Recent results on combinatorial constructions for threshold schemes

D. Chen and D. R. Stinson[1]
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2 Canada

Abstract A perfect (t, w, v; m)-threshold scheme is a type of combinatorial design that provides a way of distributing partial information (chosen from a set of v points called shadows) to w participants, so that any t of them can easily calculate one of m possible keys, but no subset of fewer than t participants can determine any partial information regarding the key. In this paper, we give a survey of recent constructions for perfect (t, w, v; m)-threshold schemes. In particular, we update results concerning perfect (3, 3, v; m)-threshold schemes.

1.1 Introduction and definitions

Informally, a *perfect threshold scheme* is a method of sharing a secret key K among w participants, in such a way that the following two properties are satisfied:

1) any t participants can determine the key K from the t shadows they collectively hold.

2) if $t' < t$, it is impossible for a subset of t' participants to obtain *any* partial information about the key.

Threshold schemes were first defined and constructed independently by Shamir [12] and Blakley [4] in 1979, and approximately 50 research papers have been published on threshold schemes since then. For a comprehensive bibliography, see Simmons [14]. Threshold schemes are also known as *secret sharing schemes*.

1 Research supported by NSERC grant A9287

We now give a formal, combinatorial definition. A *w-uniform hypergraph* is a pair $(\mathbf{X}, \mathcal{A})$, where $\mathbf{X}$ is a set of elements called *points*, and $\mathcal{A}$ is a collection of w-subsets (*blocks*) of $\mathbf{X}$. If every w-subset in $\mathcal{A}$ has multiplicity one (i.e. $\mathcal{A}$ is a set), then we say that $(\mathbf{X}, \mathcal{A})$ is *simple*.

A *(t, w, v; m)-threshold scheme* is a simple w-uniform hypergraph $(\mathbf{X}, \mathcal{A})$, where $\mathbf{X}$ is a set of v points (which we refer to as *shadows*), together with a partition of the block set $\mathcal{A}$ into m parts, say $\mathcal{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$, such that the following property is satisfied:

1) if $B \in \mathcal{A}_i$ and $C \in \mathcal{A}_j$, where $i \neq j$, then $|B \cap C| < t$ (i.e. all blocks containing any fixed subset S of t shadows occur in the same $\mathcal{A}_i$),

If the following property is also satisfied, then the threshold scheme is said to be *perfect.*

2) for any subset S of t' shadows ($t' < t$), there exists a non-negative integer $\lambda(S)$ such that for every i ($1 \leq i \leq m$) there are exactly $\lambda(S)$ blocks $B \in \mathcal{A}_i$ such that $S \subseteq B$ (i.e. there are the same number of blocks containing a subset S of t' shadows in each of the m $\mathcal{A}_i$'s).

We note that property 2) implies that every $\mathcal{A}_i$ contains the same number of blocks.

1.2 The protocol for secret sharing

The following protocol is used for secret sharing. Suppose $\mathcal{D}$ wants to "share" a secret key K ($1 \leq K \leq m$) among a group of w other people. First, a suitable perfect (t, w, v; m)-threshold scheme is made known to all the participants. $\mathcal{D}$ chooses at random a block $B \in \mathcal{A}_K$, and then $\mathcal{D}$ gives each of the w participants a different shadow in B. Suppose a subset of t participants wishes to determine the key. Let S denote the set of t shadows they collectively hold. In order to determine the key, they search through the set of blocks, finding a block B such that $S \subseteq B$. Then the key is K, where $B \in \mathcal{A}_K$.

Example 1.1 A perfect (3, 3, 9; 7)-threshold scheme. In this scheme, $\lambda(S) = 1$ for all unordered pairs of points S from the set $\{\infty, \infty', 0, 1, 2, 3, 4, 5, 6\}$.

$\mathcal{A}_0$	$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$
{∞, ∞', 0}	{∞, ∞', 1}	{∞, ∞', 2}	{∞, ∞', 3}
{0, 1, 6}	{1, 2, 0}	{2, 3, 1}	{3, 4, 2}
{0, 2, 5}	{1, 3, 6}	{2, 4, 0}	{3, 5, 1}
{0, 3, 4}	{1, 4, 5}	{2, 5, 6}	{3, 6, 0}
{1, 2, 4}	{2, 3, 5}	{3, 4, 6}	{4, 5, 0}
{3, 5, 6}	{4, 6, 0}	{5, 0, 1}	{6, 1, 2}
{∞, 1, 5}	{∞, 2, 6}	{∞, 3, 0}	{∞, 4, 1}
{∞, 2, 3}	{∞, 3, 4}	{∞, 4, 5}	{∞, 5, 6}
{∞, 4, 6}	{∞, 5, 0}	{∞, 6, 1}	{∞, 0, 2}
{∞', 3, 1}	{∞', 4, 2}	{∞', 5, 3}	{∞', 6, 4}
{∞', 6, 2}	{∞', 0, 3}	{∞', 1, 4}	{∞', 2, 5}
{∞', 5, 4}	{∞', 6, 5}	{∞', 0, 6}	{∞', 1, 0}

$\mathcal{A}_4$	$\mathcal{A}_5$	$\mathcal{A}_6$
{∞, ∞', 4}	{∞, ∞', 5}	{∞, ∞', 6}
{4, 5, 3}	{5, 6, 4}	{6, 0, 5}
{4, 6, 2}	{5, 0, 3}	{6, 1, 4}
{4, 0, 1}	{5, 1, 2}	{6, 2, 3}
{5, 6, 1}	{6, 0, 2}	{0, 1, 3}
{0, 2, 3 }	{1, 3, 4}	{2, 4, 5}
{∞, 5, 2}	{∞, 6, 3}	{∞, 0, 4}
{∞, 6, 0}	{∞, 0, 1}	{∞, 1, 2}
{∞, 1, 3}	{∞, 2, 4}	{∞, 3, 5}
{∞', 0, 5}	{∞', 1, 6}	{∞', 2, 0}
{∞', 3, 6}	{∞', 4, 0}	{∞', 5, 1}
{∞', 2, 1}	{∞', 3, 2}	{∞', 4, 3}

1.3 Security of perfect threshold schemes

We now discuss the security of threshold schemes, and show that the formal combinatorial definition satisfies the desired requirements of the informal description.

