Combinatorial Models for Perfect Secret Sharing Schemes

Wen-Ai Jackson* and Keith M. Martin†
Department of Pure Mathematics,
The University of Adelaide,
Adelaide SA 5005,
Australia

Dedicated to Anne Penfold Street.

Abstract

In this paper we review combinatorial models for secret sharing schemes. A detailed comparison of several existing combinatorial models for secret sharing sharing schemes is conducted. We pay particular attention to the ideal instances of these combinatorial models. We show that the models under examination have a natural hierarchy, but that the ideal instances of these models have a different hierarchy. We show that, in the ideal case, the combinatorial structures underlying the combinatorial models are essentially independent of the model being used. Further, we show that the matroid associated with an ideal scheme is uniquely determined by the access structure of the scheme and is independent of the model being used. We use this result to present a combinatorial classification of ideal threshold schemes.

1 Introduction

Secret sharing schemes are used to protect a *secret* among a group of *participants* by issuing each participant with a *share* of the secret. The *access structure* of a secret sharing scheme is the set of subsets of participants that are desired to be able to reconstruct the secret by pooling their shares. For a good introduction to the potential applications of secret sharing schemes, see [24].

*This work was partially supported by SERC Grant GR/G 03359
†This work was supported by the Australian Research Council

In this paper we concentrate on *unconditionally secure* secret sharing schemes. A scheme is unconditionally secure if its security is independent of the time and resources available to any party attempting to break the scheme. We will only consider access structures that are monotone; a *monotone* access structure defined on a participant set $\mathcal{P}$ is a collection Γ of subsets of $\mathcal{P}$ such that, if $A \in \Gamma$ and $B \supseteq A$ then $B \in \Gamma$ (for $A, B \subseteq \mathcal{P}$). We assume that $\Gamma \neq \emptyset$ and that $\Gamma \neq \{\emptyset\}$. Let Γ^- denote the collection of *minimal* sets of Γ, that is, $A \in \Gamma^-$ precisely when $A \in \Gamma$ and $A \backslash a \notin \Gamma$ for all $a \in A$. If there exists $A \in \Gamma^-$ such that $|A| \geq 2$ then we say that Γ is *non-trivial* (otherwise Γ is *trivial*). We say that Γ is *connected* if for each $x \in \mathcal{P}$ there exists $A \in \Gamma^-$ such that $x \in A$.

A secret sharing scheme is often loosely defined by saying that "a set in the access structure can determine the secret" and "a set not in the access structure can not determine the secret". Further, a scheme is often loosely defined as being *perfect* if "a set not in the access structure can not determine any information about the secret". We are interested in attempts to make rigorous these concepts through the establishment of precise mathematical models.

Combinatorial theory provides a very natural setting in which to model unconditionally secure secret sharing schemes. The first papers on the subject ([3] and [22]) dealt with the special case of *threshold* schemes (see Section 5). Particular combinatorial implementations of threshold schemes were discussed (using affine geometry and finite polynomials respectively). Since that time over 100 papers have been published in the area of secret sharing. As more theory is developed it is important to be aware of the subtle differences between the various existing models for secret sharing. We concentrate here on three combinatorial models that have received particular attention in recent work. We briefly review combinatorial models in Section 2 and then compare the three main models in Section 3. In Section 4 we consider the ideal cases of these models and discuss the relationships between them. In Section 5 we give a combinatorial classification of id! eal threshold schemes.

2 Review of combinatorial models

Throughout this paper $\mathcal{P}$ will denote a finite set of participants, Γ will denote a monotone access structure defined on $\mathcal{P}$ and s will denote the secret ($s \notin \mathcal{P}$). If A and B are finite sets we will write AB for $A \cup B$. Where appropriate, if x is an element from some finite set we will write x for the set $\{x\}$. For each $x \in s\mathcal{P}$ we associate some finite set $\langle x \rangle$. For a set $X \subseteq s\mathcal{P}$ let $\langle X \rangle$ be the set of tuples $\pi = (\pi_x)_{x \in X}$ (where $\pi_x \in \langle x \rangle$). For $Y \subseteq X$ and $\pi \in \langle X \rangle$ let π_Y denote the tuple $(\pi_y)_{y \in Y}$. In each of the models

we discuss, a secret sharing scheme M will (partly) consist of a subset $[s\mathcal{P}]_M$ of $\langle s\mathcal{P}\rangle$. Given $[s\mathcal{P}]_M$ and $X \subseteq s\mathcal{P}$, let $[X]_M = \{\pi_X \mid \pi \in [s\mathcal{P}]_M\}$. We will omit the subscripts M where there is no ambiguity. We denote the number of (distinct) tuples in $[X]_M$ by $|[X]_M|$.

We start by reviewing three of the most referenced combinatorial models for secret sharing.

2.1 Brickell-Davenport model (BD)

Let ρ be a probability measure defined on $\langle s\mathcal{P}\rangle$ and let $\Omega = \{\pi \in \langle s\mathcal{P}\rangle \mid \rho(\pi) > 0\}$. We say $M = (\mathcal{P}, s, \rho)$ is a BD-*secret sharing scheme* (or BD-*scheme*) for Γ if $[s\mathcal{P}]_M = \Omega$ and for $A \subseteq \mathcal{P}$,

(BD1) if $A \in \Gamma$ then $|[sA]| = |[A]|$;

(BD2) if $A \notin \Gamma$ then $|[sA]| = |[s]| \cdot |[A]|$.

We say that M is BD-*ideal* if $|[x]| = |[s]|$ for all $x \in \mathcal{P}$. This model was proposed in [7] (see also [21]). To implement a BD-scheme, a tuple $\pi \in [s\mathcal{P}]$ is selected with probability $\rho(\pi)$. The secret is given by π_s and participant $x \in \mathcal{P}$ is given share π_x. The basic property of a BD-scheme is that if an *unauthorised* set A of participants (that is, $A \notin \Gamma$) pool their shares then complete knowledge of M will leave a non-zero probability that any $\sigma \in [s]$ is π_s. Note that the properties (BD1) and (BD2) are independent of ρ.

