

On the Size of Shares for Secret Sharing Schemes*

R. M. Capocelli¹, A. De Santis², L. Gargano², U. Vaccaro²

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 multi-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 which meets the bound with equality.

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 more 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

*This work was partially supported by the Italian Ministry of the University and Scientific Research, within the framework of the Project: Progetto ed Analisi di Algoritmi and by the National Council of Research, Progetto Finalizzato Sistemi Informatici e Calcolo Parallelo.

or betrayal [Sham], [De]. 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 [GoMiWi]).

As a solution to this problem, Blakley [Bl] and Shamir [Sham] 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 [Simm] for a comprehensive bibliography on (k, n) threshold schemes).

Ito, Saito, and Nishizeki [ItSaNi] 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 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 [BeLe] gave a simpler and more efficient way to realize secret sharing schemes for any given monotone access structure.

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 secret¹. Moreover, there are access structures for which any corresponding secret sharing scheme must give to at least a participant a share of size strictly bigger than the secret size. Indeed, [BeLe] 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 [BrSt] improved on [BeLe] 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 than that of the secret were characterized by Brickell and Davenport [BrDa] 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

¹This property holds since non-qualified subset of participants have *absolutely* no information on the secret. If we relax this requirement (as is done in ramp schemes) 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 [KaGrHe] who initiated the analysis (limited to threshold schemes) of secret sharing schemes when arbitrary probability distributions are involved.

We extend the approach of [KaGrHe] 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 implies 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 [KaGrHe]. We also analyze the relationships between the size of the shares and that of the secret. We improve on the result of [BrSt] 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 [CsKo], [Ga], [Shan].

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

$$0 \leq H(X) \leq \log |X|, \quad (1)$$

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* $H(X|Y)$, 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

$$H(X|Y) \geq 0. \quad (2)$$

The entropy of the joint space XY satisfies

$$H(XY) = H(X) + H(Y|X) = H(Y) + H(X|Y). \quad (3)$$

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

$$I(X; Y) = H(X) - H(X|Y) \quad (4)$$

²All logarithms in this paper are of base 2

and enjoys the following properties:

$$I(X; Y) = I(Y; X), \quad (5)$$

and

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

From which one gets

$$H(X) \geq H(X|Y). \quad (6)$$

The *conditional mutual information* is defined by

$$I(X; Y|Z) = H(X|Z) - H(X|YZ). \quad (7)$$

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

$I(X; Y|Z)$ satisfies three important properties,

$$I(X; Y|Z) \geq 0 \quad (8)$$

$$I(X; Y|Z) = I(Y; X|Z) \quad (9)$$

and

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

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.

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 $\text{closure}(\mathcal{A}) = \{A' : A \in \mathcal{A}, A \subseteq A' \subseteq P\}$. A natural property for an access structure \mathcal{A} is that of being *monotone*, i.e., $\mathcal{A} = \text{closure}(\mathcal{A})$.

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 [KaGrHe] and [Ko], 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 a gives no information about the secret. Notice that the condition $H(S|A) = H(S)$ is equivalent to say that $\forall a \in A \ H(S|A = a) = H(S)$.

Shares given to the participants are not necessarily to be 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 $\{\{A, B\}, \{B, C\}, \{C, D\}\}$. Let the secret s be a uniformly chosen n -bit string. A possible secret sharing scheme for \mathcal{AS} consists of uniformly choosing 3 pairs of strings whose XOR give 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 [KaGrHe] 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 [KaGrHe].

Lemma 3.1 *Let $Y \notin \mathcal{A}$ and $X \cup Y \in \mathcal{A}$. Then $H(X|Y = y) \geq H(S)$ for each possible value y in Y .*

Proof. $I(X; S|Y = y)$ can be written either as $H(X|Y = y) - H(X|SY = y)$ or as $H(S|Y = y) - H(S|XY = y)$. Hence,

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

The second line follows from the first, since $H(S|XY) = 0$ implies $H(S|XY = y) = 0$ for all y such that $p(y) > 0$. \square

By averaging on the elements $y \in Y$ we get that, in the same hypothesis of Lemma 3.1, it holds $H(X|Y) \geq H(S)$. Because of (6), we obtain that $H(X) \geq H(S)$, for each $X \subset P$, which is essentially Theorem 1 of [KaGrHe] generalized to monotone access structures.

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

Lemma 3.2 *If $X \cup Y \notin \mathcal{A}$ 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 $H(S|XY) = H(S|X) = H(S)$, for $X \cup Y \notin \mathcal{A}$, we have $H(Y|X) = H(Y|XS)$. \square

Lemma 3.3 *Let $X, Y, Z \subset P$. If $X \cup Y \in \mathcal{A}$ then $H(Z|XY) \leq H(Z|XS)$.*

Proof. The conditional entropy $H(ZS|XY)$ can be written either as $H(Z|XY) + H(S|XYZ)$ or as $H(S|XY) + H(Z|XYS)$. Since $X \cup Y \in \mathcal{A}$ it follows $H(S|XY) = 0$ and $H(S|XYZ) = 0$. Hence, $H(Z|XY) = H(ZS|XY) = H(Z|XYS)$. Because of $I(Z; Y|XS) \geq 0$ one has $H(Z|XYS) \leq H(Z|XS)$ and the lemma follows. \square

4 Bounds on the size of shares

Benaloh and Leichter [BeLe] 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 $\mathcal{AS} = \text{closure}\{\{A, B\}, \{B, C\}, \{C, D\}\}$. Recently, Brickell and Stinson [BrSt] 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 above limitation. Such access structures are \mathcal{AS} and $\mathcal{AS}2 = \text{closure}\{\{A, B\}, \{B, C\}, \{C, D\}, \{B, D\}\}$. 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.

