Perfect Secret Sharing Schemes from Room Squares

Ghulam-Rasool Chaudhry
Hossein Ghodosi
Jennifer Seberry

Department of Computer Science
Centre for Computer Security Research
University of Wollongong
Wollongong, NSW 2500, AUSTRALIA

chaudhry/hossein/j.seberry@uow.edu.au

Dedicated to Anne Penfold Street.

Abstract

Secret sharing schemes are one of the most important primitives in distributed systems. In perfect secret sharing schemes, collaboration between unauthorised participants cannot reduce their uncertainty about the secret.

This paper presents a perfect secret sharing scheme arising from critical sets of Room squares.

1 Introduction

A secret sharing scheme is a method of sharing a secret S among a finite set of participants $\mathcal{P} = \{P_1, \ldots, P_n\}$ in such a way that if the participants in $\mathcal{A} \subseteq \mathcal{P}$ are qualified to know the secret, then by pooling together their partial information, they can reconstruct the secret S; but any set $\mathcal{B} \subset \mathcal{P}$, which is not qualified to know S, cannot reconstruct the secret. The key S is chosen by a special participant $\mathcal{D}$, called the *dealer*, and it is usually assumed that $\mathcal{D} \notin \mathcal{P}$. The dealer gives partial information, called the *share*, to each participant to share the secret S.

JCMCC 28 (1998), pp. 55-61

An *access structure* Γ is the family of all the subsets of participants that are able to reconstruct the secret. The sets of $\mathcal{P}$ belonging to the access structure Γ are called *authorised sets* and those not belonging to the access structure are termed as *unauthorised sets.*

A secret sharing scheme is *perfect* if an unauthorised subset of participants $\mathcal{B} \subset \mathcal{P}$ pool their shares, then they can determine nothing more than any outsider about the value of the secret S.

An authorised set $\mathcal{A}$ is *minimal* if $\mathcal{A}' \subset \mathcal{A}$ and $\mathcal{A}' \in \Gamma$ implies that $\mathcal{A}' = \mathcal{A}$. We only consider *monotone* access structures in which $\mathcal{A} \in \Gamma$ and $\mathcal{A} \subset \mathcal{A}'$ implies $\mathcal{A}' \in \Gamma$. For such access structures, the collection of minimal authorised sets uniquely determines the access structure. In the rest of this paper we use Γ to denote the representation of access structure in terms of minimal authorised sets.

Secret sharing schemes were first introduced by Blakley [1], Shamir [8] and Chaum [2] in 1979, and subsequently have been studied by numerous other authors (see, for example, [9]). 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, Latin squares and Room squares. Cooper, Donovan and Seberry [5] proposed a secret sharing scheme arising from Latin squares. Chaudhry and Seberry [4] developed secret sharing schemes based on critical sets of Room squares. Both of these schemes are not perfect. In this paper, we propose a perfect secret sharing scheme arising from critical sets of Room squares. Though we propose secret sharing scheme based on Room squares, however, the method can easily be generalised over Latin squares as well.

2 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,

(ii) every possible unordered pair of objects occurs precisely once in the whole array.

Mullin and Wallis [7] proved that, there exists a Room square of every odd integer side r , $r \geq 7$.

A *critical set* $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_c\}$, in a Room square R of order r, is a set of quadruples $Q_i = (x, y; k, \ell)$, $1 \leq i \leq c$, such that if any Q_i is removed

0,1	–	4,5	6,7	–	–	2,3
5,7	0,2	–	–	–	1,3	4,6
–	5,6	0,3	1,2	–	4,7	–
–	3,7	–	0,4	2,6	–	1,5
3,6	1,4	2,7	–	0,5	–	–
2,4	–	–	3,5	1,7	0,6	–
–	–	1,6	–	3,4	2,5	0,7

**	**	**	**	**	**	**
**	**	**	**	**	**	4,6
**	**	**	1,2	**	**	**
**	3,7	**	**	**	**	**
**	1,4	2,7	**	**	**	**
**	**	**	3,5	**	0,6	**
**	**	**	**	3,4	2,5	0,7

Table 1: A Room square of order 7 and one of its critical sets

from the set, the Room square can no longer be uniquely completed. In each Q_i, the pair (x, y) denotes the position (i.e., row x and column y) of the pair (k, ℓ) in the Room square. That is, Q provides minimal information from which R can be reconstructed uniquely.

