J. Cryptology (1997) 10: 261–289

Journal of
CRYPTOLOGY


# Mutually Trusted Authority-Free Secret Sharing Schemes*

Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe
Department of Pure Mathematics, The University of Adelaide,
Adelaide 5005, Australia

Communicated by Douglas R. Stinson

Received 13 September 1995 and revised 10 April 1996

**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 secret sharing schemes 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. Several efficiency measures are proposed and we consider how to refine the general protocol in order to improve the efficiency with respect to each of the proposed measures. Special attention is given to mutually trusted authority-free threshold schemes. Constructions are presented for such threshold schemes that are shown to be optimal with respect to each of the proposed efficiency measures.

**Key words.** Secret sharing 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 (*authorized sets*) are desired to be able to reconstruct the secret from their respective pooled shares. Further, certain sets of participants (*unauthorized sets*) are desired not to be able to reconstruct the secret from their respective pooled shares. The collections of authorized and unauthorized sets, denoted by $\Gamma$ and $\Delta$, respectively, are assumed to be disjoint and are called the *access structure* $(\Gamma, \Delta)$ of the secret sharing scheme. Further, if every subset of participants belongs to either $\Gamma$ or $\Delta$, then $(\Gamma, \Delta)$ is called *complete* and is denoted by $\Gamma$.

It is natural to make the assumption that if a set $A$ of participants contains an authorized set, then $A$ is itself authorized, and that if a set $B$ is contained in an unauthorized set, then

* A preliminary extended abstract of this paper was presented at EUROCRYPT '95. This work was supported by the Australian Research Council.

$B$ is itself unauthorized. An access structure with these properties is called *monotone*. Throughout this paper we assume that every access structure is monotone.

A secret sharing scheme on $n$ participants in which all subsets of size at least $k$ (for some $k \in \{1, \ldots, n\}$) are authorized and all subsets of size less than $k$ are unauthorized is known as a $(k, n)$-*threshold scheme* (we also call the corresponding access structure $(k, n)$-*threshold*). Threshold schemes were the first types of secret sharing scheme proposed [3], [20].

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 number within a given domain. This might be a bank account number, the number of a security box, or an enabling code. Thus, in the case of an explicit secret, the secret value comes first and the secret sharing scheme is then designed to protect that secret value. On the other hand, 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. In other words, the secret sharing scheme is set up first, and the secret value that the shares can be used to reconstruct is *subsequently* adopted as the "secret" (perhaps a cryptographic key). For instance, an application was described in [13] where the shares of an implicit secret were entered during the initialization of the locking mechanism in a vault door. The secret value corresponding to these shares was then calculated and adopted as the secret combination that, if reconstructed, would open the vault door. A secret sharing scheme can also have an implicit secret when the scheme is being used only to demonstrate that a particular concurrence has taken place during an access control protocol. In such a situation, reconstruction of the correct secret value shows that an authorized group of participants have pooled their shares, but the secret value itself has no further significance. For example, suppose concurrence of certain personnel at a bank is needed before large transactions are approved. A secret sharing scheme could be set up with the pretext that approval will only be granted if the correct secret value is reconstructed (and hence an authorized group of employees have pooled their shares). In this case, the secret value has no significance other than as a means of verifying that an authorized concurrence has taken place and hence an implicit secret is sufficient for the application.

Traditional models for secret sharing schemes rely on the existence of a *Mutually Trusted Authority* (MTA) to initialize the scheme. This authority must be trusted by all the participants and can be either human (perhaps an organization) or 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. In the proposed schemes a participant generates their own share, and communicates information about this share to other participants. We will call such schemes *MTA-free*. We replace the reliance on an MTA by the assumption that the participants can communicate securely among themselves. Thus the use of an MTA-free scheme is restricted to situations where secure channels exist between the participants

in the scheme. The MTA-free schemes that we consider all have implicit secrets. Unless an access structure admits an authorized set comprising a singleton participant, we do not believe it is possible to devise a protocol which allows a group of participants to generate their own shares to protect an explicit secret with that access structure. If there is an authorized set comprising a singleton participant 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, authorized as a singleton set.

We note first that there does exist one family of complete access structures which can be easily realized by MTA-free secret sharing schemes. A *unanimous* $(n, n)$-threshold scheme can be constructed without an MTA, as follows. Let $w \geq 2$ be a fixed positive integer.

**The Unanimous Threshold Scheme**

- 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 [19]. In this novel paper a $(k, n)$-threshold scheme is proposed which allows the first $k$ participants to generate their own (random) shares. However, a "black box" is then required to generate the shares of the remaining $n - k$ participants. This black box is 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 [13] reconsidered the design of MTA-free schemes for complete access structures and suggested an elegant protocol. The basic idea 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. In [13] it is suggested that this procedure can be used to realize an MTA-free scheme for any complete access structure. We will later prove this suggestion to be correct.

Ingemarsson and Simmons use their protocol to realize an MTA-free scheme for any $(k, n)$-threshold access structure (with $1 \leq k \leq n$) using either Maximum Distance Separable codes or finite geometric structures as the base and private schemes. Dawson and Donovan [7] reinterpret one of these schemes in terms of Shamir polynomial schemes.

It is clear that if a set of participants performs the Ingemarsson–Simmons protocol described above, then the resulting access structure can be calculated from the particular private access structures chosen. Suppose, however, that the participants wish to set up an MTA-free scheme for a particular predetermined access structure $\Gamma$. Ingemarsson and

Simmons do not provide an algorithm for doing this, and further if an MTA-free scheme for $\Gamma$ is constructed via the Ingemarsson–Simmons protocol there is no guarantee that it is done in an efficient way.

In this paper we address these questions, in the more general setting of access structures which are not necessarily complete. In particular, given an access structure $(\Gamma, \Delta)$ we determine initial MTA-free schemes and private secret sharing schemes which can be used in order to realize an MTA-free scheme for $(\Gamma, \Delta)$. There is not necessarily a unique way of doing this and so we are particularly interested in finding efficient methods, in terms of the amount of information that has to be communicated and/or stored by the participants in the scheme and in terms of the number of separate communications that have to take place in order to initiate the scheme.

In this paper we will consider schemes which provide *unconditional security*, that is, the security is independent of the amount of computing time and resources that are available in any attempt to obtain the secret by some unauthorized means. In contrast, Laih and Harn [17] considered establishing MTA-free schemes with conditional security.

The paper is ordered as follows. In Section 2 we discuss the concept of access structure domination, which is fundamental to the rest of the paper. Section 3 concerns MTA-free schemes in general, and includes a construction protocol which provides an MTA-free scheme for any access structure. Components of the construction protocol are analyzed and three efficiency measures are proposed. In Sections 4, 5, and 6 we consider each of the proposed efficiency measures in turn and discuss some implementations or refinements of the MTA-free protocol that lead to efficient schemes with respect to the appropriate measure. Finally, in Section 7 we prove some bounds on the efficiency measures of MTA-free threshold schemes and describe optimal constructions.

## 2. Access Structure Domination

We now formalize definitions from Section 1 and investigate some properties of access structures, including access structure domination. These are needed in the rest of the paper.

We say that $(\Gamma, \Delta)$ is an *access structure* on a finite set $\mathcal{P}$ of participants if $\Gamma$ and $\Delta$ are disjoint collections of subsets of $\mathcal{P}$ such that if $A \subseteq C \subseteq \mathcal{P}$ and $A \in \Gamma$, then $C \in \Gamma$, and if $C \subseteq B \subseteq \mathcal{P}$ and $B \in \Delta$, then $C \in \Delta$. We say that a set in $\Gamma$ is *authorized* and that a set in $\Delta$ is *unauthorized*. If every subset of $\mathcal{P}$ belongs to either $\Gamma$ or $\Delta$, then we say that $(\Gamma, \Delta)$ is *complete* and usually just write $\Gamma$ for $(\Gamma, \Delta)$, otherwise we say that $(\Gamma, \Delta)$ is *incomplete*. We remark that both $(\Gamma, \bar{\Gamma})$ and $(\bar{\Delta}, \Delta)$ are complete access structures on $\mathcal{P}$ (where if $X$ is a collection of subsets of $\mathcal{P}$, then $\bar{X}$ is the collection of subsets of $\mathcal{P}$ not in $X$).

Let $(\Gamma, \Delta)$ be an access structure defined on participant set $\mathcal{P}$. The monotonicity of $(\Gamma, \Delta)$ ensures that we can find a collection $\Gamma^- = \{C_1, \ldots, C_r\}$ of *minimal* authorized sets in $\Gamma$ and a set $\Delta^+ = \{S_1, \ldots, S_t\}$ of *maximal* unauthorized sets in $\Delta$. We recall from [2] that $\Gamma$ can be considered as a logical expression with the participants being Boolean variables. Let $+$ denote logical OR and let juxtaposition denote logical AND. Then the disjunctive normal form (DNF) of the *logical equivalent* of $\Gamma$ is $\Gamma = C_1 + \cdots + C_r$. It follows that a subset $A$ of participants is authorized if and only if the logical equivalent

of $\Gamma$ is *true* when the variables in $A$ are all true. For example, let $\mathcal{P} = \{a, b, c, d\}$ and $\Gamma^- = \{\{a, b, c\}, \{c, d\}\}$. Then we write $\Gamma = abc + cd$, or equivalently $\Gamma = (ab + d)c$. For notational convenience we write $\Delta = S_1 \diamond \cdots \diamond S_t$.

We now recall from [18] a useful family of access structures that can be derived from $(\Gamma, \Delta)$. Let $A \subseteq \mathcal{P}$. We define the *contraction* $(\Gamma \cdot A, \Delta \cdot A)$ of $(\Gamma, \Delta)$ at $A$ to be the access structure on $\mathcal{P}\backslash A$ such that, for $B \subseteq \mathcal{P}\backslash A$,

$$\begin{aligned} B \in \Gamma \cdot A \quad &\Leftrightarrow \quad B \cup A \in \Gamma; \\ B \in \Delta \cdot A \quad &\Leftrightarrow \quad B \cup A \in \Delta. \end{aligned}$$

Conceptually, $(\Gamma \cdot A, \Delta \cdot A)$ is the access structure that results on $\mathcal{P}\backslash A$ if the shares belonging to the participants in $A$ are publicly revealed. For example, if $(\Gamma, \Delta) = (abc + bcd, ab \diamond cd)$, then $(\Gamma \cdot c, \Delta \cdot c) = (ab + bd, d)$. It will often be convenient to regard $(\Gamma \cdot A, \Delta \cdot A)$ as an access structure on $\mathcal{P}$.

Now let $(\Gamma_0, \Delta_0)$ be an access structure defined on $\mathcal{P} = \{p_1, \ldots, p_n\}$. Associate with each $p_i \in \mathcal{P}$ an access structure $(\Gamma_i, \Delta_i)$ defined on $\mathcal{P}$. For $A \subseteq \mathcal{P}$, let $\mathcal{X}(A) = \{p_i \mid A \in \Gamma_i, 1 \leq i \leq n\}$ and let $\bar{\mathcal{X}}(A) = \{p_i \mid A \notin \Delta_i, 1 \leq i \leq n\}$. Note that for $A \subseteq \mathcal{P}$ we have that $\mathcal{X}(A) \subseteq \bar{\mathcal{X}}(A)$. We define $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$ to be such that for $A \subseteq \mathcal{P}$,

$$\begin{aligned} A \in \Gamma' \quad &\Leftrightarrow \quad \mathcal{X}(A) \in \Gamma_0, \\ A \in \Delta' \quad &\Leftrightarrow \quad \bar{\mathcal{X}}(A) \in \Delta_0. \end{aligned}$$

It is straightforward to verify that $(\Gamma', \Delta')$ is an access structure on $\mathcal{P}$.

**Example 1.** Let $\mathcal{P} = \{a, b, c, d\}$. Let $(\Gamma_0, \Delta_0) = (abc, a \diamond b \diamond c)$, $(\Gamma_a, \Delta_a) = (a + bc, b \diamond c)$, $(\Gamma_b, \Delta_b) = (b + c, a)$ and $(\Gamma_c, \Delta_c) = (ab + c, a \diamond b)$. Then, for example, $\mathcal{X}(\{a, b\}) = \{a, b, c\} \in \Gamma_0$, so $\{a, b\} \in \Gamma'$; $\bar{\mathcal{X}}(\{a\}) = \{a\} \in \Delta_0$, so $\{a\} \in \Delta'$. In fact, $((\Gamma_0, \Delta_0); (\Gamma_a, \Delta_a), (\Gamma_b, \Delta_b), (\Gamma_c, \Delta_c)) = (ab + bc + ac, a \diamond b)$.

Note that if $\Gamma_0$ and $\Gamma_1, \ldots, \Gamma_n$ are all complete, then $\Gamma' = (\Gamma_0; \Gamma_1, \ldots, \Gamma_n)$ is complete and can be interpreted as the access structure defined on $\mathcal{P}$ that is formed by replacing $p_i$ by $\Gamma_i$ in the logical equivalent of $\Gamma_0$.

**Example 2.** 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 $\Gamma' = (\Gamma_0; \Gamma_a, \Gamma_b, \Gamma_c, \Gamma_d) = (a + c)(b + d) = ab + ad + bc + cd$.

Let $(\Gamma_0, \Delta_0)$ and $(\Gamma', \Delta')$ be distinct access structures defined on $\mathcal{P} = \{p_1, \ldots, p_n\}$. Using terminology suggested by [21] and [22], we say that $(\Gamma_0, \Delta_0)$ *dominates* $(\Gamma', \Delta')$ if there exist access structures $(\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n)$ such that:

1. $\{p_i\} \in \Gamma_i$ for $i = 1, \ldots, n$; and
2. $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$.

See [21] and [22] for an alternative but equivalent definition of domination in the case in which $\Gamma'$ and $\Gamma_0$ are complete.

From Example 2, we see that $\Gamma_0 = abcd$ dominates $\Gamma' = ab + ad + bc + cd$. We now classify all the access structures that are dominated by a given access structure.

**Theorem 1.** *Let* $(\Gamma_0, \Delta_0)$ *and* $(\Gamma', \Delta')$ *be access structures defined on* $\mathcal{P}$. *Then* $(\Gamma_0, \Delta_0)$ *dominates* $(\Gamma', \Delta')$ *if and only if* $\Gamma_0 \subseteq \Gamma'$ *and* $\Delta_0 \supseteq \Delta'$.

