1-9-2005

The power and influence in some Youden squares and secret sharing

L. Fitina
University of Wollongong

Ken Russell
University of Wollongong, kerussell@csu.edu.au

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

The power and influence in some Youden squares and secret sharing

Abstract

We investigate subsets of critical sets of some Youden squares in the context of secret sharing schemes. A subset C of a Youden square is called a critical set, if C can be uniquely completed to a Youden square but any subset of C cannot does not have a unique completion to a Youden square. That part of a Youden square Y which is inaccessible to subsets of a critical set C of Y, called the strongbox of C, may be thought to contain secret information. We study the size of the secret. Seberry and Street have shown how strongboxes may be used in hierarchical and compartmentalized secret sharing schemes.

Keywords

Youden square, critical set, influence, power, secret sharing, hierarchical access schemes, compartmentalized access schemes, strongbox, AMS Subject Classification: Primary 62K10, 62K99; Secondary 05B15

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Fitina, L., Russell, K. G. & Seberry, J. R. (2007). The power and influence in some Youden squares and secret sharing. Utilitas Mathematica, 73 143-157.

The power and influence in some Youden squares and secret sharing

Lakoa Fitina, Kenneth G Russell and Jennifer Seberry
Centre for Computer Security Research
School of Mathematics & Applied Statistics
and
School of IT & Computer Science
University of Wollongong
NSW 2522
Australia

Abstract

We investigate subsets of critical sets of some Youden squares in the context of secret sharing schemes. A subset $\mathcal{C}$ of a Youden square is called a critical set, if $\mathcal{C}$ can be uniquely completed to a Youden square but any subset of $\mathcal{C}$ cannot does not have a unique completion to a Youden square.

That part of a Youden square Y which is inaccessible to subsets of a critical set $\mathcal{C}$ of Y, called the strongbox of $\mathcal{C}$, may be thought to contain secret information. We study the size of the secret. Seberry and Street have shown how strongboxes may be used in hierarchical and compartmentalized secret sharing schemes.

Key words and phrases: Youden square, critical set, influence, power, secret sharing, hierarchical access schemes, compartmentalized access schemes, strongbox.

AMS Subject Classification: Primary 62K10, 62K99; Secondary 05B15

1 Introduction

For the full definition of a *Youden square* we refer the reader to our other article [5]. Here it will be sufficient to say that a *Youden square* Y is a $k \times v$ array, where $2 \leq k < v$, each of whose cells contain an *object* from the set $V = \{1, 2, \ldots, v\}$; each *element* of Y is denoted by a triple $(i, j; x)$, which indicates that the object x lies at position (i, j) of Y.

A *critical set* $\mathcal{C}$ of a Youden square Y is a subset of Y with the property that Y is the only $k \times v$ Youden square containing $\mathcal{C}$, and no proper subset of $\mathcal{C}$ has this property.

Secret sharing is concerned with the problem of distributing a secret among a group of participating individuals, or entities, so that only pre-designated collections of individuals are able to recreate the secret by collectively combining their *shares* of the secret.

The earliest and the most widely studied type of secret sharing schemes are called (t, n)-*threshold schemes*. In these schemes the *access structure* – a specification of which collections of participants are authorized to recreate the secret – comprises all the possible t-element subsets selected from a n-element set.

In a (t, n)-threshold scheme, each of the n participants holds some *shares* of the secret. The parameter $t \leq n$ is called the *threshold* value. A fundamental property of a (t, n)-threshold scheme is that the secret can only be recreated if at least t shareholders combine their shares, but less than t shareholders cannot recreate the secret. The fact that the key can be recovered from the combined shares of any t-sized subset is a property which makes threshold schemes very useful in key management. Threshold schemes tolerate the invalidation of up to $n - t$ shares – the secret can still be recreated from the remaining intact shares. More complex secret sharing schemes include the *hierarchical* and *compartmentalized* schemes, which are described in Ghodosi, Pieprzyk and Safavi-Naini [6] and references cited therein. In a hierarchical scheme, the shareholders are divided into two or more levels of *"influence"*. The lower the level of influence, the greater the number of shareholders who must cooperate to complete the secret. In a compartmentalized scheme, the shareholders are divided into two or

more mutually exclusive and exhaustive compartments. The shareholders within a compartment must cooperate to complete their share of the secret. The entire secret cannot be uniquely completed until some (or perhaps all) compartments contribute their shares.