The notion of security is made rigorous in terms of probability distributions, as follows. We assume that there is a fixed probability distribution on the set of keys {1, ... , m},

which is known to all the participants. Suppose a subset of the participants have been given the t' shadows in the set $S \subseteq B$ ($t' < t$). They can then calculate a conditional probability distribution on the keys, given the shadows that they possess. If it happened that $p(K) \neq p(K \mid S)$ for some key K, then these participants would have obtained some (partial) information regarding the actual key that was sent. Property 2) guarantees that $p(K) = p(K \mid S)$, for every key K, and for every subset S of fewer than t shadows that occur in some block. This type of security is called *unconditional security* — no information can be obtained even with infinite computational resources.

Let's verify that we do indeed obtain the desired security. In what follows, K denotes a key, and S denotes a set of t' shadows. Also, $\sum_k$ denotes a sum over all possible keys k.

First, we note that if $t' < t$, then each $\mathcal{A}_K$ contains b blocks, where

$$b = \frac{\sum_{\{S:\,|S| = t'\}} \lambda(S)}{\binom{w}{t'}}.$$

Next, we compute

$$P(K \mid S) = \frac{p(K)p(S \mid K)}{p(S)} = \frac{p(K)p(S \mid K)}{\sum_k p(k)p(S \mid k)}.$$

However, for any key k, we have that

$$p(S \mid k) = \frac{\lambda(S)}{b \cdot \binom{w}{t'}}.$$

That is, $p(S \mid k)$ is independent of k. Then,

$$P(K \mid S) = \frac{\frac{\lambda(S)}{b\cdot\binom{w}{t'}}\, p(K)}{\frac{\lambda(S)}{b\cdot\binom{w}{t'}} \sum_k p(k)} = \frac{p(K)}{\sum_k p(k)} = p(K)$$

as desired.

2.1 A bound on the parameters of a perfect threshold scheme

The main question we shall address in this paper is the following: given t, w, and v, what is the maximum value m such that a perfect (t, w, v; m)-threshold scheme exists? Accordingly, we define M(t, w, v) to denote this maximum value of m, subject to the constraint that every shadow occurs in *at least one* block. (If some shadow is not used at all, then we can replace v by some smaller value.)

Note that *maximizing* m as a function of t, w and v is related to *minimizing* v as a function of t, w, and m. The motivation for minimizing v is as follows. If the number of shadows is v, then $\log_2 v$ bits of information are required to communicate a shadow. The shadows are information that must be distributed secretly over a secure channel; hence, by minimizing v, we are minimizing the amount of information to be communicated.

The following upper bound on M(t, w, v) was presented in [15].

Theorem 2.1 [15] $M(t, w, v) \leq \frac{v - t + 1}{w - t + 1}$.

In [15], a characterization of when equality can be met in the above bound was obtained. This characterization is given in terms of certain combinatorial designs (for a general reference on design theory, we mention [3]). Let $1 \leq t \leq w \leq v$. A *Steiner system* S(t, w, v) is a simple w-uniform hypergraph $(\mathbf{X}, \mathcal{A})$ on v points such that every t-subset of points occurs in a (unique) block. We say that the Steiner system is *partitionable* if we can partition the block set $\mathcal{A}$ into sets $\mathcal{A}_1, \ldots, \mathcal{A}_j$ such that each $(\mathbf{X}, \mathcal{A}_i)$ $(1 \leq i \leq j)$ is itself a Steiner system S(t – 1, w, v). It follows that j must equal $\frac{v - t + 1}{w - t + 1}$.

Theorem 2.2 [15] $M(t, w, v) = \frac{v - t + 1}{w - t + 1}$ if and only if there exists a Steiner system $S(t, w, v)$ that can be partitioned into Steiner systems $S(t - 1, w, v)$.

2.2 Optimal schemes

A perfect threshold scheme where $m = \frac{v - t + 1}{w - t + 1}$ will be termed *optimal*. Infinite classes of optimal schemes are known to exist for $(t, w) = (3, 3)$ or $(3, 4)$ as given in the following two theorems.

Theorem 2.3 [13] Suppose $v \equiv 1$ or 3 modulo 6, $v > 7$, and $v \neq 141, 283, 501, 789, 1501$, or 2365. Then $M(3, 3, v) = v - 2$.

Proof: For these values of v, Lu proved in [8] and [9] that the set of all 3-subsets of a v-set (i.e. an $S(3, 3, v)$) can be partitioned into designs $S(2, 3, v)$. ■

Remark: When $v = 7$, it is impossible to partition the set of all 3-subsets of a v-set into $S(2, 3, v)$. The existence of such a partition for the remaining six exceptions of v in Theorem 2.3 is unresolved.

Theorem 2.4 [13] For every integer $j \geq 1$, $M(3, 4, 2^{2j}) = 2^{2j-1} - 1$.

Proof: The planes of the affine geometry $AG(2j, 2)$ form an $S(3, 4, 2^{2j})$. In [1] and [18], it is shown that this $S(3, 4, 2^{2j})$) can be partitioned into Steiner systems $S(2, 4, 2^{2j})$. ■

No other examples of optimal schemes are known when $t \geq 3$. However, an optimal $(2, w, v; m)$-scheme is equivalent to a resolvable $(v, w, 1)$-BIBD (balanced incomplete block design). For example, known results concerning resolvable BIBDs imply the following.

