1-1-2000

Strongbox Secured Secret Sharing Schemes

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

A. Penfold Street
University of Queensland

Strongbox Secured Secret Sharing Schemes

Abstract

We present one way in which combinatorial designs can be used to give conditionally perfect secret sharing schemes. Schemes formed in this way have the advantage over classical secret sharing schemes of being easily adapted for use as compartmentalized or hierarchical access structures. We study the problem of completion of structures, given partial information, to obtain measures of how closely the behaviour of the secret sharing schemes approaches to ideal behaviour in practice. It may happen that part of a combinatorial design can never be reconstructed from a subset of a minimal defining set. That is, to find the blocks of what is called the strongbox of a given minimal defining set of a design, we must have the whole of the minimal defining set and be able to complete the whole design. The strongbox is that part of the design which may most safely be used to hold secret information. We study the size of the strongbox.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Seberry, J and Penfold-Street, A, Strongbox Secured Secret Sharing Schemes, Utilitas Mathematica, 57, 2000, 147-163. ISSN 0315 3681.

Strongbox Secured Secret Sharing Schemes

Jennifer Seberry*
Centre for Computer Security Research
University of Wollongong
NSW 2522, Australia
j.seberry@uow.edu.au

Anne Penfold Street*
Centre for Discrete Mathematics and Computing
The University of Queensland
Brisbane 4072, Australia
aps@maths.uq.edu.au

Abstract

We present one way in which combinatorial designs can be used to give conditionally perfect secret sharing schemes. Schemes formed in this way have the advantage over classical secret sharing schemes of being easily adapted for use as compartmentalized or hierarchical access structures.

We study the problem of completion of structures, given partial information, to obtain measures of how closely the behaviour of the secret sharing schemes approaches to ideal behaviour in practice.

It may happen that part of a combinatorial design can never be reconstructed from a subset of a minimal defining set. That is, to find the blocks of what is called the *strongbox* of a given minimal defining set of a design, we must have the whole of the minimal defining set and be able to complete the whole design. The strongbox is that part of the design which may most safely be used to hold secret information. We study the size of the strongbox.

Key words and phrases: Combinatorial designs, minimal defining sets, influence, power, nest, strongbox, secret sharing, access schemes.

*Research supported by ARC Grant A49802004

1. Motivation

Computer systems require sophisticated security, best attained when a key or password is shared between several people in such a way that it can only be reconstructed by a sufficiently large and responsible group acting in agreement. Shared security systems are used in banks, in other financial institutions, in communications networks and in computing systems serving educational institutions, though the best-known examples are military: for instance, in the activation of nuclear weapons or missiles, several officers must concur fully before the necessary password can be reconstructed.

Schemes for determining the distribution of the partial information to the people involved are known as *secret sharing schemes* or *access schemes,* and lead to shared control. The pieces of partial information which are distributed are known as *shares* and may be of equal value (as in the military examples mentioned above) or more often of unequal value, probably arranged according to a hierarchy of some kind. For example in a university computing system, shares which lead to the reconstruction of the system manager's or superuser's key are far more valuable than those which lead only to a student's key.

Secret sharing schemes have often been based on constructions from finite geometries [**?**], numerical linear algebra [**?**], the theory of error-correcting codes [**?**] and, more recently, design theory [**?**]. A geometric example is easy to visualise. Suppose that the secret is the combination of a safe, and that it consists of three digits, xyz. We could share the secret between a group of n people by giving each of them the equation of a plane through the point (x, y, z).

- If we choose the planes so that their pairwise intersections give distinct lines through (x, y, z), then any two people can together determine a line through the point and any three can determine the point itself, and hence the combination of the lock. This is an example of a $(3, n)$ *threshold scheme with threshold three,* meaning that any three of the n shares determine the secret, but no two shares determine it.

- Suppose, on the other hand, we choose the planes so that all but one of them have a line, l, say, in common, and the remaining plane, P, intersects l in the point (x, y, z). Then finding the point requires knowledge of the plane P and any two other planes. This means that the agreement of the person who knows P is essential for the determination of the secret, and the scheme is not just a threshold scheme.

Situations where shares of unequal value are used arise often in practice. For example, consider the authorisation of electronic transfer of large amounts of money between financial institutions. One might expect, say, that two vice-presidents could jointly authorise the transfer of amounts over \$10 000 000, two junior vice-presidents amounts between \$1 000 000 and \$10 000 000, two senior tellers amounts between \$100 000 and \$1 000 000 and two tellers lesser amounts. This is in a situation where the appropriate password is never revealed outside the electronic facility (in the bank's head office) which reconstructs the password from the information shares fed into it. What if a vice-president and a junior vice-president are delayed in another city by airport fog?

An obvious solution is to share the authorisation code for transfer of larger amounts of money between larger numbers of more junior staff, but doing this efficiently presents a problem. At present, many access schemes are known and some of them, based on combinatorial designs and finite geometries, have been proved to be the best possible (in a theoretical sense).

