Threshold Schemes from Combinatorial Designs

P. J. Schellenberg and D. R. Stinson
University of Waterloo and University of Manitoba

Abstract Informally, a (t, w, v; m)-threshold scheme is a way of distributing partial information (chosen from a set of v 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 the key. A *perfect* threshold scheme is one in which no subset of fewer than t participants can determine any partial information regarding the key. In this paper, we study the number M(t, w, v), which denotes the maximum value of m such that a perfect (t, w, v; m)-threshold scheme exists. It has been shown previously that $M(t, w, v) \le (v - t + 1) / (w - t + 1)$, with equality occurring if and only if there is a Steiner system S(t, w, v) that can be partitioned into Steiner systems S(t − 1, w, v). In this paper, we study the numbers M(t, w, v) in some cases where this upper bound cannot be attained. In particular, we determine improved bounds on the values M(3, 3, v) and M(4, 4, v).

1. Introduction

A *w-uniform hypergraph* is a pair $(X, \mathcal{A})$, where X is a set of elements called *points*, and $\mathcal{A}$ is a collection of w-subsets (*blocks*) of X. We allow $\mathcal{A}$ to contain "repeated" blocks; the *multiplicity* of a block is the number of times it occurs in $\mathcal{A}$. If every subset in $\mathcal{A}$ has multiplicity one (i.e. $\mathcal{A}$ is a set), then we say that $(X, \mathcal{A})$ is *simple*.

A *perfect (t, w, v; m)-threshold scheme* is a simple w-uniform hypergraph $(X, \mathcal{A})$, where 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 $\mathcal{A} = \{\mathcal{A}_1, \dots, \mathcal{A}_m\}$, such that the following properties are satisfied:

1) if $B \in \mathcal{A}_i$ and $B' \in \mathcal{A}_j$, where $i \neq j$, then $|B \cap B'| < t$ (i.e. all blocks containing any fixed subset S of t shadows occur in the same $\mathcal{A}_i$),
2) for any subset S of $t' < t$ shadows, there exists a non-negative integer $\lambda(S)$ such that for every i ($1 \le i \le m$) there are exactly $\lambda(S)$ blocks B such that $S \subseteq B \in \mathcal{A}_i$ (i.e. there are the same number of blocks containing a subset S of $t' < t$ 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.
The application of threshold schemes is to give partial information (shadows) to w people, so that any t of them can determine a key, but no group of fewer than t can do so. For example, the key could be the combination of a safe, and we might desire that two of three specified people be required in order to determine this combination. This would correspond to a threshold scheme with t = 2 and w = 3.

Suppose there are m possible keys, namely the integers 1, 2, ... , m. Let $(X, \mathcal{A})$ be a perfect (t, w, v; m)-threshold scheme, which is made known to all w participants. Now, suppose we want to distribute shadows corresponding to key k ($1 \le k \le m$). We do this by choosing at random a block $B \in \mathcal{A}_k$. Then, we give each of the w participants a different shadow in B. Property 1) ensures that any t participants can determine the set $\mathcal{A}_k$, and hence the key (namely, k), from the t shadows they collectively hold. Property 2) ensures that it is impossible for a group of t' (< t) participants to obtain *any* partial information about the key.

These ideas are made rigourous in terms of probability distributions, as follows. We assume that there is a fixed probability distribution on the set of keys {1, ... , m}, known to all the participants. Suppose a subset of the participants have been given the shadows in the set $S \subseteq B$. They can then calculate a conditional probability distribution on the keys, given the shadows that they possess (see, for example, [24]). 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.

Threshold schemes were first described by Shamir [12] and Blakley [3] in 1979. Since then, many constructions have been given for threshold schemes. Most of these constructions have employed techniques from linear algebra. In [14], Stinson and Vanstone investigated the combinatorial properties of threshold schemes, and gave some new constructions for threshold schemes based on combinatorial designs. They presented constructions for perfect threshold schemes with t = 3 and w = 3 and 4 that handled more keys than previously known schemes did. The implementation of these schemes was also discussed. We continue this investigation in the remainder of this paper. We note that all threshold schemes discussed in this paper are perfect.

2. A combinatorial characterization of perfect threshold schemes

A characterization of perfect threshold schemes in terms of the blocks corresponding to each key was presented in [14]. Suppose $(X, \mathcal{A})$ is a w-uniform hypergraph. Given any integer $t' \le w$, define a t'-uniform hypergraph $(X, \mathcal{A}(t'))$, where $\mathcal{A}(t')$ is the multiset union $\bigcup_{A \in \mathcal{A}} \{S : |S| = t', S \subseteq A\}$. Note that $\mathcal{A}(t')$ need not be simple, even if $\mathcal{A}$ is. We say that $(X, \mathcal{A}(t'))$ is the *t'-induced* hypergraph of $(X, \mathcal{A})$.

Two w-uniform hypergraphs $(X, \mathcal{A}_1)$ and $(X, \mathcal{A}_2)$ are defined to be *t-compatible* if the following two properties are satisfied:

1) $\mathcal{A}_1(t-1) = \mathcal{A}_2(t-1)$, and
2) $\mathcal{A}_1(t) \cap \mathcal{A}_2(t) = \emptyset$.

The following result characterizes perfect (t, w, v; m)-threshold schemes in terms of t-compatible w-uniform hypergraphs.

Theorem 2.1 [14] There exists a perfect (t, w, v; m)-threshold scheme if and only if there exist m mutually t-compatible w-uniform hypergraphs on v points.

