Efficient Secret Sharing Without a Mutually Trusted Authority

Extended Abstract

Wen-Ai Jackson, Keith M. Martin* and Christine M. O'Keefe*

Department of Pure Mathematics, The University of Adelaide, Adelaide SA 5005, Australia

Abstract. Traditional secret sharing schemes involve the use of a mutually trusted authority to assist in the generation and distribution of shares that will allow a secret to be protected among a set of participants. In contrast, this paper addresses the problem of establishing a secret sharing scheme for a given access structure *without* the use of a mutually trusted authority. A general protocol is discussed and several implementations of this protocol are presented. The efficiency of these implementations is considered. The protocol is then refined and constructions are presented for mutually trusted authority free threshold schemes.

1 Introduction

A *secret sharing scheme* is a method by which a *secret* can be protected among a group of *participants*. Each participant holds a private *share* of the secret. Only certain sets of participants (*authorised sets*) are desired to be able to reconstruct the secret from their respective pooled shares. The collection of these subsets is the *access structure* of the secret sharing scheme. For the purposes of most of this paper, sets of participants that are not in the access structure (*unauthorised sets*) will not be able to determine any more information about the secret than is known publicly. Such schemes are often referred to as being *perfect*.

It is natural to make the assumption that if a set A of participants contains a subset that belongs to an access structure then A is itself in that access structure. We call access structures with this property *monotone*. A secret sharing scheme on n participants in which precisely all subsets of size at least k ($1 \leq k \leq n$) are in the access structure is known as a (k, n)-*threshold scheme* (we say that the access structure is (k, n)-*threshold*). Threshold schemes were the first types of secret sharing scheme proposed ([2, 10]).

We make a subtle distinction between two types of secret that can be protected by a secret sharing scheme. A secret is said to be *explicit* if it takes a fixed value that is predetermined by factors outside the secret sharing scheme design. In other words, the scheme is designed to protect a particular predetermined

* This work was supported by the Australian Research Council

L.C. Guillou and J.-J. Quisquater (Eds.): Advances in Cryptology - EUROCRYPT '95, LNCS 921, pp. 183-193, 1995.

number within a given domain. This might be, say, a bank account number, the number of a security box or an enabling code. A secret is said to be *implicit* if it does not take a predetermined value. In this case the secret sharing scheme must protect a secret, but the value of the secret can be *any* number within a specified domain. A secret sharing scheme is more likely to have an implicit secret either in a situation where there is no obvious number associated with the secret, such as when the scheme is to be used to demonstrate concurrence in an access control protocol, or in a situation where the implicit secret value is *subsequently* adopted as, say, a cryptographic key or the number of a secure vault. In these situations the implicit secret, and/or the shares that generate it, must be part of the initialisation of the device that verifies the secret. For instance, an application was described in [6] where the shares of an implicit secret were manually incorporated into the initialisation process of the locking mechanism of a vault door.

Traditional models for secret sharing schemes rely on the existence of a *Mutually Trusted Authority* (*MTA*) to set up the scheme in the first place. This authority must be trusted by all the participants and can either be human (perhaps an organisation) or be a device. If the secret is explicit then the MTA is trusted with the knowledge of the explicit secret and with the generation and distribution of suitable shares that relate to the secret in question. In the case of an implicit secret, the MTA is further responsible for the generation of the implicit secret that is to be shared among the participants of the scheme.

We study here secret sharing schemes that do *not* require the existence of an MTA during their set-up protocols. We will thus refer to such schemes as being *MTA-free*. In an MTA-free scheme the participants generate their own shares. The MTA-free schemes that we consider all have implicit secrets. Unless there is a singleton participant set in the access structure of a secret sharing scheme, it does not seem very likely that a protocol can be devised which allows a group of participants to generate shares to protect an explicit secret. If there is a singleton participant set in the access structure then, since that participant effectively knows the secret directly from their share, that participant could (in theory) play the role of an MTA and generate shares of the (explicit) secret for the other participants. Indeed, a traditional secret sharing scheme can be thought of as a secret sharing scheme of this type where the MTA is an extra participant, in the access structure as a singleton set.