**Proof.** Suppose $(\Gamma_0, \Delta_0)$ dominates $(\Gamma', \Delta')$. Then there exist access structures $(\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n)$ such that $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$ and $\{p_i\} \in \Gamma_i$ for each $i = 1, \ldots, n$. Let $A = \{p_1, \ldots, p_a\} \in \Gamma_0$. For each $i = 1, \ldots, a$, $\{p_i\} \in \Gamma_i$, and hence $A \in \Gamma_i$. Thus $A \subseteq \mathcal{X}(A)$ and so $\mathcal{X}(A) \in \Gamma_0$. It follows by definition that $A \in \Gamma'$ and hence $\Gamma_0 \subseteq \Gamma'$. Let $B = \{p_1, \ldots, p_b\} \notin \Delta_0$. For each $i = 1, \ldots, b$ we have $\{p_i\} \notin \Delta_i$, so $B \subseteq \bar{\mathcal{X}}(B)$. Since $B \notin \Delta_0$, so $\bar{\mathcal{X}}(B) \notin \Delta_0$, and hence $B \notin \Delta'$. Thus $\Delta_0 \supseteq \Delta'$ and the *only if* part of the theorem is proved.

Now suppose that $(\Gamma_0, \Delta_0)$ and $(\Gamma', \Delta')$ are access structures such that $\Gamma_0 \subseteq \Gamma'$ and $\Delta_0 \supseteq \Delta'$. For $i = 1, \ldots, n$, let $\Gamma_i = p_i + \Gamma'$ and $\Delta_i = \Delta' \backslash \Gamma_i$. We show that $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$.

Let $A \subseteq \mathcal{P}$. Then $A \in \Gamma'$ implies that $A \in \Gamma_i$ for each $i$ $(1 \leq i \leq n)$. Thus $\mathcal{X}(A) = \mathcal{P}$ and so $\mathcal{X}(A) \in \Gamma_0$. Conversely, suppose $\mathcal{X}(A) \in \Gamma_0$. By hypothesis, $\mathcal{X}(A) \in \Gamma'$. Further, note that $A \subseteq \mathcal{X}(A) = \{p_i \mid A \in p_i + \Gamma'\}$. Suppose that $A \notin \Gamma'$. If $p_i \in \mathcal{X}(A)$, then $A \in p_i + \Gamma'$; but $A \notin \Gamma'$ so $p_i \in A$ and hence $\mathcal{X}(A) \subseteq A$. Thus $A \in \Gamma'$, a contradiction. It follows that $A \in \Gamma'$, and we have shown that $A \in \Gamma'$ if and only if $\mathcal{X}(A) \in \Gamma_0$.

Finally, we show that $A \in \Delta'$ if and only if $\bar{\mathcal{X}}(A) \in \Delta_0$. Suppose $A \notin \Delta'$. Then $A \notin \Delta_i$ (since $\Delta_i \subseteq \Delta'$) for $i = 1, \ldots, n$ and hence $\bar{\mathcal{X}}(A) = \mathcal{P}$. Since $\mathcal{P} \in \Gamma_0$, $\bar{\mathcal{X}}(A) \notin \Delta_0$. Conversely, suppose $\bar{\mathcal{X}}(A) \notin \Delta_0$, so $\bar{\mathcal{X}}(A) \notin \Delta'$, by hypothesis. Further, note that $A \subseteq \bar{\mathcal{X}}(A)$. Suppose, for contradiction, that $A \in \Delta'$. If $p_i \in \bar{\mathcal{X}}(A)$, then $A \notin \Delta_i$, but $A \in \Delta'$ so $p_i \in A$. Thus $\bar{\mathcal{X}}(A) \subseteq A$, implying that $A = \bar{\mathcal{X}}(A) \notin \Delta'$, a contradiction. Thus $A \notin \Delta'$. □

It is worth noting the following related result for complete schemes which is an interpretation of the main theorem in [21] and [22]. Let $\Gamma'$ and $\Gamma_0$ be complete access structures. We say that $\Gamma_0$ *directly* dominates $\Gamma'$ if there does *not* exist a complete access structure $\Gamma''$ (distinct from $\Gamma_0$ and $\Gamma'$) such that $\Gamma_0$ dominates $\Gamma''$ and $\Gamma''$ dominates $\Gamma'$ (in [22] it is said that $\Gamma_0$ *covers* $\Gamma'$).

**Result 2** [22, Theorem 3.4]. *Let* $\Gamma_0$ *and* $\Gamma'$ *be complete access structures defined on* $\mathcal{P}$. *Then* $\Gamma_0$ *directly dominates* $\Gamma'$ *if and only if there exists a* (*unique*) *maximal unauthorized set* $B$ *of* $\Gamma_0$ *such that* $\Gamma' = \Gamma_0 \cup \{B\}$.

## 3. The Theory of MTA-Free Schemes

We first give a basic model for secret sharing (see, for example, [24]), based on the *entropy* function $H$ (see, for example, [12]). We introduce the following notation: for finite sets $A$ and $B$ we write $AB$ for $A \cup B$ and we write $x$ for the set $\{x\}$.

If $\rho$ is a probability mass function on a finite set $\Omega$, then the *entropy* of $\rho$ is

$$H(\rho) = -\sum_{\omega\in\Omega} \rho(\omega)\log\rho(\omega)$$

(where if $\rho(\omega) = 0$ there is no contribution to the sum). We remark that the base of the logarithm is not specified here, but can be chosen to be any convenient value. As is illustrated by the next example, $H$ measures the uncertainty inherent in a probability mass function $\rho$ on $\Omega$, that is, the uncertainty regarding which event in $\Omega$ will occur.

**Example 3.** Let $\Omega = \{1, \ldots, n\}$. If $\rho(1) = 1$ and $\rho(i) = 0$ for $i = 2, \ldots, n$, then $H(\rho) = 0$. In this case there is no uncertainty about which event in $\Omega$ will occur since the event 1 certainly occurs. On the other hand, if $\rho(i) = 1/n$ for $i = 1, \ldots, n$, then $H(\rho) = \log n$. In this case all events in $\Omega$ are equally likely; so the uncertainty is high. In fact, it is true in general that $0 \le H(\rho) \le \log n$.

For $A \subseteq \Omega$, let $\rho_A$ be the marginal distribution on $A$, that is, $\rho_A$ is the probability mass function on $A$ defined by $\rho_A(\alpha) = \sum_{\{\omega\in\Omega:\,\omega|_A=\alpha\}} \rho(\omega)$. The entropy of $\rho_A$ is therefore $H(\rho_A) = -\sum_{\alpha\in A} \rho_A(\alpha)\log\rho_A(\alpha)$. Further,

$$\begin{aligned}
\rho_{A|B}(\alpha,\beta) &= \frac{\rho_{AB}(\alpha,\beta)}{\rho_B(\beta)},\\
H(\rho_{A|B=\beta}) &= -\sum_{\alpha\in[A]} \rho_{A|B}(\alpha,\beta)\log\rho_{A|B}(\alpha,\beta),\\
H(\rho_{A|B}) &= \sum_{\beta\in[B]} \rho_B(\beta)H(\rho_{A|B=\beta}).
\end{aligned}$$

In the following, for $H(\rho_A)$ we write $H_\rho(A)$.

Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ be a participant set, let $s$ be the secret variable, and let $(\Gamma, \Delta)$ be an access structure on $\mathcal{P}$. 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* $M = (\mathcal{P}, s, \rho)$ *for* $(\Gamma, \Delta)$ is a probability distribution $\rho$ 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 $H_\rho(s|A) = 0$; and
2. if $A \in \Delta$, then $H_\rho(s|A) = H_\rho(s)$.

Where no confusion arises we will write $H$ for $H_\rho$. It is important to notice that if $M$ is a scheme for $(\Gamma, \Delta)$, then $M$ is also a scheme for every access structure $(\Gamma'', \Delta'')$ satisfying $\Gamma'' \subseteq \Gamma$ and $\Delta'' \subseteq \Delta$. We say that $M$ *has access structure* $(\Gamma, \Delta)$ if $\Gamma = \{A \subseteq \mathcal{P} \mid H(s|A) = 0\}$ and $\Delta = \{A \subseteq \mathcal{P} \mid H(s|A) = H(s)\}$. Further, we call $M$ *trivial* if it has access structure $(\Gamma, \Delta)$ where $\Gamma = 2^{\mathcal{P}}$ and $\Delta = \emptyset$.

Secret sharing schemes for complete access structures are called *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 [24]) that in any perfect secret sharing scheme, if $p_i \in A$ for some minimal authorized set $A$, then $H(p_i) \ge H(s)$. 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

[3], [20] that ideal $(k, n)$-threshold schemes can be found for all $1 \leq k \leq n$ (recall that the $(k, n)$-threshold access structure on $\mathcal{P}$, $|\mathcal{P}| = n$, is $\Gamma = \{A \subseteq \mathcal{P} \mid |A| \geq k\}$).

For incomplete schemes note that for $A \notin \Gamma \cup \Delta$ we do not specify a value for $H(s|A)$; all we can say is that $0 \leq H(s|A) \leq H(s)$. We define the *core* of the scheme $M$ to be $\text{core}\, M = \{p \in \mathcal{P} \mid$ there exists $A \subseteq \mathcal{P}$ with $H(s|pA) < H(s|A)\}$. The participants in core $M$ are those which, possibly in cooperation with other participants, can make some contribution toward determining the secret value. If $M$ is perfect, then $\text{core}\, M = \{p \in \mathcal{P} \mid$ there exists $A \in \Gamma^-$ with $p \in A\}$, which is dependent only on $\Gamma$, hence we may denote this set by $\text{core}\, \Gamma$.

In a traditional secret sharing scheme, an MTA selects a distribution rule $\pi$ from $\Omega$ with probability $\rho(\pi)$, then distributes the entry from $[p_i]$ as a share to $p_i$. The element from $[s]$ is the secret. In an MTA-free scheme the participants indirectly select a (random) distribution rule through the generation of their own (random) shares.

Let $M = (\mathcal{P}, s, \rho)$ be a secret sharing scheme on $\mathcal{P} = \{p_1, \ldots, p_n\}$ for $(\Gamma, \Delta)$. Let $A \subseteq s\mathcal{P}$. For $\pi \in \Omega$, let $\pi_A$ denote the tuple $(\pi_a)_{a \in A}$ and let $\Omega(A) = \{\pi_A \mid \pi \in \Omega\}$. The probability distribution $\rho$ induces a probability distribution $\rho_A$ on $\Omega(A)$ such that for $\alpha \in \Omega(A)$ we have $\rho_A(\alpha) = \sum_{\{\pi \in \Omega | \pi_A = \alpha\}} \rho(\pi)$. Let $[A]_\rho = \{\alpha \in \Omega(A) \mid \rho_A(\alpha) > 0\}$. Let $B \subseteq \mathcal{P}$ and $\pi \in \Omega(AB)$ where $\pi_B \in [B]_\rho$. Then define the conditional probability $\rho_{A|B}(\pi_A, \pi_B)$ to be $\rho_{AB}(\pi)/\rho_B(\pi_B)$.

Consider the following extension of the protocol in [13] for setting up an MTA-free scheme. Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ be a set of participants.

**The MTA-Free Protocol**

**Part (A)**. Each participant in a subset $\mathcal{P}_0$ of $\mathcal{P}$ independently and randomly generates their share for a scheme $M_0 = (\mathcal{P}, s, \rho^0)$ for $(\Gamma_0, \Delta_0)$, where $\mathcal{P}_0 = \text{core}\, M_0$.

For $p_i \in \mathcal{P}$, let $x_i$ denote $p_i$'s share in the scheme $M_0$.

**Part (B)**. Each $p_i \in \mathcal{P}_0$ constructs a private secret sharing scheme $M_i = (\mathcal{P}, s_i, \rho^i)$ for some $(\Gamma_i, \Delta_i)$, where $\rho^i_{s_i} = \rho^0_{p_i}$, to protect the explicit secret $x_i$. Note that $x_i \in [s_i]_{\rho^i} = [p_i]_{\rho^0}$ and that $\Gamma_i$ necessarily has the property that $p_i \in \Gamma_i$. For $p_i \in \mathcal{P} \backslash \mathcal{P}_0$, let $M_i$ be the trivial scheme. Now $p_i$ securely communicates the shares of $M_i$ to the participants included in $M_i$.

We prove in Theorem 3 below that Parts (A) and (B) of this protocol together construct a new secret sharing scheme $M = (\mathcal{P}, s, \rho)$, and we calculate an access structure for it. We therefore call a scheme constructed by this protocol an *MTA-free* secret sharing scheme, and write $M = (M_0; M_1, \ldots, M_n)$ when we wish to indicate the construction of $M$ from its component schemes.

We now give the formal construction of an MTA-free scheme. Suppose that $M_0 = (\mathcal{P}, s, \rho^0)$ is a scheme in which each participant's share is independently generated. For $i = 1, \ldots, n$ let $M_i = (\mathcal{P}, s_i, \rho^i)$ where $\rho^i_{s_i} = \rho^0_{p_i}$ and where $p_i$'s share is the value of $s_i$. Recall that $\rho^0$ is defined on the set of tuples $[p_1]_{\rho^0} \times \cdots \times [p_n]_{\rho^0} \times [s]_{\rho^0}$ and for $i = 1, \ldots, n$, $\rho^i$ is defined on the set of tuples $[p_1]_{\rho^i} \times \cdots \times [p_n]_{\rho^i} \times [s_i]_{\rho^i}$. We define $M$ to be $(\mathcal{P}, s, \rho_{s\mathcal{P}})$, where $\rho$ is defined on a set $\Omega$ of tuples $\pi = (\pi_x)_{x \in ss_1 \ldots s_n \mathcal{P}}$ with $\pi_s \in [s]_{\rho^0}$, $\pi_{s_i} \in [s_i]_{\rho^i}$ $(1 \leq i \leq n)$ and $\pi_p = (\pi^1_p, \ldots, \pi^n_p) \in [p]_{\rho^1} \times \cdots \times [p]_{\rho^n}$. We introduce the extra variables $s_1, \ldots, s_n$ for later notational convenience. For $A \subseteq s_i\mathcal{P}$

let $\pi_A^i$ denote $(\pi_x^i)_{x\in A}$. Define $\pi^0 = (\pi_x^0)_{x\in s\mathcal{P}} \in [s\mathcal{P}]_{\rho^0}$ where $\pi_{p_i}^0 = \pi_{s_i}^i$ and $\pi_s^0$ is the unique element of $[s]_{\rho^0}$ with $\rho^0(\pi^0) \neq 0$. Let $\pi \in \Omega$ with $\pi_s = \pi_s^0$ and define $\rho(\pi)$ by

$$\rho(\pi) = \rho^0(\pi^0) \prod_{i=1}^{n} \rho^i_{\mathcal{P}|s_i}(\pi^i_{\mathcal{P}}, \pi^0_{p_i}).$$

Since $p_i$'s share is the value of $s_i$ in $M_i$, we have $\pi_{p_i}^i = \pi_{s_i}^i = \pi_{p_i}^0$. If $M = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ is a secret sharing scheme for $(\Gamma, \Delta)$, then we say that $M$ is an MTA-free secret sharing scheme for $(\Gamma, \Delta)$.

