On the Size of Shares for Secret Sharing Schemes*

R. M. Capocelli[1], A. De Santis[2], L. Gargano[2], U. Vaccaro[2]

[1] Dipartimento di Matematica, Università di Roma, 00185 Roma, Italy

[2] Dipartimento di Informatica, Università di Salerno, 84081 Baronissi (SA), Italy

Abstract

A secret sharing scheme permits a secret to be shared among participants in such a way that only qualified subsets of participants can recover the secret, but any non-qualified subset has absolutely no information on the secret. The set of all qualified subsets defines the access structure to the secret. Sharing schemes are useful in the management of cryptographic keys and in multy-party secure protocols.

We analyze the relationships among the entropies of the sample spaces from which the shares and the secret are chosen. We show that there are access structures with 4 participants for which any secret sharing scheme must give to a participant a share at least 50% greater than the secret size. This is the first proof that there exist access structures for which the best achievable information rate (i.e., the ratio between the size of the secret and that of the largest share) is bounded away from 1. The bound is the best possible, as we construct a secret sharing scheme for the above access structures that meets the bound with equality.

*This work was partially supported by "Algoritmi, Modelli di Calcolo e Sistemi Informativi" of M.U.R.S.T. and by "Progetto Finalizzato Sistemi Informatici e Calcolo Parallelo" of C.N.R. under grant n. 91.00939.PF69.

1 Introduction

Secret Sharing is an important tool in Security and Cryptography. In many cases there is a single master key that provides the access to important secret information. Therefore, it would be desirable to keep the master key in a safe place to avoid accidental and malicious exposure. This scheme is unreliable: if the master key is lost or destroyed, then all information accessed by the master key is no longer available. A possible solution would be that of storing copies of the key in different safe places or giving copies to trusted people. In such a case the system becomes more vulnerable to security breaches or betrayal [15], [9]. A better solution would be breaking the master key into pieces in such a way that only the concurrence of certain predefined trusted people can recover it. This has proven to be an important tool in the management of cryptographic keys and in multy-party secure protocols (see for example [11]).

As a solution to this problem, Blakley [2] and Shamir [15] introduced (k, n) threshold schemes. A (k, n) threshold scheme allows a secret to be shared among n participants in such a way that any k of them can recover the secret, but any $k - 1$, or fewer, have absolutely no information on the secret (see [17] for a comprehensive bibliography on (k, n) threshold schemes).

Ito, Saito, and Nishizeki [12] described a more general method of secret sharing. An access structure is a specification of all the subsets of participants who can recover the secret and it is said to be monotone if any set which contains a subset that can recover the secret, can itself recover the secret. Ito, Saito, and Nishizeki gave a methodology to realize secret sharing schemes for arbitrary monotone access structures. Subsequently, Benaloh and Leichter [1] gave a simpler and more efficient way to realize such schemes.

An important issue in the implementation of secret sharing schemes is the size of shares, since the security of a system degrades as the amount of the information that must be kept secret increases. Unfortunately, in all secret sharing schemes the size of the shares cannot be less than the size of the secret[1]. Moreover, there are access structures for which any corresponding secret sharing scheme must give to some participant a share of size strictly bigger than the secret size. Indeed, Benaloh and Leichter [1] proved that there exists an access structure for which any secret sharing scheme must give to some participant a share which is from a domain larger than that of the secret. Recently, Brickell and Stinson [6] improved on [1] by showing that for the same access structure, the number of elements in the domain of the shares must be at least $2|S| - 1$ if the cardinality of the domain of the secret is $|S|$. Ideal Secret Sharing schemes, that is sharing schemes where the shares are taken from the same domain as that of the secret were characterized by Brickell and Davenport [5] in terms of matroids.

All above results regarding the size of the domain of the shares and that of the secret, can be interpreted as relations between the entropies of the corresponding sample spaces

[1]This property holds since non-qualified subsets of participants have *absolutely* no information on the secret. If we relax this requirement (as is done in ramp schemes [3] [7]) the size of the shares might be less than the size of the secret.

when only uniform probability distributions are involved. A more general approach has been considered by Karnin, Greene, and Hellman [13] who initiated the analysis (limited to threshold schemes) of secret sharing schemes when arbitrary probability distributions are involved.