2.2 Brickell-Stinson model (BS)

Let l be a mapping from $\langle s\mathcal{P}\rangle$ to the set of non-negative integers and let p be a probability measure defined on $\langle s\rangle$. For $A \subseteq \mathcal{P}$, $\alpha \in [A]$ and $\sigma \in [s]$, let $\lambda_A(\sigma, \alpha) = \sum_{\{\pi \in \langle s\mathcal{P}\rangle \mid \pi_s = \sigma, \pi_A = \alpha\}} l(\pi)$ (if $A = \emptyset$ then let $\lambda_A(\sigma, \alpha)$ be denoted by $\lambda(\sigma)$). For each $\pi \in \langle s\mathcal{P}\rangle$ let $\rho(\pi) = p(\pi_s)l(\pi)/\lambda(\pi_s)$ and let $\Omega = \{\pi \in \langle s\mathcal{P}\rangle \mid \rho(\pi) > 0\}$. We say $M = (\mathcal{P}, s, \rho)$ is a BS-*secret sharing scheme* (or BS-*scheme*) for Γ if $[s\mathcal{P}]_M = \Omega$ and for $A \subseteq \mathcal{P}$,

(BS1) if $A \in \Gamma$ then $|[sA]| = |[A]|$;

(BS2) if $A \notin \Gamma$ and $\alpha \in [A]$ then $\lambda_A(\sigma, \alpha)$ is independent of $\sigma \in [s]$.

We say that M is BS-*ideal* if $|[x]| = |[s]|$ for all $x \in \mathcal{P}$. This model first appeared in [8] (although a similar idea was first discussed in [7]), where the tuples of $[s\mathcal{P}]$ were written as rows of a matrix in which row π was repeated precisely $l(\pi)$ times (see also, for example, [5]). In [18] the BS-model was used under the assumption that the probability measure p on $\langle s\rangle$ was uniform. Note that for this model, this is equivalent to p being uniform on $[s]$. In [25] the special case of the BS-model with $l(\pi) = 1$

for all $\pi \in [s\mathcal{P}]$ was used. Note that Example 1 shows the existence of BS-schemes that have $l(\pi) \neq 1$ for some $\pi \in \langle s\mathcal{P} \rangle$.

To implement a BS-scheme, a secret $\sigma \in \langle s \rangle$ is selected according to probability measure p and then a tuple $\pi \in [s\mathcal{P}]$ with $\pi_s = \sigma$ is chosen with probability $l(\pi)/\lambda(\sigma)$. This is effectively equivalent to selecting a tuple $\pi \in [s\mathcal{P}]$ with probability $\rho(\pi)$. BS-schemes have a stronger property than BD-schemes in that, if an unauthorised set of participants pool their shares in a BS-scheme, the probability that $\sigma \in [s]$ is π_s is the same as that for someone outside the scheme who knows M but not the values of any shares.

Example 1 *Let* $\mathcal{P} = \{a, b\}$, $\Gamma = \{ab\}$ *and* $[s] = [a] = \{0, 1\}$, $[b] = \{0, 1, 2\}$. *Let* $M = (\mathcal{P}, s, \rho)$ *be the scheme with tuples indexed by* s, a, b *given by* $l(0,0,0) = 1$, $l(0,1,1) = 2$, $l(0,0,2) = 1$, $l(1,1,0) = 1$, $l(1,0,1) = 2$, $l(1,1,2) = 1$. *Let* p *be a probability measure defined on* $[s]$ *such that* $p(0)$ *and* $p(1)$ *are non-zero. Then* M *is a BS-scheme for* Γ.

2.3 Entropy model (E)

We first introduce the idea of the *entropy* of a finite set (see [12]). All the logarithms in this paper are to the base 2. Suppose ρ is a probability measure on $\langle s\mathcal{P} \rangle$. Let $A \subseteq s\mathcal{P}$ and let $\theta(A)$ be the random variable defined by the projection $\langle s\mathcal{P} \rangle \rightarrow \langle A \rangle$. The measure ρ induces the probability mass function ρ_A of $\theta(A)$ such that for each $\alpha \in \langle A \rangle$,

$$\rho_A(\alpha) = \sum_{\{\pi \in \langle s\mathcal{P} \rangle \mid \pi_A = \alpha\}} \rho(\pi).$$

We let $[A]_\rho = \{\alpha \in \langle A \rangle \mid \rho_A(\alpha) > 0\}$. The *entropy* $H_\rho(A)$ of $\theta(A)$ is defined to be

$$H_\rho(A) = -\sum_{\alpha \in [A]_\rho} \rho_A(\alpha) \log \rho_A(\alpha).$$

When there is no ambiguity we write $[A]$ for $[A]_\rho$ and $H(A)$ for $H_\rho(A)$. Let $B \subseteq s\mathcal{P}$, $\alpha \in [A]$ and $\beta \in [B]$. Let $\rho_{AB}(\alpha, \beta) = \sum_{\{\pi \in [AB] \mid \pi_A = \alpha, \pi_B = \beta\}} \rho(\pi)$. The measure ρ induces the conditional probability mass function $\rho_{A|B}$ such that for each $\alpha \in [A]$ and $\beta \in [B]$,

$$\rho_{A|B}(\alpha, \beta) = \frac{\rho_{AB}(\alpha, \beta)}{\rho_B(\beta)}.$$

We define the *conditional entropy* $H(A|B = \beta)$ of $\theta(A)$ given $\theta(B) = \beta$ as

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

and the conditional entropy $H(A|B)$ of $\theta(A)$ given $\theta(B)$ as

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

We say $M = (\mathcal{P}, s, \rho)$ is an E-*secret sharing scheme* (or E-*scheme*) for Γ if $[s\mathcal{P}]_M = [s\mathcal{P}]_\rho$ and for $A \subseteq \mathcal{P}$,

(E1) if $A \in \Gamma$ then $H(s \mid A) = 0$;

(E2) if $A \notin \Gamma$ then $H(s \mid A) = H(s)$.

We say that M is E-*ideal* if $H(x) = H(s)$ for all $x \in \mathcal{P}$. This model was used to describe perfect threshold schemes in, for example, [14, 15] and perfect schemes with general monotone access structures in, for example, [4, 9]. In [2] a similar model was used, except that *ideal* was defined to be $|[x]| = |[s]|$ for all $x \in \mathcal{P}$. E-schemes are implemented in the same way as BD-schemes. As with BS-schemes, if an unauthorised set of participants pool their shares in an E-scheme then the probability that $\sigma \in [s]$ is π_s is the same as that for someone outside the scheme who knows M but not the values of any shares.

2.4 Other combinatorial models

The three combinatorial models discussed in Section 2.3 have been selected due to their frequency of reference and their generality. Other models have been used that are combinatorial in nature. In [6] and [27], a general secret sharing model based on vector spaces was used. In, for example, [13], [23] and [24], projective geometry was used as a framework for modelling secret sharing. Both these models can be shown to be special examples of BS-schemes (see [13]).