**Theorem 3.** *With $\rho$ defined as in the previous paragraph*:

1. *if $M_i$ is a scheme for $(\Gamma_i, \Delta_i)$ for $i = 0, \ldots, n$, then $M = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ is a scheme for $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$; and*
2. *for $A \subseteq \mathcal{P}$ we have $H_\rho(A) = \sum_{i=1}^n H_{\rho^i}(A)$.*

**Proof.** Let $A \subseteq \mathcal{P}$ and let $\pi \in \Omega$. First let $A \in \Delta'$. If $p_i \notin \bar{\mathcal{X}}(A)$, then $A \in \Delta_i$ so $H_{\rho^i}(s_i|A) = H_{\rho^i}(s_i)$; thus $H_{\rho^i}(A) = H_{\rho^i}(A|s_i)$. Hence

$$\rho^i_{A|s_i}(\pi^i_A, \pi^i_{s_i}) = \rho^i(\pi^i_A). \tag{1}$$

Note that

$$\rho_{sA}(\pi_{sA}) = \sum_{\omega\in[\mathcal{P}]_{\rho^0}} \rho^0(\pi_s\omega) \prod_{i=1}^{n} \rho^i_{A|s_i}(\pi^i_A, \omega_{p_i}) \tag{2}$$

$$= \left( \sum_{\omega\notin[\bar{\mathcal{X}}(A)]_{\rho^0}} \rho^0_{s\bar{\mathcal{X}}(A)}(\pi_s\omega) \prod_{p_i\in\bar{\mathcal{X}}(A)} \rho^i_{A|s_i}(\pi^i_A, \omega_{p_i}) \right) \left( \prod_{p_i\notin\bar{\mathcal{X}}(A)} \rho^i_A(\pi^i_A) \right). \tag{3}$$

If $A = \emptyset$, then $\rho^i_{A|s_i}(\pi^i_A, \omega_{p_i}) = 1$ and so, by (2) we have $\rho_s(\pi_s) = \rho_s^0(\pi_s)$ and therefore $\sum_{\pi\in\Omega} \rho(\pi) = \sum_{\sigma\in[s]_\rho} \rho_s(\sigma) = \sum_{\sigma\in[s]_{\rho^0}} \rho_s^0(\sigma) = 1$. Thus $\rho$ is a probability measure.

As $A \in \Delta'$, $\bar{\mathcal{X}}(A) \in \Delta_0$, so $\rho^0_{s\bar{\mathcal{X}}(A)}(\pi_s\omega) = \rho_s^0(\pi_s)\rho^0_{\bar{\mathcal{X}}(A)}(\omega)$. Thus $\rho_{sA}(\pi_{sA})$ is equal to $\rho_s(\pi_s)$ multiplied by a function independent of $\pi_s$, that is, $H_\rho(s|A) = H_\rho(s)$.

Now let $A \in \Gamma'$ and let $\pi, \tau \in \Omega$ with $\rho(\pi), \rho(\tau) > 0$. Suppose $\tau_A = \pi_A$. Then $\tau_{s_i} = \pi_{s_i}$ for each $p_i \in \mathcal{X}(A)$ (because $A \in \Gamma_i$ and therefore $H_{\rho^i}(s_i|A) = 0$), and so $\tau^0_{\mathcal{X}(A)} = \pi^0_{\mathcal{X}(A)}$. As $\mathcal{X}(A) \in \Gamma_0$ we have $\tau_s = \tau_s^0 = \pi_s^0 = \pi_s$. So $H_\rho(s|A) = 0$. This proves the first part of the theorem.

For the second part, we may assume that $\mathcal{P} \in \Gamma_0$, so $\rho^0_{s\mathcal{P}}(\pi^0_{s\mathcal{P}}) = \rho^0_{\mathcal{P}}(\pi^0_{\mathcal{P}})$. Hence $\rho_{\mathcal{P}}(\pi_{\mathcal{P}}) = \rho^0_{\mathcal{P}}(\pi^0_{\mathcal{P}}) \prod_{i=1}^n \rho^i_{\mathcal{P}|s_i}(\pi^i_{\mathcal{P}}, \pi^i_{s_i})$. Now $\pi^0_{p_i} = \pi^i_{s_i} = \pi^i_{p_i}$ and since the participants choose shares in $M_0$ independently, $\rho^0_{\mathcal{P}}(\pi^0_{\mathcal{P}}) = \prod_{i=1}^n \rho^0_{p_i}(\pi^0_{p_i})$, so $\rho_{\mathcal{P}}(\pi_{\mathcal{P}}) = \prod_{i=1}^n \rho^i_{\mathcal{P}}(\pi^i_{\mathcal{P}})$. Hence for $A \subseteq \mathcal{P}$, $\rho_A(\pi_A) = \prod_{i=1}^n \rho^i_A(\pi^i_A)$ and so $H_\rho(A) = \sum_{i=1}^n H_{\rho^i}(A)$. □

Since a scheme for $(\Gamma', \Delta')$ is also a scheme for $(\Gamma, \Delta)$ where $\Gamma \subseteq \Gamma'$ and $\Delta \subseteq \Delta'$, we have the following corollary.

**Corollary 4.** *Let $M = (M_0; M_1, \ldots, M_n)$ be an MTA-free scheme on $\mathcal{P}$, where for $i = 0, \ldots, n$, $M_i$ is a scheme for $(\Gamma_i, \Delta_i)$. Then $M$ is a scheme for $(\Gamma, \Delta)$ if $A \in \Gamma \Rightarrow \mathcal{X}(A) \in \Gamma_0$ and $A \in \Delta \Rightarrow \bar{\mathcal{X}}(A) \in \Delta_0$.*

**Proof.** By Theorem 3, $M = (\mathcal{P}, s, \rho)$ is a scheme for $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$. Let $A \subseteq \mathcal{P}$. Now $A \in \Gamma \Rightarrow \mathcal{X}(A) \in \Gamma_0 \Rightarrow A \in \Gamma'$ and $A \in \Delta \Rightarrow \bar{\mathcal{X}}(A) \in \Delta_0 \Rightarrow A \in \Delta'$, so $M$ is a scheme for $(\Gamma, \Delta)$. □

We refer to $(\Gamma_0, \Delta_0)$ as the *base* access structure and $M_0$ as the *base* scheme. We refer to $(\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n)$ as the *private* access structures and $M_1, \ldots, M_n$ as the *private* schemes. An MTA-free scheme is essentially a special type of *decomposition* as previously discussed in, for example, [25]. These special decompositions are such that the scheme $M_0$ is determined by the participants in $\mathcal{P}_0$ independently selecting random shares, and such that each access structure $(\Gamma_i, \Delta_i)$ has $p_i \in \Gamma_i$, for $i = 1, \ldots, n$.

We end this section by considering a related problem raised by Simmons [21]. Suppose we are given a scheme $M_0$ for $\Gamma_0$ (not necessarily arising by Part (A) of the MTA-free protocol). For $p_i \in \text{core } M_0$ let $x_i$ denote the share of $p_i$ in $M_0$. Now perform Part (B) of the MTA-free protocol. Simmons asks which access structures can be realized in this way. The following theorem considers the general case.

**Theorem 5.** *Let $M_0$ be any scheme for $(\Gamma_0, \Delta_0)$ and let $x_i$ denote the share of $p_i$ in $M_0$. A scheme $M = (M_0; M_1, \ldots, M_n)$ for $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$ can arise by Part (B) of the MTA-free protocol if and only if $\Gamma_0 \subseteq \Gamma'$ and $\Delta_0 \supseteq \Delta'$.*

**Proof.** Suppose $M = (M_0; M_1, \ldots, M_n)$ for $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$ arises by Part (B) of the MTA-free protocol. Then, for $i = 1, \ldots, n$ we have $p_i \in \Gamma_i$ and by definition $(\Gamma_0, \Delta_0)$ dominates $(\Gamma', \Delta')$. By Theorem 1, $\Gamma_0 \subseteq \Gamma'$ and $\Delta_0 \supseteq \Delta'$. Conversely, suppose $\Gamma_0 \subseteq \Gamma'$ and $\Delta_0 \supseteq \Delta'$. By Theorem 1, $(\Gamma_0, \Delta_0)$ dominates $(\Gamma', \Delta')$, hence there exist schemes $M_1, \ldots, M_n$ for $(\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n)$ such that $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$. Suppose Part (B) of the MTA-free protocol is performed on $M_0$, using the schemes $M_1, \ldots, M_n$. The first part of the proof of Theorem 3 shows that $M$ is a scheme for $(\Gamma', \Delta')$, as required. □

Therefore, the answer to Simmons' question is: *Given a base scheme $M_0$ for $\Gamma_0$, a scheme $M$ for $\Gamma$ can arise by Part (B) of the MTA-free protocol (using only complete schemes) if and only if $\Gamma_0 \subseteq \Gamma$.*

### 3.1. *The Base Access Structure*

The first issue to be considered in the design of an MTA-free scheme is the selection of the base access structure $(\Gamma_0, \Delta_0)$. Recall that in Part (A) of the MTA-free protocol each $p \in \mathcal{P}_0$ independently generates a random share of $M_0$ from a set $[p]$.

**Theorem 6.** *Let $M_0 = (\mathcal{P}, s, \rho^0)$ be a secret sharing scheme 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*

*$M_0$ has access structure $(\Gamma_0, \Delta_0)$ such that $\Gamma_0$ has a unique minimal authorized set. Further, this unique minimal authorized set is* core $M_0$.

**Proof.** As each $p \in \mathcal{P}$ independently generates a share, we have $H(\mathcal{P}) = \sum_{p\in\mathcal{P}} H(p)$ and so for $X, Y \subseteq \mathcal{P}$ with $X \cap Y = \emptyset$, we have $H(XY) = H(X)+H(Y)$. Using this fact, suppose there exist two minimal authorized sets $A$, $B$ of $\Gamma_0$. Let $X = A \cap B$, $A' = A\backslash X$, and $B' = B\backslash X$. Then

$$\begin{aligned} H(X) &= H(A'X) + H(B'X) - H(A'B'X) \\ &= H(sA'X) + H(sB'X) - H(sA'B'X), \qquad \text{as} \quad A, B \in \Gamma \\ &= H(sXA') - H(A'|sB'X) \\ &= H(sX) + H(A'|sX) - H(A'|sB'X) \\ &\geq H(sX). \end{aligned}$$

Hence $H(s|X) = 0$ and thus by minimality of $A$ and $B$, $X = A = B$.

Let $\mathcal{P}_0$ be the unique minimal authorized set and let $p \in \mathcal{P}_0$. Then $\mathcal{P}_0\backslash p \notin \Gamma_0$ and it follows that $0 = H(s|\mathcal{P}_0) < H(s|\mathcal{P}_0\backslash p)$, implying that $p \in$ core $M_0$. Thus $\mathcal{P}_0 \subseteq$ core $M_0$.

Now let $p \in$ core $M_0$ and let $A \subseteq \mathcal{P}$ be such that $H(s|pA) < H(s|A)$; so that $H(spA) < H(sA)+H(p)$, thus $H(p|sA) < H(p)$. Suppose $p \notin \mathcal{P}_0$, hence there exists $B \subseteq \mathcal{P}$ with $pAB$, $AB \in \Gamma$. Thus $0 = H(s|pAB) = H(s|AB)$, and so $H(psAB) - H(p) - H(AB) = H(sAB) - H(AB)$. Hence $H(p) = H(p|sAB) \leq H(p|sA) < H(p)$ (from above), a contradiction. □

Suppose we wish to apply the MTA-free protocol to construct a scheme for an access structure $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$. By Theorems 5 and 6, the base access structure $(\Gamma_0, \Delta_0)$ satisfies $\Gamma_0 \subseteq \Gamma'$, $\Delta_0 \supseteq \Delta'$, and $\Gamma_0$ has a unique minimal authorized set $\mathcal{P}_0$, which is equal to core $M_0$.

Note that if $M_0$ is a perfect secret sharing scheme, then $M_0$ is a unanimous threshold scheme defined on $\mathcal{P}_0$.

### 3.2. *The Private Access Structures*

We note the following constraint on the choice of private access structures.

**Lemma 7.** *Let $M = (M_0; M_1, \ldots, M_n)$ be an MTA-free scheme such that $M$ has access structure $(\Gamma, \Delta)$. Suppose that for $i = 0, \ldots, n$, $M_i$ has access structure $(\Gamma_i, \Delta_i)$ and let $(\Gamma', \Delta') = ((\Gamma_0, \Delta_0); (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n))$. Then $\Gamma = \Gamma'$ and for $i = 1, \ldots, n$ we have $\Gamma' \subseteq \Gamma_i$.*

**Proof.** We use the notation introduced earlier in Section 3. We first show that $\Gamma = \Gamma'$. By Theorem 3(1), we have $\Gamma' \subseteq \Gamma$. Conversely, suppose $A \in \Gamma$. For every $\pi, \tau \in \Omega$ with $\rho(\pi), \rho(\tau) > 0$ and $\tau_A = \pi_A$, then $\tau_s = \pi_s$. However, if $\mathcal{X}(A) \notin \Gamma_0$, then we can find $\pi, \tau \in \Omega$ with $\rho(\pi), \rho(\tau) > 0$ and $\tau_A = \pi_A$, $\tau^0_{\mathcal{X}(A)} = \pi^0_{\mathcal{X}(A)}$ and $\tau^0_s \neq \pi^0_s$. As $\tau_s = \tau^0_s$ and $\pi_s = \pi^0_s$, it follows that $\tau_s \neq \pi_s$, a contradiction. So $A \in \Gamma'$; hence $\Gamma = \Gamma'$.

We now show that for $i = 1, \ldots, n$, $\Gamma' \subseteq \Gamma_i$. Let $A \in \Gamma'$. Then $\mathcal{X}(A) \in \Gamma_0$, so by Theorem 6 we have $\mathcal{P}_0 \subseteq \mathcal{X}(A)$. Thus for $p_i \in \mathcal{P}_0$ we have $A \in \Gamma_i$. If $p_i \notin \mathcal{P}_0$, then $\Gamma_i^- = \{\emptyset\}$ (see Part (B) of the MTA-free protocol) so if $A \in \Gamma'$, then $A \in \Gamma_i$; hence $\Gamma' \subseteq \Gamma_i$. □

While we will primarily be interested in constructing MTA-free schemes for complete access structures, we will show that efficient schemes often arise by using base or private schemes with incomplete access structures.

