Secret Sharing Schemes Arising From Latin Squares

Joan Cooper*
Department of Information and Communication Technology
University of Wollongong
Wollongong, 2500, Australia

Diane Donovan†
Centre for Combinatorics
Mathematics Department
The University of Queenland
Brisbane, 4072, Australia

Jennifer Seberry‡
Computer Science Department
University of Wollongong
Wollongong, 2500, Australia

ABSTRACT. A critical set in a latin square is a partial latin square which has a unique completion. In this paper we demonstrate how critical sets can be used in the design of secret sharing schemes.

1. Introduction

In information based systems, the integrity of the information is commonly provided for by requiring that certain operation(s) can be carried out only by one or more participants who have access rights. Access is gained through a key, password or token, and governed by a secure key management scheme. If the key or password is shared between several participants in such a way that it can be reconstructed only by a sufficiently

*Supported by ARC Grant no. S6600306.
†Supported by ARC Grant no. 92 421420660000 and a Postdoctoral Fellowship at the Queensland University of Technology.
‡Supported by Telecom Grant no. 7027 and ARC Grant no. A49130102.

large and responsible group acting in agreement, then a high degree of security is attained. Shared security systems, of this sort, are also used in financial institutions, in communication networks, in computing systems serving educational institutions and distribution environments. However the best known examples of applications of shared security systems are in the military: For instance, in activating a nuclear weapon, several senior officers must concur before the necessary password can be reconstructed. Shared secret schemes were first introduced by Blakley [2], Shamir [14], and Chaum [4], in 1979, and subsequently have been studied by numerous other authors. For a general discussion of shared secret schemes see Simmons [16]. A number of mathematical structures have been used to model shared secret schemes. Some of these are polynomials, geometric configurations, block designs, Reed–Solomon codes, vector spaces, matroids, near–right fields, complete multipartite graphs and orthogonal arrays.

In most real–world applications there is also a need for a hierarchy to be built into the shared security system. That is, the key and password is shared between s individuals of rank $1, \ldots, r$ so that if a person of rank i is incapacitated, then a person of rank $j \geq i$, or a set of individuals of rank $l < i$, may replace the lost data. Brickell [3], Simmons [15] and [16], and Beutelspacher [1], have adapted the basic schemes and constructed multilevel systems. In this paper, we will show how general shared secret schemes can be modeled on latin squares and demonstrate how these can be adapted to realize multilevel schemes.

A *secret sharing scheme* is a method whereby n pieces of information called *shares* or *shadows* are assigned to a secret key K. The shares have the property that certain authorized groups of shares can be used to reconstruct the secret key. The secret cannot be reconstructed from an unauthorized group of shares. The recipients of the shares are called the *participants* in the scheme. The set of participants is denoted by $\mathcal{P}$. We let l denote the number of participants in the scheme; that is, $|\mathcal{P}| = l$. The *access structure* or *concurrence scheme*, Γ, of a secret sharing scheme is a subset of the power set of $\mathcal{P}$. The elements of the access structure are the authorized groupings of participants whose shares can be used to reconstruct the secret. An access structure is said to be *monotone* if for any subsets B and C of $\mathcal{P}$, where $B \subseteq C$ and $B \in \Gamma$, then $C \in \Gamma$. If, in a secret sharing scheme, the access structure is the set $\Gamma = \{A \subseteq \mathcal{P} \mid t \leq |A|\}$, then the secret sharing scheme is said to be a t–out–of–l secret sharing scheme. A *t–out–of–l secret sharing scheme* is a method where by l pieces of information called *shares* or *shadows* in a secret key K are distributed in such a way that

- the secret can be reconstructed from knowledge of any t or more shares, and
- it cannot be reconstructed from knowledge of fewer than t shares.

Such secret sharing schemes are said to be simple and referred to as *t–out–of–l threshold schemes* (or (t, l)*–threshold schemes*) with *threshold* t. A secret sharing scheme is said to be perfect if a participant, or an unauthorized group of participants, has no advantage in guessing the secret over an outsider. Therefore a t–out–of–l secret sharing scheme is *perfect* if

- knowledge of fewer than t shares provides no information about K.

