Applied Mathematical Sciences, Vol. 6, 2012, no. 56, 2785 - 2790

Perfect Secret Sharing Schemes Based on Generalized Kirkman Squares

Wang Changyuan

School of Mathematics and Statistics
Zaozhuang University, Zaozhuang, 277160, P.R. China
wcyhome2008@126.com

Abstract

Many mathematical structures have been used to model Secret Sharing Schemes. This paper firstly presents a secret sharing schemes based on starter-adder sets of generalized Kirkman squares. Finally, we prove that the scheme is perfect.

Keywords: GKS, starter-adder sets, secret sharing schemes

1 Introduction

Secret sharing is playing the crucial role in the secret data's preservation, the transmission and the use. The first secret sharing scheme is (t, n)-threshold scheme, this plan was separately proposes by Blakley [2] and Shamir [8] in 1979 based on the multi-dimensional spatial point nature and the multinomial interpolation. Secret sharing schemes subsequently have been studied by numerous other authors (see, for example, [3, 9]). A number of mathematical structures have been used to model sharing secret schemes such as polynomials, geometric configurations, block designs, vector spaces, matroids, complete multipartite graphs, orthogonal arrays, Latin squares and Room squares. Cooper, Donovan, and Seberry [4] proposed a secret sharing scheme arising from Latin squares. Chaudhry and Seberry [6] developed secret sharing schemes based on critical sets of Room squares. Both of these schemes are not perfect. In 1998, Chaudhry, Ghodosi and Seberry [5] proposed a perfect secret sharing schemes arising from critical sets of Room Squares. This paper firstly presents a perfect secret sharing scheme based on starter-adder sets of generalized Kirkman squares.

Secret sharing is a method of sharing a secret S among a finite set of participants $\mathcal{P} = \{p_1, p_2, \cdots, p_n\}$ in such a way that if the participants in $\mathcal{A} \subseteq P$ are qualified to know the secret, then by pooling together their partial information, they can reconstruct the secret S; but any set $\mathcal{B} \subseteq \mathcal{P}$, which is not

qualified to know S, cannot reconstruct the secret. The secret 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 $\mathcal{D}$ gives partial information called the share to each participant to share the secret S.

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

A secret sharing scheme is *perfect* if an unauthorised subset of participants $B \subset \mathcal{P}$ 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 set 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.

2 Generalized Kirkman Squares

A *generalized Kirkman square* of side s and order $3n$, or more briefly, a GKS$(s, 3n)$, is an $s \times s$ array in which each cell either is empty or else contains an unordered 3-subset from a $3n$-set X, such that

(a) each row and each column is Latin (namely, every element of X is in precisely one cell of each row and each column), and

(b) every unordered pair from X is in at most one cell of the square.

In fact, a generalized Kirkman square GKS$(s, 3n)$ just is the generalized Howell design GHD$(s, 3n)$ that has been defined in [10] by Wang and Du. A trivial generalized Kirkman square is a GKS$(s, 0)$ having $X = \emptyset$ and consisting of an $s \times s$ array of empty cells. A necessary condition on s and n for the existence of a nontrivial generalized Kirkman square is that $0 < n \leq s \leq \frac{3n-1}{2}$.

Suppose $G = (Z_s \times \ Z_2) \cup \{\infty_1, \infty_2 \cdots, \infty_{3n-2s}\}$, a *starter* in G is a set $S = \{\{x_i, y_i, z_i\} : 1 \leq i \leq 2s - 2n\} \cup \{\{u_i, v_i\} : u_i, v_i$ have different second subscripts, $2s - 2n + 1 \leq i \leq n\}$. That satisfies the following three properties:

(1) S is a partition of $Z_s \times \ Z_2$,

(2) If s is odd, then every element of $Z_s \backslash \{0\}$ occurs at most once as a pure (i, i) difference for $i \in \ Z_2$. If s is even, then every element of $Z_s \backslash \{0, \frac{s}{2}\}$ occurs at most once as a pure (i, i) difference for $i \in \ Z_2$.

(3) every element of Z_s occurs at most once as a mixed (j, k) difference for $j \neq k$, $j, k \in \ Z_2$. (See [1] for definitions of pure and mixed differences.)

Let $A(S)=\{a_1, a_2, \cdots, a_n\}$, where $a_i \in Z_s$ and no element of Z_s occurs more than once in $A(S)$. $A(S)$ is an *adder* for S if $S + A(S) = \{\{x_i + a_i, y_i + a_i, z_i + a_i\} :$

$1 \le i \le 3n-2s\} \cup \{\{u_i+a_i, v_i+a_i\} : 2s-2n+1 \le i \le n\}$, where all arithmetic is done modulo s, is also a partition of $Z_s \times Z_2$.

