Multi-Secret Sharing Schemes *

Extended Abstract

Carlo Blundo, Alfredo De Santis, Giovanni Di Crescenzo,
Antonio Giorgio Gaggia, and Ugo Vaccaro

Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84081 Baronissi (SA), Italy
{carblu,ads,giodic,antgio,uv}@udsab.dia.unisa.it

Abstract. A multi-secret sharing scheme is a protocol to share m arbitrarily related secrets $s_1, \ldots, s_m$ among a set of participants $\mathcal{P}$. In this paper we put forward a general theory of multi-secret sharing schemes by using an information theoretical framework. We prove lower bounds on the size of information held by each participant for various access structures. Finally, we prove the optimality of the bounds by providing protocols.

1 Introduction

A secret sharing scheme is a technique to share a secret s among a set $\mathcal{P}$ of participants in such a way that only qualified subsets, pooling together their information, can reconstruct the secret s; but subsets of participants that are not enabled to recover the secret have no information on it. Secret sharing schemes are useful in any important action that requires the concurrence of several designed people to be initiated, as launching a missile, opening a bank vault or even opening a safety deposit box. Secret sharing schemes are also used in management of cryptographic keys and multi-party secure protocols (see [10], [2]).

Secret sharing schemes were introduced by Shamir [16] and Blakley [3]. They analyzed the case when only subsets A of $\mathcal{P}$ of cardinality $|A| \geq k$, for a fixed integer k, can reconstruct the secret. These schemes are called (k, n) threshold schemes, where $n = |\mathcal{P}|$. Subsequently, Ito, Saito, and Nishizeki [11] and Benaloh and Leichter [1] 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. The recent survey by Stinson [18] contains an unified description of recent results in the area of secret sharing schemes. For different approaches to the study of secret sharing schemes, for schemes with "extended capabilities" as disenrollment, fault-tolerance, and pre-positioning and for a complete bibliography we recommend the survey article by Simmons [17].

* Partially supported by Italian Ministry of University and Research (M.U.R.S.T.) and by National Council for Research (C.N.R.).

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 150-163, 1994.

There are several situations in which more than one secret is to be shared among participants. As an example, consider the following situation, described by Simmons [17]: there is a missile battery and not all of the missiles have the same launch enable code. The problem is to devise a scheme which will allow any one, or any selected subset, of the launch enable codes to be activated in this scheme. What is needed is an algorithm such that the same pieces of private information could be used to recover different secrets. This problem could be trivially solved by realizing different secret sharing schemes, one for each of the launch enable codes, but this solution is clearly unacceptable since each participant should remember too much information.

Another scenario in which the sharing of many secrets is important was considered by Franklin and Yung [8]. 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 technique applies to all of the protocols for secure computation which use polynomial–based threshold schemes and applies to all fault–tolerant models. Franklin and Yung [8] considered also the case of dependent secrets in which the amount of information distributed to any participant is less than the information distributed with independent schemes.

The problem of sharing more than one secret was also considered in [14].

Blundo, De Santis, and Vaccaro [5] considered the case in which m secrets are shared among participants in $\mathcal{P}$ of a single access structure $\mathcal{A}$ in such a way that: 1) any qualified subset of participants can reconstruct all the secrets, 2) any non-qualified subset has absolutely no information on any secret, and 3) any non-qualified subset knowing the value of a number of secrets might determine some (possibly no) information on other secrets. They proved lower bounds on the size of the domains from which the share given to participants are taken. Moreover, they proved that the protocol proposed by Franklin and Yung [8] is optimal with respect to the amount of information given to each participant.

Recently Jackson, Martin, and O'Keefe [12] considered the problem where participants can reconstruct more than one secret using the information that they hold. In particular, they considered the situation in which there is a secret associated with each set $K \subseteq \mathcal{P}$, where $|K| = k$. This secret can be reconstructed by any t ($t \leq k$) participants of K. They proved bounds on the size of information that participants must hold in order to ensure that up to w participants ($0 \leq w \leq n - k + t - 1$) cannot obtain any information about a secret they are not associated with. In [12] such schemes are referred as multisecret threshold schemes. Finally, in [13] the authors provide an optimal scheme, with respect to the information given to each participant, for some value of the parameters t and w.

In this paper we put forward a general theory of multi-secret sharing schemes by using an information theoretical framework. We prove lower bounds on the

size of information held by each participant for various access structures. Finally, we prove the optimality of the bounds. We prove that in some cases the protocol consisting of realizing different secret sharing schemes, one for each of the secrets, is optimal with respect to the size of the share given to a single participant. In other cases the before mentioned protocol is not optimal and we exhibit schemes that give to participants shares taken from a smaller domain.

The paper is organized as follows. In Section 2 we formally define multi–secret sharing schemes by using information theoretical quantities. We consider two possible models of multi-secret sharing schemes. We model secret sharing schemes by using the entropy mainly because this leads to a compact and simple description of the scheme and because the entropy approach takes into account all probability distributions on the secret. Finally, each bound we obtain on the entropy of the share of a participant implies a bound on the amount of information held by such a participant. In Subsection 2.3 we prove that the two models proposed for multi–secret sharing are equivalent. In Section 3 we show how to construct perfect multi-secret sharing schemes for two and three secrets in which the shares distributed are taken from domains as small as possible. An important issue in the implementation of secret sharing schemes is the size of the shares given to participants, since the security of a system degrades as the amount of secret information increases. Thus, one of the basic problems in the field of secret sharing schemes is to derive bounds on the amount of information that must be kept secret. In Section 4 we prove a lower bound on the information distributed to any participant in multi–secret sharing schemes. Finally, in Section 5 we analyze the case in which all the access structures are threshold structures. We prove lower bounds on the size of information held by each participant in the scheme and provide optimal protocols for multi-secret sharing in threshold structures.
Due to the space limit on this extended abstract, some proofs are omitted. The authors will supply a complete version on request.

