1996

Secret Sharing schemes based on Room squares

Ghulam Rasool Chaudhry

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

Abstract

In this paper, we describe secret sharing schemes. We discuss Room squares and their critical sets. We propose a model of sharing based on critical sets of Room squares.

Publication Details

Chaudhry G R, and Seberry J, Secret Sharing schemes based on Room squares,Proceedings of DMTCS'96, December , 1996, Auckland, New Zealand, Combinatorics, Complexity and Logic, Springer-Verlag Singapore 1996, 158-167.

Secret Sharing Schemes Based on Room Squares

Ghulam Rasool Chaudhry and Jennifer Seberry

The Centre for Computer Security Research
Department of Computer Science
University of Wollongong
Wollongong, NSW 2522, AUSTRALIA

Abstract. In this paper, we describe secret sharing schemes. We discuss Room squares and their critical sets. We propose a model of secret sharing based on critical sets of Room squares.

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 by 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 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 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.

We describe another situation which motivates the subject of secret sharing:

> *The head of an organization keeps important documents in a safe of which only he or she knows the combination. However, the head is often absent for extended periods and occasionally information is needed from documents in the safe in order to maintain the day-to-day running of the organization. The head deems it undesirable for the combination to be trusted to any one of the five executive board members. What is regarded as acceptable, however, is a compromise situation whereby at least two of the executive board members acting together can gain access to the safe.*

Can such a system be devised?

Figure 1 provides a system to solve the above problem. The lines and points are chosen in projective space $PG(2,q)$ where $q \geq 5$. It is publicly known that the safe combination is a point on line l but the actual point is kept secret. Each of the five executives is privately given a point on line m and the safe

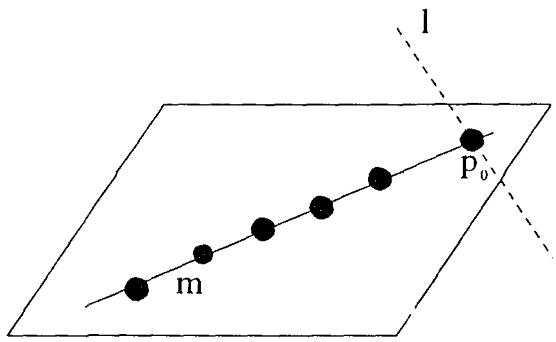

Fig. 1. A projective space

combination is chosen to be point p_0, the unique point of intersection of line m and line l. Any two executives can generate line m and hence evaluate p_0 by intersecting m and l. However, one executive acting alone knows only that the safe combination must be one of the points on line l—the actual point remains secret since for every point p on line l there is a unique line passing through the executive's point and p.

Secret sharing schemes are systems designed to solve problems of a similar type to the one we have just discussed. In general, there is a group of potential members of such a scheme and a collection of sets of these members which are desired to have access to some protected information.

The information is protected by distributing to each member of the scheme an amount of partial information which relates in some way to the protected information. This partial information is known only to the individual member to whom it is distributed and it is held secret by them. When any group of members of the scheme who are desired to have access to the protected information choose to do so, they can reconstruct it by pooling their pieces of partial information. Thus, in our opening problem, any two pieces of the partial information distributed to the executives must be sufficient to enable the combination of the safe to be determined.

Secret sharing schemes were first introduced by Blakley [2], Shamir [19] and Chaum [4] in 1979, and subsequently have been studied by numerous other authors. For a general discussion of shared secret schemes, see Simmons' paper [20]. 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, orthogonal arrays and Latin squares. In this paper, we will model a new secret sharing scheme based on Room squares.

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 [20] and Cooper, Donovan and Seberry [8] have adapted the basic schemes and constructed multilevel schemes.

We shall now introduce a more formal terminology for secret sharing schemes.

2 Secret sharing schemes

A *secret sharing scheme* is a method of sharing a secret S among a finite set of participants P in such a way that if the participants in $A \subseteq P$ are qualified to know the secret, then by pooling together their shares, they can reconstruct the secret S; but any set $B \subset P$, which is not qualified to know S, cannot reconstruct the secret. The key S is chosen by a special participant D called the *dealer* and it is usually assumed that $D \notin P$. The dealer gives partial information called a *share* to each participant to share the secret S.

Secret sharing schemes are useful in any important action that requires the concurrence of several designated people to be initiated as described in the examples in Section 1.