Table 1 illustrates a Room square of order 7 and one of its critical sets of size 10, where "**" denotes the unknown entries and "–" denotes the empty positions in the square. The critical set in this table consists of following quadruples: {(2,7;4,6), (3,4;1,2), (4,2;3,7), (5,2;1,4), (5,3;2,7), (6,4;3,5), (6,6;0,6), (7,5;3,4), (7,6;2,5), (7,7;0,7)}.

It should be noted that there is not much known about critical sets of Room squares. The number of critical sets in a Room square of order r are still unknown, but they grow exponentially for higher order Room squares (see Chaudhry and Seberry [3]).

3 Related Work

Chaudhry and Seberry [4] proposed a secret sharing scheme based on critical sets of Room squares. In their scheme, the shares of participants are the quadruples of a critical set taken from the Room square. When a group of participants, whose shares constitute a critical set, pool their shares together, they can reconstruct the Room square which is the key. But, every unauthorised set does not constitute the critical set, and thus, cannot

reconstruct the secret. For example, in order to distribute the shares (the quadruples of the critical set given in Table 1) among an authorised set $\mathcal{A}_i = \{P_{i_1}, P_{i_2}, P_{i_3}\}$, the dealer may assign three quadruples (2,7;4,6), (3,4;1,2) and (4,2;3,7) to P_{i_1}, three quadruples (5,2;1,4), (5,3;2,7) and (6,4;3,5) to P_{i_2} and remaining four quadruples (6,6;0,6), (7,5;3,4), (7,6;2,5) and (7,7;0,7) to P_{i_3} (or any other possible combinations to distribute ten shares among three participants). A similar scheme was also proposed by Cooper et al [5] arising from Latin squares. The drawbacks of the above construction are:

1. The schemes are not perfect. Since each share is a component of a critical set, it determines the exact information of a component from the Room square and therefore, the uncertainty of a participant about the secret is not equal to the uncertainty of an outsider.

2. The scheme does not work if the number of participants in an authorised set is greater than the order of the critical set (since each participant must be assigned at least one quadruple).

Now we propose a perfect secret sharing scheme that is applicable over arbitrary access structures (no matter what is the size of its authorised sets). Though we propose secret sharing scheme based on Room squares, however, it can easily be generalised over Latin squares as well.

4 The Scheme

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of all participants in the system and let $\Gamma = \{\mathcal{A}_1, \ldots, \mathcal{A}_t\}$ be an access structure with t authorised sets over $\mathcal{P}$. Let the critical set $\mathcal{Q} = \{Q_1, \ldots, Q_c\}$ of a Room square R of order r be the secret[1]. For every authorised set $\mathcal{A}_j$, $1 \leq j \leq t$, of size n_j, the dealer uses the Karnin-Greene-Hellman [6] algorithm to distribute the shares to the participants.

Set-up Phase:

1. For every participant P_{ju}, $1 \leq u \leq n_j - 1$, the dealer, $\mathcal{D}$, selects (independently at random) c quadruples $(x_{jv}, y_{jv}; k_{jv}, \ell_{jv})$, $1 \leq v \leq c$, from all possible values over $(\mathbb{Z}_{r+1}, \mathbb{Z}_{r+1}, \mathbb{Z}_{r+1}, \mathbb{Z}_{r+1})$.

2. The dealer computes the share for the last participant $P_{j_{n_j}}$, corresponding to each $Q_i = (x_i, y_i; k_i, \ell_i)$, $1 \leq i \leq c$, using

$$(x_{j_{ni}}, y_{j_{ni}}; k_{j_{ni}}, \ell_{j_{ni}}) = (x_i, y_i; k_i, \ell_i) - \left(\sum_{v=1}^{n_i - 1} (x_{jv}, y_{jv}; k_{jv}, \ell_{jv}) \right) \quad (1)$$

[1] In fact, the secret is the Room square R. However, from information point of view, the information contents of a Room square is the same as the information contents of its critical set.

where computation is done over $\mathbb{Z}_{r+1}$.

3. $\mathcal{D}$ distributes, in private, the shares to the corresponding participants.

Clearly, if participants of an authorised set pool their shares (by adding their corresponding shares over $\mathbb{Z}_{r+1}$) they can construct the critical set. Thus, the reconstruction phase could be as follows.

Secret Reconstruction Phase:

1. Participants of every authorised set $\mathcal{A}_i$ can pool their shares, that is, summation of all shares over $\mathbb{Z}_{r+1}$ gives a critical set which is the secret.