We note first that there does exist one family of monotone access structures which can be easily realised by MTA-free secret sharing schemes. A (*unanimous*) (n, n)-threshold scheme can be constructed without an MTA, as follows. Let w be a fixed positive integer.

- Each participant chooses a (random) share from $\mathbf{Z}_w$;
- The (implicit) secret is the sum of the participants' shares modulo w.

The first paper to consider constructions of more general MTA-free schemes was by Meadows [9]. In this novel paper a (k, n)-threshold scheme was proposed which allows the first k participants to generate their own (random) shares. Unfortunately a 'black box' is then required to generate the shares of the remaining

$n - k$ participants. This black box must be trusted with the knowledge of all the shares and with the value of the (implicit) secret. Thus by our definition the black box is playing the role of an MTA. The only possible advantage of this protocol is that the value of the implicit secret is directly determined from the shares chosen by the first k participants. However this does not appear to be much different from a scheme set up by a (device-based) MTA that selects the implicit secret using a random number generator.

In 1991 Ingemarsson and Simmons [6] reconsidered the design of MTA-free schemes for general monotone access structures and suggested an elegant protocol. The basic idea of [6] is that the n participants first generate shares of an (MTA-free) unanimous (n, n)-threshold scheme. The implicit secret of this unanimous scheme becomes the secret of the final scheme. Each participant then acts as their own MTA and sets up a private secret sharing scheme to protect their share of the unanimous scheme among a number of the other participants. Thus a participant's share in the unanimous scheme becomes the explicit secret of their private secret sharing scheme. It is quite possible that after carrying out this protocol, no participant will actually know the access structure of the induced secret sharing scheme. In [6] it is suggested that this procedure has the potential to realise an MTA-free scheme for any monotone access structure. We will later prove this suggestion to be correct.

The main aim of this paper is to start with a monotone access structure Γ, and determine which initial MTA-free scheme and which private secret sharing schemes should be used in order to realise an MTA-free scheme for Γ. There is not necessarily a unique way of doing this and so we are particularly interested in trying to find efficient and economical methods. These are based on trying to minimise the number of shares that have to be generated, mutually communicated and stored by the participants in the scheme. In doing so we show that *not all* of the participants need to generate shares in the first instance. It is often the case that in an efficient realisation of an MTA-free scheme for Γ, some participants need only store shares that have been generated by other participants.

In Section 2 we discuss the concept of access structure domination, which is fundamental to the rest of the paper. Section 3 is about MTA-free schemes in general and includes a construction protocol that will work for any monotone access structure. In Section 4 we concentrate on MTA-free threshold schemes and show that some variations of the standard protocol can be used to improve scheme efficiency. We have been forced to omit most proofs in this extended abstract, but it is hoped that by way of examples we can illustrate the main ideas behind the constructions presented. Complete proofs will be provided in the full paper.

2 Access Structure Domination

Let Γ be a monotone access structure defined on a participant set $\mathcal{P}$. The monotonicity of Γ ensures that we can find a collection Γ^- of *minimal* authorised

sets in Γ and a set Γ^+ of maximal unauthorised sets. Note that a participant need not belong to any minimal set in Γ. If every participant does belong to a minimal set then we say that Γ is *connected*. We recall from [1] that Γ can be considered as a logical expression with the participants being boolean variables. Let $\Gamma^- = \{C_1, \ldots, C_r\}$, let + denote logical OR and let juxtaposition denote logical AND. Then the disjunctive normal form of the *logical equivalent* of Γ is $\Gamma = C_1 + \cdots + C_r$. It follows that a subset A of participants is in the access structure Γ if and only if the logical equivalent of Γ is *true* when the variables in A are all true. For example, let $\mathcal{P} = \{a, b, c, d\}$ and $\Gamma^- = \big\{\{a, b, c\}, \{c, d\}\big\}$. Then we write $\Gamma = abc + cd$, or equivalently $\Gamma = (ab + d)c$.

