Communications in Information and Systems
Vol. 2, No. 1, pp. 1-28, June 2002

001

BOUNDS AND CONSTRUCTIONS FOR METERING SCHEMES*

CARLO BLUNDO†, ANNALISA DE BONIS†, AND BARBARA MASUCCI†

Abstract. Metering schemes are cryptographic protocols to count the number of visits received by web sites. These measurement systems may be used to decide the amount of money to be paid to web sites hosting advertisements. Indeed, the amount of money paid by the publicity agencies to the web sites depends on the number of clients which visited the sites. In this paper we consider two generalizations of the metering scheme proposed by Naor and Pinkas (Vol. 1403 of LNCS, pp. 576–590). In their scheme a web site is paid if and only if the number of clients which visit the site is greater than a fixed threshold. We consider *ramp metering schemes* and *metering schemes with pricing*, that is, a scheme providing a tradeoff between the security and the complexity of information distribution and a scheme allowing to count the exact number of visits received by each server so that each server can be paid a proportional amount of money, respectively. We provide lower bounds on the size of the information distributed to clients and servers by these metering schemes and present schemes which achieve these lower bounds.

1. Introduction.

Most of the revenues of web sites come from advertisement payments. 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 site. Consequently, advertisers should prevent the web sites from inflating the count of their visits in order to demand more money. In a typical scenario there is an audit agency whose task is to measure the interaction between a large number of servers and clients. Hence, the audit agency should dispose of a mechanism which ensures the validity and accuracy of usage measurements against fraud attempts by servers (web sites) and clients (visitors).

Even though metering originated in the field of web advertisements, there are several other applications of secure metering schemes.

- Network accounting: Network pricing is very complicated since the information transmitted through the Internet is divided into packets which travel separately and are routed through many different networks. Metering schemes can provide an effective and secure measurement of the number of packets routed by a network through several different networks.
- Target audience: Metering schemes can be used to measure the usage of a web site by a special category of users. A metering scheme can be used,

*Received on November 26, 2001, accepted for publication on June 10, 2002. This paper is a coalescing and expansion of two papers presented at the *2000 IEEE International Symposium on Information Theory (ISIT 2000)* [5] and at the *14th International Conference on Distributed Computing (DISC 2000)* [2]. This work is partially supported by National Council for Research (C.N.R.) under grant CNRRG008BF3: *"Pubblicità on line: nuove misure per nuovi media. Auditing e accounting sicuro sul WEB"*.

†Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy, E-mail: {carblu, debonis, masucci}@dia.unisa.it

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. In return, the professors receive updates on the leatest releases.

- Toll free connection: Many companies offer toll free numbers to their customers. Similarly, they might agree to pay for the cost required to access their web sites. Franklin and Malkhi [6] suggested to use metering schemes as a method to measure the amount of money that the companies should pay to the users' ISPs.

Currently, there is no standard method for web metering. The most employed measurement method to learn about the exposure of ads on the Internet is the *pay-per-click* method, which is based on the number of *click-through* on banners and other ads. Advertisers typically install a software, called the *click-through payment program*, at web servers hosting their ads, in order to collect access information. The security of this method has been analyzed in [1] and [13] where several protocols have been described to detect *hit inflation* attacks which artificially inflate the number of click-throughs. Currently used alternative to pay-per-click programs are *pay-per-lead* and *pay-per-sale* programs, where servers are paid only for visits from users who perform some substantial activity or make purchases at the web sites. It is virtually impossible for servers to mount useful hit inflation attacks on these schemes, since simple clicks are worthless to servers. However, these programs are susceptible to a different form of fraud, known as *hit shaving*, where the server fails to report that the user visit is actually associated with a lead or a sale.

Franklin and Malkhi [6] first proposed metering schemes where clients are involved in the computation of a *timing function* upon visiting a web server. The results of this computation are saved by the server along with the record of the visits, as an indication of the amount of computation performed.

Subsequently, Naor and Pinkas [10] proposed metering schemes where any server provides the audit agency with a short proof of the visits it has received. Their metering schemes involve an initialization phase during which clients receive some secret information from the audit agency. Such information is used to compute a message which is sent to the visited server. After collecting these messages from different clients each server is able to compute the proof. Clearly, such schemes require clients to register with the audit agency in order to participate in the metering process. Such registration may have several advantages for clients. For example, after registration the clients may access to additional services, such as receiving news on topics of interest, getting information on upcoming promotions, downloading coupons, participating in a forum, sending through a web site free SMS (Short Message Service), disposing of free disk space and mailbox, and many others. Moreover, registration does not require clients to disclose their real identity. The metering schemes in [10] are supposed to be active for at most τ time frames and during these time frames are *secure* against corrupt servers that cooperate in order to inflate their count of visits.

In particular, Naor and Pinkas have considered metering schemes where any server is able to compute its proof for a certain time frame if and only if it has been visited in that time frame by a number of clients greater than or equal to some threshold h.

In this paper we introduce two generalizations of Naor and Pinkas metering schemes [10]: *ramp metering schemes* [5] and *metering schemes with pricing* [2]. In the following we briefly discuss the motivations for introducing our generalizations. Both these kinds of metering schemes involve distributing information to clients and servers. 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. With this motivations, we decided mainly to focus on the communication complexity of such metering schemes.

Ramp Metering Schemes

In the schemes proposed by Naor and Pinkas [10] the audit agency sends to each client a polynomial of degree $s\tau - 1$ over $GF(q)$, where s is the maximum size of a coalition of corrupt servers and τ is the number of time frames in which the scheme is active. For any time frame, the client sends to the visited server the value obtained by evaluating its polynomial at a certain point. The proof consists of a single point in $GF(q)$ and can be computed if and only if the server has received at least h client visits.

Given the high complexity of the above said distribution mechanism, a natural step is to trade complexity for security. Hence, we consider a more flexible situation where a server which receives less than h visits is able to gain *some partial information* about its proof. This loss of security is paid back by the smaller quantity of information distributed to parties. More precisely, we introduce *ramp metering schemes* [5], in which there are two thresholds ℓ and h, where $\ell < h \leq n$, and any server can be in three different situations in a given time frame t: 1) the server is visited by a number of clients greater than or equal to h. In this case the server is able to calculate its proof; 2) the server is visited by a number of clients smaller than or equal to ℓ. In this case the server has no information about its proof; 3) the server is visited by a number of clients between $\ell+1$ and $h-1$. In this case the server has some information about its proof, but this information does not enable it to compute the proof.

Ramp metering schemes provide a separation between the capacity of the servers of computing their proofs, which is specified by the parameter h, and the security of the scheme, which is specified by the parameter ℓ. The model considered by Naor and Pinkas [10] does not provide such a separation, since in that model the capacity of the servers of computing their proofs and the security of the scheme are specified by the same parameter h. Ramp metering schemes are particularly useful for advertisement applications in which web sites are paid only if they perform a very large number of services. In such a case it might be convenient to find a compromise between the security requirements and the complexity of information distribution.

We provide lower bounds on the size of the information distributed to clients and servers in ramp metering schemes. We also present a scheme which achieves these bounds. The size of the information distributed to clients and that of the information distributed to servers decrease linearly with the difference $h - \ell$. The lower is the difference $h - \ell$, the smaller is the range of values $k < h$ such that a server which receives k visits is able to gain some information about its proof. Hence, for any value of the difference $h - \ell$, our scheme provides a distinct tradeoff between security and the complexity of information distribution.

Metering Schemes with Pricing

Metering schemes proposed by Naor and Pinkas [10] can be used to check if a server received at least h visits, where h is a predefined parameter of the schemes. Indeed, in their schemes a server that has received a number of visits less than h is in the same situation as a server which has received no visit, i.e., it has absolutely no information about its proof. Consequently, the audit agency will pay nothing to a server that has been visited by less than h clients.

In order to have a more flexible payment system which enables to count the exact number of visits that a server has received in any time frame, we introduce *metering schemes with pricing* [2]. In these schemes there are two thresholds ℓ and h, where $\ell < h \leq n$, and any server can be in three different situations in a given time frame t: 1) the server is visited by a number of clients greater than or equal to h. In this case the audit agency would pay all the negotiated amount for the exposure of the ads; 2) the server is visited by a number of clients smaller than or equal to ℓ. In this case the audit agency would pay nothing; 3) the server is visited by a number of clients between $\ell + 1$ and $h - 1$. In this case the audit agency would pay a smaller sum growing with the number of the visits. Recently the authors of [9] proposed a metering scheme with pricing within a different model than the one considered in this paper and in [2]. In their scheme there is an interaction between servers and the audit agency during the whole metering process. In our scheme, as well as in that by Naor and Pinkas [10], the audit agency communicates *only* with the clients and this interaction is restricted *only* to the initialization phase.

We provide lower bounds on the size of the information distributed to clients and servers in metering schemes with pricing. We also present a scheme which achieves these bounds.

2. The Scenario. 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. 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 $t = 1, \ldots, \tau$. A visit can be defined in several different ways according to the measurement context. For example, it might be a page hit, a session lasting more than a fixed threshold of time or any similar definition (it is beyond the scope of this paper to define what should be considered as a visit). Any client visit to a server during a time frame is called a *regular operation.*

The general structure of a metering scheme is the following:

- **Initialization**
  This step is performed once by the audit agency $\mathcal{A}$. The audit agency $\mathcal{A}$ chooses a random secret key and generates an initialization message for any client, which is a function of this key and of the identity of the client. This message is sent to any client through a private channel and should be kept secret by the client.
  For any $i = 1, \ldots, n$, we denote by c_i the information that the audit agency $\mathcal{A}$ gives to the client $\mathcal{C}_i$ during the initialization phase. Moreover, we denote by C_i the set of all possible values that c_i can assume.
- **Regular Operation in a Time Frame**
  Every time a client $\mathcal{C}_i$ visits a server $\mathcal{S}_j$ in a time frame t it uses its private information to compute a message which is sent to the visited server. 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 $\mathcal{S}_j$ during a visit in time frame t. Moreover, we denote by $C_{i,j}^t$ the set of all possible values that $c_{i,j}^t$ can assume. For any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, we denote with $X_{j,(d_j)}^t$ the set of the d_j client visits received by server $\mathcal{S}_j$ in time frame t.
- **Proof Computation for a Time Frame**
  At the end of a time frame any server uses the information provided by client visits during the time frame in order to compute its proof. Notice that the proof can be computed only is the servers has received "enough" (to be defined later) client visits. Afterwards, the proof is sent to the audit agency.
  For any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, we denote by p_j^t the proof computed by the server $\mathcal{S}_j$ in time frame t. Moreover, we denote by P_j^t the set of all values that p_j^t can assume. Given a set of server indices $B = \{j_1, \ldots, j_\beta\} \subseteq \{1, \ldots, m\}$, where $j_1 < j_2 < \ldots < j_\beta$, we denote by P_B^t the cartesian product $P_{j_1}^t \times \cdots \times P_{j_\beta}^t$.
- **Proof Verification for a Time Frame**
  During this stage the audit agency verifies if the proofs received by the servers are consistent with its private information. In this case, the audit agency will pay the server for its services, otherwise, the server will not get any money.

