A Linear Algebraic Approach to Metering Schemes*

Carlo Blundo[1], Sebastià Martín[2], Barbara Masucci[1], and Carles Padró[2]

[1] Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84081 Baronissi (SA), Italy
e-mail: {`carblu, masucci`}`@dia.unisa.it`

[2] Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya, Barcelona, Spain
e-mail: {`sebasm,matcpl`}`@mat.upc.es`

October 26, 2001

Abstract

A *metering scheme* is a method by which an audit agency is able to measure the interaction between servers and clients during a certain number of time frames. Naor and Pinkas [21] proposed metering schemes where any server is able to compute a *proof*, i.e., a value to be shown to the audit agency at the end of each time frame, if and only if it has been visited by a number of clients larger than or equal to some threshold h during the time frame. The authors of [19] showed how to construct a metering scheme realizing any access structure, where the access structure is the family of all subsets of clients which enable a server to compute its proof. They also provided lower bounds on the communication complexity of metering schemes.

In this paper we describe a linear algebraic approach to design metering schemes realizing any access structure. Namely, given any access structure, we present a method to construct a metering scheme realizing it from any linear secret sharing scheme with the same access structure. Besides, we prove some properties about the relationship between metering schemes and secret sharing schemes. These properties provide some new bounds on the information distributed to clients and servers in a metering scheme. According to these bounds, the optimality of the metering schemes obtained by our method relies upon the optimality of the linear secret sharing schemes for the given access structure.

Keywords: Distributed Audit, Metering, Secret Sharing, Cryptography, Entropy.

1 Introduction

The current trend on the Internet suggests that the majority of revenues of web sites come from the advertising potential of the World Wide Web. Like in every other advertising channel, web advertisers must have a way to measure the exposure of their ads by obtaining usage statistics about web sites which contain their ads. Indeed, the amount of money charged to display ads depends on the number of visits received by the web sites. Consequently, advertisers should prevent the web sites from inflating the count of their visits in order to demand more money.

*An extended abstract of a preliminary version of this paper can be found in [7].

A *metering scheme* is a method to measure the interaction between servers and clients over a network. In particular, we consider a scenario where there are many servers and clients, and an audit agency whose task is to count the number of clients which have been served by each server during a certain number of time frames. Even though metering originated in the field of web advertisements, there are several other applications of secure metering schemes. For example, Franklin and Malkhi [13] suggested metering schemes as a method to measure the amount of money that companies, willing to pay for the cost required to access their web sites, should pay to the users' ISPs. Naor and Pinkas [21] considered a different scenario, in which a newspaper distributes coupons to its clients, which give them access to an online service. They suggested the use of metering schemes to provide verifiable measurements of the exact number of users who have used these coupons.

Metering schemes were first described by Naor and Pinkas [21]. They analyzed metering schemes where any server which has been visited by any set of h or more clients in a time frame, where h is a parameter of the scheme, is able to compute a *proof* [1], whereas, any server receiving visits from less than h clients in a time frame has absolutely no information about its proof for that time frame. These schemes are called *threshold metering schemes.*

The authors of [19] considered a more general situation. They showed how to construct a metering scheme realizing any access structure, where the access structure is the family of all subsets of clients, called *qualified sets*, which enable a server to compute its proof (i.e., if a server receives visits from all clients belonging to some qualified set, then it can compute the *proof*). Metering schemes involve distributing information to clients and servers. The clients participating in the metering process receive some information from the audit agency and such information is used to compute the information passed to the servers when visiting them. Since such information distribution affects the overall communication complexity, a major goal is to construct metering schemes whose overhead to the overall communication is as small as possible. Thus, the problem of establishing bounds on the size of the information distributed to the parties has been addressed in several papers (see [4, 5, 12, 19, 20, 7]). A metering scheme is said to be *ideal* if the information distributed to clients and servers is the minimum possible. Any access structure for which there exists an ideal metering scheme realizing it is called an *ideal access structure.* The authors of [8] showed how to construct a metering scheme realizing any ideal access structure. The construction is based on the Brickell vector space construction for secret sharing schemes [9].

In this paper we describe a linear algebraic approach to design metering schemes realizing any access structure. Namely, given any access structure, we present a method to construct a metering scheme realizing it from any linear secret sharing scheme with the same access structure. Besides, we prove some properties about the relationship between metering schemes and secret sharing schemes. These properties provide some new bounds on the information distributed to clients and servers in a metering scheme. According to these bounds, the optimality of the metering schemes obtained by our method relies upon the optimality of the linear secret sharing schemes for the given access structure.

The paper is organized as follows: In Section 2 we review the model and notation used to describe metering schemes. In Section 3 we study the relationship between metering schemes and secret sharing schemes. This relationship enables us to derive new lower bounds on the communication complexity of metering schemes. In Section 4 we first review some concepts about linear secret sharing schemes; afterwards, we present a linear algebraic approach to design metering schemes. This approach will enable us to construct a metering scheme realizing an access structure from any linear secret sharing scheme realizing the same access structure.

[1] In metering schemes, a *proof* is a value that the server can compute at the end of each time frame if and only if it has been visited by a fixed number of clients. Such a value, at the end of each time frame, is sent to the audit agency.

2 Metering Schemes for General Access Structures

A *metering scheme* consists of n clients, say $\mathcal{C}_1, \ldots, \mathcal{C}_n$, m servers, say $\mathcal{S}_1, \ldots, \mathcal{S}_m$, and an audit agency $\mathcal{A}$ whose task is to measure the interaction between the clients and the servers in order to count the number of client visits that any server receives. We assume that the scheme is active for τ time frames and that the audit agency is interested in the number of clients which visit each server during any time frame $t = 1, \ldots, \tau$. Let $\mathcal{C} = \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$ be the set of clients. An *access structure* on $\mathcal{C}$ is a set $\Gamma \subseteq 2^{\mathcal{C}}$ of subsets of clients. The subsets in Γ are called *qualified subsets.* A metering scheme realizes the access structure Γ if any server which has been visited by at least a qualified subset of clients in Γ during a time frame is able to provide the audit agency with a proof for the visits it has received. The access structure that we consider in this paper are *monotone*, i.e., they satisfy the following property: if $\mathcal{X} \in \Gamma$ and $\mathcal{X} \subseteq \mathcal{Y} \subseteq \mathcal{C}$, then $\mathcal{Y} \in \Gamma$. Indeed, if a server receives visits by a subset $\mathcal{Y}$ of clients which contains a qualified subset $\mathcal{X}$, then it can reconstruct its proof by ignoring the information provided by clients in $\mathcal{Y} \setminus \mathcal{X}$.

