Resolvable Designs Applicable to Cryptographic Authentication Schemes

K.M. Martin  
Department of Mathematics  
RHBNC  
Egham Hill, Egham Surrey TW20 0EX  

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

P.R. Wild  
Department of Mathematics  
RHBNC  
Egham Hill, Egham Surrey TW20 0EX

Abstract. We consider certain resolvable designs which have application to doubly perfect cartesian authentication schemes. These generalise structures determined by sets of mutually orthogonal latin squares and are related to semi-latin squares and other designs which find application in the design of experiments.

1. Introduction.

Sets of mutually orthogonal latin squares find applications in design of experiments for multifactor experiments (John and Quenouille [4]). They can also be used to construct (optimal) semi-latin squares, known as Trojan squares, which find also application in design of experiments (Bailey [21]).

An orthogonal array (Raghavaro [5]) of strength 2 and index 1 is a $k \times s^2$ matrix with entries from a set of $s$ ($\geq 2$) elements such that any $2 \times s^2$ submatrix contains each possible $2 \times 1$ column vector exactly once. Such an array is equivalent to a set of $k - 2$ mutually orthogonal latin squares. Orthogonal arrays have been used to construct doubly perfect cartesian authentication schemes (Brickell [3]).

When $s$ is a prime power there exist sets of $s - 1$ mutually orthogonal latin squares, and this is the maximum number possible. For $s$ not a prime-power no set of $s - 1$ mutually orthogonal latin squares is known. Interest arises, therefore, in semi-latin squares and doubly perfect cartesian authentication schemes which do not arise from sets of mutually orthogonal latin squares. A semi-latin square arising from a set of $k$ mutually orthogonal latin squares of order $s$ has $ks$ treatments and an authentication scheme arising from such a set has $k$ source states. The problem is to construct semi-latin squares with more treatments and doubly perfect cartesian authentication schemes with more source states than would arise from a set (of maximum size) of mutually orthogonal latin squares.

Brickell [3] has defined an orthogonal multi-array $OMA(k, s; r_1, \ldots, r_k)$ as a $s^2 \times k$ matrix $A = (a_{ij})$ whose entries are subsets satisfying:

(i) $a_{ij}$ is a $r_j$-subset of the set $\{1, 2, \ldots, sr_j\}$;

(ii) given columns $i_1$ and $i_2$ and integers $x_1$ and $x_2$ with $1 \leq x_1 \leq sr_i$ and $1 \leq x_2 \leq sr_i$ there is exactly one row $i$ such that $x_1 \in a_{ij}$ and $x_2 \in a_{ij}$.

Thus, an $OMA(k, s; 1, \ldots, 1)$ is an orthogonal array.

If $A$ is an $OMA(k, s; 1, 1, 1, \ldots, 1)$ then column $\ell (3 \leq \ell \leq k)$ of $A$ determines a semi-latin square on $sr_i$ treatments. The entry in row $i$ and column $j$ of the semi-latin square is $a_{mj}$ where $a_{m_1} = i$ and $a_{m_2} = j$. Superposing (see Bailey [2]) two or more of these semi-latin squares provides other semi-latin squares.

As there do not exist a pair of orthogonal latin squares of order 6 there does not exist an $OMA(4, 6; 1, 1, 1, 1)$. However, the following example (Brickell [3]) is an $OMA(4, 6; 1, 1, 1, 2)$.

**Example 1.**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>1,2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2,4</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>5,6</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>7,8</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>1</td>
<td>9,10</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>1</td>
<td>11,12</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>9,11</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>5,7</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1,10</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2,12</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>1</td>
<td>3,8</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>1</td>
<td>4,6</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>7,12</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2,8</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4,9</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>2</td>
<td>6,10</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>2</td>
<td>1,11</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>2</td>
<td>3,5</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>5,10</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>1,6</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
<td>8,12</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>3,11</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>2</td>
<td>4,7</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>2</td>
<td>2,9</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>4,8</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>10,11</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
<td>2,3</td>
</tr>
</tbody>
</table>
5  4  6  5, 9
5  5  1  6, 12
5  6  2  1, 7
6  1  6  3, 6
6  2  4  9, 12
6  3  5  7, 11
6  4  3  1, 4
6  5  2  2, 5
6  6  1  8, 10

Rows 3 and 4 determine semi-latin squares.