2 The Models

In this section we give two different definitions of multi-secret sharing schemes and show their equivalence. Let us first briefly recall the concept of secret sharing scheme.

A secret sharing scheme permits a secret to be shared among a set $\mathcal{P}$ of n participants in such a way that only qualified subsets of $\mathcal{P}$ can recover the secret, but any non-qualified subset has absolutely no information on the secret. An access structure $\mathcal{A}$ is the set of all subsets of $\mathcal{P}$ that can recover the secret.

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 $A \in \mathcal{A}, A \subseteq A' \subseteq P \Rightarrow A' \in \mathcal{A}$.

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

For a monotone access structure $\mathcal{A}$ we have $\mathcal{A} = \mathrm{cl}(\mathcal{A})$. From now on we will consider only monotone access structures.

In multi-secret sharing schemes the problem of sharing many secrets is addressed. We consider two models of multi-secret sharing. The first model is a natural generalization of single secret sharing: we consider different access structures and in each of them we share a different secret. We will refer to this model as *Type A*. In the second model, referred to as *Type B*, each set $A \subseteq \mathcal{P}$ can recover a set S_A of secrets, where it can be $S_A = \emptyset$. This second model generalizes the one considered by Jackson, Martin, and O'Keefe [12]. Even though it could appear that the two models are different, we will show that they are indeed equivalent.

The following setting is common to both models. Let $\mathcal{P}$ be a set of participants, let S_i be the space from which the i-th secret s_i can be selected, for $i = 1, \ldots, m$, and let $\mathcal{SC}$ be the cartesian product $S_1 \times \cdots \times S_m$. Finally, let $\{p_{\mathcal{SC}}(s_1, \ldots, s_m)\}_{(s_1,\ldots,s_m)\in\mathcal{SC}}$ be a probability distribution on $\mathcal{SC}$. Let a multi-secret sharing scheme for secrets in $\mathcal{SC}$ 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. Given a set of participants $A = \{P_{i_1}, \ldots, P_{i_r}\} \subseteq \mathcal{P}$, where $i_1 < i_2 < \ldots < i_r$, set $K(A) = K(P_{i_1}) \times \cdots \times K(P_{i_r})$. Any multi-secret sharing scheme for secrets in $\mathcal{SC}$ and a probability distribution $\{p_{\mathcal{SC}}(s_1, \ldots, s_m)\}_{(s_1,\ldots,s_m)\in\mathcal{SC}}$ naturally induce a probability distribution on $K(A)$, for any $A \subseteq \mathcal{P}$. Denote such a probability distribution by $\{p_{K(A)}(a)\}_{a\in K(A)}$. Finally, denote by $H(S_i)$ the entropy[2] of $\{p_{S_i}(s)\}_{s\in S_i}$ and by $H(A)$ the entropy of $\{p_{K(A)}(a)\}_{a\in K(A)}$, for any $A \subseteq \mathcal{P}$. If S_A is a set of secrets $\{s_{i_1}, \ldots, s_{i_a}\}$, where $s_{i_j} \in S_{i_j}$, then denote by $H(S_A)$ the entropy of $\{p_{S_{i_1}\times\cdots\times S_{i_a}}(s_{i_1}, \ldots, s_{i_a})\}_{s_{i_j}\in S_{i_j},\, j=1,\ldots,a}$. To avoid overburdening the notation, we will denote with the same symbol both a random variable and the set of its possible values. As an example, with S_i we will denote both the set in which the i-th secret is chosen and the random variable that takes values in the set S_i with probability distribution $\{p_{S_i}(s)\}_{s\in S_i}$.

We will give our two definitions of multi-secret sharing schemes first in terms of the probability distribution on the secret and on the shares given to participants, and then using the entropy function as done in [14], [15], and [6].

2.1 The First Model

In the first definition of perfect 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 $\mathcal{P}$ 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 secret $s_i \in S_i$. This means that only the sets in $\mathcal{A}_i$ can recover the secret s_i, but any set $A \notin \mathcal{A}_i$ has no information on it. A multi-secret sharing scheme of Type A is defined as follows.

[2] For definition and properties of information theoretic quantities we refer to [7] and [9].

Definition 3. Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of monotone access structures on the set of participants $\mathcal{P}$. A *multi-secret sharing scheme of Type A* for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ is a sharing of the secrets $(s_1, \ldots, s_m) \in S_1 \times \cdots \times S_m$ in such a way that, for $i = 1, \ldots, m$,

1. *Any subset $A \subseteq \mathcal{P}$ of participants enabled to recover s_i can compute s_i.*
   Formally, if $A \in \mathcal{A}_i$ then for all $a \in K(A)$ with $p_{K(A)}(a) > 0$, it holds $p(s_i|a) = 1$.
2. *Any subset $A \subseteq \mathcal{P}$ of participants not enabled to recover s_i, even knowing some of the other secrets, has no more information on s_i than that already conveyed by the known secrets.*
   Formally, if $A \notin \mathcal{A}_i$ then for all $a \in K(A)$ and $t \subseteq \{s_1, \ldots, s_m\} \setminus \{s_i\}$, it holds $p(s_i|at) = p(s_i|t)$.