We consider a scenario with a certain number s of *corrupt servers* and a certain number c of *corrupt clients*, which could cooperate in order to inflate the count of the visits that a corrupt server receives. A corrupt client $\mathcal{C}_i$ can donate to a corrupt server the whole information c_i received by the audit agency during the initialization phase. In time frame t, where $t = 1, \ldots, \tau$, a corrupt server can donate to another corrupt server the information that it has received during time frames $1, \ldots, t$. For any $i = 1, \ldots, n$ and $t = 1, \ldots, \tau$, we denote by $V_j^{[t]}$ all the information received by a corrupt server $\mathcal{S}_j$ in time frames $1, \ldots, t$. This information includes the sets of client visits received by server $\mathcal{S}_j$ in time frames $1, \ldots, t$. We also define $V_j^{[0]} = \emptyset$, for any corrupt server $\mathcal{S}_j$. Given a set of server indices $B = \{j_1, \ldots, j_\beta\} \subseteq \{1, \ldots, m\}$, where $j_1 < j_2 < \ldots < j_\beta$, we denote by $V_{_B}^{[t]}$ the cartesian product $V_{_{j_1}}^{[t]} \times \cdots \times V_{_{j_\beta}}^{[t]}$.

In this paper 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 some basic properties of entropy, consult the Appendix). Let d be an arbitrary positive integer and let $\mathbf{X}_1, \ldots, \mathbf{X}_d$ be d random variables taking values on the sets $X_1, \ldots, X_d$, respectively. For any subset $V = \{i_1, \ldots, i_v\} \subseteq \{1, \ldots, d\}$, with $i_1 \leq \ldots \leq i_v$, we denote with $X_{_V}$ the set $X_{i_1} \times \ldots \times X_{i_v}$ and with $\mathbf{X}_{_V}$ the sequence of random variables $\mathbf{X}_{i_1}, \ldots, \mathbf{X}i_v$. We formally define metering schemes in terms of entropy. We use the entropy approach mainly because this leads to a compact and simple description of the schemes and because the entropy approach takes into account all probability distributions on the sets of the proofs generated by servers. For the reader's convenience, the notation introduced in this section is summarized in the Appendix.

2.1. Useful Lemmas. In order to prove our results we need the following two technical lemmas.

Lemma 2.1. *Let $\mathbf{W}$ and $\mathbf{E}$ be two random variables such that $H(\mathbf{W}|\mathbf{E}) = 0$. Then, for any two random variables $\mathbf{F}$ and $\mathbf{G}$, one has $H(\mathbf{G}|\mathbf{WEF}) = H(\mathbf{G}|\mathbf{EF})$.*

Proof. Let us consider the mutual information $I(\mathbf{W};\mathbf{G}|\mathbf{EF})$. From Equations (22) and (23) of Appendix one has

$$H(\mathbf{W}|\mathbf{EF}) - H(\mathbf{W}|\mathbf{EFG}) = H(\mathbf{G}|\mathbf{EF}) - H(\mathbf{G}|\mathbf{WEF}).$$

From Equation (24) of Appendix it follows that $H(\mathbf{W}|\mathbf{EFG}) \leq H(\mathbf{W}|\mathbf{EF})$. Since $H(\mathbf{W}|\mathbf{EF}) = 0$, then one gets $H(\mathbf{G}|\mathbf{WEF}) = H(\mathbf{G}|\mathbf{EF})$. □

Lemma 2.2. *Let α be a non negative number and let $\mathbf{E}$, $\mathbf{F}$, and $\mathbf{G}$ be three random variables such that $H(\mathbf{G}|\mathbf{EF}) = 0$ and $H(\mathbf{G}|\mathbf{E}) \geq \alpha H(\mathbf{G})$. Then, it holds that*

$$H(\mathbf{F}|\mathbf{E}) \geq \alpha H(\mathbf{G}) + H(\mathbf{F}|\mathbf{EG}).$$

Proof. Consider the mutual information $I(\mathbf{F};\mathbf{G}|\mathbf{E})$. From Equation (23) of Appendix it holds that

$$H(\mathbf{F}|\mathbf{E}) - H(\mathbf{F}|\mathbf{EG}) = H(\mathbf{G}|\mathbf{E}) - H(\mathbf{G}|\mathbf{EF}).$$

Since $H(\mathbf{G}|\mathbf{EF}) = 0$ and $H(\mathbf{G}|\mathbf{E}) \geq \alpha H(\mathbf{G})$, then it follows that $H(\mathbf{F}|\mathbf{E}) \geq \alpha H(\mathbf{G}) + H(\mathbf{F}|\mathbf{EG})$. □

3. Ramp Metering Schemes. In metering schemes proposed by Naor and Pinkas [10] the audit agency chooses a random bivariate polynomial $Q(x, y)$ having degree $h-1$ in x and $s\tau-1$ in y over $GF(q)$, where q is a large prime number. Afterwards, the audit agency sends the polynomial $Q(i,y)$ to any client $\mathcal{C}_i$. When a client $\mathcal{C}_i$ visits a server $\mathcal{S}_j$ in a time frame t it sends the value $Q(i, j \circ t)$ to $\mathcal{S}_j$, where "$\circ$" denotes an operator mapping each pair (j,t), with $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, to an element of $GF(q)$, having the property that no distinct two pairs (j,t) and (j', t') are mapped to the same element. If a server $\mathcal{S}_j$ receives at least h visits from clients in a time frame t, then it can interpolate the polynomial $Q(x, j \circ t)$ and compute its proof as $Q(0, j \circ t)$.

Given the high complexity of the above said distribution mechanism, a natural step is to trade complexity for security. Hence, we consider a more flexible situation where a server which receives less than h visits is able to gain *some partial information* about its proof. This loss of security is paid back by the smaller quantity of information distributed to parties. We refer to these metering schemes, as *ramp metering schemes*.

In ramp metering schemes there are two thresholds ℓ and h, where $\ell < h \leq n$, and any server can be in three different situations in a given time frame t: 1) the server is visited by a number of clients greater than or equal to h. In this case the server is able to compute its proof; 2) the server is visited by a number of clients smaller than or equal to ℓ. In this case the server has no information about its proof (for example, assuming that the proof belongs to a set F, the proof can be any value in F); 3) the server is visited by a number f of clients between $\ell+1$ and $h-1$. In this case the server could have *some partial information* about its proof (for example, the server will know that the proof belongs to a set whose size is smaller than $|F|$). Ramp metering schemes enable to reduce the size of the information distributed to the parties by a factor of $h-\ell$ at the price of a loss in security. The lower is the difference $h-\ell$, the smaller is the range of values $k < h$ such that a server which receives k visits is able to gain some information about its proof. Consequently, ramp metering schemes are particularly useful for advertisement applications in which web sites are paid only if they perform a very large number of services. In such a case it might be convenient to find a compromise between the security requirements and the complexity of information distribution.

We assume that the schemes are 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 $t = 1, \ldots, \tau$. Moreover, we assume that at most a certain number, say c with $c \leq \ell$, of clients and a certain number, say s with $s \leq m$, of servers can be corrupt, i.e., they can cooperate in order to inflate the count of visits received by servers.

Definition 3.1. *An* $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme *is a protocol to measure the interaction between* n *clients and* m *servers during* τ *time frames in such a way that the following properties are satisfied:*

1. *For any time frame* t *each client can compute the piece to be given to any visited server:*

Formally, it holds that $H(\mathbf{C}^t_{i,j}|\mathbf{C}_i) = 0$ for $i = 1, \dots, n$, $j = 1, \dots, m$, and $t = 1, \dots, \tau$.

2. *For any time frame t any server which has been visited by at least h clients in time frame t can compute its proof for t:*
   Formally, it holds that $H(\mathbf{P}^t_j|\mathbf{X}^t_{j,(d_j)}) = 0$, where $d_j \geq h$, for $j = 1, \dots, m$, and $t = 1, \dots, \tau$.
3. *Let us consider a coalition of $0 \leq \alpha \leq c$ corrupt clients $\mathcal{C}_{i_1}, \dots, \mathcal{C}_{i_\alpha}$ and $1 \leq \beta \leq s$ corrupt servers $\mathcal{S}_{j_1}, \dots, \mathcal{S}_{j_\beta}$, and let $B = \{1, \dots, \beta\}$. Assume that at some time frame t each server in the coalition has been visited by at most $\ell - \alpha$ clients. Then, the servers in the coalition have no information about their proofs for t:*
   Formally, it holds that
   $$H(\mathbf{P}^t_{_B}|\mathbf{C}_{i_1} \dots \mathbf{C}_{i_\alpha} \mathbf{X}^t_{j_1,(d_{j_1})} \dots \mathbf{X}^t_{j_\beta,(d_{j_\beta})} \mathbf{V}^{[t-1]}_{_B}) = H(\mathbf{P}^t_{_B}),$$
   where $\alpha \leq c \leq \ell$ and $d_{j_v} \leq \ell - \alpha$, for $v = 1, \dots, \beta$ and $t = 1, \dots, \tau$.
4. *Let us consider a coalition of $0 \leq \alpha \leq c$ corrupt clients $\mathcal{C}_{i_1}, \dots, \mathcal{C}_{i_\alpha}$ and $1 \leq \beta \leq s$ corrupt servers $\mathcal{S}_{j_1}, \dots, \mathcal{S}_{j_\beta}$, and let $B = \{1, \dots, \beta\}$. Assume that at some time frame t each server $\mathcal{S}_{j_v}$ in the coalition has been visited by d_{j_v} clients other than $\mathcal{C}_{i_1}, \dots, \mathcal{C}_{i_\alpha}$, with $\ell - \alpha < d_{j_v} < h - \alpha$. Then, the servers in the coalition may have some information about their proofs for t:*
   Formally, it holds that
   $$\begin{aligned} &H(\mathbf{P}^t_{_B}|\mathbf{C}_{i_1} \dots \mathbf{C}_{i_\alpha} \mathbf{X}^t_{j_1,(d_{j_1})} \dots \mathbf{X}^t_{j_\beta,(d_{j_\beta})} \mathbf{V}^{[t-1]}_{_B}) \\ &\geq \frac{1}{h - \ell} \sum_{v=1}^{\beta} [h - (\alpha + d_{j_v})] H(\mathbf{P}^t_{j_v}|\mathbf{P}^t_{j_1} \dots \mathbf{P}^t_{j_v - 1}), \end{aligned}$$
   where $\alpha \leq c \leq \ell$, $X^t_{j_v,(d_{j_v})}$ is a set of visits to $\mathcal{S}_{j_v}$ from d_{j_v} clients other than $\mathcal{C}_{i_1}, \dots, \mathcal{C}_{i_\alpha}$ and $\ell < d_{j_v} + \alpha < h$, for $v = 1, \dots, \beta$ and $t = 1, \dots, \tau$.

We want to point out that our definition of corrupt servers is slightly different from that given by Naor and Pinkas [10]. Indeed, in their model a corrupt server can give to another corrupt server only the information collected during the previous time frames, whereas in our model, which is closer to what can actually happen, a corrupt server can give also the information provided by the visits received in the current time frame.

3.1. Lower Bounds. In this section we provide lower bounds on the size of the information distributed to clients by the audit agency during the setup of the scheme and on the size of the information given by any client while visiting any server during any time frame.

A Lower Bound on the Size of Clients' Secret Information. Since our goal is to prove a lower bound on the size of the information distributed to clients, we consider the worst possible case that at any time frame $t = 1, \dots, \tau$ and for any corrupt server $\mathcal{S}_j$ the set $V_j^{[t]}$ contains the maximum possible information, in other words, we assume that in any time frame $t' = 1, \ldots, t$, corrupt servers receive visits from all clients. Formally, it holds $H(\mathbf{C}_{i,j}^{t'} | \mathbf{V}_j^{[t]}) = 0$, for any $i = 1, \ldots, n$, $j = 1, \ldots, m$ and $1 \leq t' \leq t \leq \tau - 1$. Consequently one has

$$H(\mathbf{P}_{j}^{t'} | \mathbf{V}_j^{[t]}) = 0, \quad \text{for any } j = 1, \ldots, m \text{ and } 1 \leq t' \leq t \leq \tau - 1. \tag{1}$$

The next lemma will be a useful tool to prove a lower bound on the size of the information distributed to clients in ramp metering schemes.