Theorem 2.5 [13]

1) For all $v \equiv 0$ modulo 2, $M(2, 2, v) = v - 1$.

2) For all $v \equiv 3$ modulo 6, $M(2, 3, v) = \frac{v-1}{2}$.

3) For all $v \equiv 4$ modulo 12, $M(2, 4, v) = \frac{v-1}{3}$.

4) For all $v \equiv 5$ modulo 20, $v \geq 7865$, $M(2, 5, v) = \frac{v-1}{4}$.

5) For any $k \geq 3$, there exists a constant $c(k)$ such that $M(2, k, v) = \frac{v-1}{k-1}$ for all $v \equiv k$ modulo $k(k-1)$, $v > c(k)$.

6) For any prime power q, $M(2, q, q^2) = q + 1$.

Proof: A resolvable (v, 2, 1)-BIBD is obtained from a one-factorization of K_v. Resolvable (v, 3, 1)-BIBDs are shown to exist in [10]; resolvable (v, 4, 1)-BIBDs in [6]; and resolvable (v, 5, 1)-BIBDs in [19]. For any $k \geq 3$, asymptotic existence of resolvable (v, k, 1)-BIBDs was shown in [11]. The resolvable BIBDs needed in 6) are affine planes. ■

3.1 Upper bounds on the numbers M(3, 3, v)

As indicated in Theorem 2.3, the numbers M(3, 3, v) are almost all determined when $v \equiv 1$ or 3 modulo 6. In this section, we survey results on these numbers when $v \equiv 0, 2, 4$, or 5 modulo 6. First, let's note that $M(3, 3, v) = 1$ if $v \leq 5$; hence we can assume that $v \geq 6$ for the remainder of this section.

Perfect (3, 3, v; m)-threshold schemes are related to packings of pairs into triples. It will be useful to define some terminology. A *(2, 3)-packing* is a 3-uniform hypergraph $(X, \mathcal{A})$, such that every pair of points is contained in at most one block. The *leave* of the packing is the graph $\mathcal{L}$ on vertex set X, having as edges all xy such that the pair {x, y} is contained in no block of the packing.

When $v \equiv 0$ or 2 modulo 6, we have the following.

Theorem 3.1 [13] Suppose $v \equiv 0$ or 2 modulo 6. Then $M(3, 3, v) \leq v - 4$. If $M(3, 3, v) = v - 4$, then all the $\mathcal{A}_i$'s are (2, 3)-packings having the same leave $\mathcal{L}$ which must be a (fixed) one-factor of K_v.

Next, we consider the case $v \equiv 5$ modulo 6.

Theorem 3.2 [13] Let $v \equiv 5$ modulo 6. Then $M(3, 3, v) \leq v - 4$. If $M(3, 3, v) = v - 4$, then all the $\mathcal{A}_i$'s are (2, 3)-packings having the same leave $\mathcal{L}$ which is a (fixed) cycle of length 4.

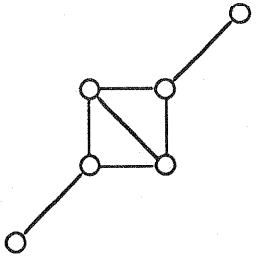
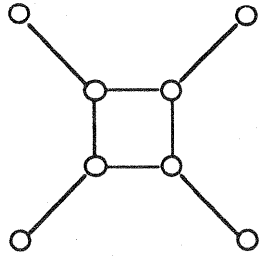
Finally, we consider the case $v \equiv 4$ modulo 6.

Theorem 3.3 [13] Let $v \equiv 4$ modulo 6. Then $M(3, 3, v) \leq v - 6$. If $M(3, 3, v) = v - 6$, then all the $\mathcal{A}_i$'s are (2, 3)-packings having the same leave $\mathcal{L}$ which must be isomorphic to one of the following four graphs:

$$K_{1,3} \cup \frac{v-4}{2} K_2 \qquad K_4 \cup \frac{v-4}{2} K_2$$

$$G_1 \cup \frac{v-6}{2} K_2 \qquad G_2 \cup \frac{v-8}{2} K_2$$

where

$G_1 =$  and $G_2 =$ 

3.2 Some new examples of perfect (3, 3, v; m)-threshold schemes meeting the upper bound

In this section, we present several new examples of schemes meeting the bounds of Section 3.1.

Example 3.1 A perfect (3, 3, 12; 8)-threshold scheme. The leave $\mathcal{L}$ is the graph having edges $\{\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}, \{9, 10\}, \{11, 12\}\}$.

$\mathcal{A}_1$				
{1,3,12}	{1,4,8}	{1,5,10}	{1,6,11}	{1,7,9}
{2,3,5}	{2,4,7,}	{2,6,10}	{2,8,11}	{2,9,12}
{3,6,7}	{3,8,10}	{3,9,11}	{4,5,11}	{4,6,9}
{4,10,12}	{5,7,12}	{5,8,9}	{6,8,12}	{7,10,11}

$\mathcal{A}_2$				
{1,3,11}	{1,4,7}	{1,6,9}	{1,5,12}	{1,8,10}
{2,3,6}	{2,4,8}	{2,5,9}	{2,7,12}	{2,10,11}
{3,5,8}	{3,7,9}	{3,10,12}	{4,6,12}	{4,5,10}
{4,9,11}	{5,7,11}	{6,8,11}	{6,7,10}	{8,9,12}

$\mathcal{A}_3$				
{1,3,10}	{1,4,12}	{1,5,9}	{1,6,7}	{1,8,11}
{2,3,9}	{2,4,6}	{2,5,11}	{2,7,10}	{2,8,12}
{3,5,12}	{3,6,8}	{3,7,11}	{4,5,7}	{4,8,9}
{4,10,11}	{5,8,10}	{6,9,11}	{6,10,12}	{7,9,12}