We extend the approach of [13] to general access structures deriving several relations among the entropies of the secret and those of the shares even when partial informations are taken into account. When we restrict probability distributions to be uniform, our results imply an improvement over the above mentioned results on the size of shares.

In this paper we prove that for any secret sharing scheme, for any set A of participants which are not qualified to recover the secret, the average uncertainty on each share of participants in another set B given that the shares of A are known (A and B are sets of participants such that they can recover the secret by pooling together their shares) must be at least as great as the *a priori* uncertainty on the secret. This is a generalization and also a sharpening of a result in [13]. We also analyze the relationships between the size of the shares and that of the secret. We improve on the result of [6] proving that there are access structures with 4 participants for which any secret sharing scheme must give to some participant shares which are from a domain of size at least $|S|^{1.5}$, $|S|$ being the secret domain size. In other words, we show that the number of bits needed for a single share is 50% bigger than those needed for the secret. This is the first proof that there exist access structures for which the best achievable information rate (i.e., the ratio between the size of the secret and that of the largest share) is bounded away from 1. We construct a secret sharing scheme for the above access structures which meets the bound with equality. Finally, the bound is generalized to access structures with any number of participants.

2 Preliminaries

In this section we shall review the information theoretic concepts we are going to use. For a complete treatment of the subject the reader is advised to consult [8], [10], [16].

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

$$H(X) = -\sum_{x \in X} p(x) \log p(x)^2.$$

The entropy $H(X)$ is a measure of the average information content of the elements in X or, equivalently, a measure of the average uncertainty one has about which element of the set X has been chosen when the choices of the elements from X are made according to the probability distribution $\{p(x)\}_{x \in X}$. It is well known that $H(X)$ is a good approximation to the average number of bits needed to faithfully represent the elements of X. The

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

following useful property of $H(X)$ will be used in the following:

$$0 \leq H(X) \leq \log |X|, \tag{1}$$

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

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

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

The conditional entropy can be written as

$$H(X|Y) = \sum_{y \in Y} p(y) H(X|Y = y)$$

where $H(X|Y = y) = -\sum_{x \in X} p(x|y) \log p(x|y)$ can be interpreted as the average uncertainty one has about which element of X has been chosen when the choices are made according to the probability distribution $\{p(x|y)\}_{x \in X}$,that is, when it is known that the value chosen from the set Y is y. From the definition of conditional entropy it is easy to see that

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

The entropy of the joint space XY satisfies

$$H(XY) = H(X) + H(Y|X) = H(Y) + H(X|Y). \tag{3}$$

Analogously, the conditional entropy of XY given Z satisfies

$$H(XY|Z) = H(X|Z) + H(Y|XZ) = H(Y|Z) + H(X|YZ). \tag{4}$$

The *mutual information* between X and Y is defined by

$$I(X; Y) = H(X) - H(X|Y) \tag{5}$$

and enjoys the following properties:

$$I(X; Y) = I(Y; X), \tag{6}$$

and

$$I(X; Y) \geq 0, \tag{7}$$

with equality in (7) if and only if $p(x, y) = p(x)p(y)$ for all $x \in X, y \in Y$. From inequality (7) one gets the following important relation between the entropy of X and the conditional entropy of X given Y

$$H(X) \geq H(X|Y). \tag{8}$$

Inequality (8) formally prove the intuitive fact that the knowledge of Y, in the average, can only decrease the uncertainty one has on X and there is no decrease if and only if X and Y are statistically independent. The *conditional mutual information* between X and Y given Z is defined by

$$I(X;Y|Z) = H(X|Z) - H(X|YZ). \tag{9}$$

Notice that $H(X|ZY) = \sum_{y \in Y} p(y) H(X|Z, Y = y)$, where

$$H(X|Z, Y = y) = -\sum_{x,z} p(xz|y) \log p(x|yz).$$

When no ambiguity arises we will drop the comma in $H(X|Z, Y = y)$. The conditional mutual information $I(X;Y|Z)$ satisfies three important properties

