AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **34** (2006), Pages 229–237

Access schemes based on perfect critical set partitions and transformations

L. F. Fitina S. P. Lal

Department of Mathematics and Computing Science
University of the South Pacific
Suva, Fiji

Abstract

We propose a secret sharing scheme based on critical sets of latin squares (quasigroups). Critical sets are first partitioned into perfect sets, then elements of the critical set are moved using some transformation.

1 Motivation

Secret sharing is concerned with the problem of distributing a secret among a group of participants, so that only authorized groups of participants can recreate the secret by combining their *shares*, but no unauthorized group of participants can. The set of all authorized groups is called an *access structure*.

Shared security systems are used in banks, communications networks, in educational institutions and in the military.

The earliest studied type of secret sharing schemes are called (t, n)-*threshold schemes*. In these schemes the access structure consists of all t-element subsets of a group of n participants. Each participant holds a share of the secret. If any t participants combine their shares they will be able to recreate the secret. A group of $t-1$ or less participants will not be able to recreate the secret.

More complex secret sharing schemes include the *hierarchical* and *compartmentalized* schemes, which are described in Ghodosi, Piepryzk and Safavi-Naini [5].

In a hierarchical scheme, the participants are divided into two or more levels of influence. The lower the level of influence, the greater the number of participants (*shareholders*) who must cooperate to reconstruct the secret.

In a compartmentalized scheme, the shareholders are divided into two or more mutually exclusive compartments. The shareholders within a compartment must coorporate to complete their share of the secret. The entire secret cannot be completed until some (perhaps all) compartments combine their shares.

Structures with rules for completion may be found to lend themselves easily to compartmentalized and hierarchical schemes. Such structures include latin squares, F-squares, Youden squares, regular graphs, colourings, etc. These are discussed more fully in [6].

In this paper we present a new way of using critical sets of latin squares in a secret sharing scheme, in which we combine the idea of a perfect set and a function to transform certain elements of the critical set.

2 Latin squares

A *partial Latin square* P of order n is an $n \times n$ array containing symbols chosen from a set V of size v in such a way that each element of V occurs at most once in each row and at most once in each column of the array. For ease of exposition, a partial Latin square P will be represented by a set of ordered triples $\{(i, j; k)\}$ where entry k occurs in cell (i, j). If all the cells of the array are filled then the partial Latin square is termed a Latin square.

That is, a *Latin square* L of order v is a $v \times v$ array with entries chosen from the set V in such a way that each element of V occurs precisely once in each row and precisely once in each column of L.

A *critical set* in a Latin square L (of order v) is a partial Latin square $\mathcal{K}$ in L, such that

(1) L is the only Latin square of order v which has element k in cell (i, j) for each $(i, j; k) \in \mathcal{K}$, and

(2) no proper subset of $\mathcal{K}$ satisfies (1).

A *transformed critical set* is a partial latin square that is not a critical set, but which results in a critical set, when almost all, but a few of its elements are moved in some specified way.

A *uniquely completable set* (UC) in a Latin square L of order v is a partial Latin square in L which satisfies condition (1) above.

Let U be a uniquely completable subset of a critical set $\mathcal{K}$. Then a triple $x = (i, j; k)$ is said to be *uniquely completable under* U, if $U \cup \{x\}$ is uniquely completable.

The set of cells $\mathcal{S}_P = \{(i, j) \mid (i, j; P_{ij}) \in P, \text{ for some } P_{ij} \in V\}$ is said to determine the *shape* of P and $|\mathcal{S}_P|$ is said to be the *volume* of the partial latin square; that is, the volume is the number of non-empty cells. For each r, $1 \leq r \leq v$, let $\mathcal{R}_P^r$ denote the set of entries occurring in row r of P. Formally, $\mathcal{R}_P^r = \{P_{rj} \mid (r, j; P_{rj}) \in P\}$. Similarly, for each c, $1 \leq c \leq v$, we define $\mathcal{C}_P^c = \{P_{ic} \mid (i, c; P_{ic}) \in P\}$ and for each element $e \in V$ we define $\mathcal{E}_P^e = \{(i, j) \mid (i, j; e) \in P\}$.