An *access structure* Γ is the family of all the subsets of participants that are able to reconstruct the secret. An access structure is said to be *monotone* if any set which contains a subset, that can recover the secret, can itself recover the secret, that is, if for any subsets B and C of P, where $B \subseteq C$ and $B \in \Gamma$, then $C \in \Gamma$. The subsets of P belonging to the access structure Γ are called *authorized sets* and those not belonging to the access structure are termed as *unauthorized sets*.

Example 1. In Figure 1, the secret sets are the points on line l and the secret is the point p_0. The shares are the five points on line m that are distributed to five participants. Finally, observing that P is the set of five participants, we have the access structure:

$$\Gamma = \{A \subseteq P : |A| \geq 2\}$$

One property of a monotone access structure is that it has a unique collection of authorized sets of minimal size. We define $B \in \Gamma$ to be a *minimal set* of Γ if $C \in \Gamma, C \subseteq B$ implies $C = B$. The collection of all minimal sets of Γ is denoted by Γ^-.

A *(k,n) threshold scheme* allows a secret to be shared among n participants in such a way that any k of them can recover the secret, but no group of $k - 1$, or fewer participants, can do so.

A monotone access structure Γ defined on a participant set P such that $|P| = n$ and $\Gamma = \{X \subseteq P : |X| \geq k\}$ is known as (k, n) *threshold access structure.*

Example 2. A Latin square of order n is an $n \times n$ array of the integers 1, 2, ..., n such that each integer occurs precisely once in each row and each column. In this example, we take a Latin square L of order 3 as a (2,3) threshold scheme.

$$L = \begin{bmatrix} 1\,2\,3 \\ 2\,3\,1 \\ 3\,1\,2 \end{bmatrix}$$

Let $S = \{(2,1;2),(3,2;1),(1,3;3)\}$, a partial Latin square, be the union of some critical sets of L, where (2,1;2) means that integer 2 is at position (2,1), (3,2;1) means that integer 1 is at position (3,2) and (1,3;3) means that integer 3 is at position (1,3) in the Latin square L. We can construct a 2-out-of-3 secret sharing scheme on this set. The Latin square L is kept secret but its order is made public. When any two participants from S collaborate, they combine their shares and reconstruct the unique Latin square containing their shares.

A secret sharing scheme is said to be *perfect* provided the following two properties are satisfied:

(i) If an authorized subset of participants $A \subseteq P$ pool their shares, then they can determine value of the secret S.
(ii) If an unauthorized subset of participants $B \subset P$ pool their shares, then they can determine nothing more than any outsider about the value of the secret S.

The security of such a scheme is unconditional since we do not place any limit on the amount of computation that can be performed by a subset of participants.

The size of each share is defined as the number of bits s of non-redundant information in the share. The size of the secret t is the number of bits of non-redundant information in the secret. How to exactly determine s and t is not yet known.

In a *multilevel scheme*, the participants are ranked and placed in levels $r_1, ..., r_w$. We assume that there are l_i participants in level r_i for $i = 1, ..., w$. So $\sum l_i = l$. A secret key S 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.

3 Room squares

A *Room square* R of order r is an $r \times r$ array each of whose cells may either be empty or contain an unordered pair of objects $0, 1, 2, ..., r$, subject to the following conditions :

(i) each of the objects $0, 1, 2, ..., r$ occurs precisely once in each row of R and precisely once in each column of R, and
every possible unordered pair of objects occurs precisely once in the whole array.

Theorem 1. (Mullin and Wallis [18]) *There exists a Room square of every odd integer order r greater than or equal to 7.*

We denote $N_r = 0, 1, 2, ...r$. A Room square of order r based on N_r is *standardized* if the ith diagonal cell, cell(i, i), contains $\{0, i\}$ for $1 \leq i \leq r$.

A *skew* Room square R is a standardized Room square with the property that when $i \neq j$, either the (i, j) or the (j, i) cell of R is occupied, but not both.

Two Room squares are said to be *isomorphic* if one can be obtained from the other by permuting the rows and columns and relabeling the elements. Two Room squares R and S are *equivalent* if R is isomorphic to S or to the transpose of S. All inequivalent Room squares of order 7 and 9 have been found by one-factorizations of graph, see [1, 11, 22] for details. There are exactly 6 inequivalent Room squares of order 7 and 257,630 inequivalent Room squares for order 9. No exact values of inequivalent Room squares are still known for higher order Room squares, although there are :

526,915,620 non-isomorphic one-factorizations of order 11,
9.876×10^{28} distinct one-factorizations of order 13,
1.148×10^{44} distinct one-factorizations of order 15,
1.520×10^{63} distinct one-factorizations of order 17,

and the number of all inequivalent Room squares for each of these orders are even much larger, see [10] for details.