LEMMA 3.2. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme. Let $\mathcal{C}_1, \ldots, \mathcal{C}_\alpha$ be a coalition of $\alpha \leq c$ corrupt clients, let $\mathcal{S}_1, \ldots, \mathcal{S}_\beta$ be a coalition of $\beta \leq s$ corrupt servers, and let $B = \{1, \ldots, \beta\}$. For $j = 1, \ldots, \beta$ and $t = 1, \ldots, \tau$, let $X_{j,(h-\alpha)}^t$ be a set of visits from $h - \alpha$ clients other than $\mathcal{C}_1, \ldots, \mathcal{C}_\alpha$ to server $\mathcal{S}_j$ in time frame t. Then it holds that*

$$\begin{aligned}
&H(\mathbf{C}_1 | \mathbf{C}_2 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&\geq \frac{1}{h-\ell} H(\mathbf{P}_{B}^t) + H(\mathbf{C}_1 | \mathbf{C}_2 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t]}).
\end{aligned}$$

Proof. From (22) of Appendix we have

$$\begin{aligned}
&I(\mathbf{C}_1; \mathbf{P}_{B}^t | \mathbf{C}_2 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&= H(\mathbf{P}_{B}^t | \mathbf{C}_2 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&\quad - H(\mathbf{P}_{B}^t | \mathbf{C}_1 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&= H(\mathbf{C}_1 | \mathbf{C}_2 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&\quad - H(\mathbf{C}_1 | \mathbf{C}_2 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{P}_{B}^t \mathbf{V}_{B}^{[t-1]}).
\end{aligned}$$

From (19) of Appendix we have

$$\begin{aligned}
&H(\mathbf{P}_{B}^t | \mathbf{C}_1 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&= H(\mathbf{P}_1^t | \mathbf{C}_1 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&\quad + \sum_{j=2}^{\beta} H(\mathbf{P}_j^t | \mathbf{P}_1^t \ldots \mathbf{P}_{j-1}^t \mathbf{C}_1 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t \ldots \mathbf{X}_{\beta,(h-\alpha)}^t \mathbf{V}_{B}^{[t-1]}) \\
&\leq H(\mathbf{P}_1^t | \mathbf{C}_1 \ldots \mathbf{C}_\alpha \mathbf{X}_{1,(h-\alpha)}^t) \\
&\quad + \sum_{j=2}^{\beta} H(\mathbf{P}_j^t | \mathbf{C}_1 \ldots \mathbf{C}_\alpha \mathbf{X}_{j,(h-\alpha)}^t) \text{ (from (24) of Appendix)} \\
&= 0 \text{ (from Property 2 of Definition 3.1).}
\end{aligned}$$

From Property 4 of Definition 3.1 we have that

$$\begin{aligned} H(\mathbf{P}^t_B|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^t_{1,(h-\alpha)}\dots\mathbf{X}^t_{\beta,(h-\alpha)}\mathbf{V}^{[t-1]}_B) &\geq \frac{h-(h-1)}{h-\ell}\sum_{j=1}^{\beta} H(\mathbf{P}^t_j|\mathbf{P}^t_1\dots\mathbf{P}^t_{j-1}) \\ &= \frac{1}{h-\ell}H(\mathbf{P}^t_B) \text{ (from (19) of Appendix).} \end{aligned}$$

Therefore, we have that

$$\begin{aligned} & H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^t_{1,(h-\alpha)}\dots\mathbf{X}^t_{\beta,(h-\alpha)}\mathbf{V}^{[t-1]}_B) \\ & \geq \frac{1}{h-\ell}H(\mathbf{P}^t_B) + H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^t_{1,(h-\alpha)}\dots\mathbf{X}^t_{\beta,(h-\alpha)}\mathbf{P}^t_B\mathbf{V}^{[t-1]}_B) \\ & = \frac{1}{h-\ell}H(\mathbf{P}^t_B) + H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^t_{1,(h-\alpha)}\dots\mathbf{X}^t_{\beta,(h-\alpha)}\mathbf{V}^{[t]}_B) \\ & \qquad\qquad \text{(from (1) of this section).} \end{aligned}$$

□

LEMMA 3.3. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme. Let $\mathcal{C}_1, \dots, \mathcal{C}_\alpha$ be a coalition of $\alpha \leq c$ corrupt clients, let $\mathcal{S}_1, \dots, \mathcal{S}_\beta$ be a coalition of $\beta \leq s$ corrupt servers, and let $B = \{1, \dots, \beta\}$. For $j = 1, \dots, \beta$ and $t = 1, \dots, \tau$, let $X^t_{j,(h-\alpha)}$ be a set of visits from $h - \alpha$ clients other than $\mathcal{C}_1, \dots, \mathcal{C}_\alpha$ to server $\mathcal{S}_j$ in time frame t. Then, it holds that*

$$\begin{aligned} & H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^1_{1,(h-\alpha)}\dots\mathbf{X}^1_{\beta,(h-\alpha)}) \\ & \geq \frac{1}{h-\ell}\sum_{t=1}^{\tau} H(\mathbf{P}^t_B) + H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^\tau_{1,(h-\alpha)}\dots\mathbf{X}^\tau_{\beta,(h-\alpha)}\mathbf{V}^{[\tau]}_B). \end{aligned}$$

Proof. The proof is by induction on τ. For $\tau = 1$ the lemma follows from Lemma 3.2. Now, suppose the lemma true for $\tau - 1$, that is

$$\begin{aligned} & H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^1_{1,(h-\alpha)}\dots\mathbf{X}^1_{\beta,(h-\alpha)}) \\ & \geq \frac{1}{h-\ell}\sum_{t=1}^{\tau-1} H(\mathbf{P}^t_B) + H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^{\tau-1}_{1,(h-\alpha)}\dots\mathbf{X}^{\tau-1}_{\beta,(h-\alpha)}\mathbf{V}^{[\tau-1]}_B). \qquad (2) \end{aligned}$$

We have that

$$\begin{aligned} & H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^{\tau-1}_{1,(h-\alpha)}\dots\mathbf{X}^{\tau-1}_{\beta,(h-\alpha)}\mathbf{V}^{[\tau-1]}_B) \\ & = H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{V}^{[\tau-1]}_B) \\ & \geq H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^{\tau}_{1,(h-\alpha)}\dots\mathbf{X}^{\tau}_{\beta,(h-\alpha)}\mathbf{V}^{[\tau-1]}_B) \text{ (from (24) of Appendix)} \\ & \geq \frac{1}{h-\ell}H(\mathbf{P}^\tau_B) + H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_\alpha\mathbf{X}^{\tau}_{1,(h-\alpha)}\dots\mathbf{X}^{\tau}_{\beta,(h-\alpha)}\mathbf{V}^{[\tau]}_B) \qquad (3) \\ & \qquad\qquad \text{(from Lemma 3.2).} \end{aligned}$$

Hence, the lemma follows from (2) and (3). □

The next theorem provides a lower bound on the size of the information distributed to clients in ramp metering schemes. The theorem states that the information that must be kept secret by clients decreases linearly with the difference $h - \ell$ and grows linearly with the number of time frames the scheme must be active and the size of the coalition of corrupt servers.

Theorem 3.4. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme. Let $\mathcal{S}_1, \dots, \mathcal{S}_\beta$ be a coalition of $\beta \leq s$ corrupt servers and let $B = \{1, \dots, \beta\}$. Then, for any $i = 1, \dots, n$, it holds that*

$$H(\mathbf{C}_i) \geq \frac{1}{h - \ell} \sum_{t=1}^{\tau} H(\mathbf{P}^t_{_B}).$$

Proof. Let $\mathcal{C}_1, \dots, \mathcal{C}_\alpha$ be a coalition of $\alpha \leq c$ corrupt clients and, for $j = 1, \dots, \beta$ and $t = 1, \dots, \tau$, let $X^t_{j,(h-\alpha)}$ be a set of visits from $h - \alpha$ clients other than $\mathcal{C}_1, \dots, \mathcal{C}_\alpha$ to server $\mathcal{S}_j$ in time frame t. We have

$$\begin{aligned} H(\mathbf{C}_1) &\geq H(\mathbf{C}_1 | \mathbf{C}_2 \dots \mathbf{C}_\alpha \mathbf{X}^1_{1,(h-\alpha)} \dots \mathbf{X}^1_{\beta,(h-\alpha)}) \text{ (from (24) of Appendix)} \\ &\geq \frac{1}{h - \ell} \sum_{t=1}^{\tau} H(\mathbf{P}^t_{_B}) + H(\mathbf{C}_1 | \mathbf{C}_2 \dots \mathbf{C}_\alpha \mathbf{X}^\tau_{1,(h-\alpha)} \dots \mathbf{X}^\tau_{\beta,(h-\alpha)} \mathbf{V}^{[\tau]}_{_B}) \\ &\quad \text{(from Lemma 3.3)} \\ &\geq \frac{1}{h - \ell} \sum_{t=1}^{\tau} H(\mathbf{P}^t_{_B}) \text{ (from (18) of Appendix).} \end{aligned}$$

□

Notice that Definition 3.1 does not say anything on the entropies of random variables $\mathbf{P}^{t_1}_{j_1}$ and $\mathbf{P}^{t_2}_{j_2}$, for different $j_1, j_2 \in \{1, \dots, m\}$ and $t_1, t_2 \in \{1, \dots, \tau\}$. For example, we could have either $H(\mathbf{P}^{t_1}_{j_1}) > H(\mathbf{P}^{t_2}_{j_2})$ or $H(\mathbf{P}^{t_1}_{j_1}) \leq H(\mathbf{P}^{t_2}_{j_2})$. Our results apply to the general case of arbitrary entropies on proofs, but for clarity we state our results for the simpler case that $H(\mathbf{P}^{t_1}_{j_1}) = H(\mathbf{P}^{t_2}_{j_2})$, for all $j_1, j_2 \in \{1, \dots, m\}$ and $t_1, t_2 \in \{1, \dots, \tau\}$. We denote this common entropy by $H(\mathbf{P})$.

The next corollary is an immediate consequence of Theorem 3.4.

Corollary 3.5. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme. If the proofs for the servers are pairwise statistically independent, then for any $i = 1, \dots, n$, it holds that*

$$H(\mathbf{C}_i) \geq \frac{s\tau}{h - \ell} H(\mathbf{P}).$$

If the random variable $\mathbf{P}$ is uniformly distributed in a finite field F, then $H(\mathbf{P}) = \log |F|$. Consequently, the size of the information owned by a client is lower bounded by $s\tau(h - \ell)^{-1} \log |F|$, and from (17) of Appendix, it follows that

$$\log |C_i| \geq \frac{s\tau}{h - \ell} \log |F|, \text{ for } i = 1, \dots, n. \tag{4}$$

In Section 3.2 we will present an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme which achieves this bound.

A Lower Bound on the Size of Servers' Secret Information. In the following we provide a lower bound on the size of the information given to servers by clients in ramp metering schemes. To prove the bound we need the following lemma.