Property 1. means that the values of the shares held by $A \in \mathcal{A}_i$ completely determine the secret s_i. Property 2. means that the probability that a secret is equal to s_i given that any subset of secrets not including s_i is equal to t and that the shares held by $A \notin \mathcal{A}_i$ are equal to a, is the same as the *a priori* probability of the secret s_i given that any subset of secrets not including s_i is equal to t. In case $t = \emptyset$, this is equivalent to say that no amount of knowledge of shares of participants not qualified to reconstruct a secret enables a Bayesian opponent to modify an *a priori* guess regarding which the secret is.

Now we can restate above conditions 1. and 2. using information theoretic tools. We model secret sharing schemes by using the entropy mainly because this leads to a compact and simple description of the scheme and because the entropy approach takes into account all probability distributions on the secret. Finally, each bound we obtain on the entropy of the share of a participant implies a bound on the amount of information held by such a participant.

Definition 4. Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of monotone access structures on the set of participants $\mathcal{P}$. A *multi-secret sharing scheme of Type A* for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ is a sharing of the secrets $(s_1, \ldots, s_m) \in S_1 \times \cdots \times S_m$ in such a way that, for $i = 1, \ldots, m$,

a. *Any subset $A \subseteq \mathcal{P}$ of participants enabled to recover s_i can compute s_i.*
   Formally, for all $A \in \mathcal{A}_i$, it holds $H(S_i|A) = 0$.
b. *Any subset $A \subseteq \mathcal{P}$ of participants not enabled to recover s_i, even knowing some of the other secrets, has no more information on s_i than that already conveyed by the known secrets.*
   Formally, for all $A \notin \mathcal{A}_i$ and $T \subseteq \{S_1, \ldots, S_m\} \setminus \{S_i\}$, it holds $H(S_i|A\,T) = H(S_i|T)$.

Notice that $H(S_i|A) = 0$ means that each set of values of the shares in A corresponds to a unique value of the secret. In fact, by definition, $H(S_i|A) = 0$ is equivalent to the fact that for all $a \in K(A)$ with $p_{K(A)}(a) > 0$ it holds $p(s_i|a) = 1$. Moreover, $H(S_i|AT) = H(S_i|T)$ is equivalent to state that S_i and $K(A)$ are statistically independent, given the secrets in T; i.e., for all $a \in K(A)$ and all

$t \in T$, it holds $p(s_i|at) = p(s_i|t)$, and therefore the knowledge of a gives no information about the secret s_i that is not already given by t. Finally, notice that in the case the access structures $\mathcal{A}_1, \ldots, \mathcal{A}_m$ are all equal to the same structure $\mathcal{A}$, a multi-secret sharing scheme for secrets $s_1, \ldots, s_m$ reduces to a secret sharing scheme for the secret $s = s_1 \circ \cdots \circ s_m$ with access structure $\mathcal{A}$, where with $x \circ y$ we denote the concatenation of x and y.

2.2 The Second Model

In our second definition of perfect multi-secret sharing schemes a set $\mathcal{S} = \{s_1, \ldots, s_m\}$ of secrets, where each s_i is chosen in a set S_i, is shared among a set $\mathcal{P}$ of participants in such a way that each subset of $\mathcal{P}$ can recover a certain subset of $\mathcal{S}$, but has absolutely no information on the remaining secrets.

For each subset of participants $A \subseteq \mathcal{P}$, we denote by $S_A \subseteq \mathcal{S}$ the set of secrets that can be recovered by A, referred to as the A-secrets-set. It should be pointed out that in some cases we could have $S_A = \emptyset$. Since we only consider monotone access structures, it turns out that for any $A, B \subseteq \mathcal{P}$ if $A \subseteq B$, then $S_A \subseteq S_B$.

Definition 5. Let $\mathcal{P}$ be a set of participants, $\mathcal{S}$ be a set of secrets, and $\{S_A\}_{A \subseteq \mathcal{P}}$ be the family of A-secrets-sets. A *multi-secret sharing scheme of Type B* for $\{S_A\}_{A \subseteq \mathcal{P}}$ is a sharing of the secrets in $\mathcal{S}$ among participants in $\mathcal{P}$ in such a way that

1'. *Any subset $A \subseteq \mathcal{P}$ of participants is enabled to recover the A-secrets-set S_A.*
Formally, for all $a \in K(A)$ with $p_{K(A)}(a) > 0$ and $s \in S_A$, it holds $p(s|a) = 1$.

2'. *Any subset $A \subseteq \mathcal{P}$ of participants has no information on any subset of secrets in $\mathcal{S} \setminus S_A$.*
Formally, for all $A \subseteq \mathcal{P}$, for all $a \in K(A)$ and $t \subseteq \mathcal{S} \setminus S_A$, it holds $p(t|a) = p(t)$.

Property 1'. means that the value of the shares held by $A \subseteq \mathcal{P}$ completely determines the secrets in S_A. Property 2'. means that the probability that a subset of secrets is equal to t given that the shares held by A are a, is the same as the *a priori* probability of the secrets in t. Therefore, no amount of knowledge of shares of participants not qualified to reconstruct a subset of secrets enables a Bayesian opponent to modify an *a priori* guess regarding which the secrets are.

For any $A \subseteq \mathcal{P}$, if $S_A = \{s_{i_1}, \ldots, s_{i_a}\}$, then with S_A we denote the family $S_A = \{S_{i_1}, \ldots, S_{i_a}\}$. Now we can restate above conditions 1'. and 2'. using information theoretic tools.

