualified set $A \in \mathcal{A}$ belongs to at least b of the access structures $\mathcal{A}_1, \ldots, \mathcal{A}_a$, then the set $\{\mathcal{A}_1, \ldots, \mathcal{A}_a\}$ is called an (a,b)-decomposition of $\mathcal{A}$.

A general upper bound for an access structure $\mathcal{A}$ that possesses an (a,b)-decomposition is the following.

Result 19. ([6]) *Let $\mathcal{A}$ be an access structure and let $\{\mathcal{A}_1, \ldots, \mathcal{A}_a\}$ be an (a,b)-decomposition of $\mathcal{A}$. The randomness coefficient $\mu(\mathcal{A})$ satisfies $\mu(\mathcal{A}) \leq \sum_{i=1}^{a} \mu_i / b$, where μ_i is the randomness coefficient of the scheme for $\mathcal{A}_i$.*

4.1 Rank t Access Structures

In this section we use a combinatorial technique to obtain a general upper bound on the randomness coefficient for an infinite class of access structures. We will use an extension of the decomposition construction presented in [24].

We present some basic terminology from design theory. A t-(v,k,λ) design is a pair $(V,\mathcal{B})$, where V is a set of v elements (called *points*) and $\mathcal{B}$ is a family of subsets of V of size k (called *blocks*), such that every subset of points of size t occurs in exactly λ blocks. A t-(v,k,λ) design is said to be *non-trivial* if $t < k < v$. A *Steiner system* is a t-$(v,k,1)$ design and usually it is denoted by $S(t,k,v)$. For general information on the existence of t-(v,k,λ) designs we refer to [2]. For a collection of surveys and the latest results on design theory we refer the reader to [12].

The following decomposition technique was first considered by Stinson [24]. Suppose $\mathcal{A}$ is a rank t access structure on a set $\mathcal{P}$ of n participants. Suppose

that there exists an $S(t,k,n)$, $(\mathcal{P},\mathcal{B})$. A decomposition of $\mathcal{A}_0$ can be constructed as follows. For every block $B \in \mathcal{B}$, define

$$\mathcal{A}_B = \{A \in \mathcal{A}_0 \mid A \subseteq B\}. \tag{2}$$

It is easy to see that $\{\mathcal{A}_B \mid B \in \mathcal{B}\}$ is a $(|\mathcal{B}|,1)$-decomposition of $\mathcal{A}$. If instead of an $S(t,k,n)$ we use a t-(n,k,λ) design, $(\mathcal{P},\mathcal{C})$, then it is easy to check that the decomposition $\{\mathcal{A}_B \mid B \in \mathcal{C}\}$ is a $(|\mathcal{C}|,\lambda)$-decomposition of $\mathcal{A}$.
The following theorem holds.

Theorem 20. *Let $\mathcal{A}$ be a rank t access structure on n participants. Suppose that a t-(n,k,λ) design exists. If the randomness coefficient of any access structure $\mathcal{A}_{k,t}$ of rank at most t on k participants is at most $\mu_{k,t}$, then the randomness coefficient $\mu(\mathcal{A})$ satisfies*

$$\mu(\mathcal{A}) \leq \frac{\binom{n}{t}}{\binom{k}{t}}\mu_{k,t}.$$

The following theorem states an upper bound on any access structure on four participants of rank at most three.

Theorem 21. *Let $\mathcal{A}$ be an access structure of rank at most 3 on four participants. Then the randomness coefficient $\mu(\mathcal{A}) \leq 2$.*

The following theorem states an upper bound any access structure on five participants of rank at most three.

Theorem 22. *Let $\mathcal{A}$ be an access structure of rank at most 3 on five participants. Then, the randomness coefficient $\mu(\mathcal{A})$ satisfies $\mu(\mathcal{A}) \leq 4$.*

The following theorem gives an upper bound for any rank 3 access structure on $n \geq 5$ participants. It uses known classes of 3-(v,k,λ) designs.