### 3.3. *The Basic Construction*

Suppose we wish to construct an MTA-free scheme for an access structure $(\Gamma, \Delta)$. It suffices to construct schemes $M_0, \ldots, M_n$ for suitable $(\Gamma_0, \Delta_0), (\Gamma_1, \Delta_1), \ldots, (\Gamma_n, \Delta_n)$ to be used in the MTA-free protocol. The results of Sections 3.1 and 3.2 imply that $\Gamma_0^- = \{\mathcal{P}_0\}$, $\mathcal{P}_0 = \text{core } M_0 \in \Gamma$, and for $i = 1, \ldots, n$ we have $\Gamma \subseteq \Gamma_i$ and $p_i \in \Gamma_i$.

The following construction, called the *Basic Construction*, was previewed in the proof of Theorem 1 and is an easy way to satisfy these requirements.

**The Basic Construction for** $(\Gamma, \Delta)$

| | |
|---|---|
| $\Gamma_0$ | $(n, n)$-threshold on $\mathcal{P}$ (so $\mathcal{P}_0 = \mathcal{P}$) |
| $\Gamma_i$ | $p_i + \Gamma$ (for each $p_i \in \mathcal{P}$) |
| $\Delta_i$ | $\Delta \backslash \Gamma_i$ (for each $p_i \in \mathcal{P}$) |
| $M_0$ | ideal unanimous threshold scheme on $\mathcal{P}$ |
| $M_i$ | scheme for $(\Gamma_i, \Delta_i)$ (for each $p_i \in \mathcal{P}$) |

**Proof (Basic Construction).** We use Corollary 4. Let $A \in \Gamma$. For $i = 1, \ldots, n$ we have $\Gamma \subseteq \Gamma_i$, so $A \in \Gamma_i$. Thus $\mathcal{X}(A) = \mathcal{P} \in \Gamma_0$. Let $A \in \Delta$. For $p_i \in \mathcal{P} \backslash A$, we have $A \notin \Gamma_i$ and therefore $A \in \Delta_i$. Thus $\bar{\mathcal{X}}(A) \neq \mathcal{P}$; so $\bar{\mathcal{X}}(A) \notin \Gamma_0$. The proof follows since $\Gamma_0$ is complete. □

An immediate but important observation to make is that since the Basic Construction can be used for any access structure $(\Gamma, \Delta)$, we have the following theorem.

**Theorem 8.** *There exists an MTA-free scheme for any access structure* $(\Gamma, \Delta)$.

### 3.4. *Measures of Efficiency*

There are a number of different parameters that may be considered as measures of efficiency of an MTA-free scheme. Recall that we allow any two participants to communicate with one another using a secure channel. We propose three different efficiency measures, each based on a different assumption. It follows that the significance of each measure in a particular situation depends on the relevance of each assumption. The three assumptions are:

1. that it is costly to initiate a communication using a secure channel;
2. that it is costly to transmit information over a secure channel; and
3. that it is costly to store information.

First, suppose we wish to minimize the number of separate communications that have to take place between pairs of participants in order for the MTA-free scheme to be initiated. This measure does not take into account the amount of information transmitted in each communication, but it is an important parameter if the cost of establishing a communication between two participants is regarded as significant. Thus if $M = (M_0; M_1, \ldots, M_n)$ is an MTA-free scheme and $M_i$ has core $\mathcal{P}_i$, then we define the *linkage* of $M$ to be

$$\ell(M) = \sum_{p_i \in \mathcal{P}_0} (|\mathcal{P}_i| - 1).$$

Second, assuming that it is expensive to transmit information, an obvious parameter to aim to minimize is the total amount of information that has to be transmitted over all the secure channels in order to initiate the MTA-free scheme. To compute this value we use the *contribution vector* (or *convec*) of a secret sharing scheme. For a scheme $M = (\mathcal{P}, s, \rho)$, this is the vector $(c_1, \ldots, c_n) = (H(p_1), \ldots, H(p_n))/H(s)$. Let $M = (M_0; M_1, \ldots, M_n)$ be an MTA-free scheme. If $M_0$ has convec $(d_1, \ldots, d_n)$ and $M_i$ has convec $(e_{i1}, \ldots, e_{in})$ $(1 \leq i \leq n)$ then we define the *potential storage* of $M$ to be

$$\mathcal{V}(M) = \sum_{i=1}^{n} \sum_{j=1}^{n} d_j e_{ji}.$$

From Theorem 3, we see that $\mathcal{V}(M) = \sum_{i=1}^{n} c_i$, where $M$ has convec $(c_1, \ldots, c_n)$ with $c_i = \sum_{j=1}^{n} d_j e_{ji}$ $(1 \leq i \leq n)$. Thus the potential storage is a measure of the total information generated by all the participants when setting up their private schemes, which in turn is the total information transmitted between all the participants plus the information that each participant generates as a share in their own private scheme.

Note that if $M$ is an MTA-free scheme arising from perfect schemes $M_0, M_1, \ldots, M_n$ for $\Gamma_0, \Gamma_1, \ldots, \Gamma_n$, respectively, then the potential storage of $M$ is dependent on $M_0$, $M_1, \ldots, M_n$ whereas the linkage is only dependent on the access structures $\Gamma_0, \Gamma_1, \ldots, \Gamma_n$. Thus it does not necessarily follow that a scheme $M$ with a low linkage will have a low potential storage, and vice versa. Neither does it follow that we can determine the potential storage directly from the linkage. However, in the event that $M_0, M_1, \ldots, M_n$ are ideal, then it follows that $\mathcal{V}(M) = \ell(M) + |\mathcal{P}_0|$.

Notice that if the participants in the scheme store all the information that is transmitted to them as their share in the final scheme, then the potential storage also measures the amount of information stored by participants. However, we call this quantity the *potential* storage because we will show that in many cases a participant only needs to store a smaller amount of information. For each participant, this reduced share can be computed from the total information transmitted to them. Let $M^*$ denote the scheme $M = (M_0; M_1, \ldots, M_n)$ after any reduction of share information has taken place and let the convec of $M^*$ be $(c_1^*, \ldots, c_n^*)$. To provide a measure of the actual storage of the reduced scheme $M^*$ we use the conventional measures of information rate and average information rate that are normally applied to traditional (perfect) secret sharing schemes (for example, [5], [6], [18], and [25]). The *information rate* and the *average information rate* of $M^*$ are thus, respectively, given by

$$\rho(M^*) = \min_{1 \leq i \leq n} \frac{1}{c_i^*}, \qquad \tilde{\rho}(M^*) = \frac{n}{c_1^* + \cdots + c_n^*}.$$

If no share reduction takes place, then $M = M^*$ and so minimizing the potential storage is equivalent to maximizing the average information rate.

Given an access structure $(\Gamma, \Delta)$, we will be interested in the minimum possible values of linkage and potential storage. We therefore denote by $\ell(\Gamma, \Delta)$ (respectively, $\mathcal{V}(\Gamma, \Delta)$) the minimum over all MTA-free schemes $M$ for $(\Gamma, \Delta)$ of the values $\ell(M)$ (respectively, $\mathcal{V}(M)$). Since $|\mathcal{P}_0| \leq n$ and $|\mathcal{P}_i| \leq n$ for $p_i \in \mathcal{P}$, it follows that $\ell(\Gamma, \Delta) \leq \sum_{i=1}^{n}(n-1) = n(n-1)$. Likewise, we will be intererested in the maximum possible values of information rate and average information rate over all MTA-free schemes $M^*$ for $(\Gamma, \Delta)$. We denote these by $\rho_{MTA}(\Gamma, \Delta)$ and $\tilde{\rho}_{MTA}(\Gamma, \Delta)$, respectively. We reserve the notation $\rho(\Gamma, \Delta)$ and $\tilde{\rho}(\Gamma, \Delta)$ for the maximum information rate and average information rate over *all* schemes for $(\Gamma, \Delta)$.

**Example 4.** 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 [23]) we can find ideal $M_a, M_b, M_c, M_d$ and thus a scheme $M$ for $\Gamma$ 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 $b$,$c$,$d$). In this case $\mathcal{V}(M) = 14$ and $\ell(M) = 10$.

## 4. Reducing the Linkage

We have already seen that the Basic Construction provides an MTA-free scheme for $\Gamma$, however we can make a considerable improvement on the linkage achieved by the Basic Construction by applying suitable contractions. We call this modified construction method the *Contraction Construction*, and remark that it works for any complete access structure $\Gamma$.

**The Contraction Construction for $\Gamma$**

| | |
|---|---|
| $\Gamma_0$ | $(a, a)$-threshold on $\mathcal{P}_0$, for some $\mathcal{P}_0 = \{p_1, \ldots, p_a\} \in \Gamma$ |
| $\Gamma_1$ | $p_1 + \Gamma$ |
| $\Gamma_2$ | $p_2 + \Gamma \cdot \{p_1\}$ |
| $\vdots$ | $\vdots$ |
| $\Gamma_a$ | $p_a + \Gamma \cdot \{p_1, p_2, \ldots, p_{a-1}\}$ |
| $\Gamma_j$ | "true," for $p_j \notin \mathcal{P}_0$ |
| $M_0$ | ideal unanimous threshold scheme on $\mathcal{P}_0$ |
| $M_i$ | (perfect) scheme for $\Gamma_i$ (for $i = 1, \ldots, a$) |

Note that a scheme produced by applying the Contraction Construction depends on both the base set $\mathcal{P}_0$ chosen and the order placed upon the participants of $\mathcal{P}_0$.

**Proof (Contraction Construction).** We use Corollary 4. Let $A \in \Gamma$. Then $A \in \Gamma \cdot X$ (for any $X \subseteq \mathcal{P}_0$), and so $A \in \Gamma_i$ for $i = 1, \ldots, a$. Thus $\mathcal{X}(A) = \mathcal{P}_0$ and so $\mathcal{X}(A) \in \Gamma_0$. Let $A \in \Delta$, so that $A \notin \Gamma$. Let $i \in \{1, \ldots, a\}$ be the integer such that $p_1, \ldots, p_{i-1} \in A$

but $p_i \notin A$ ($i$ exists for otherwise $\mathcal{P}_0 \subseteq A$, so $A \in \Gamma$). Then $A \notin \Gamma_i$, so $\mathcal{P}_0 \not\subseteq \bar{\mathcal{X}}(A)$; hence $\bar{\mathcal{X}}(A) \notin \Gamma_0$. The proof follows since $\Gamma_0$ is complete. □

**Example 5.** Let $\mathcal{P}$ and $\Gamma$ be as in Example 4. Applying the Contraction Construction with $\mathcal{P}_0 = \{a, b\}$ and $\Gamma_0 = ab$ gives $\Gamma_a = a + bcd$, $\Gamma_b = b + c$. Since $\Gamma_a$, $\Gamma_b$ are ideal (see [23]) we can find ideal $M_a$, $M_b$ and thus a scheme $M'$ for $\Gamma$ 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 $\Gamma_b$, $\Gamma_c$, $\Gamma_d$ are ideal (see [23]) we can find ideal $M_b$, $M_c$, $M_d$ and thus a scheme $M''$ for $\Gamma$ with convec $(3, 1, 2, 1)$. So $\mathcal{V}(M') = 6$, $\mathcal{V}(M'') = 7$, and $\ell(M') = \ell(M'') = 4$. Thus scheme $M'$ is slightly more efficient than $M''$ and both $M'$ and $M''$ are considerably more efficient in terms of potential storage and linkage than the scheme $M$ constructed in Example 4.

In particular, we will be interested in the Contraction Construction applied to $(k, n)$-threshold schemes.

**The Contraction Construction for $(k, n)$-Threshold $\Gamma$**

| | |
|---|---|
| $\Gamma_0$ | $(k, k)$-threshold on $\mathcal{P}_0$, for some $\mathcal{P}_0 = \{p_1, \ldots, p_k\} \in \Gamma$ |
| $\Gamma_i$ | $p_i + \Gamma_i'$ where $\Gamma_i'$ is $(k - i, n - i + 1)$-threshold on $\{p_i, \ldots, p_n\}$ for $p_i \in \mathcal{P}_0$ |
| $\Gamma_j$ | "true" for $p_j \notin \mathcal{P}_0$ |
| $M_0$ | ideal unanimous threshold scheme on $\mathcal{P}_0$ |
| $M_i$ | scheme for $\Gamma_i$, for $i = 1, \ldots, k$ |

We can calculate the convec $(c_1, \ldots, c_n)$ 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

$$\mathcal{V}(M) = \frac{k(k+1)}{2} + k(n-k) = nk - \frac{k(k-1)}{2}, \tag{4}$$

$$\ell(M) = s(M) - k = nk - \frac{k(k+1)}{2}. \tag{5}$$

**Theorem 9.** *Let $\Gamma$ be a complete access structure on $\mathcal{P}$ where $|\mathcal{P}| = n$ and let $a = \min_{A \in \Gamma} |A|$. Then $\ell(\Gamma) \leq na - a(a+1)/2$.*

**Proof.** Let $M$ be an MTA-free scheme for $\Gamma$ constructed by the Contraction Construction using a set $\mathcal{P}_0 \in \Gamma$ of cardinality $a$. Since $|\mathcal{P}_1| \leq n$, $|\mathcal{P}_2| \leq n - 1, \ldots, |\mathcal{P}_a| \leq n - (a - 1)$, we have $\ell(M) \leq \sum_{i=0}^{a-1} (n - i - 1) = na - a(a+1)/2$. □

Note that the bound of Theorem 9 is an improvement on the bound $n(n-1)$ given in the last section. We now show that for $\Gamma$ complete, the Contraction Construction is just a special case of a more general construction process. Recall from Theorem 6 that the base access structure $\Gamma_0$ is an $(a, a)$-threshold structure defined on some $\mathcal{P}_0 =$

$\{p_1, \ldots, p_a\} \in \Gamma$. It follows that $\Gamma_0$ dominates $\Gamma$ if and only if the logical equivalent of $\Gamma$ can be expressed in the form

$$\Gamma = (p_1 + \Gamma_1)(p_2 + \Gamma_2) \cdots (p_a + \Gamma_a). \tag{6}$$

The Contraction Construction is simply a method of finding a set of access structures $\Gamma_1, \ldots, \Gamma_a$ such that (6) holds. In order to find MTA-free schemes with low linkage it is desirable to find private access structures $\Gamma_1, \ldots, \Gamma_a$ that have small cores.

**Example 6.** Let $\Gamma = ac + ad + bc + bd$. By exhausting the possibilities for $\mathcal{P}_0$ and the orderings of $\mathcal{P}_0$ we see that the minimum linkage possible by applying the Contraction Construction is 4 (for example, $\mathcal{P}_0 = \{a, c\}$, $\Gamma_a = a + bc + bd$, $\Gamma_c = c + d$). However, by observing that $\Gamma = (a + b)(c + d)$ we can choose $\mathcal{P}_0 = \{a, c\}$, $\Gamma_a = a + b$, $\Gamma_c = c + d$, to achieve a linkage of 2.

