J. Cryptology (1996) 9: 233–250

Journal of
CRYPTOLOGY

Ideal Secret Sharing Schemes with Multiple Secrets*

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

Communicated by Douglas R. Stinson

Received 14 November 1994 and revised 22 March 1995

Abstract. We consider secret sharing schemes which, through an initial issuing of shares to a group of participants, permit a number of different secrets to be protected. Each secret is associated with a (potentially different) access structure and a particular secret can be reconstructed by any group of participants from its associated access structure without the need for further broadcast information. We consider ideal secret sharing schemes in this more general environment. In particular, we classify the collections of access structures that can be combined in such an ideal secret sharing scheme and we provide a general method of construction for such schemes. We also explore the extent to which the results that connect ideal secret sharing schemes to matroids can be appropriately generalized.

Key words. Ideal secret sharing schemes, Multiple secrets, Matroids.

1. Introduction

The basic idea behind secret sharing schemes and their relevance to cryptology is well documented (see [25]). Informally a *secret sharing scheme* permits a group of *participants* to jointly protect a *secret* through the issue of a related *share* of the secret to each participant. The scheme is designed so that if a set of participants pool their shares, then only those sets that are specified to be in the *access structure* of the scheme will be able to use their shares to reconstruct the secret.

Many secret sharing applications, particularly those associated with key-management and key-distribution problems, require the protection of more than one secret, possibly with different access structures associated with each secret. The precise generalization of a secret sharing scheme to include the option of protecting more than one secret is not immediately apparent. For instance:

- Should all the secrets be available for potential reconstruction during the lifetime of the scheme, or should the access of secrets be further controlled by enabling the

* The work of the second and third authors was supported by the Australian Research Council.

reconstruction of a particular secret only after extra information has been broadcast to the participants?

- Should a scheme be used just once, to reconstruct one or all of the secrets, or should the scheme be designed to enable multiple use?
- If a scheme is to be used more than once: in the event that a particular secret has been "reconstructed" by a group of participants, does the exact value of the secret remain undisclosed or is it known by the participants who enabled its reconstruction, or, indeed, is it known by all of the participants?

The desirable properties of a particular scheme depend on both the requirements of the application and also on the implementation. We consider here perhaps the most straightforward definition of a secret sharing scheme with multiple secrets. In this model all of the secrets are available for reconstruction without the need for additional broadcast information and the schemes are designed for one-time use only (of course, if an implementation is done in such a way that the value of the secret is not revealed to any of the participants, then such a scheme can be used repeatedly). Schemes of this type which have the same *threshold* access structures (see later) for each secret have been studied in [11], [16], and [21]. Schemes of this type which permit different threshold access structures for each secret have been studied in [3], [7], [14], [15], and [20] (we note that the schemes in [3], [7], and [20] can be used repeatedly as the threshold access structures are trivial). Schemes of this type which have more general monotone access structures for each secret were discussed in [6] and [23]. Schemes that allow repeated usage (a class of schemes with multiple secrets) and assume that reconstructed secrets become public knowledge have been studied in [5], [8], [13], [17], and [26]. Finally, secret sharing schemes with multiple secrets that require broadcast information have been studied in [2], [4], [5], and [19] (in particular, [2] and [19] dealt with the problem of disenrolling participants from a scheme).

All of the access structures under consideration in this paper are monotone. An access structure Γ defined on a participant set $\mathcal{P}$ is *monotone* if for all $A \subseteq B \subseteq \mathcal{P}$, if $A \in \Gamma$, then $B \in \Gamma$. We can describe Γ uniquely by the collection Γ^- of *minimal sets* of Γ, that is, the sets $A \subseteq \mathcal{P}$ such that $A \in \Gamma$ but $A \backslash a \notin \Gamma$ for all $a \in A$. We let $\text{core}(\Gamma) = \{p \in \mathcal{P}\colon p \in A$ for some $A \in \Gamma^-\}$ and say that Γ is *connected* if $\text{core}(\Gamma) = \mathcal{P}$. If $|\mathcal{P}| = n$, then, for $1 \leq k \leq n$, the *(k, n)-threshold* access structure Γ is such that $\Gamma = \{A \subseteq \mathcal{P}\colon |A| \geq k\}$. If $k = 1$, then we say that the threshold access structure is *trivial*.

A single secret sharing scheme is said to be *ideal* if the size of each share is the same as the size of the secret. We extend this definition and describe a secret sharing scheme with multiple secrets to be *ideal* if all of the secrets and all of the shares are the same size (this definition will be formalized later). Ideal single secret sharing schemes have been extensively studied (see, for example, [9] and [10]). In particular, the close relationship between ideal secret sharing schemes and matroids has been investigated in [1], [10], [12], [24], and [27].

In Section 2 we review the information-theoretic model of a single secret sharing scheme and recall the relationship between ideal schemes and matroids. In Section 3 we generalize the definition of a secret sharing scheme to permit more than one secret. Section 4 discusses separators of matroids and separators of probability measures. These concepts are fundamental to the establishment of our main result, which is described in

Section 5. This is a classification of ideal secret sharing schemes with multiple secrets. In particular we discuss which sets of access structures can "co-exist" in an ideal scheme. Finally, in Section 6 we examine the extent to which the relationship between ideal schemes and matroids can be extended to the multiple secret environment.

2. Single Secret Sharing Schemes

In this section we recall some basic results concerning (ideal) single secret sharing schemes. First, we review some notation and the definition of entropy, noting that all logarithms used in this paper have base 2. For finite sets A and B we write AB for $A \cup B$, and we write x for the set $\{x\}$. Let X be a finite set and let $\langle X \rangle$ be a finite collection of tuples, such that the entries of each $\pi \in \langle X \rangle$ are indexed by the elements of X. For $\pi = (\pi_x)_{x \in X} \in \langle X \rangle$ and for $A \subseteq X$, let π_A denote the tuple $(\pi_x)_{x \in A}$ and let $\langle A \rangle = \{\pi_A\colon \pi \in \langle X \rangle\}$. Let ρ be a probability measure on $\langle X \rangle$, and let $\theta(A)$ be the random variable defined by the projection $\langle X \rangle \to \langle A \rangle$. The measure ρ induces a probability mass function ρ_A of $\theta(A)$ on $\langle A \rangle$, such that, for each $\alpha \in \langle A \rangle$, we have $\rho_A(\alpha) = \sum_{\{\pi \in \langle X \rangle\colon\, \pi_A = \alpha\}} \rho(\pi)$. Let $[A]_\rho = \{\alpha \in \langle A \rangle\colon \rho_A(\alpha) > 0\}$. The *entropy* $H_\rho(A)$ of $\theta(A)$ is

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

When there is no ambiguity, we write $[A]$ for $[A]_\rho$ and $H(A)$ for $H_\rho(A)$. For $A, B \subseteq X$, $\alpha \in [A]$, and $\beta \in [B]$, let $\rho_{A,B}(\alpha, \beta) = \sum_{\{\pi \in [X]\colon\, \pi_A = \alpha, \pi_B = \beta\}} \rho(\pi)$. The measure ρ induces the conditional probability mass function $\rho_{A|B}$ such that, for each $\alpha \in [A]$ and $\beta \in [B]$, $\rho_{A|B}(\alpha, \beta) = \rho_{A,B}(\alpha, \beta)/\rho_B(\beta)$. The *conditional entropy* $H(A|B = \beta)$ of $\theta(A)$ given that $\theta(B) = \beta$ is $H(A|B = \beta) = -\sum_{\alpha \in [A]} \rho_{A|B}(\alpha, \beta) \log \rho_{A|B}(\alpha, \beta)$, and the *conditional entropy* $H(A|B)$ of $\theta(A)$ given $\theta(B)$ is

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

We note, in particular, the following elementary properties of entropy:

Result 1 [28]. Let ρ be a probability measure on $\langle X \rangle$ and let $A, B, C \subseteq X$. Then:

(1) $H(AB) \geq H(A)$.
(2) $H(A|B) \geq H(A|BC)$.
(3) $H(AB) \leq H(A) + H(B)$, with equality if and only if A and B are independent random variables, which is if and only if $\rho_{A,B}(\alpha, \beta) = \rho_A(\alpha)\rho_B(\beta)$ for all $\alpha \in [A]$ and $\beta \in [B]$.
(4) $H(A|B) = H(AB) - H(B)$.

Let $\mathcal{P}$ be a (finite) set of participants, let Γ denote a monotone access structure on $\mathcal{P}$, and let s ($s \notin \mathcal{P}$) denote the secret variable. Further, let ρ be a probability measure on

$\langle s\mathcal{P}\rangle$. Then $M = (\mathcal{P}, s, \rho)$ is a *secret sharing scheme* for Γ if, for $A \subseteq \mathcal{P}$:

(1) If $A \in \Gamma$, then $H(s|A) = 0$.
(2) If $A \notin \Gamma$, then $H(s|A) = H(s)$.

If Γ is connected, then we say that M is *connected.* Using Result 1, it is straightforward to show that if $p \in \text{core}(\Gamma)$, then $H(p) \geq H(s)$. Since it is desirable to minimize the *size* $H(p)$ of the share of each participant p in a secret sharing scheme, we say that M is *ideal* if $H(p) = H(s)$ for every $p \in \text{core}(\Gamma)$. We refer to $H(s)$ as the *size* of the secret s and call an access structure Γ *ideal* if there is an ideal secret sharing scheme M for Γ.

