Metering Schemes for General Access Structures

Barbara Masucci[1] and Douglas R. Stinson[2]

[1] Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy, masucci@dia.unisa.it
http://www.dia.unisa.it/~masucci
[2] Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada, dstinson@cacr.math.uwaterloo.ca
http://www.cacr.math.uwaterloo.ca/~dstinson

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 [9] considered schemes in which any server is able to construct a *proof* if and only if it has been visited by at least a number, say h, of clients in a given time frame. In this paper we construct metering schemes for more general access structures, which include *multilevel* and *compartmented* access structures. Metering schemes realizing these access structures have useful practical applications: for example, they can be used to measure the interaction of a web site with a specific audience which is of special interest. We also prove lower bounds on the communication complexity of metering schemes realizing general access structures.
Keywords: Distributed Audit, Metering, Security, Cryptography, Entropy.

1 Introduction

The growing popularity of the Internet is driving various applications, several of which are commercially oriented. One such commercial application is advertising. Most of the revenues of web sites come from advertisement payments. Access data are usually collected at web sites, which have control over the collecting process and stored data. Since the owners of the web sites can charge higher rates for advertisements by showing a higher number of visits, they have a strong economic incentive to inflate the number of visits. Consequently, web advertisers should prevent web sites displaying their ads from inflating the count of their visits. In a typical scenario there are many servers and clients, and an audit agency whose task is to measure the interaction between the servers and the clients.

Franklin and Malkhi [6] were the first to consider the metering problem in a rigourous theoretical approach. Their solutions offer only a "lightweight security" and cannot be applied if servers and clients have a strong commercial interest to falsify the metering results. Subsequently, Naor and Pinkas [9] proposed *metering schemes* in which a server is able to compute a proof for a certain time frame if and only if it has been visited by a number of clients larger than or equal

F. Cuppens et al. (Eds.): ESORICS 2000, LNCS 1895, pp. 72–87, 2000.

to some threshold h in that time frame. Recently, different kinds of metering schemes have been proposed. Metering schemes for ramp structures [1,5] have been introduced in order to reduce the overhead to the overall communication due to the metering process. Metering schemes with pricing [1,8], which allow to count the exact number of visits received by each server, and dynamic multi–threshold metering schemes [2], which are metering schemes in which there is a different threshold for any server and any time frame, have been introduced in order to have a more flexible payment system.

The measures considered in previous metering schemes are simple thresholds. In other words, these measures can distinguish between two cases: either the server has received at least a required number of visits or it has not. A more general situation is when we have a set Γ of subsets of clients, called an *access structure*, and the audit agency wants to verify if a server has received visits by at least a subset in Γ (the subsets in Γ are called *qualified subsets*).

In this paper we prove that it is possible to construct a metering scheme realizing any monotone access structure. Moreover, we provide lower bounds on the communication complexity of any metering scheme realizing a monotone access structure. Afterwards, we concentrate our attention on two particular kinds of access structures, *multilevel* and *compartmented* access structures. These access structures have useful practical applications. For example, metering schemes realizing these access structures can be used to measure the interaction of a web site with a specific audience which is of special interest. These schemes can be used, for example, by an editor of text books who pays a web site to host her advertisements and is interested in knowing how many professors visited the site.

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 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 has received. Metering schemes considered by Naor and Pinkas [9] are specified by a threshold h: the audit agency wants to count if in any time frame the number of visits received by servers is greater than or equal to h. A more general situation is when we have a set Γ of subsets of clients and the audit agency wants to verify if a server has received visits by at least a subset in Γ.

Let $\{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$ be the set of clients. An *access structure* on $\{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$ is a set $\Gamma = \{\mathcal{A}_1, \ldots, \mathcal{A}_\ell\}$ of subsets of clients, i.e., $\mathcal{A}_r \subseteq \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$ for $r = 1, \ldots, \ell$. The subsets in Γ are called *qualified subsets*. In a metering scheme realizing the access structure Γ any server which has been visited by at least a qualified subset of clients in Γ in 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 $\mathcal{A}_r \in \Gamma$ and $\mathcal{A}_r \subseteq \mathcal{A}_z \subseteq \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$, then $\mathcal{A}_z \in \Gamma$. Indeed, if a server receives visits by a subset $\mathcal{A}_z$ of clients which contains a qualified subset $\mathcal{A}_r$, then it can reconstruct its proof by ignoring the information provided by clients in $\mathcal{A}_z \setminus \mathcal{A}_r$.

The general form of a metering scheme is the following: There is an *initialization phase* in which the audit agency provides each client with some piece of information. For any $i = 1, \ldots, n$, we denote by c_i the information that the audit agency A gives to the client $\mathcal{C}_i$. Moreover, we denote by C_i the set of all possible values of c_i. Given a set of clients $\mathcal{A}_r = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_k}\} \subseteq \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$, where $i_1 < i_2 < \ldots < i_k$, we denote by A_r the cartesian product $C_{i_1} \times \cdots \times C_{i_k}$. A *regular operation* consists in a client visit to a server during a time frame. During such a visit the client gives to the visited server a piece of information which depends on its private information, on the identity of the server, and on the time frame. For any $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$, we denote by $c_{i,j}^t$ the information that the client $\mathcal{C}_i$ sends to the server $\mathcal{S}_j$ when visiting it in time frame t. Moreover, we denote by $C_{i,j}^t$ the set of all possible values of $c_{i,j}^t$. Let $B = \{1, \ldots, \beta\} \subseteq \{1, \ldots, s\}$ be a set of server indices. Given a set of clients $\mathcal{A}_r = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_k}\} \subseteq \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$, where $i_1 < i_2 < \ldots < i_k$, we denote by $A_{r,B}^t$ the cartesian product $C_{i_1,1}^t \times \cdots \times C_{i_k,1}^t \times \cdots \times C_{i_1,\beta}^t \times \cdots \times C_{i_k,\beta}^t$. At the end of any time frame t there is a *proof computation stage*. For any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, we denote by p_j^t the proof computed by the server $\mathcal{S}_j$ when it has been visited by at least a qualified set of clients in time frame t. Moreover, we denote by P_j^t the sets of all values that p_j^t can assume. Given a set of server indices $B = \{1, \ldots, \beta\} \subseteq \{1, \ldots, s\}$, we denote by P_B^t the cartesian product $P_1^t \times \cdots \times P_\beta^t$. Finally, there is a *proof verification stage* in which the audit agency A verifies the proofs received by servers. If the proof received from a server at the end of a time frame is correct, then A pays the server for its services.