Definition 6. Let $\mathcal{P}$ be a set of participants, $\mathcal{S}$ be a set of secrets, and $\{S_A\}_{A \subseteq \mathcal{P}}$ be the family of A-secrets-sets. A *multi-secret sharing scheme of Type B* for $\{S_A\}_{A \subseteq \mathcal{P}}$ is a sharing of the secrets in $\mathcal{S}$ among participants in $\mathcal{P}$ in such a way that

a'. *Any subset $A \subseteq \mathcal{P}$ of participants is enabled to recover the A-secrets-set S_A.*
Formally, for all $A \subseteq \mathcal{P}$, it holds $H(S_A|A) = 0$.

b'. *Any subset $A \subseteq \mathcal{P}$ of participants has no information on any subset of secrets in $\mathcal{S} \setminus S_A$.*
Formally, for all $A \subseteq \mathcal{P}$ and $T \subseteq \{S_1, \ldots, S_m\} \setminus S_A$, it holds $H(T|A) = H(T)$.

Notice that $H(S_A|A) = 0$ means that each set of values of the shares of participants in A corresponds to a unique value of the secrets in S_A. Moreover, $H(T|A) = H(T)$ is equivalent to state that $T \subseteq \{S_1, \ldots, S_m\} \setminus S_A$, and $K(A)$ are statistically independent and therefore the knowledge of the shares of the participants in A gives no information about the secrets in $S \setminus S_A$.

2.3 The Equivalence of the Two Models

In this section we prove that the two definitions presented for perfect multi-secret sharing schemes are equivalent; that is, each scheme satisfying one definition satisfies also the other as stated by next theorem.

Theorem 7. *Let $\mathcal{P}$ be a set of participants and let $S_1 \times \cdots \times S_m$ be a probability space from which the secrets $(s_1, \ldots, s_m)$ are chosen. The following statements hold.*

1. *Let $\mathcal{A}_1, \ldots, \mathcal{A}_m$ be access structures on the set of participants $\mathcal{P}$. If Σ is a secret sharing scheme of Type A for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$, then Σ is a secret sharing scheme of Type B for the family $\{S_A\}_{A \subseteq \mathcal{P}}$, where $S_A = \{s_i : A \in \mathcal{A}_i,\ i \in [1, m]\}$.*
2. *Let $\{S_A\}_{A \subseteq \mathcal{P}}$ be a family of A-secret-sets. If Σ is a secret sharing scheme of Type B for $\{S_A\}_{A \subseteq \mathcal{P}}$, then Σ is a secret sharing scheme of Type A for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$, where $\mathcal{A}_i = \{A \subseteq \mathcal{P} : s_i \in S_A\}$.*

Proof: Suppose Σ is a multi-secret sharing scheme of Type A. Let $(\mathcal{A}_1, ..., \mathcal{A}_m)$ be an m-tuple of access structures on participants $\mathcal{P}$ and let $(s_1, ..., s_m) \in S_1 \times \cdots \times S_m$ be the secrets shared in $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$. For any $A \subseteq \mathcal{P}$ let $S_A = \{s_i : A \in \mathcal{A}_i,\ i \in [1, m]\}$. We prove that conditions a'. and b'. of Definition 6 are satisfied. Let us prove that $H(S_A|A) = 0$. We have that

$$\begin{aligned} H(S_A|A) &= H(S_{j_1}, \ldots, S_{j_r}|A) \\ &= H(S_{j_1}|A) + \sum_{i=2}^{r} H(S_{j_i}|S_{j_1} \ldots S_{j_{i-1}} A) \\ &\leq \sum_{i=1}^{r} H(S_{j_i}|A) \\ &= 0. \end{aligned}$$

Now, we prove that for any $T \subseteq \mathcal{S} \setminus S_A$, it holds $H(T|A) = H(T)$. Suppose that $T = \{S_{j_1}, \ldots, S_{j_t}\}$. We have

$$H(T|A) = H(S_{j_1}, \ldots, S_{j_t}|A)$$

$$
\begin{aligned}
&= H(S_{j_1}|A) + \sum_{i=2}^{t} H(S_{j_i}|S_{j_1} \ldots S_{j_{i-1}} A) \\
&= H(S_{j_1}) + \sum_{i=2}^{t} H(S_{j_i}|S_{j_1} \ldots S_{j_{i-1}}) \\
&= H(S_{j_1}, \ldots, S_{j_t}) \\
&= H(T).
\end{aligned}
$$

Hence, if Σ is a multi-secret sharing scheme of Type A for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$, then Σ is also a multi-secret sharing scheme of Type B for $\{S_A\}_{A \subseteq \mathcal{P}}$.
Now we prove that statement 2. of the theorem holds. Let $\{S_A\}_{A \subseteq \mathcal{P}}$ be a family of A-secrets-sets. Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures, where $\mathcal{A}_i = \{A \subseteq \mathcal{P} : s_i \in S_A\}$. We prove that conditions *a.* and *b.* of Definition 4 are satisfied. It is easy to prove that for all $A \in \mathcal{A}_i$ it holds $H(S_i|A) = 0$. Indeed, we get $H(S_i|A) \leq H(S_A|A)$ and since $H(S_A|A) = 0$ from a'. of Definition 6, it follows that $H(S_i|A) = 0$. Now, we prove that for all $A \notin \mathcal{A}_i$ and $T \subseteq \{S_1, \ldots, S_m\} \setminus \{S_i\}$, it holds $H(S_i|A\ T) = H(S_i|T)$. Notice that if $A \notin \mathcal{A}_i$ then $s_i \notin S_A$. Let $T = T_1 \cup T_2$, where $T_1 \subseteq S_A$ and $T_2 \cap S_A = \emptyset$. We have,

$$
\begin{aligned}
H(T_2) + H(S_i|T_2) &= H(S_i T_2) \\
&= H(S_i T_2|A) \\
&= H(S_i T_2|A) + H(T_1|A) \\
&= H(S_i T_1 T_2|A) \\
&= H(T_2|A) + H(T_1|AT_2) + H(S_i|AT_1T_2) \\
&= H(T_2|A) + H(S_i|AT_1T_2) \\
&= H(T_2) + H(S_i|AT_1T_2)
\end{aligned}
$$