We therefore generalize the Contraction Construction. The main improvement with respect to linkage is that it may be possible to choose schemes $M_1, \ldots, M_n$ with cores smaller than the cores of the schemes arising under the Contraction Construction. With respect to potential storage, the shares may be smaller. This generalization also extends to incomplete access structures. Note that as in the Contraction Construction, a scheme produced by applying this Generalized Contraction Construction (GCC) depends on both the base set $\mathcal{P}_0$ chosen and the order placed upon the participants of $\mathcal{P}_0$.

**The Generalized Contraction Construction for** $(\Gamma, \Delta)$

| | |
|---|---|
| $\Gamma_0$ | $(a, a)$-threshold on $\mathcal{P}_0$, for some $\mathcal{P}_0 = \{p_1, \ldots, p_a\} \in \Gamma$ |
| $\Gamma_1$ | $p_1 + \Gamma$ |
| $\Gamma_2$ | $p_2 + \Gamma \cdot \{p_1\}$ |
| $\vdots$ | $\vdots$ |
| $\Gamma_a$ | $p_a + \Gamma \cdot \{p_1, p_2, \ldots, p_{a-1}\}$ |
| $\Delta_i$ | defined by $\Delta_i^+ = \Delta^+ \backslash (\Gamma_i \cup \Delta_1^+ \cup \cdots \cup \Delta_{i-1}^+)$ for $i = 1, \ldots, a$ |
| $\Gamma_j$ | "true" for $p_j \notin \mathcal{P}_0$ |
| $M_0$ | ideal unanimous threshold scheme on $\mathcal{P}_0$ |
| $M_i$ | scheme for $(\Gamma_i, \Delta_i)$ for $i = 1, \ldots, a$ |

**Proof (Generalized Contraction Construction).** We use Corollary 4. As in the proof of the Contraction Construction, if $A \in \Gamma$, then $\mathcal{X}(A) \in \Gamma_0$. Now suppose $A \in \Delta$, and let $B \subseteq \mathcal{P}$ be such that $A \subseteq B \in \Delta^+$. Let $i \in \{1, \ldots, a\}$ be the smallest value with $B \notin \Gamma_i$. So $B \in \Gamma_1, \ldots, \Gamma_{i-1}$ and hence $B \notin \Delta_1^+, \ldots, \Delta_{i-1}^+$. Hence $B \in \Delta_i^+$, and so $p_i \notin \bar{\mathcal{X}}(B)$. Thus $\mathcal{P}_0 \not\subseteq \bar{\mathcal{X}}(B)$ and since $\bar{\mathcal{X}}(A) \subseteq \bar{\mathcal{X}}(B)$, we have $\mathcal{P}_0 \not\subseteq \bar{\mathcal{X}}(A)$ and therefore $\bar{\mathcal{X}}(A) \in \Delta_0$. □

Note that using the GCC, the collection $\Delta^+$ of maximal unauthorized sets is partitioned by the collections $\Delta_i^+$ $(1 \leq i \leq a)$. We also note that the GCC gives the same result as the Contraction Construction for $(k, n)$-threshold schemes.

**Example 7.** Let $\Gamma = ac + ad + bc + bd$ as in Example 6. So $\Delta^+ = \{ab, cd\}$. Let $\mathcal{P}_0 = \{a, c\}$, so $\Delta_a^+ = \{cd\}$, $\Delta_c^+ = \{ab\}$. Letting $M_a$ be a scheme for $\bar{\Delta}_a$ and $M_c$ be a scheme for $\bar{\Delta}_c$ results in a linkage of 2. The reasons for this choice of $M_a$ and $M_c$ follow from the next lemma.

**Lemma 10.** *Let $M_i$ be a scheme for $(\Gamma_i, \Delta_i)$, as in the GCC for $\Gamma$. Then* core $M_i \supseteq$ core $\bar{\Delta}_i$.

**Proof.** Suppose that $M_i$ is a scheme for $(\Gamma_i, \Delta_i)$, as in the GCC. Let $p \in$ core $\bar{\Delta}_i$. So there exists $B \in \Delta_i^+$ with $p \notin B$. As $B \in \Delta^+$ we have $pB \in \bar{\Delta} = \Gamma$ and thus $pB \in \Gamma_i$. Hence $H(s|B) = H(s)$ and $H(s|pB) = 0$ in $M_i$. So, by definition, $p \in$ core $M_i$. Thus core $M_i \supseteq$ core $\bar{\Delta}_i$. □

Now for the case when $\Gamma$ is complete, we discuss a procedure for selection of a suitable base set and an order of contraction which aim to minimize the linkage.

We will use the GCC with $\mathcal{P}_0 = \{p_1, \ldots, p_a\}$ to produce a scheme for $\Gamma$. By Lemma 10, in order to minimize the linkage of the resultant scheme $M$, let $M_i$ be a scheme for $\bar{\Delta}_i$ $(1 \le i \le a)$. In this case, the linkage of $M$ is $\sum_{i=1}^{a}(|\text{core } \bar{\Delta}_i| - 1)$.

We now address the question as to which set $\mathcal{P}_0$ and which ordering of the elements in $\mathcal{P}_0$ should be used with the GCC. Intuition and experimental evidence suggest that $\mathcal{P}_0$ should be a minimal set of minimal size, however a formal proof of this remains an open problem. The following algorithm reflects this choice, and further suggests an appropriate ordering of the elements of the selected $\mathcal{P}_0$.

First we define the following sets. Let $\Pi = \{A \in \Gamma^- \mid |A| = a\}$, where $a = \min_{A \in \Gamma^-}|A|$. Let $Q(\emptyset) = \{p \in \mathcal{P} \mid \text{there exists } A \in \Pi \text{ with } p \in A\}$. For $p \in \mathcal{P}$, let $U(p) = \{B \in \Delta^+ \mid p \notin B\}$. For $i > 1$ and $p_1, \ldots, p_i \in \mathcal{P}$, let

$$Q(p_1, \ldots, p_{i-1}) = \{p \in \mathcal{P} \backslash \{p_1, \ldots, p_{i-1}\} \mid \text{there exists } A \in \Pi \text{ with } p_1, \ldots, p_{i-1}, p \in A\},$$

$$U(p_1, \ldots, p_{i-1}, p_i) = \{B \in \Delta^+ \mid p_1, \ldots, p_{i-1} \in B, p_i \notin B\}.$$

**The Linkage Algorithm for $\Gamma$**

1. We use the notation defined above. We will define a sequence $p_1, \ldots, p_a$ as follows. At stage $i = 1, \ldots, a$, let $p_i \in \mathcal{P}$ be such that $p_i \in Q(p_1, \ldots, p_{i-1})$ and $|U(p_1, \ldots, p_i)|$ is maximal. If there is more than one such $p_i$, choose $p_i$ where $|\bigcap_{B \in U(p_1, \ldots, p_i)} B|$ is minimal.
2. Apply the GCC with $\mathcal{P}_0 = \{p_1, \ldots, p_a\}$, and for $i = 1, \ldots, a$, let $M_i$ be a scheme for $\bar{\Delta}_i$.

The significance of $U(p_1, \ldots, p_i)$ becomes clear when we show that, in the application of the GCC to $\{p_1, \ldots, p_i\}$, we have $\Delta_i^+ = U(p_1, \ldots, p_i)$. Let $i \in \{1, \ldots, a\}$. Suppose $B \in U(p_1, \ldots, p_i)$; so $B \in \Delta^+$, $p_1, \ldots, p_{i-1} \in B$ and $p_i \notin B$. It follows that $B \in \Gamma_1, \ldots, \Gamma_{i-1}$ and $B \notin \Gamma_i$; so $B \notin \Delta_1, \ldots, \Delta_{i-1}$ and $B \in \Delta_i^+$. So $U(p_1, \ldots, p_i) \subseteq \Delta_i^+$.

As each of $\{U(p_1, \ldots, p_j) \mid j = 1, \ldots, a\}$ and $\{\Delta_j^+ \mid j = 1, \ldots, a\}$ partitions $\Delta^+$, we have $U(p_1, \ldots, p_i) = \Delta_i^+$.

**Example 8.** Let $\Gamma = ab+bc+bde+cde$ be complete. Then $\Delta^+ = \{ade, acd, bd, ace, be\}$, $a = 2$, and $\Pi = \{ab, bc\}$. We start by noting that $Q(\emptyset) = \{a, b, c\}$, $U(a) = \{bd, be\}$, $U(b) = \{ade, acd, ace\}$, $U(c) = \{ade, bd, be\}$, $U(d) = \{ace, be\}$, and $U(e) = \{acd, bd\}$. So we can choose $p_1$ to be either $b$ or $c$. However, $\bigcap_{B \in U(b)} B = a$ and $\bigcap_{B \in U(c)} B = \emptyset$, so we choose $\mathcal{P}_0 = \{c, b\}$. Now applying the GCC we get $\Gamma_1 = c + ab + bde$ and $\Gamma_2 = b + de$. Thus $\Delta_1^+ = \{ade, bd, be\} = U(c)$ and $\Delta_2^+ = \{acd, ace\} = U(c, b)$. Then $\bar{\Delta}_1 = c + ab + bde$ and $\bar{\Delta}_2 = b + de$, and the resulting linkage is 6. An exhaustive search through all $\mathcal{P}_0 \in \Gamma$ shows that 6 is the optimal linkage using the GCC.

Our testing of the Linkage Algorithm has suggested that the algorithm finds either an optimal or close to optimal solution.

## 5. Reducing the Potential Storage

We now show that incomplete schemes can be used to establish an MTA-free scheme with lower potential storage than that given by the Contraction Construction. The next constructions will use a special type of secret sharing scheme defined as follows. Let $0 \le c \le k$. 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 $|A| \ge k$, then $H(s|A) = 0$; and
2. if $|A| \le c$, then $H(s|A) = H(s)$.

Ramp schemes such that $H(p) = H(s)/(k-c)$ (for all $p \in \mathcal{P}$) can be constructed from ideal $(k, n)$-threshold schemes [16].

The *Base Ramp Construction* can be used to construct an MTA-free secret sharing scheme for any access structure $(\Gamma, \Delta)$. In fact, it differs from the Basic Construction for a $(k, n)$-threshold scheme only in the scheme $M_0$.

Let $c = \max_{A \in \Delta} |A|$.

**The Base Ramp Construction for** $(\Gamma, \Delta)$

| | |
|---|---|
| $(\Gamma_0, \Delta_0)$ | $(c, n, n)$-ramp on $\mathcal{P}$ |
| $\Gamma_p$ | $p + \Gamma$, for $p \in \mathcal{P}$ |
| $M_0$ | $(c, n, n)$-ramp scheme on $\mathcal{P}$ |
| $M_p$ | scheme for $\Gamma_p$, for $p \in \mathcal{P}$ |

**Proof (Base Ramp Construction).** We use Corollary 4. Let $A \in \Gamma$. Then $A \in \Gamma_p$ for each $p \in \mathcal{P}$ and so $\mathcal{X}(A) = \mathcal{P} \in \Gamma_0$. We remark that for $A \subseteq \mathcal{P}$, since $\Gamma_p = p + \Gamma$ is complete, we have $A \subseteq \mathcal{X}(A) = \bar{\mathcal{X}}(A)$. Suppose $A \in \Delta$. As $A \notin \Gamma$ we have $\mathcal{X}(A) = A$, and $|A| \le c$ implies $\bar{\mathcal{X}}(A) = \mathcal{X}(A) = A \in \Delta_0$. □

**Example 9.** Let $\Gamma$ 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 $M'''$ for $\Gamma$ with convec $(\frac{3}{2}, \frac{3}{2}, \frac{3}{2})$. Thus $M'''$ has a potential storage of $\frac{9}{2}$ which is an improvement on the potential storage 5 of $M'$ using the Contraction Construction. However, the linkage $\ell(M''') = 6$ which is higher than $\ell(M') = 3$.

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 the Base Ramp Construction for a $(k, n)$-threshold scheme gives,

$$\mathcal{V}(M) = n\left(\frac{n}{n-k+1}\right) = \frac{n^2}{n-k+1}, \tag{7}$$

$$\ell(M) = n(n-1). \tag{8}$$

Thus, with respect to potential storage, the Base Ramp scheme is an improvement on the Contraction Construction for $(k, n)$-threshold schemes (see (4) and (7)).

## 6. Reducing the Information Rate

The information rate and average information rate of an MTA-free secret sharing scheme are measures of the amount of information that has to be stored by participants in the scheme. We note first that the optimal potential storage can be used to compute an initial lower bound on the optimal average information rate. More precisely, if $(\Gamma, \Delta)$ is a monotone access structure on $n$ participants, then $\tilde{\rho}_{MTA}(\Gamma, \Delta) \geq n/\mathcal{V}(\Gamma, \Delta)$. We will show that in some cases it is possible to reduce the amount of information that each participant stores at the end of Stage (B) of the MTA-free protocol and thus increase the information rates. To do this we first discuss *homomorphic* secret sharing schemes.

### 6.1. *Homomorphic Secret Sharing*

Homomorphic secret sharing schemes were introduced in [1]. Since then a number of papers have provided examples and discussed applications, for example, [2], [8], [10], and [11]. The definition we present here is slightly more general and rigorous than those appearing in previous papers.

Let $M = (\mathcal{P}, s, \rho)$ and $N = (\mathcal{P}, s, \mu)$ be secret sharing schemes for $(\Gamma, \Delta)$ and let $\lambda \geq 2$ be an integer. We say that $M$ is $\lambda$-*homomorphic* to $N$ if there exist functions $(f_x)_{x \in s\mathcal{P}}$, with $f_x : [x]_\rho^\lambda \to [x]_\mu$ (where $[x]_\rho^\lambda$ is $[x]_\rho \times \cdots \times [x]_\rho$, $\lambda$ times), such that for $\pi^1, \ldots, \pi^\lambda \in [s\mathcal{P}]_\rho$ we have $\pi^1 * \cdots * \pi^\lambda \in [s\mathcal{P}]_\mu$, where $\pi^1 * \cdots * \pi^\lambda = (f_x(\pi_x^1, \ldots, \pi_x^\lambda))_{x \in s\mathcal{P}}$. In other words, $M$ is $\lambda$-homomorphic to $N$ if there exist combining functions $(f_x)_{x \in s\mathcal{P}}$ such that, for any $\lambda$ distribution rules $\pi^1, \ldots, \pi^\lambda$ of $M$, applying the share combining functions $(f_x)_{x \in \mathcal{P}}$ to the shares of $\pi^1, \ldots, \pi^\lambda$ results in a distribution rule of $N$ which has as its secret $f_s(\pi_s^1, \ldots, \pi_s^\lambda)$. Informally, the combined shares can be used to determine the combined secret.