We consider a scenario in which a certain number $c \leq n$ of clients and $s \leq m$ of servers can be *corrupt*. A corrupt server can be assisted by corrupt clients and other corrupt servers in computing its proof. Let $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_c}$ be the corrupt clients. We assume that any qualified subset of clients $\mathcal{A}_r \in \Gamma$ contains $c_r \leq c$ corrupt clients, that is, $|\mathcal{A}_r \cap \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_c}\}| = c_r < |\mathcal{A}_r|$, for any $r = 1, \ldots, \ell$. A corrupt client $\mathcal{C}_i$ can donate to a corrupt server the whole information received from the audit agency during the initialization phase. At time frame t, a corrupt server can donate 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 $V_j^{[t]}$ all the information known by a corrupt server $\mathcal{S}_j$ in time frames $1, \ldots, t$. We also define $V_j^{[0]} = \emptyset$.

In this paper with a boldface capital letter, say $\mathbf{X}$, we denote a random variable taking value on a set denoted by 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 by 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 some basic properties of entropy, consult the Appendix).

We formally define metering schemes for general access structures by using the entropy approach, as done in [1,5,8,2].

Definition 1. *A metering scheme realizing the access structure $\Gamma = \{\mathcal{A}_1, \ldots, \mathcal{A}_\ell\}$ is a method 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 in time frame t:*
   Formally, it holds that $H(\mathbf{C}_{i,j}^t | \mathbf{C}_i) = 0$ for $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$.
2. *For any time frame t, any server $\mathcal{S}_j$ which has been visited by a qualified subset of clients $\mathcal{A}_r \in \Gamma$ in time frame t can compute its proof for time frame t:*
   Formally, it holds that $H(\mathbf{P}_j^t | \mathbf{A}_{r,j}^t) = 0$, for $j = 1, \ldots, m$, $r = 1, \ldots, \ell$, and $t = 1, \ldots, \tau$.
3. *Let $\mathcal{S}_1, \ldots, \mathcal{S}_\beta$ be a coalition of $1 \leq \beta \leq s$ corrupt servers and let $B = \{1, \ldots, \beta\}$. Let $\mathcal{C}_1, \ldots, \mathcal{C}_\alpha$ be a coalition of $\alpha \leq c$ corrupt clients, where $|\{\mathcal{C}_1, \ldots, \mathcal{C}_\alpha\} \cap \mathcal{A}_r| = \alpha_r \leq c_r$, for any $r = 1, \ldots, \ell$. Assume that in some time frame t each server in the coalition has been visited by a set of clients $\mathcal{D} \subset \mathcal{A}_r$, where $|\mathcal{D}| < |\mathcal{A}_r| - \alpha_r$ for any $r = 1, \ldots, \ell$. Then, the servers in the coalition have no information on their proofs for time frame t:*
   Formally, it holds that $H(\mathbf{P}_B^t | \mathbf{C}_1 \ldots \mathbf{C}_\alpha \mathbf{D}_B^t \mathbf{V}_B^{[t-1]}) = H(\mathbf{P}_B^t)$.

Notice that Naor and Pinkas [9] considered metering schemes realizing the access structure $\Gamma = \{\mathcal{A} \subseteq \{\mathcal{C}_1, \ldots, \mathcal{C}_n\} : |\mathcal{A}| \geq h\}$. Such an access structure is called a *threshold access structure*.

2.1 Lower Bounds on the Communication Complexity

In this subsection we provide lower bounds on the communication complexity of metering schemes. In order to prove our results we will resort to the two following technical lemmas.

Lemma 2. *Let $\mathbf{X}$ and $\mathbf{Y}$ be two random variables such that $H(\mathbf{X}|\mathbf{Y}) = 0$. Then, for any two random variables $\mathbf{Z}$ and $\mathbf{W}$, it holds that $H(\mathbf{W}|\mathbf{XYZ}) = H(\mathbf{W}|\mathbf{YZ})$.*

Lemma 3. *Let $\mathbf{Y}$, $\mathbf{Z}$, and $\mathbf{W}$ be three random variables such that $H(\mathbf{W}|\mathbf{YZ}) = 0$ and $H(\mathbf{W}|\mathbf{Y}) = H(\mathbf{W})$. Then, it holds that $H(\mathbf{Z}|\mathbf{Y}) = H(\mathbf{W}) + H(\mathbf{Z}|\mathbf{YW})$.*

The next lemma immediately follows from Definition 1.

Lemma 4. *Let Γ be an access structure on $\{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$, let $\mathcal{X} = \{\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_k}\}$ be a set of $k \leq n$ clients, let $\mathcal{S}_1, \ldots \mathcal{S}_\beta$ be $\beta \leq m$ servers and let $B = \{1, \ldots, \beta\}$. Then, in any metering scheme realizing Γ it holds that*

$$H(\mathbf{X}_B^t | \mathbf{X}) = 0,$$

for any $t = 1, \ldots, \tau$.

Proof. We have that

$$\begin{aligned} H(\mathbf{X}_B^t|\mathbf{X}) &= H(\mathbf{C}_{i_1,B}^t \dots \mathbf{C}_{i_k,B}^t|\mathbf{C}_{i_1} \dots \mathbf{C}_{i_k}) \\ &\le \sum_{r=1}^{k}\sum_{j=1}^{\beta} H(\mathbf{C}_{i_r,j}^t|\mathbf{C}_{i_r}) \text{ (from (7) and (8) of Appendix)} \\ &= 0 \text{ (from Property 1 of Definition 1).} \end{aligned}$$

□

The next lemma will be a useful tool to prove a lower bound on the size of the information distributed to servers from clients during a visit.

Lemma 5. *Let Γ be an access structure on $\{\mathcal{C}_1, \dots, \mathcal{C}_n\}$, let $\mathcal{A}_r \in \Gamma$ be a qualified set, let $\mathcal{C}_i \in \mathcal{A}_r$, and let $\mathcal{E}_r = \mathcal{A}_r \setminus \{\mathcal{C}_i\}$. Let $\mathcal{S}_1, \dots \mathcal{S}_\beta$ be $\beta \le m$ servers and let $B = \{1, \dots, \beta\}$. Then, in any metering scheme realizing Γ it holds that*

$$H(\mathbf{C}_{i,B}^t|\mathbf{E}_{r,B}^t \mathbf{V}_B^{[t-1]}) \ge H(\mathbf{P}_B^t),$$

for any $t = 1, \dots, \tau$.