A different combinatorial model for perfect threshold schemes was used in [10, 20, 26]. Schemes of this type have been referred to as *anonymous* for the reason that, on implementation, a participant need not identify themselves when they present their share. As anonymous schemes model a slightly different problem, we will not include them in our later discussion. The schemes under discussion in this paper are easily made anonymous, at the expense of increasing the size of each share through incorporation of the participant's identity.

3 Comparison of combinatorial models

Let Γ be a monotone access structure defined on $\mathcal{P}$. In this section we make a comparison between the three combinatorial models featured in Section 2.3.

Lemma 2 *Let ρ be a probability measure defined on $\langle s\mathcal{P}\rangle$ and let $A, B \subseteq s\mathcal{P}$.*

1. *The following three statements are equivalent:*
   (a) $H(A \mid B) = 0$;
   (b) $\rho_{AB}(\pi_A, \pi_B) = \rho_B(\pi_B)$ *for all* $\pi \in [s\mathcal{P}]$;
   (c) $|[AB]_\rho| = |[B]_\rho|$.
2. *The following two statements are equivalent:*
   (a) $H(A \mid B) = H(A)$;
   (b) $\rho_{AB}(\pi_A, \pi_B) = \rho_A(\pi_A)\rho_B(\pi_B)$, *for all* $\pi \in [s\mathcal{P}]$.

   Thus if $H(A \mid B) = H(A)$ *then* $[AB]_\rho = [A]_\rho \times [B]_\rho$ *and so* $|[AB]_\rho| = |[A]_\rho||[B]_\rho|$.

Proof. First, note that $H(A \mid B) = 0$ if and only if $H(A \mid B = \beta) = 0$ for all $\beta \in [B]_\rho$, if and only if for all $\pi \in [s\mathcal{P}]$ we have that $\rho_{AB}(\pi_A, \pi_B) = \rho_B(\pi_B)$. This happens if and only if for all $\pi, \pi' \in [s\mathcal{P}]_\rho$ with $\pi_B = \pi'_B$ we have that $\pi_A = \pi'_A$, which happens if and only if $|[AB]_\rho| = |[B]_\rho|$. This proves 1.

Similarly, $H(A \mid B) = H(A)$ if and only if $H(A \mid B = \beta) = H(A)$ for all $\beta \in [B]_\rho$, if and only if for all $\pi \in [s\mathcal{P}]$ we have that $\rho_{AB}(\pi_A, \pi_B) = \rho_A(\pi_A)\rho_B(\pi_B)$. So if $H(A \mid B) = H(A)$ then for $\alpha \in [A]_\rho$ and $\beta \in [B]_\rho$ there exists $\pi \in [s\mathcal{P}]$ with $\pi_A = \alpha$ and $\pi_B = \beta$. The result follows. □

The next result shows that a BS-scheme is a special type of E-scheme.

Theorem 3 *$M = (\mathcal{P}, s, \rho)$ is a BS-scheme for Γ if and only if M is an E-scheme for Γ and $\rho_{\mathcal{P}|s}$ takes only rational values.*

Proof. Let $M = (\mathcal{P}, s, \rho)$ be a BS-scheme for Γ. Note that for any $X \subseteq s\mathcal{P}$ we have that $[X]_\rho = [X]_M$. Note also that for any $\sigma \in \langle s\rangle$, we have $\rho_s(\sigma) = p(\sigma)$. For $A \subseteq \mathcal{P}$, $\alpha \in [A]$ and $\sigma \in [s]$, we have that

$$\rho_{sA}(\sigma, \alpha) = \sum_{\{\pi \in [sA] \mid \pi_s = \sigma, \pi_A = \alpha\}} \rho(\pi) = \frac{\rho_s(\sigma)\lambda_A(\sigma, \alpha)}{\lambda(\sigma)}, \qquad (1)$$

If $A \in \Gamma$ then by (BS1), $|[sA]| = |[A]|$. Thus $H(s|A) = 0$ by Lemma 2 (1). Now suppose $A \notin \Gamma$. Then from (BS2) and (1),

$$\rho_A(\alpha) = \sum_{\sigma \in [s]} \rho_{sA}(\sigma, \alpha) = \frac{\lambda_A(\sigma, \alpha)}{\lambda(\sigma)} \sum_{\sigma \in [s]} \rho_s(\sigma) = \frac{\lambda_A(\sigma, \alpha)}{\lambda(\sigma)}.$$

Thus $\rho_{s|A}(\sigma,\alpha) = \rho_{sA}(\sigma,\alpha)/\rho_A(\alpha) = \rho_s(\sigma)$. By Lemma 2 (2), $H(s|A = \alpha) = H(s)$ and thus $H(s|A) = H(s)$. So M is an E-scheme for Γ. Further, for $\alpha \in [\mathcal{P}]$ and $\sigma \in [s]$, we have by (1) that $\rho_{\mathcal{P}|s}(\alpha,\sigma) = \rho_{s\mathcal{P}}(\sigma,\alpha)/\rho_s(\sigma) = \lambda_{\mathcal{P}}(\sigma,\alpha)/\lambda(\sigma)$, which is rational.

Conversely, let $M = (\mathcal{P}, s, \rho)$ be an E-scheme for Γ such that $\rho_{\mathcal{P}|s}$ always takes rational values. Then there exists a positive integer λ such that for each $\sigma \in [s]$ and $\alpha \in [\mathcal{P}]$, $\rho_{\mathcal{P}|s}(\alpha,\sigma)$ can be expressed as $\rho_{\mathcal{P}|s}(\alpha,\sigma) = a(\alpha,\sigma)/\lambda$, for some non-negative integer $a(\alpha,\sigma)$. Define a mapping l from $\langle s\mathcal{P}\rangle$ to the set of non-negative integers such that $l(\pi) = a(\pi_{\mathcal{P}}, \pi_s)$. For any $\sigma \in [s]$ we have $\lambda(\sigma) = \sum_{\{\pi \in \langle s\mathcal{P}\rangle | \pi_s = \sigma\}} l(\pi) = \sum_{\{\pi \in \langle s\mathcal{P}\rangle | \pi_s = \sigma\}} a(\pi_{\mathcal{P}}, \sigma) = \lambda$. Then letting $p(\sigma) = \rho_s(\sigma)$ for each $\sigma \in \langle s\rangle$, we have that for each $\pi \in [s\mathcal{P}]$, $p(\pi_s)l(\pi)/\lambda(\pi_s) = \rho_s(\pi_s)a(\pi_{\mathcal{P}}, \pi_s)/\lambda = \rho_s(\pi_s)\rho_{\mathcal{P}|s}(\pi_{\mathcal{P}}, \pi_s) = \rho(\pi)$, as required. Property (BS1) follows from Lemma 2 (1). Suppose that $A \notin \Gamma$ and let $\alpha \in [A]$. Then for each $\sigma \in ![s]$,

$$\lambda(\sigma,\alpha) = \sum_{\{\pi \in [s\mathcal{P}] \,|\, \pi_s = \sigma, \pi_A = \alpha\}} \frac{\lambda\rho(\pi)}{\rho_s(\sigma)} = \frac{\lambda\rho_{sA}(\sigma,\alpha)}{\rho_s(\sigma)} = \lambda\rho_A(\alpha),$$

by Lemma 2 (2). Hence $\lambda(\sigma,\alpha)$ is independent of σ and thus (BS2) holds. It follows that M is a BS-scheme for Γ. □

Note that not every E-scheme is such that $\rho_{\mathcal{P}|s}$ takes only rational values. Consider the following trivial example (note that examples with non-trivial access structures can be found).