To implement a secret sharing scheme, a trusted *dealer* selects a tuple $\pi \in [s\mathcal{P}]$ with probability $\rho(\pi)$. Participant $p \in \mathcal{P}$ is given share π_p and the secret value is π_s. Any subset $A \in \Gamma$ is able to determine the value of s since the probability that the secret is π_s, given the pooled shares π_A, is 1. Further, if any subset $A \notin \Gamma$ pools their shares to form π_A, then the probability that any $\sigma \in [s]$ is the secret is exactly the same as for someone outside the scheme who knows M but not the value of any shares.

2.1. *Ideal Secret Sharing Schemes and Matroids*

First we review the definition and some properties of matroids, as found in [22]. A *matroid* $T = (\mathcal{E}, \mathcal{I})$ comprises a finite set $\mathcal{E}$ and a collection $\mathcal{I}$ of subsets of $\mathcal{E}$ such that:

(1) $\emptyset \in \mathcal{I}$.
(2) If $A \in \mathcal{I}$ and $B \subseteq A$, then $B \in \mathcal{I}$.
(3) If $A, B \in \mathcal{I}$ and $|A| < |B|$, then an element $b \in B \backslash A$ with $Ab \in \mathcal{I}$ exists.

An element of $\mathcal{I}$ is an *independent set* and a subset of $\mathcal{E}$ not in $\mathcal{I}$ is a *dependent set.* A minimal dependent set of T is a *circuit.* A matroid is *connected* if, for each pair of distinct elements $x, y \in \mathcal{E}$, there is a circuit containing both x and y. Given any set $A \subseteq \mathcal{E}$, the size of a maximal independent set $B \subseteq A$ is a constant, and this constant is the *rank* of A and is denoted by $\text{rank}_T A$. The *rank* of set T is the rank of $\mathcal{E}$, denoted by $\text{rank}_T T$. When there is no confusion, rank_T is denoted by rank.

Let $T = (\mathcal{E}, \mathcal{I})$ be a matroid and let $A \subseteq \mathcal{E}$. Let $\mathcal{I}|A = \{I \subseteq \mathcal{E}\backslash A\colon I \in \mathcal{I}\}$. Then $T|A = (\mathcal{E}\backslash A, \mathcal{I}|A)$ is a matroid, called the *restriction* of T at A. We note that if $B \subseteq \mathcal{E}\backslash A$, then $\text{rank}_{T|A}(B) = \text{rank}_T(B)$. Further, let $\mathcal{I} \cdot A = \{I \subseteq \mathcal{E}\backslash A\colon CI \in \mathcal{I}$ for all $C \subseteq A$ such that $C \in \mathcal{I}\}$. Then $T \cdot A = (\mathcal{E}\backslash A, \mathcal{I} \cdot A)$ is a matroid, called the *contraction* of T at A. We note that if $B \subseteq \mathcal{E}\backslash A$, then $\text{rank}_{T \cdot A}(B) = \text{rank}_T(AB) - \text{rank}_T(A)$ [22, Proposition 3.1.6].

The following result first appeared in [10], and this version appeared in [12].

Result 2. Let $M = (\mathcal{P}, s, \rho)$ be an ideal secret sharing scheme for Γ. If Γ is connected, then associated with M there is a connected matroid $T(M) = (s\mathcal{P}, \mathcal{I})$ satisfying:

(1) If $A \subseteq s\mathcal{P}$, then $\text{rank}(A) = H(A)/H(s)$.
(2) The dependent sets of $T(M)$ are precisely the sets $A \subseteq s\mathcal{P}$ such that $a \in A$ satisfying $H(a|A\backslash a) = 0$ exists.
(3) The circuits of $T(M)$ containing s are precisely the sets sA for $A \in \Gamma^-$.

We say that $T(M)$ is the *matroid associated with M*.

Result 3 [12, Theorem 6]. Let Γ be an ideal access structure. Then the matroid $T(M)$ associated with an ideal secret sharing scheme $M = (\mathcal{P}, s, \rho)$ for Γ depends only on Γ.

Thus, for any ideal secret sharing scheme M for Γ, we may refer to the matroid associated with M as the *matroid associated with* Γ.

Conversely, let $T = (s\mathcal{P}, \mathcal{I})$ be a matroid with distinguished point s, and let $\Gamma^- = \{A \subseteq \mathcal{P}\colon sA \text{ is a circuit of } T\}$. Now let $\Gamma(T) = \{B \subseteq \mathcal{P}\colon B \supseteq A \text{ for some } A \in \Gamma^-\}$. Then $\Gamma(T)$ is a monotone access structure, called the *monotone access structure associated with* T. Given a matroid T, it is an open problem as to when $\Gamma(T)$ is ideal. It was shown in [10] that if T is representable then $\Gamma(T)$ is ideal, however, in [24] it was shown that the access structure associated with the (nonrepresentable) Vamos matroid is not ideal.

We need the following slight extension of the idea of the matroid associated with an ideal secret sharing scheme to the case of a finite set with a probability measure. Let Z be a finite set and let ρ be a probability measure on $\langle Z\rangle$, such that $H_\rho(a)$ is a constant h for all $a \in Z$. Suppose that for all $A \subseteq Z$ and for all $a \in Z$ we have $H(a|A) = 0$ or $H(a)$ (and hence for any $A \subseteq Z$, $H_\rho(A)$ is a multiple of h). Then, by a similar proof to that of Result 2, the pair (Z, ρ) has an *associated* matroid $T = (Z, \mathcal{I})$ satisfying:

(1) If $A \subseteq Z$, then $\operatorname{rank}(A) = H(A)/h$.
(2) The dependent sets of T are precisely the sets $A \subseteq Z$ such that $a \in A$ satisfying $H(a|A\backslash a) = 0$ exists.

2.2. *Restrictions and Contractions*

We now recall the definition and some properties of restrictions and contractions of an access structure from Martin [18]. We consider, in particular, the case in which the underlying access structure is ideal. Let Γ be a monotone access structure on a participant set $\mathcal{P}$, and let $A \subseteq \mathcal{P}$. The *restriction* $\Gamma|A$ of Γ at A is the access structure defined on $\mathcal{P}\backslash A$ as $\Gamma|A = \{B \subseteq \mathcal{P}\backslash A\colon B \in \Gamma\}$. The *contraction* $\Gamma \cdot A$ of Γ at A is the access structure defined on $\mathcal{P}\backslash A$ as $\Gamma \cdot A = \{B \subseteq \mathcal{P}\backslash A\colon AB \in \Gamma\}$. Note that if $A \in \Gamma$, then $(\Gamma \cdot A)^- = \{\emptyset\}$.

Result 4 [18]. Let $M = (\mathcal{P}, s, \rho)$ be a secret sharing scheme for Γ. Let $A \subseteq \mathcal{P}$ and let $\mathcal{Q} = \mathcal{P}\backslash A$. Then there is a secret sharing scheme $M|A = (\mathcal{Q}, s, \mu)$ for $\Gamma|A$, with $\mu = \rho_{s\mathcal{Q}}$. Further, if M is ideal, then $M|A$ is ideal.

Result 5 [18]. Let $M = (\mathcal{P}, s, \rho)$ be a secret sharing scheme for Γ. Let $A \subseteq \mathcal{P}$ satisfy $A \notin \Gamma$ and let $\mathcal{Q} = \mathcal{P}\backslash A$. Then there is a secret sharing scheme $M \cdot A = (\mathcal{Q}, s, \mu)$ for $\Gamma \cdot A$, where for a given $\alpha \in [A]$ we have $\mu(\omega) = \rho_{s\mathcal{Q}|A}(\omega, \alpha)$, for each $\omega \in \langle s\mathcal{Q}\rangle$. (If $A \in \Gamma$, then $(\Gamma \cdot A)^- = \{\emptyset\}$, so we need not consider this case.) Further, if M is ideal, then $M \cdot A$ is ideal.

Let $M = (\mathcal{P}, s, \rho)$ be an ideal secret sharing scheme for Γ, with associated matroid T. We remark that for $A \subseteq \mathcal{P}$ it holds that $M|A$ has associated matroid $T|A$ and if $A \notin \Gamma$, then $M \cdot A$ has associated matroid $T \cdot A$.

3. Secret Sharing Schemes with One or More Secrets

In this section we generalize the idea of a single secret sharing scheme to that of a secret sharing scheme with one or more secrets. Let $\mathcal{P}$ be a finite set of participants, and let $\mathcal{S}$ be a finite set of secrets. Let $\mathbf{\Gamma} = (\Gamma_s)_{s\in\mathcal{S}}$ be a tuple of monotone access structures on $\mathcal{P}$. Note that Γ will continue to represent an access structure associated with a single secret. Let ρ be a probability measure on $\langle\mathcal{SP}\rangle$. Then $M = (\mathcal{P}, \mathcal{S}, \rho)$ is a *secret sharing scheme* for $\mathbf{\Gamma}$ if, for each $s \in \mathcal{S}$, the scheme $M_s = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ is a secret sharing scheme for Γ_s. For $s \in \mathcal{S}$, let $\mathcal{P}_s = \mathrm{core}(\Gamma_s)$, and note that $(\mathcal{P}_s, s, \rho_{s\mathcal{P}_s})$ is a connected secret sharing scheme for Γ_s.

Note that this model is a slight generalization of the model proposed in [6]. In the model in [6] it was further required that if $T \subseteq \mathcal{S}$ and $A \notin \Gamma_s$ for each $s \in T$, then $H(T|A) = H(T)$. Note also that in both models it follows that for $s, s' \in \mathcal{S}$, if $\Gamma_s \neq \Gamma_{s'}$, then the secrets s and s' are necessarily independent.

