A Combinatorial Approach to Threshold Schemes

D. R. Stinson and S. A. Vanstone
University of Manitoba and University of Waterloo

Abstract We investigate the combinatorial properties of threshold schemes. Informally, a (t, w)-threshold scheme is a way of distributing partial information (shadows) to w participants, so that any t of them can easily calculate a key, but no subset of fewer than t participants can determine the key. Our interest is in *perfect* threshold schemes: no subset of fewer than t participants can determine any partial information regarding the key. We give a combinatorial characterization of a certain type of perfect threshold scheme. We also investigate the maximum number of keys which a perfect (t, w)-threshold scheme can incorporate, as a function of t, w, and the total number of possible shadows, v. This maximum can be attained when there is a Steiner system S(t, w, v) which can be partitioned into Steiner systems S(t - 1, w, v). Using known constructions for such Steiner systems, we present two new classes of perfect threshold schemes, and discuss their implementation.

Introduction

Let $\mathbf{X}$ be a set of v elements (which we refer to as *shadows*), and let $\mathbf{K}$ be a set of m elements (called *keys*). A *(t, w)-threshold scheme* is a pair $(\mathcal{B}, \phi)$, where $\mathcal{B}$ is a set of b (distinct) w-subsets of $\mathbf{X}$ (*blocks*), and ϕ: $\mathcal{B} \rightarrow \mathbf{K}$, such that the following properties are satisfied:

1) any t shadows determine at most one key (i.e. for every t-subset S of $\mathbf{X}$, $|\{\phi(B): S \subseteq B \in \mathcal{B}\}| = 0$ or 1).
2) any set of fewer than t shadows which occur in a block do *not* determine a unique key (i.e. for every t'-subset S of $\mathbf{X}$ where $t' < t$, $|\{\phi(B): S \subseteq B \in \mathcal{B}\}| \neq 1$).

The idea behind threshold schemes is that we wish to give partial information (shadows) to w people, so that any t of them can determine the key, but no group of fewer than t can do this. Suppose we want to send key K. We then pick a block B such that $\phi(B) = K$, and then give each of the w participants a different shadow in B.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 330-339, 1988.

Threshold schemes were first described by Shamir [7] and Blakely [3] in 1979. Since then, many constructions have been given for threshold schemes. Most of the constructions are linear algebraic in nature (see, for example, Kothari [6]). Recently, Beutelspacher [2] has given some constructions for threshold schemes using finite geometries. The purpose of this paper is to investigate the properties of threshold schemes from a combinatorial viewpoint. This more general approach enables us to give some new constructions for threshold schemes based on combinatorial designs.

Property 2) in the definition of threshold schemes says that t participants are required in order to determine the key K, but it is possible that a group of t' (< t) participants may be able to obtain some partial information, if they can rule out certain keys, for example. Ideally, we would like to have threshold schemes where no partial information would be conveyed in this instance.

To make these ideas precise, we discuss the idea of security for threshold schemes (see, for example, Blakely and Meadows [4]). First, we introduce some probability distributions. We assume that we are given a specified probability distribution on the key space **K**. For every key K, we then choose a probability distribution on the blocks in $\phi^{-1}(K)$. Together, these determine a probability distribution on $\mathcal{B}$.

Now, suppose a block B has been chosen, and the shadows distributed to the participants. Any subset of shadows $S \subseteq B$ defines a conditional probability distribution on **K**:

$$p(K \mid S) = p(S \mid K) \cdot p(K) / p(S)$$
$$= \sum_{\{B \in \phi^{-1}(K):\ S \subseteq B\}} p(B \mid K) \cdot p(K) / \sum_{K' \in \mathbf{K}} \sum_{\{B \in \phi^{-1}(K'):\ S \subseteq B\}} p(B \mid K') \cdot p(K')$$

We now can rigourously define the concept of security in a threshold scheme. Given a (t, w)-threshold scheme, and given t' < t, we say that the threshold scheme is *perfectly t'-secure* if for every subset $S \subseteq \mathbf{X}$ of cardinality t' which occurs as a subset of at least one block, and for every key K,we have that $p(K \mid S) = p(K)$.