Proof. Let $\mathcal{C}_1, \dots, \mathcal{C}_\alpha$ be a coalition of $\alpha \le c$ corrupt clients other than $\mathcal{C}_i$, and let $\mathcal{D}_r \subset \mathcal{E}_r$ be a set of $|\mathcal{A}_r| - \alpha_r - 1$ clients such that $\mathcal{D}_r \cap \{\mathcal{C}_1, \dots, \mathcal{C}_\alpha\} = \emptyset$. Assume that $\{\mathcal{C}_1, \dots, \mathcal{C}_\alpha\} \cap \mathcal{A}_r = \{\mathcal{C}_1, \dots, \mathcal{C}_{\alpha_r}\}$. We have that

$$\begin{aligned} H(\mathbf{C}_{1,B}^t \dots \mathbf{C}_{\alpha,B}^t|\mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{C}_{i,B}^t \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]}) &\le H(\mathbf{C}_{1,B}^t \dots \mathbf{C}_{\alpha,B}^t|\mathbf{C}_1 \dots \mathbf{C}_\alpha) \\ &\quad \text{(from (8) of Appendix)} \\ &= 0 \text{ (from Lemma 4).} \end{aligned}$$

Applying Lemma 2 with $\mathbf{X} = \mathbf{C}_{1,B}^t \dots \mathbf{C}_{\alpha,B}^t$, $\mathbf{Y} = \mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{C}_{i,B}^t \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]}$, and $\mathbf{W} = \mathbf{P}_B^t$ we get

$$\begin{aligned} H(\mathbf{P}_B^t|\mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{C}_{i,B}^t \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]}) &= H(\mathbf{P}_B^t|\mathbf{C}_{1,B}^t \dots \mathbf{C}_{\alpha,B}^t \mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{C}_{i,B}^t \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]}) \\ &\le H(\mathbf{P}_B^t|\mathbf{C}_{1,B}^t \dots \mathbf{C}_{\alpha_r,B}^t \mathbf{C}_{i,B}^t \mathbf{D}_{r,B}^t) \\ &\quad \text{(from (8) of Appendix, since } \alpha_r \le \alpha) \\ &= 0. \end{aligned}$$

The last equality follows from Property 2 of Definition 1, since $\{\mathcal{C}_1, \dots, \mathcal{C}_{\alpha_r}\} \cup \{\mathcal{C}_i\} \cup \mathcal{D}_r = \mathcal{A}_r$. From Property 3 of Definition 1 we have that

$$H(\mathbf{P}_B^t|\mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]}) = H(\mathbf{P}_B^t).$$

Therefore, applying Lemma 3 with $\mathbf{Y} = \mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]}$, $\mathbf{Z} = \mathbf{C}_{i,B}^t$, and $\mathbf{W} = \mathbf{P}_B^t$, we get

$$\begin{aligned} H(\mathbf{C}_{i,B}^t|\mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]}) &= H(\mathbf{P}_B^t) + H(\mathbf{C}_{i,B}^t|\mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}_{r,B}^t \mathbf{V}_B^{[t-1]} \mathbf{P}_B^t) \\ &\ge H(\mathbf{P}_B^t) \text{ (from (5) of Appendix).} \end{aligned} \quad (1)$$

We have that

$$H(\mathbf{C}^t_{1,B} \dots \mathbf{C}^t_{\alpha,B} | \mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}^t_{r,B} \mathbf{V}^{[t-1]}_B) \le H(\mathbf{C}^t_{1,B} \dots \mathbf{C}^t_{\alpha,B} | \mathbf{C}_1 \dots \mathbf{C}_\alpha)$$
$$\text{(from (8) of Appendix)}$$
$$= 0 \text{ (from Lemma 4).}$$

Therefore, applying Lemma 2 with $\mathbf{X} = \mathbf{C}^t_{1,B} \dots \mathbf{C}^t_{\alpha,B}$, $\mathbf{Y} = \mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}^t_{r,B} \mathbf{V}^{[t-1]}_B$ and $\mathbf{W} = \mathbf{C}^t_{i,B}$, we get

$$\begin{aligned} H(\mathbf{C}^t_{i,B} | \mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}^t_{r,B} \mathbf{V}^{[t-1]}_B) &= H(\mathbf{C}^t_{i,B} | \mathbf{C}^t_{1,B} \dots \mathbf{C}^t_{\alpha,B} \mathbf{C}_1 \dots \mathbf{C}_\alpha \mathbf{D}^t_{r,B} \mathbf{V}^{[t-1]}_B) \\ &\le H(\mathbf{C}^t_{i,B} | \mathbf{C}^t_{1,B} \dots \mathbf{C}^t_{\alpha_r,B} \mathbf{D}^t_{r,B} \mathbf{V}^{[t-1]}_B) \\ &\quad \text{(from (8) of Appendix, since } \alpha_r \le \alpha) \\ &= H(\mathbf{C}^t_{i,B} | \mathbf{E}^t_{r,B} \mathbf{V}^{[t-1]}_B). \end{aligned} \tag{2}$$

The last equality holds since $\mathcal{E}_r = \mathcal{D}_r \cup \{\mathcal{C}_1, \dots, \mathcal{C}_{\alpha_r}\}$. Therefore, the lemma follows from inequalities (2) and (1). □

The next corollary provides a lower bound on the size of the information distributed to servers from clients during a visit.

Corollary 6. *Let Γ be an access structure on $\{\mathcal{C}_1, \dots, \mathcal{C}_n\}$. Then, in any metering scheme realizing Γ it holds that*

$$H(\mathbf{C}^t_{i,j}) \ge H(\mathbf{P}^t_j)$$

for any $i = 1, \dots, n$, $j = 1, \dots, m$, and $t = 1, \dots, \tau$.

If the proofs for the servers are uniformly chosen in a finite field F, i.e., $H(\mathbf{P}^t_j) = \log |F|$ for any $j = 1, \dots, m$ and $t = 1, \dots, \tau$, then from Corollary 6 and from (4) of Appendix it holds that $\log |C^t_{i,j}| \ge \log |F|$ for any $i = 1, \dots, n$, $j = 1, \dots, m$, and $t = 1, \dots, \tau$. In order to prove a lower bound on the size of the information distributed to clients we need the next lemma.

