New Secret Sharing Schemes from Old

Keith M. Martin

Department of Pure Mathematics,
The University of Adelaide,
G.P.O. Box 498, Adelaide SA 5001,
Australia

Abstract. A secret sharing scheme protects a secret (key) by distributing related information among a group of participants. This is done in such a way that only certain pre-specified groups of these participants (the access structure) can reconstruct the secret. In this paper we introduce a new measure of the efficiency of a perfect secret sharing scheme and examine methods of producing new secret sharing schemes from existing ones. These constructions can be used to help determine the optimal information rates for certain access structures.

1 Introduction

A *secret sharing scheme* is a system designed to share a special piece of information or *secret* among a group of *participants* in such a way that only specified groups of participants may obtain access to the secret. This collection of groups is referred to as the *access structure* of the secret sharing scheme. Secret sharing schemes were first discussed by Blakley [3] and Shamir [9] . For a bibliography of some of the existing published work in the subject, see Simmons [10].

Let $\mathcal{P}$ denote a finite set of participants and let $\Gamma \subseteq 2^{\mathcal{P}}$ be an access structure, where $2^{\mathcal{P}}$ denotes the set of all subsets of set $\mathcal{P}$. We say that Γ is *monotone* if for all $A, A' \subseteq \mathcal{P}$ such that $A \subseteq A'$, we have that $A \in \Gamma$ implies $A' \in \Gamma$. We will only consider monotone access structures in this paper as most applications have this property as a natural requirement. We note that Beutelspacher [2] considered a non-monotone situation where larger sets have a 'veto' facility over smaller sets.

The monotone access structure given by $\Gamma = \{A \subseteq \mathcal{P} \mid |A| \geq k\}$, where k is a positive integer, is known as the $(k, |\mathcal{P}|)$ *threshold* access structure.

If set $A \in \Gamma$ is such that $A' \in \Gamma$, $A' \subseteq A$ implies $A' = A$, then we say that A is *minimal* in Γ. We denote the set of all minimal sets in Γ by Γ^- and it is easy to see that Γ^- uniquely determines Γ.

Let $\mathcal{P}(\Gamma) = \{p \in \mathcal{P} \mid p \in A \text{ for some } A \in \Gamma^-\}$. We define the *core*, Γ^c, of Γ to be the monotone access structure defined on $\mathcal{P}(\Gamma)$ such that for $A \subseteq \mathcal{P}(\Gamma)$ we have $A \in \Gamma^c$ if and only if $A \in \Gamma$. A monotone access structure Γ is said to be *connected* if $\mathcal{P}(\Gamma) = \mathcal{P}$ (and hence $\Gamma^c = \Gamma$). If $\mathcal{P}(\Gamma) \neq \mathcal{P}$ then none of the participants of $\mathcal{P} \setminus \mathcal{P}(\Gamma)$ lie in any minimal set and so they are in some sense redundant to the scheme.

We now describe a useful method of representing a monotone access structure Γ. This method was first discussed in Benaloh and Leichter [1]. Let $\Gamma^- =$

$\{C_1, C_2, \ldots, C_r\}$ where $C_i \subseteq \mathcal{P}$, $(1 \leq i \leq r)$. Consider the logical expression $\Gamma = C_1 + C_2 + \cdots + C_r$ where the participants of $\mathcal{P}$ are now considered to be boolean variables, + represents logical OR and juxtaposition represents logical AND. If $A \subseteq \mathcal{P}$ then we say that Γ is *true at* A if the logical expression Γ is true when precisely the variables in A are set to true.

Lemma 1. *Let Γ be a monotone access structure defined on participant set $\mathcal{P}$ and let $\Gamma^- = \{C_1, C_2, \ldots, C_r\}$. For any $A \subseteq \mathcal{P}$, the logical expression $\Gamma = C_1 + C_2 + \cdots + C_r$ is true at A if and only if $A \in \Gamma$.*

Proof. $A \in \Gamma$ if and only if $C_i \subseteq A$ for some $C_i \in \Gamma^-$ and hence if and only if Γ is true at A. □

We note that in fact any valid representation of the logical expression $\Gamma = C_1 + C_2 + \cdots + C_r$ will also satisfy Lemma 1 and so, due to its convenience, we will often refer to a monotone access structure in terms of an equivalent logical expression.

Example 1. Let $\mathcal{P} = \{a, b, c, d\}$ and define a monotone access structure:

$$\Gamma = \big\{\{a,c\}, \{b,c\}, \{a,d\}, \{b,d\}, \{a,b,c\}, \{a,b,d\}, \{b,c,d\}, \{a,c,d\}, \{a,b,c,d\}\big\}.$$

Then $\Gamma^- = \big\{\{a,c\}, \{b,c\}, \{a,d\}, \{b,d\}\big\}$. Thus the following are three valid ways of representing Γ: $\Gamma = ac + bc + ad + bd$, $\Gamma = (a+b)c + (a+b)d$ and $\Gamma = (a+b)(c+d)$.

Our general model for secret sharing is to take the form of a matrix with certain special properties. The model is based on the model for secret sharing first proposed by Brickell and Davenport [5] . We begin by presenting some notation and concepts that will be needed to describe the model. Let $\mathcal{M}$ be a matrix with columns indexed from set $W = \{w_0, w_1, \ldots, w_n\}$. Let $X \subseteq W$ and let r be a row of $\mathcal{M}$.

$\mathcal{M}(r, X)$ is the row r of $\mathcal{M}$ restricted to the columns of set X. Then we have

$$S_{\mathcal{M}}(X) = \{\mathcal{M}(s, X) \mid s \text{ a row of } \mathcal{M}\},$$
$$\text{Match}(r, X) = \{s \text{ a row of } \mathcal{M} \mid \mathcal{M}(s, X) = \mathcal{M}(r, X)\}.$$

For $w \in W$ and $k \in S_{\mathcal{M}}(w)$ we have

$$\text{KeyMatch}(w, k, r, X) = \{s \in \text{Match}(r, X) \mid \mathcal{M}(s, w) = k\},$$
$$\text{Key}(w, r, X) = \{\mathcal{M}(s, w) \mid s \in \text{Match}(r, X)\}.$$