We call M_s a *component* scheme of M, and we remark that M_s is not necessarily connected. We say that M is *connected* if $\mathcal{P} = \bigcup_{s\in\mathcal{S}} \mathcal{P}_s$, that is, each participant is in the core of some access structure Γ_s. Further, M is *ideal* if a constant $h > 0$ exists such that $H(x) = h$ for every $x \in \mathcal{S} \cup (\bigcup_{s\in\mathcal{S}} \mathcal{P}_s)$ (or, equivalently, if each component scheme is ideal and all the components schemes have the same secret size).

Example 6. Let $\mathcal{P} = \{a, b, c\}$, $\mathcal{S} = \{s, t\}$, $\Gamma_s^- = \{abc\}$, and $\Gamma_t^- = \{ab\}$. Let $\langle\mathcal{SP}\rangle$ be the collection of 5-tuples given by the columns of the matrix $[A_1|A_2]$, where the following two matrices are A_1 and A_2, respectively:

$$\begin{array}{c}s\\t\\a\\b\\c\end{array}\left[\begin{array}{cccccccccccccccccccccccccccccccc}
0&1&2&3&3&0&1&2&2&3&0&1&1&2&3&0&1&2&3&0&0&3&2&1&3&0&1&2&2&1&0&3\\
0&1&2&3&3&0&1&2&2&3&0&1&1&2&3&0&0&1&2&3&3&0&1&2&2&3&0&1&1&2&3&0\\
0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3&0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3\\
0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{array}\right],$$

$$\begin{array}{c}s\\t\\a\\b\\c\end{array}\left[\begin{array}{cccccccccccccccccccccccccccccccc}
2&3&0&1&1&2&3&0&0&1&2&3&3&0&1&2&3&0&1&2&2&1&0&3&1&2&3&0&0&3&2&1\\
0&1&2&3&3&0&1&2&2&3&0&1&1&2&3&0&0&1&2&3&3&0&1&2&2&3&0&1&1&2&3&0\\
0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3&0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3\\
0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3\\
2&2&2&2&2&2&2&2&2&2&2&2&2&2&2&2&3&3&3&3&3&3&3&3&3&3&3&3&3&3&3&3
\end{array}\right].$$

Let ρ be the uniform probability measure on $\langle\mathcal{SP}\rangle$. It is straightforward to verify that $M = (\mathcal{P}, \mathcal{S}, \rho)$ is a connected ideal secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s, \Gamma_t)$.

We now extend the definitions of restriction and contradiction of a single secret sharing scheme to the case of a secret sharing scheme with one or more secrets. In particular, we sometimes wish to restrict or contract at a subset of $\mathcal{SP}$, not just at a subset of $\mathcal{P}$. Let $\mathbf{\Gamma} = (\Gamma_s)_{s\in\mathcal{S}}$ be a collection of access structures on a participant set $\mathcal{P}$, and let $A \subseteq \mathcal{SP}$. Let $\mathcal{R} = \mathcal{S}\backslash A$. The *restriction* $\mathbf{\Gamma}|A$ of $\mathbf{\Gamma}$ at A is the access structure $\mathbf{\Gamma}|A = (\Gamma_s|(A \cap \mathcal{P}))_{s\in\mathcal{R}}$ defined on $\mathcal{P}\backslash A$. The *contraction* $\mathbf{\Gamma} \cdot A$ of $\mathbf{\Gamma}$ at A is the access structure $\mathbf{\Gamma} \cdot A = (\Gamma_s \cdot (A \cap \mathcal{P}))_{s\in\mathcal{R}}$ defined on $\mathcal{P}\backslash A$.

Theorem 7. *Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s\in\mathcal{S}}$. Let $A \subseteq \mathcal{SP}$ and let $\mathcal{Q} = \mathcal{P}\backslash A$ and $\mathcal{R} = \mathcal{S}\backslash A$. Then there is a secret sharing scheme $M|A = (\mathcal{Q}, \mathcal{R}, \mu)$ for $\mathbf{\Gamma}|A$, with $\mu = \rho_{\mathcal{RQ}}$. Further, if M is ideal, then $M|A$ is ideal.*

Proof. Since M is a secret sharing scheme for $\mathbf{\Gamma}$, then for each $s \in \mathcal{R}$ we have $M_s = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ is a secret sharing scheme for Γ_s. By Result 4, $M_s|(A \cap \mathcal{P}) = (\mathcal{Q}, s, \mu^s)$, with $\mu^s = \rho_{s\mathcal{Q}}$, is a secret sharing scheme for $\Gamma_s|(A \cap \mathcal{P})$. Thus $M|A = (\mathcal{Q}, \mathcal{R}, \rho_{\mathcal{RQ}})$ is a secret sharing scheme for $\mathbf{\Gamma}|A$. For $x \in \mathcal{RQ}$, we have $H_{\rho_{\mathcal{RQ}}}(x) = H_\rho(x)$; so if M is ideal, then $M|A$ is ideal. □

Theorem 8. *Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s\in\mathcal{S}}$. Let $A \subseteq \mathcal{SP}$ and let $\mathcal{Q} = \mathcal{P}\backslash A$ and $\mathcal{R} = \mathcal{S}\backslash A$. Then there is a secret sharing scheme $M \cdot A = (\mathcal{Q}, \mathcal{R}, \mu)$ for $\mathbf{\Gamma} \cdot A$, where for a given $\alpha \in [A \cap \mathcal{P}]$ we have $\mu(\omega) = \rho_{\mathcal{RQ}|(A\cap\mathcal{P})}(\omega, \alpha)$, for each $\omega \in \langle\mathcal{RQ}\rangle$. Further, if M is ideal, then $M \cdot A$ is ideal.*

Proof. Since M is a secret sharing scheme for $\mathbf{\Gamma}$, then for each $s \in \mathcal{R}$, we have $M_s = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ is a secret sharing scheme for Γ_s. Let $\alpha \in [A \cap \mathcal{P}]$. By Result 5, $M_s \cdot (A \cap \mathcal{P}) = (\mathcal{Q}, s, \mu^s)$ is a secret sharing scheme for $\Gamma_s \cdot (A \cap \mathcal{P})$, where $\mu^s(\omega) = \rho_{s\mathcal{Q}|(A\cap\mathcal{P})}(\omega, \alpha)$, for $\omega \in \langle s\mathcal{Q}\rangle$. Thus $M \cdot A = (\mathcal{Q}, \mathcal{R}, \mu)$ is a secret sharing scheme for $\mathbf{\Gamma} \cdot A$, with $\mu(\omega) = \rho_{\mathcal{RQ}|(A\cap\mathcal{P})}(\omega, \alpha)$ for $\omega \in \langle\mathcal{RQ}\rangle$. If M is ideal, then, for $s \in \mathcal{S}$ and $x \in \operatorname{core}(\Gamma_s \cdot (A \cap \mathcal{P}))$, we have $H_\rho(x) = H_{\mu^s}(x)$, so $M \cdot A$ is ideal. □

We note that if $M = (\mathcal{P}, \mathcal{S}, \rho)$ is a secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s\in\mathcal{S}}$, then $M|X$, with $X = (\mathcal{S}\backslash s)(\mathcal{P}\backslash\mathcal{P}_s)$, is a connected secret sharing scheme for Γ_s.

4. Separators of Matroids and Probability Measures

In this section we discuss the concept of *separators*, both of matroids and of probability measures. The results shown here are later used to establish our main result. Let $T = (\mathcal{E}, \mathcal{I})$ be a matroid, and let $A \subseteq \mathcal{E}$. The set A is a *separator* of T if $\operatorname{rank} A + \operatorname{rank} \mathcal{E}\backslash A = \operatorname{rank} \mathcal{E}$. We note that A is a separator of T if and only if each circuit of T lies either in A or in $\mathcal{E}\backslash A$ (see Proposition 4.2.1 of [22]). The next two results are needed to prove Theorem 11. We write $\Gamma = \Delta_1\Delta_2$ to mean that $\Gamma = \{A_1, A_2\colon A_1 \in \Delta_1, A_2 \in \Delta_2\}$.

Result 9 [22, 3.1.11]. Let $T = (\mathcal{E}, \mathcal{I})$ be a matroid, and let $X \subseteq \mathcal{E}$. Then the circuits of $T \cdot X$ are the minimal nonempty members of the set $\{C\backslash X\colon$ where C is a circuit of $T\}$.

Result 10 [22, 1.4.11]. Let T be a matroid and let C and D be two circuits in T with $C \cap D \neq \emptyset$. Then, for any $x \in C\backslash D$ and $y \in C \cap D$, there is a circuit in $(CD)\backslash y$ containing x.

Theorem 11. *Let $T = (sAB, \mathcal{I})$ be a connected matroid, where $A, B \neq \emptyset$ and $A \cap B = \emptyset$. The following three conditions are equivalent:*

(a) *A and B are separators of $T|s$.*

(b) *For any $A_1, A_2 \subseteq A$ and $B_1,.B_2 \subseteq B$ such that sA_1B_1 and sA_2B_2 are circuits of T, then sA_1B_2 and sA_2B_1 are also circuits of T.*

(c) *If the monotone access structure Γ is associated with T, then $\Gamma = \Delta_1\Delta_2$, where Δ_1 and Δ_2 are monotone access structures on A and B, respectively.*

Proof. It is clear that conditions (b) and (c) are equivalent, so it is enough to show that (a) is equivalent to (b).