$$I(X;Y|Z) \geq 0 \tag{10}$$

$$I(X;Y|Z) = I(Y;X|Z) \tag{11}$$

and

$$I(X;YZ) = I(X;Z) + I(X;Y|Z),$$

with equality in (10) if and only if $\forall z$ such that $p(z) > 0$ and $\forall x, y$ it holds $p(x, y|z) = p(x|z)p(y|z)$. Formulae (9) and (10) imply the following generalization of inequality (8)

$$H(X|Z) \geq H(X|YZ). \tag{12}$$

3 Secret Sharing Schemes

A secret sharing scheme permits a secret to be shared among n participants in such a way that only qualified subsets of them can recover the secret, but any non-qualified subset has absolutely no information on the secret. Secret sharing schemes satisfying the above two conditions are usually referred to as *perfect* as opposed to secret sharing schemes in which the concurrence of non qualified subset of participants can obtain some information on the secret (e.g., ramp schemes of [3]).

Given a set P, an *access structure* on P is a family of subsets $\mathcal{A} \subseteq 2^P$. The *closure* of a family of subsets $\mathcal{A} \subseteq 2^P$, is defined as $closure(\mathcal{A}) = \{A' : A \in \mathcal{A}, A \subseteq A' \subseteq P\}$. A natural property for an access structure $\mathcal{A}$ is that of being *monotone*, i.e., $\mathcal{A} = closure(\mathcal{A})$.

Let P be a set of participants, $\mathcal{A}$ be a monotone access structure on P and S be the set of secrets. Following the information-theoretic approach of [13] and [14], we say that a Secret Sharing Scheme is a sharing of secrets among participants in P such that

1. *Any qualified subset can reconstruct the secret.*
   For all $A \in \mathcal{A}$, $H(S|A) = 0$.

2. *Any non-qualified subset has absolutely no information on the secret.* For all $A \notin \mathcal{A}$, $H(S|A) = H(S)$.

Remark 1. Notice that $H(S|A) = 0$ means that each set of values of the shares in A determines a unique value of the secret. In fact, by definition, $H(S|A) = 0$ implies that $\forall a \in A$ with $p(a) \neq 0$ $\exists s \in S$ such that $p(s|a) = 1$. Moreover, $H(S|A) = H(S)$ means that S and A are statistically independent, i.e., $\forall a \in A\ \forall s \in S$, $p(s|a) = p(s)$ and therefore the knowledge of any a in A gives no information about the secret. Notice that the condition $H(S|A) = H(S)$ is equivalent to saying that $\forall a \in A$ $H(S|A = a) = H(S)$.

Shares given to the participants are not necessarily taken from the same domain. For instance, let the set of participants be $P = \{A, B, C, D\}$ and consider the access structure $\mathcal{AS}$ consisting of the closure of the set $\big\{\{A, B\}, \{B, C\}, \{C, D\}\big\}$. Let the secret s be a uniformly chosen n-bit string. A possible secret sharing scheme for $\mathcal{AS}$ consists of uniformly chosing 3 pairs of strings whose XOR gives the secret s, that is such that $s = a \oplus b_1 = b_2 \oplus c_1 = c_2 \oplus d$ and giving shares a to A, b_1, b_2 to B, c_1, c_2 to C and d to D. The size of the shares given to B and C is twice the size of the shares to A and D, and the size of the secret itself, that is we have $H(B) = H(C) = 2H(A) = 2H(D) = 2H(S)$.

Karnin, Greene, and Hellman [13] proved that in any threshold scheme any set X_i from which the i-th share is taken satisfies $H(X_i) \geq H(S)$. What is the uncertainty on the shares for general access structures when other shares are known? Assume a set of participants Y cannot determine the secret, but they could if another participant (or group of participants) X would be willing to pool its own share. Intuitively, for general access structures, the uncertainty on the shares given to X is at least as big as that on the secret itself, from the point of view of Y. Otherwise, the set of participants Y would have some information on the secret and could decrease their uncertainty on S. This is formally stated and proved in the next lemma which constitutes an extension and a sharpening on Theorem 1 of Karnin, Greene and Hellman [13].