A *starter-adder set* $\mathcal{Q} = \{Q_1, Q_2, \cdots, Q_n\}$, in a GKS$(s, 3n)$, is a set of quadruples $Q_i = (x_i, y_i, z_i; a_i)$ and triples $Q_j = (x_j, y_j; a_j), 1 \le i \le 2s - 2n, 2s-2n+1 \le j \le n$. In each Q_i, the triple (x_i, y_i, z_i) denotes the starter, a_i denotes the adder corresponding to the starter; In each Q_j, the triple (x_j, y_j) denotes the starter, a_j denotes the adder corresponding to the starter. For convenience (i, j) is denoted by i_j.

Example 1: A starter-adder set of GKS$(9, 24)$:

$$\begin{aligned} \mathrm{X} =& (Z_9 \times Z_2) \cup \{\infty_1, \infty_2, \cdots, \infty_6\}, \\ \mathcal{Q} =& \{(0_0, 1_0, 3_0; 0), (0_1, 1_1, 3_1; 3), (2_0, 2_1; 5), (4_0, 7_1; 1), (5_0, 6_1; 8), (6_0, 8_1; 2), \\ & (7_0, 5_1; 4), (8_0, 4_1; 7)\}. \end{aligned}$$

In 2009 , C. Wang and B. Du[10] proved the following conclusions.

Theorem 2.1 *[10] If there exists a starter S on $(Z_s \times Z_2) \cup \{\infty_1, \infty_2 \cdots, \infty_{3n-2s}\}$ and a corresponding adder $A(S)$, then there exists a GKS$(s, 3n)$.*

Proof: Use the starter-adder pair (S, A) to construct a square K of side s. Label the rows of K by $0, 1, 2, \cdots, s$, and label the columns of K by $0, s-1, s-2, \cdots, 2, 1$. In row 0 and column a_i, place the triple $\{x_i, y_i, z_i\}$ of S for $i = 1, 2, \cdots, 2s-2n$ or the triple $\{u_i, v_i, \infty_{2n-2s+i}\}$ for $i = 2s-2n+1, 2s-2n+2, \cdots, n$, where $\{u_i, v_i\} \in S$. The array is generated cyclically from this row. In row j and column $a_i - j$, place the triple $\{x_i + j, y_i + j, z_i + j\}$ or $\{u_i + j, v_i + j, \infty_{2n-2s+i} + j\}$ for $j = 0, 1, 2, \cdots, s-1$. (All arithmetic is done modulo s and $\infty_i + a = \infty_i$ for all $a \in Z_s$.) Every element of $G = (Z_s \times \{1, 2\}) \cup \{\infty_1, \infty_2, \cdots, \infty_{3n-2s}\}$ occurs precisely once in each row and each column of the resulting array, this is guaranteed by the properties of the starter and the corresponding adder. It is straightforward to check that every unordered pair of G is in at most one cell of the array.

Example 2: Table 1 illustrates GKS$(9, 24)$ which is generated cyclically from the starter-adder set of GKS$(9, 24)$ in example 1.

Theorem 2.2 *[10] There exists starter-adder sets of GKS$(n+1, 3n)$ for $n \in \{7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 23, 25, 26, 27, 29, 31, 32, 33, 39\}$.*

Theorem 2.3 *[10] There exists a GKS$(n+1, 3n)$ for $n \ge 7$ and $n \notin \{37, 38, 41, 44, 46\}$.*