1  2  3  4  5  6
2  1  6  5  3  4
3  6  1  2  4  5
4  5  2  1  6  3
5  3  4  6  1  2
6  4  5  3  2  1

1, 2  3, 4  5, 6  7, 8  9, 10  11, 12
9, 11  5, 7  1, 10  2, 12  3, 8  4, 6
7, 12  2, 8  4, 9  6, 10  1, 11  3, 5
5, 10  1, 6  8, 12  3, 11  4, 7  2, 9
4, 8  10, 11  2, 3  5, 9  6, 12  1, 7
3, 6  9, 12  7, 11  1, 4  2, 5  8, 10

whose superposing provides the following semi-latin square on 18 treatments (replacing 1, 2, 3, 4, 5, 6 of the first square with a, b, c, d, e, f):

\[
\begin{array}{cccccccc}
  a, 1, 2 & b, 3, 4 & c, 5, 6 & d, 7, 8 & e, 9, 10 & f, 11, 12 \\
  b, 9, 11 & a, 5, 7 & f, l, 10 & e, 2, 12 & c, 3, 8 & d, 4, 6 \\
  c, 7, 12 & f, 2, 8 & a, 4, 9 & b, 6, 10 & d, 1, 11 & e, 3, 5 \\
  d, 5, 10 & e, 1, 6 & b, 8, 12 & a, 3, 11 & f, 4, 7 & c, 2, 9 \\
  e, 4, 8 & c, 10, 11 & d, 2, 3 & f, 5, 9 & a, 6, 12 & b, 1, 7 \\
  f, 3, 6 & d, 9, 12 & e, 7, 11 & c, 1, 4 & b, 2, 5 & a, 8, 10 \\
\end{array}
\]

2. Resolvable designs.

An OMA(k, s; r_1, ..., r_k) corresponds to a block design on s^2 points and s(r_1 + ... + r_k) blocks. The blocks are partitioned into k classes C_1, ..., C_k where C_i contains s r_i blocks. The s^2 points correspond to the s^2 rows of A and the s r_i blocks of class C_i correspond to the s r_i elements appearing in column i. The block corresponding to element l in column j is incident with the point corresponding to row i if and only if l ∈ a_ij.

The design D has s^2 points, k r blocks where r = r_1 + ... + r_k, each block contains k points, and each point belongs to r blocks. The blocks are partitioned
into \( k \) classes \( C_1, \ldots, C_k \) such that each point is incident with \( r_i \) blocks of \( C_i \). Such a partition of the blocks is called a resolution of the design \( D \). If \( r_1 = \ldots = r_k = \alpha \) then the design is \( \alpha \)-resolvable as defined by Shrikhande and Raghavarao [7].

This resolvable design has an extra property: any two blocks from distinct classes are incident with exactly one common point. In terms of the semi-latin squares associated with an OMA, this property means that in a square obtained by superposing, treatments from different squares will have concurrence 1. Thus, as discussed by Bailey [2], since it seems likely that the most efficient semi-latin squares have concurrences 0 and 1, the efficiency of the superposed semi-latin square will be highly dependent on the concurrences and efficiencies of the component semi-latin squares. If the only concurrences are 0 and 1 then in the corresponding resolvable design two blocks from distinct classes meet in 1 point and two blocks from the same class meet in 0 or 1 point. Anthony et al [1] discuss a generalisation of an OMA which also provides doubly perfect cartesian authentication schemes. Such a generalisation also corresponds to a block design for which there is a partition of the blocks. However, this partition need not be a resolution as the condition on the blocks within a class is relaxed. No longer is it required that each point be incident with a fixed number \( r_i \) of blocks of class \( C_i \), but only that each point be incident with at least one block of each class. The requirement that two blocks from different classes meet in exactly one point is also relaxed to the requirement that two blocks from different classes meet in at most one point. If such a block design contains two classes each containing \( k \) blocks then the remaining classes determine irregular semi-latin squares (Bailey [2]) whose rows and columns are indexed by the blocks of these two special classes.