Lemma 3.1 *Let $Y \notin \mathcal{A}$ and $X \cup Y \in \mathcal{A}$. Then $H(X|Y) = H(S) + H(X|YS)$.*

Proof. Consider the conditional mutual information $I(X; S|Y)$ that can be written either as $H(X|Y) - H(X|SY)$ or as $H(S|Y) - H(S|XY)$. Hence,

$$\begin{aligned} H(X|Y) &= H(S|Y) + H(X|YS) - H(S|XY) \\ &= H(S) + H(X|YS) \end{aligned}$$

□

Note that the in the same way one can prove the slightly more general formula

$$H(X|Y = y) = H(S) + H(X|SY = y) \qquad \forall y \in Y,$$

for X and Y satisfying the same hypothesis of Lemma 3.1. From Lemma 3.1, (8) and (2) we also obtain $H(X) \geq H(S)$, for each $X \subset P$, which is essentially Theorem 1 of [13] generalized to monotone access structures.

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

Lemma 3.2 *If either* $X \cup Y \notin \mathcal{A}$ *or* $X \in \mathcal{A}$ *then* $H(Y|X) = H(Y|XS)$.

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

The proof of above lemma shows that condition 2. of perfect secret sharing schemes, namely $H(S|A) = H(S)\ \forall A \notin \mathcal{A}$, is equivalent to the condition $H(A|S) = H(A),\ \forall A \notin \mathcal{A}$.

4 Bounds on the size of shares

Benaloh and Leichter [1] gave the first example of an access structure for which any secret sharing scheme must give to some participant shares which are from a domain larger than that of the secret. The access structure they considered is $\mathcal{AS} = closure\Big\{\{A, B\}, \{B, C\}, \{C, D\}\Big\}$. Recently, Brickell and Stinson [6] showed that there are only two access structures with 4 participants which are the closure of a graph (i.e., the closure of a family whose elements are pairs of participants), satisfying the above limitation. Such access structures are $\mathcal{AS}$ and $\mathcal{AS}2 = closure\Big\{\{A, B\}, \{B, C\}, \{C, D\}, \{B, D\}\Big\}$. In this section we first give a lower bound on the entropy of the spaces from which the shares for the access structure $\mathcal{AS}$ are taken. Then, we use this result to prove an analogous lower bound for $\mathcal{AS}2$ and more general access structures. To maintain simpler notation, we shall denote both the participants and the sets of possible values of their shares with the same capital letter; therefore the letter A, for instance, will denote both the participant that can reconstruct the secret in coalition with B and the set from which the possible shares for A are taken.

A secret sharing scheme for $\mathcal{AS}$ satisfies

1. $H(S|AB) = H(S|BC) = H(S|CD) = 0$.
2. $H(S|A) = H(S|B) = H(S|C) = H(S|D) = H(S|AC) = H(S|AD) = H(S)$.

We also have $H(S|BD) = H(S)$, but we will not make use of it.

Theorem 4.1 *Any secret sharing scheme for* $\mathcal{AS}$ *satisfies*

$$H(BC) \geq 3H(S).$$

Proof. We have

$$\begin{aligned}
H(S) &\leq H(C|AD) \quad \text{(from Lemma 3.1 and (2))} \\
&\leq H(C|A) \quad \text{(from (12))} \\
&= H(C|AS) \quad \text{(from Lemma 3.2)} \\
&\leq H(CB|AS) = H(B|AS) + H(C|ABS) \quad \text{(from (4) and (2))} \\
&\leq H(B|AS) + H(C|BS) \quad \text{(from (12))} \\
&= H(B|A) - H(S) + H(C|B) - H(S) \quad \text{(from Lemma 3.1)} \\
&\leq H(BC) - 2H(S) \quad \text{(from (8) and (3))}.
\end{aligned}$$

The following corollary to Theorem 4.1 is immediate from (3) and (8).

Corollary 4.1 *Any secret sharing scheme for $\mathcal{AS}$ satisfies*

$$H(B) + H(C) \geq 3H(S).$$

A consequence of above corollary is that either B or C must have entropy at least $1.5H(S)$, that is 50% bigger than that of the secret.

Benaloh and Leichter [1] proved that for the access structure $\mathcal{AS}$ it must hold either $|B| > |S|$ or $|C| > |S|$, where with $|S|$ we denote the number of different secrets and with $|B|$ ($|C|$) the number of different shares that can be given to B (C). Then, Brickell and Stinson [6] improved on [1] proving that the number of possible shares either for B or for C must be at least $2|S|-1$. Our Corollary 4.1 implies the following sharper lower bound.

