
Designs, Codes and Cryptography, 36, 5–27, 2005

A General Approach to Robust Web Metering

S. G. BARWICK sbarwick@maths.adelaide.edu.au
Department of Pure Mathematics, University of Adelaide Adelaide 5005, Australia

WEN-AI JACKSON
Department of Pure Mathematics, University of Adelaide Adelaide 5005, Australia

KEITH M. MARTIN keith.martin@rhul.ac.uk
Information Security Group, Royal Holloway, University of London Egham, Surrey TW20 0EX, UK

Communicated by: P. Wild

Received November 13, 2002; Revised November 13, 2002; Accepted August 21, 2003

Abstract. We consider the problem of metering access to web sites. Many services, such as web advertising, have a need for accurate counts of the number of visits to a web site. We consider the robust approach to web metering by looking at techniques that provide secure proofs of visit. We refine a number of previous models for metering schemes and provide a general construction for secure and efficient schemes that meter the interaction of a web site with a targeted audience. We generalise a technique for determining the minimum information that clients in the web site audience need to secure in order to supply proofs of visit. We also show how our metering schemes can be made robust against corrupt clients who attempt to prevent web servers constructing legitimate proofs of visit.

Keywords: metering schemes, web metering, information theoretic bounds, geometric constructions

AMS Classification: 94A60

1. Introduction

The Internet has enabled a myriad of new business and service opportunities, with many more undoubtedly on the horizon. While the ability of the Internet community to perceive these new opportunities has been unrestrained, the techniques for directly exploiting them commercially have been surprisingly slow to develop. The expectations for electronic commerce have resulted in almost all commercial organisations establishing web presences, with their obvious market benefits as information hubs for self-promotional activities. However, comparatively few processes have emerged for obtaining more direct types of revenue from this potentially enormous resource. This has been partly due to a general uncertainty about the exact nature of the Internet as a marketplace, but also due to the lack of obvious revenue enabling technologies, and to a degree these two issues go hand in hand.

There have been numerous suggestions for how direct revenue could be made from the web. Apart from the obvious Internet shopping applications, these

suggestions include selling web pages themselves (information services), selling connectivity and selling advertising. The charging of information services is one of the most intriguing of these and various lightweight micropayment technologies, for example [18, 24], have been proposed for handling such payments. Despite these new developments, the selling of advertising is currently the most familiar revenue earning activity on the web. While other processes may emerge in the near future, projections such as those of Lesk [17] foresee an Internet trading place where selling advertising plays a substantial role in financing web-based services.

Inserting the search phrase "pay-per-click" into any of the well-known search engines will return hundreds of web sites claiming to offer money in exchange for referrals from sites bearing advertising banners that link to specified target web sites. The payment to the web site host for these referrals is often based simply on a count of unique referring IP addresses. Such systems are not secure against basic *hit inflation attacks*, where a knowledgeable referrer defrauds the target web site by artificially inflating the click-through count that the referrer is due to be paid [1]. A more basic procedure, even more prone to hit inflation, is simply to enumerate the number of visits a banner bearing web site receives and to reward the owner appropriately. Such procedures only make sense in the presence of reliable *meters* that accurately count visits to a web site. There have been a number of suggestions for lightweight metering schemes that are efficient to run and do provide a degree of security against hit inflation [11, 16]. The security of these lightweight schemes is traded off against efficiency in a similar way to that of the aforementioned micropayment schemes. While making this kind of trade-off is entirely justifiable in some cases, for many applications there may be an amount of discomfort about how the level of trade-off can safely be determined.

In [21, 22] secure and robust metering schemes that provide a short proof of visit by a client to a web site were first presented. These metering schemes involve clients holding secret information from which the proof of visit can be generated. While this is not as simple a solution to enable as some of the more lightweight alternatives, there is no doubt that in many cases the greater security of this robust approach is preferable. Further, secure metering services can also be used for applications such as network accounting and electronic coupon management [22]. In this paper we adopt this *robust* approach to web metering and follow on from the work of [3, 9, 19, 23] in further developing the original ideas in [21]. In particular, we will provide a new general construction for securely metering the interaction of a web site with a targeted audience.

2. Metering Schemes

2.1. Framework and Terminology

In the robust web metering model [21] there is a set $\mathcal{S} = \{S_1, \ldots, S_m\}$ of *servers*, all of whom are hosts of banner-bearing web sites. The *audience* for these servers is a set $\mathcal{C} = \{C_1, \ldots, C_n\}$ of *clients*, all of whom may pay *visits* to any of the servers in $\mathcal{S}$. The *audit agency* is an entity trusted by both the clients and the

servers to initiate a metering scheme and to monitor the metering process. The life cycle of a metering scheme is divided into a number of *time frames*. Each of the servers wishes to earn money by proving to the audit agency that it has received visits from specified groups of clients in the audience within a single time frame.

The *targeted audience* Γ of a metering scheme is the collection of subsets of clients in the audience whose visits to any server in a single time frame will result in that server being financially rewarded. In other words, for any $1 \leq j \leq m$, during any time frame t,

$$S_j \text{ will be rewarded} \iff S_j \text{ has been visited by every member from a set } A \in \Gamma.$$

The targeted audience Γ is clearly *monotone*, in other words if $A \in \Gamma$ and $A \subseteq B \subseteq \mathscr{C}$ then $B \in \Gamma$.

To initialise a metering scheme the audit agency securely issues each client with a client-specific piece of secret information called a *share*. Each time a client visits a server the client presents the server with some *evidence*, which is a value computed from the identity of the server, the client's share and the current time frame. Once the server has received sufficient evidence within a single time frame then it is able to use this to compute a *proof of visit* (or *proof*). A good metering scheme should thus have the property that for any $1 \leq j \leq m$, during any time frame t,

$$S_j \text{ can compute a proof} \iff S_j \text{ has received evidence from every client in a set } A \in \Gamma.$$

The proof of visit is then presented by the server to the audit agency. If the proof is verified as being correct by the audit agency then the server receives the agreed renumeration for its services.

2.2. *Threat Environment and Requirements*

The main threat that our metering schemes are designed to counter is hit inflation. We consider the security assumptions concerning the entities in the robust metering model.

Audit agency. The audit agency is essentially a trusted third party, trusted by clients and servers. It is assumed that the audit agency issues each client with a correct share and transfers it to the client by means of a secure channel. Servers also have access to a secure channel in order to submit proofs of visit to the audit agency. Servers trust the judgment of the audit agency as to whether they have submitted a valid proof of visit.

Clients. Honest clients are expected to keep their shares securely stored and to securely issue valid evidence to any server that they visit. Corrupt clients may collude with corrupt servers in order to assist the server in a hit inflation attack. Our model requires that a set of corrupt clients is not in the targeted audience. This is reasonable since sets in the targeted audience are likely to be much larger than a viable coalition of corrupt clients. Our basic model assumes that clients do not attempt to defraud a server by presenting invalid evidence. We discuss extensions to this model in Section 6 for coping with scenarios of this type.

Servers. Honest servers are expected to keep secure all evidence that they receive from clients and not to share this with other servers. Corrupt servers may collude with other servers, and/or clients, in order to compute a false proof of visit. We place a limit on the number of corrupt servers who can collude (this number can be traded off against scheme efficiency).

We now consider a number of other requirements of the robust metering environment.

Efficiency. It is important to keep all secure information components as small as possible in order to reduce storage and processing costs. The size of a proof of visit can be chosen to be as small as required. The most important component to minimise is the size of a client's share, and we discuss this in Section 4.

Life cycle. The metering schemes we discuss are designed to operate over a predetermined number of time frames. At the end of the last time frame a metering scheme needs to reinitialised and new shares issued to the clients. We discuss the options for having metering schemes with unlimited lifetimes in Section 6.

Security model. We concentrate on the design of metering schemes offering unconditional security. We discuss the relaxing of this demanding security requirement to computational security in Section 6, and the trade-offs that this involves.

2.3. Context of Contribution

The robust approach to web metering was first proposed in [21]. Like most authors they restricted their interest to *threshold metering*, where the targeted audience is the collection of all subsets of clients in the audience of at least some fixed threshold size k. A polynomial-based threshold metering scheme was proposed and several extensions were discussed.