1.1 Power and Influence

Fix a Youden square Y. Let $\mathcal{C}$ be a critical set of Y and let D be a subset of $\mathcal{C}$. The *power* of D in $\mathcal{C}$ is the number of distinct Youden squares that $\mathcal{C} \setminus D$ can be completed to. The *nest* $\mathcal{N}(D, \mathcal{C})$ of D in $\mathcal{C}$ is the union of $\mathcal{C} \setminus D$ and the set that be uniquely completed from $\mathcal{C} \setminus D$.

We also make corresponding *element* definitions to the *set* definitions above: For any $a \in \mathcal{C}$, the *power* (resp. *nest*) of the *element* a in $\mathcal{C}$, is just the *power* (resp. *nest*) of the singleton set $\{a\}$ in $\mathcal{C}$. (These definitions essentially allow us to omit the set braces, in the case where the set is a singleton.)

Before defining *influence* let us make the observation that:

Lemma 1 *If D is a subset of a critical set $\mathcal{C}$ of a Youden square Y then*

$$\mathcal{N}(D, \mathcal{C}) \subseteq \bigcap_{d \in D} \mathcal{N}(d, \mathcal{C}).$$

We define the *set-influence* (or just *influence*) of a set $D \subset \mathcal{C}$ to be the number

$$\sigma(D, \mathcal{C}) = |Y \setminus \mathcal{N}(D, \mathcal{C})|.$$

That is, the set-influence of D is the number of cells in Y which cannot be filled if D is removed from $\mathcal{C}$. In the case: D is a singleton $\{a\}$ we extend the definition in the same way as for nest and power, so that $\sigma(\{a\}, \mathcal{C}) = \sigma(a, \mathcal{C})$.

Also, the *element-influence* of D is defined to be the number

$$\epsilon(D, \mathcal{C}) = |Y \setminus \bigcup_{d \in D} \mathcal{N}(d, \mathcal{C})|.$$

That is, the element-influence is the number of unfilled entries not in the union of the nests of the elements of the set.

Since

$$\mathcal{N}(D,\mathcal{C}) \subseteq \bigcap_{d\in D} \mathcal{N}(d,\mathcal{C}) \subseteq \bigcup_{d\in D} \mathcal{N}(d,\mathcal{C})$$

it follows that:

Lemma 2 *For every subset D of a critical set $\mathcal{C}$ of a Youden square Y,*

$$\epsilon(D,\mathcal{C}) \leq \sigma(D,\mathcal{C}).$$

Remark 1 For any given element $a \in \mathcal{C}$,

$$\epsilon(a,\mathcal{C}) = \sigma(\{a\},\mathcal{C}) = \sigma(a,\mathcal{C}).$$

That is, the element-influence of an element of a critical set is equal to its set-influence.

A subset A of a critical set $\mathcal{C}$ is said to have *perfect influence* if $\mathcal{N}(A,\mathcal{C}) \subset \mathcal{C}$, and such a set A is called a *perfect* set.

We now direct our attention to particular subsets of a critical set known as ℓ-boxes, which we define now.