Our interest is in finding the maximum number of keys, m, that can be handled by a perfect threshold scheme, given t, w, and v. We shall also require that every shadow occurs in *at least* one block (otherwise, we can take the number of shadows to be some number less than v). This maximum number of keys is denoted M(t, w, v). In view of Theorem 2.1, M(t, w, v) also denotes the maximum number of mutually t-compatible w-uniform hypergraphs on v points (in which every point occurs in at least one block). The following upper bound on M(t, w, v) was presented in [14].

Theorem 2.2 [14] $M(t, w, v) \leq (v - t + 1) / (w - t + 1)$.

In [14], a characterization of when equality can be met in the above bound is obtained. This characterization is given in terms of certain combinatorial designs (for a general reference on design theory, we mention [2]). Let $1 \leq t \leq w < v$. 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. That is, $\mathcal{A}(t)$ consists of every t-subset of X, occurring once each. We say that the Steiner system is *partitionable* if we can partition the block set $\mathcal{A}$ into sets $\mathcal{A}_1, \ldots, \mathcal{A}_j$ (where $j = (v - t + 1) / (w - t + 1)$) such that each $(\mathbf{X}, \mathcal{A}_i)$ $(1 \leq i \leq j)$ is a Steiner system S(t − 1, w, v).

Theorem 2.3 [14] $M(t, w, v) = (v - t + 1) / (w - t + 1)$ 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).

As a consequence of this theorem, the numbers M(t, w, v) can be determined exactly in certain circumstances.

Theorem 2.4 [7, 8] 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: In [7, 8], Lu proves that the set of all 3-subsets of a v-set (where v is as stated above can be partitioned into S(2, 3, v). ■

It is worth remarking that, when v = 7, it is impossible to partition the set of all 3-subsets of a v-set into S(2, 3, v) (see, for example, [4]). The existence of such a partition for the remaining six exceptions of v in Theorem 2.4 is unresolved.

Theorem 2.5 [1, 18] For every integer $j \geq 1$, $M(3, 4, 2^{2j}) = 2^{2j-1} - 1$.

Proof: In [1] and [18], it is shown that there exists a partition of the planes of the affine geometry AG(2j, 2) (which form an $S(3, 4, 2^{2j})$) into Steiner systems $S(2, 4, 2^{2j})$. ■

Exact values of M(2, w, v) are known whenever a resolvable (v, w, 1)-BIBD exists. For example, known results concerning resolvable BIBDs imply the following.

Theorem 2.6 1) For all $v \equiv 3$ modulo 6, $M(2, 3, v) = (v - 1) / 2$.
2) For all $v \equiv 4$ modulo 12, $M(2, 4, v) = (v - 1) / 3$.
3) For all $v \equiv 5$ modulo 20, $v \geq 23105$, $M(2, 5, v) = (v - 1) / 4$.
4) For any $k \geq 3$, there exists a constant $c(k)$ such that $M(2, k, v) = (v - 1) / (k - 1)$ for all $v > c(k)$ such that $v \equiv k$ modulo $k(k - 1)$.
5) For any prime power q, $M(2, q, q^2) = q + 1$.

Proof: Resolvable (v, 3, 1)-BIBDs are shown to exist in [9]; resolvable (v, 4, 1)-BIBDs in [5]; and resolvable (v, 5, 1)-BIBDs in [19]. For any $k \geq 3$, asymptotic existence of resolvable (v, k, 1)-BIBDs was shown in [10]. The resolvable BIBDs in 5) are affine planes. ■

3. Some upper bounds on M(t, w, v)

One way to approach the construction of a perfect (t, w, v; m)-threshold scheme is to start with a fixed $(t - 1)$-uniform hypergraph on v points, say $(X, \mathcal{S})$, and attempt to find t-compatible w-uniform hypergraphs $\mathcal{A}_1, \ldots, \mathcal{A}_m$ such that $\mathcal{A}_i(t - 1) = \mathcal{S}$, $1 \leq i \leq m$ (that is, so that $(X, \mathcal{S})$ is the $(t - 1)$-induced hypergraph of $(X, \mathcal{A}_i)$, $1 \leq i \leq m$). Given t, w, v, and $\mathcal{S}$, we would want to find the maximum number of such hypergraphs (= the maximum number of keys in the resulting threshold system). We denote this number by $M(t, w, v, \mathcal{S})$. Hence,

$$M(t, w, v) = \max\{M(t, w, v, \mathcal{S}) : (X, \mathcal{S}) \text{ is a } (t - 1)\text{-uniform hypergraph on v points}\}.$$

So, we might learn more about M(t, w, v) by studying the numbers $M(t, w, v, \mathcal{S})$. The following upper bound on $M(t, w, v, \mathcal{S})$ was presented in [14].

Theorem 3.1 [14] Suppose $(X, \mathcal{S})$ is a $(t - 1)$-uniform hypergraph on v points. Let λ be the largest multiplicity of any $(t - 1)$-subset in $\mathcal{S}$. Let u denote the smallest positive integer such that

$$\binom{u}{w - t + 1} \geq \lambda.$$

Then $M(t, w, v, \mathcal{S}) \leq (v - t + 1) / u$.

Corollary 3.2 Suppose $(X, \mathcal{S})$ is a $(t - 1)$-uniform hypergraph on v points which is *not* simple. Then $M(t, w, v, \mathcal{S}) \leq (v - t + 1) / (w - t + 2)$.

Proof: In Theorem 3.1, $\lambda \geq 2$, so $u \geq w - t + 2$. ■

Corollary 3.2 suggests that we are most likely to maximize $M(t, w, v, \mathcal{S})$ when $(X, \mathcal{S})$ is simple, since the upper bound in Corollary 3.2 is already a factor of $(w - t + 1) / (w - t + 2)$ less than the upper bound of Theorem 2.2.