A *partial Room square* R of order r is an $r \times r$ array each of whose cells may either be empty or contain an unordered pair of objects $0, 1, 2, ..., r$, subject to the following conditions :

(i) each of the objects $0, 1, 2, ..., r$ occurs at most once in each row of R and at most once in each column of R, and
(ii) every possible unordered pair of objects occurs at most once in the whole array.

A *critical set* $Q = \{Q_1, Q_2, Q_3, ..., Q_c\}$, $|Q| = c$, in a Room square R of order r, is a set of quadruples $Q_a = (i, j; k, l)$ such that if any Q_a is removed from the set, it can no longer be uniquely completed. In Q_a, (i, j) shows the position of the pair (k, l) in the square. That is, Q provides minimal information from which R can be reconstructed uniquely. In this paper, we consider that empty positions with '-' in the Room square are given.

Q^* is a *minimal critical set (min.cs)* of a Room square R if $|Q^*| = c$ is minimum for all critical sets Q of a Room square of order r whereas Q^* is a *maximal critical set (max.cs)* of a Room square R if $|Q^*| = c$ is the largest for all critical sets Q of a Room square of order r.

Example 3. Room square of order 7:

8,1	-	4,5	6,7	-	-	2,3
5,7	8,2	-	-	-	1,3	4,6
-	5,6	8,3	1,2	-	4,7	-
-	3,7	-	8,4	2,6	-	1,5
3,6	1,4	2,7	-	8,5	-	-
2,4	-	-	3,5	1,7	8,6	-
-	-	1,6	-	3,4	2,5	8,7

Critical set 1 of above square is:

**	–	4,5	**	–	–	2,3
**	**	–	–	–	1,3	4,6
–	**	8,3	1,2	–	4,7	–
–	**	–	**	2,6	–	1,5
**	**	**	–	**	–	–
**	–	–	**	**	**	–
–	–	**	–	**	**	**

Critical set 2 of above square is:

**	–	**	**	–	–	**
**	8,2	–	–	–	**	**
–	**	8,3	1,2	–	**	–
–	3,7	–	8,4	**	–	**
**	**	**	–	8,5	–	–
**	–	–	**	1,7	8,6	–
–	–	**	–	**	**	**

where "**" shows an unknown pair position and "–" shows an empty position in the square.

So the critical set 1 for the above Room square is: $Q = \{(1,3;4,5), (1,7;2,3), (2,6;1,3), (2,7;4,6), (3,3;8,3), (3,4;1,2), (3,6;4,7), (4,5;2,6), (4,7;1,5)\}$. That is, Q is the only Room square of order 7 with a pair 4,5 at position (1,3), pair 2,3 at position (1,7), pair 1,3 at position (2,6), pair 4,6 at position (2,7), pair 8,3 at position (3,3), pair 1,2 at position (3,4), pair 4,7 at position (3,6), pair 2,6 at position (4,5) and pair 1,5 at position (4,7).

There is very little known about critical sets in Room squares. Chaudhry and Seberry [5] studied critical sets in Room squares for orders 7, 9 and 11.

4 Proposed scheme

A secret sharing scheme can be constructed in which the secret key is a Room square R of order r. This scheme exhibits the following characteristics: The Room square is taken to be the secret key and therefore kept private. However, the order of the Room square is made public. The shares in the secret are based on a partial Room square $S = \{\cup A_i \mid A_i \text{ is a critical set in } R\}$. The union can be taken over all possible critical sets in R or over some subset of critical sets. The number of critical sets used will be dependent on the size of the Room square and the number of participants in the secret sharing scheme. The access structure will be the set $\Gamma = \{B \mid B \subseteq S \text{ and } B \supseteq A \text{ where } A \text{ is some critical set in } R\}$. One can easily see that Γ is monotone. The protocol for secret sharing scheme, involving l participants and based on a Room square is as follows.

- A Room square R of order r is chosen. The number r is made public, but the Room square R is kept secret to be the key.

- A set S which is the union of a number of critical sets in R is defined.
- For each $(i,j;k,l) \in S$, the share $(i,j;k,l)$ is distributed privately to a participant.
- When a group of participants whose shares constitute a critical set come together, they can reconstruct the Room square R and hence the secret key.

We demonstrate here how the scheme works on a small example and then give a more general construction.