For $w \in W$ we write $X \Rightarrow w$ if for any two rows r_1, r_2 of $\mathcal{M}$ with $\mathcal{M}(r_1, X) = \mathcal{M}(r_2, X)$ it follows that $\mathcal{M}(r_1, w) = \mathcal{M}(r_2, w)$, otherwise we write $X \not\Rightarrow w$. We write $X \not\Rightarrow w$ if for all rows r of $\mathcal{M}$ there exists a positive integer λ such that for all $k \in S_{\mathcal{M}}(w)$ there are exactly λ rows s of $\mathcal{M}$ such that

$$\mathcal{M}(s, X) = \mathcal{M}(r, X) \text{ and } \mathcal{M}(s, w) = k.$$

Now let p_0 be the index of the first column of $\mathcal{M}$ and let the remaining columns be indexed by a set $\mathcal{P}$. Let Γ be a monotone access structure defined on $\mathcal{P}$. Then we define the *security* of $\mathcal{M}$ to be $\mathrm{Sec}(\mathcal{M})$ where

$$\frac{1}{\mathrm{Sec}(\mathcal{M})} = \max_{\substack{r \text{ a row of } \mathcal{M}, Q \notin \Gamma, \\ k \in S_{\mathcal{M}}(p_0)}} \frac{|\mathrm{Keymatch}(p_0, k, r, Q)|}{|\mathrm{Match}(r, Q)|}.$$

We are now ready to present our general model for secret sharing.

Let Γ be a monotone access structure defined on $\mathcal{P}$ and q be a positive integer. A *secret sharing scheme* $\mathrm{SS}(\Gamma, q)$ is a matrix $\mathcal{M}$ with $|\mathcal{P}| + 1$ columns indexed from the set $\mathcal{P} \cup \{p_0\}$ such that column p_0 contains entries from a set $\mathcal{K}$ of cardinality q, column p ($p \in \mathcal{P}$) contains entries from a finite set $S_{\mathcal{M}}(p)$ and

1. if $A \in \Gamma$ then $A \Rightarrow p_0$;
2. if $A \notin \Gamma$ then $A \not\Rightarrow p_0$;
3. $\mathrm{Sec}(\mathcal{M}) > 1$.

Further, $\mathcal{M}$ is defined to be *perfect* and is denoted $\mathrm{PS}(\Gamma, q)$ if 2. is replaced by the stronger condition:

2.* if $A \notin \Gamma$ then $A \not\rightsquigarrow p_0$.

To set up the scheme a row r must first be chosen at random. Participant p is then given $\mathcal{M}(r, p)$ and must not reveal this value to any other participant or outsider to the scheme. The value of the secret is $\mathcal{M}(r, p_0)$. When the time comes to try to reconstruct the secret, a group A of participants present their values to form $\mathcal{M}(r, A)$ and then scan the matrix $\mathcal{M}$ in search of rows s with the property that $\mathcal{M}(s, A) = \mathcal{M}(r, A)$. The definition of the scheme ensures that A can only uniquely determine the secret if $A \in \Gamma$.

Example 2. Let $\Gamma = ab + bc + cd$ be defined on participant set $\{a, b, c, d\}$. The following matrix $\mathcal{M}$ is a $\mathrm{PS}(\Gamma, 2)$.

$$\mathcal{M} = \begin{array}{c} \begin{array}{ccccc} p_0 & a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 3 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 3 & 0 \end{pmatrix} \end{array}.$$

We define the *security* of the scheme to be $\mathrm{Sec}(\mathcal{M})$. It can be easily shown that for an $\mathrm{SS}(\Gamma, q)$, $\mathrm{Sec}(\mathcal{M}) \leq q$ and that $\mathrm{Sec}(\mathcal{M}) = q$ precisely when $\mathcal{M}$ is perfect.

Note that if $A \notin \Gamma$ then we can deduce something slightly stronger than $A \not\Rightarrow p_0$.

Lemma 2. *Let $\mathcal{M}$ be an SS(Γ, q) and let $A \notin \Gamma$. Then for every row r of $\mathcal{M}$ there exists some row r' of $\mathcal{M}$ such that*

$$\mathcal{M}(r, A) = \mathcal{M}(r', A) \text{ but } \mathcal{M}(r, p_0) \neq \mathcal{M}(r', p_0).$$

Proof. Suppose that r is such that all rows r' such that $\mathcal{M}(r', A) = \mathcal{M}(r, A)$ also have the property that $\mathcal{M}(r', p_0) = \mathcal{M}(r, p_0) = k$, for some fixed $k \in S_{\mathcal{M}}(p_0)$. Then $\frac{|\text{KeyMatch}_{(p_0,k,r,A)}|}{|\text{Match}_{(r,A)}|} = 1$, and hence $\text{Sec}(\mathcal{M}) = 1$ which contradicts the definition of an SS(Γ, q). □

In the next section we discuss ways of measuring the efficiency of a perfect secret sharing scheme in terms of the sizes of the shares in the scheme. We introduce a new measure for assessing this efficiency. The remaining sections describe constructions of new secret sharing schemes from existing ones. The constructions in Section 3 all have the aim of increasing the security of existing secret sharing schemes. In Section 4 we look at the internal structure of a secret sharing scheme and identify schemes 'contained in' existing schemes. In Section 5 we build up large schemes from smaller ones and illustrate how to combine reults from Sections 4 and 5 to help in the determining of optimal information rates for monotone access structures.

2 Information Rates

Perfect secret sharing schemes are of particular interest to study since they have the property that a group of participants not in the access structure can not gain any information about the secret. In Ito et al [8] and Benaloh and Leichter [1] it was first shown that any monotone access structure can be realised a by perfect secret sharing scheme. Thus it would be useful to know how efficient a given scheme for a particular monotone access structure is. One quantity that can be considered when assessing this is the sizes of the shares held by the participants. The size of the share held by $p \in \mathcal{P}$ is represented by $|S_{\mathcal{M}}(p)|$ and it is desirable to try and keep this value small to reduce the amount of information that p must hold. It can be shown that for $\mathcal{M}$, a PS(Γ, q), we have $|S_{\mathcal{M}}(p)| \geq q$ for each $p \in \mathcal{P}(\Gamma)$. With this result in mind, Brickell and Stinson [6] proposed a measure of the efficiency of a perfect secret sharing scheme $\mathcal{M}$ in terms of the shares sizes of the participants. We call this quantity the *worst-case information rate* of $\mathcal{M}$ and denote it by

$$\dot{\rho} = \frac{\log_2 q}{\max_{p \in \mathcal{P}} \log_2 |S_{\mathcal{M}}(p)|}.$$