Let's now try to improve the bound of Theorem 3.1, when $(X, \mathcal{S})$ is a *simple* $(t - 1)$-uniform hypergraph on v points. For any induced $(t - 2)$-subset $B \in \mathcal{S}(t - 2)$, define

$$N(B) = \{x:\ B \cup \{x\} \notin \mathcal{S}\}.$$

We say that N(B) is the *neighbourhood* of B. Also, define the *deficiency* of $\mathcal{S}$ to be

$$d(\mathcal{S}) = \max\left\{ \left| \bigcup_{x \in A} N(A \setminus \{x\}) \right| :\ A \in \mathcal{S} \right\}.$$

Theorem 3.3 Suppose $(X, \mathcal{S})$ is a simple $(t-1)$-uniform hypergraph on v points. Then $M(t, w, v, \mathcal{S}) \le (v - t + 1 - d(\mathcal{S})) / (w - t + 1)$.

Proof: Suppose there exist m t-compatible w-uniform hypergraphs, $\mathcal{A}_1, \ldots, \mathcal{A}_m$, such that $\mathcal{A}_i(t-1) = \mathcal{S}$, $1 \le i \le m$. Choose $A \in \mathcal{S}$ such that $\left|\bigcup_{x \in A} N(A \setminus \{x\})\right| = d(\mathcal{S})$. Each $\mathcal{A}_i$ contains a (unique) block A_i such that $A \subseteq A_i$. Suppose $x \in A$, and $1 \le i \le m$. Then $|N(A \setminus \{x\}) \cap A_i| = 0$. Also, $|(A_i \setminus A) \cap (A_j \setminus A)| = 0$ if $i \ne j$. It follows that $m(w - t + 1) \le v - t + 1 - d(\mathcal{S})$, which gives the desired inequality. ■

4. The numbers M(3, 3, v)

As indicated in Theorem 2.4, the numbers M(3, 3, v) are almost all determined when $v \equiv 1$ or 3 modulo 6. In this section, we investigate these numbers when $v \equiv 0, 2, 4$, or 5 modulo 6. We establish upper bounds on M(3, 3, v) using the results proved in Section 3. First, let's note that $M(3, 3, v) = 1$ if $v \le 5$; hence we shall assume that $v \ge 6$ for the remainder of this section.

(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 (i.e. $\mathcal{A}(2)$ is simple). The *leave* of the packing is the graph $\mathcal{A}(2)^c$, where the superscript c denotes complement. That is, the leave consists of all pairs which do *not* occur in a block of the packing.

A (2, 3)-packing $(X, \mathcal{A})$ is said to be *maximum* if there does not exist any (2, 3)-packing on $|X|$ points with more blocks. The packing number D(2, 3, v) is defined to be the number of blocks in a maximum (2, 3)-packing on v points. The packing numbers D(2, 3, v) and the leaves of the maximum packings have been determined exactly, in [11] and [13]. We summarize these results in the following two theorems.

Theorem 4.1 [11, 13] The packing numbers D(2, 3, v) are as follows:

1) If $v \equiv 1$ or 3 modulo 6, then $D(2, 3, v) = v(v-1)/6$.
2) If $v \equiv 5$ modulo 6, then $D(2, 3, v) = (v(v-1) - 8)/6$.
3) If $v \equiv 0$ or 2 modulo 6, then $D(2, 3, v) = v(v-2)/6$.
4) If $v \equiv 4$ modulo 6, then $D(2, 3, v) = (v(v-2) - 2)/6$.

Theorem 4.2 [11, 13] Leaves of maximum (2, 3)-packings are isomorphic to the following graphs:

1) If $v \equiv 1$ or 3 modulo 6, then the leave is $(K_v)^c$.
2) If $v \equiv 5$ modulo 6, then the leave is a 4-cycle.
3) If $v \equiv 0$ or 2 modulo 6, then the leave is a one-factor.
4) If $v \equiv 4$ modulo 6, then the leave is the disjoint union of $(v - 4) / 2$ edges and one $K_{1,3}$.

In fact, the leave of *any* (2, 3)-packing must satisfy certain obvious numerical properties, which we state without proof.

Theorem 4.3 Suppose L is the leave of a (2, 3)-packing on v points. Then the following properties hold:

i) for any point x, $d_x \equiv (v - 1)$ modulo 2, where d_x denotes the degree of x in L, and
ii) $\varepsilon \equiv v(v - 1) / 2$ modulo 3, where ε denotes the number of edges in L.

Now, suppose we have 3-compatible 3-uniform hypergraphs $\mathcal{A}_1, \ldots, \mathcal{A}_m$ such that $\mathcal{A}_i(2) = \mathcal{S}$, $1 \le i \le m$. $\mathcal{S}$ is a 2-hypergraph on v points (i.e. a graph with (possibly) repeated edges, but with no isolated vertices). If $\mathcal{S}$ has a repeated edge, then $M(3, 3, v, \mathcal{S}) \le (v - 2) / 2$, by Corollary 3.2. If $\mathcal{S}$ is simple, then each $\mathcal{A}_i$ is a (2, 3)-packing with leave $\mathcal{S}^c$. Then, $M(3, 3, v, \mathcal{S}) \le v - 2 - d(\mathcal{S})$, by Theorem 3.3. A lower bound on $d(\mathcal{S})$ will give us an upper bound on $M(3, 3, v, \mathcal{S})$. Properties of leaves will then allow us to find upper bounds on $M(3, 3, v)$.

For example, when $v \equiv 0$ or 2 modulo 6, we have the following.

Lemma 4.4 If $v \equiv 0$ or 2 modulo 6, then $M(3, 3, v) \le v - 4$.