For each integer ℓ such that $1 \leq \ell \leq |\mathcal{C}|$, the *$\ell$-box* of a critical set $\mathcal{C}$ of a Youden square Y, is that part of Y that cannot be uniquely completed by any $(|\mathcal{C}|-\ell)$-subset of $\mathcal{C}$. Also, the *strongbox* of a critical set $\mathcal{C}$ of a Youden square Y is that part of Y that cannot be uniquely completed by *any* subset of $\mathcal{C}$. The *ℓ-box* can be shown to have the following defining property, which gives us a useful defining property for the *strongbox,* since it turns out to coincide with the *1-box.*

Lemma 3 *If $\mathcal{C}$ is a critical set of a Youden square Y and $1 \leq \ell \leq |\mathcal{C}|$ then*

$$\ell\text{-box}(\mathcal{C}) = Y \setminus \bigcup_{\substack{A\subset\mathcal{C}\\|A|=\ell}} \mathcal{N}(A,\mathcal{C}).$$

Corollary 1 *The strongbox of a critical set $\mathcal{C}$ of a Youden square Y is given by*

$$1\text{-box}(\mathcal{C}) = Y \setminus \bigcup_{c\in\mathcal{C}} \mathcal{N}(c,\mathcal{C}).$$

Proof. Clearly if $A \subseteq B \subseteq \mathcal{C}$, then $\mathcal{N}(B,\mathcal{C}) \supseteq \mathcal{N}(A,\mathcal{C})$. Thus if $1 \leq s \leq t \leq |\mathcal{C}|$ then s-box$(\mathcal{C}) \subseteq t$-box$(\mathcal{C})$. Since the strongbox of $\mathcal{C}$ must be a subset of any s-box of $\mathcal{C}$, the strongbox is a subset of the 1-box of $\mathcal{C}$. But since the 1-box of $\mathcal{C}$ is contained in any s-box of $\mathcal{C}$ it must also be contained in the strongbox of $\mathcal{C}$. Thus the strongbox is precisely the 1-box. □

Corollary 2 *If $\mathcal{C}$ is a critical set of a Youden square Y and $1 \leq s \leq t \leq |\mathcal{C}|$ then*

$$|s\text{-box}(\mathcal{C})| \leq |t\text{-box}(\mathcal{C})|.$$

For an example we consider the critical set at left below of the Youden square at right below:

1	2			
2				
				3
			3	4

completes to

1	2	3	4	5
2	3	4	5	1
4	5	1	2	3
5	1	2	3	4

The elements $(1,2;2)$ and $(4,4;3)$ each have an (element-)influence of 13. Their nests are

1				
2				
4				3
5			3	4

and

1	2			5
2				1
				3
				4

respectively. The union of the nests of the elements $(1,2;2)$ and $(4,4;3)$ is

1	2			5
2				1
4				3
5			3	4

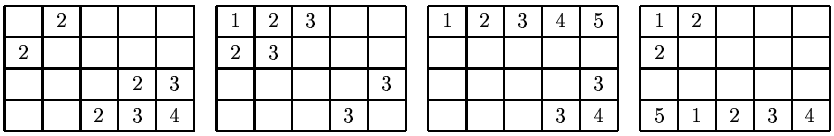
Thus the element-influence of $\{(1,2;2),(4,4;3)\}$ is 10.

By contrast, the subset $\{(1,2;2),(4,4;3)\}$ has nest

1				
2				
				3
				4

and so the set has a set-influence 16; moreover, it is perfect.

The elements $(1,1;1)$, $(4,5;4)$, $(2,1;2)$ and $(3,5;3)$ have influence 13, 13, 12, and 12 respectively. Their nests are:



The union of the nests of the six elements of the critical set above is thus:

1	2	3	4	5
2	3			1
4			2	3
5	1	2	3	4

Hence the strongbox (or 1-box) for the above example is given by the four blank cells in the above array.

One possible completion of the nest of the element $(1,2;2)$ that we considered earlier, is:

1	3	5	4	2
2	4	3	1	5
4	2	1	5	3
5	1	2	3	4

Observe that 3, 1, 2 and 1 fill the strongbox cells, namely the cells at positions $(2,3)$, $(2,4)$, $(3,2)$ and $(3,3)$, respectively.

Enumerating all the completions of the nest of the element $(1,2;2)$, we find there are 32 of them, and so the power of $(1,2;2)$ in our chosen critical set

is 32. Looking at these completions, we find exactly 2 have the tuple of entries $(3,1,2,1)$ filling the strongbox cells, but only once do they occur in the order of the above completion.