LEMMA 3.6. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme. For $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, let $X^t_{j,(h-1)}$ be a set of visits from $h-1$ clients other than $\mathcal{C}_i$ to server $\mathcal{S}_j$ in time frame t. For any $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$, it holds that*

$$H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)}) \geq \frac{1}{h-\ell} H(\mathbf{P}^t_j) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)}\mathbf{P}^t_j).$$

Proof. From (22) of Appendix we have

$$\begin{aligned} I(\mathbf{C}^t_{i,j}; \mathbf{P}^t_j|\mathbf{X}^t_{j,(h-1)}) &= H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)}) - H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)}\mathbf{P}^t_j) \\ &= H(\mathbf{P}^t_j|\mathbf{X}^t_{j,(h-1)}) - H(\mathbf{P}^t_j|\mathbf{X}^t_{j,(h-1)}\mathbf{C}^t_{i,j}). \end{aligned}$$

From Property 2 of Definition 3.1 it holds

$$H(\mathbf{P}^t_j|\mathbf{X}^t_{j,(h-1)}\mathbf{C}^t_{i,j}) = 0,$$

whereas, from Property 4 of Definition 3.1 we get

$$H(\mathbf{P}^t_j|\mathbf{X}^t_{j,(h-1)}) \geq \frac{1}{h-\ell} H(\mathbf{P}^t_j).$$

Hence, we obtain

$$H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)}) \geq \frac{1}{h-\ell} H(\mathbf{P}^t_j) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)}\mathbf{P}^t_j).$$

□

The next theorem provides a lower bound on the size of the information distributed to servers from clients in ramp metering schemes. It implicitly shows that the size of the information each client has to give out when visiting a server decreases linearly with the difference $h - \ell$. Since $H(\mathbf{C}^t_{i,j}) \geq H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)})$ and $H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h-1)}\mathbf{P}^t_j) \geq 0$, the theorem immediately follows from Lemma 3.6.

THEOREM 3.7. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme. For any $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$, it holds that*

$$H(\mathbf{C}^t_{i,j}) \geq \frac{1}{h-\ell} H(\mathbf{P}^t_j).$$

If the variable $\mathbf{P}^t_j$ is uniformly distributed in a finite field F, then $H(\mathbf{P}^t_j) = \log|F|$. Consequently, the size of the information distributed by any client to any server is lower bounded by $(h-\ell)^{-1}\log|F|$ and from (17) it follows that

$$\log|C^t_{i,j}| \geq \frac{1}{h-\ell}\log|F|, \text{ for } i = 1, \ldots, n,\ j = 1, \ldots, m, \text{ and } t = 1, \ldots, \tau. \tag{5}$$

In Section 3.2 we will present an $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme which achieves this bound. Notice that lower bounds on the size of the information distributed to parties in the threshold model considered by Naor and Pinkas [10] can be derived setting $\ell = h - 1$ in Equations (4) and (5).

3.2. A Protocol for Ramp Metering Schemes. In this section we present a ramp metering scheme which achieves the bounds (4) and (5) of Section 3.1. The scheme is a generalization of Shamir's secret-sharing scheme [14].

Let $q > n + h - \ell$ be a large prime number. In the following, we use the term *regular visit* to indicate visits performed by non-corrupt clients. Moreover, we denote by "$\circ$" an operator mapping each pair (j, t), with $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, to an element of $GF(q)$, having the property that no distinct two pairs (j, t) and (j', t') are mapped to the same element. Let $f_1, \ldots, f_{h-\ell}$ be preselected elements of $GF(q)$ distinct from $1, \ldots, n$, which are known to any client and any server. The scheme is the following:

Initialization:

- The audit agency $\mathcal{A}$ chooses $h-\ell$ polynomials $P_1(y), \ldots, P_{h-\ell}(y)$ of degree $s\tau - 1$ over $GF(q)$.
- Let $Q(x, y)$ be a bivariate polynomial over $GF(q)$ of degree $h-1$ in x and degree $s\tau - 1$ in y, such that $Q(f_r, y) = P_r(y)$, for $r = 1, \ldots, h - \ell$. (It is easy to construct such a random polynomial by using Lagrange polynomials.)
- The audit agency $\mathcal{A}$ sends the polynomial $Q(i, y)$ to each client $\mathcal{C}_i$.

Regular Operation for Time Frame t:

When the client $\mathcal{C}_i$ visits the server $\mathcal{S}_j$ in time frame t, it sends the value $Q(i, j \circ t)$ to $\mathcal{S}_j$.

Proof Generation and Verification for Time Frame t:

- Assume that the server $\mathcal{S}_j$ has been visited by at least h different clients in time frame t.
- Then, it can perform a Lagrange interpolation on the polynomial $Q(x, j \circ t)$ and compute the proof $(P_1(j \circ t), \ldots, P_{h-\ell}(j \circ t))$.
- The server $\mathcal{S}_j$ sends the proof $(P_1(j \circ t), \ldots, P_{h-\ell}(j \circ t))$ to the audit agency.
- The audit agency $\mathcal{A}$ verifies the proof by evaluating the polynomial $Q(x, y)$ at the points $(f_1, j \circ t), \ldots, (f_{h-\ell}, j \circ t)$.

FIG. 1. *An $(n, m, \tau, c, s, \ell, h)$ ramp metering scheme.*

Analysis of the Scheme. It is immediate to verify that the scheme satisfies Property 1 of Definition 3.1. Indeed, for any $i = 1, \ldots, n$, the information given by the audit agency to the client $\mathcal{C}_i$ consists of the univariate polynomial $Q(i, y)$ and for any $j = 1, \ldots, m$ and $t = 1, \ldots, \tau$, the information given to the server $\mathcal{S}_j$ by client $\mathcal{C}_i$ in time frame t is obtained by evaluating the univariate polynomial $Q(i, y)$ at $j \circ t$.

It is also easy to verify that the scheme satisfies Property 2 of Definition 3.1.

Assume that the server $\mathcal{S}_j$ has been visited by h clients in time frame t. Then, $\mathcal{S}_j$ knows h points of the polynomial $Q(x, j \circ t)$ and can perform a Lagrange interpolation on it. Hence, it can compute its proof $(Q(f_1, j \circ t), \ldots, Q(f_{h-\ell}, j \circ t))$, by evaluating the polynomial $Q(x, j \circ t)$ in the points $f_1, \ldots, f_{h-\ell}$, which are known to all parties.

To prove that our scheme satisfies Property 3 of Definition 3.1, we consider the worst possible case that in any time frame $t = 1, \ldots, \tau$, all corrupt clients decide to cooperate with all corrupt servers and that corrupt servers have collected the maximum possible information during the previous time frames $1, \ldots, t-1$. In other words, for any time frame $t = 1, \ldots, \tau$, we assume that each corrupt client $\mathcal{C}_i$ gives its polynomial $Q(i, y)$ to all corrupt servers, and that any corrupt server $\mathcal{S}_j$ knows the polynomial $Q(x, j \circ t)$ for $t' = 1, \ldots, t-1$. Without loss of generality, let $\mathcal{S}_1, \ldots, \mathcal{S}_s$ be a coalition of s corrupt servers which decide to cooperate in some time frame t, with $1 \leq t \leq \tau$. We need to prove that for any time frame $t = 1, \ldots, \tau$, the coalition of corrupt servers is not able to compute the proof $(Q(f_1, j \circ t), \ldots, Q(f_{h-\ell}, j \circ t))$, for any $j = 1, \ldots, s$ if each server in the coalition receives less than $\ell - c$ regular visits in time frame t. In order to compute $Q(f_r, j \circ t)$, for $r = 1, \ldots, h-\ell$ and $j = 1, \ldots, s$, the corrupt servers should be able to interpolate either the polynomial $Q(x, j \circ t)$ or the bivariate polynomial $Q(x, y)$. The information that a corrupt client $\mathcal{C}_i$ gives to a corrupt server is equivalent to the $s\tau$ coefficients of its polynomial $Q(i, y)$. For $j = 1, \ldots, s$, the information collected by each corrupt server $\mathcal{S}_j$ during the previous time frames is equivalent to the h coefficients of the polynomials $Q(x, j \circ t')$, for any $t' = 1, \ldots, t-1$. Suppose that in time frame t, the server $\mathcal{S}_j$, $j \in \{1, \ldots, s\}$, receives g_j^t regular visits. Then, the overall information on $Q(x, y)$ held by the servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ consists of

$$cs\tau + s(t-1)h + \sum_{j=1}^{s} g_j^t - cs(t-1) \tag{6}$$

points. The first term of (6) corresponds to the information given by the c corrupt clients, the second term corresponds to the information collected by all servers in the coalition during the previous time frames, the third term corresponds to the information provided by the client visits in time frame t, and the last term represents the information which has been counted twice. We will prove that the servers in the coalition are unable to interpolate the polynomial $Q(x, y)$ if each server in the coalition receives less than $\ell - c$ regular visits. Notice that if $g_j^t \leq \ell - c$, for any $t = 1, \ldots, \tau$ and $j = 1, \ldots, s$, then expression (6) is less than or equal to $hs\tau - s(h - \ell)$. Consequently, for any choice of $s(h-\ell)$ values $a_{v,j}$ in $GF(q)$, where $v = 1, \ldots, h-\ell$ and $j = 1, \ldots, s$, there is a polynomial $R(x, y)$ which is consistent with the information held by the servers in the coalition and such that $R(f_v, j \circ t) = a_{v,j}$ for $v = 1, \ldots, h - \ell$ and $j = 1, \ldots, s$. Hence, the corrupt servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ have probability at most $1/q^{s(h-\ell)}$ of guessing their proofs for time frame t. Notice that instead of computing all the coefficients of the polynomial $Q(x, j \circ t)$ and then evaluating the polynomial in the point 0, the servers could only compute the free coefficients of the polynomial.

In similar way we can easily prove that the scheme satisfies Property 4 of Definition 3.1. Notice that if $g_j^t \leq r$, with $\ell - c < r < h - c$, for any $t = 1, \ldots, \tau$ and $j = 1, \ldots, s$, then expression (6) is less than or equal to $hs\tau - s(h - r - c)$. Consequently, for any choice of $s(h - r - c)$ values $a_{v,j}$ in $GF(q)$, where $v = 1, \ldots, h - r - c$ and $j = 1, \ldots, s$, there is a polynomial $R(x, y)$ which is consistent with the information held by the servers in the coalition and such that $R(f_v, j \circ t) = a_{v,j}$ for $v = 1, \ldots, h - r - c$ and $j = 1, \ldots, s$. Hence, the corrupt servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ have probability at most $1/q^{s(h-r-c)}$ of guessing their proofs for time frame t. Hence, the information that the servers have on their proofs for time frame increases linearly with respect to the value r.

Efficiency of the Scheme. It is easy to see that the scheme meets the bounds (4) and (5) of Section 3.1. Indeed, during the initialization phase the audit agency sends to each client $\mathcal{C}_i$ a polynomial $Q(i, y)$ of degree $s\tau - 1$ over $GF(q)$. Hence, the bound (4) is tight. During a regular operation in time frame t each server $\mathcal{S}_j$ receives from a client $\mathcal{C}_i$ the value $Q(i, j \circ t)$, which is a point in $GF(q)$. Hence, the bound (5) is tight.

In our ramp metering scheme the proof has size $(h - \ell) \log q$, while the size of the information distributed to clients and servers does not depend on the difference $h - \ell$. On the other hand, if we use a proof of size $(h - \ell) \log q$ in Naor and Pinkas metering schemes then the size of the information distributed to the parties is increased of a factor $(h - \ell)$.

4. Metering Schemes with Pricing.

In ramp metering schemes any server that receives less than h client visits gets some partial information about its proof, but is not able to compute it. Consequently, the server does not receive any money from the audit agency, as in Naor-Pinkas schemes [10]. In this section we introduce *metering schemes with pricing.* These schemes enable a more flexible payment system than ramp metering schemes and Naor-Pinkas schemes. Indeed, these schemes allow to count the exact number of visits received by each server, which is paid accordingly.