2. Designs

A *combinatorial design* is a way of selecting, from a finite set, X, a collection of b subsets which meets certain requirements. These b subsets are usually referred to as the *blocks* of the design. If all the blocks contain the same number, k, of elements and if all the v elements of the underlying set X occur in the same number, r, of blocks, the design is said to be a *block design.* Counting the elements in the design shows that $vr = bk$. A block design in which all pairs of elements occur equally often, say λ times, is said to be *balanced*; counting pairs of elements in the design shows that $\lambda(v-1) = r(k-1)$. Such a design is often referred to as a 2–(v, k, λ) design since the parameters b and r can be calculated from v, k and λ. In particular, a 2-$(v, 3, 1)$ design is called a *Steiner triple system,* often denoted by $STS(v)$. In this paper we are concerned only with *simple* designs, that is, those in which no block is repeated.

As an example, suppose it is required to select from a given set, X, subsets (blocks) containing three elements each, and to select them in such a way that any pair of elements occurs in precisely one block. Thus if we start with the nine-element set $X = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$, then the collection of 12 blocks in any column $\mathcal{D}_i$ of Table 1 fulfils our requirements, forming an $STS(9)$. The boldface numbers in the leftmost column indicate the block numbers in each design. The horizontal lines indicate the partition of the set of blocks of each design into four collections of three pairwise disjoint blocks each, that is, into four parallel classes of blocks which partition the set X. What is more, it can be shown that every $STS(9)$ has essentially the same structure as each $\mathcal{D}_i$.

#	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$
1	123	124	125	126	127	128	129
2	456	389	378	359	368	347	367
3	789	567	469	478	459	569	458
4	147	137	139	138	134	136	135
5	258	259	268	245	269	257	247
6	369	468	457	679	578	489	689
7	159	158	148	149	156	145	146
8	267	236	279	237	248	239	238
9	348	479	356	568	379	678	579
10	168	169	167	157	189	179	178
11	249	278	234	289	235	246	256
12	357	345	589	346	467	358	349

Table 1: Large set of 2-$(9, 3, 1)$ designs

We note that the seven columns of Table 1 give a partition of the set of all $\binom{9}{3}$ triples chosen from the set X into pairwise disjoint 2-$(9, 3, 1)$ designs. Such a partition is known as a *large set* of designs and exists for all $STS(v)$ for $v \neq 7$ [?, ?]. It has been proposed by Stinson and Vanstone [?] as a foundation on which to construct a threshold scheme. Suppose for instance that the secret key is 5 and that it is to be shared among three people. Then they could be given the shares 1, 8 and 9 respectively, the key being the number of the design in which the block 189 appears. Each element occurs four times in each design, so knowing that the design has blocks containing the element '1' is of no advantage to an individual trying to guess the key. Similarly, since each pair occurs once in each design, knowing that the design has a block containing, say, the pair '18' is of no advantage to a pair of shareholders trying to guess the key. But the set of three shares uniquely identifies the design. Since this is true in general, we have a $(3, 3)$ threshold scheme.

Now we concentrate on the design labelled $\mathcal{D}_1$, and more formally, we write $\mathcal{D}_1 = (X, \mathcal{B}_1)$, where $\mathcal{B}_1$ is the set of blocks of the design. Some subsets of the set $\mathcal{B}_1$ have special properties. The set of blocks $\mathcal{S}_{(4)} = \{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{5}\}$ can be completed to a 2-$(9, 3, 1)$ design in only one way, namely to $\mathcal{D}_1$. The same is true of the set $\mathcal{S}_{(5)} = \{\mathbf{1}, \mathbf{4}, \mathbf{5}, \mathbf{7}, \mathbf{11}\}$. Each of these sets is said to be a *defining set* of the design $\mathcal{D}_1$ and, since no proper subset of either set defines $\mathcal{D}_1$ uniquely, each of them is a *minimal* defining set.

On the other hand, the set of blocks $\mathcal{R} = \{\mathbf{1}, \mathbf{2}, \mathbf{5}, \mathbf{7}\}$ can be completed to an $STS(9)$ in two ways, by adjoining the blocks $\{\mathbf{3}, \mathbf{12}\}$, together with *either*

$$\mathcal{T} = \{\mathtt{147}, \mathtt{168}, \mathtt{249}, \mathtt{267}, \mathtt{348}, \mathtt{369}\}$$

to give the design $\mathcal{D}_1$ as before, *or*

$$\mathcal{T}' = \{\mathtt{148}, \mathtt{167}, \mathtt{247}, \mathtt{269}, \mathtt{349}, \mathtt{368}\}$$

to give a new design $\mathcal{D}_1'$. Then $\mathcal{T}$ and $\mathcal{T}'$ form a *trade* in the design; that is, the set of blocks $\mathcal{T}$ can be removed from the design $\mathcal{D}_1$ and replaced by the set $\mathcal{T}'$ to give a different design with the same parameters. Since no subset of $\mathcal{T}$ can be traded to give an $STS(9)$, they form a *minimal* trade.

Every defining set and every trade within a design must have at least one common block, and the automorphism group of a defining set is a subgroup of the automorphism group of the design; see K Gray [**?**, **?**, **?**]. These properties have been essential in the development of algorithms for finding minimal defining sets; see Greenhill [**?**], Delaney [**?**]. In finding fast algorithms that complete a design from a given partial design, block intersection patterns have been important, especially linkage; see Ramsay [**?**], Utami [**?**], Lawrence [**?**].