Example 4 *Let $\mathcal{P} = \{a\}$, $\Gamma = \{a\}$ and $[s] = \{0,1\}$, $[a] = \{0,1,2\}$. Let $M = (\mathcal{P}, s, \rho)$ be the scheme with tuples indexed by s, a given by $\rho(0,0) = u$, $\rho(0,1) = v$, $\rho(1,2) = 1-u-v$, where $0 < u, v < 1$, u is irrational and v is rational. Then M is an E-scheme for Γ and $\rho_{a|s}(1,0) = v/(u+v)$, which is irrational.*

Note that it is possible for ρ to take irrational values in a BS-scheme.

Example 5 *Let $\mathcal{P} = \{a,b\}$, $\Gamma = \{ab\}$ and $[s] = [a] = [b] = \{0,1\}$. Let $M = (\mathcal{P}, s, \rho)$ be the scheme with tuples indexed by s, a, b given by $l(0,0,0) = l(0,1,1) = l(1,0,1) = l(1,1,0) = 1$, and $p(0) = u, p(1) = 1-u$, where $0 < u < 1$, and u is irrational. Then $\rho(0,0,0) = \rho(0,1,1) = u/2$, $\rho(1,0,1) = \rho(1,1,0) = (1-u)/2$ and M is a BS-scheme for Γ with $\rho(\pi)$ is irrational for all $\pi \in [s\mathcal{P}]$.*

We now show that every E-scheme for Γ is a BD-scheme for Γ.

Theorem 6 *$M = (\mathcal{P}, s, \rho)$ is an E-scheme for Γ if and only if M is a BD-scheme for Γ and (E2) holds.*

Proof. Let $M = (\mathcal{P}, s, \rho)$ be an E-scheme for Γ and let $A \subseteq \mathcal{P}$. If $A \in \Gamma$ then $H(s|A) = 0$ and by Lemma 2 (1), $||[sA]|| = ||[A]||$. If $A \notin \Gamma$ then $H(s|A) = H(s)$ and by Lemma 2 (2), $||[sA]|| = ||[s]||||[A]||$. Thus M is a BD-scheme for Γ. Conversely, let $M = (\mathcal{P}, s, \rho)$ be a BD-scheme for Γ such that (E2) holds. If $A \in \Gamma$ then $||[sA]|| = ||[A]||$ and by Lemma 2 (1), $H(s|A) = 0$. Since (E2) holds we have that M is an E-scheme for Γ. □

Note that there exist BD-schemes where (E2) does not hold.

Example 7 *Let $\mathcal{P} = \{a, b\}$, $\Gamma = \{ab\}$ and $[s] = [a] = [b] = \{0, 1\}$. Let $M = (\mathcal{P}, s, \rho)$ be the scheme with tuples indexed by s, a, b given by $\rho(0,0,0) = \rho(1,1,0) = u$, $\rho(0,1,1) = \rho(1,0,1) = (1/2) - u$, where $0 < u < 1$, and u is irrational. Thus, in particular, $u \neq 1/4$. Then M is a BD-scheme for Γ but $H(s|a) < H(s) = 1$ and so (E2) does not hold.*

Corollary 8 *$M = (\mathcal{P}, s, \rho)$ is a BS-scheme for Γ if and only if M is a BD-scheme for Γ, $\rho_{\mathcal{P}|s}$ takes only rational values and (E2) holds.*

Proof. Follows from Theorems 3 and 6. □

In summary, from Theorems 3 and 6 it is clear that there is a hierarchy of schemes with BD-schemes at the top (most general) and BS-schemes at the bottom.

4 Ideal secret sharing schemes

In Section 3 we noted that a hierarchical relationship exists between the combinatorial schemes of Section 2.3. Does this hierarchy also apply to the ideal cases of each of the these models? We will review the relationship between ideal schemes and matroids and then use this relationship to prove (perhaps surprisingly) that there is a hierarchy among the ideal cases of the models, but that it is different from the general model hierarchy. We also show, however, that in the ideal case the underlying combinatorial structure behind the three models is essentially the same. Finally we show that, regardless of the definition of ideal, the associated matroid of an ideal scheme is determined uniquely by the access structure of the scheme. Throughout this section Γ will denote a connected monotone access structure.

4.1 Ideal schemes and matroids

Some important connections have been established between ideal secret sharing schemes and matroids. A *matroid* $T = (E, I)$ consists of a finite set E and a collection I of subsets of E such that (1) $\emptyset \in I$; (2) if $A \in I$

and $B \subseteq A$ then $B \in I$; (3) if $A, B \in I$ and $|A| < |B|$ then there exists an element $b \in B \setminus A$ with $Ab \in I$. A set in I is referred to as *independent* and a subset of E not in I is referred to as *dependent*. A minimal dependent set of T is a *circuit* and a maximal independent set of T is a *base*. Given any set $A \subseteq E$, the sizes of the maximal independent set(s) $B \subseteq A$ are constant and this size is referred to as the *rank* of A. The *rank* of T is the rank of E. For a good introduction to matroid theory see [19].

The relationship between ideal secret sharing schemes and matroids was first studied in Uehara et al [27]. It was shown that BS-ideal secret sharing schemes whose access structures have minimal sets of a constant size can be linked to matroids. Brickell and Davenport [7] considered the general case and proved the following fundamental result.