Lemma 7. *Let Γ be an access structure on $\{\mathcal{C}_1, \dots, \mathcal{C}_n\}$, let $\mathcal{X} \subseteq \{\mathcal{C}_1, \dots, \mathcal{C}_n\}$, let $\mathcal{S}_1 \dots, \mathcal{S}_\beta$ be a coalition of $\beta \le s$ corrupt servers and let $B = \{1, \dots, \beta\}$. Then, in any metering scheme realizing Γ it holds that*

$$H(\mathbf{X}) \ge \sum_{t=1}^{\tau} H(\mathbf{X}^t_B | \mathbf{V}^{[t-1]}_B).$$

Proof. We have that

$$H(\mathbf{X}^1_B \dots \mathbf{X}^\tau_B | \mathbf{X}) \le \sum_{t=1}^{\tau} H(\mathbf{X}^t_B | \mathbf{X}) \text{ (from (7) of Appendix)}$$
$$= 0 \text{ (from Lemma 4).}$$

Therefore, applying Lemma 3 with $\mathbf{Z} = \mathbf{X}$ and $\mathbf{W} = \mathbf{X}_B^1 \dots \mathbf{X}_B^\tau$ we get

$$\begin{aligned} H(\mathbf{X}) &= H(\mathbf{X}_B^1 \dots \mathbf{X}_B^\tau) + H(\mathbf{X}|\mathbf{X}_B^1 \dots \mathbf{X}_B^\tau) \\ &\geq H(\mathbf{X}_B^1 \dots \mathbf{X}_B^\tau) \text{ (from (5) of Appendix)} \\ &= H(\mathbf{X}_B^1) + \sum_{t=2}^{\tau} H(\mathbf{X}_B^t|\mathbf{X}_B^1 \dots \mathbf{X}_B^{t-1}) \text{ (from (6) of Appendix)} \\ &\geq \sum_{t=1}^{\tau} H(\mathbf{X}_B^t|\mathbf{V}_B^{[t-1]}). \end{aligned}$$

□

The next lemma provides a lower bound on the size of the information distributed to clients during the initialization phase in metering schemes.

Lemma 8. *Let Γ be an access structure on $\{\mathcal{C}_1, \dots, \mathcal{C}_n\}$. Let $\mathcal{S}_1 \dots, \mathcal{S}_\beta$ be a coalition of $\beta \leq s$ corrupt servers and let $B = \{1, \dots, \beta\}$. Then, in any metering scheme realizing Γ it holds that*

$$H(\mathbf{C}_i) \geq \sum_{t=1}^{\tau} H(\mathbf{P}_B^t)$$

for any $i = 1, \dots, n$

Proof. Let $\mathcal{A}_r \in \Gamma$, let $\mathcal{C}_i \in \mathcal{A}_r$ and let $\mathcal{E}_r = \mathcal{A}_r \setminus \{\mathcal{C}_i\}$. We have that

$$\begin{aligned} H(\mathbf{C}_i) &\geq \sum_{t=1}^{\tau} H(\mathbf{C}_{i,B}^t|\mathbf{V}_B^{[t-1]}) \text{ (from Lemma 7)} \\ &\geq \sum_{t=1}^{\tau} H(\mathbf{C}_{i,B}^t|\mathbf{E}_{r,B}^t \mathbf{V}_B^{[t-1]}) \text{ (from (8) of Appendix)} \\ &\geq \sum_{t=1}^{\tau} H(\mathbf{P}_B^t) \text{ (from Lemma 5).} \end{aligned}$$

□

If the proof sequences of the corrupt servers are statistically independent, then the next corollary holds. For the sake of simplicity we state this result for the simple case where $H(\mathbf{P}_{j_1}^{t_1}) = H(\mathbf{P}_{j_2}^{t_2})$ for all $j_1, j_2 \in \{1, \dots, m\}$ and $t_1, t_2 \in \{1, \dots, \tau\}$. We denote this common entropies by $H(\mathbf{P})$. However, our result apply to the general case of arbitrary entropies on the proofs.

Corollary 9. *Let Γ be an access structure on $\{\mathcal{C}_1, \dots, \mathcal{C}_n\}$. Let $\mathcal{S}_1 \dots, \mathcal{S}_s$ be a coalition of s corrupt servers. Then, in any metering scheme realizing Γ in which the sequences of the proofs of the servers $\mathcal{S}_1, \dots, \mathcal{S}_s$ are statistically independent, it holds that*

$$H(\mathbf{C}_i) \geq s\tau H(\mathbf{P})$$

for any $i = 1, \dots, n$.

If the random variable $\mathbf{P}$ is uniformly distributed in a finite field F, i.e., $H(\mathbf{P}) = \log|F|$, then from Corollary 9 and from (4) of Appendix it holds that $\log|C_i| \geq s\tau \log|F|$ for any $i = 1, \ldots, n$.

2.2 A Protocol for Metering Schemes Realizing General Access Structures

In this subsection we will show that for any monotone access structure it is possible to construct a metering scheme realizing it. The construction uses as building blocks threshold metering schemes proposed by Naor and Pinkas [9]. The proofs are points of a finite field $GF(q)$ where q is a sufficiently large prime number. Let $\Gamma = \{\mathcal{A}_1, \ldots, \mathcal{A}_\ell\}$ be a monotone access structure on $\{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$. We denote with "$\circ$" an operator mapping each pair (j, t), with $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, to an element of $GF(q)$ and having the property that no distinct two pairs (j, t) and (j', t') are mapped to the same element. The protocol is the following:

- **Initialization**:
  The audit agency A chooses a polynomial $P_1(x, y)$ over $GF(q)$, which is of degree $h_1 - 1$ in x and $s\tau - 1$ in y. For $r = 2, \ldots, \ell$, A chooses a polynomial $P_r(x, y)$ over $GF(q)$, which is of degree $h_r - 1$ in x and $s\tau - 1$ in y and such that $P_r(0, y) = P_1(0, y)$. Afterwards, for any $r = 1, \ldots, \ell$, A gives the polynomial $P_r(i, y)$ to each client $\mathcal{C}_i \in \mathcal{A}_r$.
- **Regular Operation for Time Frame** t:
  When a client $\mathcal{C}_i$ visits a server $\mathcal{S}_j$ during a time frame t it gives the values $P_r(i, j \circ t)$, for any $r \in \{1, \ldots, \ell\}$ such that $\mathcal{C}_i \in \mathcal{A}_r$, to $\mathcal{S}_j$.
- **Proof Generation and Verification**:
  If during a time frame t a server $\mathcal{S}_j$ has received visits from a qualified set $\mathcal{A}_r$, for some $r \in \{1, \ldots, \ell\}$, then it can interpolate the polynomial $P_r(x, j \circ t)$ and compute the proof $P_r(0, j \circ t)$. When the audit agency receives the value $P_r(0, j \circ t)$ it can easily verify if this is the correct proof for server $\mathcal{S}_j$.

Analysis of the Scheme. Now we prove that the proposed scheme is a metering scheme realizing the access structure Γ.

First, we prove that Property 1 of Definition 1 is satisfied. For any $i = 1, \ldots, n$, the information given by the audit agency to the client $\mathcal{C}_i$ consists of the univariate polynomials $P_r(i, y)$, for any $r \in \{1, \ldots, \ell\}$ such that $\mathcal{C}_i \in \mathcal{A}_r$. 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 evaluating the univariate polynomials $P_r(i, y)$ at $j \circ t$, for any $r \in \{1, \ldots, \ell\}$ such that $\mathcal{C}_i \in \mathcal{A}_r$. Hence, for any time frame t, each client can compute the piece to be given to any visited server.