$\mathcal{A}_4$				
{1,3,9}	{1,4,11}	{1,5,8}	{1,6,10}	{1,7,12}
{2,3,10}	{2,4,5}	{2,6,12}	{2,7,11}	{2,8,9}
{3,5,7}	{3,6,11}	{3,8,12}	{4,6,8}	{4,7,10}
{4,9,12}	{5,9,11}	{5,10,12}	{6,7,9}	{8,10,11}

$\mathcal{A}_5$				
{1,3,8}	{1,4,9}	{1,5,7}	{1,6,12}	{1,10,11}
{2,3,12}	{2,4,11}	{2,5,10}	{2,6,8}	{2,7,9}
{3,5,11}	{3,6,9}	{3,7,10}	{4,5,8}	{4,6,10}
{4,7,12}	{5,9,12}	{6,7,11}	{8,9,11}	{8,10,12}

$\mathcal{A}_6$				
{1,3,7}	{1,4,10}	{1,5,11}	{1,6,8}	{1,9,12}
{2,3,11}	{2,4,12}	{2,5,7}	{2,6,9}	{2,8,10}
{3,5,10}	{3,6,12}	{3,8,9}	{4,5,9}	{4,6,7}
{4,8,11}	{5,8,12}	{6,10,11}	{7,9,11}	{7,10,12}

$\mathcal{A}_7$				
{1,3,6}	{1,4,5}	{1,7,11}	{1,8,9}	{1,10,12}
{2,3,8}	{2,4,10}	{2,5,12}	{2,6,7}	{2,9,11}
{3,5,9}	{3,7,12}	{3,10,11}	{4,6,11}	{4,7,9}
{4,8,12}	{5,7,10}	{5,8,11}	{6,8,10}	{6,9,12}

$\mathcal{A}_8$				
{1,3,5}	{1,4,6}	{1,7,10}	{1,8,12}	{1,9,11}
{2,3,7}	{2,4,9}	{2,5,8}	{2,6,11}	{2,10,12}
{3,6,10}	{3,8,11}	{3,9,12}	{4,5,12}	{4,7,11}
{4,8,10}	{5,7,9}	{5,10,11}	{6,7,12}	{6,8,9}

Example 3.2 A perfect (3, 3, 14; 10)-threshold scheme. We construct the scheme on points $\{A, B, C, D\} \cup (\mathbf{Z}_5 \times \mathbf{Z}_2)$. Each (2, 3)-packing has leave

$$\mathcal{L} = \{\{A, C\}, \{B, D\}\} \cup \{\{(i, 0), (i, 1)\}: i \in \mathbf{Z}_5\}.$$

The blocks corresponding to the first five keys are developed from $\mathcal{A}_0$ modulo (5, –); the blocks corresponding to the remaining five keys are developed from $\mathcal{B}_0$ modulo (5, –).

$\mathcal{A}_0$			
{A,B,(0,0)}	{A,D,(0,1)}	{C,B,(0,1)}	{C,D,(0,0)}
{A,(1,0),(3,0)}	{B,(3,0),(4,0)}	{C,(1,0),(3,1)}	{D,(3,0),(4,1)}
{A,(1,1),(3,1)}	{B,(3,1),(4,1)}	{C,(1,1),(3,0)}	{D,(3,1),(4,0)}
{A,(4,0),(2,1)}	{B,(2,0),(1,1)}	{C,(4,0),(2,0)}	{D,(2,0),(1,0)}
{A,(4,1),(2,0)}	{B,(2,1),(1,0)}	{C,(4,1),(2,1)}	{D,(2,1),(1,1)}
{(0,0),(1,0),(4,0)}	{(0,0),(1,1),4,1)}	{(0,1),(1,0),(4,1)}	{(0,1),(1,1),4,0)}
{(0,0),(2,0),(3,0)}	{(0,0),(2,1),(3,1)}	{(0,1),(2,0),(3,1)}	{(0,1),(2,1),(3,0)}

$\mathcal{B}_0$			
{A,B,(0,1)}	{A,D,(0,0)}	{C,B,(0,0)}	{C,D,(0,1)}
{A,(3,0),(4,0)}	{B,(1,0),(3,0)}	{C,(3,0),(4,1)}	{D,(1,0),(3,1)}
{A,(3,1),(4,1)}	{B,(1,1),(3,1)}	{C,(3,1),(4,0)}	{D,(1,1),(3,0)}
{A,(2,0),(1,1)}	{B,(4,0),(2,1)}	{C,(2,0),(1,0)}	{D,(4,0),(2,0)}
{A,(2,1),(1,0)}	{B,(4,1),(2,0)}	{C,(2,1),(1,1)}	{D,(4,1),(2,1)}
{(0,1),(1,1),(4,1)}	{(0,1),(1,0),4,0)}	{(0,0),(1,1),(4,0)}	{(0,0),(1,0),4,1)}
{(0,1),(2,1),(3,1)}	{(0,1),(2,0),(3,0)}	{(0,0),(2,1),(3,0)}	{(0,0),(2,0),(3,1)}

Example 3.3 A perfect (3, 3, 16; 10)-threshold scheme. Let the set of points be

$$\{A_i: 1 \le i \le 4\} \cup \{B_1, B_2\} \cup (\mathbf{Z}_5 \times \mathbf{Z}_2).$$

Each (2, 3)-packing has leave

$$\mathcal{L} = \{\{A_i, A_j\}: 1 \le i < j \le 4\} \cup \{\{B_1, B_2\}\} \cup \{\{(i, 0), (i, 1)\}: i \in \mathbf{Z}_5\}.$$

We display the first (2, 3)-packing, from which the others can be developed through $\mathbf{Z}_5 \times \mathbf{Z}_2$.