3. Secret Sharing Schemes

We are studying the problem of completion of structures, given partial information, to obtain measures of how closely the behaviour of a secret sharing scheme approaches to ideal behaviour in practice. This allows comparison of the information content of the partial structure with that of the complete structure [**?**]. In particular if the partial structure can be uniquely completed then it, together with the rules for completion, contains the same information as the entire structure.

Even for small orders the number of inequivalent combinatorial designs grows extremely rapidly. Here this feature becomes a strength, since the choice of parameters for which there are a very large number of inequivalent designs makes the secret sharing scheme more secure.

As our model, we take a situation in which the group of participants includes a dealer (or trusted authority), as well as the shareholders.

- In the **distribution phase**, the dealer chooses a 2-(v, k, λ) design, with suitable parameters, for which a (preferably minimal) defining set is known. A permutation is applied to the set of elements underlying the design, thus relabelling the elements of each blockto hide any structural information. Each participant (except the dealer) is given a suitable size share, consisting of one or more whole blocks. Note that no shareholder needs to know the parameters of the design.

- In the **combination phase**, each shareholder presents the given share to the combiner, who completes the design and hence determines the key, by using the shares, the permutation, the parameters v, k and λ, the rules for completion and an algorithm for completion. In the scheme we are proposing, the key will be contained in the *strongbox* or part of the design most difficult to reconstruct from partial information; the strongbox is defined formally in Section 4.

If a unique design is reconstructed, then each shareholder can feel confident that the others are who they say they are (a matter of mutual authentication) and that the secret is as intended. *If the design cannot be reconstructed*, then *either* someone has made a mistake *or* someone is trying to cheat. How easily can an unauthorised group of shareholders cheat?

In an ideal situation, we assume that no shareholder knows any of the following:

[A1] parameters of the design;

[A2] size of the defining set being used;

[A3] the permutation being applied to the elements.

But if there is any suspicion of cheating, it is prudent to assume that the coalition of cheaters know all of the following:

[C1] parameters of the design;

[C2] which of the inequivalent designs is being used;

[C3] which of the inequivalent permutations is being used;

[C4] all but one of the shares, and if the shares have varying properties, that the missing share is one of those with the least power.

We also *always* assume that an opponent has unlimited resources to attack the scheme. In the next section, we look at several small examples of designs and see what can be discovered about them when only part of a defining set is known.

4. Partial Defining Sets of Designs

A minimal defining set, $\mathcal{S}$, of a design $\mathcal{D}$ provides a small amount of data from which $\mathcal{D}$ can be reconstructed uniquely. Analogous subsets of Latin squares are called *critical.* These were first studied in connection with a problem at Rothamsted Experimental Station; see Nelder [**?**]. Any combinatorial structures which have rules for completion may be used to construct secret sharing schemes.

In particular we are concerned here with the problem of uniquely completing a 2-(v, k, λ) block design given a proper subset of its set of blocks $\mathcal{B}$. This is of interest in comparing the information content of the partial data with that of the whole design. A proper subset of $\mathcal{B}$ which can be uniquely completed must, together with the rules for completion, contain the same information as the whole design.

We study the information inherent in proper subsets of $\mathcal{B}$ completable to at least two distinct designs, and in the minimal defining sets of such designs. Our approach is related to that of Fitina, Seberry and Chaudhry [**?**] for Latin squares.

Let $\mathcal{S}$ be a defining set of a design $\mathcal{D} = (X, \mathcal{B})$ and let $B \in \mathcal{B}$ be a block of $\mathcal{S}$. We make the following definitions, using the term 'collection', as oppposed to 'set', when repeated objects may occur. However in our small examples multiple blocks and multiple partial blocks do not arise.

Nest: $\mathcal{N}(\mathcal{S}, B)$, the nest of B in $\mathcal{S}$, is the set of blocks of $\mathcal{S} \setminus \{B\}$, together with all the complete and partial blocks forced by the presence of $\mathcal{S} \setminus \{B\}$. More precisely, we write

$$\mathcal{N}(\mathcal{S}, B) = (\mathcal{S} \setminus \{B\}) \cup \mathcal{N}' \cup \mathcal{N}''$$

where $\mathcal{N}'$ and $\mathcal{N}''$ are, respectively, the collection of complete blocks forced by $\mathcal{S} \setminus \{B\}$, and the collection of partial blocks forced by $\mathcal{S} \setminus \{B\}$ excluding those partial blocks of t or fewer elements since these are already forced by the parameters of the design.

Power: $\mathcal{P}(\mathcal{S}, B)$, the power of B in $\mathcal{S}$, is the number of completions of $\mathcal{S} \setminus \{B\}$ to a design with the parameters of $\mathcal{D}$.

Influence: $\mathcal{I}(\mathcal{S}, B)$, the influence of B in $\mathcal{S}$, is the number of complete blocks in the design $\mathcal{D}$ which are *not* forced when the rules for completion are applied to $\mathcal{S} \setminus \{B\}$.

Strongbox: $\mathbf{S}(\mathcal{S})$, the strongbox of $\mathcal{S}$, is the set of complete blocks of $\mathcal{B}$ not contained in the nest of any block of $\mathcal{S}$; that is, the set of blocks which cannot be found from any proper subset of the minimal defining set $\mathcal{S}$ of $\mathcal{D}$.