The array (Anthony et al [1]) given in Example 2 determines a doubly perfect cartesian authentication scheme.

3. Authentication designs.

A block design is a triple \((P, B, I)\) where \( P \) is a set of points, \( B \) is a set of blocks and \( I \subseteq P \times B \) is an incidence relation between them. We define an Authentication Design \( AD(n, t) \) to be a block design \((P, B, I)\) with \( n^2 \) points \( P \) and \( n \) points per block together with a partition of the blocks \( B \) into classes \( C_1, \ldots, C_k \) such that:

(i) every point belongs to at least one block of each class;
(ii) two blocks from different classes meet in at most one point.

If \( S \) is an \( AD(n, t) \) satisfying the stronger condition

(i') for each class \( C_i \) there is an integer \( r_i \) such that every point belongs to \( r_i \) blocks of \( C_i \);
(ii') then \( S \) is called resolvable and we say \( S \) is a \( RAD(n, t; r_1, \ldots, r_k) \).

If \( S \) is a \( RAD(n, t; r_1, \ldots, r_k) \) then two blocks from different classes meet in exactly one point. (The \( n \) points of a block of class \( C_i \) are each incident with
blocks of $C_i$. If $r_1 = \ldots = r_k = 1$, the semi-latin squares obtained from distinct latin square substructures of $C_i$ are obtained as semi-latin squares. Thus, the semi-latin squares of the complete latin square of the corresponding point and line authentication procedure for which a resolution is required need only be semi-latin squares, but only one point, one line, and the rows whose rows are reliably perfect.

Let $S$ be an $AD(n, t)$. Then $t \leq n + 1$. If $t = n + 1$ then $S$ is an $OMA(n, t; r_1, \ldots, r_k)$. If $r_1 = r_2 = \ldots = r_k = 1$, it is equivalent to a collection of semi-latin squares.

**Lemma 1.** Let $S$ be an $AD(n, t)$. Then $t \leq n + 1$. If $t = n + 1$ then $S$ is an $OMA(n, n + 1; 1, \ldots, 1)$.

**Proof:** Let $P$ be a point of $S$. $P$ is incident with at least one block of each class. Let $x_1, \ldots, x_k$ be blocks incident with $P$ and belonging to distinct classes. Any two of $x_1, \ldots, x_k$ meet only in $P$. Thus, the points incident with $x_1, \ldots, x_k$ account for $1 + t(n - 1)$ points of $S$. Thus, $1 + t(n - 1) \leq n^2$, that is, $t \leq n + 1$. If $t = n + 1$ then $x_1$ is the only block of $C_i$ incident with $P$. It follows that each point is incident with exactly one block of each class.

The bound of the lemma is obtained only when there exist a set of $n + 1$ mutually orthogonal latin squares. Such sets are known only when $n$ is a prime power. When $n$ is not a prime power the following product construction (analogous to results on latin squares and orthogonal arrays) provides examples.