Thus $\dot{\rho}$ is such that $0 \leq \dot{\rho} \leq 1$ and has its value based on the largest share that is held by any participant in the scheme. Consider now a scheme where all but one of the participants hold small shares and the remaining participant holds a very large share. This scheme will have a low value of $\dot{\rho}$ but might be considered to be highly desirable by certain applications because the *average*

share size will probably be low. Thus we propose a second measure called the *average information rate* of $\mathcal{M}$ and denote it by

$$\tilde{\rho} = \frac{\log_2 q}{\frac{1}{|\mathcal{P}(\Gamma)|}\sum_{p\in\mathcal{P}(\Gamma)} \log_2 |S_{\mathcal{M}}(p)|}.$$

We acknowledge here that a similar measure has been independently proposed by Blundo [4]. It follows that for any PS(Γ, q) we have $0 \leq \dot{\rho} \leq \tilde{\rho} \leq 1$ and that $\dot{\rho} = 1$ if and only if $\tilde{\rho} = 1$. As in [5] we will refer to a PS(Γ, q) with $\dot{\rho} = \tilde{\rho} = 1$ as *ideal*. Note that these two measures of information rate both give different information about the sizes of the shares in the scheme and the importance placed on either measure will depend on the nature of the application under consideration.

Let $\mathcal{M}$ be a PS(Γ, q). We define the *contribution vector* (or *convec*) of $\mathcal{M}$ to be $\underline{u} = (u_p)_{p\in\mathcal{P}(\Gamma)}$ where for $p \in \mathcal{P}(\Gamma)$ we have $u_p = \log_q |S_{\mathcal{M}}(p)|$. The convec provides a convenient way of representing the share sizes in $\mathcal{M}$ and we can thus describe the information rates as follows,

$$\dot{\rho} = \frac{1}{\max_{p\in\mathcal{P}(\Gamma)} u_p}, \quad \tilde{\rho} = \frac{|\mathcal{P}(\Gamma)|}{\sum_{p\in\mathcal{P}(\Gamma)} u_p}.$$

Thus $\mathcal{M}$ in Example 2 has convec $\underline{u} = (u_a, u_b, u_c, u_d) = (1, 1, 2, 1)$ and hence $\dot{\rho} = \frac{1}{2}$ and $\tilde{\rho} = \frac{4}{5}$.

For access structure Γ we say that Γ has *optimal* worst-case information rate $\dot{\rho}_w$ if there exists a PS(Γ, q) (for some q) with worst-case information rate $\dot{\rho}_w$ but there does not exist any PS(Γ, q) (for any q) with worst-case information rate $\dot{\rho} > \dot{\rho}_w$. We define the optimal average information rate in an analagous way.

3 Schemes with Enhanced Security

In this section we use existing SS(Γ, q)'s to construct schemes for the same access structure Γ but with greater security. This is a generalisation of a result in [6]. We show that if a perfect secret sharing scheme can be found for any security q then a scheme can be constructed with arbitrarily high security and with information rates the same as that of the original scheme.

Theorem 3. *Let $\mathcal{M}_1$ be an SS(Γ, q_1) and let $\mathcal{M}_2$ be an SS(Γ, q_2). Then there exists $\mathcal{M}$, an SS(Γ, q_1q_2). Further, Sec$(\mathcal{M}) \geq$ Sec$(\mathcal{M}_1)$Sec$(\mathcal{M}_2)$.*

Proof. Define a new matrix $\mathcal{M}$ on columns $p_0 \cup \mathcal{P}$ with $S_{\mathcal{M}}(p) = S_{\mathcal{M}_1}(p) \times S_{\mathcal{M}_2}(p)$ for all $p \in p_0 \cup \mathcal{P}$. For every row r_1 of $\mathcal{M}_1$ and row r_2 of $\mathcal{M}_2$ define a row r of $\mathcal{M}$ by

$$\mathcal{M}(r, p) = \big(\mathcal{M}_1(r_1, p), \mathcal{M}_2(r_2, p)\big),$$

for each $p \in p_0 \cup \mathcal{P}$. With the assistance of Lemma 2 it is routine to check that $\mathcal{M}$ is an SS(Γ, q_1q_2) and that Sec$(\mathcal{M}) \geq$ Sec$(\mathcal{M}_1)$Sec$(\mathcal{M}_2)$. □

Note that we do not necessarily obtain equality in the bound on the security of Theorem 3 since it is possible that $\mathcal{M}_1$ and $\mathcal{M}_2$ attain their maximum values of $\frac{|\text{Keymatch}_{(p_0,k,r,Q)}|}{|\text{Match}_{(r,Q)}|}$ for different sets $Q \notin \Gamma$. However this problem does not arise when applying Theorem 3 with $\mathcal{M}_1 = \mathcal{M}_2 = \mathcal{M}$. Repeated applications of this give the following:

Corollary 4. *Let $\mathcal{M}$ be an $SS(\Gamma, q)$ with $Sec(\mathcal{M}) = w$ for some $w \geq 2$. Then for every $n \geq 1$ there exists $\mathcal{M}^n$, an $SS(\Gamma, q^n)$, with $Sec(\mathcal{M}^n) = w^n$.*

Hence the existence of an $SS(\Gamma, q)$ ensures the existence of schemes with access structure Γ and arbitrarily high security. In the case where the original schemes in Theorem 3 are both perfect it is straightforward to verify that we obtain [6, Theorem 3.1].

Result 5. *Let $\mathcal{M}_1$ be a $PS(\Gamma, q_1)$ and $\mathcal{M}_2$ be a $PS(\Gamma, q_2)$. Then there exists $\mathcal{M}$ a $PS(\Gamma, q_1 q_2)$.*

In [6] it was shown that if the schemes $\mathcal{M}_1$ and $\mathcal{M}_2$ in Result 5 both have worst-case information rate $\dot{\rho}$ then so too does the resulting Scheme $\mathcal{M}$. If $\mathcal{M}_1$ and $\mathcal{M}_2$ have average information rates $\tilde{\rho}_1$ and $\tilde{\rho}_2$ respectively then, since for each $p \in \mathcal{P}(\Gamma)$ we have that $S_{\mathcal{M}}(p) = |S_{\mathcal{M}_1}(p)||S_{\mathcal{M}_2}(p)|$, it can be verified that the average information rate of $\mathcal{M}$ is given by

$$\rho = \frac{\log_2 q_1 + \log_2 q_2}{\frac{\log_2 q_1}{\rho_1} + \frac{\log_2 q_2}{\rho_2}}.$$