Example: Take a Room square of order 7 given in Table 1. Let the critical set $\mathcal{Q}$ = {(2,7;4,6), (3,4;1,2), (4,2;3,7), (5,2;1,4), (5,3;2,7), (6,4;3,5), (6,6;0,6), (7,5;3,4), (7,6;2,5), (7,7;0,7)} be the secret, S.

Suppose there are three participants P_{11}, P_{12} and P_{13} in the authorised set $\mathcal{A}_1$. Let the participants P_{11} and P_{12} be given the shares s_{11} and s_{12} (selected randomly) such that:

s_{11} = {(4,5;2,3), (3,4;5,5), (1,6;0,3), (2,3;1,5), (7,1;4,7), (4,4;0,7), (2,4;1,2), (6,7;2,6), (0,0;3,5), (6,1;4,7) },

s_{12} = {(3,3;2,3), (4,7;1,0), (1,4;2,5), (5,7;6,7), (5,7;2,4), (3,7;3,4), (2,6;5,6), (7,3;4,6), (7,5;0,4), (4,4;0,1) },

The share s_{13} associated with participant P_{13} can be computed as follows (using equation (1) for every quadruple respectively),

$s_{13} = S - (s_{11} + s_{12})$

= {(3,7;0,0), (4,1;3,5), (2,0;1,7), (6,0;2,0), (1,3;4,4), (7,1;0,2), (2,4;0,6), (2,3;5,0), (0,1;7,4), (5,2;4,7) }.

In secret reconstruction phase, when these three participants collaborate, (i.e., add their shares modulo 8) they can compute the critical set $\mathcal{Q}$, which is the secret.

4.1 Security of the Scheme

In this section we prove that the proposed secret sharing scheme is perfect. That is, the uncertainty of a set of unauthorised collaborating participants (about the secret) is equal to the uncertainty of an outsider who knows nothing about the secret.

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ and let $\Gamma = \{\mathcal{A}_1, \ldots, \mathcal{A}_t\}$ be an access structure over $\mathcal{P}$. Let the critical set $\mathcal{Q} = \{Q_1, \ldots, Q_c\}$ of a Room square R of order r be the secret. Further, let a secret sharing scheme as mentioned earlier realises this access structure.

Observe that the n_j participants of every authorised set $\mathcal{A}_j$ can recover the secret using equation (1). Now we have to show that any set $\mathcal{B} \subset \mathcal{A}_j$

containing $n_j - 1$ participants cannot recover the secret. Clearly, the first $n_j - 1$ participants cannot do so, since they receive independent random tuples as their shares. Consider the $n_j - 1$ participants in the set $\mathcal{B}$ possess the shares $s_{j_1}, \ldots, s_{j_{i-1}}, s_{j_{i+1}}, \ldots, s_{j_{n_j}}$ and the missing participant's share is s_{j_i} such that,

$$s_{j_i} = S - \sum_{\substack{u=1 \\ u \neq i}}^{n_j} s_{j_u} \pmod{r+1}.$$

By summing their shares, they can compute $S - s_{j_i}$. However, they do not know the random tuples of the share s_{j_i} and hence they have no information as to the real value of S. That is, the scheme is perfect.

Acknowledgments

We thank A/Prof. Josef Pieprzyk for helpful conversations. The second author would like to thank the University of Tehran for financial support of his study.

References

[1] G. R. Blakley, Safeguarding cryptographic keys, *Proc. AFIPS 1979 Natl. Computer Conference, New York* **48** (1979), 313–317.

[2] D. Chaum, Computer Systems established, maintained and trusted by mutually suspicious groups, *Memorandum UCB/ERL M179/10* (University of California, Berkeley CA, 1979).

[3] G. R. Chaudhry and J. Seberry, Minimal critical set of a Room square of order 7. *Bull. ICA* **20** (1997), 90.

[4] G. R. Chaudhry and J. Seberry, Secret sharing schemes based on Room squares. *Combinatorics, Complexity and Logic, Proceedings of DMTCS'96* (Springer-Verlag Singapore, 1996), 158–167.

[5] J. Cooper, D. Donovan and J. Seberry, Secret sharing schemes arising from Latin squares. *Bull. ICA* **12** (1994) 33–43.

[6] E. D. Karnin, J. W. Greene and M. E. Hellman, On secret sharing systems. *IEEE Trans. Inf. Th.* **IT-29** (1983), 35–41.

[7] R. C. Mullin and W. D. Wallis, The existence of Room squares. *Aeq. Math.* **13** (1975), 1–7.

[8] A. Shamir, How to share a secret. *Comm. ACM* **22** (1979), 612–613.

[9] 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), 441–497.