We will refer to a threshold scheme as *regular* if b / m blocks correspond to each possible key; and for every key K, each block in $\phi^{-1}(K)$ is chosen with equal probability m / b. It follows that, in a regular threshold scheme, we have

$$p(K \mid S) = \sum_{\{B \in \phi^{-1}(K):\ S \subseteq B\}} p(K) / \sum_{K' \in \mathbf{K}} \sum_{\{B \in \phi^{-1}(K'):\ S \subseteq B\}} p(K').$$

Given $S \subseteq X$ and K, define $\lambda(S, K) = |\{B \in \phi^{-1}(K): S \subseteq B\}|$. It then follows that

$$p(K \mid S) = p(K) \cdot \lambda(S, K) / \sum_{K' \in K} p(K') \cdot \lambda(S, K').$$

In a regular scheme, $p(K \mid S) = p(K)$ if and only if

$$\lambda(S, K) = \sum_{K' \in K} p(K') \cdot \lambda(S, K').$$

Thus, a regular threshold scheme is perfectly t'-secure if and only if, for all $S \subseteq X$ of cardinality t', we have that $\lambda(S, K)$ is independent of the key K. Equivalently, we have the following.

Lemma 1.1 A regular (t, w)-threshold scheme $(\mathcal{B}, \phi)$ is perfectly t'-secure if and only if the following property holds: for every $S \subseteq X$ of cardinality t', there exists a non-negative integer $\lambda(S)$, such that, for every key K, we have

$$|\{B \in \phi^{-1}(K): S \subseteq B\}| = \lambda(S).$$

The following result is now an immediate consequence.

Lemma 1.2 If a regular threshold scheme is perfectly t'-secure, then it is perfectly t"-secure for all t", $1 \leq t" \leq t'$.

Proof: Given a subset T, where $|T| = t"$, we have

$$\lambda(T) = \frac{\sum_{\{S:\ |S| = t' \text{ and } T \subseteq S\}} \lambda(S)}{\binom{w - t"}{t' - t"}}$$

2. A combinatorial characterization of perfect threshold schemes

Our main interest is in regular (t, w)-threshold schemes that are perfectly (t - 1)-secure. We refer to such a threshold scheme as *perfect*. Next, we give a characterization of perfect threshold schemes in terms of the blocks corresponding to each key.

Let $\mathcal{A}$ be a set of w-subsets (*blocks*) of a v-set X. We refer to $(X, \mathcal{A})$ as a ***w-uniform hypergraph***, and we say that v is the number of *points* in the hypergraph. Given any integer $t' \leq w$, define a multiset $\mathcal{A}(t') = \bigcup_{A \in \mathcal{A}} \{S: |S| = t', S \subseteq A\}$. Note that $\mathcal{A}(t')$ can contain "repeated" t'-subsets. We say that $\mathcal{A}(t')$ is the multiset of *induced* t'-subsets of $\mathcal{A}$.

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)-threshold schemes in terms of t-compatible w-uniform hypergraphs.

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

One way to approach the construction of a perfect (t, w)-threshold scheme having v shadows is to start with a multiset $\mathcal{S}$ of (t - 1)-subsets of a v-set, 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 $\mathcal{S}$ is the multiset of induced (t - 1)-subsets of each $\mathcal{A}_i$). 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 $m(t, w, v, \mathcal{S})$. Also, denote

$$m(t, w, v) = \max\{m(t, w, v, \mathcal{S}): \mathcal{S} \text{ is a multiset of } (t - 1)\text{-subsets of a v-set}\}.$$

As one would suspect, determining the numbers $m(t, w, v, \mathcal{S})$ are very difficult. Holyer [5] has proved that the question "can a graph G be edge-decomposed into triangles?" is NP-complete. This question can be rephrased as "is $m(3, 3, v, G) \geq 1$?", where G has v vertices. Hence, determining the numbers $m(t, w, v, \mathcal{S})$ is NP-hard.

We can, however, give some upper bounds on m(t, w, v) and $m(t, w, v, \mathcal{S})$, as follows.

Theorem 2.2 Let λ be the largest multiplicity of any block in $\mathcal{S}$. Let u denote the smallest positive integer such that

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

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

Proof: Let $\mathcal{A}$ be a w-uniform hypergraph $\mathcal{A}$ on v points such that $\mathcal{A}(t - 1) = \mathcal{S}$. Let $S \in \mathcal{S}$ have multiplicity λ. The λ blocks in $\mathcal{A}$ which contain S must all be distinct. Hence, together they contain at least u different elements.

