Multisecret Threshold Schemes

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

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

Abstract. A threshold scheme is a system that protects a secret (key) among a group of participants in such a way that it can only be reconstructed from the joint information held by some predetermined number of these participants. In this paper we extend this problem to one where there is more than one secret that participants can reconstruct using the information that they hold. In particular we consider the situation where there is a secret s_K associated with each k-subset K of participants and s_K can be reconstructed by any group of t participants in K ($t \leq k$). We establish bounds on the minimum amount of information that participants must hold in order to ensure that up to w participants ($0 \leq w \leq n - k + t - 1$) cannot obtain any information about a secret with which they are not associated. We also discuss examples of systems that satisfy this bound.

1 Introduction

Secret sharing schemes have received much attention in the recent literature. The basic problem is to protect a *secret* by distributing information (*shares*) relating to it among a group of n *participants* in such a way that only certain pre-specified groups of participants can reconstruct the secret from their pooled shares. The collection of sets of participants that can reconstruct the secret in this way is called the *access structure.* If there is an integer t such that the access structure consists of all the subsets of participants of size at least t then the access structure is called a (t, n)*-threshold* access structure, and the corresponding scheme is called a (t, n)*-threshold scheme.* The collection of sets of participants that are desired not to obtain any information about the secret is called the *prohibited structure.* The access and prohibited structures of the scheme together form the *structure* of the scheme.

Threshold schemes were proposed and constructed in the first papers on this subject (see Blakley [2], Shamir [15]). Since then many authors have considered more general structures (see Ito et al [9] and Benaloh and Leichter [1]).

Secret sharing schemes (and in particular threshold schemes) have many potential uses in the area of information security (see Simmons [16]). In particular, such a scheme can be used to ensure the secure implementation of a cryptographic key in a multi-user network. It is a natural generalisation to extend

* This work was supported by the Australian Research Council

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 126-135, 1994.

this concept to a multi-user network in which many different keys need to be protected among different sets of participants in the network. The problem of determining the minimum amount of information that each user must hold in order to be able to reconstruct the appropriate keys (the minimum size of the user's share) becomes increasingly important as the complexity of the network increases.

We generalise the concept of a secret sharing scheme to allow a number of different secrets to be reconstructed by the participants. We then consider the special case of this generalisation in which each subset of k participants is associated with a secret which is protected by a (t,k)-threshold access structure. This paper is concerned with finding lower bounds on the size of a participant's share in this generalisation of a threshold scheme. This is also a generalisation of a problem previously considered by Blom [4], Matsumoto [13] and Blundo et al [5]. We call these schemes *multisecret threshold schemes* (or *multithreshold schemes* for short).

The paper is structured as follows. In Section 2 we give a formal definition of a multithreshold scheme. In Section 3 we prove lower bounds on the size of each share of a participant (or a group of participants) in a multithreshold scheme and in Section 4 we discuss some schemes that achieve these bounds.

2 Multithreshold Schemes

We first define a multisecret sharing scheme. Let $\mathcal{P}$ be a set of n *participants* and $\mathcal{K} = \{s_1, \ldots, s_r\}$ be a set of *secrets*. For each i $(1 \leq i \leq r)$ denote the access structure of secret s_i by Γ_i and the prohibited structure of s_i by Δ_i. Then we call $\boldsymbol{\Gamma} = (\Gamma_1, \ldots, \Gamma_r)$ the *access structure* of the multisecret sharing scheme and $\boldsymbol{\Delta} = (\Delta_1, \ldots, \Delta_r)$ the *prohibited structure* of the multisecret sharing scheme. We make the natural restriction that for each i $(1 \leq i \leq r)$ Γ_i is *monotone increasing* and Δ_i is *monotone decreasing*. In other words, for $A \in \Gamma_i$ we have that $A' \subseteq \mathcal{P}$, $A \subseteq A'$ implies $A' \in \Gamma_i$, and for $A \in \Delta_i$ we have that $A' \subseteq \mathcal{P}$, $A \supseteq A'$ implies $A' \in \Delta_i$. The *structure* of the multisecret sharing scheme is the pair $(\boldsymbol{\Gamma}, \boldsymbol{\Delta})$. If $\Delta_i = 2^{\mathcal{P}} \backslash \Gamma_i$ (for each $1 \leq i \leq r$) then we say that the structure $(\boldsymbol{\Gamma}, \boldsymbol{\Delta})$ is *complete*.