There is a definite need, particularly in the commercial arena, to develop multilevel schemes in which the participants have differing capabilities when reconstructing the secret. In an *intrinsic* scheme the capabilities of the participants when reconstructing the secret are a function of the information content of the shares. In such schemes, two or more shares may be assigned to one participant. However, this increases the complexity of the shares and so decreases the ability of a participant to handle the shares securely. In an *extrinsic* scheme the participants' differing capabilities when reconstructing the secret are a function of the relationship between the shares and not a function of the information content of the shares. We deal only with extrinsic schemes and give the following formal definition of a multilevel scheme. In a *multilevel* or *hierarchical scheme* the participants are ranked and placed in levels $r_1, \ldots, r_w$. We assume that there are l_i participants in level r_i, for $i = 1, \ldots, w$. So $\sum_i l_i = l$. A secret key K is chosen and l pieces of related information distributed, one piece to each participant. This is done in such a way that the secret can be recovered from the shares of t_i participants of rank r_i. However, an incapacitated participant of rank r_i can be replaced by a participant of rank $r_j \geq r_i$, or at least two participants of rank less than r_i.

2. Latin squares

Our model for a secret sharing scheme is based on the following combinatorial structure.

A *latin square* L, of order n, is an $n \times n$ array with entries chosen from a set, N, of size n such that each entry occurs precisely once in each row and column. For convenience, we sometimes talk of the latin square L as a set of ordered triples $(i, j; k)$ and take this to mean that element k occurs in position (i, j) of the latin square L. If we index the rows and columns of an array by the set $N = \{0, 1, ..., n-1\}$, with $n > 1$, then the array with integer $i + j (mod\ n)$ in position (i, j) is said to be a *back circulant* latin square. Table 1 shows a back circulant latin square of order 6.

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Table 1.

A *partial latin square*, of order n, is an $n \times n$ array with entries chosen from a set of size n in such a way that each entry occurs at most once in each row and at most once in each column. The partial latin square may contain a number of empty cells. We are interested in partial latin squares which satisfy the following properties. A *critical set* in a latin square L, of order n, is a set $A = \{(i, j; k) \mid i, j, k \in \{1, ..., n\}\}$ such that

1. L is the only latin square, of order n, which has element k in position (i, j) for each $(i, j; k) \in A$, and
2. no proper subset of A satisfies 1.

A *minimal critical set* in a latin square L is a critical set of minimum cardinality. For example, the latin square representing the abelian 2-group, of order 2^2, is given in Table 2, on the left. A minimal critical set $\{(1, 1; 1), (1, 2; 2), (2, 4; 3), (3, 2; 4), (4, 3; 2)\}$ for this latin square is given on the right.

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

Table 2.

We also require the definition of an isotopic latin square and the corresponding definitions for critical sets. Two latin squares L and M are said to be *isotopic* or *equivalent* if there exists an ordered triple (α, β, γ), of permutations, such that α, β, γ map the rows, columns, and elements, respectively, of L onto those of M. That is, two latin squares are isotopic, if one can be transformed onto the other by rearranging rows, rearranging columns or renaming elements. (For more details see [9], pages 23 and 124.) Two critical sets A and B are said to be isotopic if there exists an ordered triple of permutations (α, β, γ) which maps the entries of A onto B such that, for all $(x, y; z) \in A$, $(x\alpha, y\beta; z\gamma) \in B$.

There is not a lot known about critical sets for latin squares in general. Results on critical sets for latin squares have appeared in papers by Cooper, Donovan and Seberry [5], Donovan, Cooper, Nott and Seberry [6], Nelder [11] and [12], Colbourn, Colbourn and Stinson [7], Curran and van Rees [8], Smetaniuk [17], Stinson and van Rees [18] and Street [20]. However, a class of critical sets is known for back circulant latin squares. For back circulant latin squares of even order Curran and van Rees [8] showed that the following set is a minimal critical set.

- Let $n = 2m$, for some positive integer m, and

$$\begin{aligned} C \quad = \quad & \{(i,j;i+j) \mid \quad i = 0,\ldots,n/2-1 \\ & \qquad\qquad\quad \text{and } j = 0,\ldots,n/2-1-i\} \quad \cup \\ & \{(i,j;i+j) \mid \quad i = n/2+1,\ldots,n-1 \\ & \qquad\qquad\quad \text{and } j = n/2-i,\ldots,n-1\}, \end{aligned}$$

  where addition of the last component is taken modulo n. Then C is a minimal critical set in a back circulant latin square of order n. The cardinality of this set is $n^2/4$.

They also obtained the following result for back circulant latin squares of odd order.

- A back circulant latin square, of odd order $n = 2m+1$, is the only latin square which contains the set

$$\begin{aligned} C \quad = \quad & \{(i,j;i+j) \mid \quad i = 0,\ldots,(n-3)/2 \\ & \qquad\qquad\quad \text{and } j = 0,\ldots,(n-3)/2-i\} \quad \cup \\ & \{(i,j;i+j) \mid \quad i = (n+1)/2+1,\ldots,n-1 \\ & \qquad\qquad\quad \text{and } j = (n-1)/2-i,\ldots,n-1\}. \end{aligned}$$

  The cardinality of this set is $(n^2-1)/4$.