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. Now we state our lower bound.

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

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

Proof. From (4) we get that $H(B) = H(B|CA) + I(B; CA)$. From (7) and (9) we get that $H(B|CA) = H(S|CA) + H(B|CAS) = H(S) + H(B|CAS)$. Therefore, using formulae (4) and (3) we get

$$H(B) = H(S) + H(B|CAS) + H(A) + H(C|A) - H(A|B) - H(C|AB). \quad (10)$$

Consider now $I(BC; S)$ that can be written either as $H(BC) - H(BC|S) = H(BC) - H(B|S) - H(C|BS)$ or as $H(S) - H(S|BC) = H(S)$. We obtain

$$\begin{aligned} H(BC) &= H(S) + H(B|S) + H(C|BS) \\ &= H(S) + H(B) + H(C|BS) \quad (\text{from Lemma 3.2}) \end{aligned}$$

$$\begin{aligned}
&= H(S) + H(S) + H(B|CAS) + H(A) + H(C|A) - H(A|B) - H(C|AB) \\
&\qquad\qquad\qquad + H(C|BS) \quad (\text{from (10)}) \\
&\geq 2H(S) + H(B|CAS) + H(A) + H(C|A) - H(A|B) \quad (\text{from Lemma 3.3}) \\
&\geq 2H(S) + H(A) - H(A|B) + H(C|A) \quad (\text{from (2)}) \\
&\geq 2H(S) + H(C|A) \quad (\text{from (6)}) \\
&\geq 2H(S) + H(C|AD) \quad (\text{from (8)}) \\
&\geq 3H(S) \quad (\text{from Lemma 3.1}).
\end{aligned}$$

□

The following corollary to Theorem 4.1 is immediate from (3) and (6).

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. Recalling that the entropy of a set is a good approximation of the average number of bits needed to represent an element of the set, we get that there is a share whose size is at least 50% bigger than the secret size.

Benaloh and Leichter [BeLe] 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 [BrSt] improved on [BeLe] 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 $|B| \geq |S|^{1.5}$. \square

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 that moreover $H(A) = H(C) = H(D) = H(S) = 1$ while $H(B) = 2$ and $H(BC) = 3H(S)$. If a 2-bit secret $s_0s_1 \in \{0, 1\}^2$ 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 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 [BrSt]) 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 [BrSt].

The bound given by Corollary 4.1 is the best possible for non-uniform distributions, as well. The construction of a secret sharing scheme which meets the bound with equality is a bit involved and will be given in the final version of the paper.

Our lower bound also holds for $\mathcal{AS}2$ which is the closure of the family

$$\left\{ \{A, B\}, \{B, C\}, \{C, D\}, \{B, D\} \right\}.$$

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

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

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

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

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 Γ for 4 participants A, B, C , and D , satisfying $\{AB\}, \{BC\}, \{ACD\} \in \Gamma$ and $\{AC\}, \{B\}, \{AD\} \notin \Gamma$. The minimal such structure is the closure of $\{\{AB\}, \{BC\}, \{ACD\}\}$, which has $|\text{closure}(\Gamma)| = 7$.

Finally, exploiting the structure of \mathcal{AS} , we can prove the following result.

Theorem 4.3 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

$$\left\{ \{X_1, X_2\}, \{X_2, X_3\}, \dots, \{X_{n-1}, X_n\}, \{X_n, X_1\} \right\}.$$

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

Acknowledgments

The authors would like to express their thanks to D. R. Stinson for his comments, and to C. Blundo for useful discussions about the tightness of the results.

References

- [BeLe] J. C. Benaloh and J. Leichter, *Generalized Secret Sharing and Monotone Functions*, Crypto 88, pp. 27-35.
- [Bl] G. R. Blakley, *Safeguarding Cryptographic Keys*, Proceedings AFIPS 1979 National Computer Conference, pp. 313-317, June 1979.
- [BrDa] E. F. Brickell and D. M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, J. Cryptology, to appear.
- [BrSt] E. F. Brickell and D. R. Stinson, *Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes*, Crypto 90 (Published also as Research Report #106, May 1990, University of Nebraska).
- [CsKo] I. Csiszár and J. Körner, *Information Theory. Coding theorems for discrete memoryless systems*, Academic Press, 1981.
- [De] D. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, MA, 1983.
- [Ga] R. G. Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, New York, NY, 1968.
- [GoMiWi] 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.
- [ItSaNi] M. Ito, A. Saito, and T. Nishizeki, *Secret Sharing Scheme Realizing General Access Structure*, Proc. IEEE Global Telecommunications Conf., Globecom 87, Tokyo, Japan, 1987, pp. 99-102.
- [KaGrHe] E. D. Karnin, J. W. Greene, and M. E. Hellman, *On Secret Sharing Systems*, IEEE Trans. on Inform. Theory, vol. IT-29, no. 1, Jan. 1983, pp. 35-41.

- [Ko] S. C. Kothari, *Generalized Linear Threshold Schemes*, Crypto 84, pp. 231–241.
- [Sham] A. Shamir, *How to Share a Secret*, Communications of the ACM, vol. 22, n. 11, pp. 612–613, Nov. 1979.
- [Shan] C. E. Shannon, *The Mathematical Theory of Communication*, Bell. Syst. J., vol. 27, pp. 379–423, 623–656, July/Oct. 1948.
- [Simm] 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.
- [Simm2] G.J. Simmons, *The Geometry of Shared Secret Schemes*, Bulletin of the Institute of Combinatorics and its Applications (ICA), vol. 1, pp. 59–70, Jan. 1991.