We now recall from [8] a useful family of monotone access structures that can be derived from Γ. Let $A \subseteq \mathcal{P}$. We define the *contraction* $\Gamma \cdot A$ of Γ at A to be the monotone access structure on $\mathcal{P}$ given by

$$B \in \Gamma \cdot A \iff B \cup A \in \Gamma.$$

Conceptually, $\Gamma \cdot A$ is the access structure that results if the shares belonging to the participants in A are publicly revealed. For example, if $\Gamma = abc + cd$ then $\Gamma \cdot c = ab + d$ and $\Gamma \cdot d = c$.

Now let Γ_0 be a monotone access structure defined on $\mathcal{P} = \{p_1, \ldots, p_n\}$. Associate with each $p_i \in \mathcal{P}$ a monotone access structure Γ_i defined on $\mathcal{P}$. Let $\Gamma = (\Gamma_0; \Gamma_1, \ldots, \Gamma_n)$ be the monotone access structure defined on $\mathcal{P}$ that is formed by replacing p_i by Γ_i in the logical equivalent of Γ_0.

Example 1. Let $\mathcal{P} = \{a, b, c, d\}$. *Let* $\Gamma_0 = abcd$, $\Gamma_a = c$, $\Gamma_b = c + d$, $\Gamma_c = d$ *and* $\Gamma_d = d$. *Then* $\Gamma = (\Gamma_0; \Gamma_a, \Gamma_b, \Gamma_c, \Gamma_d) = c(c + d)dd = cd$. *Similarly, if* $\Gamma_0 = abcd$, $\Gamma_a = a + c$, $\Gamma_b = b + d$, $\Gamma_c =$ *'true' (in other words,* $(\Gamma_c)^- = \{\emptyset\}$*) and* $\Gamma_d =$ *'true' then* $\Gamma = (\Gamma_0; \Gamma_a, \Gamma_b, \Gamma_c, \Gamma_d) = (a + c)(b + d) = ab + ad + bc + cd$.

For $A \subseteq \mathcal{P}$, let $X(A) = \{p_i \mid A \in \Gamma_i\}$. We can also describe $\Gamma = (\Gamma_0; \Gamma_1, \ldots, \Gamma_n)$ in the following way.

Lemma 1. *Let* $\Gamma, \Gamma_0, \Gamma_1, \ldots, \Gamma_n$ *be monotone access structures defined on* $\mathcal{P} = \{p_1, \ldots, p_n\}$. *Then the following two statements are equivalent:*

1. $\Gamma = (\Gamma_0; \Gamma_1, \ldots, \Gamma_n)$;
2. *For every* $A \subseteq \mathcal{P}$ *we have* $A \in \Gamma$ *if and only if* $X(A) \in \Gamma_0$.

Now let Γ_0 and Γ be distinct monotone access structures defined on $\mathcal{P} = \{p_1, \ldots, p_n\}$. Using terminology suggested in [11], we say that Γ_0 *dominates* Γ if there exist monotone access structures $\Gamma_1, \ldots, \Gamma_n$ such that

1. $\{p_i\} \in \Gamma_i$ (for each i, $1 \leq i \leq n$);
2. $\Gamma = (\Gamma_0; \Gamma_1, \ldots, \Gamma_n)$.

Thus, from Example 1, we see that $\Gamma_0 = abcd$ dominates $\Gamma = ab + ad + bc + cd$. We say that Γ_0 *directly* dominates Γ if there does *not* exist a monotone access structure Γ' (distinct from Γ_0 and Γ) such that Γ_0 dominates Γ' and Γ' dominates Γ. We now classify all the monotone access structures that are (directly) dominated by a given monotone access structure.

Theorem 2. *Let Γ_0 and Γ be monotone access structures defined on $\mathcal{P}$. Then Γ_0 dominates Γ if and only if $\Gamma_0 \subseteq \Gamma$.*

The next result is an interpretation of the main theorem in [11].