A *latin interchange*, $\mathcal{I} = (I, I')$, of *volume* s, is a collection of two partial latin squares, of order v, such that

1. $\mathcal{S}_I = \mathcal{S}_{I'}$,
2. for each $(i, j) \in \mathcal{S}_I$, $I_{ij} \neq I'_{ij}$,
3. for each r, $1 \leq r \leq v$, $\mathcal{R}_I^r = \mathcal{R}_{I'}^r$, and
4. for each c, $1 \leq c \leq v$, $\mathcal{C}_I^c = \mathcal{C}_{I'}^c$.

Thus a Latin interchange is a pair of disjoint partial Latin squares of the same shape and order, which are row-wise and column-wise mutually balanced.

Bean and Donovan [1] proved that:

Theorem 2.1 *Let $\mathcal{K}$ be a subset of a Latin square L. Then $\mathcal{K}$ is a critical set of L if and only if for every $x \in \mathcal{K}$, there exists a Latin interchange I_x such that*

$$I_x \cap \mathcal{K} = \{x\}$$

Let $\mathcal{K}$ be a critical set of a Latin square L. Let A be a subset of $\mathcal{K}$. Then the *nest of* A, denoted $\mathcal{N}(A)$, is the union of $\mathcal{K} \setminus A$ and the set A^U such that $(\mathcal{K} \setminus A) \cup A^U$ is uniquely completable. Further, A is said to be *perfect*, if $A^U = \emptyset$ (that is, $\mathcal{N}(A) = \mathcal{K} \setminus A$). A singleton set $\{a\}$ which is perfect is called an *atom*.

3 Perfect partitioning of critical sets

In this section we are interested in partitioning critical sets into subsets which are perfect. This type of partition is called a *perfect partition*. Let us start with an example:

Example 3.1 Let

$$\mathcal{K} = \begin{array}{|c|c|c|c|}\hline & 2 & & \\ \hline 2 & & 4 & \\ \hline & & 1 & \\ \hline & 1 & & \\ \hline \end{array}$$

Then we note that $\mathcal{K}$ can be partitioned into perfect sets as follows:

$$\begin{array}{|c|c|c|c|}\hline & 2 & & \\ \hline 2 & & 4 & \\ \hline & & 1 & \\ \hline & 1 & & \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline & 2 & & \\ \hline 2 & & 4 & \\ \hline & & & \\ \hline & & & \\ \hline \end{array} + \begin{array}{|c|c|c|c|}\hline & & & \\ \hline & & & \\ \hline & & 1 & \\ \hline & 1 & & \\ \hline \end{array}$$

That is, the perfect sets are $\{(1, 2; 2), (2, 1; 2)\}$, $\{(2, 3; 4)\}$, and $\{(3, 3; 1), (4, 2; 1)\}$.

If x is any element or cell in L, let R_x denote the set of entries in the row containing x, and C_x denote the set of entries in the column containing x.

We note that an empty cell $c = (i, j)$ can be filled with an entry $k \in N$ if one of the following is true:

1. $(R_c \cup C_c)$, has one element, k, missing.
2. of column j, every row corresponding to each of **every other** empty cell in the column contains k, and
3. of row i, every column corresponding to each of **every other** empty cell in the row contains k.

In the following example, we have a singleton set which is perfect.

Example 3.2

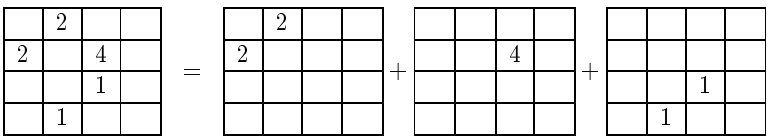
$\mathcal{K} =$

	2		
2		4	
		1	
	1		

It is the element $(2, 3; 4)$. If it is removed then no single cell can be uniquely filled.

In this paper we are interested in perfect sets that are as small in size as possible. As well, we are interested in perfect sets in which all the entries are the same. A subset of a critical set in which every entry is the same, will be called a *homogeneous set*.