We expect the numbers of completions of the nests of elements of critical sets of $v \times (v-1)$ Youden squares to explode combinatorially and to be $O(2^{v-2}(v-1)!)$.

We apply our results to obtain hierarchical and compartmentalized secret sharing schemes.

2 Coalitions, Power and Influence

For our example for $v = 5$ in §1.1, no single element of the chosen critical set has perfect influence, but some 2-subsets of the critical set do have perfect influence.

We shall call a set of ℓ elements $\{(i_1, j_1; x_1), \ldots, (i_\ell, j_\ell; x_\ell)\}$ of a Youden square a *share of a secret.*

An ℓ-subset A of a critical set $\mathcal{C}$ of a Youden square Y is said to be *ℓ-crucial* (or just *crucial*) if A is perfect and no proper subset of A is perfect. Elements of a crucial set are referred to as *crucial elements.* An element $a \in \mathcal{C}$ is called an *atom* if $\{a\}$ is crucial.

Remark 2 If A, B are crucial subsets of a critical set $\mathcal{C}$ of a Youden square Y such that $|A| \leq |B|$ then $\sigma(A, \mathcal{C}) \leq \sigma(B, \mathcal{C})$.

Lemma 4 *If a is an atom of a critical set $\mathcal{C}$ of a Youden square Y, and x is any other element in $\mathcal{C}$ then $\sigma(a, \mathcal{C}) \geq \sigma(x, \mathcal{C})$.*

That is, an atom has more influence than any other element in the critical set.

Lemma 5 *If A, B are subsets of a critical set $\mathcal{C}$ of a Youden square Y, such that $|A| = |B|$, and suppose that A is crucial but B is not, then $\sigma(B, \mathcal{C}) \leq \sigma(A, \mathcal{C})$.*

So a crucial set has more influence than any other set of the same size.

Theorem 1 *Let A, B, C, D be subsets of a critical set $\mathcal{C}$ of a Youden square Y, with $|A| = |B| = |C| = |D|$. Then:*

1. *If A and B are crucial but C and D are not, and $|A \cap B| = |C \cap D|$ then $\sigma(A \cup B, \mathcal{C}) \geq \sigma(C \cup D, \mathcal{C})$*
2. *If A is crucial but B, C and D are not, and $|A \cap B| = |C \cap D|$ then $\sigma(A \cup B, \mathcal{C}) \geq \sigma(C \cup D, \mathcal{C})$.*

Proof. The proof follows easily from simple set-theoretic arguments. □

Denote by $\psi(a, \mathcal{C})$ the power of an element a in a critical set $\mathcal{C}$, and by $\psi(A, \mathcal{C})$ the power of a subset A of $\mathcal{C}$.

Theorem 2 *If $a \in \mathcal{C}$ is an atom and $x \in \mathcal{C}$ is not an atom, then $\psi(a, \mathcal{C}) \geq \psi(x, \mathcal{C})$.*

That is, an atom has greater power than any other element in the critical set.

We observe that if the shares of the critical set consist of at least two elements, the union of the nests of the shares never contains some elements of the complete rectangle. We say that these elements are in the *strongbox of the critical set.*

If we allow the secret to be some function of the elements in the strongbox whose information content is the same size as each share, we have an *ideal* secret sharing scheme.

In a compartmentalized scheme where shares consist of two elements from the ULHC (or LRHC) we can form:

- m shares which are hybrid pairs and $(m^2 - 3m)/4$ shares which are non-crucial pairs;
- a maximum of $k = \lfloor m/2 \rfloor$ shares consisting of crucial pairs and $m - 2k$ shares consisting of hybrid pairs.

In an hierarchical scheme, shares which consist of a crucial pair have more influence and – it is conjectured – more power than do shares consisting of a hybrid pair, which in turn have more influence than do shares consisting of a non-crucial pair.

Of course, the orders of the rows and orders of the columns of the basic Youden square are permuted before the shares are distributed to hide any kind of patterns, such as back-circulancy.