From previous equalities we get $H(S_i|T_2) = H(S_i|AT)$. From well known properties of the entropy function we have $H(S_i|T_2) \geq H(S_i|T)$ and $H(S_i|AT) \leq H(S_i|T)$. Thus, the theorem holds. □

From now on, the term multi-secret sharing scheme will refer to any of the two definitions given.

3 Sharing Two and Three Secrets

In this section we describe multi-secret sharing schemes for two and three secrets. We are interested in limiting the size of the share of a fixed participant P. The scheme we propose are realized, for simplicity of the description, considering as qualified sets only pairs of participants, but they can be easily extended to handle the general case where instead of participants we have groups of them.

3.1 The Case of Two Secrets

In this section we consider the case where $\mathcal{P} = \{P, P_1, P_2\}$ and $\mathcal{S} = \{S_1, S_2\}$. Suppose that $\{P, P_1\} \in \mathcal{A}_1$, $\{P, P_2\} \in \mathcal{A}_2$, $\{P, P_1\} \notin \mathcal{A}_2$, and $\{P, P_2\} \notin \mathcal{A}_1$. If we use the single-secret sharing construction for S_1 and S_2, we obtain a perfect multi-secret sharing scheme in which the dealer gives P a share such that $H(P) \geq H(S_1S_2)$.

Assume that $\{P_1, P_2\} \in \mathcal{A}_1 \cup \mathcal{A}_2$; we describe a scheme such that, for uniformly and independently chosen 1-bit secrets, distributes shares to participants such that $H(P) = H(S_1) = H(S_2)$. Denote by $\oplus$ the logical xor between two bits.

The dealer uniformly chooses two independent bits a, b and distributes the shares as follows:

- P gets $a \oplus b$
- P_1 gets $a \oplus s_1$, b
- P_2 gets a, $b \oplus s_2$.

In the next section (Corollary 9) we will see that in the case $\{P_1, P_2\} \notin \mathcal{A}_1 \cup \mathcal{A}_2$, all multi-secret sharing schemes must satisfy $H(P) \geq H(S_1S_2)$.

3.2 The Case of Three Secrets

In this section we consider the case where $\mathcal{P} = \{P, P_1, P_2, P_3\}$ and $\mathcal{S} = \{S_1, S_2, S_3\}$. Assume that $\{P, P_j\} \in \mathcal{A}_j$, for each $j = 1, 2, 3$. We distinguish two cases according to which group of participants can recover a subset of the secrets and for each case we describe a multi-secret sharing scheme which gives P a share taken from a domain as small as possible.

1. $\{P_1, P_2, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{A}_3$, that is, participants P_1, P_2, and P_3 together are able to recover S_1, S_2, and S_3
   (a) $\{P_1, P_2\} \in \mathcal{A}_1 \cap \mathcal{A}_2, \{P_1, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_3$, and $\{P_2, P_3\} \in \mathcal{A}_2 \cap \mathcal{A}_3$
   (b) $\{P_i, P_j\} \notin \mathcal{A}_i \cap \mathcal{A}_j$, for some $i, j \in \{1, 2, 3\}$ and $i \neq j$;

2. $\{P_1, P_2, P_3\} \notin \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{A}_3$, that is, participants P_1, P_2, and P_3 together are not able to recover at least one of S_1, S_2, and S_3
   (a) $\{P_i, P_j\} \in \mathcal{A}_i \cap \mathcal{A}_j$, for some $i, j \in \{1, 2, 3\}$ and $i \neq j$;
   (b) $\{P_1, P_2\} \notin \mathcal{A}_1 \cap \mathcal{A}_2$, $\{P_1, P_3\} \notin \mathcal{A}_1 \cap \mathcal{A}_3$, and $\{P_2, P_3\} \notin \mathcal{A}_2 \cap \mathcal{A}_3$.

The above classification partitions the family of all triples of access structures we could get in four classes. We construct a multi-secret sharing scheme for each class for uniformly and independently chosen 1-bit secrets.

For all schemes the dealer uniformly chooses three independent bits a, b, and c distributing the shares as follows.

- Case 1.*a*:
  - P gets $a \oplus b \oplus c$

- P_1 gets $a \oplus s_1, b, c$
- P_2 gets $a, b \oplus s_2, c$
- P_3 gets $a, b, c \oplus s_3$

In this case we have that $\{P_1, P_2\} \in \mathcal{A}_1 \cap \mathcal{A}_2$, $\{P_1, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_3$, and $\{P_2, P_3\} \in \mathcal{A}_2 \cap \mathcal{A}_3$. It is easy to obtain from this scheme all possible schemes for access structures satisfying the conditions of case 1.*a* by distributing additional shares to participants P_1, P_2, P_3. For example, assume $\{P_1, P_2\} \in \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{A}_3$, $\{P_1, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_3$, and $\{P_2, P_3\} \in \mathcal{A}_2 \cap \mathcal{A}_3$. Then, the dealer uniformly chooses a bit d and distributes as additional shares d to P_1 and $d \oplus s_3$ to P_2.