In the following we recall the information theoretical model proposed in [19] for metering schemes realizing any access structure Γ. With a boldface capital letter, say $\mathbf{X}$, we denote a random variable taking value on a set, denoted with the corresponding capital letter X, according to some probability distribution $\{Pr_{\mathbf{X}}(x)\}_{x \in X}$. The values such a random variable can take are denoted with the corresponding lower letter. Given a random variable $\mathbf{X}$ we denote with $H(\mathbf{X})$ the *Shannon entropy* of $\{Pr_{\mathbf{X}}(x)\}_{x \in X}$. For a complete treatment of the concepts of Information Theory, the reader is advised to consult [11].

There is an *initialization phase*, in which the audit agency provides each client with some information about the server's proofs. For any $i = 1, \ldots, n$, we denote by $\mathbf{C}_i$ the random variable associated to the information that the audit agency $\mathcal{A}$ gives to the client $\mathcal{C}_i$. During a *regular operation*, a client uses the information received in the initialization phase to compute the information passed to servers when visiting them. For any $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$, we denote by $\mathbf{C}_{i,j}^t$ the random variable associated to the information that the client $\mathcal{C}_i$ sends to the server $\mathcal{S}_j$ when visiting it in time frame t. During the *proof computation phase*, servers compute the proofs to be sent to the audit agency. For any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, we denote by $\mathbf{P}_j^t$ the random variable associated to the proof computed by the server $\mathcal{S}_j$ when it has been visited by a qualified set of clients in time frame t. Given any set of clients $\mathcal{X}$ we denote by $\mathbf{X}_j^t$ the random variable associated to the information that clients in $\mathcal{X}$ send to the server $\mathcal{S}_j$ when visiting it in time frame t.

We consider a scenario in which a certain number $s \leq m$ of servers can be *corrupt.* A corrupt server can be assisted by corrupt clients and other corrupt servers in computing its proof. At time frame t, a corrupt server gives to another corrupt server the information that it has received during time frames $1, \ldots, t$. For any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, we denote by $\mathbf{V}_j^{[t]}$ the random variable associated to the information known by a corrupt server $\mathcal{S}_j$ in time frames $1, \ldots, t$. Let $\mathcal{S}_{j_1}, \ldots, \mathcal{S}_{j_\beta}$ be a coalition of $1 \leq \beta \leq s$ corrupt servers and let $B = \{j_1, \ldots, j_\beta\}$. We denote by $\mathbf{P}_B^t$ the random variable associated to the proofs computed by servers having indices in B in time frame t. Similarly, we denote by $\mathbf{V}_B^{[t]}$ the random variable associated to the information known by the servers in B in time frames $1, \ldots, t$. Given a set of clients $\mathcal{X}$ and a set of server indices B, we denote by $\mathbf{X}_B^t$ the random variable associated to the information given by clients in $\mathcal{X}$ to servers having indices in B in time frame t.

Corrupt servers can also be assisted by corrupt clients in computing their proofs. A corrupt client can donate to any corrupt server the whole information received by the audit agency during the initialization phase. A metering scheme realizing an access structure Γ is defined as follows.

Definition 2.1 *An (n, m, τ, c, s) metering scheme realizing the access structure Γ is a protocol to measure the interaction between n clients $\mathcal{C}_1, \ldots, \mathcal{C}_n$ and m server $\mathcal{S}_1, \ldots, \mathcal{S}_m$ during τ time frames in such a way that the following properties are satisfied:*

1. *For any time frame t any client is able to compute the information needed to visit any server:*
   Formally, for any $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$, it holds that
   $$H(\mathbf{C}^t_{i,j}|\mathbf{C}_i) = 0.$$

2. *For any time frame $t = 1, \ldots, \tau$, any server which has been visited by a qualified subset of clients in time frame t can compute its proof for t:*
   Formally, for any $j = 1, \ldots, m$, $t = 1, \ldots, \tau$ and any $X \in \Gamma$, it holds that
   $$H(\mathbf{P}^t_j|\mathbf{X}^t_j) = 0.$$

3. *Let $B \subseteq \{1, \ldots, m\}$, where $|B| = \beta \leq s$ be a set of indices of corrupt servers and let $\mathcal{D} \notin \Gamma$ be a coalition of corrupt clients. Assume that in some time frame t each corrupt server in the coalition has been visited by a subset of clients $\mathcal{X}$, where $\mathcal{D} \cup \mathcal{X} \notin \Gamma$. Then, the servers in the coalition have no information about their proofs for time frame t, even if they are helped by the corrupt clients in $\mathcal{D}$.*
   Formally, for any $B \subseteq \{1, \ldots, m\}$ where $|B| = \beta \leq s$, any $t = 1, \ldots, \tau$, and any $\mathcal{X} \cup \mathcal{D} \notin \Gamma$, it holds that
   $$H(\mathbf{P}^t_B|\mathbf{D}\mathbf{X}^t_B\mathbf{V}^{[t-1]}_B) = H(\mathbf{P}^t_B).$$

The authors of [19] proved several lower bounds on the communication complexity of metering schemes realizing monotone access structures. In particular, they proved that if the proofs for the servers are uniformly chosen in a finite field F then the size of the information that any client passes to any server during a visit is lower bounded by $\log |F|$, that is,

$$\log |C^t_{i,j}| \geq \log |F| \text{ for any } i = 1, \ldots, n,\ j = 1, \ldots, m, \text{ and } t = 1, \ldots, \tau. \tag{1}$$

Moreover, if also the proofs for the servers are statistically independent, then the size of the information distributed to any client during the initialization phase is lower bounded by $s\tau \log |F|$, that is

$$\log |C_i| \geq s\tau \log |F| \text{ for any } i = 1, \ldots, n. \tag{2}$$

3 Metering Schemes and Secret Sharing Schemes

In this section we study the relationship between metering schemes and secret sharing schemes. This relationship enables us to restate all the bounds on the information rates of secret sharing schemes realizing a given access structure, in order to new obtain lower bounds on the communication complexity of metering schemes realizing the same access structure. These lower bounds generalize (1) and (2) and do not depend only on the number s of corrupt servers and the number τ of time frames, but also on the information rate of the access structure realized by the metering scheme. In the following section we recall some basic concepts about secret sharing schemes. The survey by Stinson [26] contains an unified description of results in the area of secret sharing schemes.