The model we now present for a perfect multisecret sharing scheme is an extension of the model for secret sharing first proposed by Brickell and Davenport [7] and used in [8, 10, 12, 17].

Let the share held by participant p $(p \in \mathcal{P})$ come from the set $\mathcal{S}_p$ and let the value of secret s $(s \in \mathcal{K})$ come from the set $\mathcal{S}_s$ of size q. We call the sets $\mathcal{S}_p$ *share spaces* and the sets $\mathcal{S}_s$ *secret spaces*. We refer to $|\mathcal{S}_p|$ as the *size* of the share held by p and refer to q as the *size* of the secrets. A *perfect multisecret sharing scheme* with structure $(\boldsymbol{\Gamma}, \boldsymbol{\Delta})$ (denoted PS$(\boldsymbol{\Gamma}, \boldsymbol{\Delta}, q)$) is a collection $\mathcal{F}$ of (publically known) distribution rules where each $f \in \mathcal{F}$ is a one to one mapping from $\mathcal{P} \cup \mathcal{K}$ to $\left(\bigcup_{p \in \mathcal{P}} \mathcal{S}_p\right) \cup \left(\bigcup_{s \in \mathcal{K}} \mathcal{S}_s\right)$ with

$$f(p) \in \mathcal{S}_p \ \ \text{(for all } p \in \mathcal{P}) \text{ and } f(s) \in \mathcal{S}_s \ \ \text{(for all } s \in \mathcal{K}),$$

and such that for each i $(1 \le i \le r)$,

1. if $A \in \Gamma_i$ and $f, g \in \mathcal{F}$ are such that $f(x) = g(x)$ (for all $x \in A$) then $f(s_i) = g(s_i)$;
2. if $A \in \Delta_i$, and $f \in \mathcal{F}$ then there exists some integer λ such that for each $k \in \mathcal{S}_{s_i}$ there are precisely λ distribution rules $g \in \mathcal{F}$ such that $f(x) = g(x)$ (for all $x \in A$) and $f(s_i) = k$.

This is best represented by a matrix M whose rows are indexed by members of $\mathcal{F}$ and whose columns are indexed by members of $\mathcal{P} \cup \mathcal{K}$. The entry in row f and column x $(x \in \mathcal{P} \cup \mathcal{K})$ is $f(x)$. We assume that each distribution rule is equiprobable and implement the scheme by choosing a rule f at random and distributing share $f(p)$ to participant p (for all $p \in \mathcal{P}$). The secrets that these shares are protecting are the values $f(s)$ (for all $s \in \mathcal{K}$) (see [7] for more details).

We assume that a set of participants will attempt to determine a secret s by looking at their collective shares and considering only the set $\mathcal{G}$ of distribution rules f under which they could have received these shares. If the set of participants is in Γ_i then every $f \in \mathcal{G}$ will have the same value at the secret s_i. Otherwise, the structure of a perfect multisecret sharing scheme ensures that each value for the secret s_i will occur equally often among the distribution rules in $\mathcal{G}$. Note that the security offered by this model is *unconditional* in the sense that it is independent of the amount of computing time and resources that are available in any attempt to obtain a secret by some unauthorised means.

We note that the term "multisecret sharing scheme" has also been used in [6] to refer to a special class of complete multisecret sharing schemes with the same access structure for each secret.