Proof: Suppose we have 3-compatible 3-uniform hypergraphs $\mathcal{A}_1, \ldots, \mathcal{A}_m$ such that $\mathcal{A}_i(2) = \mathcal{S}$, $1 \le i \le m$. As observed above, if $\mathcal{S}$ has a repeated edge, then $M(3, 3, v, \mathcal{S}) \le (v - 2) / 2$, and if $\mathcal{S}$ is simple, then $M(3, 3, v, \mathcal{S}) \le v - 2 - d(\mathcal{S})$. Since we can assume $v \ge 6$, we will be done if we can show that $d(\mathcal{S}) \ge 2$ if $\mathcal{S}$ is simple. Since v is even, each point x has odd degree in the leave, $\mathcal{S}^c$ (Theorem 4.3). It follows that we can find an edge xy of $\mathcal{S}$ such that $|N(x) \cup N(y)| \ge 2$ (note that this is *not* true if we allow $\mathcal{S}$ to contain isolated vertices). Hence, $d(\mathcal{S}) \ge 2$, as required. ■

It is also easy to characterize $\mathcal{S}$ when equality occurs in the above bound.

Lemma 4.5 If $v \equiv 0$ or 2 modulo 6 and $M(3, 3, v, \mathcal{S}) = v - 4$, then each $\mathcal{A}_i$ is a maximum packing of pairs into triples.

Proof: For every edge xy of $\mathcal{S}$, we must have that $|N(x) \cup N(y)| \le d(\mathcal{S}) = 2$. Also, for every vertex x, x has odd degree in $\mathcal{S}^c$. This can happen only when $\mathcal{S}^c$ is a one-factor of the point set. Hence, each $\mathcal{A}_i$ is a maximum packing, by Theorem 4.2. ■

Corollary 4.6 If $v \equiv 0$ or 2 modulo 6 and $M(3, 3, v, \mathcal{S}) = v - 4$, then there exists a partition of all triples which do *not* contain a pair from $\mathcal{S}^c$ into maximum packings of triples.

Proof: The number of such triples is $v(v-1)(v-2)/6 - v(v-2)/2 = v(v-2)(v-4)/6$. Each of the $v-4$ maximum packings uses $v(v-2)/6$ of these triples, which is all of them. ∎

We can construct such a set of maximum packings of triples whenever $v \equiv 2$ or 6 modulo 12, as follows.

Theorem 4.7 If $v \equiv 2$ or 6 modulo 12, $v \geq 6$, $v \neq 14, 282, 566, 1002, 1578, 3002$, or 4730, then $M(3, 3, v) = v - 4$.

Proof: Let $v = 2v'$; then $v' \equiv 1$ or 3 modulo 6. Start with a Steiner system $S(3, 3, v')$ which is partitionable into a set of $v' - 2$ Steiner systems $S(2, 3, v')$, say $\mathcal{A}_1, \ldots, \mathcal{A}_{v'-2}$, on point set $\{1, \ldots, v'\}$. From each $\mathcal{A}_i$, $1 \leq i \leq v' - 2$, construct two maximum packings, $\mathcal{A}_{i,1}$ and $\mathcal{A}_{i,2}$, on point set $\{1, \ldots, v\}$, as follows. Define

$$\mathcal{A}_{i,1} = \{\{x, y, z\}, \{x, y+v', z+v'\}, \{x+v', y, z+v'\}, \{x+v', y+v', z\}: \{x, y, z\} \in \mathcal{A}_i\}$$

and

$$\mathcal{A}_{i,2} = \{\{x, y, z+v'\}, \{x, y+v', z\}, \{x+v', y, z\}, \{x+v', y+v', z+v'\}: \{x, y, z\} \in \mathcal{A}_i\}.$$

It is easy to see that $\mathcal{A}_{i,1}$ and $\mathcal{A}_{i,2}$ are both maximum packings, covering every pair except those in the one-factor $\mathcal{S}^c = \{\{j, j+v'\}: 1 \leq j \leq v'\}$. Also, it is easy to see that no two of these $2(v'-2) = v-4$ packings contain a common triple; hence they are 2-compatible. ∎

We can also show that $M(3, 3, 8) = 4$; see Example 4.1.

Example 4.1 A (3, 3, 8; 4)-threshold scheme. The leave $\mathcal{S}^c$ is the one-factor $\{\{1, 5\}, \{2, 6\}, \{3, 7\}, \{4, 8\}\}$.

$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$	$\mathcal{A}_4$
{1, 2, 3}	{2, 3, 4}	{3, 4, 5}	{4, 5, 6}
{5, 6, 7}	{6, 7, 8}	{7, 8, 1}	{8, 1, 2}
{1, 4, 7}	{2, 5, 8}	{3, 6, 1}	{4, 7, 2}
{5, 8, 3}	{6, 1, 4}	{7, 2, 5}	{8, 3, 6}
{1, 6, 8}	{2, 7, 1}	{3, 8, 2}	{4, 1, 3}
{5, 2, 4}	{6, 3, 5}	{7, 4, 6}	{8, 5, 7}
{2, 7, 8}	{3, 8, 1}	{4, 1, 2}	{5, 2, 3}
{6, 3, 4}	{7, 4, 5}	{8, 5, 6}	{1, 6, 7}

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

Lemma 4.8 If $v \equiv 5$ modulo 6, then $M(3, 3, v) \leq v - 4$.

Proof: As in Lemma 4.4, it suffices to show that $d(\mathcal{S}) \geq 2$ if $\mathcal{S}$ is simple. Since v is odd, every point has even degree in $\mathcal{S}^c$. As well, there must be some point x having positive degree in $\mathcal{S}^c$, since $\mathcal{S}^c$ has at least one edge (Theorem 4.3). Then, for any y such that such that xy is an edge of $\mathcal{S}$, we have that $|N(x) \cup N(y)| \geq 2$; hence, $d(\mathcal{S}) \geq 2$, as required. ■

Again, equality can occur in the above bound only when each $\mathcal{A}_i$ is a maximum packing.