3.1 Secret Sharing Schemes

A *secret sharing scheme* is a method by which a dealer shares a secret among a set $\mathcal{C}$ of parties, by distributing some information to each party, in such a way that only qualified subsets of parties, pooling together their information, can reconstruct the secret; but subsets of parties that are not enabled to recover the secret have absolutely no information about it. Secret sharing schemes were introduced by Shamir [23] and Blakley [3]. They analyzed the case when only subsets of $\mathcal{C}$ of cardinality at least h, for a fixed integer $h \le |\mathcal{C}|$, can reconstruct the secret. Subsequently, Ito, Saito, and Nishizeki [15] and Benaloh and Leichter [2] showed how to realize a secret sharing scheme realizing any monotone access structure.

Let $\mathcal{X} \subseteq \mathcal{C}$ be a set of parties. We denote by $\mathbf{X}$ the random variable associated to the information distributed by the dealer to parties in $\mathcal{X}$. Moreover, we denote by $\mathbf{P}$ the random variable associated to the secret to be shared. A secret sharing scheme is defined as follows:

Definition 3.1 *A secret sharing scheme realizing the access structure on $\mathcal{C}$ is a protocol to share a secret chosen in P among the parties in $\mathcal{C}$ in such a way that*

1. *Any qualified set of participant is able to compute the secret.*
   Formally, for any $\mathcal{X} \in \Gamma$, it holds that $H(\mathbf{P}|\mathbf{X}) = 0$.

2. *Any non-qualified set of participants has absolutely no information about the secret.*
   Formally, for any $\mathcal{X} \notin \Gamma$, it holds that $H(\mathbf{P}|\mathbf{X}) = H(\mathbf{P})$.

The efficiency of a secret sharing scheme is usually quantified by a measurement called the *information rate* of the scheme. Let Σ be a secret sharing scheme realizing an access structure Γ. The information rate $\rho(\Sigma, \Gamma, P)$ is defined as the ratio between the *size of the secret* and the *maximum size of the shares* given to the participants. Secret sharing schemes with information rate $\rho = 1$, which is the maximum possible value of this parameter, are called *ideal*. An access structure Γ on $\mathcal{C}$ is said to be *ideal* if there exists an ideal secret sharing scheme realizing it.

Given an access structure Γ on $\mathcal{C}$, we will denote by $\rho^*(\Gamma)$ the *optimal information rate* for a secret sharing scheme realizing the access structure Γ. More precisely, $\rho^*(\Gamma) = \sup \rho(\Sigma, \Gamma, P)$, where the supremum is taken over all possible sets of secrets P with $|P| \ge 2$ and all secret sharing schemes Σ realizing the access structure Γ.

3.2 New Lower Bounds on the Communication Complexity

Let us consider Properties 2. and 3. of Definition 2.1. From these properties it follows that a metering scheme realizing an access structure Γ can be seen as a secret sharing scheme realizing the access structure Γ with set of secrets P_j^t shared among the clients $\mathcal{C}_1, \ldots, \mathcal{C}_n$ for any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$. Indeed, from Property 2. of Definition 2.1, for any $j = 1, \ldots, m$, $t = 1, \ldots, \tau$, and any $\mathcal{X} \in \Gamma$, it holds that $H(\mathbf{P}_j^t|\mathbf{X}_j^t) = 0$, that is exactly the *reconstruction property* of the secret sharing scheme, i.e. Property 1. of Definition 3.1. Moreover, from Property 3. of Definition 2.1 we obtain

$$H(\mathbf{P}_j^t) = H(\mathbf{P}_j^t|\mathbf{D}\mathbf{X}_j^t\mathbf{V}_j^{[t-1]}) \le H(\mathbf{P}_j^t|\mathbf{X}_j^t) \le H(\mathbf{P}_j^t),$$

i.e., $H(\mathbf{P}_j^t|\mathbf{X}_j^t) = H(\mathbf{P}_j^t)$ for any $\mathcal{X} \notin \Gamma$, that is the *security property* of the secret sharing scheme, i.e., Property 2. of Definition 3.1.

This implies that all known results on secret sharing schemes can be adapted to metering schemes. In particular, we obtain a new lower bound on the size of the information distributed by clients to servers during their visits, as stated by the next theorem.

Theorem 3.2 *In any* (n, m, τ, c, s) *metering scheme realizing the access structure* Γ*, for any* $j = 1, \ldots, m$ *and* $t = 1, \ldots, \tau$ *it holds that*

$$\max_{i=1,\ldots,n} \log |C_{i,j}^t| \geq \frac{\log |P_j^t|}{\rho^*(\Gamma)}.$$

In a similar way we can obtain a lower bound on the size of the information distributed by the audit agency to each client during the initialization phase. Let S be the set of indices of the corrupt servers in a metering scheme. It is easy to see that a metering scheme realizing an access structure Γ can be seen as a secret sharing scheme realizing the access structure Γ with set of secrets $P_S^{[\tau]} = P_S^1 \times \cdots \times P_S^\tau$, shared among the clients $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Let $\mathcal{X} \in \Gamma$ and let $X_S^{[\tau]} = X_S^1 \times \cdots \times X_S^\tau$. From Property 2. of Definition 2.1, it holds that

$$H(\mathbf{P}_S^{[\tau]} | \mathbf{X}_S^{[\tau]}) \leq \sum_{j=1}^{s} \sum_{t=1}^{\tau} H(\mathbf{P}_j^t | \mathbf{X}_j^t) = 0,$$

that is, the *reconstruction property* of the secret sharing scheme.