We now introduce notation which we use for the remainder of the paper. Let $1 \le t \le k \le n$ and $r = \binom{n}{k}$. Let the collection of k-subsets of $\mathcal{P}$ be denoted by $\{X_1, \ldots, X_r\}$. Let $0 \le w \le n - k + t - 1$. Then for each i, $(1 \le i \le r)$ let

$$\Gamma_i = \{A \subseteq \mathcal{P} \mid |A \cap X_i| \ge t\},$$

and

$$\Delta_i = \{A \subseteq \mathcal{P} \mid |A| \le w\} \backslash \Gamma_i \quad .$$

Let $\boldsymbol{\Gamma} = (\Gamma_1, \ldots, \Gamma_r)$ and let $\boldsymbol{\Delta} = (\Delta_1, \ldots, \Delta_r)$. Then for $q > 1$ we refer to a PS$(\boldsymbol{\Gamma}, \boldsymbol{\Delta}, q)$ as a *w-secure (t, k, n)-multithreshold scheme* with *secret size q*.

Thus a w-secure (t, k, n)-multithreshold scheme has one secret s_i for each k-subset X_i of the n participants in $\mathcal{P}$. Any set of t or more of the k participants in X_i is able to reconstruct s_i. Further, a set A of w or fewer participants in $\mathcal{P}$ is unable to obtain any information about s_i unless A contains at least t members of X_i. (If $A = \emptyset$ then this is equivalent to $|\{f \in \mathcal{F} \mid f(s_i) = k\}|$ being independent of $k \in \mathcal{S}_{s_i}$.) Note that if $0 \le w < t - 1$ then it is possible that a subset of X_i of size μ, $(w < \mu < t)$ is able to obtain some information about the value of the secret.

It follows from the definition that a w-secure (t, k, n)-multithreshold scheme is also a w'-secure (t', k, n)-multithreshold scheme for all $0 \le w' \le w$ and $t \le t' \le k$.

If $w = n-k+t-1$ then the multithreshold scheme will be complete. It makes no sense to have $w > n-k+t-1$ since any set of this size can by definition reconstruct all of the secrets in $\mathcal{K}$.

Example 1. Let $\mathcal{P} = \{a, b, c\}$, $\mathcal{S} = \{s_1, s_2, s_3\}$ and $X_1 = \{a, b\}$, $X_2 = \{a, c\}$ and $X_3 = \{b, c\}$. The matrix in below represents a (complete) 1-secure $(1, 2, 3)$-multithreshold scheme with secret size 3.

$$\begin{array}{c}
\begin{matrix} a & b & c & s_1 & s_2 & s_3 \end{matrix} \\
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 0 & 2 \\
0 & 2 & 1 & 0 & 0 & 1 \\
1 & 4 & 7 & 1 & 2 & 0 \\
1 & 5 & 6 & 1 & 2 & 2 \\
1 & 3 & 8 & 1 & 2 & 1 \\
2 & 8 & 5 & 2 & 1 & 0 \\
2 & 6 & 4 & 2 & 1 & 2 \\
2 & 7 & 3 & 2 & 1 & 1 \\
3 & 3 & 3 & 1 & 1 & 1 \\
3 & 4 & 5 & 1 & 1 & 0 \\
3 & 5 & 4 & 1 & 1 & 2 \\
4 & 7 & 1 & 2 & 0 & 1 \\
4 & 8 & 0 & 2 & 0 & 0 \\
4 & 6 & 2 & 2 & 0 & 2 \\
5 & 2 & 8 & 0 & 2 & 1 \\
5 & 0 & 7 & 0 & 2 & 0 \\
5 & 1 & 6 & 0 & 2 & 2 \\
6 & 6 & 6 & 2 & 2 & 2 \\
6 & 7 & 8 & 2 & 2 & 1 \\
6 & 8 & 7 & 2 & 2 & 0 \\
7 & 1 & 4 & 0 & 1 & 2 \\
7 & 2 & 3 & 0 & 1 & 1 \\
7 & 0 & 5 & 0 & 1 & 0 \\
8 & 5 & 2 & 1 & 0 & 2 \\
8 & 3 & 1 & 1 & 0 & 1 \\
8 & 4 & 0 & 1 & 0 & 0
\end{pmatrix} .
\end{array}$$

Fig. 1. Matrix for Example 1.