Now, we prove that Property 2 of Definition 1 is satisfied. Let $\mathcal{A}_r \in \Gamma$ be a qualified subset of clients. Assume that during a time frame t a server $\mathcal{S}_j$ receives visits from all clients in $\mathcal{A}_r$. Since $|\mathcal{A}_r| = h_r$, then the server can interpolate the

polynomial $P_r(x, j \circ t)$. Afterwards, the server can compute its proof $P_r(0, j \circ t)$ for time frame t.

Finally, we prove that Property 3 of Definition 1 is satisfied. We consider the worst possible case, in which s corrupt servers and c corrupt clients decide to cooperate at time frame τ. Let $\mathcal{A}_r \in \Gamma$ be a qualified subset of clients and let c_r be the number of corrupt clients in $\mathcal{A}_r$. Assume that during time frame τ each corrupt server $\mathcal{S}_j$ in the coalition has received $g_{j,r} \leq h_r - c_r - 1$ regular visits from clients in the subset $\mathcal{A}_r \in \Gamma$. In order to compute its proof for time frame τ any server $\mathcal{S}_j$ should be able to interpolate either the univariate polynomial $P_r(x, j \circ \tau)$ or the bivariate polynomial $P_r(x, y)$ for some $r \in \{1, \ldots, \ell\}$. Therefore, we consider the two following cases:

Case 1. The server $\mathcal{S}_j$ tries to interpolate a polynomial $P_r(x, j \circ \tau)$, for some $r \in \{1, \ldots, \ell\}$.
Let $r \in \{1, \ldots, \ell\}$. Each corrupt client $\mathcal{C}_i$ in $\mathcal{A}_r$ donates the polynomial $P_r(i, y)$ to $\mathcal{S}_j$ from which $\mathcal{S}_j$ can compute the value $P_r(i, j \circ \tau)$. Since there are c_r corrupt clients in $\mathcal{A}_r$, $\mathcal{S}_j$ can compute c_r values of $P_r(x, j \circ \tau)$ in addition to those provided by the $g_{j,r}$ visits performed by non corrupt clients in $\mathcal{A}_r$. Consequently, the overall number of points of $P_r(x, j \circ \tau)$ known to $\mathcal{S}_j$ is less than or equal to $h_r - 1$. Therefore, $\mathcal{S}_j$ obtains a linear system of $h_r - 1$ equations in h_r unknowns. For any choice of a value in $GF(q)$, there is a univariate polynomial $Q_r(x, j \circ \tau)$ of degree $h_r - 1$, which is consistent with this value and with the information held by $\mathcal{S}_j$. Since there are q such polynomials, the probability of $\mathcal{S}_j$ in guessing its proof for time frame τ is at most $1/q$.

Case 2. The coalition of servers try to interpolate a polynomial $P_r(x, y)$ for some $r \in \{1, \ldots, \ell\}$.
We consider the worst possible case in which any corrupt server $\mathcal{S}_j$ in the coalition has collected the maximum possible information during the previous time frames $1, \ldots, \tau - 1$. In other words, for any time frame $t = 1, \ldots, \tau - 1$, the server $\mathcal{S}_j$ has been visited by at least a qualified set of clients, that is, there exists some index r, such that $\mathcal{S}_j$ has interpolated the polynomial $P_r(x, j \circ t)$. We consider the worst possible case in which the index r is the same for any time frame $t = 1, \ldots, \tau - 1$. This means that the information collected by each corrupt server $\mathcal{S}_j$ during the previous time frames is equivalent to the h_r coefficients of each polynomial $P_r(x, j \circ t)$, for any $t = 1, \ldots, \tau - 1$. The information that a corrupt client $\mathcal{C}_i$ donates to a corrupt server is equivalent to the $s\tau$ coefficients of the polynomial $P_r(i, y)$, for any $r \in \{1, \ldots, \ell\}$ such that $\mathcal{C}_i \in \mathcal{A}_r$. Then, the overall information on $P_r(x, y)$ held by the servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ consists of

$$c_r s\tau + s(\tau - 1)h_r + \sum_{j=1}^{s} g_{j,r} - c_r s(\tau - 1) \tag{3}$$

points. The first term of (3) is the information donated by the c_r corrupt clients in $\mathcal{A}_r$, the second term is the information collected by the

s corrupt servers during time frames $1, \ldots, \tau - 1$, the third term is the information provided by client visits at time frame τ, and the last term is the information which has been counted twice. Since $g_{j,r} \leq h_r - c_r - 1$ for $j = 1, \ldots, s$, then expression (3) is less than or equal to $h_r s\tau - s$. Therefore, the servers obtain a system of $h_r s\tau - s$ equations in $h_r s\tau$ unknowns. For any choice of s values in $GF(q)$, there is a bivariate polynomial $Q_r(x, y)$ of degree $h_r - 1$ in x and $s\tau - 1$ in y, which is consistent with these values and with the information held by the servers. Since there are q^s such polynomials, then the corrupt servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ have probability at most $1/q^s$ of guessing their proofs for time frame τ.

Efficiency of the Scheme. We now want to consider the efficiency of the scheme constructed in Subsection 2.2. For any client $\mathcal{C}_i$, let d_i be the number of sets $\mathcal{A} \in \Gamma$ such that $\mathcal{C}_i \in \mathcal{A}$. In the proposed scheme the information distributed to client $\mathcal{C}_i$ by the audit agency consists of $d_i s\tau$ points of $GF(q)$. The information given from client $\mathcal{C}_i$ to a server $\mathcal{S}_j$ during a visit in a time frame consists of d_i points of $GF(q)$.

If we construct a metering scheme realizing a threshold access structure Γ with threshold h by using the previous scheme, then the information distributed to each client by the audit agency consists in $\binom{n-1}{h-1} s\tau$ points of $GF(q)$, while the information distributed by any client to any server during a visit consists in $\binom{n-1}{h-1}$ points of $GF(q)$. This construction is very inefficient, compared to the construction proposed by Naor and Pinkas [9]. Indeed, in Naor and Pinkas' scheme the information distributed to each client by the audit agency consists only in $s\tau$ points of $GF(q)$, while the information distributed by any client to any server during a visit consists in a single point of $GF(q)$. Therefore, in general, the construction of Subsection 2.2 gives schemes which are not optimal with respect to the communication complexity.

3 Metering Schemes for Targeted Audience

In this section we concentrate our attention on two particular kinds of access structures, *multilevel access structures* and *compartmented access structures*. These access structures, introduced by Simmons in [11] and further investigated in [3] and [7], have useful practical applications. Metering schemes realizing these access structures can be used to measure the interaction of a web site with a specific audience which is of special interest. These schemes can be used, for example, by an editor of text books who pays a web site to host her advertisements and is interested in knowing how many professors visited the site.