This work formed the basis for a number of subsequent research efforts. A formal model for unconditionally secure metering schemes was given in [3]. This model was extended in [19] to cover general classes of targeted audience. Recently, in [5], this construction was generalised to a further specific class of targeted audiences. In [19] a lower bound on the size of a client's share was deduced and a number of polynomial-based constructions for specific classes of targeted audience were described. In [4] the model was slightly adjusted to cope with different targeted audiences in different time frames. The extension of these ideas to cover situations where different levels of enumeration are offered for different numbers of server visits was considered for threshold metering in [2,20]. Finally, in [23] a minor flaw in one of the extensions of the threshold metering scheme of [21] was noted and a correction was proposed.

In this paper we further develop this work by making the following contributions, each of which is presented in its own subsequent section:

- *Model*—we propose a stronger model for metering schemes than that in [3,19].
- *Bound on client share size*—we describe a general technique for obtaining bounds on the size of client's shares that generalises the work of [3,19].

- *Constructions*—we generalise the isolated efficient constructions of [19,21] to give a more efficient general construction technique for metering schemes for any targeted audience.
- *Extensions*—we describe how to adjust our general construction method to allow for practical extensions such as verifiable evidence and proofs of visit, unlimited usage and dynamicity of targeted audience.

3. Modelling Metering Schemes

3.1. Information Theory

We provide a short introduction to entropy here but refer the reader to, for example, [8] for details.

Let A and B be finite sets. To simplify the notation, we will use AB to denote $A \cup B$ and x for the singleton set $\{x\}$. Let X be a finite set and let $\langle X \rangle$ be a finite collection of tuples, such that the entries of a tuple $\pi \in \langle X \rangle$ are indexed by the elements of X. Let ρ be a probability distribution on $\langle X \rangle$. For $\pi = (\pi_x)_{x \in X} \in \langle X \rangle$ and $A \subseteq X$, let $\pi_A = (\pi_x)_{x \in A}$ and let $\langle A \rangle = \{\pi_A | \pi \in X\}$. Let ρ_A be the marginal distribution on A, that is, ρ_A is the probability distribution on $\langle A \rangle$ such that for $\alpha \in \langle A \rangle$ we have $\rho_A(\alpha) = \sum_{\{\pi \in \langle X \rangle | \pi_A = \alpha\}} \rho(\pi)$. Let $[A]_\rho = \{\alpha \in \langle A \rangle \mid \rho_A(\alpha) > 0\}$. We use the notation (ρ, X) to denote the set of tuples $[X]_\rho$ indexed by X with the associated probability distribution ρ.

The *entropy* $H_\rho(A)$ of ρ_A is defined to be $H_\rho(A) = -\sum_{\alpha \in [A]_\rho} \rho_A(\alpha) \log \rho_A(\alpha)$. We remark that the base of the logarithm is not specified here, but can be chosen to be any convenient value. Where there is no ambiguity, we will write $[A]$ for $[A]_\rho$ and H for H_ρ. Let $B \subseteq X$ and let $\beta \in [B]$. For $\alpha \in [A]$, we have the conditional probability

$$\rho_{A|B}(\alpha, \beta) = \frac{\sum_{\{\pi \in \langle X \rangle | \pi_A = \alpha, \pi_B = \beta\}} \rho(\pi)}{\rho_B(\beta)}.$$

We may write $\rho_{A|B=\beta}$ for $\rho_{A|B}(\alpha, \beta)$, so we can regard $\rho_{A|B=\beta}$ as a probability distribution on $[A]_\rho$. The *conditional entropy* $H(A|B=\beta)$ of $\rho_{A|B=\beta}$ is defined to be

$$H(A|B=\beta) = -\sum_{\alpha \in [A]} \rho_{A|B}(\alpha, \beta) \log \rho_{A|B}(\alpha, \beta).$$

The *conditional entropy* $H(A|B)$ of ρ_A given ρ_B is defined to be

$$H(A|B) = \sum_{\beta \in [B]} H(A|B=\beta)\rho_B(\beta)$$

and it can be shown that $H(A|B) = H(AB) - H(B)$. Note that if $H(A|B) = H(A)$ then A and B are independent variables and so $\rho_{A|B}(\alpha, \beta) = \rho_A(\alpha)$. Hence $H(A|B) = H(A)$ implies that $H(A|B=\beta) = H(A)$.

3.2. A Naive Metering Scheme

In [21] it was noted that metering schemes are very closely related to *secret sharing schemes* [25,27], which are methods of splitting a secret amongst a group of entities in such a way that only certain subsets can reconstruct it. To see precisely what this relationship is we propose the following naive, and somewhat artificial, metering scheme.

We consider a metering scheme with one time frame where there are no corrupt servers or clients. Note that since no server or client is corrupt, each server can have the same proof of visit p and each client C_i can present their entire private share as evidence to any server that they visit. If $A \subseteq \mathscr{C}$, let $E_{A,j}$ denote the combined evidence given to any server S_j by all the clients in A (this is simply the combined shares of the clients in A).

The following definition formally defines the properties that this naive metering scheme must satisfy.

Definition 3.1. A *naive metering scheme* for targeted audience Γ is a method to measure the interaction between n clients $C_1, \ldots, C_n$ and m servers $S_1, \ldots, S_m$ in such a way that:

1. Any server S_j that has been visited by set of clients $A \in \Gamma$ can compute a proof of visit.

   Formally it holds that if $A \in \Gamma$, then $H(p|E_{A,j}) = 0$ for $j = 1, \ldots, m$.

2. If a server S_j has only been visited by a set of clients $A \notin \Gamma$ then server S_j has no information about the proof of visit.

   Formally, it holds that if $A \notin \Gamma$, then $H(p|E_{A,j}) = H(p)$ for $j = 1, \ldots, m$.

By replacing "proof of visit" by *secret*, "targeted audience" by *access structure* and "clients" by *participants*, and restricting Definition 3.1 to a single server ($m = 1$) then we have the formal definition of a secret sharing scheme for access structure Γ [27]. Thus a metering scheme for a single time frame and single server (or multiple non-corrupt servers) and no corrupt clients can be implemented by any suitable secret sharing scheme construction. This observation presents us with a basic construction that can be carefully extended in order to obtain bounds and constructions for more practical secure metering schemes.

3.3. A Strong Model for Metering Schemes

Our strong model for metering schemes differs from the naive model in three main ways:

Corrupt Servers. We protect against *any* coalition of up to s corrupt servers, for some integer s with $2 \leq s \leq m$. Corrupt servers in a coalition may give evidence that

they have received from any client to other corrupt servers in the coalition. Servers who are not in such a coalition do not share evidence with any other servers. In contrast to the model of a naive metering scheme, each client must thus give different servers different evidence and in general must therefore hold a large client share.

Corrupt Clients. We protect against sets of corrupt clients $K \subseteq \mathcal{C}$ who donate their share to a corrupt server. Clearly we can only protect against subsets of clients $K \notin \Gamma$, otherwise a corrupt server could use the shares of the corrupt clients to obtain a legitimate proof of visit for every time frame. In the basic model we do not protect against corrupt clients who present (honest) servers with fraudulent evidence. Extensions to the basic model to deal with this situation are discussed in Section 6.

Multiple Time Frames. We operate the metering scheme over a number of distinct time frames $t = 1, \ldots, \tau$. At the end of a given time frame each server attempts to compute a proof of visit from the received evidence in that time frame. Evidence from one time frame does not contribute to the computation of a proof of visit in another time frame.

For each $1 \le j \le m$ and each $1 \le t \le \tau$, let p_j^t denote the proof of visit for server S_j in time frame t. Further, for each $1 \le i \le n$, let $E_{i,j}^t$ denote the evidence that client C_i will give to server S_j if C_i visits S_j in time frame t. For $A \subseteq \mathcal{C}$, let $E_{A,j}^t$ denote the combined evidence that the clients in A will give to server S_j if visiting in time frame t. Lastly, let $V_j^{[t]}$ denote the combined evidence that all the clients in the audience will give to server S_j if they all visit S_j in all time frames $1, \ldots, t$ (in other words, $V_j^{[t]} = \cup_{r=1}^t E_{\mathcal{C},j}^r$).