Result 3. *Let Γ_0 and Γ be monotone access structures defined on $\mathcal{P}$. Then Γ_0 directly dominates Γ if and only if there exists a (unique) maximal unauthorised subset B of Γ_0 such that $\Gamma = \Gamma_0 \cup \{B\}$.*

3 Mutually Trusted Authority free Schemes

We first give a basic model for secret sharing (see, for example, [13]). We will use the *entropy* function in our definition (see, for example, [5] for an introduction to entropy and its properties). Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ be a participant set and let s be a secret. Let participant p_i receive a share from a set $[p_i]$ and let the secret come from a set $[s]$. A *secret sharing scheme* for Γ is a probability distribution ρ defined on a set of *distribution rules* $\Omega \subseteq [p_1] \times \cdots \times [p_n] \times [s]$ such that for $A \subseteq \mathcal{P}$,

1. if $A \in \Gamma$ then $H(s|A) = 0$;
2. if $A \notin \Gamma$ then $H(s|A) > 0$.

If it is the case that for each $A \notin \Gamma$ we have $H(s|A) = H(s)$ then the secret sharing scheme is said to be *perfect*. We call $H(p_i)$ the *size* of the share associated with p_i, and $H(s)$ the *size* of the secret. It can be seen (for example [13]) that in any perfect secret sharing scheme, if $p_i \in A$ for some minimal authorised set A then $H(p_i) \geq H(s)$. If $H(p_i) = H(s)$ for all such p_i then we say that the perfect secret sharing scheme and its access structure are *ideal*. We note ([2, 10]) that ideal (k, n)-threshold schemes can be found for all $1 \leq k \leq n$.

In a traditional secret sharing scheme, an MTA selects a distribution rule π from Ω with probability $\rho(\pi)$ and then distributes the appropriate shares to the participants of the scheme. In an MTA-free scheme the participants indirectly select a (random) distribution rule through the generation of their own (random) shares.

Consider the following extension of the protocol in [6] for setting up an MTA-free scheme. Firstly, let a subset $\mathcal{P}_0$ of the participants in $\mathcal{P}$ generate shares of a perfect scheme M_0 for some access structure Γ_0. Let x_i denote the share generated by p_i ($p_i \in \mathcal{P}_0$). Then let each $p_i \in \mathcal{P}_0$ construct a private perfect secret sharing scheme M_i for Γ_i on $\mathcal{P}$ to protect the explicit secret x_i. Thus x_i can be obtained by p_i or by any authorised set in Γ_i. In the degenerate case where $\Gamma_i^- = \{\emptyset\}$, p_i publicly reveals (*broadcasts*) their share. Otherwise p_i communicates the shares of M_i to the participants included in M_i. This process creates a new perfect secret sharing scheme M for access structure $\Gamma = (\Gamma_0; \Gamma_1, \ldots, \Gamma_n)$, where for each $p_i \notin \mathcal{P}_0$ we take Γ_i to be such that $\Gamma_i^- = \{\emptyset\}$ and thus for each i $(1 \leq i \leq n)$, $\{p_i\} \in \Gamma_i$. For the structure of the distribution rules of M in terms of those of M_0 and M_i, we refer to [8, 14], where constructions of this type were fully described.

Simmons [11] asked which access structures Γ could be realised from Γ_0 in this manner. In other words, *which access structures Γ are dominated by Γ_0?* Theorem 2 concisely answers this question by showing that these are precisely the access structures Γ such that $\Gamma \supseteq \Gamma_0$. We approach the problem from another direction in this paper. Namely, given an access structure Γ, exactly which access structures $\Gamma_0, \Gamma_1, \ldots, \Gamma_n$ such that $\Gamma = (\Gamma_0; \Gamma_1, \ldots, \Gamma_n)$ should be chosen in order to (efficiently) generate an MTA-free scheme for Γ?

3.1 The Base Access Structure

The first issue to be considered in the design of an MTA-free scheme for Γ is which initial access structure Γ_0 should be chosen. We refer to Γ_0 as the *base* access structure. We assume that each $p \in \mathcal{P}_0$ independently generates a random share of M_0 from set $[p]$.

Theorem 4. *Let Γ_0 be the access structure of a secret sharing scheme M_0 defined on $\mathcal{P}$ such that for each $p \in \mathcal{P}$ the share held by p in M_0 is independently and randomly chosen from the set $[p]$. Then Γ_0 has a unique minimal authorised set $\mathcal{P}_0$.*

If M_0 is a perfect secret sharing scheme then it follows from Theorem 4 that M_0 is a unanimous threshold scheme defined on $\mathcal{P}_0$, and thus that the participants in $\mathcal{P} \setminus \mathcal{P}_0$ need not generate shares in the initial stage of the protocol. Thus from Theorems 2 and 4 we have the following criteria for selection of the base access structure Γ_0.