Table 1: This is GKS$(9, 24)$

$0_0 1_0 3_0$	$5_0 6_1 \infty_6$	$8_0 4_1 \infty_5$		$2_0 2_1 \infty_4$	$7_0 5_1 \infty_3$	$0_1 1_1 3_1$	$6_0 8_1 \infty_2$	$4_0 7_1 \infty_1$
$5_0 8_1 \infty_1$	$1_0 2_0 4_0$	$6_0 7_1 \infty_6$	$0_0 5_1 \infty_5$		$3_0 3_1 \infty_4$	$8_0 6_1 \infty_3$	$1_1 2_1 4_1$	$7_0 0_1 \infty_2$
$8_0 1_1 \infty_2$	$6_0 0_1 \infty_1$	$2_0 3_0 5_0$	$7_0 8_1 \infty_6$	$1_0 6_1 \infty_5$		$4_0 4_1 \infty_4$	$0_0 7_1 \infty_3$	$2_1 3_1 5_1$
$3_1 4_1 6_1$	$0_0 2_1 \infty_2$	$7_0 1_1 \infty_1$	$3_0 4_0 6_0$	$8_0 0_1 \infty_6$	$2_0 7_1 \infty_5$		$5_0 5_1 \infty_4$	$1_0 8_1 \infty_3$
$2_0 0_1 \infty_3$	$4_1 5_1 7_1$	$1_0 3_1 \infty_2$	$8_0 2_1 \infty_1$	$4_0 5_0 7_0$	$0_0 1_1 \infty_6$	$3_0 8_1 \infty_5$		$6_0 6_1 \infty_4$
$7_0 7_1 \infty_4$	$3_0 1_1 \infty_3$	$5_1 6_1 8_1$	$2_0 4_1 \infty_2$	$0_0 3_1 \infty_1$	$5_0 6_0 8_0$	$1_0 2_1 \infty_6$	$4_0 0_1 \infty_5$	
	$8_0 8_1 \infty_4$	$4_0 4_1 \infty_3$	$6_1 7_1 0_1$	$3_0 5_1 \infty_2$	$1_0 4_1 \infty_1$	$6_0 7_0 0_0$	$2_0 3_1 \infty_6$	$5_0 1_1 \infty_5$
$6_0 2_1 \infty_5$		$0_0 0_1 \infty_4$	$5_0 3_1 \infty_3$	$7_1 8_1 1_1$	$4_0 6_1 \infty_2$	$2_0 5_1 \infty_1$	$7_0 8_0 1_0$	$3_0 4_1 \infty_6$
$4_0 5_1 \infty_6$	$7_0 3_1 \infty_5$		$1_0 1_1 \infty_4$	$6_0 4_1 \infty_3$	$8_1 0_1 2_1$	$5_0 7_1 \infty_2$	$3_0 6_1 \infty_1$	$8_0 1_0 2_0$

Therefore, a starter-adder set $\mathcal{Q}$ decides completely generalized Kirkman square GKS$(s, 3n)$. That is, a starter-adder set $\mathcal{Q}$ provides minimal information from which GKS$(s, 3n)$ can be reconstructed uniquely.

It should be noted that there is not much known about starter-adder sets of GKS$(s, 3n)$. Through computer search, different starter-adder sets of a generalized Kirkman square GKS$(s, 3n)$ for fixed s and n have been found, therefore there exist different generalized Kirkman squares GKS$(s, 3n)$s for fixed s and n. The number of starter-adder sets of a generalized Kirkman square GKS$(s, 3n)$ for fixed s and n are still unknown. Even if there is only one GKS$(s, 3n)$ for fixed s and n, the secret is difficult to be guess because of great amount of calculation. Consequently, it is significance to present a secret sharing scheme from generalized Kirkman squares.

3 The Scheme

In the perfect secret sharing scheme, it is important to prevent participant's secret part to be disclosed. In fact, the dealer must use the pseudo-share, but cannot use its secret part directly. Similarly, the verifier can use the various participants' pseudo-share to carry on the confirmation, but does not need to know its secret part.

Let $\mathcal{P} = \{p_1, p_2, \cdots, p_n\}$ be the set of all participants in the system and let $\Gamma = \{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_t\}$ be an access structure with t authorised sets over $\mathcal{P}$. Let the starter-adder set of GKS$(s, 3n)$ be the secret. For every authorised set $\mathcal{A}_j$, $1 \leq j \leq t$, of size n_j, the dealer uses the Karnin-Greene-Hellman [7] algorithm to distribute the shares to the participants.

Set-up Phase:

(a) every participant p_{ju}, For $1 \leq u \leq n_j - 1$, the dealer $\mathcal{D}$, selects (independently at random) $2s - 2n$ quadruples $(x_i, y_i, z_i; a_i)$ and $3n - 2s$ triples $(x_j, y_j; a_j)$, from all possible values over $(Z_s \times Z_2, Z_s \times Z_2, Z_s \times Z_2; Z_s)$ and $(Z_s \times Z_2, Z_s \times Z_2; Z_s)$. Let $s_{ju} = \{(x_i, y_i, z_i; a_i) | 1 \leq i \leq 2s - 2n\} \cup \{(x_j, y_j; a_j) | 2s - 2n + 1 \leq j \leq n\}$.