Benaloh [1] discussed 2-homomorphisms for $(k, n)$-threshold schemes. Precisely, in [1] it was required that for any $K \subseteq \mathcal{P}$ with $|K| = k$ and $\alpha \in [sK]_\rho$, there exists $\pi \in [s\mathcal{P}]_\mu$ with $\pi_{sK} = \alpha$ (for example, this property holds if $M$=$N$).

While previous definitions of secret sharing homomorphism ensure that the combined shares of authorized sets can be used to determine the combined secret, they do not guarantee that the combined shares of unauthorized sets do not give any information about the combined secret. As we will need this property, we now introduce the idea of a *perfect* homomorphism.

Let $M = (\mathcal{P}, s, \rho)$ be a scheme for $(\Gamma, \Delta)$. Define a collection of tuples $\Pi$ indexed by $\{x^i \mid x \in s\mathcal{P},\ 1 \leq i \leq \lambda\} \cup \{x^* \mid x \in s\mathcal{P}\}$. For $\pi^1, \ldots, \pi^\lambda \in [s\mathcal{P}]_\rho$ define a tuple $\pi \in \Pi$ by concatenating the components of $\pi^1, \ldots, \pi^\lambda$ and $\pi^1 * \cdots * \pi^\lambda$. Further, we define a probability measure $\nu$ on the tuples of $\Pi$ such that for $\pi \in \Pi$ formed as above, $\nu(\pi) = \prod_{i=1}^{\lambda} \rho(\pi^i)$. For $A \subseteq s\mathcal{P}$ and $Y \subseteq \{1, \ldots, \lambda, *\}$ let $A^Y = \{x^i \mid x \in A, i \in Y\}$.

We say that $M$ is *perfectly* $\lambda$-homomorphic to $N = (\mathcal{P}, s, \mu)$ if:

(1) $M$ is $\lambda$-homomorphic to $N$;
(2) for each $\pi^* \in [s\mathcal{P}]_\mu$, letting $C(\pi^*) = \{(\pi^1, \ldots, \pi^\lambda) \mid \pi^1, \ldots, \pi^\lambda \in [s\mathcal{P}]_\rho,\ \pi^1 * \cdots * \pi^\lambda = \pi^*\}$, we have

$$\mu(\pi^*) = \sum_{(\pi^1,\ldots,\pi^\lambda) \in C(\pi^*)} \prod_{i=1}^{\lambda} \rho(\pi^i);$$

(3) for each $i$ $(1 \leq i \leq \lambda)$ and $B \in \Delta$ $(B \subseteq \mathcal{P})$ we have $H_\nu(s^* | B^i (s\mathcal{P})^{\{1,\ldots,\lambda\}\setminus i}) = H_\nu(s^*)$.

Property (2) says that the probability of a distribution rule $\pi^*$ of $N$ is equal to the probability that $\pi^*$ is formed by applying $*$ to $\lambda$ distribution rules of $M$. In other words, the scheme $N$ is the result of applying $*$ to all sets of $\lambda$ distribution rules of $M$. Property (3) ensures that knowledge of $\lambda - 1$ distribution rules used to form a distribution rule of $N$ and the shares of an unauthorized set give no information about the secret of the combined distribution rule.

The following theorem illustrates the significance of perfect homomorphisms to MTA-free secret sharing.

**Theorem 11.** *Let $M = (\mathcal{P}, s, \rho)$ be perfectly $\lambda$-homomorphic to $N = (\mathcal{P}, s, \mu)$, where $M$ is a scheme for $(\Gamma, \Delta)$ and there exists $A \in \Gamma$ with $|A| = \lambda$. Then there exists an MTA-free scheme for $(\Gamma, \Delta)$ with information rates the same as $N$.*

**Proof.** Suppose that $M = (\mathcal{P}, s, \rho)$ is perfectly $\lambda$-homomorphic to $N = (\mathcal{P}, s, \mu)$, with corresponding combining functions $(f_x)_{x \in s\mathcal{P}}$ and probability measure $\nu$ as in the definitions immediately above.

Let $A = \{p_1, \ldots, p_\lambda\} \in \Gamma$. We first note that the Basic Construction can be easily modified so that the base access structure is $(\lambda, \lambda)$-threshold on $A$ and the base scheme is a perfect $(\lambda, \lambda)$-threshold scheme on $A$. For each $i = 1, \ldots, \lambda$, let $p_i$ choose a distribution rule $r^i$ from $M$. Equivalently, the private scheme $M_i$ is the scheme obtained from $M$ when $p_i$'s share in $M$ is replaced by the secret value. Now $p_i$ distributes shares $r_x^i (x \in \mathcal{P})$ in the scheme $M_i$. Let $M'$ be the MTA-free scheme for $(\Gamma, \Delta)$ arising from this choice of base and private schemes. Each participant $x \in \mathcal{P}$ then computes $f(r_x^1, \ldots, r_x^\lambda)$ $(\in [x]_\mu)$ and stores this as their share. As these computed shares form a distribution rule of $N$ and $N$ is a scheme for $(\Gamma, \Delta)$, it follows that any $B \in \Gamma$ can reconstruct the secret $s^*$ in $N$.

Let $B \in \Delta$ and let $p_i \in A \backslash B$. Note that if $p_j \in A$, then $p_j$ knows $r^j$ whereas if $p_j \notin A$, then $p_j$ only knows $r^k_{p_j}$ $(k = 1, \ldots, \lambda)$. Thus $H_\nu(s^*|B^{A\backslash B}(s\mathcal{P})^{A\cap B}) \geq H_\nu(s^*|B^i(s\mathcal{P})^{A\backslash p_i}) = H_\nu(s^*)$, by definition of perfectly $\lambda$-homomorphic. Thus all the information available to an unauthorized set does not give them any information about the secret $s^*$ of $N$.

Thus $M'$ is an MTA-free scheme for $(\Gamma, \Delta)$ which can be reduced to $N$ and hence has the same information rates as $N$. □

The MTA-free scheme $M'$ for $(\Gamma, \Delta)$ on $n$ participants, constructed using Theorem 11, has $\ell(M') = \lambda(n-1)$, $\mathcal{V}(M') = \lambda \sum_{x\in\mathcal{P}} c_x$ (where $M$ has convec $(c_1, \ldots, c_n)$ ) and information rates as in $N$. Thus in order to use Theorem 11 profitably we seek a scheme $M$ with convec $(c_1, \ldots, c_n)$ that is perfectly $\lambda$-homomorphic to a scheme $N$ with convec $(d_1, \ldots, d_n)$, where for each $i = 1, \ldots, n$ we have $d_i \leq \lambda c_i$. One class of such schemes $M$ are the schemes that are perfectly $\lambda$-homomorphic to themselves. We now discuss a family of such schemes.

### 6.2. *Geometric Secret Sharing Schemes*

Recall the definition of geometric secret sharing scheme (see also the related vector space construction [4] and linear scheme construction [9]). Let $q$ be a prime power, let $d$ be a positive integer and let $\Sigma = PG(d, q)$ denote the projective space of dimension $d$ over the field $GF(q)$. Let $[\Sigma]$ denote the collection of subspaces of $\mathrm{PG}(d, q)$. A *geometric* secret sharing scheme for $(\Gamma, \Delta)$ is a function $\sigma: s\mathcal{P} \mapsto [\Sigma]$, such that for $A \subseteq \mathcal{P}$:

1. if $A \in \Gamma$, then $A^\sigma \supseteq s^\sigma$; and
2. if $A \in \Delta$, then $A^\sigma \cap s^\sigma = \emptyset$,

where $A^\sigma$ is the subspace spanned by the subspaces $x^\sigma$ $(x \in A)$. Geometric schemes can be found for all monotone access structures [23].

From $\sigma$ we can obtain a set $\Omega$ of tuples as in [14]. For each $x \in s\mathcal{P}$, let $k^1_x, \ldots, k^{d_x}_x$ be the homogeneous coordinates ($(d+1)$-tuples over $GF(q)$) of a point basis for $x^\sigma$. Let $h_1, \ldots, h_{q^{d+1}}$ denote the $q^{d+1}$ $(d+1)$-tuples over $GF(q)$. For $i = 1, \ldots, q^{d+1}$, let $\sigma \circ h_i = (\pi_x)_{x\in s\mathcal{P}}$, where $\pi_x = (k^1_x \circ h_i, \ldots, k^{d_x}_x \circ h_i)$ $(x \in s\mathcal{P})$, and $k^j_x \circ h_i$ is the dot product of the two $(d+1)$-tuples. Let $\Omega = \{\sigma \circ h_i \mid 1 \leq i \leq q^{d+1}\}$ and let $\rho$ be the uniform probability measure on $\Omega$. As in [14] we can show that $(\mathcal{P}, s, \rho)$ is a secret sharing scheme for $(\Gamma, \Delta)$. We also call a scheme $(\mathcal{P}, s, \rho)$ resulting in this way a *geometric* secret sharing scheme.

**Theorem 12.** *Let $M = (\mathcal{P}, s, \rho)$ be a geometric secret sharing scheme for $(\Gamma, \Delta)$. Then for any integer $\lambda \geq 2$, $M$ is perfectly $\lambda$-homomorphic to itself.*

**Proof.** Let $M = (\mathcal{P}, s, \rho)$ be a geometric secret sharing scheme for $(\Gamma, \Delta)$. We use the notation defined above. For $x \in s\mathcal{P}$ and $\pi \in [s\mathcal{P}]_\rho$, $\pi_x$ is a $d_x$-tuple over $GF(q)$. Hence we can define $f_x: [x]^\lambda_\rho \mapsto [x]_\rho$ to be vector addition (denoted $+$). Let $\sigma \circ h_1, \ldots, \sigma \circ h_\lambda$ be $\lambda$ rules of $M$. Then $(\sigma \circ h_1) * \cdots * (\sigma \circ h_\lambda) = \sigma \circ (h_1 + \cdots + h_\lambda)$. Since $h_1 + \cdots + h_\lambda$ is a $(d+1)$-tuple we have $\sigma \circ (h_1 + \cdots + h_\lambda) \in [s\mathcal{P}]_\rho$. Thus $M$ is $\lambda$-homomorphic to itself, proving Part 1.

Now note that for any $(d+1)$-tuples $h_1, \ldots, h_{\lambda-1}, h$, we have $(\sigma \circ h_1) * \cdots * (\sigma \circ h_{\lambda-1}) * (\sigma \circ (h - h_1 - \cdots - h_{\lambda-1})) = \sigma \circ h$. Hence for $\pi^* = \sigma \circ h \in \Pi$,

$$C(\pi^*) = \{(\sigma \circ h_1, \ldots, \sigma \circ h_{\lambda-1}, \sigma \circ (h - h_1 - \cdots - h_{\lambda-1}) \mid h_1, \ldots, h_{\lambda-1} \text{ are } (d+1)\text{-tuples}\}.$$

Now

$$\sum_{(\pi^1,\ldots,\pi^\lambda) \in C(\pi^*)} \rho(\pi^1) \ldots \rho(\pi^\lambda) = (q^{d+1})^{\lambda-1}(1/q^{d+1})^\lambda = 1/q^{d+1} = \rho(\pi^*),$$

proving Part 2.

For Part 3, fix $\sigma \circ h_1, \ldots, \sigma \circ h_{\lambda-1} \in [s\mathcal{P}]_\rho$ and let $B \in \Delta$. We show that if $\beta \in [B]_\rho$, then $\rho(\pi_{s^*} = \alpha | \pi_{s^i \mathcal{P}^i} = \sigma \circ h_i \ (1 \le i \le \lambda - 1), B^\lambda = \beta)$ is independent of $\alpha \in [s]_\rho$. First note that as $B \in \Delta$, for each $\alpha \in [s]_\rho$ and $\beta \in [B]_\rho$, $|\{h \mid (\sigma \circ h)_s = \alpha, (\sigma \circ h)_B = \beta\}|$ is independent of $\alpha \in [s]_\rho$ and $\beta \in [B]_\rho$. Let $A(\alpha, \beta) = \{h \mid ((\sigma \circ h_1) * \cdots * (\sigma \circ h_{\lambda-1}) * (\sigma \circ h))_s = \alpha, (\sigma \circ h)_B = \beta\}$. We have $((\sigma \circ h_1) * \cdots * (\sigma \circ h_{\lambda-1}) * (\sigma \circ h))_s = (\sigma \circ (h_1 + \cdots + h_{\lambda-1}))_s + (\sigma \circ h)_s$. From our note and properties of $GF(q)$ we see that $|A(\alpha, \beta)|$ is independent of $\alpha$ and $\beta$. So $H_\nu(s^* | B^\lambda s\mathcal{P}^{\{1,\ldots,\lambda-1\}}) = H_\nu(s^*)$, as required. □

**Example 10.** Let $(\Gamma, \Delta) = \{abc, ab \diamond ac \diamond ad\}$. Define $\sigma : s\mathcal{P} \mapsto [PG(2,2)]$ by $s^\sigma = (1,1,1)$, $a^\sigma = (1,0,0)$, $b^\sigma = (0,1,0)$, $c^\sigma = (0,0,1)$. We obtain the tuples indexed by $s, a, b, c$: $(0,0,0,0)$, $(1,0,0,1)$, $(1,0,1,0)$, $(0,0,1,1)$, $(1,1,0,0)$, $(0,1,0,1)$, $(0,1,1,0)$, $(1,1,1,1)$. Let $abc \in \Gamma$. Suppose $r^a = (1,0,0,1)$, $r^b = (0,0,1,1)$, $r^c = (1,1,1,1)$. Then $a, b, c$ calculate their shares to be $0+0+1=1$, $0+1+1=0$, $1+1+1=1$, corresponding to rule $(0,1,0,1) = r^a + r^b + r^c$.

Thus from Theorems 11 and 12 we have the following.

**Corollary 13.** *Let $M = (\mathcal{P}, s, \rho)$ be a geometric scheme for $(\Gamma, \Delta)$. Then there exists an MTA-free scheme for $(\Gamma, \Delta)$ with information rates the same as $M$.*

Let $(\Gamma, \Delta)$ be an access structure defined on $\mathcal{P}$. Clearly we have that $\rho_{MTA}(\Gamma, \Delta) \le \rho(\Gamma, \Delta)$ and $\tilde{\rho}_{MTA}(\Gamma, \Delta) \le \tilde{\rho}(\Gamma, \Delta)$. However, for complete access structures, thus far the best-known information rates and average information rates can be achieved by geometric schemes (for example, [14] and [15]). Thus at the time of writing, for any access structure $\Gamma$ where $\rho(\Gamma)$ and $\tilde{\rho}(\Gamma)$ are known, we have $\rho_{MTA}(\Gamma) = \rho(\Gamma)$ and $\tilde{\rho}_{MTA}(\Gamma) = \tilde{\rho}(\Gamma)$.