Suppose (b) holds. We show that each circuit in T not containing s is contained in either A or B, implying that A and B are separators of $T|s$. First, let the set of circuits in T through s be $C = \{sA_iB_j\colon\ A_i \subseteq A, B_j \subseteq B, 1 \le i \le a, 1 \le j \le b\}$. By 4.3.2 of [22], the circuits of T nót containing s are the minimal sets of the form

$$\begin{aligned} D_{i,j,k,l} &= sA_iB_jA_kB_l - \bigcap_{sA_cB_d \subseteq sA_iA_kB_jB_l} sA_cB_d \\ &= \left(A_iA_k - \bigcap_{A_c \subseteq A_iA_k} A_c\right) \cup \left(B_jB_l - \bigcap_{B_d \subseteq B_jB_l} B_d\right), \end{aligned} \tag{1}$$

where sA_iB_j and sA_kB_l are distinct members of C. If $B_j = B_l$, then we have

$$D_{i,j,k,j} = A_iA_k - \bigcap_{A_c \subseteq A_iA_k} A_c. \tag{2}$$

Thus if $B_j \neq B_l$, then (1) does not represent a minimal set, since $D_{i,j,k,j} \subseteq D_{i,j,k,l}$. Hence the only circuits not through s are of the form of (2) (or the equivalent for $A_i = A_k$), that is, contained in either A or B. Hence A and B are separators of $T|s$, and (a) holds.

For the converse, suppose that (a) holds. First we prove that

$$\text{if } sA_1B_1 \text{ and } sA_2B_2 \text{ are any two circuits of } T, \text{ then } \quad A_1 \not\subset A_2 \quad \text{and} \quad B_1 \not\subset B_2. \tag{3}$$

Suppose, on the contrary, that $A_1 \subset A_2$, and let $p \in A_2 \backslash A_1$. Applying Result 10 using circuits sA_2B_2 and sA_1B_1, a circuit $psA_2B_2 \subseteq B_1A_2B_2$ exists. Since A is a separator of $T|s$ and $p \in A$, it follows that $psA_2B_2 \subseteq A$ and hence $psA_2B_2 \subseteq A_2$. However, A_2 is an independent set (as it is a proper subset of the circuit sA_2B_2), so cannot contain a circuit. This contradiction proves that $A_1 \not\subset A_2$, and a similar argument shows that $B_1 \not\subset B_2$, hence (3) holds.

For $X \subseteq AB$, we have $\operatorname{rank}_T(X) = \operatorname{rank}_{T|s}(X)$. Also, since T is connected, $\operatorname{rank}_T(sAB) = \operatorname{rank}_T(AB)$ so

$$\operatorname{rank}_T(sAB) = \operatorname{rank}_T(AB) = \operatorname{rank}_T(A) + \operatorname{rank}_T(B). \tag{4}$$

Let sA_1B_1 be a circuit of T, where $A_1 \subseteq A$ and $B_1 \subseteq B$. In the contraction $T \cdot B_1$, sA_1 is a circuit (by (3) and Result 9), so $\operatorname{rank}_{T \cdot B_1}(sA_1) = \operatorname{rank}_{T \cdot B_1}(A_1)$ and hence

$$\operatorname{rank}_{T \cdot B_1}(sA) = \operatorname{rank}_{T \cdot B_1}(A). \tag{5}$$

For $X \subseteq sAB\backslash B_1$,

$$\operatorname{rank}_{T \cdot B_1}(X) = \operatorname{rank}_T(XB_1) - \operatorname{rank}_T(B_1). \tag{6}$$

Substituting $X = A$, and noting that $s \notin AB$ and A is a separator of $T|s$, we have $\mathrm{rank}_{T \cdot B_1}(A) = \mathrm{rank}_T(AB_1) - \mathrm{rank}_T(B_1) = \mathrm{rank}_{T|s}(AB_1) - \mathrm{rank}_{T|s}(B_1) = \mathrm{rank}_{T|s}(A) = \mathrm{rank}_T(A)$. Combining with (5) gives

$$\mathrm{rank}_{T \cdot B_1}(sA) = \mathrm{rank}_T(A). \tag{7}$$

Also from (6)

$$\begin{aligned} \mathrm{rank}_{T \cdot B_1}(B \backslash B_1) &= \mathrm{rank}_T(B) - \mathrm{rank}_T(B_1), & (8) \\ \mathrm{rank}_{T \cdot B_1}(sAB \backslash B_1) &= \mathrm{rank}_T(sAB) - \mathrm{rank}_T(B_1). & (9) \end{aligned}$$

So

$$\begin{aligned} &\mathrm{rank}_{T \cdot B_1}(sA) + \mathrm{rank}_{T \cdot B_1}(B \backslash B_1) \\ &\quad = \mathrm{rank}_T(A) + (\mathrm{rank}_T(B) - \mathrm{rank}_T(B_1)) \qquad \text{by (7) and (8)} \\ &\quad = \mathrm{rank}_{T \cdot B_1}(sAB \backslash B_1) \qquad \text{by (4) and (9),} \end{aligned}$$

that is, sA is a separator of $T \cdot B_1$. Now let sA_2B_2 be another circuit in T. By Result 9, $sA_2B_2 \backslash B_1$ contains a circuit in $T \cdot B_1$. As B_2 is an independent set, and as sA is a separator of $T \cdot B_1$, there is a circuit sA_2' in $T \cdot B_1$ for some $A_2' \subseteq A_2$. By Result 9, $sA_2'B_1'$ is a circuit in T for some $B_1' \subseteq B_1$. Applying (3) twice, we see that $A_2' = A_2$ and $B_1' = B_1$. Thus sA_2B_1 is a circuit in T, and, similarly, sA_1B_2 is a circuit in T. Hence (b) holds, as required. □

We now define separators of probability measures. We then show the relationship between separators of probability measures and separators of their associated matroid, and then prove some properties of separators. Let ρ be a probability measure on a finite set $\langle Z \rangle$, and let $A \subseteq B \subseteq Z$. We say that A is a *separator* of (B, ρ) if $H(A|B\backslash A) = H(A)$, which holds if and only if $H(B\backslash A|A) = H(B\backslash A)$ which is if and only if $H(B) = H(A) + H(B\backslash A)$. So A is a separator of B if and only if $B\backslash A$ is a separator of B, which is if and only if $\theta(A)$ and $\theta(B\backslash A)$ are independent random variables. Note that A is a separator of (B, ρ) if and only if A is a separator of (B, ρ_B).

Lemma 12. *Let ρ be a probability measure on a finite set $\langle Z \rangle$ for which an associated matroid $T = (Z, \mathcal{I})$ exists. Then the separators of (Z, ρ) are precisely the separators of T.*

Proof. By definition of (Z, ρ) being associated with the matroid T, there is a constant $h > 0$ with $H(A) = h \times \mathrm{rank}_T(A)$ for all $A \subseteq Z$. Let $A \subseteq Z$ and $B = Z\backslash A$. Then A is a separator of (Z, ρ) if and only if $H(Z) = H(A) + H(B)$. Dividing by h, this holds if and only if $\mathrm{rank}_T(Z) = \mathrm{rank}_T(A) + \mathrm{rank}_T(B)$, hence if and only if A is a separator of T. □

We now give some properties of separators of probability measures. Note that although what follows could be stated in terms of independent random variables (in particular, Lemma 13), we find the language of separators convenient in this context.

Lemma 13. *Let ρ be a probability measure on a finite set $\langle Z\rangle$, and let $A, B \subseteq Z$. If A and B are both separators of (Z, ρ), then so are AB and $A \cap B$. Further, suppose $A \subseteq B$. If A is a separator of (Z, ρ), then A is a separator of (B, ρ), and if B is a separator of (Z, ρ), then A is a separator of $(A(Z\backslash B), \rho)$.*

Proof. First, note that for any three disjoint subsets W, X, Y of Z we have (by Result 1)

$$\begin{aligned} H(WX) + H(WY) - H(WXY) &= H(WY) - H(Y|WX) \\ &= H(W) + H(Y|W) - H(Y|WX) \\ &\geq H(W). \end{aligned} \tag{10}$$

Now let $X = A \cap B$, $Y = Z\backslash(AB)$, $A_1 = A\backslash B$, and $B_1 = B\backslash A$, so that Z is the disjoint union of X, Y, A_1, B_1. Since $A = XA_1$ and $B = XB_1$ are separators of (Z, ρ), it follows that

$$H(A_1B_1XY) = H(A_1X) + H(B_1Y) \tag{11}$$

$$= H(B_1X) + H(A_1Y). \tag{12}$$

Thus

$$\begin{aligned} H(X) + H(Y) &\geq H(X|A_1B_1Y) + H(Y|A_1B_1X) \\ &= H(A_1B_1XY) - H(A_1B_1Y) + H(A_1B_1XY) - H(A_1B_1X) \\ &= H(A_1X) + H(B_1Y) - H(A_1B_1Y) + H(B_1X) \\ &\quad + H(A_1Y) - H(A_1B_1X) \qquad \text{by (11) and (12)} \\ &= (H(A_1X) + H(B_1X) - H(A_1B_1X)) \\ &\quad + (H(A_1Y) + H(B_1Y) - H(A_1B_1Y)) \\ &\geq H(X) + H(Y) \qquad \text{by applying (10) twice.} \end{aligned}$$

Hence equality holds throughout, and in particular $H(X|A_1B_1Y) = H(X)$ and $H(Y|A_1B_1X) = H(Y)$. Thus $X = A \cap B$ and $Y = Z\backslash(AB)$ are separators of (Z, ρ), implying that AB is also a separator of (Z, ρ).