2.1 Implementing Secret Sharing Schemes

The scheme we give here makes full use of the critical set being comprised of two subsets which appear as disjoint triangles in the pictorial representation of the critical set. It appears likely that in a situation where two (or more) distinct sets of shareholders must be identified these subsets make it very easy to allocate shares to each of the distinct sets. For example, in Australia water from the Murray River is shared between Victoria and New South Wales. For persons living in each of these states being able to ensure their state's votes are all included by the software before water is released from the dam is a politically attractive move. We will call this a *partitioned* secret sharing scheme.

To ensure the strongbox is as large as possible, we would like each share to consist of either a crucial pair or a hybrid pair.

We consider a partitioned scheme and suppose that the critical set is in standard form. Then if each share is chosen with its elements either all in the ULHC or all in the LRHC, then all shareholders with shares from the ULHC (LRHC) must cooperate in order to complete the square and any shareholder with a share from the LRHC (ULHC) can prevent the formation of the secret by withholding just their own share.

So far in this paper we have considered only back-circulant Latin squares. However Cooper, Donovan and Seberry [2], Chaudhry, Peddada and Seberry (unpublished) and Du and Cao [4] have shown many variations of Latin Squares which allow partitions of different size, type and number when $v = pq$. If the portion of a critical set of a partition is in a $q \times q$ subsquare then there can be up to p^2 partitions. The number can be easily

arranged by the dealer (the person distributing the shares). If the number of elements in the critical set is not a multiple of the share size, then shares may be different sizes. However, in general, a smaller share is more vulnerable to being guessed.

Suppose, for example, we use shares which are pairs of elements of the critical set $\mathcal{C}_v$ in standard form. In a 2-partitioned scheme for a Youden square, if we count the number of elements in the first row and column and the last row and column of $\mathcal{C}_v$ in standard form, we find $2v-4$ elements.

This means there are

$$\begin{cases} \dfrac{v^2}{4} - 2v + 4 & = \dfrac{v^2 - 8v + 16}{4}, \quad \text{if } v \text{ is even,} \\ \dfrac{v^2 - 1}{4} - 2v + 4 & = \dfrac{v^2 - 8v + 15}{4}, \quad \text{if } v \text{ is odd,} \end{cases}$$

non-crucial elements in the critical set. Hence for $v \geq 14$ there are more non-crucial than crucial elements. This means that for $v \geq 14$, the strongbox will not have maximum size

$$\begin{cases} \dfrac{3v^2 - 8v + 16}{4} & \text{if } v \text{ is even,} \\ \dfrac{3v^2 - 8v + 17}{4} & \text{if } v \text{ is odd.} \end{cases}$$

As the size of the Youden square increases we recommend that each share should contain one element from each of the first i rows or columns or one element each from the last i rows or columns of the Youden square. Provided i is kept as small as possible the strongbox will be as large as possible. As the size of the square increases the dealer may choose to increase the size of the shares in order to reduce the number of shares. This gives the dealer and the parameters of the secret sharing scheme considerable flexibility.

We shall quantify the size of the strongbox for $v \geq 14$ in a subsequent paper.

We observe that any share which contains an element from the first or last row or column of the square has greater influence than any share not containing a crucial element.

Similarly any share containing an element of the Youden Square's critical set (in standard form) from the ith row or column or the $(v-i)$th row

and $(v+1-i)$th column has greater influence than any share containing an element of the critical set from the $(i+j)$th row or column or the $(v-i-j)$th row and $(v+1-i-j)$th column, $j \geq 1$.

Thus the shares have an inbuilt hierarchy depending on the position of the elements of the share in the normalized form of the critical set.

The dealer has freedom to alter the size of the shares keeping in mind that the size of the strongbox is determined by the position of the least influential share subset.

In the following and subsequent examples we will find it convenient to write shares of a secret in the form

$$e_1 \oplus e_2 \oplus \cdots \oplus e_\ell$$

rather than $\{e_1, e_2, \ldots, e_\ell\}$, for elements e_i of a Youden square.