Definition 3.2. An (s, τ)-*metering scheme* for targeted audience Γ is a method to measure the interaction between n clients $C_1, \ldots, C_n$ and m servers $S_1, \ldots, S_m$ during τ time frames in such a way that the following properties are satisfied.

1. Any client can compute the evidence for visiting any server in any time frame t:

   Formally it holds that $H(E_{i,j}^t | C_i) = 0$ for $i = 1, \ldots, n$, $j = 1, \ldots, m$, $t = 1, \ldots, \tau$.

2. Any server S_j that has been visited by a set of clients $A \in \Gamma$ in time frame t can compute the proof of visit for time frame t:

   Formally it holds that if $A \in \Gamma$, then $H(p_j^t | E_{A,j}^t) = 0$ for $j = 1, \ldots, m$, $t = 1, \ldots, \tau$.

3. Suppose that in time frame t, for some coalition of up to s corrupt servers and a set $K \notin \Gamma$ of corrupt clients, one of the servers S_j in the coalition has not received enough other evidence to use the shares of K to construct a proof of visit. Then by pooling the evidence received by the coalition servers in all time frames up to and including t (we assume the worst case scenario that in all time frames prior to t every server in the coalition was visited by every client in

the audience), together with the shares of K, the coalition have no information about the proof of visit for server S_j in time frame t.

Formally, let $1 \leq t \leq \tau$, $\{S_1, \ldots, S_\beta\} \subseteq \mathscr{S}$ $(\beta \leq s)$ and let $K \subseteq \mathcal{C}$, $K \notin \Gamma$. For each $1 \leq i \leq m$, let D_i be the set of clients who have visited S_i in time frame t. If $D_j \cup K \notin \Gamma$ for some $j \in \{1, \ldots, \beta\}$ then

$$H(p_j^t | K, E_{D_1,1}^t \cdots E_{D_\beta,\beta}^t V_1^{[t-1]} \cdots V_\beta^{[t-1]}) = H(p_j^t).$$

Note that the information available to a set of β corrupt servers in part 3 of Definition 3.2 automatically includes the proofs of evidence for each of these servers for each previous time frame, since we assume that in each time frame prior to t they have received visits from each client in the audience.

Part 3 of Definition 3.2 is stronger than the definition proposed in [19]. The main difference is that in our definition we allow for the situation where in a coalition of corrupt servers, in the current time frame t, some servers may have been visited by sets of clients in the targeted audience (and hence can compute their proofs of visit). In the weaker definition in [19], it is assumed that in the current time frame none of the corrupt servers have been visited by a set of clients in the targeted audience. Further, the definition in [19] assumes that each of the coalition servers has been visited by exactly the same set of clients D in time frame t (we allow D to vary between servers), and that D is strictly contained in a minimal set of the targeted audience Γ (which is a weaker requirement than allowing D to be any set of clients such that $D \notin \Gamma$).

None of the extra assumptions in [19] seem to be necessary. We will see in Section 4 that the bound on the size of a client's share proved in [19] also holds, and in some sense applies more naturally, under this stronger definition. We will also show in Section 5 that the metering schemes proposed in [19] also satisfy our stronger requirements.

4. Bounding the Client's Share in a Metering Scheme

In this section we provide a generalised technique for establishing lower bounds on the share size of clients in a metering scheme. Throughout this section we will assume that the size $H(p_j^t)$ of a proof of visit is constant over all servers and time frames, and where appropriate will simply denote this by $H(p)$. The following result was established in [19]:

Result 4.1. In an (s, τ)-metering scheme where the proofs of visit of any s servers are statistically independent then it follows that $H(C_i) \geq s\tau H(p)$.

We note that under our stronger definition of a metering scheme Result 4.1 holds without the need for the independence condition. To see this, using the notation of Section 3, let $D_i = \mathscr{C}$ for all $1 \leq i \leq \beta$, $i \neq j$. Then $H(p_i^t | E_{D_i,i}^t) = 0$ for $i \neq j$, and

so

$$H(p_j^t | K E_{D_1,1}^t \cdots E_{D_s,s}^t V_1^{[t-1]} \cdots V_s^{[t-1]} p_1^t, \ldots, p_{j-1}^t p_{j+1}^t, \ldots, p_s^t) = H(p_j^t).$$

It thus follows that

$$H(p_j^t | p_1^t \ldots p_{j-1}^t p_{j+1}^t \ldots p_s^t) = H(p_j^t). \tag{1}$$

Recall now the relationship between Definitions 3.1 and 3.2. Since a naive metering scheme is effectively a secret sharing scheme, we can immediately apply a fundamental secret sharing bound [27] to see that, for naive metering, $H(C_i) \geq H(p)$. Result 4.1 is the analogous basic bound on a client's share size for an (s, τ)-metering scheme. However, there are a considerable number of more precise lower bounds for client share size in naive metering schemes that also immediately apply from the secret sharing literature (for example [27]). These take the general form "if Γ has certain properties then for some $X \subseteq \mathscr{C}$ in any naive metering scheme for Γ we have that $H(X) \geq \lambda H(p)$." We now show that all such results translate into analogous lower bounds on client share size in (s, τ)-metering schemes in a rather similar way to that of Result 4.1, thus generating a suite of new relevant results.

Recall the notation of Section 3. Let $Y \subseteq \mathscr{C}$ and $Z = \{S_1, \ldots, S_\beta\} \subseteq \mathscr{S}$. Then let

$$E_{Y,Z}^t = \bigcup_{j=1}^{\beta} E_{Y,j}^t \qquad \text{and} \qquad V_Z^{[t]} = \bigcup_{j=1}^{\beta} V_j^{[t]}.$$

We now recall another result from [19].

Result 4.2. Let B be a set of $\beta \leq s$ servers and X be a subset of clients. Then in any (s, τ)-metering scheme for Γ it holds that

$$H(X) \geq \sum_{t=1}^{\tau} H(E_{X,B}^t | V_B^{[t-1]}).$$

We are now ready to prove the main result of this section.

THEOREM 4.3. *Let Γ be a targeted audience defined on $\mathscr{C}$, let $X \subseteq \mathscr{C}$ and suppose that $H(X) \geq \lambda H(p)$ for all naive metering schemes for Γ. Then in any (s, τ)-metering scheme for Γ it follows that*

$$H(X) \geq s\tau\lambda H(p).$$

Proof. Let $B = \{S_1, \ldots, S_s\}$ be a collection of s servers and let $j \in \{1, \ldots, s\}$ be fixed. Put $D_i = \mathscr{C}$ (for each $i \neq j$) and suppose that $D_j = J$, $J \notin \Gamma$. By part 3 of Definition 3.2 we see that in an (s, τ)-metering scheme for Γ,

$$H(p_j^t | E_{J,j}^t E_{\mathscr{C},B\setminus S_j}^t V_B^{[t-1]}) = H(p_j^t). \tag{2}$$

Now, suppose instead that $D_j = L$, $L \in \Gamma$. By part 2 of Definition 3.2 we see that $H(p_j^t | E_{L,j}^t) = 0$ and so

$$H(p_j^t | E_{L,j}^t E_{\mathscr{C},B\setminus S_j}^t V_B^{[t-1]}) = 0. \tag{3}$$

Observe now that an (s,τ)-metering scheme can be reduced to a naive metering scheme defined on clients $\mathscr{C}$ where client C_i holds share $E_{i,j}^t$ and the generic proof of visit is $p = p_j^t$ (j as above). We can see this as follows. Let ρ be the probability distribution associated with the (s,τ)-metering scheme. We reduce themetering scheme to a secret sharing scheme on $\mathscr{C}_j^t = \{C_i \in \mathscr{C}$ such that C_i holds the share $E_{i,j}^t\}$ with secret p_j^t by fixing values $\alpha \in [E_{\mathscr{C},B\setminus S_j}^t]_\rho$ and $\beta \in [V_B^{[t-1]}]_\rho$. More formally, we can define the probability distribution ϕ defined on $Y = \mathscr{C}_j^t \cup \{p_j^t\}$ by

$$\phi(y) = \rho_{Y | \mathscr{C}_{B\setminus S_j}^t = \alpha,\ V_B^{[t-1]} = \beta}(y).$$