Result 9 *A BD-ideal scheme $M = (\mathcal{P}, s, \rho)$ for Γ is associated with a connected matroid $T(M)$ on $s\mathcal{P}$ such that*

1. *the sets $\Delta(M) = \{A \subseteq s\mathcal{P} \mid$ there exists $a \in A$ with $|[A \backslash a]| = |[A]|\}$, form the dependent sets of $T(M)$;*
2. *the circuits of $T(M)$ through s are precisely the sets sA where $A \in \Gamma^-$;*
3. *if $A \subseteq s\mathcal{P}$ then $|[A]| = |[s]|^{r(A)}$, where $r(A)$ is the rank of A in $T(M)$.*

We can show an equivalent theorem to Result 9 for the case of E-ideal schemes.

Theorem 10 *An E-ideal scheme $M = (\mathcal{P}, s, \rho)$ for Γ is associated with a connected matroid $T(M)$ on $s\mathcal{P}$ such that*

1. *the sets $\Delta(M) = \{A \subseteq s\mathcal{P} \mid$ there exists $a \in A$ with $H(a \mid A \backslash a) = 0\}$, form the dependent sets of $T(M)$;*
2. *the circuits of $T(M)$ through s are precisely the sets sA where $A \in \Gamma^-$;*
3. *if $A \subseteq s\mathcal{P}$ then $r(A) = H(A)/H(s)$, where $r(A)$ is the rank of A in $T(M)$.*

Proof. Follows in a straightforward way by arguing as in the proof of Result 9 and recalling that by Lemma 2 (1) $H(a \mid A \backslash a) = 0$ if and only if $|[A]| = |[A \backslash a]|$. □

We note that Kurosawa et al [16] proved Theorem 10 under the assumptions that $H(s) = \log |[s]|$ and $|[x]| = |[s]|$ for all $x \in \mathcal{P}$. We will see in Lemma 11 that for non-trivial access structures these assumptions are not necessary.

4.2 Combinatorial models of ideal schemes

We now compare the ideal cases of the three combinatorial models. We show first that although BS-schemes are special cases of E-schemes (Theorem 3), E-ideal schemes are special cases of BS-ideal schemes. First we need two lemmas.

Lemma 11 *Let Γ be a non-trivial monotone access structure. If $M = (\mathcal{P}, s, \rho)$ is an E-ideal scheme for Γ then ρ is uniform on $[s\mathcal{P}]$, $|[x]| = |[s]|$ for all $x \in \mathcal{P}$ and $H(s) = \log |[s]|$.*

Proof. Let B be a basis of $T(M)$ and let $b \in B$. Then $H(b \mid (B \backslash b)) = H(B) - H(B \backslash b) = H(s)$, by Theorem 10 (3). Since M is E-ideal, $H(b \mid (B \backslash b)) = H(b)$ and thus, by Lemma 2 (2) we have $[B] = [b] \times [B \backslash b]$. By repeated applications of this argument, $[B] = [b_1] \times \ldots \times [b_r]$. As B is a basis, $H(s\mathcal{P} \mid B) = H(s\mathcal{P}B) - H(B) = 0$ (by Theorem 10 (3)). Thus Lemma 2 (1) and (2) imply that for $\pi \in [s\mathcal{P}]$,

$$\rho(\pi) = \rho_B(\pi_B) = \prod_{b \in B} \rho_b(\pi_b). \tag{2}$$

Further, by Lemma 2 (1),

$$|[s\mathcal{P}]| = |[B]| = \prod_{b \in B} |[b]|. \tag{3}$$

Let $x \in \mathcal{P}$. Suppose $Ax \in \Gamma^-$, $A \subseteq \mathcal{P} \setminus x$. By Theorem 10 (2) sAx is a circuit of $T(M)$ and so Ax is an independent set. Hence there exists $B \supseteq Ax$ with B a basis of $T(M)$. Then $sB \backslash x$ is also a basis (see [19, p21, Ex. 6] for example). Applying (3) twice, we get $\prod_{b \in B} |[b]| = \prod_{b \in sB \backslash x} |[b]|$ and so $|[s]| = |[x]|$, as required.

As Γ is non-trivial, there exists $y \in \mathcal{P}$ with $y \notin \Gamma$. Suppose $D \subseteq s\mathcal{P} \setminus y$ such that $Dy \in \Gamma^-$. Then Dy is independent in $T(M)$ and thus there exists $E \supseteq Dy$ such that E is a basis of $T(M)$. As above, $sE \backslash y$ is a basis of $T(M)$. As $y \notin \Gamma^-$, $H(s \mid y) = H(s)$ so by Lemma 2 (2) $[sy] = [s] \times [y]$. Let $\sigma \in [s]$ and $\psi \in [y]$. Then there exists $\pi \in [s\mathcal{P}]$ such that $\pi_s = \sigma$ and $\pi_y = \psi$. Applying (2) twice (with bases E and $sE \backslash y$) we see that $\rho_y(\psi) = \rho_s(\sigma)$. Since $\sigma \in [s]$ was chosen arbitrarily, it follows that ρ_s is uniform on $[s]$ and that $H(s) = \log |[s]|$. As M is ideal, $H(x) = H(s)$ for all $x \in \mathcal{P}$ and since $|[x]| = |[s]|$ it follows that the probability mass function on $[x]$ is also uniform. Using this with (2) shows that the probability measure ρ is uniform on $[s\mathcal{P}]$. □

Lemma 12 *Let $M = (\mathcal{P}, s, \rho)$ be an E-ideal scheme for the trivial access structure Γ defined on $\mathcal{P}$. If $x \in \mathcal{P}$ then $|[x]| = |[s]|$.*

Proof. Let $x \in \mathcal{P}$. Since $H(s|x) = 0$ it follows that $||[x]|| \geq ||[s]||$. For $\sigma \in [s]$, let $\sigma(x) = \{\alpha \in [x] \,|\, \exists \pi \in [s\mathcal{P}]$ such that $\pi_s = \sigma, \pi_x = \alpha\}$. Thus, $\rho_s(\sigma) = \sum_{\alpha \in \sigma(x)} \rho_x(\alpha)$. Hence,

$$\begin{aligned} H(x) &= -\sum_{\sigma \in [s]} \sum_{\alpha \in \sigma(x)} \rho_x(\alpha) \log \rho_x(\alpha) \geq -\sum_{\sigma \in [s]} \sum_{\alpha \in \sigma(x)} \rho_x(\alpha) \log \rho_s(\sigma) \\ &= -\sum_{\sigma \in [s]} \log \rho_s(\sigma) \sum_{\alpha \in \sigma(x)} \rho_x(\alpha) = -\sum_{\sigma \in [s]} \log \rho_s(\sigma) \rho_s(\sigma) = H(s). \end{aligned}$$