$\mathcal{A}_0$			
{A_1,B_1,(1,1)}	{A_2,B_1,(4,1)}	{A_3,B_1,(2,1)}	{A_4,B_1,(0,1)}
{A_1,B_2,(0,0)}}	{A_2,B_2,(4,0)}	{A_3,B_2,(2,0)}	{A_4,B_2,(3,0)}
{A_1,(2,0),(4,0)}	{A_2,(1,0),(3,0)}	{A_3,(1,1),(4,1)}	{A_4,(0,0),(2,0)}
{A_1,(0,1),(4,1)}	{A_2,(2,1),(3,1)}	{A_3,(3,0),(4,0)}	{A_4,(4,1),(3,1)}
{A_1,(2,1),(3,0)}	{A_2,(0,0),(1,1)}	{A_3,(0,1),(1,0)}	{A_4,(1,0),(2,1)}
{A_1,(1,0),(3,1)}	{A_2,(0,1),(2,0)}	{A_3,(0,0),(3,1)}	{A_4,(1,1),(4,0)}
{B_1,(0,0),(3,0)}	{B_2,(0,1),(3,1)}	{B_1,(1,0),(2,0)}	{B_2,(1,1),(2,1)}
{B_1,(3,1),(4,0)}	{B_2,(1,0),(4,1)}	{(0,0),(1,0),(4,0)}	{(4,0),(0,1),(2,1)}
{(2,0),(3,1),(1,1)}	{(3,0),(0,1),(1,1)}	{(0,0),(2,1),(4,1)}	{(4,1),(2,0),(3,0)}

Example 3.4 A perfect (3, 3, 16; 10)-threshold scheme. The set of points is

$$\{A_i: 1 \le i \le 6\} \cup (\mathbf{Z}_5 \times \mathbf{Z}_2).$$

Each (2, 3)-packing has leave

$$\mathcal{L} = \{\{A_1, A_2\}, \{A_2, A_3\}, \{A_2, A_4\}, \{A_3, A_4\}, \{A_3, A_5\}, \{A_4, A_5\}, \{A_5, A_6\}\} \cup \{\{(i, 0), (i, 1)\}: i \in \mathbf{Z}_5\}.$$

We display the first (2, 3)-packing, from which the others can be developed through $\mathbf{Z}_5 \times \mathbf{Z}_2$.

$\mathcal{A}_0$			
$\{A_1,A_3,(0,0)\}$	$\{A_1,A_4,(4,1)\}$	$\{A_1,A_5,(2,1)\}$	$\{A_1,A_6,(3,0)\}$
$\{A_2,A_5,(2,0)\}$	$\{A_2,A_6,(0,1)\}$	$\{A_3,A_6,(1,1)\}$	$\{A_4,A_6,(4,0)\}$
$\{A_1,(0,1),(3,1)\}$	$\{A_2,(0,0),(3,0)\}$	$\{A_3,(2,0),(4,0)\}$	$\{A_4,(1,0),(3,0)\}$
$\{A_1,(1,0),(2,0)\}$	$\{A_2,(1,1),(2,1)\}$	$\{A_3,(0,1),(4,1)\}$	$\{A_4,(2,1),(3,1)\}$
$\{A_1,(1,1),(4,0)\}$	$\{A_2,(3,1),(4,0)\}$	$\{A_3,(2,1),(3,0)\}$	$\{A_4,(0,0),(1,1)\}$
$\{A_2,(1,0),(4,1)\}$	$\{A_3,(1,0),(3,1)\}$	$\{A_4,(0,1),(2,0)\}$	$\{A_5,(1,1),(4,1)\}$
$\{A_6,(0,0),(2,0)\}$	$\{A_5,(3,0),(4,0)\}$	$\{A_6,(4,1),(3,1)\}$	$\{A_5,(1,0),(0,1)\}$
$\{A_6,(1,0),(2,1)\}$	$\{A_5,(0,0),(3,1)\}$	$\{(0,0),(1,0),(4,0)\}$	$\{(4,0),(0,1),(2,1)\}$
$\{(2,0),(3,1),(1,1)\}$	$\{(3,0),(0,1),(1,1)\}$	$\{(0,0),(2,1),(4,1)\}$	$\{(4,1),(2,0),(3,0)\}$

Example 3.5 A perfect (3, 3, 16; 10)-threshold scheme. Define the point set to be

$$\{A_i: 1 \le i \le 4\} \cup \{B_1, B_2\} \cup (\mathbf{Z}_5 \times \mathbf{Z}_2).$$

Each (2, 3)-packing has leave

$$\mathcal{L} = \{\{A_1, A_2\}, \{A_1, A_3\}, \{A_1, A_4\}\} \cup \{\{B_1, B_2\}\} \cup \{\{(i, 0), (i, 1)\}: i \in \mathbf{Z}_5\}.$$

We display the first (2, 3)-packing, from which the others can be developed through $\mathbf{Z}_5 \times \mathbf{Z}_2$.