In order to test the suitability of a defining set S to be used for a secret sharing scheme we need to assess how easy it is for an attacker to guess the design from partial information.

We consider three small examples, each with $t = 2$. In Example 1, $t = k - 1$; in Examples 2 and 3, $t < k - 1$. In Examples 1 and 2, $\lambda = 1$; in Example 3, $\lambda = 2$. In Example 1, the smallest defining set (4 blocks) has a strongbox of 6 blocks but the other minimal defining set (5 blocks) has a strongbox of only one block. In Example 2, the two smallest defining sets have six blocks each, but one has a strongbox of three blocks and the other of only one block. In Example 3, the two smallest defining sets have five blocks each and each has a strongbox consisting of one block.

We note that the designs of Examples 1 and 2 are related, in that the first is a residual of the second. However we have been unable to relate the behaviour of their defining sets.

Example 1

Suppose we wish to recreate the 2-$(9,3,1)$ design $\mathcal{D}_1$, given that the parameters are known, from one of the minimal defining sets $\mathcal{S}_{(4)}$ and $\mathcal{S}_{(5)}$. This is the affine plane of order 3.

Table 2 shows the blocks of $\mathcal{S}_{(4)}$, the triples in their nests, and the pairs still required to complete the design, where $\pi(\mathbf{x})$ denotes the set of pairs covered by the block $\mathbf{x}$. Each block in $\mathcal{S}_{(4)}$ has power 4, and influence 8. Thus knowing three of the four blocks in the defining set gives a 1 in 4 chance of finding the correct design. The strongbox of $\mathcal{S}_{(4)}$ is $\mathbf{S}(\mathcal{S}_{(4)}) = \{\mathbf{7},\mathbf{8},\mathbf{9},\mathbf{10},\mathbf{11},\mathbf{12}\}$. This shows the possibility of having a strongbox bigger than the original defining set.

B	$\mathcal{N}'(\mathcal{S}_{(4)},B)$	$\mathcal{N}''(\mathcal{S}_{(4)},B)$	Pairs still needed
1	**6**	$\emptyset$	$\pi(\mathbf{1},\mathbf{3},\mathbf{7},\mathbf{8},\mathbf{9},\mathbf{10},\mathbf{11},\mathbf{12})$
2	**6**	$\emptyset$	$\pi(\mathbf{2},\mathbf{3},\mathbf{7},\mathbf{8},\mathbf{9},\mathbf{10},\mathbf{11},\mathbf{12})$
4	**3**	$\emptyset$	$\pi(\mathbf{4},\mathbf{6},\mathbf{7},\mathbf{8},\mathbf{9},\mathbf{10},\mathbf{11},\mathbf{12})$
5	**3**	$\emptyset$	$\pi(\mathbf{5},\mathbf{6},\mathbf{7},\mathbf{8},\mathbf{9},\mathbf{10},\mathbf{11},\mathbf{12})$

Table 2: Properties of $\mathcal{S}_{(4)}$ in design $\mathcal{D}_1$

Table 3 shows the analogous information for $\mathcal{S}_{(5)}$, using the notation $\pi(\mathbf{x})$ as before. Each block in $\mathcal{S}_{(5)}$ has power 2, and influence 6. Thus knowing four of the five blocks in the defining set gives a 1 in 2 chance of finding the correct design. The strongbox of $\mathcal{S}_{(5)}$ is $\mathbf{S}(\mathcal{S}_{(\mathbf{5})}) = \{\mathbf{2}\}$. Since **2** consists of the elements `4,5,6`, this might for example be used to store the combination of a lock.

B	$\mathcal{N}'(\mathcal{S}_{(5)},B)$	$\mathcal{N}''(\mathcal{S}_{(5)},B)$	Pairs still needed
1	**3, 6**	$\emptyset$	$\pi(\mathbf{1},\mathbf{2},\mathbf{8},\mathbf{9},\mathbf{10},\mathbf{12})$
4	**8, 9**	$\emptyset$	$\pi(\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{6},\mathbf{10},\mathbf{12})$
5	**10, 12**	$\emptyset$	$\pi(\mathbf{2},\mathbf{3},\mathbf{5},\mathbf{6},\mathbf{8},\mathbf{9})$
7	**6, 8**	$\emptyset$	$\pi(\mathbf{2},\mathbf{3},\mathbf{7},\mathbf{9},\mathbf{10},\mathbf{12})$
11	**6, 10**	$\emptyset$	$\pi(\mathbf{2},\mathbf{3},\mathbf{8},\mathbf{9},\mathbf{11},\mathbf{12})$

Table 3: Properties of $\mathcal{S}_{(5)}$ in design $\mathcal{D}_1$

No secret sharing scheme in which a block of a design is given to a shareholder is perfect. For example, on a given set of 9 elements, there are 840 2-(9,3,1) designs, but if one block is specified, only 120 of these are possible. The strongbox tells us the portion of the design with regard to which the scheme is conditionally perfect.

In this example, $t = k - 1$, so the maximal partial blocks forced by the subsets of minimal defining sets are always t-sets, that is, in this case, pairs. Thus $\mathcal{N}'' = \emptyset$. Also, since $\lambda = 1$, $\mathcal{N}'$ is always a set.