In this example, we note that the sets $\{(1, 2; 2), (2, 1; 2)\}, \{(3, 3; 1), (4, 2; 1)\}$ are perfect. Thus we can partition $\mathcal{K}$ into homogeneous perfect sets as follows:



It is easy to see that:

Theorem 3.2 *The union of two or more perfect sets is perfect.*

From Fitina, Seberry and Chaudhry [4] we have that:

Theorem 3.3 *The union of a perfect set and any other set, is perfect.*

Corollary 3.1 *A critical set which has at least two atoms has a perfect partition.*

Theorem 3.4 *If $v \geq 3$ then the complement of a $(v-2)$-set is perfect.*

Proof. Suppose that P is a subset of a critical set of order v, with $\mathcal{S}_P = v - 2$. Each column or row must have at least two entries missing. There are not enough entries to force any cell to be uniquely filled. ■

Fitina, Seberry and Chaudhury [4] proved that:

Theorem 3.5 *The union of two sets is perfect if their nests do not have an intersection outside the critical set.*

4 Transformed critical sets

Consider a critical set of a Latin square of order n. Further, suppose the size of the critical set is z. We will consider different ways of forming transformed critical sets from critical sets.

In this section, addition is done modulo $z + 1$.

4.1 Transformed critical sets with one absolute element

Let the elements of a critical set of size z be denoted by

$$\lambda_1 = (i_1, j_1; k_1), \lambda_2 = (i_2, j_2; k_2), \vdots, \lambda_z = (i_z, j_z; k_z).$$

Then, given some function $f(x)$ and permutation $\rho(x)$, we form a transformed critical set $\mathcal{K}_T$ with elements $\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_z$ given by

$$\gamma_1 = \lambda_1$$

and for $2 \leq t \leq z$,

$$\gamma_t = (f(i_t), f(j_t); \rho(k_t)),$$

where the functions f and ρ have the following properties:

For function f, if $u \neq v$ then one of the following conditions is true:

1. $f(i_u) \neq f(i_v)$ and $f(j_u) \neq f(j_v)$;
2. $f(i_u) = f(i_v)$ and $f(j_u) \neq f(j_v)$;
3. $f(j_u) = f(j_v)$ and $f(i_u) \neq f(i_v)$.

For ρ, the following must be true:

4. $\rho(k_u) = \rho(k_v) \Rightarrow f(i_u) \neq f(i_v), \quad \rho(k_u) = \rho(k_v) \Rightarrow f(j_u) \neq f(j_v)$.

We call γ_1 the *absolute* element and $\gamma_2, \gamma_3 \cdots, \gamma_{z-1}$ the *relative* elements of the transformed critical set. Here γ_1 maybe chosen arbitrarily.

If $A \subset \mathcal{K}$, then the subset $A' \subset \mathcal{K}_T$ is called the *derived set* of A if each element of A' is a transformed element of A.

Example 4.3 As an example, consider the case where

$$f(x) = x + \epsilon$$

for some suitable ϵ. That is, for each $t, 2 \leq t \leq z$,

$$\gamma_t = (i_t + \epsilon, j_t + \epsilon; \rho(k_t)),$$

where ρ is the permutation given by $k_2 \to k_3, k_3 \to k_4, \cdots, k_z \to k_2$.

We note that ϵ should be chosen so that $i_t + \epsilon \neq i_1$ and $j_t + \epsilon \neq j_1, \forall t \neq 1$.

We note that the last elements of each triple $(i_t, j_t; k_t), 2 \leq t \leq z$, are permuted using some permutation, ρ.

Consider the given critical set $\mathcal{K}$ of a 4×4 Latin square

$$\mathcal{K} = \begin{array}{|c|c|c|c|} \hline & 2 & & \\ \hline 2 & & 4 & \\ \hline & & 1 & \\ \hline & 1 & & \\ \hline \end{array}$$

Let us denote:

$$\lambda_1 = (2, 3; 4)$$
$$\lambda_2 = (2, 1; 2)$$
$$\lambda_3 = (4, 2; 1)$$
$$\lambda_4 = (1, 2; 2)$$
$$\lambda_5 = (3, 3; 1).$$

The absolute element is $\gamma_1 = (2, 3; 4)$, which corresponds to the only atom in the critical set.

Using $\epsilon = 1$, we obtain the relative elements:

$$\gamma_2 = (4, 3; 1), \quad \gamma_3 = (2, 4; 2), \quad \gamma_4 = (3, 4; 1), \quad \gamma_5 = (1, 1; 2).$$

This results in the following transformed critical set:

$$\begin{array}{|c|c|c|c|} \hline 2 & & & \\ \hline & & 4 & 2 \\ \hline & & & 1 \\ \hline & & 1 & \\ \hline \end{array}$$

This is in fact a critical set for the latin square:

2	1	3	4
1	3	4	2
3	4	2	1
4	2	1	3

It can be verified that this is not the original latin square.