Now suppose that $A \subseteq B$. We have $H(A) \geq H(A|B\backslash A) \geq H(A|Z\backslash A) = H(A)$, since A is a separator of (Z, ρ). Thus equality holds throughout, and, in particular, A is a separator of (B, ρ). If B is a separator of (Z, ρ), then $Z\backslash B$ is a separator of (Z, ρ), so, by the previous part of this lemma, $Z\backslash B$ is a separator of $(A(Z\backslash B), \rho)$. Hence A is a separator of $(A(Z\backslash B), \rho)$, as required. □

Lemma 14. *Let ρ be a probability measure on a finite set $\langle Z\rangle$, let $A \subseteq B \subseteq Z$ and $a \in Z$. Suppose that A is a separator of (B, ρ) and that $H(a|A) = 0$. Then for $A' \subseteq A$ we have $H(a|A'(B\backslash A)) = H(a|A')$. Further, aA is a separator of (aB, ρ).*

Proof. Let $B' = B\backslash A$. First note that since A is a separator of $(B = AB', \rho)$, then A' is a separator of $(A'B', \rho)$, by Lemma 13. Also, aA' is a separator of $(aA'B', \rho)$, as we now show, using $H(aA) = H(A)$. $H(B') = H(B'|A') \geq H(B'|aA) = H(aAB') - H(aA) \geq H(AB') - H(A) = H(A) + H(B') - H(A) = H(B')$; so equality holds throughout, implying that B', and hence also aA', is a separator of $(aA'B', \rho)$ (choosing $A' = A$ shows that aA is a separator of (aB, ρ)). Thus, $H(a|A') \geq H(a|A'B') = H(aA'B') - H(A'B') = H(aA') + H(B') - H(A') - H(B') = H(a|A')$. Equality holds throughout, hence $H(a|A'B') = H(a|A')$, as required. □

5. Construction and Classification of Ideal Secret Sharing Schemes

In this section we give a complete classification of the collections of secret sharing schemes which occur as the components of an ideal secret sharing scheme. In doing so, we show explicitly how to construct a secret sharing scheme from such a collection of components.

Lemma 15. *Let $M = (\mathcal{P}, s, \rho)$ be an ideal secret sharing scheme for Γ, let $\mathcal{P}_s =$ core(Γ) and let $A \subseteq \mathcal{P} \backslash \mathcal{P}_s$. Then $\Gamma | A = \Gamma \cdot A$ and $H(B|A) = H(B)$ for any $B \subseteq \mathcal{P}_s$.*

Proof. Let $A \subseteq \mathcal{P} \backslash \mathcal{P}_s$. For $B \subseteq \mathcal{P}_s$ we have $B \in \Gamma$ if and only if $AB \in \Gamma$. Thus $\Gamma | A = \Gamma \cdot A$.

In particular, if $\mathcal{Q} = \mathcal{P} \backslash \mathcal{P}_s$, then $\Gamma | \mathcal{Q} = \Gamma \cdot \mathcal{Q}$ ($= \Gamma'$, say). Hence $\mathcal{P}_s =$ core$(\Gamma | \mathcal{Q}) =$ core$(\Gamma \cdot \mathcal{Q})$. By Results 4 and 5 $M | \mathcal{Q} = (\mathcal{P}_s, s, \tau)$ and $M \cdot \mathcal{Q} = (\mathcal{P}_s, s, \mu)$ are ideal secret sharing schemes for Γ', where $\tau = \rho_{s\mathcal{P}_s}$ and for some fixed $\alpha \in [\mathcal{Q}]$, and any $\omega \in \langle s\mathcal{P}_s \rangle$, $\mu(\omega) = \rho_{s\mathcal{P}_s | \mathcal{Q}}(\omega, \alpha)$. As $M | \mathcal{Q}$ and $M \cdot \mathcal{Q}$ are connected ideal schemes for the same access structure Γ', they are associated with the same matroid $T = (s\mathcal{P}_s, \mathcal{I})$. Further, $H_\tau(s) = H_\mu(s)$ ($= h$, say). So for $B \subseteq \mathcal{P}_s$, $H_\tau(B) = h \times \text{rank}_T(B)$ and $H_\mu(B) = h \times \text{rank}_T(B)$. However, $H_\tau(B) = H_\rho(B)$ and $H_\mu(B) = H_\rho(B | \mathcal{Q} = \alpha)$. Hence $H_\rho(B) = H_\rho(B|\mathcal{Q})$. So B is a separator of $(B\mathcal{Q}, \rho)$ and by Lemma 13, for any $A \subseteq \mathcal{Q}$, B is a separator of (AB, ρ) and so $H_\rho(B|A) = H_\rho(B)$. □

For the remainder of this section, let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a connected, ideal secret sharing scheme for $\boldsymbol{\Gamma} = (\Gamma_s)_{s \in \mathcal{S}}$, and let $\mathcal{P}_s =$ core(Γ_s) (for $s \in \mathcal{S}$). For each $X \subseteq \mathcal{S}$, let

$$\mathcal{P}^X = \left(\bigcap_{s \in X} \mathcal{P}_s \right) \cap \left(\bigcap_{s \notin X} \mathcal{P} \backslash \mathcal{P}_s \right).$$

That is, $\mathcal{P}^X$ is the set of participants which are in $\mathcal{P}_s$ for all $s \in X$ and not in $\mathcal{P}_s$ for any $s \notin X$. We note that the nonempty sets $\mathcal{P}^X$, for $X \subseteq \mathcal{S}$, partition $\mathcal{P}$ and that the nonempty sets $\mathcal{P}^X$, for $s \in X \subseteq \mathcal{S}$, partition $\mathcal{P}_s$.

Lemma 16. *For any $X \subseteq \mathcal{S}$, $\mathcal{P}^X$ is a separator of $(\mathcal{P}, \rho)$ and of $(\mathcal{P}_s, \rho_{\mathcal{P}_s})$ for each $s \in X$.*

Proof. Let $s \in \mathcal{S}$ and let $A = \mathcal{P} \backslash \mathcal{P}_s$. By Lemma 15, $H(\mathcal{P}_s | A) = H(\mathcal{P}_s)$ so that $\mathcal{P}_s$ is a separator of $A\mathcal{P}_s = \mathcal{P}$. Thus $\mathcal{P} \backslash \mathcal{P}_s$ is also a separator of $(\mathcal{P}, \rho)$, and the result follows from Lemma 13. □

The next result gives necessary and sufficient conditions on a collection of ideal single secret sharing schemes in order that it can occur as the collection of components of an ideal secret sharing scheme with multiple secrets. These conditions are that each access structure is a product of access structures on the subsets $\mathcal{P}^X$ of participants, and that the respective probability mass functions agree on the subsets $\mathcal{P}^X$. Our theorem shows explicitly the construction of an ideal secret sharing scheme from its component schemes.

Theorem 17. *Let $h > 0$. Let $\Gamma = (\Gamma_s)_{s\in\mathcal{S}}$ be a collection of ideal access structures on a participant set $\mathcal{P}$, with set $\mathcal{S}$ of secrets. For $s \in \mathcal{S}$, let $\mathcal{P}_s = \operatorname{core}(\Gamma_s)$ and let $T_s = (s\mathcal{P}_s, \mathcal{I}_s)$ be the matroid associated with Γ_s. Suppose that $\mathcal{P} = \bigcup_{s\in\mathcal{S}} \mathcal{P}_s$. There is a connected ideal secret sharing scheme $M = (\mathcal{P}, \mathcal{S}, \rho)$ for Γ with $H(s) = h$ for $s \in \mathcal{S}$ if and only if the following conditions hold*:

(a) *For each $s \in \mathcal{S}$ and each $X \subseteq \mathcal{S}$ with $s \in X$, $\mathcal{P}^X$ is a separator of $T_s|s$ (equivalently, for each $s \in \mathcal{S}$ we have $\Gamma_s = \prod_{s\in X\subseteq\mathcal{S}} \Delta_s^X$ where each Δ_s^X is a (possibly empty) access structure on $\mathcal{P}^X$).*

(*b*) *For each $s \in \mathcal{S}$ there are secret sharing schemes $M_s = (\mathcal{P}_s, s, \rho^s)$ for Γ_s satisfying $H_{\rho^s}(s) = h$ and such that for each s, t with $s, t \in \mathcal{S}$ and each $X \subseteq \mathcal{S}$ with $s, t \in X$ we have $(\rho^s)_{\mathcal{P}^X} = (\rho^t)_{\mathcal{P}^X}$.*

Proof. Suppose there is a connected ideal secret sharing scheme $M = (\mathcal{P}, \mathcal{S}, \rho)$ for Γ with $H(s) = h$ for $s \in \mathcal{S}$. For $s \in \mathcal{S}$ let M_s be the ideal single secret sharing scheme $M_s = (\mathcal{P}_s, s, \rho^s = \rho_{s\mathcal{P}_s})$ for Γ_s, and note that M_s has associated matroid T_s. Let $s \in \mathcal{S}$. By Lemma 16, $\mathcal{P}^X$ is a separator of $(\mathcal{P}, \rho)$ and of $(\mathcal{P}_s, \rho_{\mathcal{P}_s})$. By Lemma 12, $\mathcal{P}^X$ is a separator of $T_s|s$ and the first part of (a) holds. Since $\mathcal{P}_s = \bigcup_{\{X:\, s\in X\subseteq\mathcal{S}\}} \mathcal{P}^X$, the equivalent statement follows from repeated applications of Theorem 11. Further, $H_{\rho^s}(s) = H_{\rho_{s\mathcal{P}_s}}(s) = H_\rho(s) = h$ and for each $s, t \in \mathcal{S}$ with $s \neq t$ and each $X \subseteq \mathcal{S}$ with $s, t \in X$, then $\mathcal{P}^X \subseteq \mathcal{P}_s \cap \mathcal{P}_t$ so that $(\rho^s)_{\mathcal{P}^X} = \rho_{\mathcal{P}^X} = (\rho^t)_{\mathcal{P}^X}$ and (b) holds.