Cooper, Donovan and Seberry [5] subsequently showed that this set is a critical set. Donovan, Cooper, Nott and Seberry [6] have also shown that given a latin square L and a critical set A in L, then a class of critical sets in L may be obtained by taking certain isotopic images of A. Similarly a class of critical sets in L may be obtained by taking certain conjugates of A.

3. Proposed scheme

A secret sharing scheme can be constructed in which the secret key is a latin square L, of order n. This scheme exhibits the following characteristics. The latin square is taken to be the secret key and therefore kept private.

However, the order of the latin square is made public knowledge. The shares in the secret are based on a partial latin square $\mathcal{S} = \{\cup A_i \mid A_i$ is a critical set in $L\}$. The union can be taken over all possible critical sets in L or over some subset of critical sets. The number of critical sets used will be dependent on the size of the latin square and the number of participants in the secret sharing scheme. The access structure will be the set $\Gamma = \{B \mid B \subseteq \mathcal{S}$ and $B \supseteq A$ where A is some critical set in $L\}$. One can easily see that Γ is monotone. The protocol for a secret sharing scheme, involving l participants and based on a latin square is as follows.

Protocol:

- A latin square L of order n is chosen. The number n is made public, but the latin square L is kept secret and taken to be the key.
- A set $\mathcal{S}$ which is the union of a number of critical sets in L is defined.
- For each $(i, j; k) \in S$, the share $(i, j; k)$ is distributed privately to a participant.
- When a group of participants whose shares constitute a critical set come together, they can reconstruct the latin square L and hence the secret key.

We will demonstrate how the scheme works on a few small examples and then give a more general construction.

Take the latin square of order 3 given in Table 3.

1	2	3
2	3	1
3	1	2

Table 3.

Let $\mathcal{S}$= $\{(2,1;2),(3,2;1),(1,3;3)\}$. We can construct a 2–out–of–3 secret sharing scheme on this set. The secret is taken to be the latin square given above. When any two participants come together they combine their shares and reconstruct the unique latin square containing their shares.

For a slightly larger example, take the latin square given in Table 2. Let $\mathcal{S}$ be the partial latin square $\{(1,1;1),(1,2;2),(2,4;3),(3,2;4),(4,3;2),(1,3;3),(1,4;4),(2,2;1),(3,4;2),(4,1;4)\}$. All parties are told that the order of the latin square is 4. Each participant is given a share $(i, j; k)$, for one such element of $\mathcal{S}$. In order to recover the secret an authorized group of participant must place their shares in a partial latin square. They then

reconstruct the unique latin square containing these elements. These authorized groups are based on the critical sets contained in $\mathcal{S}$. Some of the critical sets contained in $\mathcal{S}$ are

$$A_1 = \{(1,1;1),(1,2;2),(2,4;3),(3,2;4),(4,3;2)\},$$
$$A_2 = \{(1,1;1),(1,3;3),(2,4;3),(3,2;4),(4,3;2)\},$$
$$A_3 = \{(1,1;1),(1,4;4),(2,4;3),(3,2;4),(4,3;2)\},$$
$$A_4 = \{(1,1;1),(2,2;1),(2,4;3),(3,2;4),(4,3;2)\},$$
$$A_5 = \{(1,1;1),(3,4;2),(2,4;3),(3,2;4),(4,3;2)\},$$
$$A_6 = \{(1,1;1),(4,1;4),(2,4;3),(3,2;4),(4,3;2)\},$$
$$A_7 = \{(1,3;3),(1,4;4),(2,2;1),(3,4;2),(4,1;4)\},$$
$$A_8 = \{(1,3;3),(1,1;1),(2,2;1),(3,4;2),(4,1;4)\}.$$

Now for a more general example. Let L be a latin square isotopic to a back circulant latin square of order n and C an appropriate critical set isotopic to the set given by Curran and van Rees. Define $\mathcal{C} = \{C' \mid C' \text{ is the conjugate or isotopic image of } C\}$. Let $\mathcal{S}' = \{C' \mid C' \in \mathcal{C} \text{ and } C' \text{ is a critical set in } L\}$. We may now use the protocol given above to construct a secret sharing scheme where the shares are drawn from the set $\mathcal{S}'$.

The following points should be made about the secret sharing scheme.