Example 2

Consider the $2\text{-}(13, 4, 1)$ design, unique to isomorphism; this is the projective plane of order 3, isomorphic to an extension of $\mathcal{D}_1$. The quartic residues modulo 13, together with `0`, form a starter block for the design $\mathcal{P}$; that is, $P = \{\mathtt{0}, \mathtt{1}, \mathtt{3}, \mathtt{9}\}$ is taken as the first block, and the remaining blocks formed by addition modulo 13. Letting `A, B, C` respectively denote `10, 11, 12`, we have $\mathbf{1} = P$, $\mathbf{2} = P + \mathtt{1} =$ `124A`, $\mathbf{3} = P + \mathtt{2} =$ `235B` and so on, till $\mathbf{0} = P + \mathtt{C} =$ `C028`. This design is *symmetric*; that is, it has $b = v$ and consequently also $r = k$. Its smallest defining sets have 6 blocks each [**?**].

B	$\mathcal{N}'(\mathcal{S}_{(c)}, B)$	$\mathcal{N}''(\mathcal{S}_{(c)}, B)$	$K_{2,9}$
1	**9,A**	**1B0** $\setminus$ `0`; **78C** $\setminus$ `7`	`(0,7; 1,2,3,6,8,9,A,B,C)`
2	**8,A**	**270** $\setminus$ `2`; **9BC** $\setminus$ `B`	`(2,B; 1,4,6,7,8,9,A,C,0)`
3	**9,C**	**370** $\setminus$ `2`; **8AB** $\setminus$ `A`	`(2,A; 3,5,6,7,8,9,B,C,0)`
4	**A,C**	**47B** $\setminus$ `6`; **890** $\setminus$ `8`	`(6,8; 2,3,4,7,9,A,B,C,0)`
5	**8,C**	**5B0** $\setminus$ `0`; **79A** $\setminus$ `9`	`(9,0; 2,4,5,6,7,8,A,B,C)`
6	**8,9**	**67B** $\setminus$ `6`; **AC0** $\setminus$ `C`	`(6,C; 1,2,5,7,8,9,A,B,0)`

Table 4: Properties of $\mathcal{S}_{(c)}$ in design $\mathcal{P}$

In a $2\text{-}(v, k, 1)$ design, the set of all the blocks which do *not* contain some fixed element form a defining set [**?**]. In this particular case, six of the nine such blocks form a smallest defining set, such as $\mathcal{S}_{(8)} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{7}\}$ which omits the element `8`. The only other smallest defining set is isomorphic to $\mathcal{S}_{(c)} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}\}$ consisting of six consecutive blocks.

Table 4 shows the blocks of $\mathcal{S}_{(c)}$, the blocks and partial blocks in their nests, and the pairs still needed in the completion to a design with the parameters of $\mathcal{P}$. In describing triples in the nest of block $\mathbf{1}$, for instance, we use the notation $\mathbf{1B0} \setminus \mathtt{0}$ to mean that from each of the blocks **1, B** and $\mathbf{0}$, we delete the element 0, leaving the triples 139, 6AB and 28C in $\mathcal{N}''(\mathcal{S}_{(c)}, \mathbf{1})$. The rightmost column shows the pairs still needed; since they happen to form a copy of the complete bipartite graph $K_{2,9}$ we show only the labels of the two parts of this graph. Each block of this defining set has power 2 and influence 6, and the strongbox consists of three blocks, $\mathbf{S}(\mathcal{S}_{(\mathbf{c})}) = \{\mathbf{7}, \mathbf{B}, \mathbf{0}\}$.

B	$\mathcal{N}'(\mathcal{S}_{(8)}, B)$	$\mathcal{N}''(\mathcal{S}_{(8)}, B)$	$K_{2,9}$
1	**9,0**	$\mathbf{16C} \setminus \mathtt{1}; \mathbf{8AB} \setminus \mathtt{A}$	(1,A; 3,5,6,7,8,9,B,C,0)
2	**8,C**	$\mathbf{690} \setminus \mathtt{8}; \mathbf{2AB} \setminus \mathtt{A}$	(8,A; 1,2,4,5,6,9,B,C,0)
3	**9,A**	$\mathbf{680} \setminus \mathtt{8}; \mathbf{3BC} \setminus \mathtt{B}$	(8,B; 1,2,3,5,6,7,A,C,0)
4	**B,0**	$\mathbf{689} \setminus \mathtt{8}; \mathbf{4AC} \setminus \mathtt{C}$	(8,C; 1,3,4,5,6,7,9,A,B)
5	**8,0**	$\mathbf{56A} \setminus \mathtt{5}; \mathbf{9BC} \setminus \mathtt{B}$	(9,0; 2,4,5,6,7,8,A,B,C)
7	**8,9**	$\mathbf{67B} \setminus \mathtt{6}; \mathbf{AC0} \setminus \mathtt{C}$	(6,C; 1,2,5,7,8,9,A,B,0)

Table 5: Properties of $\mathcal{S}_{(8)}$ in design $\mathcal{P}$

Table 5 shows the blocks of $\mathcal{S}_{(8)}$, the blocks and partial blocks in their nests, and the pairs still needed in the completion to a design with the parameters of $\mathcal{P}$. We use the same notation as in Table 4 for listing the triples and pairs. Again each block of the defining set has power 2 and influence 6, but now the strongbox consists of only one block, $\mathbf{S}(\mathcal{S}_{(\mathbf{8})}) = \{\mathbf{6}\}$.