Lemma 4.9 If $v \equiv 5$ modulo 6 and $M(3, 3, v, \mathcal{S}) = v - 4$, then each $\mathcal{A}_i$ is a maximum packing of pairs into triples.

Proof: It is easy to see that if $d(\mathcal{S}) = 2$, then $\mathcal{S}^c$ is a 4-cycle. ■

Example 4.2 The following is a (3, 3, 11; 7)-threshold scheme. Each of the $\mathcal{A}_i$'s is a maximum (2, 3)-packing and each of them has the same leave $\mathcal{S}^c$ consisting of the 4-cycle 7 8 9 t.

$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$	$\mathcal{A}_4$	$\mathcal{A}_5$	$\mathcal{A}_6$	$\mathcal{A}_7$
079	179	279	379	479	579	679
08t	18t	28t	38t	48t	58t	68t
016	120	231	342	453	564	605
025	136	240	351	462	503	614
034	145	256	360	401	512	623
712	724	736	741	751	761	704
735	730	745	750	760	702	713
746	756	701	762	723	734	725
813	823	835	840	852	863	802
826	846	841	856	861	801	815
845	850	860	812	803	824	834
914	925	930	945	950	962	901
923	934	946	961	963	904	924
956	960	951	902	912	913	935
t15	t26	t34	t46	t56	t60	t03
t24	t35	t50	t52	t02	t14	t12
t36	t40	t61	t01	t13	t23	t45

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

Lemma 4.10 If $v \equiv 4$ modulo 6, then $M(3, 3, v) \leq v - 6$.

Proof: Here, it suffices to show that $d(\mathcal{S}) \geq 4$ if $\mathcal{S}$ is simple. Since v is even, every point has odd degree in $\mathcal{S}^c$. Also, there must be some point x having degree ≥ 3 in $\mathcal{S}^c$, since $\mathcal{S}^c$ has more than $v / 2$ edges (Theorem 4.3). Then, there exists a y such that xy is an edge of $\mathcal{S}$ having $|N(x) \cup N(y)| \geq 4$; hence, $d(\mathcal{S}) \geq 4$, as required. ■

We now characterize when equality can occur in the above bound.

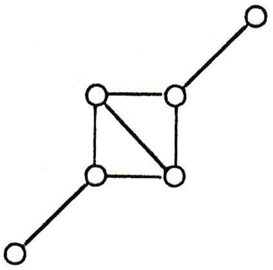
Lemma 4.11 If $v \equiv 4$ modulo 6 and $M(3, 3, v) = v - 6$, then all the $\mathcal{A}_i$'s are (2, 3)-packings having the same leave $\mathcal{S}^c$ which must be isomorphic to one of the following four graphs:

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

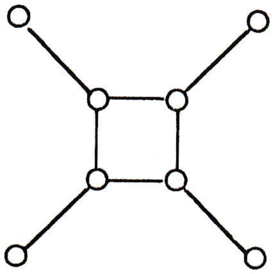
$G_1 \cup (v-6)/2\, K_2$ $\qquad$ $G_2 \cup (v-8)/2\, K_2$

where

$G_1 =$



and $G_2 =$

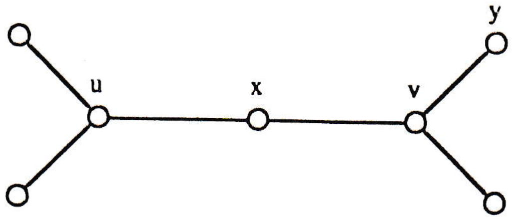


Proof: It is easy to see that for each $\mathcal{S}^c$ above, $d(\mathcal{S}) = 4$.

If $\mathcal{S}^c$ has a vertex of degree 5, then $d(\mathcal{S}) \geq 5$, and if $\mathcal{S}^c$ has two vertices of degree 3 at a distance greater than 2, then $d(\mathcal{S}) \geq 6$. Therefore, we only consider leaves $\mathcal{S}^c$ having degrees 1 and 3, and in which the distance between any two vertices of degree 3 is at most 2. Furthermore, the number of vertices of degree 3 is congruent to 1 modulo 3 because $\mathcal{S}^c$ is the leave of a (2, 3)-packing on $v \equiv 4$ modulo 6 elements.

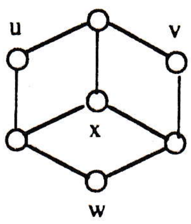
Let $\mathcal{S}^c$ be a leave for which $d(\mathcal{S}) = 4$. Then the induced subgraph of the vertices of degree 3 in $\mathcal{S}^c$ is a connected graph of diameter at most 2. Call this graph T.

To obtain a contradiction, assume $\mathcal{S}^c$ has at least 7 vertices of degree 3. Then no vertex of T can have degree 1 because of the diameter and degree constraints. If T has a vertex x of degree 2, then the diameter and degree constraints imply that T contains a subgraph isomorphic to



This completely determines the neighbourhoods of u and v in $\mathcal{S}^c$. It follows that $|N(x) \cap N(y)| = 1$ and hence, $d(\mathcal{S}) \geq 5$. This establishes that T is a 3-regular graph.

If x and y are two nonadjacent vertices of T and $|N(x) \cap N(y)| = 1$, then $d(\mathcal{S}) \geq 5$. Hence, T must contain a subgraph isomorphic to



in which each of u, v and w has two common neighbours with x. Now, the distance constraint implies that T contains no further vertices. Thus we must conclude that T has 7 vertices of degree 3, which is impossible.