3.1 Multilevel Access Structures

Consider the following situation: there are two disjoint classes, L_1 and L_2, where the clients in L_1 are professors and the ones in L_2 are PhD students. We require that a server containing information related to a research topic can reconstruct

its proof for a time frame t if it receives at least two visits from professors or three visits from PhD students in that time frame. Now, assume that the server is visited by one professor and two PhD students during a time frame t: then, it would be probably unacceptable that the server would be not able to reconstruct its proof for time frame t. In this situation what is needed is a metering scheme in which the information provided by clients in different classes is related. This means that the information provided by clients in a certain class should be useful not only when combined with information provided by clients in the same class, but also when combined with information provided by clients in all lower level classes.

In a *multilevel access structure* there are u disjoint classes of clients (also called *levels*), $L_1, \ldots, L_u$, where each class $L_r \subseteq \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$ is associated to a positive integer $h_r \leq n_r = |L_r|$, for $r = 1, \ldots, u$, and such that $h_1 < h_2 < \cdots < h_u$. A multilevel access structure consists of those subsets which contain at least h_r clients all of level *at most* L_r for some $r \in \{1, \ldots, u\}$. Therefore, in any metering scheme realizing a multilevel access structure, any server is able to compute its proof for a given time frame if and only if it has received at least h_r visits from clients of level *at most* L_r for some $r \in \{1, \ldots, u\}$ during that time frame. Of course, the audit agency must know the identities of all participants in order to set up a metering scheme for a multilevel access structure.

In a multilevel access structure the information provided by clients in a level L_z to servers during their visits should be more valuable than the information provided by clients in levels L_r, with $r > z$, in order to compute a proof. A trivial way to realize schemes with this property could be the following: the audit agency distributes more information to clients in high level classes. In this case the pieces distributed to clients in high level classes are more valuable because they contain more information about the servers' proofs. The disadvantage of this solution is that it penalizes clients in high level classes by requiring them to handle more information than clients in low level classes. Since we are interested in the efficiency of metering schemes, we would like to have schemes in which the size of the information distributed to clients is the same, even though the pieces provided to servers by some clients may be more effective in computing a proof than others.

A Protocol for Metering Schemes Realizing Multilevel Access Structures. In this subsection we will prove that for any multilevel access structure it is possible to construct a metering scheme realizing it. Let Γ be a multilevel access structure with u levels $L_1, \ldots, L_u$ and let $h_r \leq n_r = |L_r|$ be the threshold associated to level L_r, for any $r = 1, \ldots, u$. Let $h_1 < h_2 < \cdots < h_u$. The protocol is the following:

- **Initialization**: The audit agency A chooses a polynomial $P_u(x, y)$ over $GF(q)$, which has degree $h_u - 1$ in x and $s\tau - 1$ in y. Afterwards, for any $r = 1, \ldots, u-1$, A constructs the polynomial $P_r(x, y)$ of degree $h_r - 1$ in x and $s\tau - 1$ in y, by truncating the polynomial $P_u(x, y)$ at degree $h_r - 1$. For any $r = 1, \ldots, u$ and for any client $\mathcal{C}_i \in L_r$, A picks a value $x_i \in GF(q)$

and constructs the h_u-dimensional vector $v_i = (1, x_i, x_i^2, \ldots, x_i^{h_r-1}, 0, \ldots, 0)$, which is made public (we will explain later how A chooses the value x_i for any client $\mathcal{C}_i$). Afterwards, A gives the polynomial $P_r(x_i, y)$ to any client $\mathcal{C}_i \in L_r$.

- **Regular Operation for Time Frame** t:
  When a client $\mathcal{C}_i \in L_r$ visits a server $\mathcal{S}_j$ during a time frame t, it gives the value $P_r(x_i, j \circ t)$ to $\mathcal{S}_j$.
- **Proof Generation and Verification**:
  Let $r \in \{1, \ldots, u\}$ and let $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_{h_r}}$ be h_r clients of level *at most* L_r visiting a server $\mathcal{S}_j$ in time frame t. Suppose that there is no subset of this set of clients which contains h_z clients of level *at most* L_z, for any $1 \leq z < r$. Let M be the $h_r \times h_u$ matrix with rows $v_{i_1}, \ldots v_{i_{h_r}}$, where v_{i_k} is the h_u-dimensional vector corresponding to client $\mathcal{C}_{i_k}$, for $k = 1, \ldots, h_r$; let $b = (b_0, \ldots, b_{h_r-1})$ be the h_r-dimensional vector whose elements are the coefficients of the polynomial $P_r(x, j \circ t)$, and let d be the h_r-dimensional vector containing the visits from clients $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_{h_r}}$ to server $\mathcal{S}_j$ in time frame t. The server $\mathcal{S}_j$ obtains a system of h_r equations in h_r unknowns, whose matrix form is $Mb = d$. This system has a unique solution over $GF(q)$, constituted by the h_r coefficients $b_0, \ldots, b_{h_r-1}$ of the polynomial $P_r(x, j \circ t)$, if and only if the matrix M is nonsingular, i.e., if and only if the vectors $v_{i_1}, \ldots v_{i_{h_r}}$ are independent. In this case the server can compute all the coefficients $b_0, \ldots, b_{h_r-1}$ of the polynomial $P_r(x, j \circ t)$, and reconstruct its proof $P_r(0, j \circ t) = b_0$. When the audit agency receives the value $P_r(0, j \circ t)$, for some $r \in \{1, \ldots, u\}$, from server $\mathcal{S}_j$ then it can easily verify if this is the correct proof for server $\mathcal{S}_j$ in time frame t.

In the next lemma, following the line of Theorem 1 in [3], we prove that for any multilevel access structure there is a method for the audit agency to choose the x_i's in such a way that, for any $r \in \{1, \ldots, u\}$, any h_r vectors corresponding to clients of level *at most* L_r are independent.

Lemma 10. *Let Γ be a multilevel access structure with u levels $L_1, \ldots, L_u$ and let $h_r \leq n_r = |L_r|$ be the threshold associated to level L_r, for any $r = 1, \ldots, u$. Let $h_1 < h_2 < \cdots < h_u$. Let $n = \sum_{r=1}^{u} n_r$ be the total number of clients. If $q > (h_u - 1)\binom{n}{h_u - 1}$ then it is possible to choose the values $x_1, \ldots, x_n$ associated to the clients $\mathcal{C}_1, \ldots, \mathcal{C}_n$ in such a way that for any $r \in \{1, \ldots, u\}$, any h_r vectors corresponding to clients of level* at most *L_r are independent.*

Proof. Let v_0 be the h_u dimensional vector $(1, 0, \ldots, 0)$. Let $\mathcal{C}_1 \in L_z$, for some $z \in \{1, \ldots, u\}$. The audit agency chooses the value $x_1 \in GF(q)$ in such a way that the h_u dimensional vectors $v_1 = (1, x_1, x_1^2, \ldots, x_1^{h_z-1}, 0, \ldots, 0)$ and v_0 are independent.