Here we have an example where, although power and influence of blocks in each defining set are the same, the nests in each case contain six triples, and the pairs still needed for completion correspond to the 18 edges of $K_{2,9}$, the strongboxes are of quite different sizes. In either case however, knowing five of the six blocks of a smallest defining set gives us a 1 in 2 chance of finding the correct design.

Example 3

Consider the 2-$(11, 5, 2)$ design, unique to isomorphism. The quadratic residues modulo 11 form a starter block for the design $\mathcal{Q}$; that is, $Q = \{\mathtt{1}, \mathtt{3}, \mathtt{4}, \mathtt{5}, \mathtt{9}\}$ is taken as the first block, and the remaining blocks formed by addition modulo 11. Letting A denote 10, we have $\mathbf{1} = Q$, $\mathbf{2} = Q + \mathtt{1} =$

$\texttt{2456A}$, $\mathbf{3} = Q + 2 = \texttt{35670}$ and so on, till $\mathbf{0} = Q + \texttt{A} = \texttt{02348}$. This design is also symmetric and its smallest defining set has 5 blocks [**?**, **?**].

In a symmetric 2-$(v, k, 2)$ design, the set of all the blocks which do *not* contain some fixed element form a defining set [**?**]. In this particular case, any five of the six such blocks form a smallest defining set [**?**]. We consider the set $\mathcal{C}_0$ of blocks which do not contain the element $\texttt{0}$, that is, the set of blocks $\{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \mathbf{A}\} = \mathcal{C}_0$.

Table 6 shows what portions of the design can be completed from any of the 15 sets of four blocks at a time which can be chosen from $\mathcal{C}_0$. For instance, given any of the sets $\{\mathbf{1},\ \mathbf{2},\ \mathbf{4},\ \mathbf{5}\}$ or $\{\mathbf{4},\ \mathbf{5},\ \mathbf{6},\ \mathbf{A}\}$ or $\{\mathbf{1},\ \mathbf{2},\ \mathbf{6},\ \mathbf{A}\}$, completion forces one extra whole block, **9**, and six partial blocks, each of which contains four elements. In the partial blocks, either $\texttt{7}$ or $\texttt{8}$ must be added as shown to give a complete block, and choosing $\texttt{7}$ or $\texttt{8}$ in any one case forces the rest of the design. Thus there are two possible completions of the set $\{\mathbf{1},\ \mathbf{2},\ \mathbf{4},\ \mathbf{5}\}$: choosing the first option to complete each partial block gives the original design; choosing the second option gives the design

$$\{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{5}, \mathbf{9}\} \cup \{\texttt{123A8}, \texttt{35608}, \texttt{49A08}, \texttt{369A7}, \texttt{15A07}, \texttt{23407}\}.$$

For each smallest defining set contained in $\mathcal{C}_0$, the power of each block is 2 since two completions are possible in each case; similarly since six blocks are not forced in each completion, the influence of each block is 6. Thus knowing any four blocks of $\mathcal{C}_0$ gives us a 1 in 2 chance of finding the correct design.

In this case, we can regard the set $\mathcal{C}_0 \setminus \{\mathbf{A}\}$ as a defining set $\mathcal{S}_1$, the set $\mathcal{C}_0 \setminus \{\mathbf{6}\}$ as a defining set $\mathcal{S}_2$ and the set $\{\mathbf{1},\ \mathbf{2},\ \mathbf{4},\ \mathbf{5}\}$ as either $\mathcal{S}_1 \setminus \{\mathbf{6}\}$ or $\mathcal{S}_2 \setminus \{\mathbf{A}\}$. Then in our previous notation, $\mathcal{N}'(\mathcal{S}_1, \mathbf{6}) = \mathcal{N}'(\mathcal{S}_2, \mathbf{A}) = \mathbf{9}$, and

$$\begin{aligned}
&\mathcal{N}''(\mathcal{S}_1, \mathbf{6}) = \mathcal{N}''(\mathcal{S}_2, \mathbf{A}) = \\
&\qquad \{\texttt{123A}, \texttt{3560}, \texttt{49A0}, \texttt{369A}, \texttt{15A0}, \texttt{2340}\} \cup \\
&\qquad \{\texttt{3A7}, \texttt{1A7}, \texttt{237}, \texttt{367}, \texttt{507}, \texttt{307}, \texttt{9A7}, \texttt{A07}, \texttt{407}\} \cup \\
&\qquad \{\texttt{3A8}, \texttt{368}, \texttt{9A8}, \texttt{1A8}, \texttt{508}, \texttt{A08}, \texttt{238}, \texttt{308}, \texttt{408}\}.
\end{aligned}$$

Now regard the set $\{\mathbf{1},\ \mathbf{2},\ \mathbf{4},\ \mathbf{5}\}$ as $\mathcal{S}_1 \setminus \{\mathbf{6}\}$. To find the strongbox of $\mathcal{S}_1 = \{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{5}, \mathbf{6}\}$, note that the only block neither in the set $\mathcal{S}_1$, nor forced by any of its 4-block subsets, is the block **A**; hence $\mathbf{S}(\mathcal{S}_1) = \{\mathbf{A}\}$. Similarly, $\mathbf{S}(\mathcal{S}_2) = \{\mathbf{6}\}$.