**Example 2.**

\[
\begin{array}{cccc}
1 & 1 & 1 & 1,7 \\
1 & 2 & 2 & 2 \\
1 & 3 & 3 & 5 \\
1 & 4 & 4 & 6 \\
1 & 5 & 5 & 3 \\
1 & 6 & 6 & 4,8 \\
2 & 1 & 2 & 6 \\
2 & 2 & 3 & 1,8 \\
2 & 3 & 6 & 3 \\
2 & 4 & 1 & 2 \\
2 & 5 & 4 & 4,7 \\
2 & 6 & 5 & 5 \\
3 & 1 & 3 & 3 \\
3 & 2 & 6 & 6 \\
3 & 3 & 2 & 4,7 \\
3 & 4 & 5 & 1,8 \\
3 & 5 & 1 & 5 \\
3 & 6 & 4 & 2 \\
4 & 1 & 4 & 8 \\
4 & 2 & 1 & 4 \\
4 & 3 & 5 & 2,6 \\
4 & 4 & 2 & 3,5 \\
4 & 5 & 6 & 1 \\
4 & 6 & 3 & 7 \\
5 & 1 & 5 & 4 \\
\end{array}
\]
\[ \begin{array}{cccc}
5 & 2 & 4 & 3, 5 \\
5 & 3 & 1 & 8 \\
5 & 4 & 6 & 7 \\
5 & 5 & 3 & 2, 6 \\
5 & 6 & 2 & 1 \\
6 & 1 & 6 & 2, 5 \\
6 & 2 & 4 & 7 \\
6 & 3 & 5 & 1 \\
6 & 4 & 3 & 4 \\
6 & 5 & 2 & 8 \\
6 & 6 & 1 & 3, 8 \\
\end{array} \]

The fourth column determines the following irregular semi-latin square:

\[ \begin{array}{cccc}
1, 7 & 2 & 5 & 6 & 3 & 4, 8 \\
6 & 1, 8 & 3 & 2 & 4, 7 & 5 \\
3 & 6 & 4, 7 & 1, 8 & 5 & 2 \\
8 & 4 & 2, 6 & 3, 5 & 1 & 7 \\
4 & 3, 5 & 8 & 7 & 2, 6 & 1 \\
2, 5 & 7 & 1 & 4 & 8 & 3, 6 \\
\end{array} \]

Theorem 1. Let \( S \) be an \( AD(n_1, t_1) \) with classes \( C_1, \ldots, C_{n_1} \), and \( S_2 = (P, B, T) \) be an \( AD(n_2, t_2) \) with classes \( C'_1, \ldots, C'_{n_2} \). Put \( t = \min(t_1, t_2) \). Define a design \( S = (P_1 \times P_2, B, T) \) where \( B = C_1 \times C'_1 \cup \ldots \cup C_i \times C'_i \) and \( (P, Q) \in (x, y) \) if and only if \( P \in x \) and \( Q \in y \). Then \( S \) is an \( AD(n_1 n_2, t) \). If \( S_1 \) is an \( RAD(n_1, t_1, r_1, \ldots, r_{n_1}) \) and \( S' \) is an \( RAD(n_2, t_2; r'_1, \ldots, r'_{n_2}) \), then \( S \) is an \( RAD(n_1 n_2, t; r_1 r'_1, \ldots, r_{n_1} r'_{n_1}) \).

Proof: Clearly, \( S \) has \( (n_1 n_2)^2 \) points and any block \((x, y)\) of \( S \) is incident with the \( n_1 n_2 \) points \((P, Q)\) where \( P \in x \) and \( Q \in y \). We show that \( S \) is an \( AD(n_1 n_2, t) \) with classes \( C_1 \times C'_1, \ldots, C_i \times C'_i \). Let \((P, Q)\) be any point of \( S \). For each \( i \), \( P \) belongs to at least one block \( x \) of \( C_i \) and \( Q \) belongs to at least one block \( y \) of \( C'_i \). Thus, \((P, Q)\) belongs to at least one block \((x, y)\) of \( C_i \times C'_i \). Any block \((x_i, y_i) \in C_i \times C'_i \) meets a block \((x_j, y_j) \in C'_j \times C_j \) in a point \((P, Q)\) such that \( P \in x_i, \ P \in x_j \) and \( Q \in y_i, \ Q \in y_j \). Since there is at most one such \( P \) and at most one such \( Q \), \((x_i, y_i) \) and \((x_j, y_j)\) meet in at most one point.

If \( S_1 \) and \( S_2 \) are resolvable then any point \( P \) of \( S_1 \) is incident with \( r_i \) blocks of \( C_i \) and any point \( Q \) of \( S_2 \) is incident with \( r'_i \) blocks of \( C'_i \). Thus, \((P, Q)\) is incident with \( r_i r'_i \) blocks of \( C_i \times C'_i \) and \( S \) is resolvable.