Suppose the audit agency has chosen the value x_i for any client $\mathcal{C}_i$ with $1 \leq i < k \leq n$, and let $\mathcal{C}_k \in L_r$ for some $r \in \{1, \ldots, u\}$. Let Ω_k be the set of subspaces spanned by some subset of size $h_r - 1$ of the k vectors $v_0, \ldots, v_{k-1}$. It is easy to see that $|\Omega| < \binom{k}{h_r - 1}$. Then, the audit agency A picks the value x_k in $GF(q)$ in

such a way that the h_u dimensional vector $v_k = (1, x_k, x_k^2, \ldots, x_k^{h_r-1}, 0, \ldots, 0)$ is not in any of the subspaces in Ω_k. To see that this is possible, let $R \in \Omega_k$, and let $w = (w_0, w_1, \ldots, w_{h_r-1}, 0 \ldots, 0)$ be a normal vector to R. Then the equation $\sum_{i=0}^{h_r-1} w_i x^i = 0$ has at most $h_r - 1$ solutions over $GF(q)$.

Since there exist at least h_r clients of level L_r, for any $r = 1, \ldots, u$, it follows that we need $q > (h_u - 1)\binom{n}{h_u-1}$ in order to be able to choose the x_i's as explained above. Now, consider a set of h_r vectors corresponding to h_r clients of level *at most* L_r and suppose that there is no subset of this set which contains z participants of level *at most* L_z, for any $z < r$. Then, by construction, the h_r vectors are independent. □

It is easy to see that the proposed scheme is a metering scheme realizing the multilevel access structure Γ. Indeed, following the line of Subsection 2.2 we can prove that Properties 1, 2, and 3 of Definition 1 are satisfied.

Efficiency of the Scheme. In the proposed scheme the information distributed to any client $\mathcal{C}_i$ by the audit agency consists of $s\tau$ points of $GF(q)$. The information given from client $\mathcal{C}_i$ to any server $\mathcal{S}_j$ during a visit consists of a single point of $GF(q)$. It is easy to see that the scheme of Subsection 3.1 meets the bounds of Corollary 6 and Lemma 8, and hence it is optimal with respect to the communication complexity.

One other issue to consider is the amount of computation needed for the audit agency to set up a metering scheme realizing a multilevel access structure. The problem of the scheme we have presented is that it requires the audit agency to do many checks to be sure that the points x_i's are in the right positions (i.e., that the vectors associated to any set of h_r clients all of level *at most* L_r are independent). Brickell [3] has proposed different ways to choose the x_i's which do not require such checking. It is easy to modify our metering scheme, since we only need to modify the initialization phase according to the constructions proposed by Brickell [3]. These constructions involve irreducible polynomials over $GF(q^\gamma)$, where $\gamma = uh_u^2$ and q is a prime such that $q > |L_r| + 1$ for any $r = 1, \ldots, u$. In particular, Brickell proved that the x_i's can be constructed in time polynomial in $(|L_1|, \ldots, |L_u|, q)$.

3.2 Compartmented Access Structures

Consider the following situation: there are two disjoint compartments, L_1 and L_2, where the clients in L_1 are professors and the ones in L_2 are PhD students. We require that a server containing information related to a research topic can reconstruct its proof for a time frame t if it receives at least two visits from professors *and* three visits from PhD students in that time frame. Now, assume that the server is visited by one professor during a time frame t. Then, no matter how many PhD students concur, the reconstruction of the proof for a server should be inhibited unless it receives at least a visit from another professor.

In a *compartmented access structure* there are u disjoint classes of clients (also called *compartments*), $G_1, \ldots, G_u$, where each class $G_r \subseteq \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$ is

associated to a positive integer $h_r \leq n_r = |G_r|$, for $r = 1, \ldots, u$. The compartmented access structure consists of those subsets which contain at least h_r clients from compartment G_r, *for any* $1 \leq r \leq u$. Therefore, in any metering scheme realizing a compartmented access structure, any server $\mathcal{S}_j$ is able to compute its proof for a given time frame if and only if it has received at least h_r visits from clients in compartment G_r, *for any* $1 \leq r \leq u$, during that time frame.

A Protocol for Compartmented Access Structures. In this subsection we will prove that for any compartmented access structure it is possible to construct a metering scheme realizing it. Let Γ be a compartmented access structure with u compartments $G_1, \ldots, G_u$ and let $h_r \leq n_r = |G_r|$ be the threshold associated to compartment G_r, for any $r = 1, \ldots, u$. The protocol is the following:

- **Initialization**:
  The audit agency A chooses u independent polynomials $P_1(x, y), \ldots, P_u(x, y)$ over $GF(q)$, where for any $r = 1, \ldots, u$, the polynomial $P_r(x, y)$ has degree $h_r - 1$ in x and $s\tau - 1$ in y. For any $r = 1, \ldots, u$, A gives the polynomial $P_r(i, y)$ to each client $\mathcal{C}_i \in G_r$.
- **Regular Operation for Time Frame** t:
  When a client $\mathcal{C}_i \in G_r$ visits a server $\mathcal{S}_j$ during a time frame t, it gives the value $P_r(i, j \circ t)$ to $\mathcal{S}_j$.
- **Proof Generation and Verification**:
  Assume that in time frame t a server $\mathcal{S}_j$ has received visits from at least h_r clients in the compartment G_r, for any $r = 1, \ldots, u$. Then, the server $\mathcal{S}_j$ can interpolate the polynomial $P_r(x, j \circ t)$ and compute the value $P_r(0, j \circ t)$ for any $r = 1, \ldots, u$. Finally, $\mathcal{S}_j$ can compute the value $\sum_{r=1}^{u} P_r(0, j \circ t)$, which is its proof for time frame t. When the audit agency receives the value $\sum_{r=1}^{u} P_r(0, j \circ t)$ from server $\mathcal{S}_j$ then it can easily verify if this is the correct proof for server $\mathcal{S}_j$ in time frame t.

It is easy to see that the proposed scheme is a metering scheme realizing the compartmented access structure Γ. Indeed, following the line of Subsection 2.2 we can prove that Properties 1, 2, and 3 of Definition 1 are satisfied.