Thus in the special case that $\tilde{\rho}_1 = \tilde{\rho}_2$ then we see that the average information rate of $\mathcal{M}$ is also left unchanged by the construction in Result 5. We also note that in the event that $q_1 = q_2$ we can express the convec of $\mathcal{M}$ neatly in terms of the convecs of $\mathcal{M}_1$ and $\mathcal{M}_2$. If $\mathcal{M}_1$ and $\mathcal{M}_2$ have convecs $\underline{u} = (u_p)_{p \in \mathcal{P}(\Gamma)}$ and $\underline{v} = (v_p)_{p \in \mathcal{P}(\Gamma)}$ then the convec of $\mathcal{M}$ is given by $\underline{w} = (w_p)_{p \in \mathcal{P}(\Gamma)}$ where $w_p = \frac{1}{2}(u_p + v_p)$ $(p \in \mathcal{P}(\Gamma))$.

Thus repeated applications of Result 5 give the following extension of [6, Corollary 3.2]:

Corollary 6. *Let $\mathcal{M}$ be a $PS(\Gamma, q)$ with information rates $\dot{\rho}$ and $\tilde{\rho}$. Then for every $n \geq 1$ there exists $\mathcal{M}^n$ a $PS(\Gamma, q^n)$ with information rates $\dot{\rho}$ and $\tilde{\rho}$.*

4 Restrictions and Contractions

In this section we study the internal structure of a secret sharing scheme and look at two constructions that produce schemes within existing schemes. These provide us with interesting information about constructing secret sharing schemes and also have a number of useful applications. We will illustrate one of these, which is to the determining of the optimal infromation rates of a monotone access structure.

Let Γ be a monotone access structure defined on set $\mathcal{P}$ and let $Q \subseteq \mathcal{P}$. The *restriction* of Γ at Q, $\Gamma_{|Q}$, and the *contraction* of Γ at Q, $\Gamma \cdot Q$, are monotone access structures defined on $\mathcal{P} \setminus Q$ such that for each $A \subseteq \mathcal{P} \setminus Q$,

$$A \in \Gamma_{|Q} \quad \Leftrightarrow A \in \Gamma,$$
$$A \in \Gamma \cdot Q \Leftrightarrow A \cup Q \in \Gamma.$$

Thus the members of $(\Gamma_{|Q})^-$ are precisely the members of Γ^- that do not contain any member of Q. If $Q \in \Gamma$ then the only member of $(\Gamma \cdot Q)^-$ is the emptyset $\emptyset$. If $Q \notin \Gamma$ then $(\Gamma \cdot Q)^-$ comprises of all the minimal non empty sets of the form $A \cap (\mathcal{P} \setminus Q)$, where $A \in \Gamma^-$.

Example 3. If Γ is a monotone access structure defined on participant set $\mathcal{P}$ then $\Gamma_{|(\mathcal{P} \setminus \mathcal{P}(\Gamma))} = \Gamma^c$.

Example 4. Let Γ be the (k, n) threshold access structure defined on participant set $\mathcal{P}$ and let $p \in \mathcal{P}$. If $k \neq n$ then $\Gamma_{|p}$ is the $(k, n-1)$ threshold access structure defined on $\mathcal{P} \setminus p$ and if $k \neq 1$ then $\Gamma \cdot p$ is the $(k-1, n-1)$ threshold access structure defined on $\mathcal{P} \setminus p$.

The next result is a generalisation of [6, Theorem 3.3].

Theorem 7. *Let $\mathcal{M}$ be an SS(Γ, q) and $Q \subset \mathcal{P}$. Then there exists $\mathcal{M}_{|Q}$, an SS$(\Gamma_{|Q}, q)$ with Sec$(\mathcal{M}_{|Q}) \geq$ Sec$(\mathcal{M})$.*

Proof. Form a new matrix $\mathcal{M}_{|Q}$ on columns $p_0 \cup (\mathcal{P} \setminus Q)$ by deleting the columns Q of $\mathcal{M}$. It is easy to see that $\mathcal{M}_{|Q}$ is an SS$(\Gamma_{|Q}, q)$. Further, if $A \notin \Gamma_{|Q}$ then $A \notin \Gamma$ and thus Sec$(\mathcal{M}_{|Q}) \geq$ Sec$(\mathcal{M})$. □

Corollary 8. *Let $\mathcal{M}$ be a PS(Γ, q) and $Q \subset \mathcal{P}$. Then there exists $\mathcal{M}_{|Q}$, a PS$(\Gamma_{|Q}, q)$.*

Proof. Apply Theorem 7 to form $\mathcal{M}_{|Q}$. Since $q \geq$ Sec$(\mathcal{M}_{|Q}) \geq$ Sec$(\mathcal{M}) = q$, it follows that Sec$(\mathcal{M}_{|Q}) = q$ and hence $\mathcal{M}_{|Q}$ is perfect. □

Now we consider contractions of a monotone access structure.

Theorem 9. *Let $\mathcal{M}$ be an SS(Γ, q) and let $Q \subset \mathcal{P}, Q \notin \Gamma$. Then there exists $\mathcal{M} \cdot Q$, an SS$(\Gamma \cdot Q, q')$ where Sec$(\mathcal{M}) \leq q' \leq q$ and Sec$(\mathcal{M} \cdot Q) \geq$ Sec$(\mathcal{M})$.*

Proof. Form a new matrix $\mathcal{M} \cdot Q$ on columns $p_0 \cup (\mathcal{P} \setminus Q)$ in the following manner. Let $(\alpha_1, \alpha_2, \ldots, \alpha_{|Q|}) \in S_{\mathcal{M}}(Q)$. Then for every row s of $\mathcal{M}$ such that $\mathcal{M}(s, Q) = (\alpha_1, \alpha_2, \ldots, \alpha_{|Q|})$, form a row r of $\mathcal{M} \cdot Q$ such that $\mathcal{M} \cdot Q(r, c) = \mathcal{M}(s, c)$ for all $c \in p_0 \cup (\mathcal{P} \setminus Q)$. It is straightforward, with the assistance of Lemma 2 to see that $\mathcal{M} \cdot Q$ is an SS$(\Gamma \cdot Q, q')$, where Sec$(\mathcal{M}) \leq q' \leq q$. Using the fact that $A \notin \Gamma \cdot Q$ if and only if $A \cup Q \notin \Gamma$, we can see that Sec$(\mathcal{M} \cdot Q) \geq$ Sec$(\mathcal{M})$. □

Note that we can thus produce $|S_{\mathcal{M}}(Q)|$ matrices $\mathcal{M} \cdot Q$ that have access structure $\Gamma \cdot Q$ by contracting on different members of $S_{\mathcal{M}}(Q)$. It is possible, however, that some of these schemes may have different securities.