- Case 1.*b*:
  Assume, wlog, that $\{P_1, P_2\} \notin \mathcal{A}_1 \cap \mathcal{A}_2$.
  - P gets $a \oplus c, b$
  - P_1 gets $a \oplus s_1, b, c$
  - P_2 gets $b \oplus s_2, c$
  - P_3 gets $a, c \oplus s_3$

In this case we have that $\{P_1, P_2\} \in \mathcal{A}_2$ $\{P_2, P_3\} \in \mathcal{A}_3$, and $\{P_1, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_3$. It is easy to obtain from this scheme all possible schemes for access structures satisfying the conditions of case 1.*b* by distributing additional shares to participants P_1, P_2, P_3. For example, assume $\{P_1, P_2\} \in \mathcal{A}_2 \cap \mathcal{A}_3$, $\{P_1, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{A}_3$, and $\{P_2, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{A}_3$. Then, the dealer uniformly chooses three bits d, e, and f distributing as additional shares $d, f \oplus s_2$ to P_1, $d \oplus s_3, e$ to P_2, and $b, e \oplus s_1, f$ to P_3.

- Case 2.*a*:
  Assume, wlog, that $\{P_1, P_2\} \in \mathcal{A}_1 \cap \mathcal{A}_2$.
  - P gets $a \oplus b, c$
  - P_1 gets $a \oplus s_1, b$
  - P_2 gets $a, b \oplus s_2$
  - P_3 gets $a, b, c \oplus s_3$

In this case we have that $\{P_1, P_2\} \in \mathcal{A}_1 \cap \mathcal{A}_2$, $\{P_1, P_3\} \in \mathcal{A}_1$, and $\{P_2, P_3\} \in \mathcal{A}_2$. It is easy to obtain from this scheme all possible schemes for access structures satisfying conditions of case 2.*a* by distributing additional shares to participants P_1, P_2, and P_3. For example, assume $\{P_1, P_2\} \in \mathcal{A}_1 \cap \mathcal{A}_2, \{P_1, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_2$, and $\{P_2, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_2$. Then, the dealer uniformly chooses two bits d and e distributing as additional shares $d, c \oplus s_2$ to P_3 $d \oplus s_1$ to P_2, and e to P_1.

- Case 2.*b* :
  - P gets a, b, c
  - P_1 gets $a \oplus s_1$
  - P_2 gets $a, b \oplus s_2$
  - P_3 gets $a, b, c \oplus s_3$

In this case we have that $\{P_1, P_2\} \in \mathcal{A}_1$, $\{P_1, P_3\} \in \mathcal{A}_1$, and $\{P_2, P_3\} \in \mathcal{A}_2$. It is easy to obtain from this scheme all possible schemes for access structures satisfying case 2.*b* by distributing additional shares to participants P_1, P_2, and P_3. For example, assume $\{P_1, P_2\} \in \mathcal{A}_1, \{P_1, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_2$, $\{P_2, P_3\} \in \mathcal{A}_1 \cap \mathcal{A}_2$. Then, the dealer uniformly chooses two bits d and e distributing as additional shares $d \oplus s_2$ to P_1, e to P_2, and $d, e \oplus s_1$ to P_3.

In the next section we will prove that the above schemes are optimal with respect to the entropy of P's share.

4 Bounds on the Size of the Shares

In the previous section we have investigated the possibility of constructing perfect multi-secret sharing schemes without using necessarily different single-secret sharing schemes one for each of the secrets. We have seen that in some cases the shares given to participants are taken from smaller domains. In this section we give lower bounds on the entropy of the share of a single participant.

Theorem 8. *Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. Assume that for all $S_i \in \{S_1, \ldots, S_m\}$ and $T \subseteq \{S_1, \ldots, S_m\} \setminus \{S_i\}$ it holds $H(S_i|T) > 0$. If there exist a participant P and $j \leq m$ subsets of participants $X_{i_1}, \ldots, X_{i_j} \subset \mathcal{P}$, such that $\{P\} \cup X_{i_1} \cup \cdots \cup X_{i_t} \in \mathcal{A}_{i_t}$ and $X_{i_1} \cup \ldots \cup X_{i_t} \notin \mathcal{A}_{i_t}$ for $1 \leq t \leq j$, then in any multi-secret sharing scheme for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ the entropy of the share given to P satisfies*

$$H(P) \geq H(S_{i_1}, \ldots, S_{i_j}) + H(P|X_{i_1}, \ldots, X_{i_j}, S_{i_1}, \ldots, S_{i_j}).$$

Corollary 9. *Given the secrets S_1, S_2 and the set of participants $\mathcal{P} = \{P, P_1, P_2\}$, let $(\mathcal{A}_1, \mathcal{A}_2)$ be a pair of access structures such that $\{P, P_1\} \in \mathcal{A}_1$, $\{P, P_2\} \in \mathcal{A}_2$, $\{P, P_1\} \notin \mathcal{A}_2, \{P, P_2\} \notin \mathcal{A}_1$, and $\{P_1, P_2\} \notin \mathcal{A}_1 \cap \mathcal{A}_2$. Then, in any multi-secret sharing scheme for $(\mathcal{A}_1, \mathcal{A}_2)$ the entropy of the share given to P satisfies $H(P) \geq H(S_1 S_2)$.*