This establishes that T has either 1 or 4 vertices. The result now follows by considering all possible induced subgraphs T on 4 vertices. ■

We now consider the construction of (3, 3, 10; 4)-threshold schemes, for each of the four possible leaves of Lemma 4.11.

Example 4.3 A (3, 3, 10; 4)-threshold scheme. The leave of each packing is the disjoint union of K_4 with 3 K_2.

$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$	$\mathcal{A}_4$
157	257	357	457
169	269	369	469
180	280	380	480
258	358	458	158
260	360	460	160
279	379	479	179
359	459	159	259
368	468	168	268
370	470	170	270
450	150	250	350
467	167	267	367
489	189	289	389

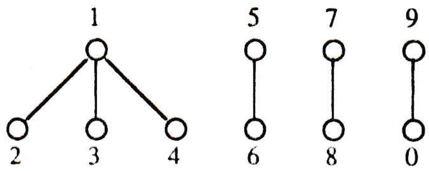
Another (3, 3, 10; 4)-threshold scheme is given by the following example.

Example 4.4 The leave of each packing is the union of G_1 with 2 K_2.

$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$	$\mathcal{A}_4$
157	158	159	150
169	160	168	167
180	179	170	189
259	250	258	257
268	267	260	269
270	289	279	280
340	349	347	348
367	368	369	360
389	370	380	379
458	457	450	459
479	480	489	470
560	569	567	568

Lemma 4.12 There do not exist four compatible packings on 10 points having leaves $K_{1,3} \cup 3\ K_2$.

Proof: We consider maximal (2, 3)-packings which have the graph



as their leave $\mathcal{S}$. We will show that $K_{10} \setminus \mathcal{S}$ does not admit 4 block-disjoint maximal (2, 3)-packings.

There are 2 types of maximal (2, 3)-packings, namely those that contain the block 234 and those that do not. In order to establish that there do not exist four block-disjoint maximal (2, 3)-packings, it is sufficient to prove that there do not exist three such packings which avoid the block 234.

It can be shown that every maximal (2, 3)-packing which avoids 234 is isomorphic to the following packing (1):

uvw	23u	34v	42w
1uW	2vW	3wU	4uV
1vU	2VU	3WV	4UW
1wV			

where

$$\{\{u, U\}, \{v, V\}, \{w, W\}\} = \{\{5, 6\}, \{7, 8\}, \{9, 0\}\}.$$

Therefore, without loss of generality, we may assume that the set of block-disjoint packings we are seeking contains the particular packing (2):

579	235	347	429
150	270	396	458
176	286	308	460
198			

It is easy to see that there are only 2 maximal (2,3)-packings which contain the 4 blocks

uvw 23u 34v 42w;

namely, the one exhibited above and one consisting of the blocks

uvw	23u	34v	42w
1uV	2vU	3wV	4uW
1vW	2VW	3WU	4UV
1wU			

which we name (3). (Note that the permutation (2 3)(v w)(V W) is an isomorphism which maps packing (3) onto (1).) It can be shown that there are precisely 12 maximal (2, 3)-packings which are block-disjoint from packing (2) and avoid the block 234, namely,

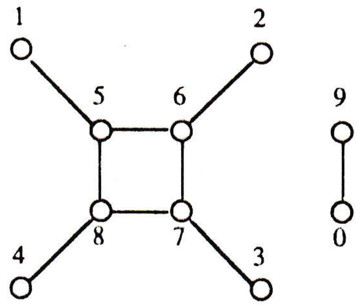
$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	$\mathcal{P}_4$	$\mathcal{P}_5$	$\mathcal{P}_6$
570	589	580	679	670	689
237	238	238	237	236	239
340	349	345	349	340	348
245	245	240	246	247	246
179	180	168	170	169	179
160	169	159	159	180	158
158	157	170	168	157	160
280	279	257	289	250	280
269	260	269	250	289	257
368	367	379	358	358	350
359	350	360	360	379	367
467	468	489	457	468	459
489	470	467	480	459	470

$\mathcal{P}_7$	$\mathcal{P}_8$	$\mathcal{P}_9$	$\mathcal{P}_{10}$	$\mathcal{P}_{11}$	$\mathcal{P}_{12}$
680	680	680	680	680	680
236	236	238	238	230	230
348	340	346	340	346	348
240	248	240	246	248	246
158	158	158	158	158	158
169	169	169	169	169	169
170	170	170	170	170	170
257	250	267	279	259	289
289	279	259	250	267	257
350	357	379	367	389	359
379	389	350	359	357	367
467	467	489	489	450	450
459	459	457	457	479	479

Now it is easy to check that every pair of these packings has at least one common block. Hence, there do not exist 3 block-disjoint maximal packings which avoid the block 234. ■

Lemma 4.13 There do not exist four compatible packings on 10 points having leaves $G_2 \cup K_2$.

Proof: Consider (2, 3)-packings which have the graph



as their common leave $\mathcal{S}^c$. Observe that each of the edges (pairs) 57, 68, 95, 96, 97, 98, 05, 06, 07 and 08 is contained in precisely four triples which avoid the 9 edges of $\mathcal{S}^c$. Hence, if there are four (2, 3)-packings having this graph as their common leave, then all 32 of these triples must appear in the packings. We now show that it is impossible to distribute these 32 pairs among four packings.

The four triples 572, 574, 579 and 570 must each be contained in a different packing. Let us call these four packings $\mathcal{A}_2$, $\mathcal{A}_4$, $\mathcal{A}_9$, and $\mathcal{A}_0$ respectively. Now the triple 459 cannot be in either of $\mathcal{A}_4$ or $\mathcal{A}_9$. We have two cases to consider.