Now, suppose we have m t-compatible hypergraphs. From each of the m hypergraphs, we obtain a set of u elements as described above. These m sets must be disjoint, since otherwise the respective multisets of induced t-subsets would not be disjoint. Also, these m sets are disjoint from S. Hence, $m \leq (v - t + 1) / u$.

Corollary 2.3 $m(t, w, v) \leq (v - t + 1) / (w - t + 1)$.

Proof: In order to maximize the bound on m, we minimize u. This occurs when $\lambda = 1$. Then $u = w - t + 1$, and $m \leq (v - t + 1) / (w - t + 1)$.

We can give a nice characterization of when equality can be met in the above bound.

Theorem 2.4 $m(t, w, v) = (v - t + 1) / (w - t + 1)$ if and only if there exists a Steiner system S(t, w, v) which can be partitioned into Steiner systems S(t - 1, w, v).

Proof: First, suppose that we have an S(t, w, v) which can be partitioned into S(t - 1, w, v). The number of these S(t - 1, w, v) is $(v - t + 1) / (w - t + 1)$, and they are t-compatible, so $m(t, w, v) = (v - t + 1) / (w - t + 1)$.

Conversely, suppose $m(t, w, v) = m = (v - t + 1) / (w - t + 1)$. Let $\mathcal{S}$ denote the multiset of induced (t - 1)-subsets of t-compatible w-uniform hypergraphs $\mathcal{A}_1, \ldots, \mathcal{A}_m$. Let S be any (t - 1)-subset in $\mathcal{S}$. Then, S has multiplicity 1. Also, since $m = (v - t + 1) / (w - t + 1)$, we see that every t-subset of the form $S' = S \cup \{x\}$ occurs exactly once in $\bigcup_{1 \leq i \leq m} \mathcal{A}_i(t)$.

We now prove that *any* t-subset of points S" occurs as an induced t-subset in $\bigcup_{1 \leq i \leq m} \mathcal{A}_i(t)$. Fix some t-subset $S' = S \cup \{x\}$. We prove that S" occurs as an induced t-subset by reverse induction on $|S' \cap S"|$. As an induction assumption, suppose that S" occurs as an induced t-subset exactly once if $|S' \cap S"| \geq t - j$. Clearly, we can start the induction at $j = 0$.

Now, suppose that $|S' \cap S''| = t - j - 1$. Let $y \in S' \setminus S''$ and let $z \in S'' \setminus S'$. Define $S^* = S'' \cup \{y\} \setminus \{z\}$. Then, $|S' \cap S^*| = t - j$, so, by the induction assumption, S^* occurs exactly once as an induced t-subset. Now, $S^* \setminus \{y\}$ has cardinality $t - 1$, and is a member of $\mathcal{S}$. Hence, $S^* \setminus \{y\} \cup \{z\} = S''$ occurs exactly once as an induced t-subset in $\bigcup_{1 \le i \le m} \mathcal{A}_i(t)$.

So, we have proved that $\bigcup_{1 \le i \le m} \mathcal{A}_i$ is a S(t, w, v). Each induced (t - 1)-subset occurs once in each $\mathcal{A}_i(t - 1)$, so each of $\mathcal{A}_1, \ldots, \mathcal{A}_m$ is an S(t - 1, w, v). This completes the proof.•

We will define an *optimal (t, w, v)-threshold scheme* to be a perfect (t, w)-threshold scheme having v shadows and $(v - t + 1) / (w - t + 1)$ keys. Unfortunately, there are not too many examples known of partitionable Steiner systems, so optimal threshold schemes are difficult to construct. We present two infinite classes in Section 3.

We finish this section by presenting an example of a well-known threshold system in this combinatorial setting. The scheme we discuss is the Shamir threshold scheme [7].

A prime number $p > w$ is chosen, and the key can be any integer $K \in \mathbf{Z}_p$ (so $m = p$). The set of shadows $X = \{(x, y) \in \mathbf{Z}_p \times \mathbf{Z}_p, 1 \le x \le w\}$ (so $v = pw$). Now, for every polynomial $h(x) \in \mathbf{Z}_p[x]$ having degree at most $t - 1$, we construct a block B(h) as follows. The shadows in B(h) are $(u, h(u))$, $1 \le u \le w$, and the key for B(h) is h(0). Hence, the number of blocks $b = p^t$.