Given blocks	$\mathcal{N}'$	Completions		
1, 2, 4, 5	**9**	123A[78],	3560[78],	49A0[78]
		369A[87],	15A0[87],	2340[87]
4, 5, 6, A		1459[3A],	5670[3A],	2480[3A]
		2456[A3],	1580[A3],	4790[A3]
1, 2, 6, A		2789[45],	3670[45],	18A0[45]
		1678[54],	2380[54],	79A0[54]
1, 2, 4, 6	**8**	127A[39],	5670[39],	2480[39]
		2578[93],	47A0[93],	1260[93]
1, 5, 6, A		456A[27],	3480[27],	1690[27]
		3560[72],	49A0[72],	1468[72]
2, 4, 5, A		79A0[46],	1359[46],	2380[46]
		389A[64],	3570[64],	1290[64]
1, 2, 4, A	**3**	3480[2A],	5789[2A],	1690[2A]
		4790[A2],	3689[A2],	1580[A2]
1, 4, 5, 6		256A[14],	79A0[14],	2380[14]
		2690[41],	237A[41],	58A0[41]
2, 5, 6, A		15A0[89],	1467[89],	2340[89]
		1345[98],	47A0[98],	1260[98]
1, 2, 5, 6	**0**	1478[6A],	3570[6A],	1290[6A]
		1580[A6],	4790[A6],	1237[A6]
1, 4, 5, A		3670[59],	246A[59],	18A0[59]
		368A[95],	47A0[95],	1260[95]
2, 4, 6, A		3459[17],	2690[17],	58A0[17]
		3560[71],	49A0[71],	2589[71]
1, 2, 5, A	**7**	58A0[13],	2690[13],	4678[13]
		5670[31],	689A[31],	2480[31]
2, 4, 5, 6		18A0[25],	1349[25],	3670[25]
		3480[52],	137A[52],	1690[52]
1, 4, 6, A		1290[68],	245A[68],	3570[68]
		2579[86],	15A0[86],	2340[86]

Table 6: 2-$(11, 5, 2)$ design completions from four blocks of $\mathcal{C}_0$

The other smallest defining set (up to isomorphism) of this design consists of any four blocks containing one particular element, together with any block not containing it. We consider here the defining set $\mathcal{S}_5 = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$ in which all the blocks except **4** contain the element 5. Table 7 shows information corresponding to that of Table 6, for the blocks **1, 2, 3** and **5**; in fact, that for block **3** repeats the first line of the previous table so we need not recalculate $\mathcal{N}''$.

Given blocks	$\mathcal{N}'$	Completions		
2, 3, 4, 5	**0**	127A[30], 1269[03],	1459[30], 158A[03],	689A[30] 479A[03]
1, 3, 4, 5	**6**	2380[41], 2690[14],	79A0[41], 58A0[14],	256A[41] 237A[14]
1, 2, 4, 5	**9**	3560[78], 15A0[87],	49A0[78], 2340[87],	123A[78] 369A[87]
1, 2, 3, 4	**A**	1690[2A], 1580[A2],	0348[2A], 4790[A2],	5789[2A] 3689[A2]

Table 7: 2-$(11, 5, 2)$ design completions from four blocks of $\mathcal{S}_5$

Block **4** behaves rather differently: the set $\{\mathbf{1},\ \mathbf{2},\ \mathbf{3},\ \mathbf{5}\}$ forces the additional complete block $\mathbf{8} = \mathcal{N}'(\mathcal{S}_5, \mathbf{4})$; the two possible completions are *either* the original design $\mathcal{Q}$ containing the blocks

$$\mathcal{U} = \{\mathtt{3689A}, \mathtt{14678}, \mathtt{1237A}, \mathtt{479A0}, \mathtt{23480}, \mathtt{12690}\}$$

or a new design $\mathcal{Q}'$ containing the blocks

$$\mathcal{U}' = \{\mathtt{12470}, \mathtt{239A0}, \mathtt{46890}, \mathtt{12368}, \mathtt{1679A}, \mathtt{3478A}\}.$$

This ordering shows the blocks in $\mathcal{U}$ and $\mathcal{U}'$ as disjoint pairs, but to calculate $\mathcal{N}''$ we need to look at intersections. This time $\mathcal{N}''$ contains no partial blocks of size 4, but instead consists of 30 triples:

$$\begin{aligned}
&\mathcal{N}''(\mathcal{S}_5, \mathbf{4}) = \\
&\qquad \{\mathtt{39A}, \mathtt{689}, \mathtt{368}, \mathtt{69A}, \mathtt{38A}, \mathtt{147}, \mathtt{468}, \mathtt{168}, \mathtt{167}, \mathtt{478}\} \cup \\
&\qquad \{\mathtt{127}, \mathtt{23A}, \mathtt{123}, \mathtt{17A}, \mathtt{37A}, \mathtt{470}, \mathtt{9A0}, \mathtt{490}, \mathtt{79A}, \mathtt{47A}\} \cup \\
&\qquad \{\mathtt{240}, \mathtt{230}, \mathtt{480}, \mathtt{238}, \mathtt{348}, \mathtt{120}, \mathtt{290}, \mathtt{690}, \mathtt{126}, \mathtt{169}\}.
\end{aligned}$$

These triples form a partially balanced block design, in which each pair of elements chosen from the set {`1, 2, 3, 4, 6, 7, 8, 9, A, 0`} appears in either four triples (for 15 pairs) or one triple (for the remaining 30 pairs).