Corollary 4.2 *Suppose the secret is uniformly chosen in S. Any secret sharing scheme for $\mathcal{AS}$ satisfies either $|B| \geq |S|^{1.5}$ or $|C| \geq |S|^{1.5}$.*

Proof. If the secret is uniformly chosen in S we have that $H(S) = \log|S|$, and from Corollary 4.1 it follows $H(B) + H(C) \geq 3\log|S|$. Hence, either B or C have entropy at least $1.5\log|S|$. Assume $H(B) \geq 1.5\log|S|$. From (1) we have $|B| \geq 2^{H(B)}$, and thus the number of different shares for B must be greater than or equal to $2^{1.5\log|S|}$, which implies that $|B| \geq |S|^{1.5}$. □

Notice that Corollary 4.1 gives a more general result, since it takes into account the probability distribution according to which the secret and the shares are chosen.

Remark 2. The bound given by Corollary 4.2 is the best possible. Indeed, consider the following secret sharing scheme for $\mathcal{AS}$. For a binary secret $s \in S = \{0,1\}$, uniformly choose 2 pairs of bits whose XOR give the secret s, that is such that $s = a \oplus b = c \oplus d$ and give share a to the participant A, bd to B, c to C, and d to D. It can be easily seen that this scheme meets all requirements for a secret sharing scheme, and moreover that $H(A) = H(C) = H(D) = H(S) = 1$ while $H(B) = 2$ and $H(BC) = 3H(S)$. If a 2-bit secret $s_0 s_1 \in \{0,1\}^2$ is to be shared, then the following scheme can be used. For $i = 0, 1$,

uniformly choose bits a_i, b_i, c_i, d_i, such that $a_i \oplus b_i = c_i \oplus d_i = s_i$ and give share a_0a_1 to A, $b_0d_0b_1$ to B, $c_0c_1a_1$ to C and d_0d_1 to D. This is a secret sharing scheme which satisfies $H(A) = H(D) = H(S) = 2$ and $H(B) = H(C) = 1.5H(S) = 3$. The generalization to n-bit secrets, as well as to non-binary cases, is straightforward. In general, if $|S| = q^2$, q an integer greater than 2, the above procedure yields a scheme for which $|A| = |D| = q^2$ and $|B| = |C| = q^3 = (q^2)^{1.5}$.
Assume that all shares for participants are chosen from the same space K. As a consequence of Corollary 4.2 we get that the *information rate* $\log|S|/\log|K|$ (as defined in [6]) for any secret sharing scheme for $\mathcal{AS}$ is at most 2/3. The scheme above described has an information rate of exactly 2/3 when $|S| = q^2$. Thus, the bound of 2/3 is optimal for $\mathcal{AS}$ and settles a problem by [6].
In case $S = \{0, 1\}$ the bound given by Corollary 4.1 is the best possible for non-uniform distributions as well. Let $Pr(S = 0) = p$ and $Pr(S = 1) = 1 - p$, $p \leq 1/2$. We first construct a $(2, 2)$ threshold scheme for A and B that satisfies $H(A) = H(B) = H(S)$. The shares are given to A and B according to the following probability distribution:

$$\begin{aligned}
Pr(A = 0, B = 0|S = 0) &= 1/2 \\
Pr(A = 1, B = 1|S = 0) &= 1/2 \\
Pr(A = 0, B = 1|S = 1) &= \frac{p}{2(1-p)} \\
Pr(A = 1, B = 0|S = 1) &= 1 - \frac{p}{2(1-p)}
\end{aligned}$$

It is clear that $Pr(A = 0) = p$ and $Pr(B = 0) = 1 - p$. Therefore $H(A) = H(B) = H(S)$ and it is trivial to check that both $H(S|A) = H(S|B) = H(S)$ and $H(S|AB) = 0$ hold. Independently, apply the same threshold scheme to C and D and give a copy of the share that has been given to D also to B. It is easily seen that the constructed secret sharing scheme satisfy all required properties and that $H(B) + H(C) = 3H(S)$.