Complete (t, k, k)-multithreshold schemes are just perfect threshold schemes as first studied in [2] and [15] (see Section 4). They can be used to show the existence of complete (t, k, n)-multithreshold schemes (and thus w-secure (t, k, n)-multithreshold schemes for $0 \leq w \leq n-k+t-1$) through the following result:

Theorem 1. *Let $1 \leq t \leq k \leq n$. If there exists a complete (t,k,k)-multithreshold scheme with secret size q then there exists a complete (t,k,n)-multithreshold scheme with secret size q.*

Proof. Let r and the sets X_i be as defined earlier. For each i $(1 \leq i \leq r)$ let $\mathcal{F}_i$ be the distribution rules of a complete (t,k,k)-multithreshold scheme defined on participant set X_i with secret s_i. For each $(f_1,\dots,f_r)$ $(f_i \in \mathcal{F}_i)$, define a new rule f as follows: for each $p \in \mathcal{P}$, $f(p)$ is the $\binom{n-1}{k-1}$-tuple with entries $f_i(p)$ for each i with $p \in X_i$, and for each s_i, $f(s_i) = f_i(s_i)$. The collection of these rules f form a complete (t,k,n)-multithreshold scheme with secret size q. □

Although Theorem 1 guarantees the existence of multithreshold schemes it produces schemes with the relatively large sharc size of $q^{\binom{n-1}{k-1}}$. We address this problem in the next section.

The special case of w-secure $(1,2,n)$-multithreshold schemes was first discussed in [4] and the generalisation to $(1,k,n)$-multithreshold schemes was studied in [13] where the use of symmetric functions was considered. The special case of symmetric polynomials was analysed in [5] for w-secure $(1,k,n)$ schemes. The later paper also produced a lower bound on the size of share that each participant holds, and an example of a scheme that achieves this bound. We will generalise this bound to the case of w-secure (t,k,n)-multithreshold schemes and discuss examples of schemes that achieve this bound.

We note that the application of a w-secure (t,k,n)-multithreshold scheme with $t > 1$ to a multi-user network as mentioned in the introduction will in general be different from the scenario for $t = 1$ discussed in [4, 5, 13]. The case $t = 1$ deals with the situation where any of the k participants can at any time *non-interactively* establish a common key. If it is required that members of a k-set of participants should reach some threshold of consensus before establishing their common key, then it is necessary that $t > 1$.

3 Bounds on Share Size

In the last section we showed that it is possible to find a w-secure (t,k,n)-multithreshold scheme with $1 \leq t \leq k \leq n$ and $0 \leq w \leq n-k+t-1$. Note however, that the construction in the proof of Theorem 1 is equivalent to simply giving each participant one share from each of the $\binom{n-1}{k-1}$ complete (t,k,k)-multithreshold schemes in which the participant is involved. We would like to be able to construct multithreshold schemes in which each participant has a share which is much smaller than that which arises from the construction of Theorem 1.

We will denote by $\mathcal{M}(t,k,n,w,q)$ the minimum size of share that a participant holds in any w-secure (t,k,n)-multithreshold scheme with secret size q taken over all schemes with these parameters.

The following well known result can be found in [17].

Result 2. *Let $1 \leq t \leq k$. Then $\mathcal{M}(t,k,k,t-1,q) \geq q$.*

Since complete (t,k,k)-multithreshold schemes with participant share size q can be found for all prime powers $q \geq k$ (so $\mathcal{M}(t,k,k,t-1,q) = q$ in this case, see Section 4.4) we can combine Result 2 and Theorem 1 to obtain the following:

Corollary 3. *Suppose* $1 \leq t \leq k \leq n$ *and* $0 \leq w \leq n-k+t-1$. *Let* q *be a prime power* $(q \geq k)$. *Then* $\mathcal{M}(t,k,n,w,q) \leq q^{\binom{n-1}{k-1}}$.

We now recall a result from [5].

Result 4. *Let* $0 \leq w \leq n-1$ *and* $k \leq n$. *Then*

$$\mathcal{M}(1,k,n,w,q) \geq q^{\binom{w+k-1}{k-1}}.$$

The main result of this paper is a generalisation of Result 4 to w-secure (t,k,n)-multithreshold schemes for any t $(1 \leq t \leq k)$ and $w \geq t-1$ (see Theorem 5). For $w < t-1$ the situation is slightly different; here we obtain a bound for the share size of a *group* of $t-w$ participants (see Corollary 8).