Since $H(x) = H(s)$ we have equality in the above and so $\rho_x(\alpha) = \rho_s(\sigma)$ for all $\alpha \in \sigma(x)$. Thus $|\sigma(x)| = 1$ and hence $||[x]|| = ||[s]||$, as required. □

Theorem 13 *$M = (\mathcal{P}, s, \rho)$ is an E-ideal scheme for Γ if and only if M is a BS-ideal scheme for Γ with ρ_s uniform or Γ trivial.*

Proof. Let $M = (\mathcal{P}, s, \rho)$ be an E-ideal scheme for Γ. Suppose that Γ is non-trivial. Then by Lemma 11, ρ is uniform on $[s\mathcal{P}]$ and ρ_s is uniform on $[s]$. Thus for any $\alpha \in [\mathcal{P}]$ and any $\sigma \in [s]$ we have that $\rho_{\mathcal{P}|s}(\alpha, \sigma) = \rho(\alpha, \sigma)/\rho_s(\sigma) = ||[s]||/||[s\mathcal{P}]||$. Hence $\rho_{\mathcal{P}|s}$ always takes rational values and thus by Theorem 3, M is a BS-scheme for Γ. Further, by Lemma 11, $||[x]|| = ||[s]||$ for all $x \in \mathcal{P}$ and thus M is a BS-ideal scheme for Γ. If Γ is trivial then for all $x \in \mathcal{P}$ we have $H(x|s) = 0$ and hence by Theorem 3, M is a BS-scheme for Γ. The fact that M is BS-ideal follows from Lemma 12.

Conversely, let $M = (\mathcal{P}, s, \rho)$ be a BS-ideal scheme for Γ. By Theorem 3, M is an E-scheme for Γ. Suppose ρ_s is uniform. Now for any $x \in \mathcal{P}$, $H(x) \geq H(s)$ (a straightforward generalisation of a result first shown in [14] for threshold schemes), and thus $\log ||[x]|| \geq H(x) \geq H(s) = \log ||[s]||$. Since M is BS-ideal it follows that we have equality throughout, and in particular $H(x) = H(s)$. Hence M is E-ideal for Γ. Now suppose that Γ is trivial. Let $x \in \mathcal{P}$. Since $||[x]|| = ||[s]||$ it follows that for any pair $\pi, \tau \in [s\mathcal{P}]$, $\pi_x = \tau_x$ if and only if $\pi_s = \tau_s$. Thus $H(x) = H(s)$ and consequently M is E-ideal for Γ. □

Note that Example 5 is a BS-ideal scheme that is also an E-scheme, but that is not E-ideal, since $H(s) < H(a) = H(b) = 1$. We now consider the relationship between BD-ideal schemes and BS-ideal schemes.

Theorem 14 *$M = (\mathcal{P}, s, \rho)$ is a BS-ideal scheme for Γ if and only if M is a BD-ideal scheme for Γ, (E2) holds, and $\rho_{\mathcal{P}|s}$ takes only rational values.*

Proof. Let $M = (\mathcal{P}, s, \rho)$ be a BS-ideal scheme for Γ. By Theorem 3 it follows that M is an E-scheme for Γ (hence (E2) holds) and that $\rho_{\mathcal{P}|s}$

takes only rational values. Further, by Theorem 6 it follows that M is a BD-scheme for Γ. Since $||[x]|| = ||[s]||$ for all $x \in \mathcal{P}$, M is in BD-ideal for Γ.

Conversely, let $M = (\mathcal{P}, s, \rho)$ be a BD-ideal scheme for Γ such that (E2) holds and $\rho_{\mathcal{P}|s}$ takes only rational values. By Theorem 6 it follows that M is an E-scheme for Γ. Further, by Theorem 3, since $\rho_{\mathcal{P}|s}$ takes only rational values, it follows that M is a BS-scheme for Γ. Since $|[x]| = |[s]|$ for all $x \in \mathcal{P}$, M is BS-ideal for Γ. □

Corollary 15 *$M = (\mathcal{P}, s, \rho)$ is an E-ideal scheme for Γ if and only if M is a BD-ideal scheme for Γ, (E2) holds, $\rho_{\mathcal{P}|s}$ takes only rational values, and either ρ_s is uniform or Γ is trivial.*

Proof. Follows from Theorems 13 and 14. □

Note that Example 7 is a BD-ideal scheme that is not an E-scheme and consequently is neither E-ideal nor BS-ideal. We now consider the underlying combinatorial structure $[s\mathcal{P}]$ of the ideal case of the three models. If $A \subseteq s\mathcal{P}$ and $\alpha \in [A]$ then let $\mu_A(\alpha) = |\{\pi \in [s\mathcal{P}] \,|\, \pi_A = \alpha\}|$. Similarly for $A, B \subseteq s\mathcal{P}$ and $\alpha \in [A], \beta \in [B]$, let $\mu_{AB}(\alpha, \beta) = |\{\pi \in [s\mathcal{P}] \,|\, \pi_A = \alpha, \pi_B = \beta\}|$.

Result 16 *[7] Let $M = (\mathcal{P}, s, \rho)$ be a BD-ideal scheme for Γ. Let $A \notin \Gamma$ and $\alpha \in [A]$. Then $\mu_{sA}(\sigma, \alpha)$ is independent of $\sigma \in [s]$ (if $A = \emptyset$ then $\mu_{sA}(\sigma, \alpha) = \mu_s(\sigma)$).*

Lemma 17 *Let $M = (\mathcal{P}, s, \rho)$ be a BD-ideal scheme for Γ. Let τ be the uniform probability measure defined on $[s\mathcal{P}]$. Then $M' = (\mathcal{P}, s, \tau)$ is an E-ideal scheme for Γ.*

Proof. Let $M = (\mathcal{P}, s, \rho)$ be a BD-ideal scheme for Γ and let τ be uniform on $[s\mathcal{P}]$. Let $A \in \Gamma$. By Lemma 2 (1), $H(s|A) = 0$. Now suppose $A \notin \Gamma$ and $\alpha \in [A]$. By Result 16, $\mu_{sA}(\sigma, \alpha)$ is independent of $\sigma \in [s]$. So $\tau_{s|A}(\sigma, \alpha) = \tau_{sA}(\sigma, \alpha)/\tau_A(\alpha) = \mu_{sA}(\sigma, \alpha)/\mu_A(\alpha)$ is independent of $\sigma \in [s]$. Thus $\tau_{s|A}(\sigma, \alpha) = 1/|[s]|$. By Result 16 with $A = \emptyset$, we see that τ_s is uniform on $[s]$. Thus $\tau_{s|A}(\sigma, \alpha) = \tau_s(\sigma)$. By Lemma 2 (2), $H(s|A = \alpha) = H(s)$, $H(s|A) = H(s)$ and thus M' is an E-scheme for Γ.