Our lower bound also holds for $\mathcal{AS}2$ which is the closure of the family $\big\{\{A, B\}, \{B, C\}, \{C, D\}, \{B, D\}\big\}$. It is easily seen that Theorem 4.1 also applies, since in the proof we did not make any use of the relation $H(S|BD) = H(S)$ (for $\mathcal{AS}2$ it holds $H(S|BD) = 0$). Hencefrom, the following theorem holds.

Theorem 4.2 *Any secret sharing scheme for $\mathcal{AS}2$ satisfies*

$$H(BC) \geq 3H(S) \quad \textit{and} \quad H(BD) \geq 3H(S).$$

Remark 3. The bound given by Theorem 4.2 is best possible for uniform distributions. Indeed, consider the following secret sharing scheme for $\mathcal{AS}2$. For a binary secret $s \in S = \{0, 1\}$, uniformly choose 2 pairs of bits whose XOR give the secret $s \in S$, that is such that $s = a \oplus b = c \oplus d$ and give share a to participant A, b to B, ac to C, and ad to D. This is a secret sharing scheme which satisfies $H(BC) = H(BD) = 3H(S)$. The scheme can be easily generalized to any non-binary space.

An immediate consequence of Theorem 4.2 is the following corollary.

Corollary 4.3 *If the secret is uniformly chosen in S then any secret sharing scheme for $\mathcal{AS}2$ satisfies either*

$$|B| \geq |S|^{1.5},$$

or

$$|C| \geq |S|^{1.5} \ \ and \ \ |D| \geq |S|^{1.5}.$$

Remark 4. A close look to the proof of Theorem 4.1 reveals that exactly the same bound (i.e, $H(BC) \geq 3H(S)$) holds for any access structure ? for 4 participants A, B, C, and D, satisfying $\{AB\}, \{BC\}, \{ACD\} \in$? and $\{AC\}, \{B\}, \{AD\} \notin$?. The minimal such structure is the closure of $\{\{AB\}, \{BC\}, \{ACD\}\}$, which has $|closure(?)| = 7$.

The reader may wonder why to prove lower bounds on the entropy of sample spaces from which the shares are drawn we consider pairs of participants with the consequence of beeing forced to assertions like "*...either the entropy of ... or the entropy of ... is bigger than 1.5H(S)*". It would be certainly more desirable to prove results which would imply that the entropy of a *given* participant is bigger than $\alpha H(S)$, $\alpha > 1$ (say). Actually, this cannot be achieved. Indeed, given an access structure $\mathcal{A} \subseteq 2^P$ and a fixed participant X one cannot prove a bound on $H(X)$ better than the trivial one $H(X) \geq H(S)$ as the following result shows.

Theorem 4.3 *Let an access structure $\mathcal{A} \subseteq 2^P$ and a participant $X \in P$ be fixed. Then there exists a secret sharing scheme for $\mathcal{A}$ such that $H(X) = H(S)$.*

Proof. Let $A_1, \ldots, A_r$ be all subsets of P such that $X \in A_i$, $i = 1, \ldots, r$ and suppose that the secrets s are chosen from the set S according to the probability distribution $\{p(s)\}_{s \in S}$. Let $S = \{0, 1, \ldots, q-1\}$ and $|A_i| = n_i$, $i = 1, \ldots, r$. Shares given to participant X are chosen from S according to the probability distribution $\{p(s)\}_{s \in S}$. Therefore $H(X) = H(S)$. Now, if a given value x has been given to X, let y be such that $x \oplus y = s$, where $\oplus$ is now the addition modulo q. Divide the value y among the remaining participants in A_i, $i = 1, \ldots, r$, giving randomly chosen values $y_{i_1}, \ldots, y_{n_i - 1}$ such that $y_{i_1} \oplus \ldots \oplus y_{n_i - 1} = y$. The rest of the secret sharing scheme is completed according to any protocol which assures perfect secrecy. $\square$

Note that the above construction, even though it achieves the optimal value of $H(X)$, does not prevent the entropy of other participants from becoming very large.
The same proof can be applied, *mutatis mutandis*, to show that in any access structure which is the closure of the edge set of some graph, if one fixes two participants X and Y then no better bound than $3H(S)$ on the joint entropy $H(XY)$ can be proved.