Now, let $\mathcal{X} \notin \Gamma$. We have that

$$\begin{aligned} H(\mathbf{P}_S^{[\tau]} | \mathbf{X}_S^{[\tau]}) &= H(\mathbf{P}_S^1 \ldots \mathbf{P}_S^\tau | \mathbf{X}_S^{[\tau]}) \\ &= H(\mathbf{P}_S^1 | \mathbf{X}_S^{[\tau]}) + \sum_{t=2}^{\tau} H(\mathbf{P}_S^t | \mathbf{X}_S^{[\tau]} \mathbf{P}_S^1 \ldots \mathbf{P}_S^{t-1}). \end{aligned} \tag{3}$$

Moreover,

$$\begin{aligned} H(\mathbf{P}_S^t | \mathbf{X}_S^{[\tau]} \mathbf{P}_S^1 \ldots \mathbf{P}_S^{t-1}) &\geq H(\mathbf{P}_S^t | \mathbf{X}_S^{[\tau]} \mathbf{V}_S^{[t-1]}) \\ &\geq H(\mathbf{P}_S^t | \mathbf{X} \mathbf{V}_S^{[t-1]}) \\ &\geq H(\mathbf{P}_S^t | \mathbf{X} \mathbf{D}_B^t \mathbf{V}_S^{[t-1]}) \\ &= H(\mathbf{P}_S^t). \end{aligned} \tag{4}$$

Therefore, from (3) and (4) it follows that, for any $\mathcal{X} \notin \Gamma$,

$$H(\mathbf{P}_S^{[\tau]} | \mathbf{X}_S^{[\tau]}) = H(\mathbf{P}_S^{[\tau]})$$

and also the *security property* of the secret sharing scheme holds. Therefore, we obtain the following theorem, which establishes a lower bound on the size of the information distributed by the audit agency to the clients during the initialization phase.

Theorem 3.3 *In any* (n, m, τ, c, s) *metering scheme realizing the access structure* Γ *it holds that*

$$\max_{i=1,\ldots,n} \log |C_i| \geq \frac{\log |P_S^{[\tau]}|}{\rho^*(\Gamma)}.$$

4 Designing Metering Schemes from Linear Secret Sharing Schemes

In this section, we present a method to construct an (n, m, τ, c, s) metering scheme realizing an access structure Γ from any linear secret sharing scheme realizing the same access structure. The optimality of the metering scheme relies upon the optimality of the linear secret sharing scheme, that is, if we can find a linear secret sharing scheme with optimal information rate for the access structure Γ, we will be able to construct an optimal metering scheme realizing the access structure Γ.

4.1 Linear Secret Sharing Schemes

In this section we recall next some basic facts about linear secret sharing schemes. Let E be a vector space with finite dimension over the finite field $GF(q)$ and let $\mathcal{C} = \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$ be a set of participant. For any $\mathcal{C}_i \in \mathcal{C} \cup \{\mathcal{A}\}$, where $\mathcal{A} = \mathcal{C}_0 \notin \mathcal{C}$ is a special participant called *dealer*, let us consider a vector space E_i over $GF(q)$ and a surjective linear mapping $\pi_i : E \rightarrow E_i$. Let us suppose that these linear mappings verify that, for any $\mathcal{X} \subset \mathcal{C}$,

$$\bigcap_{\mathcal{C}_i \in \mathcal{X}} \ker \pi_i \subset \ker \pi_0 \quad \text{or} \quad \bigcap_{\mathcal{C}_i \in \mathcal{X}} \ker \pi_i + \ker \pi_0 = E.$$

This family of vector spaces and linear surjective mappings determines the access structure

$$\Gamma = \left\{ \mathcal{X} \subset \mathcal{C} \; : \; \bigcap_{\mathcal{C}_i \in \mathcal{X}} \ker \pi_i \subset \ker \pi_0 \right\}.$$

A secret sharing scheme with set of secrets $P = E_0$ and access structure Γ is defined as follows: for a secret value $p \in E_0$, a vector $v \in E$ such that $\pi_0(v) = p$ is chosen at random and any participant $\mathcal{C}_i \in \mathcal{C}$ receives the vector $a_i = \pi_i(v) \in E_i$ as its share.

The information rate of this scheme is $\rho = \dim E_0 / (\max_{1 \leq i \leq n} \dim E_i)$. Secret sharing schemes constructed in this way are called *linear secret sharing schemes* (LSSSs for short). In a LSSS, the secret is computed by a linear mapping from the shares of the participants in a qualified subset. That is, for every $\mathcal{X} = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_\ell}\} \in \Gamma$, there exists a linear mapping $\mathcal{M}_{\mathcal{X}} : E_{i_1} \times \cdots \times E_{i_\ell} \rightarrow E_0$ that enables the participants in $\mathcal{X}$ to compute the secret.

Linear secret sharing schemes were first introduced by Brickell [9], who considered only *ideal* linear schemes, i.e., with $\dim E_i = 1$, for any $\mathcal{C}_i \in \mathcal{C} \cup \{\mathcal{A}\}$. General linear secret sharing schemes were introduced by Simmons [24], Jackson and Martin [16] and Karchmer and Wigderson [18] under other names, such as *geometric secret sharing schemes* or*monotone span programs*.

In an ideal linear secret sharing scheme with $\dim E_0 = 1$, we can consider that the surjective linear mappings π_i are non-zero vectors in the dual space E^*. In that case, a subset $\mathcal{X} \subset \mathcal{C}$ is qualified if and only if the vector $\pi_0 \in E^*$ can be expressed as a linear combination of the vectors $\{\pi_i \,|\, \mathcal{C}_i \in \mathcal{X}\}$. The access structures that can be defined in this way are called *vector space access structures*. Threshold, multilevel, and compartmented access structures [9] are a particular case of vector space access structures. For example, if Γ is the (h, n)-threshold access structure, we can take $q > n$ a prime power and $x_i \in GF(q)$, for any $\mathcal{C}_i \in \mathcal{C}$, non-zero pairwise different elements and consider $E = GF(q)^h$, $\pi_0 = (1, 0, \ldots, 0) \in E^*$ and $\pi_i = (1, x_i, x_i^2, \ldots, x_i^{h-1}) \in E^*$ for any $i = 1, \ldots, n$. The ideal linear scheme we obtain in this way is in fact equivalent to the Shamir's threshold scheme [23].