From (2) we have $H_\rho(p) = H_\phi(p)$ and also using (3) we get

$$\begin{aligned} H_\phi(p | E_{J,j}^t) &= H_\phi(p) \qquad J \notin \Gamma, \\ H_\phi(p | E_{L,j}^t) &= 0 \qquad\quad\ L \in \Gamma. \end{aligned}$$

So ϕ induces a naive metering scheme for targeted audience Γ. By our initial assumption, it thus follows that

$$H_\phi(E_{X,j}^t) \geq \lambda H_\phi(p_j^t).$$

Translating this to ρ we get

$$\begin{aligned} H_\rho(E_{X,j}^t | E_{\mathscr{C},B\setminus S_j}^t V_B^{[t-1]}) &\geq \lambda H_\rho(p_j^t | E_{\mathscr{C},B\setminus S_j}^t V_B^{[t-1]}) \\ &= \lambda H_\rho(p_j^t), \end{aligned} \tag{4}$$

by part 3 of Definition 3.2. But by definition $E_{X,B}^t = E_{X,1}^t E_{X,2}^t \cdots E_{X,s}^t$ and so

$$\begin{aligned} H_\rho(E_{X,B}^t | V_B^{[t-1]}) &= \sum_{j=1}^{s} H_\rho(E_{X,j}^t | E_{X,j-1}^t \cdots E_{X,1}^t V_B^{[t-1]}) \\ &\geq \sum_{j=1}^{s} H_\rho(E_{X,j}^t | E_{X,B\setminus S_j}^t V_B^{[t-1]}) \\ &\geq \sum_{j=1}^{s} H_\rho(E_{X,j}^t | E_{\mathscr{C},B\setminus S_j}^t V_B^{[t-1]}) \\ &\geq \sum_{j=1}^{s} \lambda H_\rho(p_j^t) \quad \text{by (4).} \end{aligned}$$

As we are assuming that $H_\rho(p_j^t)$ is constant $H_\rho(p)$ for all j and t ($1 \le j \le s$, $1 \le t \le \tau$), then

$$H_\rho(E_{X,B}^t \mid V_B^{[t-1]}) \ge s\lambda H_\rho(p)$$

and so the theorem follows by Result 4.2. ■

We now give a simple example to show how Theorem 4.3 can be used.

EXAMPLE 1. In [7] it was shown that if Γ is a targeted audience defined on clients $\mathscr{C} = \{C_1, C_2, C_3, C_4\}$ with the property that

$$\{C_1, C_2\},\ \{C_2, C_3\},\ \{C_3, C_4\} \in \Gamma$$

and

$$\{C_1, C_3\},\ \{C_1, C_4\},\ \{C_2\} \notin \Gamma,$$

then for any naive metering scheme for Γ it holds that

$$H(C_2C_3) \ge 3H(p).$$

We can now apply Theorem 4.3 directly to show that in an (s, τ)-metering scheme for Γ it holds that

$$H(C_2C_3) \ge 3s\tau H(p).$$

5. A Metering Scheme for General Targeted Audiences

In this section we construct a family of (s, τ)-metering schemes for general targeted audiences. We first recall a method for constructing naive metering schemes and then present the main construction, which we compare with previous work.

5.1. A Construction for Naive Metering

We saw in Section 3.2 that a naive metering scheme can be implemented by any secret sharing construction. We recall here a secret sharing construction based on projective geometry.

5.1.1. Geometrical Configurations

The concept of a geometrical subspace configuration and its subsequent implementation as a secret sharing scheme (naive metering scheme) [13, 26] is a simple one, and has appeared under a variety of guises (for example vector spaces [6] and linear codes [10]).

Let $\Sigma = \mathrm{PG}(r, q)$, the projective geometry of dimension r over the field $\mathrm{GF}(q)$. So Σ consists of the points $(x_0, \ldots, x_r)$ where $x_i \in \mathrm{GF}(q)$ not all zero and with the convention that $\alpha(x_0, \ldots, x_r) = (x_0, \ldots, x_r)$ for any $\alpha \in \mathrm{GF}(q) \setminus \{0\}$. We can think of

this in terms of vector spaces if desired: the empty space, points, lines, planes, ..., i-dimensional subspaces of $\mathrm{PG}(r,q)$ are merely the 0-dimensional, 1-dimensional, 2-dimensional, 3-dimensional, ... $(i+1)$-dimensional vector subspaces of the vector space of (vector) dimension $r+1$ over $\mathrm{GF}(q)$. Hence we can identify a subspace Π of $\mathrm{PG}(r,q)$ with any matrix $[\Pi]$ over $\mathrm{GF}(q)$ with $r+1$ columns whose row space corresponds to the subspace Π. For more details, see [12].

Let Γ be a targeted audience defined on clients $\mathscr{C}$ with proof p. A *subspace configuration* for Γ is a mapping $\sigma: p\mathscr{C} \to \Sigma$ such that, for $A \subseteq \mathscr{C}$,

$$A^\sigma \cap p^\sigma = \begin{cases} p^\sigma & \text{if } A \in \Gamma; \\ \emptyset & \text{if } A \notin \Gamma. \end{cases}$$

That is, each client C_i is associated with a subspace C_i^σ in Σ and the proof p is associated with a subspace p^σ. The set A^σ is the span of all the subspaces associated with the clients in A, and this subspace contains the proof p^σ if and only if $A \in \Gamma$.

5.1.2. Implementation of Geometrical Naive Metering Scheme

For any subspace Π of $\Sigma = \mathrm{PG}(r,q)$, let $[\Pi]$ denote some matrix with $r+1$ columns over $\mathrm{GF}(q)$ whose row space is equal to the subspace Π. We will swap between the subspace notation Π and matrix notation $[\Pi]$ at our convenience.

Assume that σ is a publicly known subspace configuration for Γ, so the matrices $[C^\sigma]$ $(C \in \mathscr{C})$ and $[p^\sigma]$ are also publicly known. The audit agency secretly chooses a random vector $\mathbf{h} \in \mathrm{GF}(q)^{r+1}$. It then securely distributes the value of $[C^\sigma]\mathbf{h}^t$ to each $C \in \mathscr{C}$ (where $\mathbf{h}^t$ denotes the *transpose* of $\mathbf{h}$). The proof of visit is $[p^\sigma]\mathbf{h}^t$.

To see that this naive metering schemes works, consider attempting to use the shares of a group of clients $A \subseteq \mathscr{C}$ to determine the proof $[p^\sigma]\mathbf{h}^t$. The shares of A can be used to calculate $[A^\sigma]\mathbf{h}^t$. If $p^\sigma \subseteq A^\sigma$, then $[p^\sigma]\mathbf{h}^t$ can also be computed. If $p^\sigma \cap A^\sigma = \emptyset$, then the row spaces of the matrices $[A^\sigma]$ and $[p^\sigma]$ are independent, so the shares of the clients in A do not contain any information about $[p^\sigma]\mathbf{h}^t$.

EXAMPLE 2. Shamir's threshold scheme.

Consider Shamir's polynomial (k,n)-threshold scheme [25] (a naive threshold metering scheme with threshold k and n clients). The audit agency privately selects a polynomial $P(x)$ of degree $k-1$ over $\mathrm{GF}(q)$. Each client C_i is associated with a public value α_i and the audit agency issues C_i with the share $P(\alpha_i)$. The proof of visit is $P(0)$. If $P(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{k-1}x^{k-1}$ then

$$P(x) = (1, x, x^2, \ldots, x^{k-1})\mathbf{h}^t$$

where $\mathbf{h} = (h_0, h_1, h_2, \ldots, h_{k-1})$ and

$$P(0) = (1, 0, 0, \ldots, 0)\mathbf{h}^t.$$

We can see that this corresponds to the subspace configuration $\sigma: p\mathscr{C} \to \mathrm{PG}(k-1, q)$ given by

$$C_i^\sigma = (1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{k-1}),$$
$$p^\sigma = (1, 0, 0, \ldots, 0).$$

The set of points $\{(1, x, \ldots, x^n) | x \in \mathrm{GF}(q)\} \cup \{(0, 0, \ldots, 0, 1)\}$ form a *normal rational curve* in $\mathrm{PG}(n, q)$. Thus the points $p^\sigma, C_1^\sigma, \ldots, C_n^\sigma$ lie on a normal rational curve in $\mathrm{PG}(k-1, q)$. A normal rational curve in $\mathrm{PG}(2, q)$ is a *conic* of $\mathrm{PG}(2, q)$. See [12] for more details on normal rational curves and conics.