Example, $v = 9$. Consider the critical set for the Youden square

1	2	3	4	·	·	·	·	·	20
2	3	4	·	·	·	·	·	·	
3	4	·	·	·	·	·	·	·	
4	·	·	·	·	·	·	·	·	
·	·	·	·	·	·	·	·	5	
·	·	·	·	·	·	·	5	6	
·	·	·	·	·	·	5	6	7	
·	·	·	·	·	5	6	7	8	72

Suppose the shares given out in the ULHC are

$$(1,1;1) \oplus (2,2;3), \quad (1,2;2) \oplus (2,3;4), \quad (1,3;3) \oplus (3,2;4),$$
$$(1,4;4) \oplus (2,1;2), \quad (3,1;3) \oplus (4,1;4).$$

Now all these shares are equally influential and if just one of these 5 shareholders does not join a cheating coalition the strongbox cannot be accessed. Now suppose, in the LRHC the shares

$$(8,6;5) \oplus (5,9;5), \quad (8,7;6) \oplus (6,8;6), \quad (8,8;7) \oplus (8,9;8),$$
$$(6,8;5) \oplus (7,9;7), \quad (7,7;5) \oplus (7,8;6),$$

are given out then for this set of shares it requires two shareholders not to join a cheating coalition to protect the strongbox. These means the distribution of shares from the LRHC, in which there is a share not containing any crucial elements is more vulnerable to a cheating coalition. For the scheme with these 10 shares the strongbox has size 33 as the nest of the subsets, which are the shares, will contain the second last row of the square.

In a scheme resistant to cheating coalitions shares may have elements all from the ULHC, all from the LRHC, and some from the ULHC and some from the LRHC. All combinations are permitted. However as we saw in the example some share distributions are more resistant to cheating than others.

Continuing the example: if we use the 7 shares

$$(8,6;5) \oplus (5,9;5) \oplus (2,2;3), \quad (8,7;6) \oplus (6,9;6) \oplus (1,1;1),$$
$$(8,8;7) \oplus (8,9;8) \oplus (1,2;2), \quad (6,8;5) \oplus (7,9;7) \oplus (2,3;4),$$
$$(7,7;5) \oplus (7,8;6) \oplus (1,3;3), \quad (1,4;4) \oplus (2,1;2) \oplus (3,2;4),$$
$$(3,1;3) \oplus (4,1;4),$$

then a single shareholder not joining a cheating coalition protects the strongbox and the strongbox has maximum size 36. □

In this case the last share, being the smallest, is most vulnerable to attack by a coalition of all 6 other shareholders. However, because the last share has elements in the first column, this scheme illustrates the case where, for larger v, it would be computationally infeasible to find this share. Elsewhere we will quantify suitable sizes for v.

3 Implementing Hierarchical Schemes

As we saw with the discussion for the 2-compartmentalized scheme, any share which contains an element from the first or last row or column of the square has greater influence than any share not containing a crucial element.

Similarly any share containing an element of the Youden square's critical set (in standard form) from the ith row or column or the $(v-i)$th row and $(v+1-i)$th column has greater influence than any share containing an element of the critical set from the $(i+j)$th row or column or the $(v-i-j)$th row and $(v+1-i-j)$th column, $j \geq 1$.

Thus the shares have an inbuilt hierarchy depending on the position of the elements of the share in the normalized form of the critical set.

The dealer has freedom to alter the size of the shares keeping in mind that the size of the strongbox is determined by the position of the least influential share subset.