Corollary 10. *Let $\mathcal{M}$ be a PS(Γ, q) and let $Q \subset \mathcal{P}, Q \notin \Gamma$. Then there exists $\mathcal{M}\cdot Q$, a PS$(\Gamma\cdot Q, q)$.*

Proof. Apply Theorem 9 to form $\mathcal{M}\cdot Q$. Since $q \geq \mathrm{Sec}(\mathcal{M}\cdot Q) \geq \mathrm{Sec}(\mathcal{M}) = q$, it follows that $\mathrm{Sec}(\mathcal{M}\cdot Q) = q$ and hence that $\mathcal{M}\cdot Q$ is perfect. □

Suppose $\mathcal{M}$ a PS(Γ, q) has convec $\underline{u} = (u_p)_{p\in\mathcal{P}(\Gamma)}$ and for $Q \subset \mathcal{P}$, the participants of $\mathcal{P}(\Gamma|Q)$ correspond to the first r entries in $\underline{u}$. Then $\mathcal{M}|Q$ will have convec $\underline{v} = (u_p)_{p\in\mathcal{P}(\Gamma|Q)}$. We can also see that if the participants of $\mathcal{P}(\Gamma\cdot Q)$ $(Q \notin \Gamma)$ correspond to the first s entries in $\underline{u}$ then $\mathcal{M}\cdot Q$ will have convec $\underline{w} = (w_p)_{p\in\mathcal{P}(\Gamma\cdot Q)}$, where $w_p \leq u_p$ $(p \in \mathcal{P}(\Gamma\cdot Q))$. Thus both restrictions and contractions of ideal schemes will themselves be ideal. We can use this information to obtain bounds on the optimal information rates of certain access structures. We first recall the following special case of a result from Capocelli et al [7].

Result 11. *Let $\mathcal{M}$ be a PS(Γ, q) with convec $\underline{u} = (u_a, u_b, u_c, u_d)$ where $\Gamma = ab + bc + cd$. Then $(u_b + u_c) \geq 3$.*

Example 5. Let $\mathcal{M}$ be a PS(Γ, q) with convec $\underline{u} = (u_a, \ldots, u_e)$ where $\Gamma = ab + bc + cde$. Let $\mathcal{M}\cdot e$ be the PS$(\Gamma\cdot e, q)$ with convec $\underline{v} = (v_a, \ldots, v_d)$ formed by contracting $\mathcal{M}$ at e. Now $\Gamma\cdot e = ab + bc + cd$ and by Result 11 the convec $\underline{v}$ must be such that $(v_b + v_c) \geq 3$. Hence we have that $(u_b + u_c) \geq 3$ and thus that the average information rate $\tilde{\rho}$ of $\mathcal{M}$ must be such that $\tilde{\rho} \leq \frac{5}{6}$. Since this result holds for any PS(Γ, q) we have that the optimal average information for Γ is bounded above by $\frac{5}{6}$.

Example 6. Let $\mathcal{M}$ be a PS(Γ, q) with convec $\underline{u} = (u_a, \ldots, u_e)$ where $\Gamma = ab + bc + cd + ade$. Since $\Gamma|e = ab + bc + cd$ we can apply a similar argument to Example 5 to show that the optimal average information rate for Γ is bounded above by $\frac{5}{6}$.

In the next section we will construct perfect secret sharing schemes with the access structures as in Examples 5 and 6 that have $\tilde{\rho} = \frac{5}{6}$. This will show that $\frac{5}{6}$ is the optimal average information rate for both of these access structures.

5 Insertions, Sums and Products

In this section we present a useful general construction which allows us to start with 'small' perfect schemes on a few participants and build up to 'large' perfect schemes on a greater number of participants. This provides us with a procedure for constructing perfect secret sharing schemes for complex access structures. We also show that there is a very simple description of the information rates of schemes that are consructed using this procedure.

Let Γ_1 and Γ_2 be two monotone access structures defined on participant sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively ($\mathcal{P}_1$ and $\mathcal{P}_2$ not necessarily disjoint), and let $z \in \mathcal{P}_1$. We

define the *insertion* of Γ_2 at z in Γ_1, $\Gamma_1(z \to \Gamma_2)$, to be the monotone access structure defined on set $(\mathcal{P}_1 \setminus z) \cup \mathcal{P}_2$ such that for $A \subseteq (\mathcal{P}_1 \setminus z) \cup \mathcal{P}_2$ we have

$$A \in \Gamma_1(z \to \Gamma_2) \Leftrightarrow \begin{cases} A \cap \mathcal{P}_1 \in \Gamma_1, \text{ or} \\ (A \cap \mathcal{P}_1) \cup z \in \Gamma_1 \text{ and } A \cap \mathcal{P}_2 \in \Gamma_2. \end{cases}$$

In other words, $\Gamma_1(z \to \Gamma_2)$ is the monotone access structure Γ_1 with participant z 'replaced' by the sets of Γ_2.

Example 7. If $\Gamma_1 = ab + bc + de$ and $\Gamma_2 = df$ then $\Gamma_1(b \to \Gamma_2) = adf + dfc + de$.