As in ramp metering schemes considered in Section 3, in metering schemes with pricing there are two thresholds ℓ and h, where $\ell < h \leq n$, and any server can be in three different situations in a given time frame t: 1) the server is visited by a number of clients greater than or equal to h. In this case the server receives a full payment of the negotiated amount of money; 2) the server is visited by a number of clients smaller than or equal to ℓ. In this case the server receives no money; 3) the server is visited by a number f of clients between $\ell + 1$ and $h - 1$. In this case the server receives a partial payment of the negotiated amount of money, which grows with the number of clients which have been served. To this aim, a server which has been visited by a number f of clients between $\ell + 1$ and h should be able to provide the audit agency with a proof of the number of visits it has received. A server which has been visited by more than h clients would provide the agency with the same proof it would have provided if it had received h visits. For any $j = 1, \ldots, m$, $t = 1, \ldots, \tau$, and $f = \ell + 1, \ldots, h$, we denote with $p^t_{j,f}$ the proof computed by the server $\mathcal{S}_j$ when it has been visited by f distinct clients in time frame t. We refer to such a proof as the f-proof of $\mathcal{S}_j$ in time frame t. Moreover, we denote with $P^t_{j,f}$ the set of all values that $p^t_{j,f}$ can assume. For any $r = \ell+1,\ldots,h$, we define $L_r = \{\ell+1,\ldots,r\}$ and we denote by p^t_{j,L_r} the proofs $p^t_{j,\ell+1}\ldots p^t_{j,r}$. Moreover, we denote with P^t_{j,L_r} the set of all values that p^t_{j,L_r} can assume. We also define $L_r = \emptyset$, for any $r < \ell+1$. To simplify the notation, we define $P^t_{j,L_\ell} = \emptyset$, for any $j = 1,\ldots,m$ and $t = 1,\ldots,\tau$.

As in ramp metering schemes, we assume that at most a certain number, say c with $c \le \ell$, of clients and a certain number, say s with $s \le m$, of servers can be corrupt, i.e., they can cooperate in order to inflate the count of visits received by servers.

Definition 4.1. *An* (n,m,τ,c,s,ℓ,h) metering scheme with pricing *is a protocol to measure the interaction between n clients and m servers during τ time frames in such a way that the following properties are satisfied:*

1. *For any time frame $t = 1,\ldots,\tau$ each client can compute the piece to be given to any visited server:*
   Formally, it holds that $H(\mathbf{C}^t_{i,j}|\mathbf{C}_i) = 0$ for $i = 1,\ldots,n$, $j = 1,\ldots,m$, and $t = 1,\ldots,\tau$.
2. *For any time frame $t = 1,\ldots,\tau$ and any $z = \ell+1,\ldots,h$, any server which has been visited by z different clients in time frame t, can compute its $(\ell+1)$-proof,…,z-proof for time frame t:*
   Formally, it holds that $H(\mathbf{P}^t_{j,L_z}|\mathbf{X}^t_{j,(z)}) = 0$ for $j = 1,\ldots,m$, $t = 1,\ldots,\tau$, and $z = \ell+1,\ldots,h$.
3. *Let us consider a coalition of $\alpha \le c$ corrupt clients $\mathcal{C}_{i_1},\ldots,\mathcal{C}_{i_\alpha}$, and $1 \le \beta \le s$ corrupt servers $\mathcal{S}_{j_1},\ldots,\mathcal{S}_{j_\beta}$, and let $B = \{1,\ldots,\beta\}$. Assume that at some time frame t each server in the coalition has been visited by at most $f-\alpha$ clients, with $f < h$. Then,for any $z = f+1,\ldots,h$ the servers in the coalition have no information about their z-proofs for t:*
   Formally, it holds that
   $$H(\mathbf{P}^t_{B,z}|\mathbf{C}_{i_1}\ldots\mathbf{C}_{i_\alpha}\mathbf{X}^t_{j_1,(d_{j_1})}\ldots\mathbf{X}^t_{j_\beta,(d_{j_\beta})}\mathbf{V}^{[t-1]}_B) = H(\mathbf{P}^t_{B,z})$$
   for $f < z \le h$, $t = 1,\ldots,\tau$, $0 \le \alpha \le c$, and $d_{j_v} + \alpha \le f$, for $v = 1,\ldots,\beta$.

4.1. Lower Bounds. In this section we provide lower bounds on the size of the information distributed to clients by the audit agency and on the size of the information given to servers by clients. The next lemma immediately follows from Definition 4.1.

Lemma 4.2. *Let $\mathcal{M}$ be an (n,m,τ,c,s,ℓ,h) metering scheme with pricing. Let $A = \{1,\ldots,\alpha\}$ be a set of client indices and let $B = \{1,\ldots,\beta\}$ be a set of server indices. Then, for any time frame $t = 1,\ldots,\tau$, it holds that*

$$H(\mathbf{C}^t_{A,B}|\mathbf{C}_A) = 0.$$

Proof. We have that

$$\begin{aligned} H(\mathbf{C}^t_{A,B}|\mathbf{C}_A) &\leq \sum_{i=1}^{\alpha}\sum_{j=1}^{\beta} H(\mathbf{C}^t_{i,j}|\mathbf{C}_A) \text{ (from Eq. (21) of Appendix)} \\ &\leq \sum_{i=1}^{\alpha}\sum_{j=1}^{\beta} H(\mathbf{C}^t_{i,j}|\mathbf{C}_i) \text{ (from Eq. (24) of Appendix)} \\ &= 0 \text{ (from Property 1 of Definition 4.1).} \end{aligned}$$

Hence, the lemma holds. □

A Lower Bound on the Size of Clients' Secret Information. Since our goal is to prove a lower bound on the size of the information distributed to clients we consider the worst possible case that, at any time frame $t = 1, \ldots, \tau$ and for any corrupt server $\mathcal{S}_j$, the sets $V_j^{[1]}, \ldots, V_j^{[t-1]}$ contain the maximum possible information. In other words, corrupt servers receive visits from all clients during the previous time frames $1, \ldots, t-1$. Formally, it holds that

$$(7) \quad H(\mathbf{C}^{t'}_{i,j}|\mathbf{V}^{[t]}_j) = 0, \quad \text{for any } i = 1, \ldots, n, \ j = 1, \ldots, m, \text{ and } 1 \leq t' \leq t \leq \tau - 1.$$

Consequently, one has

$$(8) \qquad H(\mathbf{P}^{t'}_{j,L_h}|\mathbf{V}^{[t]}_j) = 0, \quad \text{for any } j = 1, \ldots, m, \text{ and } 1 \leq t' \leq t \leq \tau - 1.$$

In the following we present a lower bound on the size of the information given to clients by the audit agency during the initialization phase. The following technical lemma will be used in the proof of Lemma 4.4.

Lemma 4.3. *Let $\mathcal{M}$ be an $(\ell, h, n, m, \tau, c, s)$ metering scheme with pricing. Let $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_c}$ be the corrupt clients and let B, with $|B| = \beta \leq s$, be a set of indices of corrupt servers. For any $j \in B$, $t = 1, \ldots, \tau$, and $z = \ell - c, \ldots, h - c$, let $X^t_{j,(z)}$ be a set of visits from z clients other than $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_c}$ to server $\mathcal{S}_j$ in time frame t. Then, for any $v = 1, \ldots, c$, $t = 1, \ldots, \tau$, and $r = \ell + 1, \ldots, h$, it holds that*

$$\begin{aligned} &H(\mathbf{C}_{i_v}|\mathbf{C}_{\{i_1,\ldots,i_c\}\setminus\{i_v\}}\mathbf{X}^t_{B,(r-c-1)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{V}^{[t-1]}_B) \\ &\geq H(\mathbf{P}^t_{B,r}) + H(\mathbf{C}_{i_v}|\mathbf{C}_{\{i_1,\ldots,i_c\}\setminus\{i_v\}}\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_r}\mathbf{V}^{[t-1]}_B). \end{aligned}$$

Proof. For the sake of simplicity and w.l.o.g., we will assume $\{i_1, \ldots, i_c\} = \{1, \ldots, c\}$ and $B = \{1, \ldots, \beta\}$, and will prove the lemma for $\mathbf{C}_{i_v} = \mathbf{C}_1$. Let us consider the random variables $\mathbf{A} = \mathbf{P}^t_{B,L_{r-1}}$, $\mathbf{A}' = \mathbf{C}^t_{2,B}, \ldots, \mathbf{C}^t_{c,B}$, $\mathbf{D} = \mathbf{C}_1$, $\mathbf{E} = \mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{V}^{[t-1]}_B$, $\mathbf{E}' = \mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{V}^{[t-1]}_B$, and $\mathbf{F} = \mathbf{P}^t_{B,r}$. One has

$$\begin{aligned} &H(\mathbf{C}^t_{2,B}, \ldots, \mathbf{C}^t_{c,B}|\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{V}^{[t-1]}_B) \\ &\leq H(\mathbf{C}^t_{2,B}, \ldots, \mathbf{C}^t_{c,B}|\mathbf{C}_2 \ldots \mathbf{C}_c) \text{ (from (24) of Appendix)} \\ &= 0 \text{ (from Lemma 4.2).} \end{aligned}$$

Hence, $\mathbf{A}'$ and $\mathbf{E}'$ satisfy the hypothesis of Lemma 2.1, and one has $H(\mathbf{A}|\mathbf{E}') = H(\mathbf{A}|\mathbf{A}'\mathbf{E}')$. For $r = \ell + 2, \ldots, h$, one gets

$$\begin{aligned}
&H(\mathbf{P}^t_{B,L_{r-1}}|\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{V}^{[t-1]}_B)\\
&= H(\mathbf{P}^t_{B,L_{r-1}}|\mathbf{C}^t_{2,B} \ldots \mathbf{C}^t_{c,B}\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{V}^{[t-1]}_B) \text{ (from Lemma 2.1)}\\
&\le H(\mathbf{P}^t_{B,L_{r-1}}|\mathbf{C}^t_{2,B} \ldots \mathbf{C}^t_{c,B}\mathbf{X}^t_{B,(r-c)}) \text{ (from (24) of Appendix)}\\
&\le \sum_{j=1}^{\beta} H(\mathbf{P}^t_{j,L_{r-1}}|\mathbf{C}^t_{2,B} \ldots \mathbf{C}^t_{c,B}\mathbf{X}^t_{B,(r-c)}) \text{ (from (21) of Appendix)}\\
&\le \sum_{j=1}^{\beta} H(\mathbf{P}^t_{j,L_{r-1}}|\mathbf{C}^t_{2,j} \ldots \mathbf{C}^t_{c,j}\mathbf{X}^t_{j,(r-c)}) \text{ (from (24) of Appendix)}\\
&= 0 \text{ (from Property 2 of Definition 4.1).}
\end{aligned}$$

Since $P^t_{B,L_\ell} = \emptyset$, then the above equality trivially holds also for $r = \ell + 1$. Hence, the random variables $\mathbf{A}$ and $\mathbf{E}'$ satisfy the hypothesis of Lemma 2.1, and one has $H(\mathbf{F}|\mathbf{A}\mathbf{E}') = H(\mathbf{F}|\mathbf{E}')$. Consequently, for any $r = \ell + 1, \ldots, h$, one gets

$$\begin{aligned}
&H(\mathbf{P}^t_{B,r}|\mathbf{P}^t_{B,L_{r-1}}\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{V}^{[t-1]}_B)\\
&= H(\mathbf{P}^t_{B,r}|\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{V}^{[t-1]}_B) \text{ (from Lemma 2.1)}\\
&= H(\mathbf{P}^t_{B,r}) \text{ (from Property 3 of Definition 4.1).}
\end{aligned}$$