Example, $v = 9$. Consider the critical set for the Youden square

1	2	3	4	·	·	·	·	·	20
2	3	4	·	·	·	·	·	·	
3	4	·	·	·	·	·	·	·	
4	·	·	·	·	·	·	·	·	
·	·	·	·	·	·	·	·	5	
·	·	·	·	·	·	·	5	6	
·	·	·	·	·	·	5	6	7	
·	·	·	·	·	5	6	7	8	72

Suppose the shares given out in the ULHC are

$$(1,1;1) \oplus (2,2;3), \quad (1,2;2) \oplus (2,3;4), \quad (1,3;3) \oplus (3,2;4),$$
$$(1,4;4) \oplus (2,1;2), \quad (3,1;3) \oplus (4,1;4).$$

Now all these shares are equally influential and if just one of these 5 shareholders does not join a cheating coalition the strongbox cannot be accessed. Now suppose, in the LRHC the shares

$$(8,6;5) \oplus (5,9;5), \quad (8,7;6) \oplus (6,8;6), \quad (8,8;7) \oplus (8,9;8),$$
$$(6,8;5) \oplus (7,9;7), \quad (7,7;5) \oplus (7,8;6).$$

are given out then for this set of shares two shareholders not joining a cheating coalition protects the strongbox. For the scheme with these 10 shares the strongbox has size 33 as the nest of the subsets, which are the shares, will contain the second last row of the square.

In a hierarchical scheme shares may have elements all from the ULHC, all from the LRHC, and some from the ULHC and some from the LRHC. All combinations are permitted.

Continuing the example: if we use the 7 shares

$$(8,6;5) \oplus (5,9;5) \oplus (2,2;3), \quad (8,7;6) \oplus (6,9;6) \oplus (1,1;1),$$
$$(8,8;7) \oplus (8,9;8) \oplus (1,2;2), \quad (6,8;5) \oplus (7,9;7) \oplus (2,3;4),$$
$$(7,7;5) \oplus (7,8;6) \oplus (1,3;3), \quad (1,4;4) \oplus (2,1;2) \oplus (3,2;4),$$
$$(3,1;3) \oplus (4,1;4),$$

then a single shareholder not joining a cheating coalition protects the strongbox and the strongbox has maximum size 36. □

In this case the last share, being the smallest, is most vulnerable to attack by a coalition of all 6 other shareholders. However, because the last share has elements in the first column, this scheme illustrates the case where, for larger v, it would be computationally infeasible to find this share. Elsewhere we will quantify suitable sizes for v.

References

[1] Ghulam Chaudhry, Hossein Ghodosi and Jennifer Seberry, *Perfect secret sharing schemes from Room squares,* JCMCC, **28**, (1998), 55–61.

[2] J.Cooper, D.Donovan and J.Seberry, *Latin squares and critical sets of minimal size,* Aust. J. Combinatorics, **4**, (1991), 113–120.

[3] D. Curran and G.H.J. Van Rees, *Critical sets in Latin squares,* in Proc. Eighth Manitoba Conference on Numerical Math. and Computing, 1978, pp. 165–168.

[4] Beiliang Du and Haitao Cao, *Critical sets in $C_3 \times C_n$,* Third Shanghai Conference on Designs, Codes and Finite geometries, Shanghai Jiao Tong University, May 14–18, 1999.

[5] Lakoa Fitina, Kenneth Russell and Jennifer Seberry, *A minimal critical set of a class of Youden squares*, Util. Math., to appear.

[6] Hossein Ghodosi, Josef Pieprzyk and Rei Safavi-Naini, *Secret Sharing in multi level and compartmented groups,* Information and Privacy, eds C Boyd and E Dawson, *LNCS,* Springer-Verlag, Berlin, **1438**, (1998), 367–378.

[7] E.S. Mahmoodian, R. Naserasr and M. Zaker, *Defining sets in vertex colourings of graphs and latin rectangles,* Discrete Math., **167/168** (1997), 451–460.

[8] J. Nelder, *Critical sets in Latin squares,* CSIRO Div. of Math. and Stats, Newsletter, **38**, (1977).

[9] Jennifer Seberry and Anne Penfold Street, *Strongbox secured secret sharing schemes*, Util. Math., **57** (2000), 147–163.

[10] Gustavus J. Simmons, (ed), *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, Piscataway, NJ, 1991.

[11] B. Smetaniuk, *On the minimal critical set of a Latin square,* Util. Math., **16**, (1979), 97–100.

[12] D.R. Stinson and G.H.J. Van Rees, *Some large critical sets,* Congr. Numer., **34**, (1982), 441–456.