Theorem 12. *Let Γ_1 and Γ_2 be monotone access structures defined on participant sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, and let $z \in \mathcal{P}_1$. Let $\mathcal{M}_1$ be a PS(Γ_1, q) and let $\mathcal{M}_2$ be a PS$(\Gamma_2, |S_{\mathcal{M}_1}(z)|)$. Then there exists $\mathcal{M}$, a PS$(\Gamma_1(z \to \Gamma_2), q)$.*

Proof. Without loss of generality let $S_{\mathcal{M}_1}(z) = S_{\mathcal{M}_2}(p_0)$. First, pad out $\mathcal{M}_1$ and $\mathcal{M}_2$ to form matrices $\mathcal{M}_1'$ and $\mathcal{M}_2'$ by adding $|\mathcal{P}_2 \setminus \mathcal{P}_1|$ new columns to $\mathcal{M}_1$ labelled by $\mathcal{P}_2 \setminus \mathcal{P}_1$ and containing fixed entry x_1, and adding $|\mathcal{P}_1 \setminus \mathcal{P}_2|$ new columns to $\mathcal{M}_2$ labelled by $\mathcal{P}_1 \setminus \mathcal{P}_2$ and containing fixed entry x_2. Now form a new matrix $\mathcal{M}$ from $\mathcal{M}_1'$ and $\mathcal{M}_2'$ as follows. For any row r_1 of $\mathcal{M}_1'$ and row r_2 of $\mathcal{M}_2'$ such that $\mathcal{M}_1'(r_1, z) = \mathcal{M}_2'(r_2, p_0)$, form a row $r_1 r_2$ of $\mathcal{M}$ such that

$$\mathcal{M}(r_1 r_2, c) = \begin{cases} (\mathcal{M}_1'(r_1, c), \mathcal{M}_2'(r_2, c)), & \text{if } c \in (\mathcal{P}_1 \cup \mathcal{P}_2) \setminus z; \\ \mathcal{M}_1'(r_1, p_0), & \text{if } c = p_0. \end{cases}$$

It is routine to show that $\mathcal{M}$ is a PS$(\Gamma_1(z \to \Gamma_2), q)$. □

Example 8. Let $\Gamma_1 = ab + ac$ and $\Gamma_2 = de$ and let $\mathcal{M}_1$ and $\mathcal{M}_2$ be the PS$(\Gamma_1, 2)$ and PS$(\Gamma_2, 2)$ given by

$$\mathcal{M}_1 = \begin{array}{c} \begin{array}{cccc} p_0 & a & b & c \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \end{array}, \quad \mathcal{M}_2 = \begin{array}{c} \begin{array}{ccc} p_0 & d & e \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \end{array}.$$

Then following the construction of Theorem 12, we produce $\mathcal{M}$, a PS$(\Gamma_1(b \to \Gamma_2))$ given by

$$\mathcal{M} = \begin{array}{c} \begin{array}{ccccc} p_0 & a & d & e & c \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}.$$

There are many special cases of this general construction which are both interesting and useful. We will consider just two of these here.

If Γ_1 and Γ_2 are defined on $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively then we define the *sum* $\Gamma_1 + \Gamma_2$ and the *product* $\Gamma_1\Gamma_2$ to be the monotone access structures defined on $\mathcal{P}_1 \cup \mathcal{P}_2$ such that for $A \subseteq \mathcal{P}_1 \cup \mathcal{P}_2$,

$$A \in \Gamma_1 + \Gamma_2 \Leftrightarrow A \cap \mathcal{P}_1 \in \Gamma_1 \text{ or } A \cap \mathcal{P}_2 \in \Gamma_2,$$
$$A \in \Gamma_1\Gamma_2 \Leftrightarrow A \cap \mathcal{P}_1 \in \Gamma_1 \text{ and } A \cap \mathcal{P}_2 \in \Gamma_2.$$

The following is a generalisation of [6, Theorem 3.4].

Theorem 13. *Let $\mathcal{M}_1$ be a PS(Γ_1, q) be defined on participant set $\mathcal{P}_1$ and let $\mathcal{M}_2$ be a PS(Γ_2, q) be defined on participant set $\mathcal{P}_2$ with convecs $\underline{u} = (u_p)_{p\in\mathcal{P}_1(\Gamma_1)}$ and $\underline{v} = (v_p)_{p\in\mathcal{P}_2(\Gamma_2)}$ respectively. Then there exists $\mathcal{M}$, a PS$(\Gamma_1 + \Gamma_2, \rho, q)$ such that if $\Gamma_1^c + \Gamma_2^c$ is connected then the convec of $\mathcal{M}$ is given by $\underline{w} = (w_p)_{p\in\mathcal{P}_1(\Gamma_1)\cup\mathcal{P}_2(\Gamma_2)}$ where $w_p = u_p$ if $p \in (\mathcal{P}_1(\Gamma_1) \setminus \mathcal{P}_2(\Gamma_2))$, $w_p = v_p$ if $p \in (\mathcal{P}_2(\Gamma_2) \setminus \mathcal{P}_1(\Gamma_1))$, and $w_p = u_p + v_p$ if $p \in (\mathcal{P}_1(\Gamma_1) \cup \mathcal{P}_2(\Gamma_2))$.*

Proof. Let $\Gamma = a + b$ be defined on $\{a, b\}$, where a, b are not in $\mathcal{P}_1 \cup \mathcal{P}_2$. Let $\mathcal{N}$ be the ideal PS(Γ, q) given by three identical columns each containing the q distinct elements. Now produce a perfect scheme whose access structure is $\Gamma(a \to \Gamma_1)$ using the construction of Theorem 12 . Then use Theorem 12 once more to construct a perfect scheme for the insertion of Γ_2 at b in $\Gamma(a \to \Gamma_1)$. The result is a matrix $\mathcal{M}$, a PS$(\Gamma_1 + \Gamma_2, q)$.

It is easy to verify that for $p \in \mathcal{P}_1 \setminus \mathcal{P}_2$ we have $|S_{\mathcal{M}}(p)| = |S_{\mathcal{M}_1}(p)|$, for $p \in \mathcal{P}_2 \setminus \mathcal{P}_1$ we have $|S_{\mathcal{M}}(p)| = |S_{\mathcal{M}_2}(p)|$ and for $p \in \mathcal{P}_1 \cap \mathcal{P}_2$ we have $|S_{\mathcal{M}}(p)| = |S_{\mathcal{M}_1}(p)||S_{\mathcal{M}_2}(p)|$. Thus $\mathcal{M}$ has convec $\underline{w}$ as stated. □

Note that we can describe the average infromation rate $\tilde{\rho}$ of $\mathcal{M}$ constructed as in Theorem 13 in terms of the average information rates $\tilde{\rho}_1$ and $\tilde{\rho}_2$ of $\mathcal{M}_1$ and $\mathcal{M}_2$ repectively.

$$\begin{aligned}\tilde{\rho} &= \frac{|\mathcal{P}_1(\Gamma_1)\cup\mathcal{P}_2(\Gamma_2)|}{\sum_{p\in\mathcal{P}_1(\Gamma_1)\cup\mathcal{P}_2(\Gamma_2)} w_p} \\ &= \frac{|\mathcal{P}_1(\Gamma_1)\cup\mathcal{P}_2(\Gamma_2)|}{\sum_{p\in\mathcal{P}_1(\Gamma_1)} u_p + \sum_{p\in\mathcal{P}_2(\Gamma_2)} v_p} \\ &= \frac{|\mathcal{P}_1(\Gamma_1)\cup\mathcal{P}_2(\Gamma_2)|}{\frac{|\mathcal{P}_1(\Gamma_1)|}{\tilde{\rho}_1} + \frac{|\mathcal{P}_2(\Gamma_2)|}{\tilde{\rho}_2}}. \end{aligned} \tag{1}$$

The following corollary to Theorem 13 is worth stating because of its connection with Corollary 8.