## 7. MTA-Free Threshold Schemes

In this section we determine the optimal linkage, potential storage and information rates for an MTA-free $(k, n)$-threshold scheme. In each case, a scheme discussed earlier in this paper achieves the optimal value.

### 7.1. *Optimal Linkage for MTA-Free Threshold Schemes*

We show here that the Contraction Construction gives an optimal construction for threshold schemes with respect to the linkage.

**Lemma 14.** *Let $M$ be an MTA-free $(k, n)$-threshold scheme with $1 \leq k < n$. For $a \in \mathcal{P}_0$, let $r_a = |\mathcal{P}\backslash \operatorname{core} M_a|$ and let $W(a) = \{p \in \mathcal{P}_0\backslash a \mid a \in \operatorname{core} M_p\}$. Then $|W(a)| \geq r_a$.*

**Proof.** Let $M = (M_0; M_1, \ldots, M_n)$ and suppose that $M_i$ is a scheme for $(\Gamma_i, \Delta_i)$ for $i = 0, \ldots, n$. Let $a \in \mathcal{P}_0$. Let $R = \mathcal{P}\backslash \operatorname{core} M_a$ and let $r_a = |R|$. Let $W(a) = \{p \in \mathcal{P}_0\backslash a \mid a \in \operatorname{core} M_p\}$. It follows from Lemma 7 that $\Gamma_a \supseteq \Gamma$ and thus, since $R \notin \Gamma_a$, it follows that $0 \leq r_a \leq k-1$. Consequently, since $k < n$ we have $|\mathcal{P}\backslash a| \geq k$, so there exists a $(k-1)$-set $C_1$ such that $R \not\subseteq C_1 \subseteq \mathcal{P}\backslash a$. Now $C_1 \notin \Gamma$, so it follows that there exists $b_1 \in \mathcal{P}_0$ with $C_1 \notin \Gamma_{b_1}$. Further, $|aC_1| = k$, so $aC_1 \in \Gamma$ and hence by Lemma 7, $aC_1 \in \Gamma_{b_1}$. So $a \in \operatorname{core} M_{b_1}$.

Suppose $C_1 \notin \Gamma_a$. By definition of $R$, we have $C_1 R \notin \Gamma_a$. As $\Gamma_a \supseteq \Gamma$ it follows that $|C_1 R| \leq k-1$ and as $|C_1| = k-1$ we have $R \subseteq C_1$, contradicting the definition of $C_1$. So $C_1 \in \Gamma_a$; hence $b_1 \neq a$ and $b_1 \in W(a)$.

Repeating the above process we generate a set of distinct elements $b_1, b_2, \ldots, b_{r_a} \in W(a)$ as follows. For $i = 2, 3, \ldots, r_a$, at Stage $i$ take a $(k-1)$-set $C_i$ containing $b_1, \ldots, b_{i-1}$ such that $R \not\subseteq C_i \subseteq \mathcal{P}\backslash a$ (this is possible since $i - 1 \leq r_a - 1 < |R|$). Then there exists a $b_i \in \mathcal{P}_0$ with $C_i \notin \Gamma_{b_i}$. It follows that $a \in \operatorname{core} M_{b_i}$ and that $b_i \neq a$. Further, $b_i \neq b_1, \ldots, b_{i-1}$ since $b_1, \ldots, b_{i-1} \in C_i$ and so $C_i \in \Gamma_{b_1}, \ldots, \Gamma_{b_{i-1}}$. Thus $b_1, b_2, \ldots, b_{r_a} \in W(a)$ and so $|W(a)| \geq r_a$. □

In order to prove our bound on linkage, we use the following definition and results on the contraction of an MTA-free scheme.

Let $M = (M_0; M_1, \ldots, M_n)$, $M = (\mathcal{P}, s, \rho)$, be an MTA-free scheme for $(\Gamma, \Delta)$. Let $a \in \mathcal{P}$ and let $\alpha \in [a]_\rho$. The *contraction* $M \cdot (a = \alpha)$ of $M$ at $a = \alpha$ is the scheme $M \cdot (a = \alpha) = (\mathcal{P}\backslash a, s, \rho')$ where for $\pi \in [s\mathcal{P}\backslash a]_\rho$ we have $\rho'(\pi) = \rho_{s\mathcal{P}\backslash a|a}(\pi, \alpha)$. In particular, $M \cdot (a = \alpha)$ is a scheme for $\Gamma \cdot a$ (see [15]). Suppose $a \notin \mathcal{P}_0$. Since $\alpha = (\alpha^1, \ldots, \alpha^n)$ where $\alpha^i \in [a]_{\rho^i}$, it follows that $M \cdot (a = \alpha)$ is an MTA-free scheme for $\Gamma \cdot a$ arising from the component schemes $M_0, M_1 \cdot (a = \alpha^1), \ldots, M_n \cdot (a = \alpha^n)$. On the other hand, suppose $a \in \mathcal{P}_0$. In this case, if $a = p_i$, then $M_i \cdot (a = \alpha^i)$ is equivalent to $M_i \cdot (s_i = \alpha^i)$. Thus $M \cdot (a = \alpha)$ is an MTA-free scheme for $\Gamma \cdot a$ arising from the component schemes $M_0 \cdot (a = \alpha^0), M_1 \cdot (a = \alpha^1) \ldots M_n \cdot (a = \alpha^n)$, where $\alpha = (\alpha^0, \alpha^1, \ldots, \alpha^n)$ and $\alpha^i \in [a]_{\rho^i}$ for $i = 0, \ldots, n$.

**Theorem 15.** *Let $\Gamma$ be a $(k, n)$-threshold access structure, $1 \leq k < n$. Then $\ell(\Gamma) \geq nk - k(k+1)/2$.*

**Proof.** Let $M$ be an MTA-free scheme for $\Gamma$. Let $T(k, m) = mk - k(k+1)/2$. We proceed by induction on $k$. Let $k = 1$. For $p \in \mathcal{P}_0$ it follows from Lemma 7 that $\Gamma_p \supseteq \Gamma$ and so either $\Gamma_p^- = \{\emptyset\}$ or $\Gamma_p = \Gamma = p_1 + \cdots + p_n$, where $\mathcal{P} = \{p_1, \ldots, p_n\}$. If $\Gamma_p^- = \{\emptyset\}$ for each $p \in \mathcal{P}_0$, then $\emptyset \in \Gamma$, a contradiction, and so there exists some $a \in \mathcal{P}_0$ with $\Gamma_a = p_1 + \cdots + p_n$. Thus $\ell(M) \geq n - 1 = T(1, n)$.

Suppose that $\ell(M') \geq T(k-1, n-1)$ for any MTA-free $(k-1, n-1)$-threshold scheme $M'$. Let $M$ be an MTA-free $(k, n)$-threshold scheme $(2 \leq k \leq n)$; so $|\mathcal{P}_0| \geq k$. Let $a \in \mathcal{P}_0$ and $\alpha \in [a]_\rho$. As above, the contraction $M \cdot (a = \alpha)$ of $M$ at $a = \alpha$ is an

MTA-free $(k-1, n-1)$-threshold scheme, and by the inductive hypothesis we have $\ell(M \cdot (a = \alpha)) \geq T(k-1, n-1)$. To compute $\ell(M)$ we must add to $\ell(M \cdot (a = \alpha))$ the number of connections involving $a$. Participant $a$ transmitted shares to $|\text{core } M_a| - 1$ other participants. Further, the number of participants who transmitted shares to participant $a$ is $|W(a)|$, where $W(a) = \{p \in \mathcal{P}_0 \backslash a \mid a \in \text{core } M_p\}$. So by Lemma 14, letting $r_a = |\mathcal{P} \backslash \text{core } M_a|$, we have that

$$\begin{aligned} \ell(M) &\geq T(k-1, n-1) + (n - r_a - 1) + r_a \\ &= (n-1)(k-1) - \frac{(k-1)k}{2} + n - 1 \\ &= nk - \frac{k(k+1)}{2}. \end{aligned}$$

Thus $\ell(M) \geq T(k, n)$ as required. □

**Corollary 16.** *Let $\Gamma$ be a $(k, n)$-threshold access structure. The optimal linkage of $\ell(\Gamma) = nk - k(k+1)/2$ is achieved by the Contraction Construction.*

**Proof.** Equation (5) and Theorem 15. □

### 7.2. *Optimal Potential Storage for MTA-Free Threshold Schemes*

In this section we show that the Base Ramp Construction gives an optimal construction for threshold schemes with respect to the potential storage. We need the following construction, which is a generalization of constructions in, for example, [5] and [18].

#### 7.2.1. *A Construction*

Let $M = (\mathcal{P}, s_M, \rho_M)$ be a secret sharing scheme for $(\Gamma_M, \Delta_M)$ with distribution rules from set $\Omega_M \subseteq [p_1]_M \times \cdots \times [p_n]_M \times [s]_M$. Let $N = (\mathcal{P}, s_N, \rho_N)$ be a secret sharing scheme for $(\Gamma_N, \Delta_N)$ with distribution rules from set $\Omega_N \subseteq [p_1]_N \times \cdots \times [p_n]_N \times [s]_N$. We define a new scheme $M \oplus N = (\mathcal{P}, s, \rho)$. Each participant $p_i$ receives a share from set $[p_i] = [p_i]_M \times [p_i]_N$ and the secret comes from set $[s] = [s]_M \times [s]_N$. For each $\alpha = (\alpha_1, \ldots, \alpha_n, \alpha_0) \in \Omega_M$ and $\beta = (\beta_1, \ldots, \beta_n, \beta_0) \in \Omega_N$, define a tuple $\alpha \oplus \beta = ((\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n), (\alpha_0, \beta_0))$. Define $\rho(\alpha \oplus \beta)$ to be $\rho_M(\alpha)\rho_N(\beta)$. We see that

$$\rho(\alpha \oplus \beta) \log_2 \rho(\alpha \oplus \beta) = \rho_N(\beta)(\rho_M(\alpha) \log_2 \rho_M(\alpha)) + \rho_M(\alpha)(\rho_N(\beta) \log_2 \rho_N(\beta)).$$

Using this it follows that for any $A, B \subseteq s\mathcal{P}$ we have

$$H_\rho(A|B) = H_{\rho_M}(A|B) + H_{\rho_N}(A|B). \tag{9}$$

So $M \oplus N$ is a secret sharing scheme for $(\Gamma, \Delta)$, where $\Gamma = \Gamma_M \cap \Gamma_N$ and $\Delta = \Delta_M \cap \Delta_N$. Informally, $M \oplus N$ is the scheme that results by distributing shares independently from schemes $M$ and $N$ and defining the secret to be the ordered pair $(s_M, s_N)$.

Now let $(\Gamma, \Delta)$ be an access structure. Let $M = (M_0; M_1, \ldots, M_n)$ be an MTA-free scheme for $(\Gamma, \Delta)$, where for $i = 1, \ldots, n$ $M_i$ has access structure $(\Gamma_i, \Delta_i)$. Let

$N = (N_0; N_1, \ldots, N_n)$ be another MTA-free scheme for $(\Gamma, \Delta)$, where for $i = 1, \ldots, n$ $N_i$ has access structure $(\Gamma_i', \Delta_i')$. Since $M \oplus N$ is the independent "product" of $M$ and $N$, the scheme $M \oplus N$ is also an MTA-free scheme for $(\Gamma, \Delta)$. Further, it follows that $M \oplus N = (M_0 \oplus N_0; M_1 \oplus N_1, \ldots, M_n \oplus N_n)$.

### 7.2.2. *The Lower Bound*

Let $(\Gamma, \Delta)$ be an access structure defined on $\mathcal{P} = \{p_1, \ldots, p_n\}$ $(1 \le k \le n)$. Let $\mathrm{Sym}(n)$ denote the symmetric group on $\{1, \ldots, n\}$ (the set of all permutations of $\{1, \ldots, n\}$). For $A \subseteq \mathcal{P}$ and $\sigma \in \mathrm{Sym}(n)$ let $A^\sigma = \{p_{i\sigma} \mid p_i \in A\}$, where $i\sigma$ is the image of $i$ under the permutation $\sigma$. Let $(\Gamma^\sigma, \Delta^\sigma)$ be the access structure defined as follows. Let $A \subseteq \mathcal{P}$. Then $A^\sigma \in \Gamma^\sigma$ if and only if $A \in \Gamma$ and $A^\sigma \in \Delta^\sigma$ if and only if $A \in \Delta$. Note that if $(\Gamma, \Delta)$ is the $(k, n)$-threshold access structure, then $(\Gamma^\sigma, \Delta^\sigma) = (\Gamma, \Delta)$.

Now let $M = (\mathcal{P}, s, \rho)$ be a secret sharing scheme and define $M^\sigma = (\mathcal{P}, s\sigma, \rho\sigma)$ as follows. If $\alpha = (\alpha_1, \ldots, \alpha_n, \alpha_0)$ is a distribution rule of $M$ where $\alpha_i \in [p_i]$ for $i = 1, \ldots, n$ and $\alpha_0 \in [s]$, then define $\alpha^\sigma = (\alpha_{1\sigma}, \ldots, \alpha_{n\sigma}, \alpha_0)$ to be a distribution rule of $M^\sigma$, with $\rho\sigma(\alpha^\sigma) = \rho(\alpha)$. If $M$ is a scheme for $(\Gamma, \Delta)$, then it follows that $M^\sigma$ is a scheme for $(\Gamma^\sigma, \Delta^\sigma)$.