$\mathcal{A}_0$			
$\{A_2,A_3,(2,1)\}$	$\{A_2,A_4,(1,0)\}$	$\{A_3,A_4,(1,1)\}$	$\{A_1,B_1,(2,0)\}$
$\{A_2,B_1,(3,1)\}$	$\{A_3,B_1,(4,0)\}$	$\{A_4,B_1,(4,1)\}$	$\{A_1,B_2,(2,1)\}$
$\{A_2,B_2,(3,0)\}$	$\{A_3,B_2,(0,0)\}$	$\{A_4,B_2,(0,1)\}$	$\{A_1,(0,1),(3,1)\}$
$\{A_2,(0,0),(2,0)\}$	$\{A_3,(1,0),(3,0)\}$	$\{A_4,(2,0),(4,0)\}$	$\{A_1,(3,0),(4,0)\}$
$\{A_2,(0,1),(4,1)\}$	$\{A_3,(3,1),(4,1)\}$	$\{A_4,(2,1),(3,0)\}$	$\{A_1,(0,0),(1,1)\}$
$\{A_2,(1,1),(4,0)\}$	$\{A_3,(0,1),(2,0)\}$	$\{A_4,(0,0),(3,1)\}$	$\{A_1,(1,0),(4,1)\}$
$\{B_1,(0,0),(3,0)\}$	$\{B_2,(1,1),(4,1)\}$	$\{B_1,(1,1),(2,1)\}$	$\{B_2,(1,0),(2,0)\}$
$\{B_1,(0,1),(1,0)\}$	$\{B_2,(3,1),(4,0)\}$	$\{(0,0),(1,0),(4,0)\}$	$\{(4,0),(0,1),(2,1)\}$
$\{(2,0),(3,1),(1,1)\}$	$\{(3,0),(0,1),(1,1)\}$	$\{(0,0),(2,1),(4,1)\}$	$\{(4,1),(2,0),(3,0)\}$

Examples 3.3, 3.4, and 3.5 provide perfect (3, 3, 16; 10)-threshold schemes having as leaves three of the four possibilities given in Theorem 3.3. A scheme having leave $G_2 \cup 4\ K_2$ is unknown.

Example 3.6 A perfect (3, 3, 17; 13)-threshold scheme. Let the point set be $\mathbf{Z}_{13} \cup \{A, B, C, D\}$. Each (2, 3)-packing has leave $\{\{A, B\}, \{B, C\}, \{C, D\}, \{D, A\}\}$. We give the construction of the first (2, 3)-packing, from which the others can be developed modulo 13. The first (2, 3)-packing consists of the following triples.

$\mathcal{A}_0$				
{1,3,4}	{1,2,7}	{2,12,8}	{0,1,8}	{0,2,4}
{2,5,6}	{3,9,12}	{3,6,8}	{6,10,11}	{0,3,11}
{0,6,12}	{4,12,10}	{9,1,10}	{9,5,11}	{5,4,7}
{0,9,7}	{0,5,10}	{8,7,11}	{A,1,6}	{A,4,8}
{A,3,5}	{A,12,11}	{A,9,2}	{A,10,7}	{B,2,3,}
{B,4,11}	{B,6,9}	{B,12,7}	{B,5,1}	{B,10,8}
{C,1,12}	{C,2,11}	{C,3,10}	{C,6,7}	{C,9,4}
{C,5,8}	{D,1,11}	{D,4,6}	{D,3,7}	{D,12,5}
{D,9,8}	{D,10,2}	{A,C,0}	{B,D,0}	

Example 3.7 A perfect (3, 3, 23; 19)-threshold scheme. Let the point set be $\mathbf{Z}_{19} \cup \{A, B, C, D\}$. Each (2, 3)-packing has leave $\{\{A, B\}, \{B, C\}, \{C, D\}, \{D, A\}\}$. We give the construction of the first (2, 3)-packing, from which the others can be developed modulo 19. The first (2, 3)-packing consists of the following triples.

$\mathcal{A}_0$				
{1,9,7}	{3,8,2}	{9,5,6}	{8,15,18}	{5,7,16}
{15,2,10}	{7,6,11}	{2,18,14}	{6,16,4}	{18,10,12}
{16,11,17}	{10,14,13}	{11,4,1}	{14,12,3}	{4,17,9}
{12,13,8}	{17,1,5}	{13,3,15}	{1,16,14}	{3,10,4}
{9,11,12}	{8,14,17}	{5,4,13}	{15,12,1}	{7,17,3}
{2,13,9}	{6,1,8}	{18,3,5}	{16,9,15}	{10,8,7}
{11,5,2}	{14,15,6}	{4,7,18}	{12,2,16}	{17,6,10}
{13,18,11}	{A,1,3}	{A,9,8}	{A,5,15}	{A,7,2}
{A,6,18}	{A,16,10}	{A,11,14}	{A,4,12}	{A,17,13}
{B,3,9}	{B,8,5}	{B,15,7}	{B,2,6}	{B,18,16}
{B,10,11}	{B,14,4}	{B,12,17}	{B,13,1}	{C,1,2}
{C,9,18}	{C,5,10}	{C,7,14}	{C,6,12}	{C,16,13}
{C,11,3}	{C,4,8}	{C,17,15}	{D,3,6}	{D,8,16}
{D,15,11}	{D,2,4}	{D,18,17}	{D,10,1}	{D,14,9}
{D,12,5}	{D,13,7}	{A,C,0}	{B,D,0}	

3.3 Lower bounds on the numbers M(3, 3, v)

As we have noted, the cases $v \equiv 1$ or 3 modulo 6 are essentially complete. We now discuss $v \equiv 0$ or 2 modulo 6.

Theorem 3.4 [13] Suppose $v \equiv 1$ or 3 modulo 6 and $M(3, 3, v) = v - 2$. Then $M(3, 3, 2v) = 2v - 4$.

Corollary 3.5 [13] If $v \equiv 2$ or 6 modulo 12 and $\frac{v}{2} \neq 1$, 141, 283, 501, 789, 1501, or 2365, then $M(3, 3, v) = v - 4$.

Proof: Except for $v = 14$, the result follows from Theorems 2.3 and 3.4. The case $v = 14$ was done in Example 3.2. ■

Theorem 3.6 [5] Suppose $v \equiv 1$ or 3 modulo 6 and $M(3, 3, v) = v - 2$, and suppose also that $k \equiv 1$ or 2 modulo 3 and $M(3, 3, 4k + 4) = 4k$. Then $M(3, 3, 4k(v - 2) + 4) = 4k(v - 2)$.

Note that Theorem 3.6 cannot be applied with $v = 7$, since $M(3, 3, 7) \neq 5$. However, a modification of the construction will work. We state this as follows.