We first discuss two operations that can be performed on a multithreshold scheme.

Let $\mathcal{F}$ be the set of distribution rules of a w-secure (t,k,n)-multithreshold scheme with secret size q. Let M be the representation of $\mathcal{F}$ as a matrix and let $X \subseteq \mathcal{P} \cup \mathcal{K}$. The *restriction* of M at X is the matrix that is obtained from M by deleting the columns in X. Now let $f \in \mathcal{F}$. The *contraction* of M at X with respect to f is the matrix obtained from M by selecting only the rows of M that agree with f on the columns of X and then taking the restriction of the resulting matrix at X. Note that these are extensions of the definitions of restrictions and contractions of a perfect secret sharing scheme that were given in [12].

Theorem 5. *Let* $1 \leq t \leq k$ *and* $t-1 \leq w \leq n-k+t-1$. *Then*

$$\mathcal{M}(t,k,n,w,q) \geq q^{\binom{w+k-2t+1}{k-t}}.$$

Proof. If $t = 1$ then the theorem follows from Result 4. Let $t \geq 2$ and let M be a w-secure (t,k,n)-multithreshold scheme with secret size q with a set $\mathcal{F}$ of distribution rules. Let X be a subset of $t-1$ participants and let $W_X = \{s_i \mid X \not\subseteq X_i,\ 1 \leq i \leq r\}$ (with r, X_i as described earlier). Let $f \in \mathcal{F}$. Construct the matrix M' formed from M by taking the contraction of M at X with respect to f and then taking the restriction of the resulting matrix at W_X. The rows of M' correspond to the distribution rules of a $(w-t+1)$-secure $(1,k-t+1,n-t+1)$-multithreshold scheme defined on the participants of $\mathcal{P}\backslash X$. M' also has secret size q since X lies in the prohibited structure of each secret in M. Applying Result 4 we see that

$$\mathcal{M}(t,k,n,w,q) \geq q^{\binom{(w-t+1)+(k-t+1)-1}{(k-t+1)-1}} = q^{\binom{w+k-2t+1}{k-t}},$$

as required. □

Note that putting $w = n - k + t - 1$ in Theorem 5 gives us the bound on each participant's share for the case of complete multithreshold schemes.

Corollary 6. *Let M be a complete (t, k, n)-multithreshold scheme with secret size q. Then each participant must have a share of size at least $q^{\binom{n-t}{k-t}}$.*

We finish this section by considering the remaining case of w-secure (t, k, n)-multithreshold schemes with $w \leq t - 1$. As mentioned earlier, in this case we do not get a bound on an *individual* participant's share; instead we get a bound for a group of $t - w$ participants.

Let $\mathcal{F}$ be a set of distribution rules for a multisecret sharing scheme defined on participant set $\mathcal{P}$ and let $X = \{x_1, \ldots, x_u\} \subseteq \mathcal{P} \cup \mathcal{K}$. Let $\mathcal{S}_X = \{(f(x_1), \ldots, f(x_u)) \mid f \in \mathcal{F}\}$ and let $\sharp(x_1 \ldots x_u) = |\mathcal{S}_X|$.

Result 7 [6]. *Let $1 \leq t \leq k$, $0 \leq w \leq t-1$ and let M be a matrix for a w-secure (t, k, k)-multithreshold scheme with secret s of size q and participant set $\mathcal{P}$. Let $X \subseteq \mathcal{P}$ such that $|X| = t - w$. Then $\prod_{p \in X} |\mathcal{S}_p| \geq q$.*

Corollary 8. *Let $1 \leq t \leq k \leq n$ and $0 \leq w \leq t - 1$. Let M be a matrix for a w-secure (t, k, n)-multithreshold scheme with secret size q and participant set $\mathcal{P}$. Let $X \subseteq \mathcal{P}$ such that $|X| = t - w$. Then $\prod_{p \in X} |\mathcal{S}_p| \geq q$.*

Proof. Let $X \subseteq \mathcal{P}$ with $|X| = t - w$. Let X_i be such that $X \subseteq X_i$. The restriction of M at $(\mathcal{P} \backslash X_i) \cup (\mathcal{K} \backslash s_i)$ is a w-secure (t, k, k) multithreshold scheme and the corollary now follows from Result 7. □

Note that when $w = t - 1$, Theorem 5 and Corollary 8 both give the same lower bound q for the participant share size.