5.1.3. Finding a Suitable Subspace Configuration

We observe that the efficient *linear* secret sharing scheme constructions [6,10] are based on subspace configurations, although not actually described explicitly in terms of projective geometry. Some work has been done in order to try to develop algorithms to generate efficient subspace configurations (for example [15]), but in practice optimal configurations for specific access structures (targeted audiences) have often been determined by ad hoc methods. For information about more refined techniques, see [27].

5.2. *A Construction for* (s, τ)*-Metering*

We now describe how to adapt the construction of a naive metering scheme based on subspace configurations to construct (s, τ)-metering schemes for general targeted audiences. We first show how to do this for metering schemes with a single time frame ($\tau = 1$) and then how to generalise to multiple time frames.

5.2.1. A Construction for One Time Frame

Let Γ be a targeted audience defined on $\mathscr{C} = \{C_1, \ldots, C_n\}$. The scheme is as follows:

Initialisation:

- The audit agency selects a subspace configuration $\sigma: p\mathscr{C} \to \mathrm{PG}(r, q)$ for Γ and a random $r \times s$ matrix M. Suppose this subspace configuration associates each client C_i with a subspace C_i^σ in $\mathrm{PG}(r, q)$ (and hence with the associated matrix $[C_i^\sigma]$).
- The audit agency securely issues client C_i with share $[C_i^\sigma]M(1, y, y^2, \ldots, y^{s-1})^t$.
- The audit agency publicly assigns server S_j an identifier $\gamma_j \in \mathrm{GF}(q)$.

Presentation of evidence:

- When client C_i visits server S_j, it gives S_j the evidence $[C_i^\sigma]M(1, \gamma_j, \gamma_j^2, \ldots, \gamma_j^{s-1})^t$.

Construction and verification of proof:

- When server S_j has been visited by a set of clients in the targeted audience, it has enough information to construct the proof $[p^\sigma]M(1, \gamma_j, \gamma_j^2, \ldots, \gamma_j^{s-1})^t$ and then sends this securely to the audit agency.
- The audit agency verifies the correctness of the presented proof and rewards the server appropriately.

In order to prove that this is an $(s, 1)$-metering scheme we will interpret it as a subspace configuration ω and demonstrate the proof in the framework of projective spaces. At the end of this section we illustrate the projective space setting of this construction with a small example.

We will show that the construction above is obtained by taking the original subspace configuration $\sigma: p\mathscr{C} \to \mathrm{PG}(r, q)$ for Γ and *expanding* each point of $\Sigma = \mathrm{PG}(r, q)$ into an $(s-1)$-dimensional subspace of $\mathrm{PG}((r+1)s-1, q)$. More specifically, if C_i^σ is a point of $\mathrm{PG}(r, q)$ then we expand it to an $(s-1)$-dimensional subspace of $\mathrm{PG}((r+1)s-1, q)$; and if C_i^σ is a subspace of dimension d_i, we expand it to a subspace of dimension $(d_i+1)s-1$ in $\mathrm{PG}((r+1)s-1, q)$.

Suppose $(a_0, a_1 \ldots, a_r) \in C_i^\sigma$, then part of the share of C_i is

$$
\begin{aligned}
&(a_0, a_1, \ldots, a_r)M(1, y, \ldots, y^{s-1})^t \\
&\quad = (a_0, a_1, \ldots, a_r)\begin{bmatrix} m_{11}+m_{12}y+\cdots+m_{1s}y^{s-1} \\ m_{21}+m_{22}y+\cdots+m_{2s}y^{s-1} \\ \vdots \\ m_{r1}+m_{r2}y+\cdots+m_{rs}y^{s-1} \end{bmatrix} \\
&\quad = a_0(m_{11}+m_{12}y+\cdots+m_{1s}y^{s-1})+\cdots+a_r(m_{r1}+m_{r2}y+\cdots+m_{rs}y^{s-1}) \\
&\quad = \Big(a_0(1, y, \ldots, y^{s-1}), a_1(1, y, \ldots, y^{s-1}), \ldots, a_r(1, y, \ldots, y^{s-1})\Big) \\
&\qquad \times (m_{11}, m_{12}, \ldots, m_{1s}, \quad m_{21}, m_{22}, \ldots, m_{2s}, \ldots, m_{r1}, m_{r2}, \ldots, m_{rs})^t.
\end{aligned} \tag{5}
$$

For $y \in \mathrm{GF}(q)$, let $\mathbf{y} = (1, y, y^2, \ldots, y^{s-1})$ and label the following $r+1$ independent points of $\mathrm{PG}((r+1)s-1, q)$ as shown

$$
\begin{aligned}
U_0(y) &= (\mathbf{y}, \mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) \\
U_1(y) &= (\mathbf{0}, \mathbf{y}, \mathbf{0}, \ldots, \mathbf{0}) \\
&\vdots \\
U_r(y) &= (\mathbf{0}, \mathbf{0}, \mathbf{0}, \ldots, \mathbf{y}).
\end{aligned}
$$

Further, label the r-dimensional subspace generated by these points by $U(y)$. Note that $U(y)$ is isomorphic to Σ and that

$$[U(y)] = \begin{bmatrix} [U_0(y)] \\ \vdots \\ [U_r(y)] \end{bmatrix}.$$

So (5) can be expressed as $(a_0, a_1, \ldots, a_r)[U(y)]$ multiplied by a randomising vector. Moreover,

$$\begin{aligned}
&(a_0, a_1, \ldots, a_r)[U(y)] \\
&\quad = \Big(a_0(1, y, \ldots, y^{s-1}), a_1(1, y, \ldots, y^{s-1}), \ldots, a_r(1, y, \ldots, y^{s-1})\Big) \\
&\quad = (a_0, 0, \ldots, 0,\ \ a_1, 0, \ldots, 0, \ldots\ \ a_r, 0, \ldots, 0) \\
&\qquad + y(0, a_0, 0, \ldots, 0,\ \ 0, a_1, 0, \ldots, 0, \ldots, 0, a_r, 0, \ldots, 0) \\
&\qquad\quad + \cdots + y^{s-1}(0, \ldots, 0, a_0,\ \ 0, \ldots, 0, a_1, \ldots, 0, \ldots, 0, a_r),
\end{aligned}$$

and so is a normal rational curve in an $(s-1)$-dimensional subspace. Further, by properties of normal rational curves, for any s distinct values $\gamma_1, \ldots, \gamma_s$ in $\mathrm{GF}(q)$ the r-dimensional subspaces $U(\gamma_1), \ldots, U(\gamma_s)$ are independent, that is, they satisfy

$$U(\gamma_i) \cap \langle \{U(\gamma_1), \ldots, U(\gamma_s)\} \backslash U(\gamma_i) \rangle = \emptyset. \tag{6}$$

Consequently in $\mathrm{PG}((r+1)s-1, q)$ for any other value γ of $\mathrm{GF}(q)$ distinct from $\gamma_1, \ldots, \gamma_s$ we have

$$U(\gamma) \subseteq \langle U(\gamma_1), \ldots, U(\gamma_s) \rangle. \tag{7}$$

Initially we have a subspace configuration σ for Γ in $\mathrm{PG}(r, q)$ with proof p. In order to expand this to allow corrupt servers, we need to have a distinct proof p_j for each server S_j. We define a subspace configuration ω: $p_1 \cdots p_m \mathscr{C} \to \mathrm{PG}((r+1)s-1, q)$ in the following way. To each server S_j associate a distinct value $\gamma_j \in \mathrm{GF}(q)$. For $C_i \in \mathscr{C}$ $(1 \le i \le n)$ define

$$[C_i^\omega] = \begin{bmatrix} [C_i^\sigma][U(\gamma_1)] \\ \vdots \\ [C_i^\sigma][U(\gamma_s)] \end{bmatrix}.$$

We call this *expanding* C_i's share. We will use $C_i^\sigma U(\gamma_j)$ to denote the subspace whose row space is equal to $[C_i^\sigma][U(\gamma_j)]$. We note from (7) that $C_i^\sigma U(\gamma) \subseteq C_i^\omega$, for any $\gamma \in \mathrm{GF}(q)$. The proof for server S_j $(1 \le j \le m)$ is

$$p_j^\omega = p^\sigma U(\gamma_j)$$

and the evidence C_i $(1 \le i \le n)$ presents S_j $(1 \le j \le m)$ is

$$E_{i,j} = C_i^\sigma U(\gamma_j).$$

Note that for a fixed server S_j, the evidence $E_{1,j}, \ldots, E_{n,j}$ and the proof $p_j = p^\sigma U(\gamma_j)$ all lie in the r-dimensional subspace $U(\gamma_j)$ and form a subspace configuration which is isomorphic to σ.