This scheme is perfect. It is not difficult to see that any t-subset of shadows determine h(x), and hence K = h(0), uniquely, by means of Lagrange interpolation. Define a subset of shadows to be a *transversal* if no x-coordinate is repeated. Then is is easy to see, for each $\mathcal{A} = \phi^{-1}(K)$ ($K = 0, \ldots, p - 1$), that $\mathcal{A}(t - 1) = \{$every transversal of size $t - 1$, once each$\}$. Hence, no (t - 1)-subset gives any information as to the value of K.

It is also interesting to compare the number of keys to the bound on m(t, w, v). The Shamir scheme has $v = pw$ and $m = p$, so $m = v / w$. The upper bound on m given in Corollary 2.3 is

$$(v - t + 1) / (w - t + 1).$$

Hence, for large values of v, the number of keys in the Shamir scheme is less than optimal by a factor of about

$$(w - t + 1) / w.$$

3. Some constructions for optimal threshold schemes

In this section, we present constructions for two classes of optimal threshold schemes with $t = 3$, and discuss their implementation. Our first construction is based on partitioning the set of all triples into Steiner triple systems.

Construction 1 Suppose $p \equiv 7 \bmod 8$ is a prime. Then there exists an optimal $(3, 3, p + 2)$ threshold scheme.

We describe a partition of the Steiner system $S(3, 3, p + 2)$ into p Steiner systems $S(2, 3, p + 2)$, due to R. Wilson [8]. Let $X = GF(p) \cup \{\infty, \infty'\}$. Define $\mathcal{A}_0$ to consist of the following blocks:

one block: $\{\infty, \infty', 0\}$;
$(p^2 - 3p + 2) / 6$ blocks: $\{a, b, c\}$, where $a \neq b \neq c \neq a$, and $a + b + c = 0$;
$(p - 1) / 2$ blocks: $\{\infty, a, -2a\}$, where a is a quadratic residue in GF(p); and
$(p - 1) / 2$ blocks: $\{\infty', a, -2a\}$, where a is a quadratic non-residue in GF(p).

Then $\mathcal{A}_0$ is a $S(2, 3, p + 2)$. Define $\infty + i = \infty$ and $\infty' + i = \infty'$, for any $i \in GF(p)$. Now, for any $i \in GF(p)$, define

$$\mathcal{A}_i = \{x + i, y + i, z + i\}: \{x, y, z\} \in \mathcal{A}_0\}.$$

It is not difficult to show that $\bigcup_{0 \leq i < p} \mathcal{A}_i$ is an $S(3, 3, p + 2)$; hence we have the desired optimal threshold scheme.

Example: Suppose $p = 7$. Then $\mathcal{A}_0$ contains blocks:

$\{\infty, \infty', 0\}$, $\{0, 1, 6\}$, $\{0, 2, 5\}$, $\{0, 3, 4\}$, $\{1, 2, 4\}$, $\{3, 5, 6\}$, $\{\infty, 1, 5\}$, $\{\infty, 2, 3\}$, $\{\infty, 4, 6\}$, $\{\infty', 3, 1\}$, $\{\infty', 6, 2\}$, $\{\infty', 5, 4\}$.

Let's now briefly consider implementing such a scheme. We could take p to be some large prime, having 50 digits, for example. A key is any element i of GF(p). To determine shadows, it is necessary only to generate a random block of $\mathcal{A}_0$ and add i to each element. Observe that we can easily generate a random block of $\mathcal{A}_0$ from the recipe given above. It is unnecessary to construct any blocks ahead of time.

Given a block $\{x, y, z\}$, how is the key computed? Again, this is not difficult, if we consider the various possibilities. If $\{x, y, z\} = \{\infty, \infty', i\}$, then the key is i. If $\infty, \infty' \notin \{x, y, z\}$, then the key is $(x + y + z) / 3$. If the block is $\{\infty, x, y\}$, we proceed as follows. We know that $\{x, y\} = \{a + i, -2a + i\}$, where i is the key and a is a quadratic residue. Hence, $a = \pm (x - y) / 3$. Thus, we calculate $(x - y) / 3$, and test to see if it is a quadratic residue. We can do this easily in time $O(\log p)$. If $(x - y) / 3$ is a quadratic residue, then $a = (x - y) / 3$ and $i = x - a$; otherwise, $a = (y - x) / 3$ and $i = y - a$. Finally, if the block is $\{\infty', x, y\}$, the calculations are similar.