Conversely, suppose (a) and (b) hold. For $X \subseteq \mathcal{S}$, let ρ^X denote $(\rho^s)_{\mathcal{P}^X}$ for any $s \in X$. Property (b) ensures that ρ^X is well defined. For $s \in \mathcal{S}$ and $X \subseteq \mathcal{S}$ with $s \in X$, $\mathcal{P}^X$ is a separator of $T_s|s$ (by (a)) and $\mathcal{P}^X$ is a separator of $(\mathcal{P}_s, \rho^s)$, by (b) and Lemma 12. By Result 1(3), this means $\rho^s_{\mathcal{P}_s}(\pi) = \prod_{\{X\subseteq\mathcal{S}:\, s\in X\}} \rho^X(\pi_{\mathcal{P}^X})$ for $\pi \in \langle\mathcal{P}_s\rangle$. For $w \in [s\mathcal{P}_s]_{\rho^s}$, since $H_{\rho^s}(s|\mathcal{P}_s) = 0$,

$$\rho^s(w) = \rho^s_{\mathcal{P}_s}(w_{\mathcal{P}_s})\rho^s_{s|\mathcal{P}_s}(w_s|w_{\mathcal{P}_s}) = \rho^s_{\mathcal{P}_s}(w_{\mathcal{P}_s}) = \prod_{\{X\subseteq\mathcal{S}:\, s\in X\}} \rho^X(w_{\mathcal{P}^X}). \tag{13}$$

Let $\langle\mathcal{SP}\rangle$ be the collection of tuples $\pi \in (\times_{s\in\mathcal{S}}[s]_{\rho^s}) \times (\times_{X\subseteq\mathcal{S}}[\mathcal{P}^X]_{\rho^X})$ such that $\pi_{s\mathcal{P}_s} \in [s\mathcal{P}_s]_{\rho^s}$ for each $s \in \mathcal{S}$. For each $\pi \in \langle\mathcal{SP}\rangle$, let

$$\rho(\pi) = \prod_{X\subseteq\mathcal{S}} \rho^X(\pi_{\mathcal{P}^X}) \tag{14}$$

(so $\langle\mathcal{SP}\rangle = [\mathcal{SP}]_\rho$). We now show that $M = (\mathcal{P}, \mathcal{S}, \rho)$ is an ideal secret sharing scheme for Γ (which is necessarily connected, by hypothesis). We first show that ρ is a probability measure. We have

$$\sum_{\pi\in\langle\mathcal{SP}\rangle}\rho(\pi) = \sum_{\pi\in\langle\mathcal{SP}\rangle}\prod_{X\subseteq\mathcal{S}}\rho^X(\pi_{\mathcal{P}^X}) \qquad \text{by (14)}$$
$$= \prod_{X\subseteq\mathcal{S}}\sum_{\pi'\in[\mathcal{P}]_{\rho^X}}\rho^X(\pi') = 1.$$

Thus ρ is a probability measure on $\langle\mathcal{SP}\rangle$. By (14) and Result 1(3), for any $X \subseteq \mathcal{S}$, $\mathcal{P}^X$ is a separator of $(\mathcal{P}, \rho)$, hence

$$H(\mathcal{P}^X|\mathcal{P}\backslash\mathcal{P}^X) = H(\mathcal{P}^X). \tag{15}$$

We now show that $M_s' = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ is a secret sharing scheme for Γ_s. Since we already know that $M_s = (\mathcal{P}_s, s, \rho^s)$ is a secret sharing scheme for Γ_s, it is enough to show that the following two conditions are satisfied:

$$M_s = M_s'|(\mathcal{P}\backslash\mathcal{P}_s), \qquad \text{that is,} \quad \rho_{s\mathcal{P}_s} = \rho^s, \tag{16}$$
$$\text{for all} \quad A \subseteq \mathcal{P}_s \quad \text{and} \quad B \subseteq \mathcal{P}\backslash\mathcal{P}_s, \quad \text{we have} \quad H_\rho(s|AB) = H_\rho(s|A). \tag{17}$$

Let $w \in [s\mathcal{P}_s]_\rho$. Then

$$\rho_{s\mathcal{P}_s}(w) = \sum_{\{\pi\in[\mathcal{SP}]_\rho:\ \pi_{s\mathcal{P}_s}=w\}}\rho(\pi) = \sum_{\{\pi\in[\mathcal{SP}]_\rho:\ \pi_{s\mathcal{P}_s}=w\}}\prod_{X\subseteq\mathcal{S}}\rho^X(\pi_{\mathcal{P}^X}) \qquad \text{by (14)}$$
$$= \prod_{\{X\subseteq\mathcal{S}:\ s\in X\}}\rho^X(w_{\mathcal{P}^X}) = \rho^s(w) \qquad \text{by (13)}.$$

Hence (16) holds. We now prove (17). Let $A \subseteq \mathcal{P}_s$ and $B \subseteq \mathcal{P}\backslash\mathcal{P}_s$. As $\mathcal{P}_s = \bigcup_{\{X\subseteq\mathcal{S}:\ s\in X\}}\mathcal{P}^X$ and each $\mathcal{P}^X$ is a separator of $(\mathcal{P}, \rho)$ (by (15)), it follows by Lemma 13 that $\mathcal{P}_s$ is a separator of $(\mathcal{P}, \rho)$. Since $H_\rho(s|\mathcal{P}_s) = 0$, by definition of ρ and Lemma 14, $s\mathcal{P}_s$ is a separator of $(s\mathcal{P}, \rho)$. Again by Lemma 13, sA is a separator of $(sA(\mathcal{P}\backslash\mathcal{P}_s), \rho)$. By Lemma 14, $H_\rho(s|A) = H_\rho(s|AB)$ as required. It follows that M is an ideal secret sharing scheme for Γ. □

Example 18. We verify conditions (a) and (b) of Theorem 17 in the case of Example 6. The participant set $\mathcal{P} = \{a, b, c\}$ is partitioned by $\mathcal{P}^s = \{c\}$ and $\mathcal{P}^{st} = \{a, b\}$.

(a) $\Gamma_s = \{abc\}$ on $\mathcal{P}_s$, so $\Gamma_s = \Delta_s^s\Delta_s^{st}$ where $\Delta_s^s = \{c\}$ and $\Delta_s^{st} = \{ab\}$. Similarly, $\Gamma_t = \{ab\}$ on $\mathcal{P}_t$, so $\Gamma_t = \Delta_t^t\Delta_t^{st}$ where $\Delta_t^t = \emptyset$ and $\Delta_s^{st} = \{ab\}$.

(b) Note that $M_s = (abc, s, \rho_{sabc})$ is an ideal secret sharing scheme for Γ_s, with $H_{\rho_{sabc}}(s) = H_\rho(s)$. Similarly, $M_t = (ab, t, \rho_{tab})$ is an ideal secret sharing scheme for Γ_t, with $H_{\rho_{tab}}(t) = H_\rho(t)$. Since M is ideal, $H_\rho(s) = H_\rho(t) = h$, say. Further, $(\rho_{sabc})_{ab} = \rho_{ab} = (\rho_{tab})_{ab}$.

Example 19. Let $\mathcal{S} = \{s, t\}$ and $\mathcal{P} = \{a, b, c, d\}$. Let $\Gamma_s^- = \{ab, acd, bcd\}$ and $\Gamma_t^- = \{ab, cd\}$. So $\mathcal{P}_s = \mathcal{P}_t = \mathcal{P}$ and hence $\mathcal{P}^s = \mathcal{P}^t = \emptyset$ and $\mathcal{P}^{st} = \mathcal{P}$. We have $\Gamma_s = \Delta_s^s\Delta_s^{st}$, where $\Delta_s^s = \emptyset$ and $\Delta_s^{st} = \Gamma_s$. Also $\Gamma_t = \Delta_t^t\Delta_t^{st}$, where $\Delta_t^t = \emptyset$ and $\Delta_t^{st} = \Gamma_t$. An ideal secret sharing scheme for (Γ_s, Γ_t) is given by the set of tuples

$$\{(s, t, a, b, c, d) = (\alpha, \beta, \alpha + \beta, \alpha + 2\beta, \beta + \gamma, \gamma)|\alpha, \beta, \gamma \in GF(3)\},$$

with each tuple occurring with probability $1/27$.

6. Ideal Secret Sharing Schemes and Matroids

As mentioned in Section 2.1, the matroid associated with an ideal single secret sharing scheme has proved to be an extremely important tool in the attempt to characterize such schemes. It is natural to ask whether an ideal secret sharing scheme (with more than one secret) determines a matroid in the same way. To be precise, let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be an ideal secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s\in\mathcal{S}}$, and let $\Delta(M) = \{A \subseteq \mathcal{SP}$: there is $a \in A$ such that $H(a|A\backslash a) = 0\}$ (see Section 2.1). If $\Delta(M)$ is the collection of dependent sets of a matroid $T = (\mathcal{SP}, \mathcal{I})$, then we say that T is the *matroid associated with M.*

We first show by counterexample that, in contrast to the single secret case, not every connected ideal secret sharing scheme has an associated matroid. Motivated by this example, we investigate which sets $X \subseteq \mathcal{SP}$ are always associated with a matroid. In Theorem 20 we show that there is always an associated matroid when $X = s\mathcal{P}$ for some $s \in \mathcal{S}$. In Theorem 21 and its corollary we consider the special case where the cores of a subset of the access structures are pairwise disjoint.

We then view the matroid association from a different viewpoint. By Theorem 20 we can find a matroid on $s\mathcal{P}$ for any $s \in \mathcal{S}$, and, by the counterexample below, there is not necessarily a matroid on $st\mathcal{P}$ for two secrets s and t. If there is not a matroid on $st\mathcal{P}$, this means that there is $A \subseteq \mathcal{P}$ with either $0 < H(s|tA) < H(s)$ or $0 < H(t|sA) < H(t)$. In Theorem 24 we investigate how this affects the relationship between the access structures Γ_s and Γ_t.

