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 \(P = \{p_1, p_2, \ldots, p_n\}\) in such a way that if the participants in \(A \subseteq P\) are qualified to know the secret, then by pooling together their partial information, they can reconstruct the secret \(S\); but any set \(B \subseteq P\), which is not
qualified to know $S$, cannot reconstruct the secret. The secret $S$ is chosen by a special participant $D$, called the dealer, and it is usually assumed that $D \notin P$. The dealer $D$ gives partial information called the share to each participant to share the secret $S$.

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

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

An authorised set $A$ is minimal if $A' \subset A$ and $A' \in \Gamma$ implies that $A' = A$. We only consider monotone access structures in which $A \in \Gamma$ and $A \subset A' \implies A' \in \Gamma$. For such access structures, the collection of minimal authorised set uniquely determines the access structure. In the rest of this paper we use $\Gamma$ 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 $G = (Z_s \times Z_2) \cup \{\infty_1, \infty_2, \ldots, \infty_{3n-2s}\}$, a starter in $G$ is a set $S = \{(x_i, y_i, z_i) : 1 \leq i \leq 2s - 2n\} \cup \{(u_i, v_i) : u_i, v_i \text{ have different second subscripts}, 2s - 2n + 1 \leq i \leq n\}$. 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 $Z_s \setminus \{0\}$ occurs at most once as a pure $(i, i)$ difference for $i \in Z_2$. If $s$ is even, then every element of $Z_s \setminus \{0, \frac{s}{2}\}$ 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 $A(S) = \{a_1, a_2, \ldots, a_n\}$, 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 ≤ i ≤ 3n−2s} ⊔ \{\{u_i + a_i, v_i + a_i\} : 2s−2n+1 ≤ i ≤ n\}, where all arithmetic is done modulo s, is also a partition of \(Z_s \times Z_2\).

A starter-adder set \(Q = \{Q_1, Q_2, \cdots, Q_n\}\), 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 ≤ i ≤ 2s−2n, 2s−2n+1 ≤ j ≤ 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):

\[
X = (Z_9 \times Z_2) \cup \{\infty_1, \infty_2, \cdots, \infty_6\},
\]
\[
Q = \{(0_0, 1_0, 0_3; 0), (0_1, 1_1, 3_1; 3), (2_0, 2_1; 5), (4_0, 7_1; 1), (5_0, 6_1; 8), (6_0, 8_1; 2), (7_0, 5_1; 4), (8_0, 4_1; 7)\}.
\]


**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, · · · , \(s\), and label the columns of \(K\) by 0, \(s−1\), \(s−2\), · · · , 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 \(\infty_1+a = \infty_i\) 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 \(n \geq 7\) and \(n \not\in \{37, 38, 41, 44, 46\}\).
Table 1: This is GKS(9, 24)

<table>
<thead>
<tr>
<th>001030</th>
<th>5061∞0</th>
<th>8041∞5</th>
<th>2021∞4</th>
<th>7051∞3</th>
<th>011131</th>
<th>6081∞2</th>
<th>4071∞1</th>
</tr>
</thead>
<tbody>
<tr>
<td>5081∞1</td>
<td>102040</td>
<td>6071∞0</td>
<td>0051∞5</td>
<td>3031∞4</td>
<td>8061∞3</td>
<td>112141</td>
<td>7001∞2</td>
</tr>
<tr>
<td>8011∞2</td>
<td>6001∞1</td>
<td>203050</td>
<td>7081∞0</td>
<td>1061∞5</td>
<td>4041∞4</td>
<td>0171∞3</td>
<td>213151</td>
</tr>
<tr>
<td>314161</td>
<td>0021∞2</td>
<td>7111∞1</td>
<td>304060</td>
<td>8091∞6</td>
<td>2071∞5</td>
<td>5091∞4</td>
<td>1081∞3</td>
</tr>
<tr>
<td>2001∞3</td>
<td>415171</td>
<td>1013∞2</td>
<td>8021∞4</td>
<td>405070</td>
<td>0011∞6</td>
<td>3081∞5</td>
<td>6061∞4</td>
</tr>
<tr>
<td>7071∞4</td>
<td>3011∞3</td>
<td>516181</td>
<td>2041∞2</td>
<td>0031∞1</td>
<td>506080</td>
<td>1021∞5</td>
<td>4001∞5</td>
</tr>
<tr>
<td>8081∞4</td>
<td>4041∞3</td>
<td>617101</td>
<td>3051∞2</td>
<td>1041∞1</td>
<td>607000</td>
<td>2031∞6</td>
<td>5011∞5</td>
</tr>
<tr>
<td>6021∞5</td>
<td>0001∞4</td>
<td>5031∞3</td>
<td>718111</td>
<td>4061∞2</td>
<td>2051∞1</td>
<td>708010</td>
<td>3041∞6</td>
</tr>
<tr>
<td>4051∞6</td>
<td>7031∞5</td>
<td>1011∞4</td>
<td>6041∞3</td>
<td>810121</td>
<td>5071∞2</td>
<td>3061∞1</td>
<td>801020</td>
</tr>
</tbody>
</table>

Therefore, a starter-adder set $Q$ decides completely generalized Kirkman square GKS($s, 3n$). That is, a starter-adder set $Q$ 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($s, 3n$) 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 $P = \{p_1, p_2, \cdots, p_n\}$ be the set of all participants in the system and let $\Gamma = \{A_t, A_{t+1}, \cdots, A_{t+s}\}$ be an access structure with $t$ authorised sets over $P$. Let the starter-adder set of GKS($s, 3n$) be the secret. For every authorised set $A_j$, $1 \leq j \leq t$, 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 $D$, 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 $D$ computes the share for the last participant $p_{jn}$, using
where computation is done over $\mathbb{Z}_s$.  
(c) The dealer $D$ 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 $\mathbb{Z}_s \times \mathbb{Z}_2$) 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 $A_i$ can pool their shares, that is, summation of all shares over $\mathbb{Z}_s$ gives a starter-adder set $Q$ which is the secret.

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

Suppose there are three participants $p_{11}, p_{12}, p_{13}$ in the authorised set $A_1$. Let the participants $p_{11}$ and $p_{12}$ be given the shares $s_{11}$ and $s_{12}$ (selected randomly) such that:

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

$$s_{12} = \{(3, 1, 2; 3), (4, 7, 1; 0), (1, 4; 2), (5, 7; 6), (5, 6; 2), (3, 8; 3), (7, 5; 4), (8, 4; 7)\}$$

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

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

$$= \{(2, 1, 8; 3), (2, 8, 1; 7), (0, 1; 3), (6, 6; 3), (2, 8; 2), (8, 5; 8), (7, 5; 8), (3, 2; 7)\}$$

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 $P = \{p_1, p_2, \ldots, p_n\}$, let $\Gamma = \{A_1, A_2, \ldots, A_t\}$ be an access structure over $P$. 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 $A_j$ can recover the secret using (1). Now we have to show that any set $B \subseteq A_j$ 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 \( B \) possess the shares \( s_{j1}, \ldots, s_{j_{i-1}}, s_{j_{i+1}}, \ldots, s_{j_{nj}} \) and the missing participant’s share is \( s_{ji} \), such that

\[
s_{ji} = Q - \sum_{u=1, u \neq i}^{n_j} s_{ju} \quad \text{(superscripts modulo } s \text{ and subscripts modulo } 2)\]

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

**References**


**Received:** January, 2012