Hence, the key is calculated in time $O(1)$, unless the given block contains exactly one of ∞, ∞', in which case the calculation requires time $O(\log p)$. However, this second situation occurs with probability $O(1 / p)$, so on average, the calculation requires time $O(1)$. As well, we observe that the only arithmetic operations required (other than testing quadratic reciprocity) are a small number of addition or subtraction operations, and dividing by 3. The multiplicative inverse of 3 can be calculated ahead of time, so only a single multiplication operation would be required during key calculation.

We also observe that the number of keys, $v - 2$, is roughly three times the number of keys, $v / 3$, in the Shamir scheme when $t = w = 3$.

Our second construction is a partition of the planes of AG(2m, 2) into 2-designs.

Construction 2 For every integer $m \geq 1$, there exists an optimal $(3, 4, 2^{2m})$ threshold scheme.

This is obtained by constructing a Steiner system $S(3, 4, 2^{2m})$ which can be partitioned into $2^{2m - 1} - 1$ Steiner systems $S(2, 4, 2^{2m})$. This result is due to Baker [1].

Let $\mathbf{X} = GF(2^{2m - 1}) \times GF(2)$. Define $\mathcal{A}$ to consist of the planes of the affine geometry AG(2m, 2), as follows:

blocks: $\{(a, i), (b, j), (c, k), (d, l)\}$ where $a + b + c + d = 0$ (in $GF(2^{2m - 1})$) and $i + j + k + l = 0$ (in $GF(2)$).

Clearly, every block has the form $\{(a, 0), (b, 0), (c, 0), (d, 0)\}$, $\{(a, 1), (b, 1), (c, 1), (d, 1)\}$, or $\{(a, 0), (b, 0), (c, 1), (d, 1)\}$. Define a function $k: \mathcal{A} \rightarrow GF(2^{2m - 1}) \setminus \{0\}$ as follows:

$$k(A) = (a^3 + b^3 + c^3 + d^3)^{1 / 3}, \text{ if } A = \{(a, 0), (b, 0), (c, 0), (d, 0)\},$$

$k(A) = (a^3 + b^3 + c^3 + d^3)^{1/3}$, if $A = \{(a, 1), (b, 1), (c, 1), (d, 1)\}$,
$k(A) = (a^3 + b^3 + c^3 + d^3 + (c + d)^3)^{1/3}$, if $A = \{(a, 0), (b, 0), (c, 1), (d, 1)\}$.

Then, define $\mathcal{A}_x = \{A: k(A) = x\}$ $(x \in GF(2^{2m-1}) \setminus \{0\})$. Then, it can be proved that each $\mathcal{A}_x$ is a $S(2, 4, 2^{2m})$ (see [1]).

Key calculation is accomplished as follows. We observe that, since $GCD(2^{2m-1} - 1, 3) = 1$, there exists a (unique) multiplicative inverse of 3 (mod $2^{2m-1} - 1$). Denote this number by t. Then, $x^{1/3} = x^t$, for any $x \in GF(2^{2m-1})$.

Let's also consider how to generate a random block in $\mathcal{A}_x$. This is made easier by the observation that, for any $\omega \in GF(2^{2m-1}) \setminus \{0\}$, $k(\omega A) = \omega \cdot k(A)$, where ωA is defined to be the block

$$\{(\omega a, i), (\omega b, j), (\omega c, k), (\omega d, l)\} \text{ (where } A = \{(a, i), (b, j), (c, k), (d, l)\}).$$

Hence, if we generate any random block $A \in \mathcal{A}$, we can then obtain a random block in $\mathcal{A}_x$ by multiplying A by $x \cdot k(A)^{-1}$.

In this scheme, the number of keys, $(v - 2) / 2$, is about 2 times the number of keys, $v / 4$, in the Shamir (3, 4)-scheme.

References

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

2. A. Beutelspacher, Geometric structures as threshold schemes, preprint.

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

4. G. R. Blakely and C. Meadows, Security of ramp schemes, Lecture Notes in Computer Science 196 (1985), 242-268.

5. I. Holyer, The NP-completeness of edge-colouring, SIAM J. Computing 10 (1981), 718-720.

6. S. C. Kothari, Generalized linear threshold scheme, Lecture Notes in Computer Science 196 (1985), 231-241.

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

8. R. M. Wilson, Some partitions of all triples into Steiner triple systems, Lecture Notes in Math. 411 (1974), 267-277.