The final theorem in this section remarks that if $\mathcal{SP}$ is associated with a representable matroid T, then an ideal secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s\in\mathcal{S}}$ can be easily obtained using known methods (where, for $s \in \mathcal{S}$, Γ_s is the access structure associated with $T|(\mathcal{S}\backslash s)$).

Suppose that the secret sharing scheme $M = (\mathcal{P}, \mathcal{S}, \rho)$ has associated matroid $T = (\mathcal{SP}, \mathcal{I})$. It then follows that $H(a|A) = H(a)$ or 0 for all $a \in \mathcal{SP}$, and $A \subseteq \mathcal{SP}$ (since the rank function is integer-valued, and so every $H(a|A)$ is a multiple of $H(a)$). However, for the ideal secret sharing scheme M given in Section 3, we have $0 < H(s|ct) = H(stc) - H(ct) < H(s)$ since, for example, $000 \in [stc]$ occurs with probability $1/16$ and $121, 123 \in [stc]$ each occur with probability $1/32$. Thus an ideal secret sharing scheme does not necessarily have an associated matroid defined on $\mathcal{SP}$, associated in the same way as in the single secret case.

We now investigate to what extent we can guarantee an associated matroid.

First we recall the following definition. Let $T_1 = (\mathcal{E}_1, \mathcal{I}_1)$ and $T_2 = (\mathcal{E}_2, \mathcal{I}_2)$ be matroids, satisfying $\mathcal{E}_1 \cap \mathcal{E}_2 = \emptyset$. The *direct sum* of T_1 and T_2 is the matroid $T_1 \oplus T_2 = (\mathcal{E}_1\mathcal{E}_2, \mathcal{I})$ where $\mathcal{I} = \{I_1 I_2\colon I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2\}$. Since for each $I_1 \in \mathcal{I}_1$, $I_2 \in \mathcal{I}_2$ we have $|I_1 I_2| = |I_1| + |I_2|$, it follows that $\operatorname{rank}(\mathcal{E}_1\mathcal{E}_2) = \operatorname{rank}(\mathcal{E}_1) + \operatorname{rank}(\mathcal{E}_2)$; hence $\mathcal{E}_1$ and $\mathcal{E}_2$ are separators of $T_1 \oplus T_2$. Further, $T|\mathcal{E}_1 = T_2$ and $T|\mathcal{E}_2 = T_1$. In a similar way, we can define the direct sum of a finite number of matroids, provided they are defined on disjoint sets. Conversely, given any matroid $T = (\mathcal{E}, \mathcal{I})$ with a separator A, and $B = \mathcal{E}\backslash A$ we have $T = (T|A) \oplus (T|B)$. Finally, we note that in the case of matroids $T_1 = (\mathcal{E}_1, \mathcal{I}_1)$ and $T_2 = (\mathcal{E}_2, \mathcal{I}_2)$ satisfying $\mathcal{E}_1 \cap \mathcal{E}_2 \neq \emptyset$, it is not always possible to find a matroid $T = (\mathcal{E}_1\mathcal{E}_2, \mathcal{I})$ such that $T|\mathcal{E}_1 = T_2$ and $T|\mathcal{E}_2 = T_1$.

We note the following useful observation, which is the basis of Theorems 20 and 21. Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be an ideal secret sharing scheme for $\mathbf{\Gamma}$. Suppose there are

$X \subseteq \mathcal{SP}$ and separators $X_1, \ldots, X_r$ of (X, ρ_X) which partition X. Suppose there are matroids $T_1, \ldots, T_r$ associated with $X_1, \ldots, X_r$. Then $M' = M|\mathcal{SP}\backslash X$ has an associated matroid, which is $T = T_1 \oplus \cdots \oplus T_r$, defined on the set X. We use this observation, together with Lemmas 14 and 16, to show there is a matroid associated with the union of the set of participants with the set containing any one secret.

Theorem 20. *Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a connected ideal secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s \in \mathcal{S}}$, and consider the secret sharing scheme $M|(\mathcal{S}\backslash s) = (\mathcal{P}, s, \rho_{s\mathcal{P}})$ for Γ_s. Then a matroid defined on the set $s\mathcal{P}$ and associated with $M|(\mathcal{S}\backslash s)$ exists.*

Proof. For each $s \in \mathcal{S}$ let $T_s = (s\mathcal{P}_s, \mathcal{I}_s)$ be the matroid associated with the (connected ideal) secret sharing scheme $M_s = (\mathcal{P}_s, s, \rho_{s\mathcal{P}_s})$. By Lemmas 12 and 16, for each $X \subseteq \mathcal{S}$, $\mathcal{P}^X$ is a separator of $T_s|s$. Let $X \subseteq \mathcal{S}$. For $s, t \in X$, $\mathcal{P}^X \subseteq \mathcal{P}_s \cap \mathcal{P}_t$, so $T_s|(\mathcal{SP}\backslash\mathcal{P}^X) \cong T_t|(\mathcal{SP}\backslash\mathcal{P}^X)$. Hence we can define $T_X = T_s|(\mathcal{SP}\backslash\mathcal{P}^X) = (\mathcal{P}^X, \mathcal{I}^X)$, for any $s \in X$. Since $s\mathcal{P} = (s\mathcal{P}_s) \cup (\bigcup_{\{X:\, s \notin X \subseteq \mathcal{S}\}} \mathcal{P}^X)$, the required matroid is $(\bigoplus_{X \subseteq \mathcal{S}\backslash s} T_X) \oplus T_s$. □

Now consider again Example 6. We showed that there is a matroid $T_1 = (sabc, \mathcal{I})$ with circuit set $\{abcs\}$ associated with the secret sharing scheme $M_1 = (abc, s, \rho_1)$ for Γ_s. There is a second secret sharing scheme $M_2 = (ab, t, \rho_2)$ for Γ_t with associated matroid $T_2 = (tab, \mathcal{I}_2)$ with circuit set $\{abt\}$. The example shows that the secret t and the circuit abt cannot be adjoined to the matroid T_1 to form a new matroid associated with the secret sharing scheme M whose component parts are M_1 and M_2. In the next theorem we show conditions under which the matroid associated with one of the components of a secret sharing scheme can be extended in this way to include other component schemes.

Theorem 21. *Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a connected ideal secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s \in \mathcal{S}}$. Suppose $X \subseteq \mathcal{S}$ exists such that for each $s \in X$ there is a set $X_s \subseteq \mathcal{S}$ with $s \in X_s$ and $H(s|\mathcal{P}^{X_s}) = 0$. Then there is a matroid defined on the set $X\mathcal{P}$ and associated with $M|(\mathcal{S}\backslash X) = (\mathcal{P}, X, \rho_{X\mathcal{P}})$ for $(\Gamma_s)_{s \in X}$.*

Proof. We show that $\mathcal{P}^{X_s} = \mathcal{P}_s$ for each $s \in X$. For $s \in X$, as $\mathcal{P}^{X_s}$ is a separator of $(\mathcal{P}_s, \rho_{\mathcal{P}_s})$ (Lemma 16), and $H(s|\mathcal{P}^{X_s}) = 0$, then $s\mathcal{P}^{X_s}$ is a separator of $(s\mathcal{P}_s, \rho_{s\mathcal{P}_s})$ by Lemma 14. Let $T_s = (s\mathcal{P}_s, \mathcal{I}_s)$ be the matroid associated with $M_s = (\mathcal{P}_s, s, \rho_{s\mathcal{P}_s})$ for Γ_s. By Lemma 12, $s\mathcal{P}^{X_s}$ is a separator of T_s, so each circuit sC of T_s lies in $s\mathcal{P}^{X_s}$ (Section 4); hence $\mathcal{P}_s = \mathcal{P}^{X_s}$ (Result 2(3)), as we claimed. Note that the existence of the sets X and X_s ($s \in X$) is equivalent to the existence of $X \subseteq \mathcal{S}$ with the properties: (a) $\mathcal{P}_s \cap \mathcal{P}_t = \emptyset$ for each $s, t \in X$ with $s \neq t$, and (b) for each $s \in X$ and each $u \in \mathcal{S}\backslash X$ either $\mathcal{P}_s \cap \mathcal{P}_u = \emptyset$ or $\mathcal{P}_s \subseteq \mathcal{P}_u$. This follows by the equality $\mathcal{P}_s = \mathcal{P}^{X_s}$. As $X\mathcal{P} = (\bigcup_{s \in X} s\mathcal{P}_s) \cup (\bigcup_{Y \subseteq \mathcal{S}\backslash X} \mathcal{P}^Y)$, the associated matroid is

$$\left(\bigoplus_{s \in X} T_s\right) \oplus \left(\bigoplus_{Y \subseteq \mathcal{S}\backslash X} T_Y\right),$$

where T_Y is as defined in Theorem 20. □

As a corollary, we obtain the (unsurprising) result that if an ideal secret sharing scheme has component schemes defined on pairwise disjoint sets of participants, then the secret sharing scheme has an associated matroid, which is the direct sum of the matroids associated with the component schemes.

Corollary 22. *Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a connected ideal secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s \in \mathcal{S}}$. If for each $s, t \in \mathcal{S}$, $s \neq t$, we have $\mathcal{P}_s \cap \mathcal{P}_t = \emptyset$, then there is a matroid defined on the set $\mathcal{S}\mathcal{P}$ and associated with M.*

Since not every ideal secret sharing scheme has an associated matroid, and as suggested by the idèa of direct sums of matroids, we now ask: given an ideal secret sharing scheme $M = (\mathcal{P}, \mathcal{S}, \rho)$ for $\mathbf{\Gamma}$, does a matroid $T = (\mathcal{S}\mathcal{P}, \mathcal{I})$ exist such that $T|\mathcal{S}\mathcal{P}\backslash(s\mathcal{P}_s) = T_s$ for each $s \in \mathcal{S}$? Our next example shows that such a matroid T can sometimes be found. Note that we are not asking that the matroid be associated with M, and indeed in this example it is not, as argued above.