- Since the authorized groups are based on critical sets in latin squares, the absence of one share implies that the secret cannot be recovered uniquely.
- The scheme is obviously not perfect as an outsider must guess from the set of all possible latin squares of order n, whereas an unauthorized group of participants knows that the latin square must contain the partial latin square defined by their shares.
- The security of the scheme is based on the number of possible latin squares containing the partial latin square defined by an unauthorized group of participants. Rezny [13] has estimated this for a number of back circulant latin squares of small order. He took the critical set

$$\begin{aligned} C = \{(i,j;i+j) \mid\ & i = 0,\ldots,(n-3)/2 \\ & \text{and } j = 0,\ldots,(n-3)/2 - i\} \quad \cup \\ \{(i,j;i+j) \mid\ & i = (n+1)/2+1,\ldots,n-1 \\ & \text{and } j = (n-1)/2 - i,\ldots,n-1\}. \end{aligned}$$

and for $n = 3$, 5, 7, 9 and 11 he systematcially removed an element from C and used a computer to obtain the number of latin squares which contain $C \setminus \{(i,j;k)\}$, for some element $(i,j;k)$ of C. Rezny's results are summarized in Table 4.

n	Number of latin squares containing the set $C \setminus \{(i,j;k)\}$
3	4
5	32
7	$\geq$ 880
9	$\geq$ 75232
11	$\geq$ 19000000

Table 4.

4. Multilevel scheme

In many situations we require a secret sharing scheme in which some shares are more equal than others. That is, we require a multilevel scheme. As stated earlier, these schemes incorporate levels each of which has a number of authorized groups who can reconstruct the secret. However, for the system to be truly functional we also require that the share of a participant at level i can be replaced by two or more participants at a lower level. Consider the case of an electronic transfer of funds between financial institutions. This transfer can only be initiated when a electronic signature is received. The signature will be reconstructed when the shares of two senior tellers and one vice president, or two vice presidents, are entered. We can use the latin square given in Table 3 to construct a secret sharing scheme which satisfies these requirements. Let $\mathcal{S}$= $\{(2,1;2),(3,2;1),(1,1;1),\ (1,2;2)\}$. The access structure for this scheme will be based on the critical sets

$$A_1 = \{(1,1;1),(1,2;2),(2,1;2)\}$$
$$A_2 = \{(1,1;1),(1,2;2),(3,2;1)\}$$
$$A_3 = \{(3,2;1),(2,1;2)\}.$$

The latin square can be reconstructed from the shares $(2,1;2)$ and $(3,2;1)$. However either of these two shares can be replaced by the two shares $(1,1;1)$ and $(1,2;2)$. To satisfy the requirements of the model we could distribute the shares as follows:

1. The senior tellers each receive a share corresponding to one of the triples $(1,1;1)$ and $(1,2;2)$, respectively, and
2. the vice presidents each receive a share corresponding to one of the triples $(2,1;2)$ and $(3,2;1)$, respectively,

thus satisfying the requirement.

5. A further application

Consider the situation where there are a number of secret sharing schemes all of which contain a common participant. This participant may be re-

quired to remember a number of shares. For example, a medical administrator may require access to several restricted files. These files may contain, say, patient data, hospital resources and organ bank data. Access to these files may be via a secret sharing scheme in which the registrar of the hospital always has a critical share. The registrar may be required to remember several different shares. This obviously increases the complexity of the registrar's role and consequently reduces the security of the schemes. Therefore we wish to develop a key management scheme in which a secret key is common to a number of secret sharing schemes. The shares related to this key are such that a primary share is held by one participant and this share is a necessary part of the reconstruction process in each scheme. Each scheme will involve a number of minor shares which when combined with the primary share can be used to reconstruct the secret. In addition it is required that the secret cannot be recovered uniquely from the combined information held by the minor shares.

Inequivalent critical sets in a latin square can be used to model a key management scheme of this nature. We illustrate this with an example. Take the latin square of order 5 given in Table 5.

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

Table 5.

Using results obtained by Cooper, Donovan and Seberry in [5] and the computer program nauty [10] it can be shown that there are 41 distinct minimal critical sets of order 7, three of these are listed below.

$$A_1 = \{(1,1;1),(2,5;3),(3,5;4),(4,2;3),(4,3;5),(5,1;5),(5,3;2)\}$$
$$A_2 = \{(1,1;1),(1,5;5),(3,2;5),(3,5;4),(4,2;3),(5,3;2),(5,4;3)\}$$
$$A_3 = \{(1,1;1),(1,5;5),(3,4;2),(4,2;3),(4,5;2),(5,2;4),(5,4;3)\}$$

Each department is assigned a different critical set A_i with the common participant receiving a share common to each A_i. In this case the registrar will be given the share $(1,1;1)$. All departments will reconstruct the same secret, but each has a different sets of keys to this secret. However if all participants in the minor levels pool their information the secret cannot be reconstructed uniquely. To see this consider the partial latin square containing all the minor shares.