**Lemma 17.** *Let $M = (\mathcal{P}, s, \rho)$ be an MTA-free $(k, n)$-threshold scheme. Let $M = (M_0; M_1, \ldots, M_n)$, where $M_0 = (\mathcal{P}, s, \rho^0)$ and $M_i = (\mathcal{P}, s_i, \rho^i)$ with $\rho^i_{s_i} = \rho^0_{p_i}$ $(1 \le i \le n)$. Then $M^* = \oplus_{\sigma \in \mathrm{Sym}(n)} M^\sigma$ is an MTA-free $(k, n)$-threshold scheme with the following properties*:

1. *$M^* = (M_0^*; M_1^*, \ldots, M_n^*)$, where for $i = 1, \ldots, n$ and $\sigma \in \mathrm{Sym}(n)$, $M_i^\sigma = (\mathcal{P}, s_i\sigma, \rho^i\sigma)$ (with $s_i\sigma = s_{i\sigma}$) and for $i = 1, \ldots, n$, $M_i^* = (\mathcal{P}, s_i^*, \rho^{i*}) = \bigoplus_{\sigma \in \mathrm{Sym}(n)} M^\sigma_{i\sigma^{-1}}$;*
2. *the potential storage of $M^*$ is the same as the potential storage of $M$;*
3. *for all $p_i \in \mathcal{P}$, $H(p_i)$ in $M_i^*$ is independent of $i$ and $H(p_i)$ in $M_j^*$ is independent of $i, j, i \ne j$;*
4. *for all $p_i \in \mathcal{P}$ and all $(k-1)$-subsets $B$ of $\mathcal{P} \backslash p_i$, $H(s_i|B)$ in $M_i^*$ is independent of $i$ and $B$; and*
5. *for all $p_i \in \mathcal{P}$, $H(p_i)$ in $M^*$ is independent of $i$.*

**Proof.** Observe that for each $\sigma \in \mathrm{Sym}(n)$, $M^\sigma = (\mathcal{P}, s\sigma, \rho\sigma) = (M_0^\sigma; M^\sigma_{1\sigma^{-1}}, \ldots, M^\sigma_{n\sigma^{-1}})$ is an MTA-free $(k, n)$-threshold scheme. Then by repeated applications of the construction $\oplus$ we have that $M^* = (M_0^*; M_1^*, \ldots, M_n^*)$ is also an MTA-free $(k, n)$-threshold scheme. Suppose that $M^* = (\mathcal{P}, s^*, \rho^*)$. By (9) the potential storage is given by

$$\begin{aligned}\mathcal{V}(M^*) &= \sum_{i=1}^{n} \frac{H_{\rho^*}(p_i)}{H_{\rho^*}(s^*)} = \left(\sum_{i=1}^{n} \sum_{\sigma \in \mathrm{Sym}(n)} H_{\rho\sigma}(p_i)\right) \Bigg/ \left(\sum_{\sigma \in \mathrm{Sym}(n)} H_{\rho\sigma}(s)\right) \\ &= \sum_{\sigma \in \mathrm{Sym}(n)} \left(\sum_{i=1}^{n} H_{\rho\sigma}(p_i)\right) \Bigg/ \left(\sum_{\sigma \in \mathrm{Sym}(n)} H_{\rho}(s)\right)\end{aligned}$$

$$= \sum_{\sigma \in \mathrm{Sym}(n)} \left( \sum_{i=1}^{n} H_\rho(p_i) \right) \Big/ \left( \sum_{\sigma \in \mathrm{Sym}(n)} H_\rho(s) \right)$$
$$= \sum_{i=1}^{n} \frac{H_\rho(p_i)}{H_\rho(s)} = \mathcal{V}(M).$$

Thus both Parts 1 and 2 hold. Further,

$$H_{\rho^{i*}}(p_i) = \sum_{\sigma \in \mathrm{Sym}(n)} H_{(\rho^{i\sigma^{-1}})\sigma}(p_i) = \sum_{\sigma \in \mathrm{Sym}(n)} H_{\rho^{i\sigma^{-1}}}(p_{i\sigma^{-1}}) = (n-1)! \sum_{\ell=1}^{n} H_{\rho^\ell}(p_\ell),$$

which is independent of $i$. For $i \neq j$,

$$H_{\rho^{i*}}(p_j) = \sum_{\sigma \in \mathrm{Sym}(n)} H_{(\rho^{i\sigma^{-1}})\sigma}(p_j) = \sum_{\sigma \in \mathrm{Sym}(n)} H_{\rho^{i\sigma^{-1}}}(p_{j\sigma^{-1}})$$
$$= (n-2)! \sum_{\ell=1}^{n} \sum_{m=1, m\neq\ell}^{n} H_{\rho^\ell}(p_m),$$

which is independent of $i$ and $j$. Hence Part 3 holds. Also, for $B$ a $(k-1)$-subset of $\mathcal{P}\backslash p_i$, by definition we have $(s_{i\sigma^{-1}})\sigma = s_i$ and so

$$H_{\rho^{i*}}(s_i|B) = \sum_{\sigma \in \mathrm{Sym}(n)} H_{(\rho^{i\sigma^{-1}})\sigma}(s_i|B) = \sum_{\sigma \in \mathrm{Sym}(n)} H_{\rho^{i\sigma^{-1}}}(s_{i\sigma^{-1}}|B^{\sigma^{-1}})$$
$$= (k-1)!\,(n-k)! \sum_{\ell=1}^{n} \sum_{C \subseteq \mathcal{P}\backslash p_1, |C|=k-1} H_{\rho_\ell}(s_\ell|C),$$

which is independent of $i$ and $B$. Hence Part 4 holds. Lastly, by (9),

$$H_{\rho^*}(p_i) = \sum_{\ell=1}^{n} H_{\rho^{\ell*}}(p_i) = H_{\rho^{i*}}(p_i) + \sum_{\ell=1, \ell\neq i}^{n} H_{\rho^{\ell*}}(p_i),$$

which is independent of $p_i$ by Part 3. □

**Theorem 18.** *Let $\Gamma$ be a $(k, n)$-threshold access structure. Then $\mathcal{V}(\Gamma) \geq n^2/(n-k+1)$.*

**Proof.** Let $M = (M_0; M_1, \ldots, M_n)$ be an MTA-free scheme for $\Gamma$, where $M = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ and $\rho$ is as defined preceding Theorem 3, $M_0 = (\mathcal{P}, s, \rho_0)$ is a secret sharing scheme for $(\Gamma_0, \Delta_0)$ and $M_i = (\mathcal{P}, s_i, \rho^i)$ is a secret sharing scheme for $(\Gamma_i, \Delta_i)$ with $\rho^i_{s_i} = \rho^0_{p_i}$. We may assume that $M$ has Properties 1–5 of Lemma 17. Thus, in particular, there exist constants $a$ and $b$ such that $H_{\rho^i}(p_i) = a$ and $H_{\rho^i}(s_i|B) = b$ for all $i = 1, \ldots, n$ and all $(k-1)$-subsets $B$ of $\mathcal{P}\backslash p_i$. Note that $a \geq b$. For $p_j \notin Bp_i$ we have $H_{\rho^i}(p_i|Bp_j) = H_{\rho^i}(s_i|Bp_j) = 0$ and hence $H_{\rho^i}(p_j) \geq H_{\rho^i}(p_j|B) = H_{\rho^i}(s_i\, p_j|B) \geq b$. Thus

$$\sum_{j=1}^{n} H_{\rho^i}(p_j) \geq a + (n-1)b = nb + (a-b). \tag{10}$$

By Theorem 3, $H_\rho(B) = \sum_{i=1}^{n} H_{\rho^i}(B)$. Now $H_\rho(sB) \leq H_\rho(ss_1 \dots s_n B)$. For each $\pi \in \Omega$, $\pi^0_{p_i} = \pi^i_{s_i} = \pi^i_{p_i}$ (for $i = 1, \dots, n$) and $H_{\rho^0}(s|\mathcal{P}) = 0$, so $H_\rho(s|s_1 \dots s_n) = 0$. So $H_\rho(ss_1 \dots s_n B) = H_\rho(s_1 \dots s_n B)$. This is equal to $\sum_{i=1}^{n} H_{\rho^i}(s_i B)$ as for $\pi \in \Omega$

$$\begin{aligned}\rho_{s_1 \dots s_n B}(\pi_{s_1 \dots s_n B}) &= \rho^0_{\mathcal{P}}(\pi^0_{\mathcal{P}}) \prod_{i=1}^{n} \rho^i_{B|s_i}(\pi^i_B, \pi^i_{s_i}) \\ &= \prod_{i=1}^{n} \rho^i_{s_i B}(\pi^i_{s_i B}),\end{aligned}$$

as $\pi^0_{p_i} = \pi^i_{s_i}$. Therefore

$$\begin{aligned}H_\rho(s) &= H_\rho(sB) - H_\rho(B) \leq \sum_{i=1}^{n} (H_{\rho^i}(s_i B) - H_{\rho^i}(B)) = \sum_{i=1}^{n} H_{\rho^i}(s_i|B) \\ &= (k-1).0 + (n-k+1)b.\end{aligned}$$

Combining this with (10) allows us to bound the potential storage:

$$\mathcal{V}(M) = \sum_{i=1}^{n} \frac{H_\rho(p_i)}{H_\rho(s)} \geq \frac{n(nb + (a-b))}{(n-k+1)b} = \frac{n}{n-k+1}\left(n + \frac{a-b}{b}\right). \tag{11}$$

The expression (11) is minimized when $a = b$. Thus $\mathcal{V}(M) \geq n^2/(n-k+1)$, as required. □

Note that if the bound (11) is to be minimized then $a = b$ and thus for any $p_i$ and any $(k-1)$-subset $B$, $p_i \notin B$, we have $H_{\rho^i}(s_i|B) = H_{\rho^i}(p_i)$. Hence if the hypotheses of Lemma 17 hold, then the minimum potential storage case occurs when all the $M_i$ are perfect $(k, n)$-threshold schemes. Further $H_\rho(s) = (n-k+1)a$ and it follows that $M_0$ is a modified $(k-1, n, n)$ ramp scheme. This is exactly the case of the Base Ramp Construction.

**Corollary 19.** *Let $\Gamma$ be a $(k, n)$-threshold access structure. The optimal potential storage of $\mathcal{V}(\Gamma) = n^2/(n-k+1)$ is achieved by the Base Ramp Construction.*

**Proof.** Equation (7) and Theorem 18. □

### 7.3. *Optimal Information Rates for MTA-Free Threshold Schemes*

First we recall that if $\Gamma$ is a complete access structure, then $\rho(\Gamma) \leq \tilde{\rho}(\Gamma) \leq 1$ (when these bounds are met we call the scheme *ideal*). From [3] we see that if $\Gamma$ is a $(k, n)$-threshold access structure, then $\rho(\Gamma) = \tilde{\rho}(\Gamma) = 1$ and that these optimal values can both be met by geometric schemes. Hence we have:

**Theorem 20.** *Let $\Gamma$ be a $(k, n)$-threshold access structure. The optimal information rate and optimal average information rates $\rho_{MTA}(\Gamma) = \tilde{\rho}_{MTA}(\Gamma) = 1$ are achieved simultaneously by applying Corollary* 13 *to an ideal geometric $(k, n)$-threshold scheme.*

## 8. Conclusions and Further Work

We have discussed the idea of an MTA-free secret sharing scheme and have given some construction methods. We have presented three efficiency measures and then constructed MTA-free schemes designed to be efficient with respect to each of these measures. Finally, we have presented bounds on the efficiency of $(k, n)$-threshold schemes and given optimal constructions.

Three topics immediately beg further attention. First, bounds on the linkage and potential storage have not been given for general access structures. It is hoped that some results will be forthcoming that provide bounds on these measures, particularly for general complete access structures. Secondly we have not considered constructing MTA-free schemes that perform well with respect to more than one of the efficiency measures. In particular, it would be good to try and adapt the reduction technique to produce schemes that had good linkage (or potential storage) *and* had good information rates. Finally, much work is needed to produce constructions and efficiency bounds for incomplete access structures. Since many of our constructions hold for incomplete access structures, such bounds would be of considerable interest.

## Acknowledgments

The authors thank Yvo Desmedt for pointing out the useful role of homomorphic secret sharing in constructing efficient MTA-free schemes. We also thank Peter Wild and Stamatis Koumandos for profitable discussions.

## References

[1] J. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret secret. *Advances in Cryptology—Crypto* '86. Lecture Notes in Computer Science, Vol. 263, pp. 251–260, 1987.

[2] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology—Crypto* '88. Lecture Notes in Computer Science, Vol. 403, pp. 27–35, 1990.

[3] G. R. Blakley. Safeguarding cryptographic keys. *Proceedings of AFIPS* 1979 *National Computer Conference*, Vol. 48, pp. 313–317, 1979.

[4] E. F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. Combin. Comput.*, 9:105–113, 1989.

[5] 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.

[6] 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.

[7] E. Dawson and D. Donovan. Shamir's scheme says it all. *Proceedings of IFIP/Sec* '93, Toronto, pp. 69–80, 1993.

[8] Y. G. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM J. Discrete Math.*, 4:667–679, 1994.

[9] M. van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptogr.*, 6:143–169, 1995.

[10] Y. Frankel and Y. Desmedt. Classification of ideal homomorphic threshold schemes over finite Abelian groups. *Advances in Cryptology—EUROCRYPT* '92, Lecture Notes in Computer Science, Vol. 658, pp. 25–34, 1992.

[11] Y. Frankel, Y. Desmedt, and M. Burmester. Non-existence of homomorphic general secret sharing schemes for some key spaces. *Advances in Cryptology—Crypto* '92, Lecture Notes in Computer Science, Vol. 740, pp. 549–557, 1993.

[12] R. G. Gallager. *Information Theory and Reliable Communication*. Wiley, New York, 1968.
[13] I. Ingemarsson and G. J. Simmons. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. *Advances in Cryptology—EUROCRYPT* '90. Lecture Notes in Computer Science, Vol. 473, pp. 266–282, 1991.
[14] W.-A. Jackson and K. M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.*, 4:83–95, 1994.
[15] W.-A. Jackson and K. M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.*, 9:267–286, 1996.
[16] W.-A. Jackson and K. M. Martin. A combinatorial interpretation of ramp schemes. *Australas. J. Combin.*, 14:51–60, 1996.
[17] C.-S. Laih and L. Harn. Generalized threshold cryptosystems. *Advances in Cryptology—ASIACRYPT* '91. Lecture Notes in Computer Science, Vol. 739, pp. 159–165, 1993.
[18] K. M. Martin. New secret sharing schemes from old. *J. Combin. Math. Combin. Comput.*, 14:65–77, 1993.
[19] C. Meadows. Some threshold schemes without central key distributors. *Congress. Numer.*, 46:187–199, 1985.
[20] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979.
[21] G. J. Simmons. The consequences of trust in shared secret schemes. *Advances in Cryptology—EUROCRYPT* '93. Lecture Notes in Computer Science, Vol. 765, pp. 448–452, 1994.
[22] G. J. Simmons and C. Meadows. The role of trust in information protocols. *J. Comput. Security*, 3:71–84, 1994/95.
[23] G. J. Simmons, W.-A. Jackson, and K. Martin. The geometry of shared secret schemes. *Bull. Inst. Combin. Appl.*, 1:71–88, 1991.
[24] D. R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.*, 2:357–390, 1992.
[25] D. R. Stinson. Decomposition constructions for secret sharing schemes. *IEEE Trans. Inform. Theory*, 40:118–125, 1994.