Theorem 3.7 [5] Suppose that $k \equiv 1$ or 2 modulo 3 and $M(3, 3, 4k + 4) = 4k$. Then $M(3, 3, 20k + 4) = 20k$.

Corollary 3.8 [5] If $v \equiv 0$ or 8 modulo 24 and $\frac{v + 4}{4} \neq 141, 283, 501, 789, 1501$, or 2365, then $M(3, 3, v) = v - 4$.

Proof: $M(3, 3, 8) = 4$ [13, Example 4.1]. Apply Theorems 2.3, 3.6 and 3.7. ■

Corollary 3.9 [5] If $v \equiv 12$ or 44 modulo 48 and $\frac{v + 12}{8} \neq 141, 283, 501, 789, 1501$, or 2365, then $M(3, 3, v) = v - 4$.

Proof: $M(3, 3, 12) = 8$ (Example 3.1). Apply Theorems 2.3, 3.6 and 3.7. ■

Summarizing Corollaries 3.5, 3.8 and 3.9, we get the following result.

Theorem 3.10 Suppose $v \equiv 0$ or 2 modulo 6 and $v \not\equiv 20$ or 36 modulo 48. Then $M(3, 3, v) = v - 4$, with 18 possible exceptions, namely those v in the set

{282, 560, 566, 1002, 1116, 1128, 1578, 2000, 2252, 3002, 3152, 3996, 4730, 6000, 6300, 9456, 11996, 18908}.

In the cases $v \equiv 4$ or 5 modulo 6, we have presented examples where the bounds of Theorems 3.2 and 3.3 are exact, though we know of no infinite classes of threshold schemes meeting these bounds with equality. The following result allows us to get close to the upper bounds infinitely often.

Theorem 3.11 [13] For all positive integers v and w, $M(3, 3, vw) \geq w \cdot M(3, 3, v)$.

We note that Theorem 3.5 is essentially the special case of Theorem 3.11 when $w = 2$. Letting $w = 4$ and 5, we obtain in a similar fashion the following corollaries.

Corollary 3.12 Suppose $v \equiv 4$ or 12 modulo 24, $\frac{v}{4} \neq 7$, 141, 283, 501, 789, 1501, or 2365. Then $M(3, 3, v) \geq v - 8$.

Corollary 3.13 Suppose $v \equiv 5$ modulo 30, $\frac{v}{5} \neq 7$, 283, 1501, or 2365. Then $M(3, 3, v) \geq v - 10$.

Remark: We do not consider $v \equiv 15$ modulo 30 in Corollary 3.13, since $v \equiv 3$ modulo 6 in this case and hence $M(3, 3, v) = v - 2$ for almost all such v.

Note also that we can prove $M(3, 3, v) \geq v - 8$ for most $v \equiv 16$ modulo 48, and for most $v \equiv 88$ modulo 96, by applying Theorem 3.11 with $w = 2$ to the schemes constructed in Corollaries 3.8 and 3.9.

We summarize our results on $M(3, 3, v)$ in Table 1. Table 1 contains all the exact values of $M(3, 3, v)$ that we know for $v \leq 31$, and lower bounds, if an exact value is not known.

Table 1

Bounds on $M(3, 3, v)$, $v \leq 31$

v	M(3, 3, v)	authority	v	M(3, 3, v)	authority
6	2	Corollary 3.5	19	17	Theorem 2.3
7	3	[13]	20	≥ 8	Theorem 3.11
8	4	[13]	21	19	Theorem 2.3
9	7	Theorem 2.3	22	≥ 14	Theorem 3.11
10	4	[13]	23	19	Example 3.7
11	7	[13]	24	20	Theorem 3.10
12	8	Example 3.1	25	23	Theorem 2.3
13	11	Theorem 2.3	26	22	Corollary 3.5
14	10	Example 3.2	27	25	Theorem 2.3
15	13	Theorem 2.3	28	≥ 20	Theorem 3.11
16	10	Examples 3.3 – 3.5	29	???	
17	13	Example 3.6	30	26	Corollary 3.5
18	14	Corollary 3.5	31	29	Theorem 2.3

4. Lower bounds on M(t, w, v), $t \geq 4$

Shamir's construction for perfect threshold schemes [12] gives lower bounds on M(t, w, v) whenever $p = \frac{v}{w}$ is a prime and $p > w$. In this scheme, the key can be any $K \in GF(p)$ (so $m = p$). The set of shadows is the set

$$X = \{(x, y) \in GF(p) \times GF(p),\ 1 \leq x \leq w\}.$$

Hence, $v = pw$. Now, for every polynomial $h(x) \in GF(p)[x]$ having degree less than *t*, we construct a block B(h) as follows. The shadows in B(h) are $\{(u, h(u)): 1 \leq u \leq w\}$, and the key for B(h) is h(0).

It is not difficult to see that the scheme is perfect (see, for example, [15]). Hence, we obtain the following lower bound on M(t, w, v).

Theorem 4.1 Suppose $p = \frac{v}{w}$ is prime, $p > w$, and $t \leq w$. Then $M(t, w, v) \geq \frac{v}{w}$.

Remark: An obvious modification allows the construction of schemes with these parameters if *p* is a prime power.

In the remainder of this section, we present some other lower bounds on M(t, t, v), improving Theorem 4.1 under certain circumstances.

First, we quote two bounds on M(4, 4, v) proved in [13].

Theorem 4.2 [7] For all $v \equiv 8$ or 16 modulo 24, $M(4, 4, v) \geq \frac{3v}{4}$.

Theorem 4.3 [16] If $v \equiv 0$ or 6 modulo 12, then $M(4, 4, v) \geq \frac{v}{3}$.

Next we describe a construction of Teirlinck.