Using the *monotone circuit construction* due to Ito, Saito and Nishizeki [14], Simmons, Jackson and Martin [25] proved that any access structure Γ can be realized by a linear secret sharing scheme. The main drawback of the LSSSs that are constructed by using the general method proposed in [25] is that their information rate is in general very small.

Nevertheless, using decomposition techniques, linear secret sharing schemes with much better information rate can be found for some access structures. Those techniques consist of decomposing the given access structure Γ into several substructures and combining secret sharing schemes on these substructures in order to obtain a secret sharing scheme for Γ. For instance, one of the most powerful decomposition techniques to construct secret sharing schemes with good information rate is the *λ-decomposition construction* due to Stinson [27]. A linear secret sharing scheme is obtained when combining linear schemes in a λ-decomposition construction.

4.2 The Scheme

In this section, we present a method to construct a metering scheme realizing an access structure Γ from any linear secret sharing scheme realizing the same access structure.

Let Γ be an access structure on the set of clients $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n\}$. Let s be the maximum number of corrupt servers and let τ be the number of time frames the scheme must be active. Let $\pi_i : E \to E_i$, where $i = 0, \ldots, n$, be surjective linear mappings defining a LSSS with access structure Γ and set of secrets $E_0 = GF(q)^r$. As we have mentioned in Section 3.1, for any $\mathcal{X} = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_\ell}\} \in \Gamma$, there exists a linear mapping $\mathcal{M}_{\mathcal{X}} : E_{i_1} \times \cdots \times E_{i_\ell} \to E_0$ that enables the clients in $\mathcal{X}$ to compute the secret.

Initialization Phase

- For any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, the audit agency $\mathcal{A}$ chooses (and makes public) the linear map $\Pi_j^t : GF(q)^{s\tau} \longrightarrow GF(q)$ defined by

  $$\Pi_j^t(y_1, \ldots, y_{s\tau}) = \sum_{k=1}^{s\tau} \lambda_{j,k}^t y_k,$$

  where $\lambda_{j,k}^t \in GF(q)$, for any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, in such a way that any set of $s\tau$ such linear maps Π_j^t the corresponding vectors in the dual space $(GF(q)^{s\tau})^*$ are linearly independent.

- For any linear map Π_j^t and for any $i = 0, 1, \ldots, n$, consider the linear map $\Pi_{i,j}^t : E_i^{s\tau} \longrightarrow E_i$ defined by

  $$\Pi_{i,j}^t(v_1, \ldots, v_{s\tau}) = \sum_{k=1}^{s\tau} \lambda_{j,k}^t v_k \in E_i.$$

- Next, $\mathcal{A}$ chooses a random matrix $M = (x_k^h)_{k=1,\ldots,s\tau,\ h=1,\ldots,r}$, with $s\tau$ rows and r columns, where $x_k^h \in GF(q)$, for any $k = 1, \ldots, s\tau$ and $h = 1, \ldots, r$.

- Afterwards, $\mathcal{A}$ distributes each row $c_{0,k} = (x_k^1, \ldots, x_k^r) \in E_0$ into shares, in such a way that each client $\mathcal{C}_i$ receives $s\tau$ shares:

  $$c_i = (c_{i,1}, \ldots, c_{i,s\tau}) \in E_i^{s\tau}.$$

  In this way, given a qualified set of clients $\mathcal{X} = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_\ell}\} \in \Gamma$, we have that the k-th row in M satisfies

  $$c_{0,k} = \mathcal{M}_{\mathcal{X}}(c_{i_1,k}, \ldots, c_{i_\ell,k}).$$

Regular Operation Phase

- When client $\mathcal{C}_i$ visits server $\mathcal{S}_j$ in time frame t, $\mathcal{C}_i$ computes

  $$c_{i,j}^t = \Pi_{i,j}^t(c_{i,1}, \ldots, c_{i,s\tau}) = \sum_{k=1}^{s\tau} \lambda_{j,k}^t c_{i,k} \in E_i$$

  and sends it to server $\mathcal{S}_j$.

Proof Generation Phase

- Let us suppose that clients in $\mathcal{X} = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_\ell}\} \in \Gamma$ have visited a server $\mathcal{S}_j$ in time frame t.
- Then, server $\mathcal{S}_j$ possesses $c^t_{i_1,j}, \ldots, c^t_{i_\ell,j}$ and has to compute the proof p^t_j, which is defined by $p^t_j = \Pi^t_{0,j}(c_0) = \sum_{k=1}^{s\tau} \lambda^t_{j,k} c_{0,k}$, where $c_0 = (c_{0,1}, \ldots, c_{0,s\tau})$.
- Let us see how server $\mathcal{S}_j$ can obtain p^t_j:

$$p^t_j = \sum_{k=1}^{s\tau} \lambda^t_{j,k} c_{0,k} = \sum_{k=1}^{s\tau} \lambda^t_{j,k} \mathcal{M}_{\mathcal{X}}(c_{i_1,k}, \ldots, c_{i_\ell,k}).$$

Since $\mathcal{M}_{\mathcal{X}}$ is linear,

$$p^t_j = \mathcal{M}_{\mathcal{X}}\left(\sum_{k=1}^{s\tau} \lambda^t_{j,k}(c_{i_1,k}, \ldots, c_{i_\ell,k})\right) = \mathcal{M}_{\mathcal{X}}\left(\sum_{k=1}^{s\tau} \lambda^t_{j,k} c_{i_1,k}, \ldots, \sum_{k=1}^{s\tau} \lambda^t_{j,k} c_{i_\ell,k}\right) = \mathcal{M}_{\mathcal{X}}(c^t_{i_1,j}, \ldots, c^t_{i_\ell,j}). \tag{5}$$

Since server $\mathcal{S}_j$ possesses $(c^t_{i_1,j}, \ldots, c^t_{i_\ell,j})$, it obtains the proof p^t_j.