4 Optimal Multithreshold Scheme Constructions

In this section we discuss some constructions for multithreshold schemes. Let $1 \leq t \leq k \leq n$ and let $0 \leq w \leq n - k + t - 1$. We will call a w-secure (t, k, n)-multithreshold scheme with secret size q *optimal* if one of the following holds:

1. The size of each participant's share meets the bound for $\mathcal{M}(t, k, n, w, q)$ given in Theorem 5 (for $t - 1 \leq w \leq n - k + t - 1$);
2. The share size of each set of $t - w$ participants meets the bound given in Corollary 8 (for $0 \leq w < t - 1$).

4.1 Case $t = 1$

Optimal w-secure $(1, k, n)$-multithreshold schemes with secret size q were constructed in [5] using symmetric polynomials ($0 \leq w \leq n - k$). Such a scheme can be found for each prime power q ($q \geq n$). In fact, Example 1 was constructed using this method.

4.2 Case $t = 2$

We have the following result for the case $t = 2$:

Theorem 9 [11]. *Let $2 \leq k \leq n$ and q be a prime power such that $q > \binom{n-1}{k-2}+1$. Then there exists an optimal complete $(2, k, n)$-multithreshold scheme with secret size q.*

4.3 Case $t = k$

From Theorem 5 it follows that in any optimal w-secure (k, k, n)-multithreshold scheme with secret size q each participant holds a share of size q. Since the share size is independent of w it is of greatest interest to construct optimal complete (k, k, n)-multithreshold schemes. This can be done as follows:

Theorem 10. *Let $1 \leq k \leq n$ and $q \geq k$. Then there exists an optimal complete (k, k, n)-multithreshold scheme with secret size q.*

Proof. To construct an optimal complete (k, k, n)-multithreshold scheme with secret size q $(q \geq k)$ proceed as follows. Let $\mathcal{P} = \{p_1, \ldots, p_n\}$. Let the q^n distribution rules $\mathcal{F}$ of the scheme be such that the set $\mathcal{F}(\mathcal{P}) = \{(f(p_1), \ldots, f(p_n)) \mid f \in \mathcal{F}\}$ is equal to the set $\{(x_1, \ldots, x_n) \mid x_i \in Z_q\}$. Label the k-subsets of $\mathcal{P}$ by X_i $(1 \leq i \leq \binom{n}{k})$ and let X_i be associated with secret s_i $(1 \leq i \leq \binom{n}{k})$. Then for any $f \in \mathcal{F}$ and i $(1 \leq i \leq \binom{n}{k})$ let $f(s_i) = \sum_{p \in X_i} f(p) \pmod{q}$. The rules in $\mathcal{F}$ form an optimal complete (k, k, n)-multithreshold scheme with secret size q. □

4.4 Case $k = n$

Optimal complete (t, k, k)-multithreshold schemes with secret size q have been studied extensively in the literature (originally in [2, 15]). In such a scheme there is only one secret and every participant receives a share of size q. These schemes are normally referred to as *ideal* (t, k)-threshold schemes (see [7] or [10]). In [10] they were shown to be equivalent to a certain class of transversal designs. It is known that ideal (t, k)-threshold schemes with secret size q can be constructed for all prime powers $q \geq k$ (see for example [2, 15]). The case $w \leq t - 1$ is considered in the next subsection.