Theorem 4.4 [17] Suppose there exist perfect $(t_i, t_i, v_i; m)$-threshold schemes, for $1 \le i \le n$. Then there exists a perfect $(t, t, v; m)$-threshold scheme, where $t = \sum_{i=1}^{n} t_i$ and $v = \sum_{i=1}^{n} v_i$.

Proof: For $1 \le i \le n$, let $(\mathbf{X}(i), \mathcal{A}(i))$ be a perfect $(t_i, t_i, v_i; m)$-threshold scheme, where the sets $\mathbf{X}(i)$ are disjoint $(1 \le i \le n)$. For each i, we have a partition of $\mathcal{A}(i)$ into m parts, say $\mathcal{A}(i) = \{\mathcal{A}(i)_1, \ldots, \mathcal{A}(i)_m\}$. We define a threshold scheme $(\mathbf{X}, \mathcal{A})$, having $\mathbf{X} = \bigcup_{i=1}^{n} \mathbf{X}(i)$ and $\mathcal{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$, where

$$\mathcal{A}_K = \{ \bigcup_{i=1}^{n} A(i): A(i) \in \mathcal{A}(i)_{K(i)} \ (1 \le i \le n), \sum_{i=1}^{n} K(i) \equiv K \text{ modulo } m\}.$$

(So, blocks are obtained by taking the union of one block from each of the n input schemes, and the key associated with a block is the sum modulo m of the keys of the n blocks.) We leave it as a simple exercise to verify that this scheme is perfect. ■

Remark: A similar construction was used by Beneloh and Leichter in [2].

We give some applications of Theorem 4.4 in Corollary 4.5.

Corollary 4.5 [17]

1) If $M(3, 3, u) = u - 2$, then $M(3n, 3n, un) \ge u - 2$.
2) If $M(3, 3, u) = u - 2$, then $M(3n + 2, 3n + 2, un + u - 1) \ge u - 2$.
3) If $M(3, 3, u) = u - 2$, then $M(3n + 4, 3n + 4, un + 2u - 2) \ge u - 2$.

Proof: In 1), take every $t_i = 3$ and every $v_i = u$, and apply Theorem 2.5. In 2), take $t_i = 3$ and $v_i = u$ $(1 \le i \le n)$; take $t_{n+1} = 2$, $v_{n+1} = u - 1$, and apply Theorem 2.5. In 3), take $t_i = 3$ and $v_i = u$ $(1 \le i \le n)$; take $t_i = 2$, $v_i = u - 1$ $(i = n + 1, n + 2)$, and apply Theorem 2.5. ■

In Corollary 4.5, the number of keys obtained is approximately $\frac{3v}{w}$. Hence, when $t = w$, we have improved the bound of Theorem 4.1 by a factor of almost 3. More precisely, we have the following theorem, which we state without proof.

Theorem 4.6 Let $w \geq 3$, and let $\varepsilon > 0$. Then there exist infinitely many values of v such that $M(w, w, v) \geq \frac{(3 - \varepsilon)v}{w}$.

References

1. R. D. Baker, *Partitioning the planes of $AG_{2m}(2)$ into 2-designs*, Discrete Math. 15 (1976), 205-211.

2. J. Beneloh and J. Leichter, *Generalized secret sharing and monotone functions*, presented at CRYPTO '88.

3. Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Bibliographisches Institut, Zurich, 1985.

4. G. R. Blakley, *Safeguarding cryptographic keys*, Proc. N. C. C., vol. 48, AFIPS Conference Proceedings 48 (1979), 313-317.

5. D. Chen and D. R. Stinson, *On the construction of large sets of disjoint group-divisible designs*, preprint.

6. H. Hanani, D. K. Ray-Chaudhuri and R. M. Wilson, *On resolvable designs*, Discrete Math. 3 (1972), 75-97.

7. C. C. Lindner, *On the construction of pairwise disjoint Steiner quadruple systems*, Ars Combin. 19 (1985), 153-156.

8. J. X. Lu, *On large sets of disjoint Steiner triple systems I, II, and III*, J. Combin. Theory A 34 (1983), 140-146, 147-155, and 156-182.

9. J. X. Lu, *On large sets of disjoint Steiner triple systems IV, V, and VI*, J. Combin. Theory A 37 (1984), 136-163, 164-188, and 189-192.

10. D. K. Ray-Chaudhuri and R. M. Wilson, *Solution of Kirkman's schoolgirl problem*, Amer. Math. Soc. Symp. Pure Math. 19 (1971), 187-204.

11. D. K. Ray-Chaudhuri and R. M. Wilson, *The existence of resolvable block designs*, in "A Survey of Combinatorial Theory", J. N. Srivastava et al., eds., North-Holland Publishing Company, 1973, pp. 361-375.

12. A. Shamir, *How to share a secret*, Commun. of the ACM 22, (1979), 612-613.

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

14. Gustavus J. Simmons, *Robust shared secret schemes or "how to be sure you have the right answer even though you don't know the question"*, Congressus Numer. 68 (1989), 215-248.

15. D. R. Stinson and S. A. Vanstone, *A combinatorial approach to threshold schemes*, SIAM J. on Discrete Math. 1 (1988), 230-236.

16. L. Teirlinck, *On large sets of disjoint quadruple systems*, Ars Combin. 17 (1984), 173-176.

17. L. Teirlinck, private communication.

18. G. V. Zaicev, V. A. Zinoviev and N. V. Semakov, *Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double error-correcting codes*, Proc. 2nd Internat. Sympos. Information Theory, Tsahkadsor, Armenia, USSR, 1971 (Akademiai Kiado, Budapest, 1973), 257-263.

19. Zhu Lie, Du Beiliang and Zhang Xuebin, *A few more RBIBDs with $k = 5$ and $\lambda = 1$*, Discrete Math., to appear.