Let $\mathbf{A}'' = \mathbf{C}^t_{1,B} \ldots \mathbf{C}^t_{c,B}$ and $\mathbf{E}'' = \mathbf{C}_1 \ldots \mathbf{C}_c$. From Lemma 4.2 it holds that $\mathbf{A}''$ and $\mathbf{E}''$ satisfy the hypothesis of Lemma 2.1. Hence, one has $H(\mathbf{F}|\mathbf{E}'') = H(\mathbf{F}|\mathbf{A}''\mathbf{E}'')$, and consequently, for any $r = \ell + 1, \ldots, h$, one gets

$$\begin{aligned}
&H(\mathbf{P}^t_{B,r}|\mathbf{C}_1 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{V}^{[t-1]}_B)\\
&= H(\mathbf{P}^t_{B,r}|\mathbf{C}_1 \ldots \mathbf{C}_c\mathbf{C}^t_{1,B} \ldots \mathbf{C}^t_{c,B}\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{V}^{[t-1]}_B) \text{ (from Lemma 2.1))}\\
&\le H(\mathbf{P}^t_{B,r}|\mathbf{C}^t_{1,B} \ldots \mathbf{C}^t_{c,B}\mathbf{X}^t_{B,(r-c)}) \text{ (from (24) of Appendix)}\\
&\le \sum_{j=1}^{\beta} H(\mathbf{P}^t_{j,r}|\mathbf{C}^t_{1,B} \ldots \mathbf{C}^t_{c,B}\mathbf{X}^t_{B,(r-c)}) \text{ (from (21) of Appendix)}\\
&\le \sum_{j=1}^{\beta} H(\mathbf{P}^t_{j,r}|\mathbf{C}^t_{1,j} \ldots \mathbf{C}^t_{c,j}\mathbf{X}^t_{j,(r-c)}) \text{ (from (24) of Appendix)}\\
&= 0 \text{ (from Property 2 of Definition 4.1).}
\end{aligned}$$

Hence, one has that $\mathbf{D}$, $\mathbf{E}$ and $\mathbf{F}$ satisfy the hypothesis of Lemma 2.2. Consequently, one has $H(\mathbf{D}|\mathbf{E}) = H(\mathbf{F}) + H(\mathbf{D}|\mathbf{E}\mathbf{F})$, and for any $r = \ell + 1, \ldots, h$, one gets

$$\begin{aligned}
&H(\mathbf{C}_1|\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{V}^{[t-1]}_B)\\
&= H(\mathbf{P}^t_{B,r}) + H(\mathbf{C}_1|\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{P}^t_{B,r}\mathbf{V}^{[t-1]}_B) \text{ (from Lemma 2.2)}\\
&= H(\mathbf{P}^t_{B,r}) + H(\mathbf{C}_1|\mathbf{C}_2 \ldots \mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_r}\mathbf{V}^{[t-1]}_B).
\end{aligned}$$

The lemma follows from the above equality and from (24) of Appendix which implies

$$\begin{aligned}&H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(r-c-1)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{V}_B^{[t-1]})\\ &\geq H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(r-c)}\mathbf{P}^t_{B,L_{r-1}}\mathbf{V}_B^{[t-1]}).\end{aligned}$$

Hence, the lemma holds. □

The next lemma states that the uncertainty that a coalition of β corrupt servers and $c-1$ corrupt clients has at time frame $t-1$ about the secret information held by another client is lower bounded by the uncertainty about the proofs that the coalition of corrupt servers can reconstruct in time frame t. In other words, for the coalition the task of "guessing" the secret information held by any other client is at least as hard as the task of "guessing" its proofs for time frame t.

Lemma 4.4. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ metering scheme with pricing. Let $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_c}$ be the corrupt clients and let B, with $|B| = \beta \leq s$, be a set of indices of corrupt servers. For any $v = 1, \ldots, c$ and $t = 1, \ldots, \tau$, it holds that*

$$H(\mathbf{C}_{i_v}|\mathbf{C}_{\{i_1,\ldots,i_c\}\setminus\{i_v\}}\mathbf{V}_B^{[t-1]}) \geq H(\mathbf{P}^t_{B,L_h}) + H(\mathbf{C}_{i_v}|\mathbf{C}_{\{i_1,\ldots,i_c\}\setminus\{i_v\}}\mathbf{V}_B^{[t]}).$$

Proof. For the sake of simplicity and w.l.o.g., we will assume $\{i_1, \ldots, i_c\} = \{1, \ldots, c\}$ and $B = \{1, \ldots, \beta\}$, and prove the lemma for $\mathbf{C}_{i_v} = \mathbf{C}_1$. Starting from $H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(\ell-c)}\mathbf{P}^t_{B,L_\ell}\mathbf{V}_B^{[t-1]})$ and iteratively applying Lemma 4.3, we get

$$\begin{aligned}&H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(\ell-c)}\mathbf{P}^t_{B,L_\ell}\mathbf{V}_B^{[t-1]})\\ &\geq \sum_{r=\ell+1}^{h} H(\mathbf{P}^t_{B,r}) + H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(h-c)}\mathbf{P}^t_{B,L_h}\mathbf{V}_B^{[t-1]}).\end{aligned} \tag{9}$$

Let us consider the two random variables $\mathbf{A} = \mathbf{X}^t_{B,(h-c)}\mathbf{P}^t_{B,L_h}$ and $\mathbf{E} = \mathbf{V}_B^{[t]}$. Using equations (7) and (8), one can prove that $H(\mathbf{X}^t_{B,(h-c)}\mathbf{P}^t_{B,L_h}|\mathbf{V}_B^{[t]}) = 0$.
Hence, $\mathbf{A}$ and $\mathbf{E}$ satisfy the hypothesis of Lemma 2.1, and one has

$$\begin{aligned}&H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(h-c)}\mathbf{P}^t_{B,L_h}\mathbf{V}_B^{[t-1]})\\ &\geq H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(h-c)}\mathbf{P}^t_{B,L_h}\mathbf{V}_B^{[t]}) \text{ (from (24) of Appendix)}\\ &= H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{V}_B^{[t]}) \text{ (from Lemma 2.1).}\end{aligned} \tag{10}$$

It follows that

$$\begin{aligned}&H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{X}^t_{B,(\ell-c)}\mathbf{P}^t_{B,L_\ell}\mathbf{V}_B^{[t-1]})\\ &\geq \sum_{r=\ell+1}^{h} H(\mathbf{P}^t_{B,r}) + H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{V}_B^{[t]}) \text{ (from (9)–(10))}\\ &\geq H(\mathbf{P}^t_{B,L_h}) + H(\mathbf{C}_1|\mathbf{C}_2\ldots\mathbf{C}_c\mathbf{V}_B^{[t]}) \text{ (from (21) of Appendix).}\end{aligned}$$

Then, the lemma follows from the above inequality and from (24) of Appendix which implies

$$H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_c\mathbf{V}_B^{[t-1]}) \geq H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_c\mathbf{X}^t_{B,(\ell-c)}\mathbf{P}^t_{B,L_\ell}\mathbf{V}_B^{[t-1]}).$$

□

The next theorem provides a lower bound on the information distributed to clients in metering schemes with pricing. The theorem implies Corollary 4.6, which states that the information that must be kept secret by clients grows linearly with the number of time frames the scheme must be active, the size of coalition of servers, and the "granularity" (i.e., $h-\ell$) of the system itself.

THEOREM 4.5. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ metering scheme with pricing. Let B, with $|B| = \beta \leq s$, be a set of indices of corrupt servers. For any $i = 1, \dots, n$, it holds that*

$$H(\mathbf{C}_i) \geq \sum_{t=1}^{\tau} H(\mathbf{P}^t_{B,L_h}), \quad \textit{for } i = 1, \dots, n.$$

Proof. W.l.o.g. we will assume that $\mathcal{C}_1, \dots, \mathcal{C}_c$ are the corrupt clients and prove the bound for $\mathcal{C}_1$.
Starting from $H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_c\mathbf{V}_B^{[0]})$ and iteratively applying Lemma 4.4, we get

$$H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_c\mathbf{V}_B^{[0]}) \geq \sum_{t=1}^{\tau} H(\mathbf{P}^t_{B,L_h}) + H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_c\mathbf{V}_B^{[\tau]}). \tag{11}$$

Hence, one has

$$\begin{aligned} H(\mathbf{C}_1) &\geq H(\mathbf{C}_1|\mathbf{C}_2\dots\mathbf{C}_c\mathbf{V}_B^{[0]}) \text{ (from (24) of Appendix)} \\ &\geq \sum_{t=1}^{\tau} H(\mathbf{P}^t_{B,L_h}) \text{ (from (11) and (18) of Appendix) .} \end{aligned}$$

Then, the theorem follows. □

Notice that in Section 2 we did not say anything on the entropies of random variables $\mathbf{P}^t_{j,f}$ and $\mathbf{P}^t_{j,L_f}$, for $j \in \{1, \dots, m\}$, $f \in \{\ell+1, \dots, h\}$, and $t \in \{1, \dots, \tau\}$. Our results apply to the general case of arbitrary entropies, but for clarity, we state the next corollary for the simpler case that $H(\mathbf{P}^{t_1}_{j_1,f_1}) = H(\mathbf{P}^{t_2}_{j_2,f_2})$ and $H(\mathbf{P}^{t_1}_{j_1,L_f}) = H(\mathbf{P}^{t_2}_{j_2,L_f})$, for all $j_1, j_2 \in \{1, \dots, m\}$, $f_1, f_2, f \in \{\ell+1, \dots, h\}$, and $t_1, t_2 \in \{1, \dots, \tau\}$. We denote these common entropies by $H(\mathbf{P})$ and $H(\mathbf{P}_{L_f})$, respectively. If the proof sequences of the corrupt servers are statistically independent, then the following corollary holds.

COROLLARY 4.6. *In any $(n, m, \tau, c, s, \ell, h)$ metering scheme with pricing in which the proofs of corrupt servers are statistically independent, it holds that*

$$H(\mathbf{C}_i) \geq s\tau H(\mathbf{P}_{L_h}), \ \textit{for} \ \ i = 1, \dots, n.$$

If for any server $\mathcal{S}_j$ the random variables $\mathbf{P}^t_{j,\ell+1}, \dots, \mathbf{P}^t_{j,h}$ are statistically independent, i.e.,

$$H(\mathbf{P}^t_{j,L_h}) = \sum_{f=\ell+1}^{h} H(\mathbf{P}^t_{j,f}),$$

then Corollary 4.6 implies $H(\mathbf{C}_i) \geq s\tau(h-\ell)H(\mathbf{P})$, for $i = 1, \ldots, n$. Moreover, if the random variable $\mathbf{P}$ is uniformly distributed in a finite field F then $H(\mathbf{P}) = \log|F|$. Consequently, the size of the information owned by a client is lower bounded by $s\tau(h-\ell)\log|F|$ and from Eq. (17) it follows that

$$\log|C_i| \geq s\tau(h-\ell)\log|F|, \text{ for } i = 1, \ldots, n. \tag{12}$$

In Section 4.2 we will present an $(n, m, \tau, c, s, \ell, h)$ metering scheme with pricing which achieves it.

A Lower Bound on the Size of Servers' Secret Information. In the following we provide a lower bound on the size of the information given to servers by clients in metering schemes with pricing. To prove the bound we need the following lemma.