THEOREM 5.1. *The scheme ω defined above is an $(s, 1)$-metering scheme.*

Proof. By definition, $E_{i,j}$ is a subspace of C_i^ω, so $H(E_{i,j}|C_i) = 0$, so part 1 of the definition is satisfied. For part 2, suppose server S_j has been visited by a set A of clients with $A \in \Gamma$. Then $p^\sigma \subseteq A^\sigma$ and so $p^\sigma U(\gamma_j) \subseteq A^\sigma U(\gamma_j)$. Hence $H(p_j|E_{A,j}) = 0$.

For part 3, it is sufficient to consider the worst case. That is, suppose that K is the set of corrupt clients and that $S_1, \ldots, S_s$ are a coalition of corrupt servers. Further suppose that $S_1, \ldots, S_{s-1}$ are visited by all the clients and that S_s has been visited by a set of clients D where $KD \notin \Gamma$. Then by pooling all this information, the server S_s can generate the subspace

$$R = \langle K^\sigma U(\gamma_1), \ldots, K^\sigma U(\gamma_s), U(\gamma_1), \ldots, U(\gamma_{s-1}), D^\sigma U(\gamma_s)\rangle$$

As $K^\sigma U(\gamma_j) \subseteq U(\gamma_j)$, $R = \langle (KD)^\sigma U(\gamma_s), U(\gamma_1), \ldots, U(\gamma_{s-1})\rangle$. We are interested in $p^\sigma U(\gamma_s) \cap R$. As $p^\sigma U(\gamma_s) \subseteq U(\gamma_s)$, by (6) we have

$$\begin{aligned} p^\sigma U(\gamma_s) \cap R &= p^\sigma U(\gamma_s) \cap (KD)^\sigma U(\gamma_s) \\ &= (p^\sigma \cap (KD)^\sigma) U(\gamma_s). \end{aligned}$$

As $KD \notin \Gamma$, $p^\sigma \cap (KD)^\sigma = \emptyset$ and so $p^\sigma U(\gamma_s) \cap R = \emptyset$. Hence

$$H(p_s | K E_{\mathscr{C},1}, \ldots, E_{\mathscr{C},s-1}, E_{D,s}) = H(p_s)$$

as required. Thus we have shown that the system is safe under collusion of s corrupt servers. That is, the scheme is an $(s, 1)$-metering scheme. ∎

We now give a small example with $r = 2$, $s = 2$ and a simple targeted audience in order to illustrate the geometric construction. To implement the example, we merely post-multiply by an appropriate randomising matrix as in Section 5.1.2.

EXAMPLE 3. The geometric construction for a $(2, 1)$-metering scheme for a 3-threshold targeted audience.

Suppose the targeted audience Γ is a $(3, n)$-threshold on a set of clients $\mathscr{C} = \{C_1, \ldots, C_n\}$ with proof p. A subspace configuration σ for this associates with each C_i a point $C_i^\sigma = (a_{i0}, a_{i1}, a_{i2})$ and with the proof p a point $p^\sigma = (p_0, p_1, p_2)$, where $C_1^\sigma, \ldots, C_n^\sigma, p^\sigma$ are distinct points on a conic in $\Sigma = \mathrm{PG}(2, q)$. Suppose we want to protect against a coalition of two corrupt servers. We associate with each server S_j a public identifier $\gamma_j \in \mathrm{GF}(q)$ and we need to expand the client and proof subspaces into lines as described earlier. We have $\mathbf{y} = (1, y)$ and so

$$U_0(y) = (1, y, 0, 0, 0, 0), \quad U_1(y) = (0, 0, 1, y, 0, 0), \quad U_2(y) = (0, 0, 0, 0, 1, y) \tag{8}$$

and

$$C_i^\sigma U(y) = (a_{i0}, a_{i1}, a_{i2}) \begin{bmatrix} U_0(y) \\ U_1(y) \\ U_2(y) \end{bmatrix}$$
$$= (a_{i0}, 0, a_{i1}, 0, a_{i2}, 0) + y(0, a_{i0}, 0, a_{i1}, 0, a_{i2}),$$

which is a line ℓ_i of PG$(5, q)$. Similarly, the proof $p^\sigma = (p_0, p_1, p_2)$ is expanded into the line $\ell = \{(p_0, 0, p_1, 0, p_2, 0) + \gamma(0, p_0, 0, p_1, 0, p_2) | \gamma \in \mathrm{GF}(q)\}$. Note that the lines $\ell, \ell_1, \ldots, \ell_n$ are disjoint.

When client C_i visits server S_j, C_i presents the point

$$c_{i,j} = C_i^\sigma U(\gamma_j) = (a_{i0}, \gamma_j a_{i0}, a_{i1}, \gamma_j a_{i1}, a_{i2}, \gamma_j a_{i2}) \in \ell_i$$

to S_j. The server S_j's proof is a point $p_j = p^\sigma U(\gamma_j) = (p_0, \gamma_j p_0, p_1, \gamma_j p_1, p_2, \gamma_j p_2)$ on the line ℓ. Moreover, each server S_j has an associated plane $\Sigma_j = U(\gamma_j)$ with basis $(1, \gamma_j, 0, 0, 0, 0), (0, 0, 1, \gamma_j, 0, 0), (0, 0, 0, 0, 1, \gamma_j)$ and the points $c_{1,j}, \ldots, c_{n,j}$, p_j all lie on a conic in Σ_j. Thus if server S_j has received three client shares, it can generate the plane Σ_j and hence obtain its proof. Note that the planes Σ_j are disjoint for distinct servers, and the shares and proof in each plane form a subspace configuration isomorphic to the original one in Σ.

Suppose S_j and S_k are two corrupt servers and K is a set of corrupt clients. Suppose a set D of clients have visited S_k, with $KD \notin \Gamma$. We show that S_k cannot successfully collude with S_j and K to reconstruct the proof p_k. In the worst case, S_j knows Σ_j, so S_k knows the subspace $R = \langle (KD)^\sigma U(\gamma_k) \rangle, (KD)^\sigma U(\gamma_j), U(\gamma_j) \rangle$. As Σ_j and Σ_k are disjoint subspaces, R meets Σ_k in the subspace $(KD)^\sigma U(\gamma_k)$. Further, as $KD \notin \Gamma$, we have $(KD)^\sigma \cap p^\sigma = \emptyset$, hence $(KD)^\sigma U(\gamma_k) \cap p^\sigma U(\gamma_k) = \emptyset$. Thus K and S_j cannot collude with S_k to reconstruct S_k's proof.

Note, in general, to protect against s corrupt servers, C_i's point share would need to be expanded to a normal rational curve in an $(s-1)$-dimensional subspace.

5.2.2. Generalising to Multiple Time Frames

The easiest way to deal with multiple time frames is to use independent (one time frame) schemes for each time frame. We comment in the next section that it is efficient to use this technique.