Take a Room square of order 7 given in example 3. Let S be the partial Room square {(1,3;4,5), (1,7;2,3), (2,2;2,8), (2,6;1,3), (2,7;4,6), (3,3;8,3), (3,4;1,2), (3,6;4,7), (4,2;3,7), (4,4;4,8), (5,5;5,8), (4,5;2,6), (4,7;1,5), (6,5;1,7), (6,6;6,8) }. All the parties are told that the order of the Room square is 7. Each participant is given a share $(i,j;k,l)$, for one such element of S. In order to recover the secret, an authorized group of participants must place their shares in a partial Room square. They then reconstruct the unique Room square containing these entries. These authorized groups are based on the critical sets contained in S. Two of the critical sets contained in S are:

$$\begin{aligned} A_1 = \{&(1,3;4,5),(1,7;2,3),(2,6;1,3),(2,7;4,6),(3,3;8,3),\\ &(3,4;1,2),(3,6;4,7),(4,5;2,6),(4,7;1,5)\}\\ A_2 = \{&(2,2;2,8),(3,3;8,3),(3,4;1,2),(4,2;3,7),\\ &(4,4;4,8),(5,5;5,8),(6,5;1,7),(6,6;6,8)\}\end{aligned}$$

Note that $|A_1| = 9$ while $|A_2| = 8$.

Now for a more general example. Let R be a Room square of order r and Q be a critical set. Define $\mathcal{Q} = \{Q' \mid Q' \text{ is the isotopic image of Q}\}$. Let $S' = \{Q' \mid Q' \in \mathcal{Q} \text{ and } Q' \text{ is a critical set in } R\}$. We may use the protocol given above to construct a secret sharing scheme where the shares are drawn from the set S'.

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

- Since the authorized groups are based on critical sets in Room squares, the absence of one share implies that secret cannot be recovered uniquely.
- The scheme is obviously not perfect as an outsider can guess from the set of all possible Room squares of order r, whereas an unauthorized group of participants knows that the Room square must contain the partial Room square defined by their shares.
- The security of the scheme is based on the number of possible Room squares containing the partial Room square defined by an unauthorized group of participants.
- The number of inequivalent Room squares for higher order grows exponentially as mentioned earlier. The number of inequivalent Room squares of order greater than or equal to 11 are still unknown under the current computing resources, although lower bounds on these numbers are known. So the probability of guessing a secret key consisting of a Room square of order greater than or equal to 11 is very very small, and the scheme is very secure though not perfect.

5 Key management scheme

In this section we consider the situations where there are a number of secret sharing schemes all of which contain a common participant. This participant may be required to remember a number of shares. For example, a medical administrator (Registrar) 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 role. The registrar always has to remember several different shares. This obviously increases the complexity of the registrar's role and consequently reduces the security of the schemes.

We wish to model 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. It is also required that the secret can not be reconstructed uniquely from the combined information held by the minor shares.

Inequivalent critical sets in a Room square can be used to model a key management scheme of this nature. We illustrate this with an example. Take the Room square of order 7 given in example 3. Following are three distinct minimal critical sets of this Room square which have the common pairs (3,3;8,3) and (3,4;1,2).

$$\begin{aligned}
A_1 = \{&(1,3;4,5),(1,7;2,3),(2,6;1,3),(2,7;4,6),(3,3;8,3),\\
&(3,4;1,2),(3,6;4,7),(4,5;2,6),(4,7;1,5)\}\\
A_2 = \{&(2,2;2,8),(3,3;8,3),(3,4;1,2),(4,2;3,7),\\
&(4,4;4,8),(5,5;5,8),(6,5;1,7),(6,6;6,8)\}\\
A_3 = \{&(1,1;1,8),(1,3;4,5),(1,4;6,7),(2,1;5,7),(2,7;4,6),\\
&(3,3;8,3),(3,4;1,2),(4,7;1,5),(1,5;3,6),(6,6;6,8)\}
\end{aligned}$$

Note that $|A_1| = 9$, $|A_2| = 8$ and $|A_3| = 10$.

Each department is assigned a different critical set A_i with the same participant receiving a share which is common to each A_i. In this case the registrar will be given the common share (3,3;8,3) or (3,4;1,2). All departments will reconstruct the same secret, but each has a different set of keys to this secret. However if all participants in the minor (lower than registrar) level pool their shares, the secret cannot be reconstructed uniquely.

Another key management scheme can be developed to allow each department a different secret, but still have a common primary share using inequivalent Room squares of same order with some common pairs and same positions.