Lemma 4.7. *Let $\mathcal{M}$ be an $(n, m, \tau, c, s, \ell, h)$ metering scheme with pricing. For $j = 1, \ldots, m$, $t = 1, \ldots, \tau$, and $r = \ell+1, \ldots, h$, let $X^t_{j,(r-1)}$ be a set of visits from $r-1$ clients other than $\mathcal{C}_i$ to server $\mathcal{S}_j$ in time frame t. Then, for any $i = 1, \ldots, n$, $j = 1, \ldots, m$, $t = 1, \ldots, \tau$, and $r = \ell+1, \ldots, h$, it holds that*

$$H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_{r-1}}) \geq H(\mathbf{P}^t_{j,r}) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(r)}\mathbf{P}^t_{j,L_r}).$$

Proof. Let $\mathbf{A}' = \mathbf{P}^t_{j,L_{r-1}}$, $\mathbf{D} = \mathbf{C}^t_{i,j}$, $\mathbf{E} = \mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_{r-1}}$, $\mathbf{E}' = \mathbf{X}^t_{j,(r-1)}$, and $\mathbf{F} = \mathbf{P}^t_{j,r}$. If $\ell+2 \leq r \leq h$, then from Property 2 of Definition 4.1 one has $H(\mathbf{P}^t_{j,L_{r-1}}|\mathbf{X}^t_{j,(r-1)}) = 0$. If $r = \ell+1$ then $P^t_{j,L_\ell} = \emptyset$ and consequently $H(\mathbf{P}^t_{j,L_\ell}|\mathbf{X}_{j,(\ell)}) = 0$. Hence, one has that the random variables $\mathbf{A}'$ and $\mathbf{E}'$ satisfy the hypothesis of Lemma 2.1 and consequently $H(\mathbf{F}|\mathbf{A}'\mathbf{E}') = H(\mathbf{F}|\mathbf{E}')$. Then, it results that

$$\begin{aligned}
H(\mathbf{P}^t_{j,r}|\mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_{r-1}}) &= H(\mathbf{P}^t_{j,r}|\mathbf{X}^t_{j,(r-1)}) \text{ (from Lemma 2.1)}\\
&\geq H(\mathbf{P}^t_{j,r}|\mathbf{X}^t_{j,(r-1)}\mathbf{V}^{[t-1]}_j) \text{ (from (24) of Appendix)}\\
&= H(\mathbf{P}^t_{j,r}) \text{ (from Property 3 of Definition 4.1).}
\end{aligned}$$

From the above inequality and from (24) of Appendix which implies

$$H(\mathbf{P}^t_{j,r}|\mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_{r-1}}) \leq H(\mathbf{P}^t_{j,r}),$$

it follows that

$$H(\mathbf{P}^t_{j,r}|\mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_{r-1}}) = H(\mathbf{P}^t_{j,r}). \tag{13}$$

Moreover, it results that

$$\begin{aligned}
H(\mathbf{P}^t_{j,r}|\mathbf{X}^t_{j,(r-1)}\mathbf{C}^t_{i,j}\mathbf{P}^t_{j,L_{r-1}}) &\leq H(\mathbf{P}^t_{j,r}|\mathbf{X}^t_{j,(r-1)}\mathbf{C}^t_{i,j}) \text{ (from (24) of Appendix)}\\
&= 0 \text{ (from Property 2 of Definition 4.1).} \qquad (14)
\end{aligned}$$

Equations (13)–(14) imply that the random variables $\mathbf{D}$, $\mathbf{E}$, and $\mathbf{F}$ satisfy the hypothesis of Lemma 2.2, and consequently one has $H(\mathbf{D}|\mathbf{E}) = H(\mathbf{F}) + H(\mathbf{D}|\mathbf{EF})$. Hence, one gets

$$\begin{aligned} H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_{r-1}}) &= H(\mathbf{P}^t_{j,r}) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_{r-1}}\mathbf{P}^t_{j,r}) \text{ (from Lemma 2.2)} \\ &= H(\mathbf{P}^t_{j,r}) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(r-1)}\mathbf{P}^t_{j,L_r}) \\ &\geq H(\mathbf{P}^t_{j,r}) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(r)}\mathbf{P}^t_{j,L_r}) \text{ (from (24) of Appendix).} \end{aligned}$$

Thus, the lemma follows. □

The next theorem provides another lower bound on the communication complexity of metering schemes with pricing. It implicitly shows that the size of the information each client has to give out when visiting a server is lower bounded by the size of the proofs the server could reconstruct.

THEOREM 4.8. *In any $(n, m, \tau, c, s, \ell, h)$ metering scheme with pricing it holds that*

$$H(\mathbf{C}^t_{i,j}) \geq H(\mathbf{P}^t_{j,L_h}),$$

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

Proof. Starting from $H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(\ell)}\mathbf{P}^t_{j,L_\ell})$ and iteratively applying Lemma 4.7, one gets

$$\begin{aligned} H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(\ell)}\mathbf{P}^t_{j,L_\ell}) &\geq \sum_{r=\ell+1}^{h} H(\mathbf{P}^t_{j,r}) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h)}\mathbf{P}^t_{j,L_h}) \\ &\geq H(\mathbf{P}^t_{j,L_h}) + H(\mathbf{C}^t_{i,j}|\mathbf{X}^t_{j,(h)}\mathbf{P}^t_{j,L_h}) \text{ (from (20) of Appendix)} \\ &\geq H(\mathbf{P}^t_{j,L_h}) \text{ (from (18) of Appendix).} \end{aligned}$$

The theorem follows from the above inequality and from (18) of Appendix. □

If for any server $\mathcal{S}_j$ the variables $\mathbf{P}^t_{j,\ell+1}, \ldots, \mathbf{P}^t_{j,h}$ are statistically independent then Theorem 4.8 implies $H(\mathbf{C}^t_{i,j}) \geq \sum_{f=\ell+1}^{h} H(\mathbf{P}^t_{j,f})$, for any $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$. Moreover if $\mathbf{P}^t_{j,\ell+1}, \ldots, \mathbf{P}^t_{j,h}$ are uniformly distributed in a finite field F, one has

$$\log|C^t_{i,j}| \geq (h-\ell)\log|F|, \text{ for } i = 1, \ldots, n,\ j = 1, \ldots, m, \text{ and } t = 1, \ldots, \tau. \tag{15}$$

4.2. A Protocol for Metering Schemes with Pricing. In this section we present an unconditionally secure $(n, m, \tau, c, s, \ell, h)$ metering scheme with pricing achieving the bounds (12) and (15) of Section 4.1. The proofs are points of a finite field $GF(q)$ where q is a large prime.

Analysis of the Scheme. It is immediate to verify that the scheme satisfies Property 1 of Definition 4.1. Indeed, for any $i = 1, \ldots, n$, the information given by the audit agency to the client $\mathcal{C}_i$ consists of the univariate polynomials $P_{\ell+1}(i, y), \ldots, P_h(i, y)$, and for any $j = 1, \ldots, m$, the information given to the server $\mathcal{S}_j$ by client $\mathcal{C}_i$ is obtained by evaluating the univariate polynomials $P_{\ell+1}(i, y), \ldots, P_h(i, y)$ at $j \circ t$.

It is also easy to verify that the scheme satisfies Property 2 of Definition 4.1. Assume that a server $\mathcal{S}_j$ has been visited by f, with $\ell + 1 \leq f \leq h$, clients in time

Initialization:

- The audit agency $\mathcal{A}$ chooses $h-\ell$ random bivariate polynomials $P_{\ell+1}(x,y),\ldots,P_h(x,y)$ over $GF(q)$, where, for $z=\ell+1,\ldots,h$, the polynomial $P_z(x,y)$ is of degree $z-1$ in x and degree $s\tau-1$ in y.
- $\mathcal{A}$ sends the $h-\ell$ univariate polynomials $P_{\ell+1}(i,y),\ldots,P_h(i,y)$, which are of degree $s\tau-1$, to each client $\mathcal{C}_i$.

Regular Operation for Time Frame t:

When the client $\mathcal{C}_i$ visits the server $\mathcal{S}_j$ in time frame t, it sends the $h-\ell$ points $P_{\ell+1}(i,j\circ t)$, $\ldots,P_h(i,j\circ t)$ to $\mathcal{S}_j$.

Proof Generation and Verification for Time Frame t:

- Assume that the server $\mathcal{S}_j$ has been visited by a number z of clients, $\ell<z\leq h$, in time frame t.
- The server $\mathcal{S}_j$ performs a Lagrange interpolation of the polynomial $P_z(x,j\circ t)$ and computes the value $P_z(0,j\circ t)$. This value constitutes the z-proof of $\mathcal{S}_j$, i.e., the proof that $\mathcal{S}_j$ has received z visits.
- The server $\mathcal{S}_j$ sends the pair $(P_z(0,j\circ t),z)$ to the audit agency.
- The audit agency verifies the proof by evaluating the polynomial $P_z(x,y)$ at the point $(0,j\circ t)$.

FIG. 2. *An (n,m,τ,c,s,ℓ,h) metering scheme with pricing.*

frame t. Then, the server knows f points of each of the polynomials $P_{\ell+1}(x,j\circ t),\ldots,P_f(x,j\circ t)$. Since these polynomials are all of degree less than or equal to $f-1$ in x, then the server can compute their coefficients by using Lagrange interpolation. In particular, it can compute its f-proof for t by evaluating the polynomial $P_f(x,j\circ t)$ at 0. If the server $\mathcal{S}_j$ has been visited by a number of clients greater than or equal to h in time frame t, then it can reconstruct all the $h-\ell$ polynomials. Hence, the server can reconstruct all the proofs for the time frame t.

To prove that our scheme satisfies Property 3 of Definition 4.1, we consider the worst possible case that in any time frame $t=1,\ldots,\tau$, all corrupt clients decide to cooperate with all corrupt servers and that corrupt servers have collected the maximum possible information during the previous time frames $1,\ldots,t-1$. In other words, for any time frame $t=1,\ldots,\tau$, we assume that each corrupt client $\mathcal{C}_i$ gives its polynomials $P_{\ell+1}(i,y),\ldots,P_h(i,y)$ to all corrupt servers, and that any corrupt server $\mathcal{S}_j$ knows the polynomials $P_{\ell+1}(x,j\circ t'),\ldots,P_h(x,j\circ t')$, for $t'=1,\ldots,t-1$. Without loss of generality, let $\mathcal{S}_1,\ldots,\mathcal{S}_s$ be a coalition of corrupt servers. In order to prove that our scheme satisfies Property 3 of Definition 4.1, we need to prove that for any time frame $t = 1, \ldots, \tau$, and for any $z = \ell + 1, \ldots, h$, the coalition of corrupt servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ is not able to calculate the proofs $P_z(0, 1 \circ t), \ldots, P_z(0, j_s \circ t)$ if each server in the coalition receives less than $z - c$ regular visits in time frame t. In order to calculate $P_z(0, j \circ t)$, the servers should be able to interpolate either the polynomial $P_z(x, j \circ t)$ or the bivariate polynomial $P_z(x, y)$. The information that a corrupt client $\mathcal{C}_i$ gives to a corrupt server is equivalent to the $s\tau$ coefficients of each of the polynomials $P_{\ell+1}(i, y), \ldots, P_h(i, y)$. For $j = 1, \ldots, s$, the information collected by each corrupt server $\mathcal{S}_j$ during the previous time frames is equivalent to the coefficients of the polynomials $P_{\ell+1}(x, j \circ t'), \ldots, P_h(x, j \circ t')$, for any $t' = 1, \ldots, t - 1$. Suppose that in time frame t, the server $\mathcal{S}_j$, $j \in \{1, \ldots, s\}$, receives g_j^t regular visits. Then, the overall information on $P_z(x, y)$ held by the servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ consists of

$$cs\tau + s(t-1)z + \sum_{j=1}^{s} g_j^t - cs(t-1) \tag{16}$$

points. The first term of (16) corresponds to the information given by the c corrupt clients, the second term corresponds to the information collected by all servers in the coalition during the previous time frames, the third term corresponds to the information provided by the client visits in time frame t, and the last term represents the information which has been counted twice. For any $z = \ell + 1, \ldots, h$, we will prove that the servers in the coalition are unable to interpolate the polynomial $P_z(x, y)$ if each server in the coalition receives less than $z - c$ regular visits. Notice that, for any $j = 1, \ldots, s$, $t = 1, \ldots, \tau$ and $z = \ell + 1, \ldots, h$, if $g_j^t < z - c$, then expression (16) is strictly less than $zs\tau$. Consequently, for any choice of $a \in GF(q)$ and for any $j = 1, \ldots, s$, there is a polynomial $R(x, y)$ which is consistent with the information held by the servers in the coalition and such that $R(0, j \circ t) = a$. Hence, the corrupt servers $\mathcal{S}_1, \ldots, \mathcal{S}_s$ have probability at most $1/q$ of guessing the z-proof $P_z(0, j \circ t)$, for any $j = 1, \ldots, s$ and any time frame $t = 1, \ldots, \tau$. Notice that instead of computing all the coefficients of the polynomial $P_z(x, j \circ t)$ and then evaluating the polynomial in the point 0, the servers could only compute the free coefficients of the polynomial.