- $\Gamma_0 \subseteq \Gamma$;
- Γ_0 is unanimous threshold on $\mathcal{P}_0$ ($P_0 \subseteq \mathcal{P}$).

3.2 Measures of Efficiency

There are three parameters that we might want to minimise for reasons of economy and efficiency in an MTA-free scheme. These are the total size $g(\mathcal{P})$ of shares *generated* by the participants, the total size $c(\mathcal{P})$ of shares *communicated* by participants, and the total size $s(\mathcal{P})$ of shares *stored* by participants in the scheme. For a participant $p \in \mathcal{P}$ let $g(p)$ be the sum of the sizes of shares generated by p, $c(p)$ be the sum of the sizes of shares communicated by p and $s(p)$ be the sum of the sizes of shares stored by p.

In the light of Section 3.1, we assume that M_0 is chosen to be ideal and hence the shares of M_0 (and thus the secrets of M_i, for $p_i \in \mathcal{P}_0$) all have the same size h. For the purposes of the discussion immediately following we will take h as the size of a 'unit' share.

Let $p \in \mathcal{P}$. If $p \notin \mathcal{P}_0$ then $g(p) = c(p) = 0$. Otherwise, if $p \in \mathcal{P}_0$ then p generates one share x_p of the initial scheme and then a number (possibly zero) of shares of a private scheme to protect x_p. These extra shares are communicated

to some of the other participants. Thus if $p \in \mathcal{P}_0$ then $g(p) = 1 + c(p)$. Hence in total,

$$g(\mathcal{P}) = c(\mathcal{P}) + |\mathcal{P}_0|. \tag{1}$$

A participant $p \in \mathcal{P}_0$ either keeps the share x_p secure or broadcasts it and hence does not need to store it. Let $\mathcal{P}_0'$ be the subset of $\mathcal{P}_0$ who store their shares. All shares of private schemes that are communicated to $p \in \mathcal{P}$ are stored securely. Hence we have in total,

$$s(\mathcal{P}) = c(\mathcal{P}) + |\mathcal{P}_0'|. \tag{2}$$

Then from (1) and (2) we have,

$$g(\mathcal{P}) = s(\mathcal{P}) + |\mathcal{P}_0 \setminus \mathcal{P}_0'| \; ; \qquad c(\mathcal{P}) = s(\mathcal{P}) - |\mathcal{P}_0'|. \tag{3}$$

Thus from (3) we see that $s(\mathcal{P})$ alone is an effective measure of efficiency since $g(\mathcal{P})$ and $c(\mathcal{P})$ are directly proportional to $s(\mathcal{P})$. In the event that two different schemes have the same total storage $s(\mathcal{P})$ then (3) suggests that a scheme which has a large value of $|\mathcal{P}_0'|$ relative to $|\mathcal{P}_0|$ is preferable.

Minimising storage has been the most studied measure of efficiency for traditional secret sharing schemes (for example [3, 4, 8, 14]). Efficiency rates can be calculated from the *contribution vector* (or *convec*) of the scheme. This is the vector $(c_1, \ldots, c_n) = (1/H(s))(H(p_1), \ldots, H(p_n))$. For perfect secret sharing schemes the most common efficiency measures are the *information rate*, which is the minimum $1/c_i$ $(1 \leq i \leq n)$, and the *average information rate*, which is $n/(c_1 + \cdots + c_n)$. For MTA-free schemes we see that the total storage $s(\mathcal{P})$ is $c_1 + \cdots + c_n$. For simplicity, in this paper we only consider minimising the total storage, which is equivalent to maximising the average information rate.

3.3 The Private Access Structures

The problem of constructing an efficient MTA-free scheme for Γ is thus the problem of selecting a base access structure Γ_0 (subject to the constraints of Section 3.1) and a collection of private access structures Γ_p $(p \in \mathcal{P}_0)$ in such a way that $s(\mathcal{P})$ is minimised. As a standard for comparison we use what we call the *Basic* construction. This is in effect the most 'obvious' way of constructing an MTA-free scheme for Γ. The Basic construction is used in the proof of Theorem 2.