We illustrate this by comparing it with the threshold polynomial construction. To implement a (k, n)-threshold targeted audience with one time frame, we can use a polynomial of degree $k-1$ in x and $s-1$ in y (see [19,21]). For τ time frames, we can use a polynomial $P(x, y)$ of degree $k-1$ in x and $s\tau - 1$ in y. We note however, that perhaps the situation of multiple time frames is clearer if we consider the scheme for τ time frames as τ independent polynomials

$$P_1(x, y), \ldots, P_\tau(x, y)$$

(each of degree $k-1$ in x and $s-1$ in y). Note that for time frame t $(1 \le t \le \tau)$ client C_i uses the polynomial $P_t(\alpha_i, y)$ which has degree $s-1$. So each client has

a share of size $s\tau H(p)$ which is the same size as storing the polynomial $P(\alpha_i, y)$ of degree $s\tau - 1$.

5.2.3. Efficiency
Recall Result 4.1 [19] that in an (s, τ)-metering scheme,

$$H(C_i) \geq s\tau H(p).$$

If the targeted audience Γ is realised by a subspace configuration σ (where client C_i has a subspace C_i^σ as a share), then our construction results in a share size $H(C_i) = sH(C_i^\sigma)$ for one time frame and $H(C_i) = s\tau H(C_i^\sigma)$ for τ time frames. Thus if the original access structure Γ can be realised by an ideal geometric scheme (that is, $H(C_i^\sigma) = H(p)$) then our construction has optimal share size.

Note, we can see from this that using τ independent schemes, one for each time frame is an efficient solution.

5.3. Comparison of Metering Schemes

We now compare the metering scheme proposed in Section 5.2 with other proposed solutions. We compare it against the original robust threshold metering scheme proposed in [21], the metering scheme for general targeted audiences proposed in [19] and the more efficient metering schemes for special families of targeted audience, also proposed in [19]. It is shown that all these proposed schemes are special cases of our construction.

5.3.1. Threshold Metering Scheme of Naor and Pinkas
Naor and Pinkas [21] generalise Shamir's polynomial scheme to satisfy the requirements for a metering scheme secure against coalitions of up to s corrupt servers. We assume that there is only time frame and show how their scheme can be thought of as a special example of our construction. They used a bivariate polynomial $P(x, y)$ of degree $k-1$ in x and degree $s-1$ in y. Each client C_i receives the polynomial $P(\alpha_i, y)$. Now, we can write $P(x, y)$ as

$$P(x, y) = (1, x, x^2, \ldots, x^{k-1}) M (1, y, y^2, \ldots, y^{s-1})^t$$

where M is a $k \times s$ matrix over GF(q). This is precisely how our construction would implement a (k, n)-threshold targeted audience.

5.3.2. General Metering Scheme of Masucci and Stinson
In [19], the authors write the targeted audience Γ in terms of its minimal sets $\mathscr{A}_1, \ldots, \mathscr{A}_\ell$. Each $\mathscr{A}_k$ is regarded as an $|\mathscr{A}_k|$ out of $|\mathscr{A}_k|$ threshold scheme on set $\mathscr{A}_k$ $(1 \leq k \leq \ell)$. Their general metering scheme associates a polynomial $P_k(x, y)$ of degree $|\mathscr{A}_k| - 1$ and $s-1$ in y with each $\mathscr{A}_k$, such that $P_k(0, y)$ is the same for

Table 1. Comparison of schemes of [19] and Section 5.2.

Ex #	Access structure	General construction [19] $(m_1, m_2, \dots)$	Best geometric construction $(m_1, m_2, \dots)$
1	$\Gamma = ab + bc + cd$	(1, 2, 2, 1)	(1, 2, 1, 1)
2	$\Gamma = ab + ac + ad + bcd + ae$	(3, 2, 2, 2, 1)	(3, 1, 1, 1, 1)
3	$\Gamma = ab + ac + bc + ad + bd + cde$	(3, 2, 3, 2, 3)	(2, 2, 1, 1, 1)

all k $(1 \le k \le \ell)$. Let

$$
\begin{aligned}
S_1 &= (1, \alpha_i, \dots, \alpha_i^{|\mathscr{A}_1|-1}, \quad \mathbf{0}, \quad \dots \quad \mathbf{0}) \\
S_2 &= (1, \quad \mathbf{0}, \quad \alpha_i, \dots, \alpha_i^{|\mathscr{A}_2|-1}, \dots \quad \mathbf{0}) \\
&\vdots \\
S_\ell &= (1, \quad \mathbf{0}, \quad \mathbf{0}, \quad \dots \alpha_i, \dots, \alpha_i^{|\ A_\ell|-1})
\end{aligned}
$$

be points of $\mathrm{PG}(|\mathscr{A}_1| + \cdots + |\mathscr{A}_\ell| - \ell, q)$, where $\mathbf{0}$ is a vector of zeros of appropriate length.

Ignoring the effect of corrupt clients, we note that the above technique is equivalent geometrically to each client C_i receiving the subspace generated by the points $\{S_k | C_i \in \mathscr{A}_k, 1 \le k \le \ell\}$. The point associated with the secret is, as before $(1, \mathbf{0}, \dots, \mathbf{0})$. To protect against coalitions of up to s corrupt servers, we expand as before. Thus we can see that this scheme is a special case of the above geometric scheme, but in general has poor efficiency rates as each client has to hold a large share.

EXAMPLE 4. Let $\mathscr{C} = \{C_1, \dots, C_n\}$ and let $H(C_i) = m_i s \tau H(P)$ $(1 \le i \le n)$. Table 1 gives some examples of the share sizes comparing the construction in [19] and the best geometric construction from Section 5.2.

Note that Examples 2 and 3 are from [14] [Examples 2 and 6 respectively]. Note also that the geometric constructions for Examples 1, 2 and 3 can be shown to achieve the bounds discussed in Section 4.

5.3.3. Special Metering Schemes of Masucci and Stinson

Metering schemes for two special families of targeted audience were proposed in [19]. We again show that these metering schemes are special cases of our general construction.

Multilevel metering. A multilevel access structure Γ has u disjoint levels $L_1, \dots, L_u$ with a $(h_r, |L_r|)$ threshold scheme on level r $(1 \le r \le u)$ with $h_1 < h_2 < \cdots < h_u$. Further, for each r $(1 \le r \le u)$ Γ contains those subsets which contain at least h_r clients

all of level at most L_r. That is,

$$\Gamma = \left\{ A \subseteq \bigcup_{r=1}^{u} L_r \,\middle|\, \text{there exists } r \text{ with } A \subseteq \bigcup_{i=1}^{r} L_i \text{ and } |A| \geq h_r. \right\}$$

The construction in [19] is a special case of the geometric construction as follows. Using the notation from [19], for each $r = 1, \ldots, u$ and $C_i \in L_r$ there is a vector $v_i = (1, x_i, x_i^2, \ldots, x_i^{h_r - 1}, 0, \ldots, 0)$ associated with C_i, and the point associated with the secret is $(1, 0, \ldots, 0)$.

Compartmented metering. Here we have disjoint *compartments* $G_1, \ldots, G_u$ of clients where $\mathscr{C} = G_1 \cup \cdots \cup G_u$ each associated with a number $h_r < n_r = |G_r|$ $(1 \leq r \leq u)$. The compartmented access structure consists of those subsets which contains at least h_r clients from compartment G_r for every r $(1 \leq r \leq u)$. The construction presented in [] consists of u independent bivariate polynomials $P_1(x, y), \ldots, P_u(x, y)$ over $\mathrm{GF}(q)$ where $P_r(x, y)$ has degree $(h_r - 1, s\tau - 1)$. The audit agency gives $C_i \in G_r$ the polynomial $P_r(i, y)$. The secret value is $\sum_{r=1}^{u} P_r(0, j \circ t)$. The geometric equivalent is the point

$$(1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{h_1 - 1}, \mathbf{0}, \ldots, \mathbf{0})$$

to C_i in G_1 and so on with the point

$$(\mathbf{0}, \ldots, \mathbf{0}, 1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{h_u - 1})$$

to C_i in G_u, with the point associated with the secret being

$$(1, 0, \ldots, 0, \quad 1, 0, \ldots, 0, \quad \ldots \quad , 1, 0, \ldots, 0).$$

6. Practical Extensions

We now briefly identify three extensions to the basic metering concept that are easily implemented in order to add practical functionality to the constructions described in Section 5.