From the above discussion it follows that both in the case when $\mathcal{S}_1 \ldots, \mathcal{S}_s$ are trying to interpolate the bivariate polynomial $P_z(x, y)$, and in the case when $\mathcal{S}_1 \ldots, \mathcal{S}_s$ are trying to interpolate the polynomial $P_z(x, j \circ t)$, the probability that they guess one of the z-proofs $P_z(0, 1 \circ t), \ldots, P_z(0, s \circ t)$ is at most $1/q$. Consequently, the probability that a coalition of s corrupt servers guesses the whole vector of proofs $(P_z(0, 1 \circ t), \ldots, P_z(0, s \circ t))$ is at most $1/q^s$.

Efficiency of the Scheme. It is easy to see that the scheme meets the bounds (12) and (15) of Section 4.1. Indeed, the size of the information given to any client is $(h - \ell)s\tau \log q$, whereas the size of the information that each server receives from a client during a regular visit is $(h - \ell) \log q$.

Hence, our protocol is optimal both with respect to the size of the information distributed to clients and with respect to the size of information given to servers by clients.

5. Conclusions. In this paper we have introduced two generalizations of Naor and Pinkas metering schemes [10]: *ramp metering schemes* [5] and *metering schemes with pricing* [2]. We have analyzed the efficiency of these schemes in terms of the information exchanged among the parties. In the following we summarize the comparison between Naor and Pinkas metering schemes [10] and our schemes. As for ramp metering schemes, they enable to reduce the size of the information distributed to the parties by a factor of $h - \ell$ at the price of a loss in security. The lower is the difference $h - \ell$, the smaller is the range of values $k < h$ such that a server which receives k visits is able to gain some information about its proof. As for metering schemes with pricing they provide a more flexible payment system at the expense of an increasement of a factor $h-\ell$ in the overall communication complexity, where $h-\ell$ is the number of different payments associated to client visits.

We have assumed that clients provide correct shares when they visit servers. Naor and Pinkas [10] have also considered the case when clients try to disrupt the metering process sending incorrect information to the visited servers. This problem has been also addressed by Ogata and Kurosawa [12], who proposed a scheme in which any server can verify with non-negligible probability that the shares received by clients are correct. Moreover, we have assumed that the schemes can be used for a fixed number τ of time frames, which is a parameter of the schemes. Naor and Pinkas [10] have also proposed schemes that can be used for a number of time frames which is not fixed a priori. The security of their schemes is based on the assumed intractability of the computational Diffie-Hellman problem.

Acknowledgements. We would like to thank the anonymous referees for their useful comments.

Appendix. Information Theory Background. In this Appendix 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, the Shannon *entropy* of $\mathbf{X}$, denoted by $H(\mathbf{X})$, is defined as

$$H(\mathbf{X}) = -\sum_{x\in X} Pr_{\mathbf{X}}(x)\log Pr_{\mathbf{X}}(x)$$

(all logarithms in this paper are to the base 2). The entropy $H(\mathbf{X})$ is a measure of the average uncertainty one has about which element of the set X has been chosen when the choices of the elements from X are made according to the probability distribution $\{Pr_{\mathbf{X}}(x)\}_{x\in X}$. It is well known that $H(\mathbf{X})$ is a good approximation to the average number of bits needed to faithfully represent the elements of X.
The entropy satisfies the following property:

$$0 \le H(\mathbf{X}) \le \log|X|, \tag{17}$$

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

$$H(\mathbf{X}|\mathbf{Y}) \geq 0. \tag{18}$$

We have that $H(\mathbf{X}|\mathbf{Y}) = 0$ when the value chosen from Y completely determines the value chosen from X; whereas, $H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X})$ means that choices from X and Y are independent, that is, the probability that the value x has been chosen from X given that from Y we have chosen y is the same as the *a priori* probability of choosing x from X. Therefore, knowing the values chosen from Y does not enable a Bayesian opponent to modify an *a priori* guess regarding which element has been chosen from X.

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

$$H(\mathbf{X}_1 \ldots \mathbf{X}_n) = H(\mathbf{X}_1) + \sum_{i=2}^{n} H(\mathbf{X}_i | \mathbf{X}_1 \ldots \mathbf{X}_{i-1}) \tag{19}$$

and

$$H(\mathbf{X}_1 \ldots \mathbf{X}_n) \leq \sum_{i=1}^{n} H(\mathbf{X}_i). \tag{20}$$

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

$$H(\mathbf{X}_1 \ldots \mathbf{X}_n | \mathbf{Y}) \leq \sum_{i=1}^{n} H(\mathbf{X}_i | \mathbf{Y}). \tag{21}$$

Given three sets X, Y, Z and a joint probability distribution on their cartesian product, the *conditional mutual information* $I(\mathbf{X}; \mathbf{Y}|\mathbf{Z})$ between $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{Z}$ is

$$I(\mathbf{X}; \mathbf{Y}|\mathbf{Z}) = H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{Z}\mathbf{Y}) \tag{22}$$

and satisfies the following properties:

$$I(\mathbf{X}; \mathbf{Y}|\mathbf{Z}) = I(\mathbf{Y}; \mathbf{X}|\mathbf{Z}) \tag{23}$$

and $I(\mathbf{X}; \mathbf{Y}|\mathbf{Z}) \geq 0$. Since the conditional mutual information is always non-negative we get

$$H(\mathbf{X}|\mathbf{Z}) \geq H(\mathbf{X}|\mathbf{Z}\mathbf{Y}). \tag{24}$$

Parameters and Variables Frequently Used in the Paper.

ℓ, h	thresholds
n	number of clients
m	number of servers
τ	number of time frames
c	number of corrupt clients
s	number of corrupt servers
$\mathbf{C}_i$	information distributed to client $\mathcal{C}_i$
$\mathbf{C}_{i,j}^t$	visit from client $\mathcal{C}_i$ to server $\mathcal{S}_j$ in time frame t
$B = \{j_1, \ldots, j_\beta\}$	indices of the corrupt servers, $\beta \leq s$
$\mathbf{C}_{i,B}^t$	visits from client $\mathcal{C}_i$ to servers $\mathcal{S}_{j_1}, \ldots, \mathcal{S}_{j_\beta}$ in time frame t
$\mathbf{X}_{j,(d_j)}^t$	visits from d_j clients to server $\mathcal{S}_j$ in time frame t
$\mathbf{X}_{B,(z)}^t$	visits from z clients to servers $\mathcal{S}_{j_1}, \ldots, \mathcal{S}_{j_\beta}$ in time frame t
$\mathbf{V}_j^{[t]}$	information collected by server $\mathcal{S}_j$ in time frames $1, \ldots, t$
$\mathbf{V}_B^{[t]}$	information collected by servers $\mathcal{S}_{j_1}, \ldots, \mathcal{S}_{j_\beta}$ in time frames $1, \ldots, t$
$\mathbf{P}_{j,f}^t$	f-proof for server $\mathcal{S}_j$, where $f \in \{\ell + 1, \ldots, h\}$
$\mathbf{P}_{B,f}^t$	f-proofs for servers $\mathcal{S}_{j_1}, \ldots, \mathcal{S}_{j_\beta}$
$L_r = \{\ell + 1, \ldots, r\}$	indices of proofs, where $r \in \{\ell + 1, \ldots, h\}$
$\mathbf{P}_{j,L_r}^t$	$(\ell + 1)$-proof,. . . r-proof for server $\mathcal{S}_j$
$\mathbf{P}_{B,L_r}^t$	$(\ell + 1)$-proofs,. . . r-proofs for servers $\mathcal{S}_{j_1}, \ldots, \mathcal{S}_{j_\beta}$

REFERENCES

[1] V. Anupam, A. Mayer, K. Nissim, B. Pinkas, and M. K. Reiter, *On the Security of Pay-Per-Click and Other Web Advertising Schemes*, Computer Networks, 31(1999), pp. 1091–1100.

[2] C. Blundo, A. De Bonis, and B. Masucci, *Metering Schemes with Pricing*, in Proceedings of the 14th International Conference on Distributed Computing (DISC 2000), Lecture Notes in Computer Science, Vol. 1914, pp. 194–208, 2000.

[3] C. Blundo, A. De Bonis, B. Masucci, and D. R. Stinson, *Dynamic Multi-Threshold Metering Schemes*, in Proceedings of Selected Areas in Cryptography (SAC 2000), Lecture Notes in Computer Science, Vol. 2012, pp. 130–143, 2001.

[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*, in Proceedings of 2000 IEEE International Symposium on Information Theory (ISIT 2000), 49, 2000.

[6] M. Franklin and D. Malkhi, *Auditable Metering with Lightweight Security*, Journal of Computer Security, 6:4(1998), pp. 237–255.

[7] M. Jakobsson, P. D. MacKenzie, and J. P. Stern, *Secure and Lightweight Advertising on the Web*, 8th International World Wide Web Conference, 1999.

[8] B. Masucci and D. R. Stinson, *Metering Schemes for General Access Structures*, in Proceedings of 6th European Symposium on Research in Computer Security - ESORICS 2000, Lecture Notes in Computer Science, Vol. 1895, pp. 72–87, 2000.

[9] B. Masucci and D. R. Stinson, *Efficient Metering Schemes with Pricing*, IEEE Transactions on Information Theory, 47:7(2001), pp. 2835–2844.

[10] M. Naor and B. Pinkas, *Secure and Efficient Metering*, in Proceedings of Advances in Cryptology - EUROCRYPT '98, Lecture Notes in Computer Science, Vol. 1403, pp. 576–590, 1998.

[11] M. Naor and B. Pinkas, *Secure Accounting and Auditing on the Web*, Computer Networks and ISDN Systems, 40:1-7(1998), pp. 541-550.

[12] W. Ogata and K. Kurosawa, *Provably Secure Metering Schemes*, in Proceedings of Advances in Cryptology - ASIACRYPT 2000, Lecture Notes in Computer Science, Vol. 1976, pp. 388–398, 2000.

[13] M. K. Reiter, V. Anupam, and A. Mayer, *Detecting Hit Shaving in Click-Through Payment Schemes*, in Proceedings of 3rd USENIX Workshop on Electronic Commerce, pp. 155–166, 1998.

[14] A. Shamir, *How to Share a Secret,* Communications of the ACM, 22(1979), pp. 612–613.