Proof: Assume $\{P_1, P_2\} \in \mathcal{A}_1$. Thus, $P_1 \notin \mathcal{A}_1$ and $\{P_1, P_2\} \notin \mathcal{A}_2$. Participants P_1 and P_2 satisfy the hypothesis of Theorem 8, hence $H(P) \geq H(S_1 S_2)$. □

Corollary 10. *Given the secrets S_1, S_2, and S_3, and the set of participants $\mathcal{P} = \{P, P_1, P_2, P_3\}$, let $(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ be a triple of access structures such that $\{P, P_j\} \in \mathcal{A}_j$ and $\{P, P_j\} \notin \mathcal{A}_i$, for each $i, j \in \{1, 2, 3\}$ with $i \neq j$. Then, in any multi-secret sharing schemes for $(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ the entropy of the share given to P satisfies*

1. *$H(P) \geq H(S_1)$ in Case 1.a of Section 3.2.*
2. *$H(P) \geq H(S_1 S_2)$ in Cases 1.b and 2.a of Section 3.2.*
3. *$H(P) \geq H(S_1 S_2 S_3)$ in Case 2.b of Section 3.2.*

The previous corollaries prove the optimality of the sharing schemes given in Sections 3.1 and 3.2 with respect to the entropy of P's share.

5 Multi-Secret Schemes for Threshold Structures

In this section we consider the problem of sharing secrets in different threshold structures. More precisely, we analyze the case in which for each secret s_i, the access structure $\mathcal{A}_i$ is the set of all subsets consisting of at least k_i participants in $\mathcal{P}_i$, and will be denoted by $\mathcal{A}_{(k_i,\mathcal{P}_i)}$. Next corollaries immediately follow from Theorem 8.

Corollary 11. *Let $(\mathcal{A}_{(k,\mathcal{P}_1)},\ldots,\mathcal{A}_{(k,\mathcal{P}_m)})$ be an m-tuple of threshold structures on a set of participants $\mathcal{P}=\cup_{i=1}^{m}\mathcal{P}_i$. If $\mathcal{P}_1\subseteq\mathcal{P}_2\subseteq\cdots\subseteq\mathcal{P}_m$, then in any multi-secret sharing scheme for $(\mathcal{A}_{(k,\mathcal{P}_1)},\ldots,\mathcal{A}_{(k,\mathcal{P}_m)})$ the entropy of the share given to any participant $P\in\mathcal{P}_j$ satisfies*

$$H(P)\geq H(S_jS_{j+1}\ldots S_m).$$

Proof: Let P be a participant in $\mathcal{P}_j$. Construct the sets $X_j,X_{j+1},\ldots,X_m$ as follows. Let the set X_j be equal to $X_j=\{P_{i_1},\ldots,P_{i_{k-1}}\}$, with $X_j\subseteq\mathcal{P}_j\backslash\{P\}$. For $i=j+1,\ldots,m$, let $X_i=X_j$. It is easy to see that the participant P and the sets $X_j,X_{j+1},\ldots,X_m$ satisfies the hypothesis of Theorem 8, thus the corollary is proved. □

Corollary 12. *Let $(\mathcal{A}_{(k_1,\mathcal{P}_1)},\ldots,\mathcal{A}_{(k_m,\mathcal{P}_m)})$ be an m-tuple of threshold structures on a set of participants $\mathcal{P}=\cup_{i=1}^{m}\mathcal{P}_i$, with $k_1\leq k_2\cdots\leq k_m$. Suppose $\cap_{i=1}^{m}\mathcal{P}_i\neq\emptyset$. Let $\ell<m$ be the smallest integer such that $|\cap_{i=1}^{m}\mathcal{P}_i|<k_\ell$. Then in any multi-secret sharing scheme for $(\mathcal{A}_{(k_1,\mathcal{P}_1)},\ldots,\mathcal{A}_{(k_m,\mathcal{P}_m)})$ the entropy of the share given to any participant $P\in\cap_{i=1}^{m}\mathcal{P}_i$ satisfies*

$$H(P)\geq H(S_1S_2\ldots S_{\ell+1}).$$

Remark. *If in the previous corollary an integer $\ell<m$ such that $|\cap_{i=1}^{m}\mathcal{P}_i|<k_\ell$ does not exist, then it can be easily proved that for any participant $P\in\cap_{i=1}^{m}\mathcal{P}_i$ the entropy of the share given to P satisfies $H(P)\geq H(S_1S_2\ldots S_m)$.*

Corollary 13. *Let $(\mathcal{A}_{(k_1,\mathcal{P}_1)},\mathcal{A}_{(k_2,\mathcal{P}_2)},\mathcal{A}_{(k_3,\mathcal{P}_3)})$ be an m-tuple of threshold structures on a set of participants $\mathcal{P}=\cup_{i=1}^{3}\mathcal{P}_i$. Suppose $\cap_{i=1}^{3}\mathcal{P}_i\neq\emptyset$. Then, in any multi-secret sharing scheme for $(\mathcal{A}_{(k_1,\mathcal{P}_1)},\mathcal{A}_{(k_2,\mathcal{P}_2)},\mathcal{A}_{(k_3,\mathcal{P}_3)})$ the entropy of the share given to any participant $P\in\cap_{i=1}^{3}\mathcal{P}_i$ satisfies*

$$H(P)\geq H(S_1S_2S_3).$$

Before to state a general theorem on a multi-threshold structure we need the following two lemmas. They hold for any multi-secret sharing scheme of Type A not just for the case of multi-threshold structures. These two lemmas are the generalization to multi-secret sharing schemes of the ones proved in [6] for the case of single secret sharing.