Multilevel schemes, based on critical sets of Room squares, can also be developed in which some participants are more important than others. In multilevel schemes, the share of a participant at level j can be replaced by two or more participants at level i, where $i < j$. Consider the case of an electronic transfer of funds between financial institutions. This transfer can only be initiated when an 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. Critical sets for Room squares fulfilling these requirements are still not known.

6 Conclusion

In this paper, we have proposed a secret sharing scheme based on critical sets of Room squares. Since there is very little known about critical sets of Room squares, the implementation of this scheme is limited at the moment. However, the directions for future research are:

- Construct families of critical sets for Room squares.
- Construct families of smallest and largest critical sets for Room squares without a priori constraints on the Room square.
- Quantify the security of the scheme more effectively, that is, decide which critical sets are more secure than others.
- Find a general process that will start with an access structure and result in a Room square.
- Investigate the structure of critical sets from Room squares to see if possible to construct perfect secret sharing schemes.
- Devise multilevel schemes based on critical sets of Room squares.

References

1. D. S. Archdeacon, J. H. Dinitz and W. D. Wallis. *Sets of pairwise orthogonal one-factorizations of* K_{10}. Congr. Numer. 43 (1984), pp. 45-79.
2. G. R. Blakley. *Safeguarding cryptographic keys.* Proc. AFIPS 1979 Natl. Computer Conference, New York, 48, June (1979), pp. 313-317.
3. E.F. Brickel. *Some ideal secret sharing schemes.* J. Comb. Math. and Comb. Computing, 9, (1989), pp. 105-113.
4. D. Chaum. *Computer Systems established, maintained and trusted by mutually suspicious groups*, Memorandum No. UCB/ERL M179/10, University of California Berkley CA, 1979.
5. G. R. Chaudhry and J. Seberry. *Minimal and maximal critical sets in Room squares.* 7th Australasian Workshop on Combinatorial Algorithms (AWOCA'96), Magnetic Island, Australia, July 15-19 (1996), Technical Report 508, July 1996, Dept. of Computer Science, University of Sydney, Australia pp 75-86.
6. D. Chen and D.R. Stinson, *Recent results on combinatorial constructions for threshold schemes.* Aust. J. of Combin., 1 (1990), pp. 29-48.
7. J. Cooper, D. Donovan and J. Seberry. *Latin squares and critical sets of minimal size.* Aust. J. Combinatorics 4 (1991), pp. 113-120.
8. J. Cooper, D. Donovan and J. Seberry. *Secret sharing schemes arising from Latin squares.* Bull. of the Inst. of Combinatorics and its Applications, September (1994) pp. 33-43.
9. D. Curran and G.H.J. Van Rees. *Critical sets in Latin squares.* in Proc. Eighth Manitoba Conference on Numer. Math. and Computing, (1978), pp. 165-168.

10. J. H. Dinitz, D. K. Garnick and B. D. Mackay. *Non-isomorphic one-factorizations of K_{12}*. J. Comb. Design, Vol. 2, No. 4 (1994), pp. 273-285.
11. J. H. Dinitz and D. R. Stinson. *Room squares, Contemporary Design Theory: a Collection of Surveys.* John Wiley & Sons, Inc. (1992), pp. 137-204.
12. J. H. Dinitz and W. D. Wallis. *Four orthogonal one-factorizations on 10 points.* Ann. Disc. Math. 26 (1985), pp. 143-150.
13. M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* W. H. Freeman and Company, San Francisco, 1979.
14. K. B. Gross. *Equivalence of Room designs I.* J. Comb. Theory A 16 (1974), pp. 264-265.
15. K. B. Gross. *Equivalence of Room designs II.* J. Comb. Theory A 17 (1974), pp. 299-316.
16. K. M. Martin, *Discrete Structures in the Theory of Secret Sharing.* PhD thesis, Royal Holloway and Bedford New College, University of London, 1991.
17. K. M. Martin, *New secret sharing schemes from old.* JCCMCC 14 (1993), pp. 65-77.
18. R. C. Mullin and W. D. Wallis. *The existence of Room squares.* Aequa. Math. 13 (1975), pp. 1-7.
19. A. Shamir *How to share a secret.* Comm. ACM, 22, No. 11, Nov. 1979, pp. 612-613.
20. 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.
21. D.R. Stinson, *An explication of secret sharing schemes.* Design, Codes and Cryptography, 2 (1992), pp. 357-390.
22. W.D. Wallis, A. P. Street and J. S. Wallis. *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices.* Lect. Notes Math. 293, Springer-Verlag Berlin (1972).