Corollary 14. *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be disjoint participant sets. Then there exist $\mathcal{M}_1$, an ideal PS(Γ_1, q) and $\mathcal{M}_2$, an ideal PS(Γ_2, q), on participant sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, if and only if there exists $\mathcal{M}$, an ideal PS$(\Gamma_1 + \Gamma_2, q)$.*

Proof. Theorem 13 deals with the construction of $\mathcal{M}$ from $\mathcal{M}_1$ and $\mathcal{M}_2$. If $\mathcal{M}$ is an ideal PS$(\Gamma_1 + \Gamma_2, q)$ then by Corollary 8 we see that $\mathcal{M}|_{\mathcal{P}_2\setminus\mathcal{P}_1}$ is a PS(Γ_1, q) and $\mathcal{M}|_{\mathcal{P}_1\setminus\mathcal{P}_2}$ is a PS(Γ_2, q). Since restrictions of ideal schemes are ideal the result follows. □

We now present the analogous results for the product of two perfect secret sharing schemes.

Theorem 15. *Let $\mathcal{M}_1$ be a PS(Γ_1, q) be defined on participant set $\mathcal{P}_1$ and let $\mathcal{M}_2$ be a PS(Γ_2, q) be defined on participant set $\mathcal{P}_2$ with convecs $\underline{u} = (u_p)_{p\in\mathcal{P}_1(\Gamma_1)}$ and $\underline{v} = (v_p)_{p\in\mathcal{P}_2(\Gamma_2)}$ respectively. Then there exists $\mathcal{M}$, a PS($\Gamma_1\Gamma_2, \rho, q$) such that if $\Gamma_1^c\Gamma_2^c$ is connected then the convec of $\mathcal{M}$ is given by $\underline{w} = (w_p)_{p\in\mathcal{P}_1(\Gamma_1)\cup\mathcal{P}_2(\Gamma_2)}$ where $w_p = u_p$ if $p \in (\mathcal{P}_1(\Gamma_1) \setminus \mathcal{P}_2(\Gamma_2))$, $w_p = v_p$ if $p \in (\mathcal{P}_2(\Gamma_2) \setminus \mathcal{P}_1(\Gamma_1))$, and $w_p = u_p + v_p$ if $p \in (\mathcal{P}_1(\Gamma_1) \cup \mathcal{P}_2(\Gamma_2))$.*

Proof. Let $\Gamma = ab$ be defined on $\{a, b\}$, where a, b are distinct from $\mathcal{P}_1 \cup \mathcal{P}_2$. Let $\mathcal{N}$ be the ideal PS(Γ, q) whose q^2 rows are of the form $x, y, x+y \pmod q$, where x, y vary over all the ordered pairs defined on $\mathbf{Z}_q$. Now produce a perfect scheme whose access structure is $\Gamma(a \to \Gamma_1)$ using the construction of Theorem 12 . Then use Theorem 12 once more to construct a perfect scheme for the insertion of Γ_2 at b in $\Gamma(a \to \Gamma_1)$. The result is a matrix $\mathcal{M}$, a PS($\Gamma_1\Gamma_2, q$).

For $p \in \mathcal{P}$ we can show that the values of $|S_{\mathcal{M}}(p)|$ are identical to those calculated in the construction of Theorem 13. It then follows that if $\Gamma_1^c\Gamma_2^c$ is connected, the convec of $\mathcal{M}$ is as calculated in Theorem 13. □

Note that since the convec of $\mathcal{M}$ in Theorem 15 is the same as that produced in Theorem 13 we can state the average information rate $\tilde{\rho}$ of $\mathcal{M}$ in terms of the average information rates of $\mathcal{M}_1$ and $\mathcal{M}_2$ as given by (1).

Corollary 16. *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be disjoint participant sets. Then there exist $\mathcal{M}_1$, an ideal PS(Γ_1, q) and $\mathcal{M}_2$, an ideal PS(Γ_2, q), on participant sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, if and only if there exists $\mathcal{M}$, an ideal PS($\Gamma_1\Gamma_2, q$).*

Proof. Theorem 15 deals with the construction of $\mathcal{M}$ from $\mathcal{M}_1$ and $\mathcal{M}_2$. If $\mathcal{M}$ is an ideal PS($\Gamma_1\Gamma_2, q$) then by Corollary 10 we see that $\mathcal{M}\cdot_{\mathcal{P}_2\setminus\mathcal{P}_1}$ is a PS(Γ_1, q) and $\mathcal{M}\cdot_{\mathcal{P}_1\setminus\mathcal{P}_2}$ is a PS(Γ_2, q). Since contractions of ideal schemes are ideal the result follows. □

We now use Theorems 13 and 15 to illustrate combinatorially the general construction method for producing a perfect secret sharing scheme for a given monotone access structure of [1]. We show that the information rates for schemes constructed in this way can be neatly described.

Define a logical expression to be *admissable* if it can be constructed from variables in such a way that it remains connected at every stage of its construction. Further, we define the number of *literals* of a logical expression to be the total number of occurences of variables in the expression. Then we have the following result.