Lemma 14. *Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. Let $X, Y \subseteq \mathcal{P}$ such that $Y \notin \mathcal{A}_i$ and $X \cup Y \in \mathcal{A}_i$. Then, in any multi-secret sharing scheme, it holds $H(X|Y) = H(S_i) + H(X|YS_i)$.*

An immediate consequence of Lemma 14 is that for any $P \in \cup_{A \in \mathcal{A}_i} A$ it holds $H(P) \geq H(S_i)$. We will see that under some condition this bound can be improved when the m-tuple of access structures consists of threshold structures.

Next lemma proves that the uncertainty on shares of a non-qualified set of participants cannot be decreased by the knowledge of the secret.

Lemma 15. *Let $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$ be an m-tuple of access structures on the set of participants $\mathcal{P}$. Let $X, Y \subseteq \mathcal{P}$ such that $X, Y \notin \mathcal{A}_i$ Then, in any multi-secret sharing scheme for $(\mathcal{A}_1, \ldots, \mathcal{A}_m)$, it holds $H(X|Y) = H(X|YS_i)$.*

The following theorem states a lower bound on the size of the share held by any participant in an m-tuple of threshold structures. In the following we will show that if the secrets are uniformly chosen, then the bound is tight.

Theorem 16. *Let $\mathcal{A}_{(k_1,\mathcal{P})}, \ldots, \mathcal{A}_{(k_m,\mathcal{P})}$ be threshold structures on a set of participants $\mathcal{P}$. In any multi-secret sharing scheme for $(\mathcal{A}_{(k_1,\mathcal{P})}, \ldots, \mathcal{A}_{(k_m,\mathcal{P})})$ the entropy of the share given to any participant $P \in \mathcal{P}$ satisfies*

$$H(P) \geq \sum_{i=1}^{m} H(S_i).$$

If each secret s_i is uniformly chosen in $S_i = GF(q_i)$, with q_i prime, then it is possible to realize a multi-secret sharing scheme that meets the bound of Theorem 16. To accomplish this it is enough to combine m independent threshold schemes, say Shamir's schemes [16], one for each threshold structure. In the same way we can construct an optimal multi-secret sharing sheme for the m-tuple of threshold structures $(\mathcal{A}_{(k,\mathcal{P}_1)}, \ldots, \mathcal{A}_{(k,\mathcal{P}_m)})$ considered in Corollary 11.

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. M. Ben-Or, S. Goldwasser, and A. Wigderson, *Completeness Theorems for Non-Cryptographic Fault–Tolerant Distributed Computation*, Proceedings of 20th Annual ACM Symposium on Theory of Computing, pp. 1–10, 1988.
3. G. R. Blakley, *Safeguarding Cryptographic Keys,* Proceedings AFIPS 1979 National Computer Conference, 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", E. Brickell Ed., "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, and U. Vaccaro, *Efficient Sharing of Many Secrets*, in "Proceedings of STACS '93 (10*th* Symp. on Theoretical Aspects of Computer Science)", P. Enjalbert, A. Finkel, K. W. Wagner Eds., "Lecture Notes in Computer Science", Vol. **665**, Springer–Verlag, Berlin, pp. 692–703, 1993.
6. 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**, pp. 57–167, 1993.
7. I. Csiszár and J. Körner, *Information Theory. Coding Theorems for Discrete Memoryless Systems*, Academic Press, 1981.
8. M. Franklin and M. Yung, *Communication Complexity of Secure Computation*, Proceedings of 24th Annual ACM Symposium on Theory of Computing", pp. 699–710, 1992.
9. R. G. Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, New York, NY, 1968.
10. O. Goldreich, S. Micali, and A. Wigderson, *How to Play any Mental Game*, Proceedings of 19th ACM Symposium on Theory of Computing, pp. 218–229, 1987.
11. 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.
12. W.-A. Jackson, K. M. Martin, and C. M. O'Keefe, *Multisecret Threshold Schemes*, in "Advances in Cryptology - CRYPTO '93", D.R. Stinson Ed., "Lecture Notes in Computer Science", Vol. **773**, Springer-Verlag, Berlin, pp. 126–135, 1994.
13. W.-A. Jackson, K. M. Martin, and C. M. O'Keefe, *A Construction for Multisecret Threshold Schemes*, Preprint, 1994.
14. E. D. Karnin, J. W. Greene, and M. E. Hellman, *On Secret Sharing Systems*, IEEE Trans. on Inform. Theory, Vol. IT-29, no. 1, pp. 35–41, Jan. 1983.
15. S. C. Kothari, *Generalized Linear Threshold Schemes*, in "Advances in Cryptology - CRYPTO '84", G. R. Blakley, D. Chaum Eds., "Lecture Notes in Computer Science", Vol. **196**, Springer-Verlag, Berlin, pp. 231–241, 1985.
16. A. Shamir, *How to Share a Secret*, Communications of the ACM, Vol. **22**, n. 11, pp. 612–613, Nov. 1979.
17. G. J. Simmons, *An Introduction to Shared Secret and/or Shared Control Schemes and Their Application*, Contemporary Cryptology, IEEE Press, pp. 441–497, 1991.
18. D. R. Stinson, *An Explication of Secret Sharing Schemes*, Design, Codes and Cryptography, Vol. **2**, pp. 357–390, 1992.