4.2.1 Analysis of the Scheme

Now we prove that the above scheme is a metering scheme realizing the access structure Γ. We need to prove that the scheme satisfies Properties 1., 2, and 3. of Definition 2.1.

It is immediate to verify that the scheme satisfies Property 1 of Definition 2.1. Indeed, for any $i = 1, \ldots, n$, the information given by the audit agency to the client $\mathcal{C}_i$ consists of a vector $c_i = (c_{i,1}, \ldots, c_{i,s\tau}) \in E_i^{s\tau}$. For any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, the information given to the server $\mathcal{S}_j$ by client $\mathcal{C}_i$ during a visit in time frame t is obtained by computing $c^t_{i,j} = \Pi^t_{i,j}(c_{i,1}, \ldots, c_{i,s\tau}) \in E_i$. Hence, for any time frame t, each client can compute the piece to be given to any visited server.

It is also easy to verify that the scheme satisfies Property 2 of Definition 2.1. Let $\mathcal{X} = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_\ell}\} \in \Gamma$ be a qualified set of clients visiting a server $\mathcal{S}_j$ in time frame t. Then, $\mathcal{S}_j$ has the values $(c^t_{i_1,j}, \ldots, c^t_{i_\ell,j})$ and can compute the proof p^t_j as seen in Equation (5).

Finally, we prove that the scheme satisfies Property 3 of Definition 2.1. Instead of distinguishing between a set of corrupt clients $\mathcal{D}$ and a set $\mathcal{X}$, where $\mathcal{D} \cup \mathcal{X} \notin \Gamma$, of honest clients visiting the servers on time frame t, we can consider that the clients in $\mathcal{X}$ are also corrupt. That is, we simply consider a subset $\mathcal{D} \subset \mathcal{C}$, $\mathcal{D} \notin \Gamma$, of corrupt clients helping a coalition of s corrupt servers in computing their proofs for time frame τ. The total information known to the coalition of corrupt servers is constituted by the information collected in time frames $1, \ldots, \tau - 1$ and the information received in time frame τ. We consider the worst possible case, in which the corrupt servers have collected the maximum possible information in time frames $1, \ldots, \tau - 1$, that is, we assume that each server $\mathcal{S}_j$ in the coalition has been visited by all clients $\mathcal{C}_1, \ldots, \mathcal{C}_n$ in time frames $1, \ldots, \tau - 1$. Therefore, we have to prove that

$$H(\mathbf{P}^\tau_B | \mathbf{D}\mathbf{V}^{[\tau-1]}_B) = H(\mathbf{P}^\tau_B) \tag{6}$$

for any subset B of corrupt servers, with cardinality at most s. We need the following result.

Lemma 4.1 *Let E, E_0 and E_1 be vector spaces over a finite field $GF(q)$. Let us consider two linear mappings, $\varphi_0 : E \to E_0$ and $\varphi_1 : E \to E_1$, where φ_0 is surjective. Let us suppose that a vector $x \in E$ is chosen uniformly at random and let us consider the random variables $\mathbf{X}_0$ and $\mathbf{X}_1$ corresponding, respectively,to $x_0 = \varphi_0(x)$ and $x_1 = \varphi_1(x)$. Then,*

1. $H(\mathbf{X}_0|\mathbf{X}_1) = 0$ *if and only if* $\ker\varphi_1 \subset \ker\varphi_0$,

2. $H(\mathbf{X}_0|\mathbf{X}_1) = H(\mathbf{X}_0)$ *if and only if* $\ker\varphi_1 + \ker\varphi_0 = E$.

Proof. If we know the value of $x_1 = \varphi_1(x)$, then, we know that $x_0 \in \varphi_0(x') + \varphi_0(\ker\varphi_1)$, where $x' \in E$ is any vector with $\varphi_1(x') = x_1$. Besides, all values in $\varphi_0(x') + \varphi_0(\ker\varphi_1)$ are equiprobable.

Then, x_0 can be uniquely determined from x_1 if and only if $\varphi_0(\ker\varphi_1) = \{0\}$, that is, if and only if $\ker\varphi_1 \subset \ker\varphi_0$. The value of x_1 does not provide any information about the value of x_0 if and only if $\varphi_0(\ker\varphi_1) = E_0$. In any other case, the value of x_1 provides partial information about the value of x_0.

Finally, we have to prove that $\varphi_0(\ker\varphi_1) = E_0$ if and only if $\ker\varphi_1 + \ker\varphi_0 = E$. Let us suppose that $\varphi_0(\ker\varphi_1) = E_0$. Then, for any $x \in E$, there exists $y \in \ker\varphi_1$ such that $\varphi_0(x) = \varphi_0(y)$. Therefore, $x = y + (x - y)$, where $y \in \ker\varphi_1$ and $x - y \in \ker\varphi_0$. Reciprocally, if $\ker\varphi_1 + \ker\varphi_0 = E$, then $E_0 = \varphi_0(E) = \varphi_0(\ker\varphi_1 + \ker\varphi_0) = \varphi_0(\ker\varphi_1)$. ■

In order to prove Equation (6) by means of Lemma 4.1, we need to determine the linear maps φ_0 and φ_1 corresponding, respectively, to the random variables $\mathbf{P}_B^\tau$ and $\mathbf{DV}_B^{[\tau-1]}$. Let us observe that the information $c_i = (c_{i,1}, \ldots, c_{i,s\tau})$ held by each client $\mathcal{C}_i$ has been obtained from the LSSS defined by mappings $\pi_i : E \to E_i$, where $i = 0, \ldots, n$. Therefore,

$$c_i = (c_{i,1}, \ldots, c_{i,s\tau}) = (\pi_i(y_1), \ldots, \pi_i(y_{s\tau})),$$

where $y = (y_1, \ldots, y_{s\tau})$ is a random vector such that $\pi_0(y_k) = c_{0,k}$, for every $k = 1, \ldots, s\tau$.