It remains to show that M' is E-ideal. Let $x \in \mathcal{P}$. If $x \in \Gamma$ then since $||[x]|| = ||[s]||$ and $H(s|x) = 0$, it follows that $H(x) = H(s)$. Now suppose that $x \notin \Gamma$. Since τ_s is uniform on $[s]$ and Γ is connected we have $\log ||[x]|| \geq H(x) \geq H(s) = \log ||[s]||$. Thus we have equality throughout, and in particular $H(x) = H(s)$. Thus M' is an E-ideal scheme for Γ. □

Let BD(Γ) be the set of all collections of tuples $[s\mathcal{P}]_M$ for which there exists a probability measure ρ such that $M = (\mathcal{P}, s, \rho)$ is a BD-ideal scheme

for Γ. In a similar way we can define sets BS(Γ) and E(Γ). We show that these sets are all identical and hence the set of combinatorial structures that underly ideal schemes for a connected monotone access structure Γ is independent of the model being used.

Theorem 18 *Let Γ be a connected monotone access structure on $\mathcal{P}$. Then* BD(Γ)=BS(Γ)=E(Γ).

Proof. By Theorems 13 and 14 we see that E(Γ) $\subseteq$ BS(Γ) $\subseteq$ BD(Γ). Suppose that BD(Γ) $\neq \emptyset$. Then there exists $M = (\mathcal{P}, s, \rho)$, a BD-ideal scheme for Γ. By Lemma 17, there exists an E-ideal scheme $M' = (\mathcal{P}, s, \tau)$ for Γ such that $[s\mathcal{P}]_{M'} = [s\mathcal{P}]_M$. Hence $[s\mathcal{P}]_M \in$ E(Γ). Thus BD(Γ) $\subseteq$ E(Γ) and hence BD(Γ)=BS(Γ)=E(Γ). □

4.3 Uniqueness of the associated matroid

The following theorem was first given for BS-ideal schemes in Martin [17] and stated in Beimel and Chor [2].

Theorem 19 *Let M be either a BD, BS or E-ideal scheme for Γ. Then the matroid $T(M)$ associated with M is independent of M, and uniquely determined by Γ.*

Proof. If M is either a BS or a E-ideal scheme for Γ, then from Theorem 14 and Corollary 15 we see that M is a BD-ideal scheme for Γ. Hence by Result 9 we see that the circuits of $T(M)$ are precisely the sets sA for $A \in \Gamma^-$. As $T(M)$ is connected it follows by [19, p133] that $T(M)$ is uniquely determined by the circuits through s and hence by Γ. □

In the light of Theorem 19 we refer to the matroid associated with a BD,BS or E-ideal scheme for Γ as the *associated matroid $T(\Gamma)$ of Γ*. For further results concerning the relationship between ideal secret sharing schemes and matroids see [2, 7, 21].

5 Classification of ideal threshold schemes

For the purposes of this section (and in the light of Theorem 14 and Corollary 15) we will use the term *ideal scheme* to mean a BD-ideal scheme. We say that an access structure Γ is *ideal* if there exists an ideal scheme for Γ. In this section we present a combinatorial classification of ideal threshold schemes. Let $1 \leq k \leq |\mathcal{P}| = n$. A (k,n)-*threshold* access structure is an access structure defined on $\mathcal{P}$, such that $\Gamma = \{A \subseteq \mathcal{P} \,|\, |A| \geq k\}$. Note that all (k,n)-threshold access structures are ideal ([22]). We describe any secret

sharing scheme for a (k,n)-threshold access structure as a (k,n)-*threshold* scheme.

Lemma 20 *Let Γ be a (k,n)-threshold access structure. Then the bases of the associated matroid $T(\Gamma)$ are precisely the subsets of $s\mathcal{P}$ of size k.*

Proof. By Result 9, the circuits of $T(\Gamma)$ containing s are precisely the sets of $H = \{A \mid A = Xs, |X| = k\}$. Further, by [19, p133], the remaining circuits of $T(\Gamma)$ are the minimal sets of the form $D(A_iA_j) = (A_iA_j) \setminus \bigcap\{A \in H \mid A \subseteq A_iA_j\}$, where A_i, A_j are distinct members of H. Note that for distinct $A_i, A_j \in H$ we have that $\bigcap\{A \in H \mid A \subseteq A_iA_j\} = \{s\}$, and hence the minimal sets $D(A_iA_j)$ will be those of the form $D(A_iA_j)$ where $|A_i \cap A_j| = k$. In this case $|D(A_iA_j)| = k+1$.

Now let X be a subset of $s\mathcal{P}$ of size $k+1$. If $s \in X$ then $X \in H$. Otherwise, let $x, y \in X$. Then $sX \setminus x$ and $sX \setminus y$ are both in H and intersect in k points. Hence $X = D\big((sX \setminus x)(sX \setminus y)\big)$ is a circuit of $T(\Gamma)$. Thus every subset of $s\mathcal{P}$ of size $k+1$ is a circuit of $T(\Gamma)$ and so any subset of size k is a base of $T(\Gamma)$. □

A *transversal design* $\mathrm{TD}_\mu(t,r,q)$, $\mathcal{D}$, is an incidence structure consisting of qr points and μq^t blocks. The points of $\mathcal{D}$ are partitioned into r classes of q points each and each block of $\mathcal{D}$ intersects each point class in precisely one point. Further, every set of t points from distinct point classes is incident with precisely μ blocks.

Theorem 21 *$M = (\mathcal{P}, s, \rho)$ is an ideal (k,n)-threshold scheme for which $|[s]_M| = q$ if and only if the tuples of $[s\mathcal{P}]_M$ form a $TD_1(k, n+1, q)$.*

Proof. Let $\mathcal{D}$ be a $\mathrm{TD}_1(k, n+1, q)$ and order each block of $\mathcal{D}$ such that for each i $(1 \le i \le n+1)$ the point in class i of a given block lies in position i of the ordered block. Consider the ordered blocks as tuples Ω indexed by a set $\mathcal{P}$ of n participants and a secret s. It is straightforward to verify that by defining an arbitrary probability measure on Ω we have that $M = (\mathcal{P}, s, \rho)$, with $[s\mathcal{P}]_M = \Omega$, is an ideal (k,n)-threshold scheme with $|[s]_M| = q$.