*	*	*	*	5
*	*	*	*	3
*	5	*	2	4
*	3	5	*	2
5	4	2	3	*

It is not a critical set as it has four completions.

This key management system can be adapted to allow each department a different secret, but still have a common primary share. This idea can be extended further to each department's having a latin square of a different order.

6. Concluding comments

In this paper we have proposed a viable secret sharing scheme based on latin squares. Unfortunately, not a great deal is known about critical sets for latin squares and so the implementation of this scheme is limited at the present time. One obvious direction for future research is the construction of general families of critical sets for latin squares. Another is to investigate the structure of these critical sets to see if it is possible to construct general t–out–of–l perfect threshold schemes from latin squares. Stinson [19], and others have been studying the information rates of secret sharing schemes.

References

[1] Albrecht Beutelspacher, *Enciphered geometry: some applications of geometry to cryptography*, Proc. Combinatorics '86, in Annals of Discrete Mathematics, **37**, A. Barlotti, M. Marchi and G. Tallini, Eds., Amsterdam: North Holland, 1988, pp. 59–68.

[2] G.R. Blakley, *Safeguarding cryptographic keys*, Proc. AFIPS 1979 Natl. Computer Conf, New York, 48, June 1979, pp. 313–317.

[3] E.F. Brickell, *Some ideal secret sharing schemes*, J.Combin. Math and Combin. Comput., **9**, 1989, pp. 105–113.

[4] D. Chaum, *Computer systems established, maintained, and trusted by mutually suspicious groups*, Memorandum No. UCB/ERL MI79/10, University of California Berkley CA, 1979.

[5] Joan Cooper, Diane Donovan and Jennifer Seberry, *Latin squares and critical sets of minimal size*, Australas. J. Combin., 4, 1991, pp. 113–120.

[6] Diane Donovan, Joan Cooper, D.J. Nott and Jennifer Seberry, *Latin squares: critical sets and their lower bounds*, Ars Combinatoria, to appear.

[7] C.J. Colbourn, M.J. Colbourn and D.R. Stinson, *The computational complexity of recognizing critical sets*, in Proc. 1st Southeast Asian Graph Theory Colloquium, Lecture Notes in Math., **1073**, Springer–Verlag, 1984, pp. 248–253.

[8] D. Curran and G.H.J. van Rees, *Critical sets in latin squares*, Proc. 8th Manitoba Conference on Numerical Mathematics and Computing, (Congressus Numerantium XXII), Utilitas Math. Pub., Winnipeg, 1978, pp. 165–168.

[9] J. Dénes and A.D. Keedwell, Latin Squares and their Applications, The English Universities Press Ltd, London, 1974.

[10] Brendan D. McKay, *nauty User's Guide (Version 1.2)*, Australian National University Computer Science Technical Report TR:CS–87–03, 1987.

[11] John Nelder, *Critical sets in latin squares*, CSIRO Div. of Math. and Stats, Newsletter, **38** 1977.

[12] John Nelder, *Private communication from John Nelder of J Seberry*, 1979.

[13] M. Rezny, *A secret sharing scheme based on latin squares*, a private communication, 1992.

[14] A. Shamir, *How to share a secret*, Comm. A.C.M., **22**, No. 11, Nov. 1979, pp. 612–613.

[15] G.J. Simmons, *How to (really) share a secret*, in Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto '88, S. Goldwasser, Ed., Santa Barbara, CA, Aug. 21–25, 1987, Berlin: Springer–Verlag, 1990, pp. 390–448.

[16] G.J. Simmons, *An introduction to shared secret and/or shared control schemes and their applications*, in Contemporary Cryptology, the Science of Information Integrity, IEEE Press, Piscataway, 1991, pp. 441–497.

[17] Bohdan Smetaniuk, *On the minimal critical set of a latin square*, Utilitas Math., **16**, 1979, pp. 97–100.

[18] D.R. Stinson and G.H.J. van Rees, *Some large critical sets*, Congressus Numerantium, **34**, 1982, pp. 441–456.

[19] D.R. Stinson, *An explication of secret sharing schemes*, Designs, Codes and Cryptography, **2**, (1992), pp. 357–390.

[20] Anne Penfold Street, *Defining sets for t–designs and critical sets for latin squares*, New Zealand Journal of Math., **21**, 1992, pp 133–144.