Again the power of each block in $\mathcal{S}_5$ is 2, and its influence is 6, so as before, knowing four of the five blocks of this defining set gives a 1 in 2 chance of finding the correct design. The strongbox $\mathbf{S}(\mathcal{S}_5) = \{\mathbf{7}\}$. However, a 4-element subset of the block **7** appears in each of the nests of $\mathcal{S}_5$ for the blocks **1, 2, 3** or **5**, and five 3-element subsets of **7** for the block **4**, suggesting, first, that perhaps this strongbox is not particularly secure and, secondly, that we should also consider the use of partial blocks in a defining set.

We note that, if we consider the block numbers as the elements of a dual design, then the 66 sets of five blocks which are not defining sets of the design $\mathcal{Q}$ form a 4-$(11, 5, 1)$ design.

5. Further Questions

The examples discussed above have been chosen to illustrate the concepts of nest, power, influence and strongbox, but are far too small for practical use. We are now investigating similar structures in larger designs, with a view to determining their suitability for realistic applications.

References

[1] M Bertilson and I Ingemarsson, *A construction of practical secret sharing schemes using linear block codes,* Proceedings of AUSCRYPT'92, LNCS **718** 67–69, Springer–Verlag (1993).

[2] G R Blakley, *Safeguarding cryptographic keys,* Proceedings of NCC, AFIPS Conference Proceedings **48** 313–317 (1979).

[3] Cathy Delaney, Martin J Sharry and Anne Penfold Street, *bds* – Rationale and User's Guide, CCRR-02-96, Centre for Combinatorics, Department of Mathematics, The University of Queensland, Brisbane, Australia, 1996.

[4] L F Fitina, Jennifer Seberry and Ghulam R Chaudhry, *Back Circulant Latin squares and the influence of a set,* Australasian Journal of Combinatorics **20** (1999), 163–180.

[5] Ken Gray, *On the minimum number of blocks defining a design,* Bulletin of the Australian Mathematical Society **41** (1990), 97–112.

[6] Ken Gray, *Further results on smallest defining sets of well-known designs,* Australasian Journal of Combinatorics **1** (1990), 91–100.

[7] Ken Gray, *Defining sets of single-transposition-free designs,* Utilitas Mathematica **38** (1990), 97–103.

[8] Catherine S Greenhill, *An algorithm for finding smallest defining sets of t–designs,* Journal of Combinatorial Mathematics and Combinatorial Computing **14** (1993), 39–60.

[9] Catherine S Greenhill and Anne Penfold Street, *Smallest defining sets of some small t–designs and relations to the Petersen graph,* Utilitas Mathematica **48** (1995), 5–31.

[10] Julie L Lawrence, personal communication to Anne Penfold Street, 1999.

[11] Lu Jia–Xi, *On large sets of Steiner triple systems I–VI*, Journal of Combinatorial Theory (A) **34** (1983), 140–146, 147–155, 156–182; **37** (1984), 136–163, 164–188, 189–192.

[12] John Nelder, *Critical sets in Latin squares*, CSIRO Division of Mathematics and Statistics Newsletter **38** (1977).

[13] Colin Ramsay, *An algorithm for completing partials, with an application to the smallest defining sets of the STS(*15*)*, Utilitas Mathematica **52** (1997), 205–221.

[14] Jennifer Seberry, *Secret sharing and group identification*, Research and Development Studies, Stage 3 report from the Centre for Computer and Communications Security Research to Telecom Australia (June 1990).

[15] Jennifer Seberry, *On small defining sets for some SBIBD(*$4t-1,\ 2t-1,\ t-1$*),* Bulletin of the Institute of Combinatorics and its Applications **4** (1992), 58-62.

[16] A Shamir, *How to share a secret,* Communications of the Association for Computing Machinery **22**(11) (1979), 612–613.

[17] P J Schellenberg and D R Stinson, *Threshold schemes from combinatorial designs,* Journal of Combinatorial Mathematics and Combinatorial Computing **5** (1989), 143–160.

[18] D.R.Stinson and S.A.Vanstone, *A combinatorial approach to threshold schemes*, SIAM Journal of Discrete Mathematics **1** (1988), 230–236.

[19] Luc Teirlinck, *A completion of Lu's determination of the spectrum for large sets of disjoint Steiner triple systems*, Journal of Combinatorial Theory (A) **57** (1991), 302–305.

[20] Juliati Utami, *Algebraic Completions of SBIBDs*, M.Sc.(Hons) Thesis, University of Wollongong, 1999.