(b) The dealer $\mathcal{D}$ computes the share for the last participant p_{jn_j}, using

$$s_{jn_j} = \mathcal{Q} - \sum_{u=1}^{n_j-1} s_{j_u} \tag{1}$$

where computation is done over Z_s.

(c) The dealer $\mathcal{D}$ 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 $Z_s \times Z_2$) they can construct the starter-adder sets of GKS$(s, 3n)$. Thus, the reconstruction phase could be as follows.

Secret Reconstruction Phase:

Participants of every authorised set $\mathcal{A}_i$ can pool their shares, that is, summation of all shares over Z_s gives a starter-adder set $\mathcal{Q}$ which is the secret.

Example 3: Take GKS$(9, 24)$ given in table 1. Let the starter-adder set $\mathcal{Q}$ in example 1 be the secret S.

Suppose there are three participants p_{11}, p_{12}, 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:

$$\begin{aligned} s_{11} = \{&(4_0, 5_0, 2_1; 3), (3_1, 4_0, 5_1; 5), (1_0, 6_1; 0), (2_0, 3_0; 1), (7_1, 1_1; 4), (4_0, 4_1; 0), \\ &(2_0, 4_0; 1), (6_1, 7_1; 2)\} \\ s_{12} = \{&(3_1, 3_1, 2_0; 3), (4_1, 7_0, 1_1; 0), (1_0, 4_1; 2), (5_0, 7_0; 6), (5_1, 6_1; 2), (3_0, 8_1; 3), \\ &(7_0, 5_1; 4), (8_0, 4_1; 7)\} \end{aligned}$$

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

$$\begin{aligned} s_{13} =& \mathcal{Q} - (s_{11} + s_{12}) \\ =& \{(2_1, 2_1, 8_1; 3), (2_1, 8_1, 6_1; 7), (0_0, 1_1; 3), (6_0, 6_1; 3), (2_0, 8_1; 2), (8_0, 5_1; 8), \\ &(7_0, 5_0; 8), (3_1, 2_1; 7)\} \end{aligned}$$

In secret reconstruction phase, when these three participants collaborate, (i.e., add their shares with superscripts modulo 9 and subscripts modulo 2) they can compute the starter-adder set which is the secret.

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 $\mathcal{P} = \{p_1, p_2, \cdots, p_n\}$, let $\Gamma = \{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_t\}$ be an access structure over $\mathcal{P}$. Let the starter-adder set of GKS$(s, 3n)$ 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 (1). Now we have to show that any set $\mathcal{B} \subseteq \mathrm{A}_j$ containing $n_j - 1$ participants cannot recover the secret. Clearly, the first $n_j - 1$

participants canot 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 $s_{j_1}, \cdots, s_{j_{i-1}}, s_{j_{i+1}}, \cdots, s_{j_{n_j}}$ and the missing participant's share is s_{j_i}, such that $s_{j_i} = \mathcal{Q} - \sum_{u=1, u\neq i}^{n_j} s_{j_u}$ (superscripts modulo s and subscripts modulo 2). By summing their shares, they can compute $\mathcal{Q} - s_{j_i}$. 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 $\mathcal{Q}$. That is, the scheme is perfect.

References

[1] I.Anderson, Combinatorial Designs: Construction Methods, Ellis Horwood Limited, Chichester England, 1990.

[2] G.R.Blakley, Safeguarding cryptographic keys, Proc. AFIPS 1979 NCC, **48**(1979), Arlington, Va., 313-317.

[3] J.C.Benaloh, J.Leichter, Generalized secret sharing and monotone functions, Goldwasser S. Avdances in Cryptology Crypto' 88, LNCS 403, Heidelberg : Springer Verlag, 1990, 27-35.

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

[5] G.R.Chaudhry, H.Ghodosi and J.Seberry, Perfect Secret Sharing Schemes from Room Squares, JCMCC, **28**(1998), 55-61.

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

[7] E.D.Karnin, J.W.Greene and M.E.Hellman, On secret sharing systems,IEEE Transactions on Information Theory, **IT-29**(1983), 35-41.

[8] A.Shamir, How to share a secret, Communications of the ACM, **22**(11), 612-613, 1979.

[9] M.Itoh, A.Saito, T.Nishizeki, Secret sharing scheme realizing general access structure, In IEEE Globecom, 1987, 99-102.

[10] C.Wang and B.Du, Existence of generalized Howell designs of side n+1 and order 3n, UTILITAS MATHEMATICA, **80**(2009), 143-159.

Received: January, 2012