The Basic Construction

Γ_0	(n, n)-threshold on $\mathcal{P}$
Γ_p	$p + \Gamma$ (for each $p \in \mathcal{P}$)
M_0	ideal unanimous threshold scheme on $\mathcal{P}$
M_p	perfect scheme for Γ_p (for each $p \in \mathcal{P}$)

Example 2. Let $\mathcal{P} = \mathcal{P}_0 = \{a, b, c, d\}$ *and* $\Gamma = ab + ac + bcd$. *Applying the Basic construction gives* $\Gamma_0 = abcd$, $\Gamma_a = a + bcd$, $\Gamma_b = b + ac$, $\Gamma_c = c + ab$ *and* $\Gamma_d = d + ab + ac$. *Since* $\Gamma_a, \Gamma_b, \Gamma_c, \Gamma_d$ *are all ideal (see [12]) we can find ideal* M_a, M_b, M_c, M_d *and thus a scheme* M *for* Γ *with convec* $(c_a, c_b, c_c, c_d) = (4, 4, 4, 2)$ *(for example, participant a generates one unit share, and receives one unit share from each of b,c,d).*

We show that, by applying contractions, the Basic construction can be quite considerably improved upon. We call this modified construction method the *Contraction* construction.

The Contraction Construction

Γ_0	(a, a)-threshold on $\mathcal{P}_0$, for some $\mathcal{P}_0 = \{p_1, \ldots, p_a\} \in \Gamma$
Γ_1	$p_1 + \Gamma$
Γ_2	$p_2 + \Gamma \cdot p_1$
$\vdots$	$\vdots$
Γ_a	$p_a + \Gamma \cdot p_1 p_2 \ldots p_{a-1}$
M_0	ideal unanimous threshold scheme on A
M_i	perfect scheme for Γ_i (for each i, $1 \leq i \leq a$)

Example 3. Let $\mathcal{P}$ *and* Γ *be as in Example 2. Applying the Contraction construction with* $\mathcal{P}_0 = \{a, b\}$ *and* $\Gamma_0 = ab$ *gives* $\Gamma_a = a + bcd$, $\Gamma_b = b + c$. *Since* Γ_a, Γ_b *are ideal (see [12]) we can find ideal* M_a, M_b *and thus a scheme* M_1 *for* Γ *with convec* $(1, 2, 2, 1)$. *Alternatively, applying the Contraction construction with* $\mathcal{P}_0 = \{b, c, d\}$ *and* $\Gamma_0 = bcd$ *gives* $\Gamma_b = b + ac$, $\Gamma_c = c + a$, $\Gamma_d = d + a$. *Since* Γ_b, Γ_c, Γ_d *are ideal (see [12]) we can find ideal* M_b, M_c, M_d *and thus a scheme* M_2 *for* Γ *with convec* $(3, 1, 2, 1)$. *Both* M_1 *and* M_2 *are considerably more efficient in terms of total storage (and information rate) than the scheme* M *constructed in Example 2. Scheme* M_1 *is slightly more efficient than* M_2.

4 Mutually Trusted Authority free Threshold Schemes

We now consider the special case of realising an MTA-free (k, n)-threshold scheme. We assume that $k < n$ since the case $k = n$ was covered in Section 1. Let $\mathcal{P} = \{p_1, \ldots, p_n\}$, let $1 \leq k < n$ and let Γ be (k, n)-threshold on $\mathcal{P}$. The most efficient MTA-free scheme for Γ we have seen thus far is by the Contraction construction applied to a minimal authorised set of Γ. In this case,

- $\Gamma_0 = (k, k)$-threshold on $\mathcal{P}_0 = \{p_1, \ldots, p_k\}$;
- $\Gamma_i = p_i + \big((k-i+1, n-i)$-threshold on $\{p_{i+1}, \ldots, p_n\}\big)$ (for each i, $1 \leq i \leq k$).