Theorem 23. *Let $\mathcal{A}$ be a rank 3 access structure on n participants, where $n \geq 5$. The randomness randomness coefficient $\mu(\mathcal{A})$ satisfies*

$$\mu(\mathcal{A}) \leq \frac{n(n-1)(n-2)}{15}.$$

4.2 Uniform Rank t Access Structures

In this section we give an upper bound on the randomness coefficient for any uniform rank t access structure. To this aim we need to introduce an access structure called *generalized star*. Stinson [24] defined the generalized star and used it to give a lower bound on the information rates of uniform rank t access structures. We denote a generalized star of rank t on r participants by $\mathcal{A}(t,r)$. Its basis is defined as $\mathcal{A}^0(t,r) = \{\{P_1,\ldots,P_{t-1},P_j\} : t \leq j \leq r\}$. The *center* of a generalized star $\mathcal{A}(t,r)$ is the intersection of all qualified subsets in the basis (i.e., $\{P_1,\ldots,P_{t-1}\}$ in the above definition). It is easy to see that the randomness

coefficient $\mu(\mathcal{A}(t,r))$ of a generalized star is equal to $\mu(\mathcal{A}(t,r)) = t-1$. Indeed, $P_1, \ldots, P_{t-1}$ constitutes an independent sequence; hence $\mu(\mathcal{A}(t,r)) \geq t-1$. A scheme that meets this bound can be constructed by a simple modification of a Shamir (t,t) threshold scheme [22].

The following theorem states an upper bound on the randomness coefficient for any uniform rank t access structure.

Theorem 24. *Let $\mathcal{A}$ be uniform rank t access structures on a set $\mathcal{P}$ of n participants. The randomness coefficient $\mu(\mathcal{A})$ satisfies*

$$\mu(\mathcal{A}) \leq \binom{n}{t-1}\frac{t-1}{t}.$$

The following corollary is a consequence.

Corollary 25. *Let $\mathcal{A}$ be uniform rank 3 access structures on a set $\mathcal{P}$ of n participants. The randomness coefficient $\mu(\mathcal{A})$ satisfies $\mu(\mathcal{A}) \leq n(n-1)/3$.*

5 Anonymous Threshold Schemes

In this section we give upper bounds on the randomness coefficient of anonymous threshold schemes. Informally, in an anonymous secret sharing scheme the secret is reconstructed without knowledge of which participants hold which shares. In such schemes the computation of the secret can be carried out by giving the shares to a black box that does not know the identities of the participants holding those shares.

Anonymous threshold schemes were first analyzed in [28]. Following the characterization of [28] and [20] we can define anonymous threshold schemes as follows.

Definition 26. Let $\mathcal{P}$ be a set of k participants. A (t,k) *anonymous threshold scheme*, $1 \leq t \leq k$, is a (t,k) threshold scheme satisfying the following properties

1. Different participants receive different shares.
2. The key is determined as a function of the set of shares held by an authorized subset of participants.

Let S be the set of possible secrets and V, with $|V| = v$, be the set from which the shares are taken in a (t,k) anonymous threshold scheme. Stinson and Vanstone [28] proved that in any (t,k) anonymous threshold scheme,

$$v \geq (k-t+1)|S| + t - 1. \tag{3}$$

For an information theoretic proof of this bound see [9].

We recall the following condition of *regularity* that in [20] and [28] was made on the distribution of shares of the participants.

R.1 There exists a positive integer ℓ such that any $s \in S$ it is associated with a subset $\phi(s) \subset V^k$ consisting of ℓ elements. To share a secret $s \in S$, an element from $\phi(s)$ is chosen with uniform probability and the components of the chosen vector are given to participants as shares.

To analyze the randomness needed by the dealer we define the *randomness coefficient* of a (t,k) anonymous threshold secret sharing scheme Σ, where the probability distribution on the set of secrets S is Π_S, to be

$$\mu_A(t,k,\Pi_S,\Sigma) = \frac{H(P_1 \dots P_n|S)}{H(S)}.$$

The value $\mu_A(t,k,\Pi_S,\Sigma)$ represents the amount of randomness per bit of the secret required by the dealer to set up the scheme when using the scheme Σ, where Π_S is the probability distribution on the secret.