4.5 Case $w \leq t-1$

Optimal w-secure (t, k, k) multithreshold schemes with $1 \leq w \leq t - 1$ have been given in [3, 14]. These schemes are examples of *linear ramp schemes.*

In an optimal w-secure (t, k, n)-multithreshold scheme with $k \leq n$ and $w \leq t - 1$, it is not inconsistent with the definition that every set X of t participants can reconstruct not just the secrets that correspond to sets Y of size k such that $X \subseteq Y$, but in fact *all* of the $\binom{n}{k}$ secrets in $\mathcal{K}$. (However, from a more practical point of view it would seem unlikely that such a property would be desirable.)

Hence, a w-secure (t, n, n)-multithreshold scheme with secret s can be thought of as a w-secure (t, k, n)-multithreshold scheme where s is the secret associated with every k-set of participants. Thus we can obtain optimal w-secure (t, k, n)-multithreshold schemes from optimal w-secure (t, n, n)-multithreshold schemes. (In fact, a reverse correspondence can also be shown.)

5 Conclusions

We have introduced the general concept of a w-secure (t, k, n)-multithreshold scheme and given a lower bound on the size of share that a participant (or a group of participants) in such a scheme must hold. We have exhibited examples of *optimal* multithreshold schemes, that is, schemes which meet this lower bound. We note that some authors (for example [5, 6]) prefer to define secret sharing schemes in information theoretic terms. We have chosen to use a combinatorial model but we remark that all the results in this paper can be translated into equivalent information theoretic statements.

The authors acknowledge their useful discussions with Peter Wild regarding some of the ideas in this paper.

References

1. J. Benaloh and J. Leichter: Generalized Secret Sharing and Monotone Functions. Advances in Cryptology – Crypto '88, Lecture Notes in Comput. Sci. **403** (1990) 27–35
2. G. R. Blakley: Safeguarding cryptographic keys. Proceedings of AFIPS 1979 National Computer Conference **48** (1979) 313–317
3. G. R. Blakley and C. Meadows: Security of Ramp Schemes. Advances in Cryptology – Crypto '84, Lecture Notes in Comput. Sci. **196** (1985) 411–431
4. R. Blom: An Optimal Class of Symmetric Key Generation Systems. Advances in Cryptology – Eurocrypt'84, Lecture Notes in Comput. Sci. **209** (1984) 335–338
5. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung: Perfectly-Secure Key Distribution for Dynamic Conferences. Presented at Crypto'92
6. C. Blundo, A. De Santis and U. Vaccaro: Efficient Sharing of Many Secrets. Proceedings of STACS '93, Lec. Notes in Comput. Sci. **665** (1993) 692–703
7. E. F. Brickell and D. M. Davenport: On the Classification of Ideal Secret Sharing Schemes. J. Cryptology **2** (1991) 123–124
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. M. Ito, A. Saito and T. Nishizeki: Secret Sharing Scheme Realizing General Access Structure. Proceedings IEEE Global Telecom. Conf., Globecom '87, IEEE Comm. Soc. Press (1987) 99–102
10. W.-A. Jackson and K. M. Martin: On Ideal Secret Sharing Schemes. Preprint
11. W.-A. Jackson, K. M. Martin and C. M. O'Keefe: A construction for multisecret threshold schemes. Preprint

12. K. M. Martin: New Secret Sharing Schemes from Old. To appear in J. Combin. Math. Combin. Comput.
13. T. Matsumoto and H. Imai: On the KEY PREDISTRIBUTION SYSTEM: a Practical Solution to the Key Predistribution Problem. Advances in Cryptology: Crypto '87, Lecture Notes in Comput. Sci. **293** (1987) 185–193
14. R. J. McEliece and D. V. Sarwate: On Sharing Secrets and Reed Solomon Codes. Comm. ACM **24** (1981) 583–584
15. A. Shamir: How to Share a Secret. Comm. ACM Vol 22 **11** (1979) 612–613
16. G. J. Simmons: An Introduction to Shared Secret and/or Shared Control Schemes and their Application. Contemporary Cryptology: The Science of Information Integrity, IEEE Press (1992)
17. D. R. Stinson: An Explication of Secret Sharing Schemes. Des. Codes Cryptogr. **2** (1992) 357–390