6.1. Verifiable Evidence

As noted in Section 2.2 the basic model used in this paper assumes that clients do not present incorrect evidence to a server, thus preventing the server from constructing its proof. Ogata and Kurosawa [23] describe a method of extending Naor and Pinkas' [21] polynomial construction for threshold targeted audience to allow a server to verify with non-negligible probability that the client is not giving false evidence. This comes at the expense of an increase in the size of the private share of each client and some additional processing and storage requirements for each of the servers. The construction in Section 5 can be extended in a very similar way to give a verifiable metering scheme for any targeted audience. We outline the method below.

The construction in Section 5.2.1 assigns clients C_i as share points in $\mathrm{PG}((r+1)s-1,q)$. We will expand these points into lines using the same construction as in Section 5.2.1, resulting in a geometric scheme in $\mathrm{PG}(2(r+1)s-1,q)$. This expansion works in the same way the original construction does. Client C_i receives as share $C_i^{\sigma}U(\gamma)V(y)$ (where the $V(y)$ represents this second expansion). Each server S_j is associated with a random element $r_j \in \mathrm{GF}(q)$ and receives the check values $C_i^{\sigma}U(\gamma_j)V(r_j)$. When client C_i visits server S_j he presents the evidence $C_i^{\sigma}U(\gamma_j)V(y)$. Server S_j can then compute this at the value $y=r_j$ and compare it with the appropriate check value. To construct its proof, S_j uses the value $C_i^{\sigma}U(\gamma_j)V(0)$ to compute its proof as in Section 5. As this is essentially a straightforward generalisation of [23], the reader is referred to [23] for details.

6.2. Unlimited Metering

Another restriction of the scheme described in Section 5 is that it can only be used for a predetermined finite number of time periods. Both Naor and Pinkas [21] and Ogata and Kurosawa [23] observed that for their polynomial constructions for threshold targeted audiences this restriction can be removed if unconditional security is sacrificed and replaced by conditional security based on the assumed difficulty of the computational Diffie–Hellman problem. These conditionally secure metering schemes are based on an unconditionally secure scheme for a single time frame. At the start of each time frame the audit agency generates a random number u and publishes the challenge g^u, where g is a generator of the prime subfield of $\mathrm{GF}(q)$ (assuming the prime subfield is sufficiently large). Essentially each component value z in the unconditionally secure metering scheme is now replaced by g^{uz} and all linear relationships between such values now become product relationships involving exponents. The once one-time values z are now all re-usable since they are protected by the difficulty of computing discrete logarithms. The reader is again referred to [23] for details. Generalising the scheme in Section 5 (and its verifiable extension in Section 6.1) to this model is straightforward.

6.3. Dynamic Metering

As a last observation, we note that throughout this paper we have assumed that during the operating life cycle of a metering scheme the targeted audience does not change between time frames. There is no need for such a restriction and it is quite possible to have dynamic metering with different targeted audiences for different time frames, as noted in [4]. This is very straightforward to implement, by combining independent metering for single time frames, so long as the targeted audience for each time frame is known by the audit agency when the metering scheme is initialised. A more interesting problem is how to adjust the targeted audience after initialisation of the metering scheme, following some change in the metering rules. Such problems have been investigated for secret sharing schemes (naive metering

schemes) but the investigation of techniques for application in the strong metering model would be worthy of further investigation.

7. Conclusion

In this paper we have studied the problem of constructing robust web metering schemes. We have shown that a number of previous constructions can be unified and generalised, and have presented a general technique for obtaining lower bounds on the amount of client side information. We have also indicated several ways in which this model can be extended to offer further features.

At the time of writing the business models for charging for Internet services are highly volatile and the precise environments within which technological solutions will have to operate is fairly unclear. It is however very likely that a need for a variety of secure metering applications for Internet services within the client/server framework will emerge, and the solutions described in this (and related) work, even if not adopted for secure advertisement metering, will be suitable for consideration in these environments.

References

1. V. Anupam, A. Mayer, K. Nassim, B. Pinkas and M.K. Reiter, On the Security of Pay-Per-Click and Other Wed Advertising Schemes, *Computer Networks*, Vol. 31 (1999) pp. 1091–1100.
2. C. Blundo, A. De Bonis and B. Masucci. Metering schemes with pricing, In *Proceedings of the DISC 2000, Lecture Notes in Computer Science*, Vol. 1914 (2000) pp. 194–208.
3. C. Blundo, A. De Bonis and B. Masucci, Bounds and constructions for metering schemes, *Technical Report, Universita di Salerno* (1999).
4. C. Blundo, A. De Bonis, B. Masucci and D. R. Stinson, Dynamic multi-threshold metering schemes, In *Selected Areas in Cryptography 2000, Lecture Notes in Computer Science*, Vol. 2012 (2001) pp. 131–144.
5. C. Blundo and B. Masucci, A note on ideal metering schemes. Preprint.
6. E. F. Brickell, Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol. 9 (1989) pp. 105–113.
7. R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, On the size of shares for secret sharing schemes, *Journal of Cryptology*, Vol. 6 (1993) pp. 157–169.
8. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons (1991).
9. A. De Bonis and B. Masucci, An information theoretical approach to metering schemes, *Technical Report, Universita di Salerno* (2000). (Abstract in *Proceedings of ISIT 2000*, Sorrento, Italy.)
10. M. van Dijk, A linear construction for perfect secret sharing schemes, In *Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science*, Vol. 950 (1995) pp. 23–34.
11. M. Franklin and D. Malkhi, Auditable metering with lightweight security, *Journal of Computer Security*, Vol. 6 No. 4 (1998) pp. 237–255.
12. J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries,* Oxford University Press (1991).
13. W.-A. Jackson and K. M. Martin, Geometric secret sharing schemes and their duals, *Designs, Codes and Cryptography*, Vol. 4 (1994) pp. 83–95.
14. W.-A. Jackson and K. M. Martin, Perfect secret sharing schemes on five participants, *Designs, Codes and Cryptography*, Vol. 9 (1996) pp. 267–286.
15. W.-A. Jackson and K. M. Martin, An algorithm for efficient geometric secret sharing, *Utilitas Mathematica*, Vol. 54 (1998) pp. 127–150.

16. M. Jakobsson, P. D. MacKenzie and J. P. Stern, Secure and lightweight advertising on the Web, In: *Proceedings of the 8th World Wide Web Conference* (1999).
17. M. Lesk, Projections for making money on the Web, *Harvard Infrastructure Conference, 23–25 January 1997*. Available at http://www.lesk.com/mlesk/iih/iih.html.
18. M. Manasse, The Millicent protocols for electronic commerce, In *Proceedings of the 1st USENIX Workshop on Electronic Commerce, July 11–12, 1995*. Available at http://www.research.digital.com/SRC/millicent/.
19. B. Masucci and D. R. Stinson, Metering schemes for general access structures, In *Proceedings of ESORICS 2000, Lecture Notes in Computer Science*, Vol. 1895 (2000) pp. 72–87.
20. 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).
21. M. Naor and B. Pinkas, Secure and efficient metering, In *Advances in Cryptology – EUROCRYPT'98, Lecture Notes in Computer Science*, Vol. 140 (1998) pp. 576–590.
22. M. Naor and B. Pinkas, Secure accounting and auditing on the Web, *Computer Networks*, Vol. 30 (1998) pp. 541–550.
23. W. Ogata and K. Kurosawa, Provably secure metering scheme. In *Advances in Cryptology – ASIACRYPT 2000, Lecture Notes in Computer Science*, Vol. 1976 (2000) pp. 388–398.
24. T. Pedersen, Electronic payments of small amounts, In *Proceeding of the International Workshop Security Protocols, Lecture Notes in Computer Science*, Vol. 1189 (1996) pp. 56–68.
25. A. Shamir, How to share a secret, *Comm. ACM*, Vol. 22, No. 11, (1979) pp. 612–613.
26. G. J. Simmons, An introduction to shared secret and/or shared control schemes and their applications, In: *Contemporary Cryptology*, IEEE Press (1992) pp. 441–497.
27. D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, Vol. 2 (1992), pp. 357–390.