Conversely, let $M = (\mathcal{P}, s, \rho)$ be an ideal (k,n)-threshold scheme with $|[s]|_M| = q$. Relabel the sets $[s]_M$ and $[x]_M$ $(x \in \mathcal{P})$ using elements of distinct sets $S_1, \ldots, S_{n+1}$, each of size q. Now let $\mathcal{D}$ be an incidence structure whose points are the points of $\cup_{i=1}^{n+1} S_i$ and whose blocks are the tuples of $[s\mathcal{P}]_M$. Suppose $X \subseteq s\mathcal{P}$ such that $|X| = t$. By Lemma 20 , B is a base of $T(\Gamma)$. Then by Result 9, $|[B]_M| = q^t$, and hence every possible tuple of $[B]_M$ occurs in some $\pi \in [s\mathcal{P}]_M$. In other words every possible t points from distinct classes of $\mathcal{D}$ occur together in some block of $\mathcal{D}$. But, by Result 9, we see that $|[s\mathcal{P}]_M| = |[B]_M|$, and so every t points from distinct classes of

$\mathcal{D}$ occur together in exactly one block of $\mathcal{D}$. Hence $\mathcal{D}$ is a $\mathrm{TD}_1(k, n+1, q)$ as required. □

We note that the classification in Theorem 21 has previously appeared in [17] and in [11] for special classes of BS-ideal threshold schemes. Both BS-ideal and E-ideal threshold schemes will also give rise to transversal designs, however when constructing either a BS-ideal or an E-ideal threshold scheme from a transversal design only certain probability measures can be imposed on the induced tuples $[s\mathcal{P}]$ (for E-ideal schemes only the uniform measure on $[s\mathcal{P}]$ can be imposed).

6 Conclusions

We have discussed three combinatorial models that have been proposed for secret sharing schemes, and have compared them. The precise combinatorial requirements of a perfect secret sharing scheme are subjective and thus there is no concept of a 'correct' model. While BD-schemes have been shown to be the most general, it is probably more realistic to require the property that an unauthorised set of participants who pool their shares obtain no extra probabilistic information about the value of the secret. While BS-schemes are perhaps the more combinatorially asthetic of the other two models, the greater generality of E-schemes has led to this model for secret sharing being the most used and the most cited. We have shown, interestingly, that E-ideal schemes are more specialised than BS-schemes, but that the underlying combinatorial structures behind the ideal case of the three models are the same.

Amongst this discussion are two results of particular interest. The uniqueness of the associated matroid of an ideal secret sharing scheme has useful implications in the classification of ideal access structures. It means that the properties of matroids can be applied directly to an access structure when testing to see if the access structure is ideal. The combinatorial classification of ideal threshold schemes is of theoretical interest as more literature exists on the construction of transversal designs than on the construction of threshold schemes (see [1] for example), hence such a classification increases our knowledge of the parameters for which such schemes exist.

References

[1] Th. Beth, D. Jungnickel and H. Lenz, *Design Theory* (Bibliographisches Institut, Mannheim, 1985).

[2] A. Beimel and B. Chor, Universally ideal secret sharing schemes, *IEEE Trans. Inf. Th.*, **40** (1994), 786–794.

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

[4] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, On the information rate of secret sharing schemes, *Adv. in Cryptology - CRYPTO'92*, Lecture Notes in Comput. Sci. **740** (Springer-Verlag, 1993), 149–169.

[5] C. Blundo, A De Santis, D. R. Stinson, and U. Vaccaro, Graph decompositions and secret sharing schemes, *J. Cryptology*,**8** (1995), 39–64.

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

[7] E. F. Brickell and D. M. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptology*, **2** (1991), 123–134.

[8] 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.

[9] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, A note on secret sharing schemes, In *Sequences II: Methods in Communications, Security and Computer Science* (Springer Verlag, 1993), 335–344.

[10] D. Chen and D. R. Stinson, Recent results on combinatorial constructions for threshold schemes, *Austral. J. Combin.*, **1** (1990), 29–48.

[11] E. Dawson, E. S. Mahmoodian, and A. Rahilly, Orthogonal arrays and ordered threshold schemes, *Austral. J. Combin.*, **8** (1993), 27–44.

[12] R.G. Gallager, *Information theory and reliable communication* (John Wiley and Sons, New York, 1979).

[13] W.-A. Jackson and K. M. Martin, Geometric secret sharing schemes and their duals, *Des. Codes Cryptogr.*, **4** (1994), 83–95.

[14] E. D. Karnin, J. W. Greene, and M. E. Hellman, On secret sharing systems, *IEEE Trans. Inf. Th.*, **29** (1983), 35–41.

[15] S. Kothari, Generalised linear threshold scheme, *Adv. in Cryptology - CRYPTO'84*, Lecture Notes in Comput. Sci., **196** (Springer-Verlag, 1985), 231–241.

[16] K. Kurosawa, K. Okada, K. Sakano, W. Ogata and S. Tsujii, Nonperfect Secret Sharing Schemes and Matroids, *Adv. in Cryptology - EUROCRYPT'93*, Lecture Notes in Comput. Sci., **765** (1994), 126–141.

[17] K. M. Martin. *Discrete structures in the theory of secret sharing*, PhD thesis (University of London, 1991).

[18] K. M. Martin, New secret sharing schemes from old, *J. Combin. Math Combin. Comput.*, **14** (1993), 65–77.

[19] J. G. Oxley, *Matroid Theory* (Oxford University Press, Oxford, 1992).

[20] P. J. Schellenberg and D. R. Stinson, Threshold schemes from combinatorial designs., *J. Combin. Math. Combin. Comput.*, **5** (1989), 143–160.

[21] P. D. Seymour, On secret-sharing matroids, *J. Combin. Theory Ser B*, **56B** (1992),69–73.

[22] A. Shamir, How to share a secret, *Comm. ACM*, **22**(11) (1979), 612–613.

[23] G. J. Simmons, How to (really) share a secret. *Adv. in Cryptology - CRYPTO'88*, Lecture Notes in Comput. Sci. **403** (Springer-Verlag, 1990), 390–448.

[24] G. J. Simmons, An introduction to shared secret and/or shared control schemes and their application, In *Contemporary Cryptology* (IEEE Press, 1991), 441–497. .

[25] D. R. Stinson, An explication of secret sharing schemes, *Des. Codes Cryptogr.*, **2** (1992), 357–390.

[26] D. R. Stinson and S. A. Vanstone, A combinatorial approach to threshold schemes, *SIAM J. Discrete Math.*, 1 (1988), 230–237.

[27] T. Uehara, T. Nishizeki, and K. Nakamura, A secret sharing system with matroidal access structure, *Trans. IECE Japan* J69-A, **9** (1986), 1124–1132.