Stinson and Vanstone [28] defined an *optimal* (t,k,v) *threshold scheme* as a (t,k) anonymous threshold scheme having v shares and $(v-t+1)/(k-t+1)$ possible secrets (i.e., in such a scheme the equation (3) is satisfied with equality). Let $(V,\mathcal{B})$ be a Steiner system $S(t,k,v)$. We say that $S(t,k,v)$ is *partitionable* if we can partition the set of blocks $\mathcal{B}$ into sets $\mathcal{B}_1,\dots,\mathcal{B}_\ell$, in such a way that each $(V,\mathcal{B}_j)$, for $1 \le j \le \ell$, is a Steiner system $S(t-1,k,v)$. Stinson and Vanstone [28] proved the following.

Result 27. ([28]) *An optimal (t,k,v) threshold schemes exist if and only if a Steiner system $S(t,k,v)$ can be partitioned into Steiner systems $S(t-1,k,v)$.*

Let us see how to construct an optimal (t,k,v) threshold scheme. Let $(V,\mathcal{B})$ be a partitionable Steiner system $S(t,k,v)$ and let $\mathcal{B}_1,\dots,\mathcal{B}_\ell$ be a partition of the set of blocks $\mathcal{B}$ such that $(V,\mathcal{B}_j)$, for $1 \le j \le \ell$, is a Steiner system $S(t-1,k,v)$. It is known that $\ell = (v-t+1)/(k-t+1)$. For $1 \le j \le \ell$, to each set of blocks $\mathcal{B}_j$ the dealer associates a secret s_j. When the dealer wants to share a secret s_j then he/she randomly chooses a block in $\mathcal{B}_j$ and randomly distributes to participants the elements of this block as shares. (This is the construction from [28].) It is well known that the number of blocks in a Steiner system $S(t-1,k,v)$ is equal to $\binom{v}{t-1}/\binom{k}{t-1}$ (see for instance [2]). When the dealer has chosen a block he/she has $k!$ ways to distribute to the k participants the elements of this block as shares. Hence, to share a secret of $\log((v-t+1)/(k-t+1))$ bits the dealer uses $\log((\binom{v}{t-1}/\binom{k}{t-1})k!)$ bits of randomness. Thus, the following theorem holds.

Theorem 28. *Let Π_S be the uniform probability distribution on the secret. The randomness coefficient $\mu_A(t,k,\Pi_S,\Sigma)$ of any optimal (t,k,v) threshold scheme satisfies*

$$\mu_A(t,k,\Pi_S,\Sigma) \le \frac{\sum_{i=0}^{t-2}\log(v-i) + \sum_{j=1}^{k-t+1}\log j}{\log\frac{v-t+1}{k-t+1}}.$$

The following corollary provides upper bounds on the randomness coefficient of (t,k) anonymous threshold schemes for parameters t and k for which both partitionable Steiner systems and ordered designs exist.

Corollary 29. *Let Π_S be the uniform probability distribution on the secret. The randomness coefficient $\mu_A(t,n,\Pi_S,\Sigma)$ of (t,k) anonymous threshold schemes satisfies*

$$\mu_A(t,n,\Pi_S,\Sigma) \leq \begin{cases} \frac{\log v}{\log(v-1)-\log(k-1)} & \text{if } t=2,\ 2\leq k\leq 4, \text{ and } v \equiv k \bmod k(k-1) \\ \frac{\log v+\log(v-1)}{\log(v-1)-1} & \text{if } t=3,\ k=3, \text{ and } v \equiv 1,3 \bmod 6,\ v \neq 7 \\ \frac{\log v+\log(v-1)}{\log(v-1)-\log 3} & \text{if } t=3,\ k=4, \text{ and } v=4^m, \text{ where } m \geq 2. \end{cases}$$

Acknowledgement

D. R. Stinson's research is supported by NFS grant CCR–9121951. C. Blundo and A. Giorgio Gaggia research's is supported by Italian Ministry of University and Scientific Research in the framework of the project: "Algoritmi, Modelli di Calcolo e Strutture Informative" and by the National Council of Research. The authors would like to thank Keith Martin and Wen-Ai Jackson for helpful comments about Theorem 22.