Example 23. Recall the ideal secret sharing scheme $M = (abc, st, \rho)$ for $\mathbf{\Gamma} = (\Gamma_s, \Gamma_t)$ where $\Gamma_s^- = \{abc\}$ and $\Gamma_t^- = \{ab\}$ discussed in Example 6. Let $T_1 = (sabc, \mathcal{I}_1)$ and $T_2 = (tab, \mathcal{I}_2)$ denote the matroids associated with Γ_s and Γ_t, respectively. Let $T = (stabc, \mathcal{I})$ be the matroid with the set of circuits $\{abcs, abt, cst\}$, so that the dependent sets of T are

$$\Delta = \{abcs, abcst, abt, abct, abst, cst, acst, bcst\}$$

and each other subset of $stabc$ is independent. It is straightforward to verify that $T|t = T_1$ and $T|sc = T_2$.

As discussed at the beginning of this section we now consider the case when two secrets $s, t \in \mathcal{S}$ cannot be adjoined to $\mathcal{P}$ in such a way that there is an associated matroid on $(st\mathcal{P}, \rho_{st\mathcal{P}})$. By Theorem 20, for $a \in s\mathcal{P}$ and $A \subseteq s\mathcal{P}$ we have either $H(a|A) = H(a)$ or 0. Similarly for $t\mathcal{P}$. So if there is no matroid associated with $st\mathcal{P}$, then $A \subseteq \mathcal{P}$ with $0 < H(s|tA) < H(s)$ exists.

Theorem 24. *Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s \in \mathcal{S}}$. Suppose there is $A \subseteq \mathcal{P}$ for which $H(s|tA) < H(s)$ for some $s \neq t$, $s, t \in \mathcal{S}$. Then $A\Gamma_t \subseteq \Gamma_s$, where $A\Gamma_t = \{AB | B \in \Gamma_t\}$.*

Proof. Suppose $B \in \Gamma_t$, so that $H(t|B) = 0$. Now $H(sAB) = H(stAB) = H(s|tAB) + H(tAB) \leq H(s|tA) + H(AB) < H(s) + H(AB)$. Hence $H(s|AB) < H(s)$ so $AB \in \Gamma_s$. □

Corollary 25. *Let $M = (\mathcal{P}, \mathcal{S}, \rho)$ be a secret sharing scheme for $\mathbf{\Gamma} = (\Gamma_s)_{s \in \mathcal{S}}$. Suppose $H(s|t) < H(s)$ for some $s \neq t$, $s, t \in \mathcal{S}$. Then $\Gamma_s = \Gamma_t$.*

Proof. We apply Theorem 24 and $A = \emptyset$. So $\Gamma_t \subseteq \Gamma_s$. Now $H(t|s) = H(s|t) + H(t) - H(s) < H(t)$, so applying Theorem 24 again we obtain $\Gamma_s \subseteq \Gamma_t$. Hence $\Gamma_t = \Gamma_s$. □

Illustrating Theorem 24 with Example 6, where $A = \{c\}$, we have $0 < H(s|At) < H(s)$, and so $c\Gamma_s \subseteq \Gamma_t$. Actually, in this case $\Gamma_s^- \{abc\}$ and $\Gamma_t^- = \{ab\}$, so $c\Gamma_s = \Gamma_t$.

We now complete this section by remarking that, as in the single secret sharing case [10], if there is an appropriate representable matroid, then we can find an ideal secret sharing scheme.

Theorem 26. *Let $T = (\mathcal{SP}, \mathcal{I})$ be a representable matroid. For each $s \in \mathcal{S}$ suppose that $T|(\mathcal{S}\backslash s)$ has associated access structure Γ_s, and let $\mathcal{P}_s = \text{core}\,\Gamma_s$. If $\mathcal{P} = \bigcup_{s\in\mathcal{S}} \mathcal{P}_s$, then there is a connected ideal secret sharing scheme $M = (\mathcal{P}, \mathcal{S}, \rho)$ for $\Gamma = (\Gamma_s)_{s\in\mathcal{S}}$.*

Proof. To obtain the tuples $[\mathcal{SP}]_\rho$ with a uniform probability measure ρ is a straightforward generalization of the technique in [10]. □

7. Concluding Remark

We have classified ideal secret sharing schemes with more than one secret in terms of the ideal single secret sharing schemes that must exist for such a scheme to be formed. These schemes thus allow a group of participants to share more than one secret, while holding a share whose size is the same as that of each of the secrets. We have also shown that the link between matroids and ideal secret sharing schemes does extend to these more complex schemes, but have shown that the relationship is less straightforward in this case.

Acknowledgment

We would like to thank the anonymous referees whose meticulous appraisal of the paper resulted in many improvements.

References

[1] A. Beimel and B. Chor. Universally ideal secret sharing schemes. *Advances in Cryptology—CRYPTO '92*. Lecture Notes in Computer Science, Vol. 740, pp. 183–195. Springer-Verlag, Berlin, 1993.

[2] B. Blakley, G. R. Blakley, A. H. Chan, and J. Massey. Threshold schemes with disenrollment. *Advances in Cryptology—CRYPTO '92*. Lecture Notes in Computer Science, Vol. 740, pp. 540–548. Springer-Verlag, Berlin, 1993.

[3] R. Blom. An optimal class of symmetric key generation systems. *Advances in Cryptology—EUROCRYPT '84*. Lecture Notes in Computer Science, Vol. 209, pp. 335–338. Springer-Verlag, Berlin, 1984.

[4] C. Blundo and A. Cresti. Space requirements for broadcast encryption. Presented at *EUROCRYPT '94*, 1994.

[5] C. Blundo, A. Cresti, A. De Santis, and U. Vaccaro. Fully dynamic secret sharing schemes. *Advances in Cryptology—CRYPTO '93*. Lecture Notes in Computer Science, Vol. 773 pp. 110–125.

[6] C. Blundo, A. De Santis, G. Di Crescenzo, A. Giorgio Gaggia, and U. Vaccaro. Multi-secret sharing schemes. *Advances in Cryptology—CRYPTO '94*. Lecture Notes in Computer Science, Vol. 839, pp. 150–163. Springer-Verlag, Berlin, 1994.

[7] C. Blundo, A. De Santis, A. Herzberg, and S. Kutten, Perfectly-secure key distribution for dynamic conferences. *Advances in Cryptology—CRYPTO '92*. Lecture Notes in Computer Science, Vol. 740, pp. 471–486.

[8] C. Blundo, A. De Santis, and U. Vaccaro. Efficient sharing of many secrets. *Proc. STACS* '93. Lecture Notes in Computer Science, Vol. 665 pp. 692–703. Springer-Verlag, Berlin, 1993.

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

[10] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4:123–134, 1991.

[11] M. Franklin and M. Yung. Communication complexity of secure computation. *Proc. 24th ACM Symp. on the Theory of Computing* (*STOC*), pp. 699–710, 1992.

[12] W.-A. Jackson and K. M. Martin. Combinatorial models for perfect secret sharing schemes. *J. Combin. Math. Combin. Comput.*, to appear.

[13] W.-A. Jackson and K. M. Martin. Efficient constructions for one sharing of many secrets. PM95-003, Pure Mathematics Preprint Series, University of Adelaide.

[14] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe. Multisecret threshold schemes. *Advances in Cryptology—CRYPTO* '93. Lecture Notes in Cpmputer Science, Vol. 773, pp. 126–135. Springer-Verlag, Berlin, 1994.

[15] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe. A construction for multisecret threshold schemes. PM95-004, Pure Mathematics Preprint Series, University of Adelaide.

[16] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory*, 29:35–41, 1983.

[17] C.-S. Laih, L. Harn, J.-Y. Lee, and T. Hwang. Dynamic threshold scheme based on the definition of cross-product in an N-dimensional linear space. *Advances in Cryptology—CRYPTO* '89. Lecture Notes in Computer Science, Vol. 435, pp. 286–297. Springer-Verlag, Berlin, 1990.

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

[19] K. M. Martin. Untrustworthy participants in secret sharing schemes. *Proc. 3rd IMA Conf. on Cryptography and Coding*, pp. 255–264, 1993.

[20] T. Matsumoto and H. Imai. On the key predistribution system: a practical solution to the key distribution problem. *Advances in Cryptology—CRYPTO* '87. Lecture Notes in Computer Science, Vol. 293, pp. 185–193. Springer-Verlag, Berlin, 1988.

[21] R. J. McEliece and D. Sarwate. On sharing secrets and Reed–Solomon codes. *Comm. ACM*, 24(9):583–584, 1981.

[22] J. G. Oxley. *Matroid Theory*. Oxford University Press, Oxford, 1992.

[23] C. Schulze. Multifunctional shared secret schemes. Preprint, 1994.

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

[25] G. J. Simmons. An introduction to shared secret and/or shared control schemes and their application. In *Contemporary Cryptology*, pp. 441–497. Edited by G. J. Simmons. IEEE Press, New York, 1991.

[26] H.-M. Sun and S.-P. Shieh. On dynamic threshold schemes. *Inform. Process. Lett.*, 52:201–206, 1994.

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

[28] D. Welsh. *Codes and Cryptography*. Clarendon Press, Oxford, 1988.