Using ideal threshold schemes $M_0, M_1, \ldots, M_a$ we can calculate the convec for the resulting scheme M. Each p_i $(1 \leq i \leq k)$ stores their share of M_0 and receives

one share from each of $p_1, \ldots, p_{i-1}$. Each p_i $(k+1 \leq i \leq n)$ receives one share from each of $p_1, \ldots, p_k$. Thus $c_i = i$ $(1 \leq i \leq k)$ and $c_i = k$ $(k+1 \leq i \leq n)$. So

$$s(\mathcal{P}) = \frac{1}{2}k(k+1) + k(n-k) = nk - \frac{1}{2}k(k-1). \tag{4}$$

We show that the Contraction construction gives an optimal construction for threshold schemes under certain assumptions.

Theorem 5. *Let M be an MTA-free (k,n)-threshold scheme that is constructed from an ideal unanimous threshold scheme M_0 on a k-subset A of $\mathcal{P}$, and, for each $p \in A$, a perfect scheme M_p for some Γ_p. Then $s(\mathcal{P}) \geq nk - (1/2)k(k-1)$.*

We now show that if the protocol for establishing an MTA-free scheme is generalised to permit the use of secret sharing schemes that are not perfect then we can always improve on the total storage given by the Contraction construction. Let $0 \leq c \leq k$. A (c,k,n)-*ramp scheme* on an n-set $\mathcal{P}$ is a secret sharing scheme such that for $A \subseteq \mathcal{P}$,

1. if $|A| \geq k$ then $H(s|A) = 0$;
2. if $|A| \leq c$ then $H(s|A) = H(s)$.

Ramp schemes such that $H(p) = H(s)/(k-c)$ $(p \in \mathcal{P})$ can be constructed from ideal (k,n)-threshold schemes ([7]).

We now present a construction which works for all $k \leq \frac{1}{2}(n+1)$. This construction relies on implementing the private access structures by using ramp schemes as opposed to perfect threshold schemes. For this reason we call it the *Private Ramp* construction.

The Private Ramp Construction

Γ_0	(n,n)-threshold on $\mathcal{P}$
Γ_p	$p + \big((k, n-1)$-threshold on $\mathcal{P} \setminus \{p\}\big)$
M_0	ideal (n,n)-threshold scheme on $\mathcal{P}$
M_p	modified $(0,k,n-1)$-ramp scheme on $\mathcal{P} \setminus \{p\}$

We say that M_p is 'modified' because $p \in \Gamma_p$ and so every distribution rule of M_p must also distribute a copy of the secret of M_p to participant p.

Example 4. Let Γ be $(2,3)$-threshold defined on $\mathcal{P} = \{a,b,c\}$. Using the Contraction construction with $\mathcal{P}_0 = \{a,b\}$ and $\Gamma_0 = ab$, gives $\Gamma_a = a+bc$, $\Gamma_b = b+c$ and a scheme M_1 for Γ with convec $(c_a, c_b, c_c) = (1,2,2)$. Using the Private Ramp construction gives $\Gamma_a = a + bc$, $\Gamma_b = b + ac$, $\Gamma_c = c + ab$. We then use the $(0,2,2)$-ramp schemes M_a, M_b, M_c to construct a scheme M_2 for Γ with convec $(2,2,2)$. Thus M_2 has a total storage of 6 which is slightly more than the total storage 5 of M_1.

Thus for the $(2,3)$ case, the Private Ramp construction did not perform as well as the Contraction construction. In the Private Ramp construction each participant $p \in \mathcal{P}$ generates a share of unit size and then receives $n-1$ other shares, each of size $1/k$, from the other participants. So for the Private Ramp construction,

$$s(\mathcal{P}) = n(1 + \frac{n-1}{k}) = \frac{n(k+n-1)}{k}. \tag{5}$$

Thus we can see from (4) and (5) that, generally, the Contraction construction has a lower total storage than the Private Ramp construction when k is small with respect to n, but the Private Ramp construction is an improvement on the Contraction construction when k is close to $\frac{1}{2}(n+1)$.

We show now that if a ramp scheme is used to implement the base access structure instead of the private access structures then we can do even better. The *Base Ramp* construction has the added advantage that it works for all $1 \leq k \leq n-1$.