Case 1: $459 \in \mathcal{A}_2$.

This implies that the packings have the following substructure:

$\mathcal{A}_2$	$\mathcal{A}_4$	$\mathcal{A}_9$	$\mathcal{A}_0$
572	574	579	570
459			
053	052	054	
	953		952
074	071	072	
971	972		974

Now the triple 689 can go in any one of these four packings. Notice that two of these subcases are isomorphic under the isomorphism (1 3)(2 4)(5 7)(6 8). In each case, the triples containing 69, 89 and 68 can be placed in these packings in only one way. Then the triples containing 08 cannot be placed without violating the definition of a (2, 3)-packing.

Case 2: $459 \in \mathcal{A}_0$.

This implies that the packings have the following substructure:

$\mathcal{A}_2$	$\mathcal{A}_4$	$\mathcal{A}_9$	$\mathcal{A}_0$
572	574	579	570
			459

935	925		
045	035	025	
017	027	047	
947	917		927

This substructure is isomorphic to that in Case 1, by applying the permutation (2 4)(6 8). This establishes that there do not exist four packings which have $G_2 \cup K_2$ as their common leave. ■

We have presented examples where the bounds of Lemmata 4.8 and 4.10 are exact, though we know of no infinite classes of threshold schemes meeting these bounds with equality. However, by means of a generalization of Theorem 4.7, we can construct infinite classes of threshold schemes where the number of keys is close to these upper bounds.

Our construction is based on the trivial observation that one can easily construct n Latin squares of order n, on the same symbol set, such that no two of these Latin squares contain the same symbol in the same cells. (For example, start with any Latin square L of order n, with the symbol set $\mathbf{Z}_n$. For every i, $0 \le i \le n-1$, define $L_i(a, b) = (L(a, b) + i)$ modulo n.) We say that the n Latin squares are *disjoint*. This immediately gives rise to the following recursive construction.

Theorem 4.14 For all positive integers n and v such that $v \equiv 0$ modulo n, $M(3, 3, v) \ge n \cdot M(3, 3, v / n)$.

Proof: Denote $v' = v / n$ and $m = M(3, 3, v')$. Let $\mathcal{A}_1, \ldots, \mathcal{A}_m$ be 3-compatible 3-uniform hypergraphs on a v'-set **X**, such that $\mathcal{A}_i(2) = \mathcal{S}$, $1 \le i \le m$. Let L_j, $1 \le j \le n$, be n disjoint Latin squares of order n, on symbol set $\{1, 2, \ldots, n\}$. For every $x \in \mathbf{X}$, we will take n copies of x, named x_j, $1 \le j \le n$. Impose an arbitrary ordering on the elements of **X**.

Now, for every $\mathcal{A}_i$, $1 \le i \le m$, we construct n 3-uniform hypergraphs on the v points in $\{x_j\colon 1 \le j \le n,\ x \in \mathbf{X}\}$, denoted $\mathcal{A}_{i,j}$, $(1 \le j \le n)$, as follows. Define

$$\mathcal{A}_{i,j} = \{\{x_a, y_b, z_c\}\colon \{x, y, z\} \in \mathcal{A}_i,\ 1 \le a \le n,\ 1 \le b \le n,\ L_j(a, b) = c,\ x < y < z\}.$$

It is easy to see that $\mathcal{A}_{i,j}(2) = \mathcal{A}_{i',j'}(2)$, for all $(i, j) \ne (i', j')$. As well $\mathcal{A}_{i,j} \cap \mathcal{A}_{i',j'} = \emptyset$ for all $(i, j) \ne (i', j')$. Hence, $M(3, 3, v) \ge n \cdot M(3, 3, v')$. ■

We note that Theorem 4.7 is essentially the special case of Theorem 4.14 when n = 2.

Corollary 4.15 Suppose $v \equiv 4$ or 12 modulo 24, $v / 4 \ne 7, 141, 283, 501, 789, 1501$, or 2365. Then $M(3, 3, v) \ge v - 8$.

Proof: Apply Theorem 4.14 with n = 4. $M(3, 3, v / 4) = (v - 8) / 4$ by Theorem 2.4. ■

Letting n = 5, we obtain in a similar fashion the following corollary.

Corollary 4.16 Suppose $v \equiv 5$ modulo 30, $v / 5 \neq 7, 141, 283, 501, 789, 1501$, or 2365. Then $M(3, 3, v) \geq v - 10$.

Finally, we summarize our results on M(3, 3, v) in Tables 1 and 2. Table 1 contains all values M(3, 3, v) that we know for $v \leq 13$. For the sake of completeness, we observe that M(3, 3, 7) = 3. It is well-known that the maximum number of disjoint S(2, 3, 7) designs is 2 (this was first shown by Cayley in [4]). However, we can obtain a (3, 3, 7; 3)-threshold scheme as follows.

Example 4.5 A (3, 3, 7; 3)-threshold scheme. The leave of each packing is the triangle 123.