In some cases it is also useful to know the total amount of secret information that must be given to the participants of a secret sharing scheme. The following result shows that there are acces structures in which the sum of the shares sizes is equal to $1.5|P||S|$. Thus, "in average", any participant must have a share of size at least 1.5 times the size of the secret.

Theorem 4.4 *There is an access structure of $n \geq 5$ participants, for which any scheme requires a total entropy of*

$$\sum_{i=1}^{n} H(X_i) \geq (3n/2)H(S).$$

Proof. Consider the 'circular' access structure defined as the closure of the following set

$$\Big\{\{X_1, X_2\}, \{X_2, X_3\}, ..., \{X_{n-1}, X_n\}, \{X_n, X_1\}\Big\}.$$

For each pair of set of shares X_i and X_{i+1}, we have $H(X_i)+H(X_{i+1}) \geq 3H(S)$. Moreover, $H(X_1)+H(X_n) \geq 3H(S)$. Summing over all pairs we get $H(X_1)+H(X_n)+\sum_{i=1}^{n-1} H(X_i)+H(X_{i+1}) \geq 3nH(S)$. Hence, $\sum_{i=1}^{n} H(X_i) \geq (3n/2)H(S)$. □

Acknowledgments

The authors would like to express their thanks to C. Blundo, A. Orlitsky and D. R. Stinson for useful discussions and comments.

References

[1] J. C. Benaloh and J. Leichter, Generalized Secret Sharing and Monotone Functions, Proceedings of Crypto '88, *Advances in Cryptology*, Lecture Notes in Computer Science, vol. 403, S. Goldwasser, Ed., Springer–Verlag, Berlin, 1990, pp. 27–35.

[2] G. R. Blakley, Safeguarding Cryptographic Keys, *Proceedings of AFIPS 1979 National Computer Conference*, vol. 48, New York, NY, pp. 313-317, June 1979.

[3] G. R. Blakley and C. Meadows, Security of Ramp Schemes, Proceedings of Crypto '84, *Advances in Cryptology*, Lecture Notes in Computer Science, vol. 196, G. R. Blakley and D. Chaum, Eds., Springer–Verlag, Berlin, 1985, pp. 411–431.

[4] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, Graph Decomposition and Secret Sharing Schemes, Proceedings of Eurocrypt '92, *Advances in Cryptology*, Lecture Notes in Computer Science, Springer–Verlag, Berlin, to appear.

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

[6] E. F. Brickell and D. R. Stinson, Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes, Proceedings of Crypto '90, *Advances in Cryptology*, Lecture Notes in Computer Science, vol. 576, S. A. Vanstone, Ed., Springer–Verlag, Berlin, 1992, pp. 242–252.

[7] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, A Note on Secret Sharing Schemes, in: *Sequences '91: Methods in Communications, Security and Computer Science*, R. M. Capocelli, A. De Santis, and U. Vaccaro, Eds., Springer–Verlag, to appear.

[8] I. Csiszár and J. Kőrner, *Information Theory. Coding theorems for discrete memoryless systems,* Academic Press, 1981.

[9] D. Denning, *Cryptography and Data Security,* Addison–Wesley, Reading, MA, 1983.

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

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

[12] M. Ito, A. Saito, and T. Nishizeki, Secret Sharing Scheme Realizing General Access Structure, Proceedings of IEEE Global Telecommunications Conference, Globecom 87, Tokyo, Japan, 1987, pp. 99–102.

[13] E. D. Karnin, J. W. Greene, and M. E. Hellman, On Secret Sharing Systems, *IEEE Transactions on Information Theory*, vol. IT-29, no. 1, Jan. 1983, pp. 35-41.

[14] S. C. Kothari, Generalized Linear Threshold Schemes, Proceedings of Crypto '84, *Advances in Cryptology*, Lecture Notes in Computer Science, vol. 196, G. R. Blakley and D. Chaum, Eds., Springer–Verlag, Berlin, 1985, pp. 231–241.

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

[16] C. E. Shannon, The Mathematical Theory of Communication, *Bell. Syst. J.*, vol. 27, pp. 379–423, 623–656, July/Oct. 1948.

[17] G.J. Simmons, Robust Shared Secret Schemes or "How to be Sure You Have the Right Answer even though You don't Know the Question", *Congressus Numerantium*, vol. 8, pp. 215–248, 1989.