Theorem 17. *Let Γ be a monotone access structure defined on set $\mathcal{P}$ that can be represented by an admissable logical expression involving N literals such that the most frequently occurring literal appears exactly M times in the expression, and let $q \geq 2$. Then there exists a PS(Γ, q) with average information rate $\tilde{\rho} = \frac{|\mathcal{P}|}{N}$ and worst-case information rate $\dot{\rho} = \frac{1}{M}$.*

Proof. First we note the following. Let Γ_1, Γ_2 be connected monotone access structures defined on $\mathcal{P}_1, \mathcal{P}_2$ respectively, and let $\mathcal{M}_1$ and $\mathcal{M}_2$ be a PS(Γ_1, q) and a PS(Γ_2, q) respectively, with $\tilde{\rho}_1 = \frac{|\mathcal{P}_1|}{N_1}$ and $\tilde{\rho}_2 = \frac{|\mathcal{P}_2|}{N_2}$ where N_1, N_2 denote the the number of literals in admissable logical expressions for Γ_1, Γ_2. Then if $\Gamma_1 + \Gamma_2$ is connected, by applying Theorem 13 we construct a PS$(\Gamma_1 + \Gamma_2, q)$ with $\tilde{\rho} =, \frac{|\mathcal{P}_1 \cup \mathcal{P}_2|}{N_1 + N_2}$. Similarly, if $\Gamma_1 \Gamma_2$ is connected then by applying Theorem 15 we can construct a PS$(\Gamma_1 \Gamma_2, q)$ with $\tilde{\rho} = \frac{|\mathcal{P}_1 \cup \mathcal{P}_2|}{N_1 + N_2}$.

We are now ready to construct our matrix $\mathcal{M}$. For each $p \in \mathcal{P}$, form an ideal PS(p, q) given by a $q \times 2$ matrix comprising of two identical columns each containing distinct entries. Note that these schemes all have $\tilde{\rho} = 1$ which in each case corresponds to the number of participants in their access structure divided by the number of literals in an admissable logical expression for their access structure (one divided by one). Then by taking the admissable logical expression for Γ and applying Theorem 13 and Theorem 15 where appropriate, we can construct a perfect scheme with access structure Γ. Since our logical expression for Γ was admissable, we see that the final average information rate is $\tilde{\rho} = \frac{|\mathcal{P}|}{N}$. As Γ is gradually constructed the entry in the convec corresponding to participant p icreases by one each time p occurs as a literal in the logical expression for Γ. Hence the worst-case information rate of the final matrix will be $\dot{\rho} = \frac{1}{M}$. □

We now illustrate the use of Theorem 17.

Example 9. Writing $\Gamma = ab + bc + cde$ in the form $\Gamma = b(a + c) + cde$ shows that there must exist a PS(Γ, q) with convec $(1, 1, 2, 1, 1)$, $\dot{\rho} = \frac{1}{2}$ and $\tilde{\rho} = \frac{5}{6}$. By Example 5 we see that this scheme is optimal with respect to average information rate.

Example 10. Writing $\Gamma = ab + bc + cd + ade$ in the form $\Gamma = \big(b + d(c + e)\big)(a + c)$ shows that there must be a PS(Γ, q) with convec $(1, 1, 2, 1, 1)$, $\dot{\rho} = \frac{1}{2}$ and $\tilde{\rho} = \frac{5}{6}$. By Example 6 we see that this scheme is optimal with respect to average information rate.

Example 11. Consider $\Gamma = ab + bc + cd$. Writing $\Gamma = b(a + c) + cd$ we produce a PS(Γ, q) with convec $(1, 1, 2, 1)$ and writing $\Gamma = ab + c(b + d)$ we produce a PS(Γ, q) with convec $(1, 2, 1, 1)$. Combining these by the method of Corollary 5 produces the PS(Γ, q^2) with convec $(1, \frac{3}{2}, \frac{3}{2}, 1)$ constructed in [7, Remark 2]. All three of these schemes have average information rate equal to $\frac{4}{5}$ and hence by Result 11 all have optimal average information rate. The first two scheme have worst-case information rate equal to $\frac{1}{2}$ but the third scheme has worst-case information rate $\frac{2}{3}$. As observed in [7] the worst-case information rate of $\frac{2}{3}$ is optimal.

6 Conclusions

We have proposed a second type of information rate for use in assessing the efficiency of a perfect secret sharing scheme. We have also presented a collec-

tion of constructions that can be used to produce new secret sharing schemes from existing schemes. The main application of these constructions is to the determining of optimal information rates of monotone access structures. Some examples of this have been given but more detailed results obtained using extensions of this technique will appear in a future paper. It should be noted that although the lower bounds for optimal information rates obtained by the method of Theorem 17 are adequate for many access structures, there is some room for improvement in the general case. In [1] it was noted that the representing of a monotone access structure simply as a logical expression featuring AND and OR functions is not the most efficient way since, for example, threshold functions could be introduced which made the description more concise an d lowered the size of some of the shares in the corresponding secret sharing scheme. There are many other functions (for example any function based on an access structure which can be represented by an ideal scheme) which can be used in this way to describe the access structure more concisely and hence lead to more efficient general constructions. This is an area worthy of further study.

References

1. J. Benaloh and J. Leichter: Generalized Secret Sharing and Monotone Functions. Advances in Cryptology – Crypto '88, Lecture Notes in Comput. Sci. 403 (1990) 27–35
2. A. Beutelspacher: How to say 'No'. Advances in Cryptology – Eurocrypt '89, Lecture Notes in Comput. Sci. 434 (1990) 491–496
3. G. R. Blakley: Safeguarding cryptographic keys. Proceedings of AFIPS 1979 National Computer Conference 48 (1979) 313–317
4. C. Blundo: Secret sharing schemes for access structures based on graphs. Tesi di Laurea, University of Salerno, Italy. (1991)
5. E. F. Brickell and D. M. Davenport: On the Classification of Ideal Secret Sharing Schemes. J. Cryptology 2 (1991) 123–124
6. E. F. Brickell and D. R. Stinson: Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes. J. Cryptology 2 (1992) 153–166
7. R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro: On the size of shares for secret sharing schemes. Advances in Cryptology – Crypto '91, Lecture Notes in Comput. Sci. 576 (1992) 101–113
8. M. Ito, A. Saito and T. Nishizeki: Secret Sharing Scheme Realising General Access Structure. Proceedings IEEE Global Telecom. Conf., Globecom '87, IEEE Comm. Soc. Press (1987) 99–102
9. A. Shamir: How to Share a Secret. Comm. ACM Vol 22 11 (1979) 612–613
10. G. J. Simmons: An Introduction to Shared Secret and/or Shared Control Schemes and their Application. Contemporary Cryptology: The Science of Information Integrity, IEEE Press (1992)
11. G. J. Simmons, W.–A. Jackson and K. Martin: The Geometry of Shared Secret Schemes. Bull. Inst. Combin. Appl. 1 (1991) 71–88

This article was processed using the LaTeX macro package with LLNCS style