The Base Ramp Construction

Γ_0	(n,n)-threshold on $\mathcal{P}$
Γ_p	$p + ((k, n-1)$-threshold on $\mathcal{P} \setminus \{p\})$
M_0	$(k-1, n, n)$-ramp scheme on $\mathcal{P}$
M_p	ideal scheme for Γ_p $(p \in \mathcal{P})$

Example 5. As in Example 4, let Γ be $(2,3)$-threshold defined on $\mathcal{P} = \{a,b,c\}$. Using the Base Ramp construction gives $\Gamma_a = a + bc$, $\Gamma_b = b + ac$, $\Gamma_c = c + ab$ and a scheme M_3 for Γ with convec $(3/2, 3/2, 3/2)$. Thus M_3 has a total storage of $9/2$ which is an improvement on the total storage 5 of M_1 using the Contraction construction, and on the total storage 6 of M_2 using the Private Ramp construction.

Note that the Base Ramp construction is essentially the same as the Basic construction for a (k,n)-threshold scheme, except with a different M_0. Each participant $p \in \mathcal{P}$ generates a share of size $1/(n-k+1)$ and then receives $n-1$ other shares, each of size $1/(n-k+1)$, from the other participants. So for the Base Ramp construction,

$$s(\mathcal{P}) = n(\frac{n}{n-k+1}) = \frac{n^2}{n-k+1}. \tag{6}$$

Thus from (4) and (6), and from (5) and (6), we see that the Base Ramp scheme is an improvement on both the Contraction construction and the Private Ramp construction (when applicable) for (k,n)-threshold schemes. We note that the Base Ramp Construction for threshold schemes can be generalised to other monotone access structures.

We conclude by presenting a table containing the values for the total storage of various MTA-free (k,n)-threshold schemes under the constructions discussed

in this paper ($*$ denotes that the construction is not possible for these parameters).

	Total Storage			
(k, n)	Basic	Contraction	Private Ramp	Base Ramp
$(2, 3)$	9	5	6	9/2
$(2, 4)$	16	7	10	16/3
$(2, 5)$	25	9	15	25/4
$(3, 4)$	16	9	$*$	8
$(3, 5)$	25	12	35/3	25/3
$(4, 5)$	25	14	$*$	25/2
$(5, 10)$	100	40	28	100/6
$(10, 20)$	400	155	58	400/11

Table 1. Various total storage values for MTA-free (k, n)-threshold schemes.

References

1. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. *Adv. in Cryptology - CRYPTO'88, Lecture Notes in Comput. Sci*, 403:27–35, 1990.
2. G. R. Blakley. Safeguarding cryptographic keys. *Proceedings of AFIPS 1979 National Computer Conference*, 48:313–317, 1979.
3. E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology*, 5:153–166, 1992.
4. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology*, 6:157–167, 1993.
5. R. G. Gallager. *Information theory and reliable communication.* John Wiley and Sons, New York, 1968.
6. I. Ingemarsson and G. J. Simmons. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. *Adv. in Cryptology – EUROCRYPT'90, Lecture Notes in Comput. Sci.*, 473:266–282, 1991.
7. W.-A. Jackson and K. M. Martin. A combinatorial interpretation of ramp schemes. Submitted, 1994.
8. K. M. Martin. New secret sharing schemes from old. *J. Combin. Math Combin. Comput.*, 14:65–77, 1993.
9. C. Meadows. Some threshold schemes without central key distributors. *Congressus Numerantium*, 46:187–199, 1985.
10. A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979.
11. G. J. Simmons. The consequences of trust in shared secret schemes. *Adv. in Cryptology – EUROCRYPT'93, Lecture Notes in Comput. Sci.*, 765:448–452, 1994.
12. G. J. Simmons, W.-A. Jackson, and K. Martin. The geometry of shared secret schemes. *Bull. Inst. Combin. Appl.*, 1:71–88, 1991.
13. D. R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.*, 2:357–390, 1992.
14. D. R. Stinson. Decomposition constructions for secret sharing schemes. *IEEE Trans. Inform. Theory*, 40:118–125, 1994.