On the other hand, we consider the linear map $\phi_j^t : E^{s\tau} \to E_0$ defined by $\phi_j^t(y) = \Pi_{0,j}^t(\pi_0(y_1), \ldots, \pi_0(y_{s\tau}))$. Then, for any corrupt server S_j, where $j \in B$ and any time frame $t \in \{1, \ldots, \tau - 1\}$,

$$p_j^t = \Pi_{0,j}^t(c_{0,1}, \ldots, c_{0,s\tau}) = \Pi_{0,j}^t(\pi_0(y_1), \ldots, \pi_0(y_{s\tau})) = \phi_j^t(y).$$

Therefore, the kernel of the linear map φ_1 associated to the random variable $\mathbf{DV}_B^{[\tau-1]}$ is

$$\ker\varphi_1 = \left(\bigcap_{i\in\mathcal{D}} \ker\overline{\pi_i}\right) \bigcap \left(\bigcap_{j\in B\,,\,t<\tau} \ker\phi_j^t\right),$$

where $\overline{\pi_i} : E^{s\tau} \to E_i^{s\tau}$ is the linear map defined by $\overline{\pi_i}(y_i) = (\pi_i(y_1), \ldots, \pi_i(y_{s\tau}))$.

Analogously, $p_j^\tau = \phi_j^\tau(y)$. Therefore, the kernel of the linear map φ_0 associated to the random variable $\mathbf{P}_B^\tau$ is

$$\ker\varphi_0 = \bigcap_{j\in B} \ker\phi_j^\tau.$$

At this point, we just have to prove that

$$\ker\varphi_0 + \ker\varphi_1 = E^{s\tau}.$$

Let $y = (y_1, \ldots, y_{s\tau})$ be any vector in $E^{s\tau}$. From the independence of maps $\{\Pi_{0,j}^t\}_{j\in B\,,\,t\le\tau}$, we have that

$$\bigcap_{j\in B\,,\,t<\tau} \ker\Pi_{0,j}^t + \bigcap_{j\in B} \ker\Pi_{0,j}^\tau = E_0.$$

Then,

$$(\pi_0(y_1), \ldots, \pi_0(y_{s\tau})) = (a_{0,1}, \ldots, a_{0,s\tau}) + (b_{0,1}, \ldots, b_{0,s\tau}),$$

where $\Pi^t_{0,j}(a_{0,1},\ldots,a_{0,s\tau})=0$, for any $j\in B$ and any $t<\tau$, and $\Pi^\tau_{0,j}(b_{0,1},\ldots,b_{0,s\tau})=0$, for any $j\in B$. Since $\mathcal{D}\notin\Gamma$, from the properties of the LSSS it holds that, for any $k=1,\ldots,s\tau$, there exists $z_k\in E$ such that $\pi_0(z_k)=a_{0,k}$ and $\pi_i(z_k)=0$, for any $\mathcal{C}_i\in\mathcal{D}$. Therefore,

$$(z_1,\ldots,z_{s\tau})\in\ker\varphi_1.$$

On the other hand, observe that

$$\Pi^\tau_{0,j}(\overline{\pi_0}(y_1-z_1,\ldots,y_{s\tau}-z_{s\tau}))=\Pi^\tau_{0,j}(b_{0,1},\ldots,b_{0,s\tau})=0.$$

Hence, $(w_1,\ldots,w_{s\tau})=(y_1,\ldots,y_{s\tau})-(z_1,\ldots,z_{s\tau})\in\ker\varphi_0$. Finally, we conclude that

$$(y_1,\ldots,y_{s\tau})=(w_1,\ldots,w_{s\tau})+(z_1,\ldots,z_{s\tau})\in\ker\varphi_0+\ker\varphi_1.$$

4.2.2 Efficiency of the Scheme

In this section we show that the scheme described in Section 4 meets the bounds of Theorems 3.2 and 3.3.

Let

$$\rho=\frac{\dim E_0}{\max_{1\le i\le n}\dim E_i}$$

be the information rate of the LSSS Σ. Let q (a power of a prime) be the cardinality of the finite field F_q. The amount of information that a client $\mathcal{C}_i\in\mathcal{C}$ receives by the audit agency during the initialization phase is $\log|C_i|=s\tau\log q\dim E_i$. Observe that

$$\begin{aligned}\max_{i=1,\ldots,n}\log|C_i| &= s\tau\log q\dim E_0\frac{\max_{i=1,\ldots,n}\dim E_i}{\dim E_0}\\ &= \frac{s\tau\log q\dim E_0}{\rho}\\ &= \frac{\log|P^{[\tau]}_S|}{\rho}.\end{aligned}$$

Therefore, the bound given in Theorem 3.3 is attained if Σ has optimal information rate, that is, if $\rho=\rho^*(\Sigma)$.

The amount of information that a client sends to a server during a visit is $\log|C^t_{i,j}|=\log q\dim E_i$. Observe that

$$\begin{aligned}\max_{i=1,\ldots,n}\log|C^t_{i,j}| &= \log q\dim E_0\frac{\max_{i=1,\ldots,n}\dim E_i}{\dim E_0}\\ &= \frac{\log|P^t_j|}{\rho}.\end{aligned}$$

Therefore, the bound given in Theorem 3.2 is attained if Σ has optimal information rate, that is, if $\rho=\rho^*(\Sigma)$.

5 Some Examples

Optimal metering schemes can be constructed for any access structure $\mathcal{A}$ such that a LSSS with optimal information rate is known for $\mathcal{A}$. For example, let us consider the access structure on a set

$\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4\}$ of 4 clients whose minimal authorized subsets are $\mathcal{A}_0 = \{\{\mathcal{C}_1, \mathcal{C}_2\}, \{\mathcal{C}_2, \mathcal{C}_3\}, \{\mathcal{C}_3, \mathcal{C}_4\}\}$. This access structure is well known in the literature concerning secret sharing schemes [10]. It has been proved in [10] that the information rate of any SSS for this access structure is at most $2/3$. Besides, there exists a linear secret sharing scheme Σ with information rate $\rho = 2/3$. That is, the optimal information rate of this access structure is $\rho^*(\mathcal{A}) = 2/3$ and there exists a LSSS for $\mathcal{A}$ with $\rho = \rho^*$. Therefore, we can construct a metering scheme realizing $\mathcal{A}$ and attaining the bounds showed in Section 3.