$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$
145	146	147
167	157	156
246	247	245
257	256	267
347	345	346
356	367	357

Table 1
M(3, 3, v) for $v \leq 13$

v	M(3, 3, v)	authority
6	2	Theorem 4.7
7	3	Example 4.5
8	4	Example 4.1
9	7	Theorem 2.4
10	4	Examples 4.3 and 4.4
11	7	Example 4.2
12	???	
13	11	Theorem 2.4

Table 2
Bounds on M(3, 3, v)

v	bounds on M(3, 3, v)
$v \equiv 1$ or 3 modulo 6, $v > 1$	$M(3, 3, v) \leq v - 2$
$v \equiv 0, 2$, or 5 modulo 6, $v > 2$	$M(3, 3, v) \leq v - 4$
$v \equiv 4$ modulo 6, $v > 4$	$M(3, 3, v) \leq v - 6$
$v \equiv 1$ or 3 modulo 6, $v \neq 1, 7, 141, 283, 501, 789, 1501, 2365$	$M(3, 3, v) = v - 2$
$v \equiv 2$ or 6 modulo 12, $v / 2 \neq 1, 7, 141, 283, 501, 789, 1501, 2365$	$M(3, 3, v) = v - 4$
$v \equiv 4$ or 12 modulo 24, $v / 4 \neq 7, 141, 283, 501, 789, 1501, 2365$	$M(3, 3, v) \geq v - 8$
$v \equiv 5$ modulo 30, $v / 5 \neq 7, 141, 283, 501, 789, 1501, 2365$	$M(3, 3, v) \geq v - 10$

5. Some bounds on M(4, 4, v)

Shamir's construction for threshold schemes [12] gives lower bounds on M(t, w, v) whenever $p = v / w$ 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 $X = \{(x, y) \in GF(p) \times GF(p),\ 1 \leq x \leq w\}$ (so $v = pw$). Now, for every polynomial $h(x) \in GF(p)[x]$ having degree at most $t - 1$, 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). Hence, the number of blocks $b = p^t$.
It is not difficult to see that the scheme is perfect (see, for example, [14]). Hence, we obtain the following lower bound on M(t, w, v).

Theorem 5.1 Suppose $p = v / w$ is prime, $p > w$, and $t \leq w$. Then $M(t, w, v) \geq v / w$.

For $t = w = 3$, the bounds of Section 4 are superior. However, for most other values of t and w, this result provides the best known lower bounds on M(t, w, v). In the remainder of this section, we present some lower bounds on M(4, 4, v).

From our general results, we know that $M(4, 4, v) \leq v - 3$, with equality occurring if and only if there is a Steiner system S(4, 4, v) which can be partitioned into $v - 3$ Steiner systems S(3, 4, v). This is of course equivalent to finding a set of $v - 3$ *disjoint* S(3, 4, v) (on the same set of points). Aside from the trivial case $v = 4$, no example is known. The best result in this direction is a construction due to Lindner [6].

Theorem 5.2 [6] For all $v \equiv 8$ or 16 modulo 24, there exist at least $3v / 4$ disjoint S(3, 4, v); hence $M(4, 4, v) \geq 3v / 4$ for these values of v.

Note that this is a considerable improvement over the lower bound of $v / 4$ given by Theorem 5.1.

The lower bound of $v / 4$ for M(4, 4, v) can also be improved when $v \equiv 0$ or 6 modulo 12, by means of a result of Teirlinck [15]. The result concerns designs with $\lambda > 1$; for our purposes it is sufficient to define an $S_\lambda(3, 4, v)$ to be a 4-uniform hypergraph on v points such that every three points occur in exactly λ blocks. Teirlinck proved the following.

Theorem 5.3 [15] If $v \equiv 0$ or 6 modulo 12, then there exist $v / 3$ disjoint simple $S_\lambda(3, 4, v)$; hence $M(4, 4, v) \geq v / 3$ for these values of v.

We summarize our bounds on M(4, 4, v) in Table 3.

Table 3
Bounds on M(4, 4, v)

v	bounds on M(4, 4, v)
all v	$M(4, 4, v) \leq v - 3$
$v \equiv 8$ or 16 modulo 24	$M(4, 4, v) \geq 3v / 4$
$v \equiv 0$ or 6 modulo 12	$M(4, 4, v) \geq v / 3$
$v \equiv 4$ or 20 modulo 24, $v / 4$ a prime power	$M(4, 4, v) \geq v / 4$

6. Summary

A very interesting open problem is to improve the lower bounds on $M(t, t, v)$ when $t \geq 4$. Theorem 5.1 tells us that $M(t, t, v) \geq v / t$ under certain circumstances. On the other hand, the upper bound provided by Theorem 2.2 is $M(t, t, v) \leq v - t + 1$. Hence, there is room for an improvement by a factor of almost t. One approach to take would be to attempt to decompose $S(t, t, v)$ (the set of all t-subsets of a v-set) into $S_\lambda(t - 1, t, v)$; then $M(t, t, v) \geq (v - t + 1) / \lambda$. Teirlinck's remarkable results on the existence of t-designs for all t [16, 17] provide such decompositions; however, the values of the resulting λ's are too large. In order to improve upon the bound of Theorem 5.1, we would require that $\lambda \leq t - 1$ in such a decomposition. This is undoubtedly a difficult problem!

A much more tractable open problem would be to finish the determination of the numbers $M(3, 3, v)$. Can the upper bounds given in Table 2 always be attained, perhaps with finitely many exceptions?

References

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

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

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

4. A. Cayley, *On the triadic arrangements of seven and fifteen things*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. 37 (1850), 50-53.

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

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

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

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

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

10. 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.

11. J. Schonheim, *On maximal systems of k-tuples*, Studia Sci. Math. Hung. 1 (1966), 363-368.

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

13. J. Spencer, *Maximal consistent families of triples*, J. Comb. Theory 5 (1968), 1-8.

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

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

16. L. Teirlinck, *Non-trivial t-designs without repeated blocks exist for all t*, Discrete Math. 65 (1987), 301-311.

17. L. Teirlinck, *Locally trivial t-designs and t-designs without repeated blocks*, preprint.

18. G. V. Zaicev, V. A. Zinoviev and N. V. Semakov, *Interrelation of Preperata 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, Chen Demeng and Du Beiliang, *On the existence of (v, 5, 1)-resolvable BIBD*, preprint.