Efficiency of the Scheme. In the proposed scheme the information distributed to client $\mathcal{C}_i$ by the audit agency consists of $s\tau$ points of $GF(q)$. The information given from client $\mathcal{C}_i$ to any server $\mathcal{S}_j$ during a visit consists of a single point of $GF(q)$. It is easy to see that the scheme of Subsection 3.2 meets the bounds of Corollary 6 and Lemma 8, and hence it is optimal with respect to the communication complexity.

4 Conclusions

In this paper we have considered metering schemes in which it is necessary for the servers to know the identities of visiting clients in order to reconstruct their

proofs. A nice property for a metering scheme would be to enable *client and server anonymity*. Client anonymity is possible in some particular situations: in a threshold access structure, visits can be anonymous, provided that the servers do not know the correspondence between the values i and the client $\mathcal{C}_i$. In multilevel and compartmented access structures, anonymity can be preserved "within levels" and "within compartments", respectively.

Moreover, in this paper we have assumed that clients provide correct shares when they visit servers. In a practical implementation of a metering scheme, some method of authentication should be used. However, the method of authentication used would be, in general, independent of the specific metering scheme and it could be incorporated as an additional feature in any metering scheme, if desired.

Acknowledgements. We would like to thank the anonymous referees for their useful comments. This work was done while the first author was visiting the Department of Combinatorics and Optimization at the University of Waterloo. She wants to thank the Department for its hospitality. The research of the second author is supported by the Natural Sciences and Research Council of Canada under grants NSERC-IRC 216431-96 and NSERC-RGPIN 203114-98.

References

1. C. Blundo, A. De Bonis, and B. Masucci, *Bounds and Constructions for Metering Schemes*, Technical Report, Università di Salerno, October 1999.
2. C. Blundo, A. De Bonis, B. Masucci, and D. R. Stinson, *Dynamic Multi-Threshold Metering Schemes*, Technical Report CORR **2000-18**, Centre for Applied Cryptographic Research, University of Waterloo, 2000.
3. E. F. Brickell, *Some Ideal Secret Sharing Schemes*, The Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. **6**, pp. 105–113, 1989.
4. T. M. Cover and J. A. Thomas, Elements of Information Theory. John Wiley & Sons, 1991.
5. A. De Bonis and B. Masucci, *An Information Theoretic Approach to Metering Schemes*, to appear in "IEEE International Symposium on Information Theory (ISIT 2000)".
6. M. Franklin and D. Malkhi, *Auditable Metering with Lightweight Security*, Journal of Computer Security, Vol. **6**, No. 4, pp. 237–225, 1998.
7. H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini, *Secret Sharing in Multilevel and Compartmented Groups*, in "Australasian Conference on Information Security and Privacy - ACISP '98", LNCS, Vol. **1438**, pp. 367–378, 1998.
8. B. Masucci and D. R. Stinson, *Efficient Metering Schemes with Pricing*, Technical Report CORR **2000-06**, Centre for Applied Cryptographic Research, University of Waterloo, 2000.
9. M. Naor and B. Pinkas, *Secure and Efficient Metering*, in "Advances in Cryptology - EUROCRYPT '98", LNCS, Vol. **1403**, pp. 576–590, 1998.
10. A. Shamir, *How to Share a Secret,* Communications of the ACM, Vol. **22**, pp. 612–613, 1979.
11. G. J. Simmons, *How to (Really) Share a Secret,* in "Advances in Cryptology - CRYPTO '88", LNCS, Vol. **403**, pp. 390–448, 1988.

Appendix - Information Theory Background

In this section we review the basic concepts of Information Theory used in our definitions and proofs. For a complete treatment of the subject the reader is advised to consult [4].

Given a probability distribution $\{Pr_{\mathbf{X}}(x)\}_{x\in X}$ on a set X, we define the *entropy* [1] of $\mathbf{X}$, as $H(\mathbf{X}) = -\sum_{x\in X} Pr_{\mathbf{X}}(x) \log Pr_{\mathbf{X}}(x)$. The entropy satisfies the following property:

$$0 \leq H(\mathbf{X}) \leq \log |X|, \tag{4}$$

where $H(\mathbf{X}) = 0$ if and only if there exists $x_0 \in X$ such that $Pr_{\mathbf{X}}(x_0) = 1$; whereas $H(\mathbf{X}) = \log |X|$ if and only if $Pr_{\mathbf{X}}(x) = 1/|X|$, for all $x \in X$.

Given two sets X and Y and a joint probability distribution on their cartesian product, the *conditional entropy* $H(\mathbf{X}|\mathbf{Y})$, is defined as

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

From the definition of conditional entropy it is easy to see that

$$H(\mathbf{X}|\mathbf{Y}) \geq 0. \tag{5}$$

Given n sets $X_1, \ldots, X_n$ and a joint probability distribution on their cartesian product, the entropy of $\mathbf{X}_1 \ldots \mathbf{X}_n$ satisfies

$$H(\mathbf{X}_1 \ldots \mathbf{X}_n) = H(\mathbf{X}_1) + \sum_{i=2}^{n} H(\mathbf{X}_i|\mathbf{X}_1 \ldots \mathbf{X}_{i-1}). \tag{6}$$

Given $n+1$ sets $X_1, \ldots, X_n, Y$ and a joint probability distribution on their cartesian product, the entropy of $\mathbf{X}_1 \ldots \mathbf{X}_n$ given $\mathbf{Y}$ satisfies

$$H(\mathbf{X}_1 \ldots \mathbf{X}_n|\mathbf{Y}) \leq \sum_{i=1}^{n} H(\mathbf{X}_i|\mathbf{Y}). \tag{7}$$

Given $n+2$ sets $X_1, \ldots, X_n, Y, Z$ and a joint probability distribution on their cartesian product, the *conditional mutual information* $I(\mathbf{Y}; \mathbf{Z}|\mathbf{X}_1 \ldots \mathbf{X}_n)$ between $\mathbf{Y}$ and $\mathbf{Z}$ given $\mathbf{X}_1, \ldots, \mathbf{X}_n$ is defined as

$$I(\mathbf{Y}; \mathbf{Z}|\mathbf{X}_1 \ldots \mathbf{X}_n) = H(\mathbf{Y}|\mathbf{X}_1 \ldots \mathbf{X}_n) - H(\mathbf{Y}|\mathbf{X}_1 \ldots \mathbf{X}_n\mathbf{Z})$$

and enjoys the following property: $I(\mathbf{Y}; \mathbf{Z}|\mathbf{X}_1 \ldots \mathbf{X}_n) \geq 0$, from which one gets

$$H(\mathbf{Y}|\mathbf{X}_1 \ldots \mathbf{X}_n) \geq H(\mathbf{Y}|\mathbf{X}_1 \ldots \mathbf{X}_n\mathbf{Z}). \tag{8}$$

[1] All logarithms in this paper are to the base 2.