References

1. J. C. Benaloh and J. Leichter, *Generalized Secret Sharing and Monotone Functions*, in "Advances in Cryptology - Crypto '88", S. Goldwasser Ed., "Lecture Notes in Computer Science", Vol. 403, Springer–Verlag, Berlin, pp. 27–35, 1990.
2. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Bibliographisches Institut, Zurich, 1985.
3. G. R. Blakley, *Safeguarding Cryptographic Keys*, Proceedings of AFIPS 1979 National Computer Conference, Vol. 48, New York, NY, pp. 313–317, June 1979.
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", Ed. E. Brickell, "Lecture Notes in Computer Science", Vol. 740, Springer-Verlag, Berlin, 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*, Journal of Cryptology, Vol. 8, (1995), pp. 39-64. A preliminary version appeared in "Advances in Cryptology – Eurocrypt '92", Lecture Notes in Computer Science, Vol. 658, R. Rueppel Ed., Springer-Verlag, pp. 1–24, 1993.
6. C. Blundo, A. De Santis, and U. Vaccaro, *Randomness in Distribution Protocols*, in "21st International Colloquium on Automata, Languages and Programming" (ICALP '94), Serge Abiteboul and Eli Shamir Eds., vol. 820 di "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*, J. Cryptology, Vol. 4, No. 2, pp. 123–124, 1991.
8. E. F. Brickell and D. R. Stinson, *Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes*, J. Cryptology, Vol. 5, No. 3, pp. 153-166, 1992.
9. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, *A Note on Secret Sharing Schemes*, Sequences II: Methods in Communication, Security and Computer Science, Springer-Verlag. Positano, Italy, pp. 335–344, June 1991.

10. 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, Pag. 157-169, 1993.
11. I. Csiszár and J. Körner, *Information Theory. Coding Theorems for Discrete Memoryless Systems*, Academic Press, 1981.
12. J. H. Dinitz and D. R. Stinson, *Contemporary Design Theory. A Collection of Surveys*, Wiley-Interscience Series in Discrete Mathematics and Optimization, 1992.
13. R. G. Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, New York, NY, 1968.
14. O. Goldreich, S. Micali, and A. Wigderson, *How to Play any Mental Game*, Proceedings of 19th ACM Symp. on Theory of Computing, pp. 218–229, 1987.
15. R. Impagliazzo and D. Zuckerman, *How to Recycle Random Bits*, Proceedings of 30th Annual Symposium of Computer Science, pp. 248–255, 1989.
16. M. Ito, A. Saito, and T. Nishizeki, *Secret Sharing Scheme Realizing General Access Structure*, Proceedings of IEEE Global Telecommunications Conference, Globecom 87, Tokyo, Japan, pp. 99–102, 1987.
17. 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.
18. D. Krizane, 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.
19. K.M. Martin, *New Secret Sharing Schemes from Old*, J. Comb. Math. Comb. Comp. Vol. 14, pp. 65–77, 1993.
20. P. J. Schellenberg and D. R. Stinson, *Threshold Schemes from Combinatorial Designs*, J. Combin. Math. and Combin. Computing, Vol. 5, pp. 143–160, 1989.
21. D. K. Ray-Chaudhuri and R. M. Wilson, *Solution of Kirkman's Schoolgirl Problem*, Amer. Math. Soc. Proc. Symp. Pure Math., Vol. 19, pp. 187–204, 1971.
22. A. Shamir, *How to Share a Secret*, Communications of the ACM, Vol. 22, n. 11, pp. 612–613, Nov. 1979.
23. G.J. Simmons, *An Introduction to Shared Secret and/or Shared Control Schemes and Their Application*, Contemporary Cryptology, IEEE Press, pp. 441–497, 1991.
24. D. R. Stinson, *New General Lower Bounds on the Information Rate of Secret Sharing Schemes*, in "Advances in Cryptology - CRYPTO '92", Ed. E. Brickell, "Lecture Notes in Computer Science", Vol. 740, Springer-Verlag, Berlin, pp. 170–184, 1993.
25. D. R. Stinson, *An Explication of Secret Sharing Schemes*, Design, Codes and Cryptography, Vol. 2, pp. 357–390, 1992.
26. D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, IEEE Trans. Inform. Theory Vol. 40 (1994), pp. 118-125.
27. D. R. Stinson, *Combinatorial Designs and Cryptography*, in "Surveys in Combinatorics, 1993", K. Walker Ed., Cambridge Univ. Press, pp. 257–287.
28. D. R. Stinson and A. Vanstone, *A Combinatorial Approach to Threshold Schemes*, SIAM J. Disc. Math., Vol. 1, May 1988, pp. 230–236.