Remark:

1. It is worth mentioning that the choice of transformation function, the absolute element and the order of relative elements influences the resulting transformed critical set. In some cases reconstructing the transformed critical set yields many possible Latin squares.
2. If there is more than one atom in a critical set, then these elements could form the absolute elements of the transformed critical set. Indeed, absolute elements may be chosen because of some other properties, like that of being most "influential". The other elements would then be the relative elements.

However we will not explore this possibility here.

5 A quick survey on secret sharing schemes based on latin squares

In [2], a secret sharing scheme based on a latin square of order n was constructed, which has the following properties:

1. The latin square is kept private.
2. The order of the latin square is made public.
3. Each share is based on a partial latin square that is uniquely completable.
4. The access structure is defined as $\Gamma = \{B : B \subset P \& A \subset B\}$ where A is some critical set in the latin square.
5. Γ is monotone.

In this scheme a latin square of order n is chosen. The number n is made public, but the latin square, which is the key, is kept secret.

Each element of the partial latin square P is given as a share to a participant.

A group of participants whose shares make up a critical set can recreate the latin square.

The merits of a scheme based on a latin square have been outlined by several people, including [2] and [7]. It is noted for example, that

- Latin squares of large order provide relatively secure systems.

The security of such a scheme depends on the number of latin squares containing the partial latin square corresponding to the shares of a group of unfaithful shareholders. Furthermore Colbourn [3] computed that the complexity of completing a partial latin square is NP-complete.

Nevertheless it may be possible to compute, given a partial latin square, all possible completions.

6 A secret sharing scheme based on transformed latin squares

6.1 With an access structure containing one authorized group

Given a critical set $\mathcal{K}$ with one atom λ_1, a secret sharing scheme could be formed as follows:

1. Partition $\mathcal{K}$ into perfect sets.
2. Form a transformed critical set $\mathcal{K}_T$ with λ_1 as the absolute element, using some functions f and ρ.
3. Form a partition of $\mathcal{K}_T$ into derived sets of perfect sets in $\mathcal{K}$.
4. Give each derived set as a share to each participant.

To reconstruct the original critical set, the participants would have to know the function f, and the permutation ρ. Each participant would then have to reconstruct the perfect set corresponding to his or her derived set.

Since each share corresponds to a perfect set, the shares of any $z-1$ participants would amount to a perfect set, by Theorem 3.3. A group of $z-1$ or fewer people who want to cheat will first of all have to reconstruct their individual shares, and then group those shares to determine the secret. Since, however, whatever is missing from those share constitutes a perfect set, they will have no information about the rest of the shares.

Thus even after reconstructing the perfect sets of the original critical set, no group of any $z-1$ participants can reconstruct a unique latin square from the information contained in their shares.

6.2 With an access structure containing more than one authorized group

By Theorem 3.2 and Theorem 3.3, one can obtain many perfect sets in a critical set. There are therefore many perfect partitions for any one critical set. Each

perfect partition gives rise to a potential authorized group. Thus the shares given to shareholders in a particular authorized group must come from a specific partition of the critical set.

This construction access structure is therefore different from that offered by Cooper, Donovan and Seberry, [2].

References

[1] R. Bean and D. Donovan, Closing a gap in the spectrum of critical sets. *Australas. J. Combin.* **22** (2000), 199–210.

[2] J. Cooper, D. Donovan and J. Seberry, Secret sharing schemes arising from latin squares, *Bull. ICA* **12** (1994), 33–42.

[3] C. J. Colbourn, The complexity of completing partial latin squares, *Discrete Applied Math.* **8** (1984), 25–30.

[4] L.F. Fitina, J. Seberry and G. R. Chaudhry, Back circulant latin squares and the influence of a set, *Australas. J. Combin.* **20** (1999), 163–180.

[5] H. Ghodosi, J. Pieprzyk and R. Safavi-Naini, Secret sharing in multilevel and compartmented groups, *Information and Privacy*, eds. C. Boyd and E. Dawson, *LNCS*, Springer-Verlag, Berlin, Vol. 1438 (1998), 367–378.

[6] J. Seberry and A. P. Street, Strongbox secured secret sharing schemes, *Utilitas Mathematica* **57** (2000), 147–163.

[7] A. P. Street, Defining sets for t-designs and critical sets for latin squares, *New Zealand J. Math.* **21** (1992), 133–144.

(Received 21 June 2004)