6 Conclusions

In this paper we have described a linear algebraic approach to design metering schemes realizing any access structure. Namely, we have presented a method to construct a metering scheme realizing any access structure, from any linear secret sharing scheme realizing the same access structure.

We have also proved some properties about the relationship between metering schemes and secret sharing schemes. These properties provide some new bounds on the information distributed to clients and servers in a metering scheme. According to these bounds, the optimality of the metering schemes obtained by our method relies upon the optimality of the linear secret sharing schemes for the given access structure.

Acknowledgements

This work was done while the third author was visiting the Departament de Matemàtica Aplicada IV at the Universitat Politècnica de Catalunya, Barcelona, Spain She would like to thank the Department for its hospitality.

The research of the first and the third author is partially supported by C.N.R. under grant CNRRG008BF3: "Pubblicità Online: Nuove Misure per Nuovi Media. Auditing e Accounting Sicuro sul WEB".

References

[1] A. Beimel, *Secure Schemes for Secret Sharing Schemes and Key Distribution*, PhD Thesis, Dept. of Computer Science, Technion, 1996. Available at `http://www.cs.bgu.ac.il/ beimel/pub.html`

[2] J. C. Benaloh and J. Leichter, *Generalized Secret Sharing and Monotone Functions*, in Proc. of CRYPTO '88, LNCS, Vol. 403, pp. 27–35, 1990.

[3] G.R. Blakley, *Safeguarding Cryptographic Keys*, in Proc. of AFIPS 1979 National Computer Conference, Vol. 48, pp. 313-317, 1979.

[4] C. Blundo, A. De Bonis, and B. Masucci, *Metering Schemes with Pricing*, in Proc. of DISC 2000, LNCS, Vol. 1914, pp. 194–208, 2000.

[5] C. Blundo, A. De Bonis, B. Masucci, and D. R. Stinson, *Dynamic Multi-Threshold Metering Schemes*, in Proc. of SAC 2000, LNCS, Vol. 2012, pp. 130–144, 2001.

[6] C. Blundo, A. De Santis, R. De Simone and U. Vaccaro, *Tigh bounds on the Information Rate of Secret Sharing Schemes*, Design, Codes and Cryptography, 11, 107-122, 1997.

[7] C. Blundo, S. Martin, B. Masucci, and C. Padró, *New Bounds on the Communication Complexity of Metering Schemes*, submitted for publication, 2001.

[8] C. Blundo and B. Masucci, *A Note on Ideal Metering Schemes*, submitted for publication, 2001.

[9] E. F. Brickell, *Some Ideal Secret Sharing Schemes*, The Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. **6**, pp. 105–113, 1989.

[10] R. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, *On the Size of the Shares in Secret Sharing Schemes*, Journal of Cryptology.

[11] T. M. Cover and J. A. Thomas, Elements of Information Theory. John Wiley & Sons, 1991.

[12] A. De Bonis and B. Masucci, *An Information Theoretic Approach to Metering Schemes*, in Proc. of ISIT 2000, IEEE International Symposium on Information Theory.

[13] M. Franklin and D. Malkhi, *Auditable Metering with Lightweight Security*, Journal of Computer Security, Vol. **6**, No. 4, pp. 237–255, 1998.

[14] M. Ito, A. Saito and T, Nishizeki, *Secret sharing scheme realizing any access structure*, in Proceedings of IEEE Globecom'87,pp. 99–102, 1987.

[15] M. Ito, A. Saito and T, Nishizeki, *Secret Sharing Schemes Realizing any Access Structure*, in Proc. of IEEE Globecom'87, pp. 99–102, 1987.

[16] W. Jackson and K. Martin, *Geometric Secret Sharing Schemes and Their Duals* Design, Codes, and Cryptography, No. **4**, pp. 83–95, 1994.

[17] M. Jakobsson, P. D. MacKenzie, and J. P. Stern, *Secure and Lightweight Advertising on the Web*, 8th International World Wide Web Conference, 1999.
Available at `http://www8.org/w8-papers/1a-electronic-market/secure/secure.html`

[18] M. Karchmer, A. Wigderson, *On Span Programs*, in Proc. of the 8th Annual IEEE Symposium on Structure in Complexity, pp. 102–111, 1993.

[19] B. Masucci and D. R. Stinson, *Metering Schemes for General Access Structures*, in Proc. of ESORICS 2000, LNCS, Vol. 1895, pp. 72–87, 2000.

[20] B. Masucci and D. R. Stinson, *Efficient Metering Schemes with Pricing*, IEEE Transactions on Information Theory, Vol. 47, No. 7, November 2001, to appear.

[21] M. Naor and B. Pinkas, *Secure and Efficient Metering*, in Proc. of EUROCRYPT '98, LNCS, Vol. 1403, pp. 576–590, 1998.

[22] M. Naor and B. Pinkas, *Secure Accounting and Auditing on the Web*, Computer Networks and ISDN Systems, Vol. **40**, Issues 1-7, pp. 541–550, 1998.

[23] A. Shamir, *How to Share a Secret*, Comm. of ACM, Vol. 22, No. 11, pp. 612–613, 1979.

[24] G.J. Simmons, *How to (Really) Share a Secret*, in Proceedings of CRYPTO 88, Lecture Notes in Computer Science, Vol. **403**, pp. 390–448, 1990.

[25] G.J. Simmons, W. Jackson and K. Martin, *The Geometry of Secret Sharing Schemes*, Bulletin of the ICA, Vol. **1**, pp. 71–88, 1991.

[26] D.R. Stinson, *An Explication of Secret Sharing Schemes*, Designs, Codes, and Cryptography, Vol. 2, pp. 357–390, 1992.

[27] D.R. Stinson, *Decomposition Constructions for Secret-Sharing Schemes*, IEEE Transactions on Information Theory, Vol. **40**, pp. 118–125, 1994.