Generalised Bhaskar Rao Designs or GBRD's (Seberry [6]) also determine authentication designs. Let \( G \) be a group of order \( g \) and let \( A \) be \( GBRD(v, v; g; G) \). \( A = (a_{ij}) \) is a \( v \times g \) array whose columns are labelled by the \( g \) elements of \( G \) and whose entries come from \( G \), such that, for all \( i \neq j \), the elements \( a_{ij} a_{jk}^{-1} \) \((k \in G)\) constitute \( t \) as follows.

\[ P = G \]
\[ B = \{ \} \]

Incidence i

block

The sets \( C \) to exactly \( t \) classes meet.

A skew order \( r \) on a symmetric square of size \( n \) elements for once in each in the array and for \( i \neq j \).

Let \( R \) be by removing with a, b, \ldots, and \( R_{a} \) is Example 3
constitute the $g$ elements of $G$. Define a $RAD(g, v + 1; 1, \ldots, l)$ $S = (P, B, l)$ as follows.

\[ P = G \times G \]
\[ B = \{(h, i) \mid h \in G, 0 \leq i \leq v\} \]

Incidence is determined by:

- block $[h, 0]$ is incident with the points $\{(h, x) \mid x \in G\}$
- block $[h, i](i \neq 0)$ is incident with the points $\{(x, z) \mid x \in G, z_{a_{i(0)}} = h\}$.

The sets $C_t = \{(h, i) \mid h \in G\}$ partition the blocks and every point belongs to exactly one block of each of these classes. Furthermore, blocks from distinct classes meet in exactly one point.

A skew symmetric Room square of side $r$ determines a semi-latin square of order $r$ on $2r$ treatments. This corresponds to an $RAD(r, 3, 1, 1, 2)$. A skew symmetric Room square of side $r$ exists for all odd $r \neq 3, 5$ (Stinson [8]). A Room square of side $r$ is an $r \times r$ array such that each cell either is empty or contains two elements from the set $\{0, 1, \ldots, r\}$ and such that every element appears exactly once in each row and each column and every pair of elements appears exactly once in the array. A Room square is skew symmetric if every diagonal cell contains $0$, and for $i \neq j$ the $i, j$ cell is empty if and only if the $j, i$ cell is not empty.

Let $R$ be a skew symmetric Room square of side $r$. Let $R_0$ be obtained from $R$ by removing the symbol $0$. Let $R_0'$ be obtained from $R_0$ by replacing $1, 2, \ldots, r$ with $a, b, \ldots, g$ and let $R_0'$ be the transpose of $R_0$. Then the superposition of $R_0$ and $R_0'$ is a semi-latin square.

Example 3. The following is a skew symmetric Room square of side 7,

\[
\begin{array}{cccccc}
01 & \_ & 45 & 67 & \_ & \_ \\
57 & 02 & \_ & \_ & 13 & 46 \\
\_ & \_ & 56 & 03 & 12 & \_ \\
\_ & \_ & \_ & 37 & 04 & 26 \\
36 & 14 & \_ & \_ & 05 & \_ \\
24 & \_ & \_ & 35 & 17 & 06 \\
\_ & \_ & \_ & \_ & 16 & 25 \\
\_ & \_ & \_ & \_ & \_ & 34 \\
\end{array}
\]

and determines the following semi-latin square.

\[
\begin{array}{cccccc}
a1 & eg & 45 & 67 & cf & bd \\
57 & b2 & ef & cg & ad & 13 \\
de & 56 & c3 & 12 & bg & 47 \\
f & 37 & ab & d4 & 26 & ce \\
36 & 14 & 27 & bf & e5 & ag \\
c4 & ac & dg & 35 & 17 & f6 \\
b & \_ & df & 16 & ae & 34 \\
g & \_ & \_ & \_ & \_ & 25 \\
\end{array}
\]
References


1. Introduction

All graphs in this paper are simple undirected graphs. For the notation and properties of graphs, see [1]. The number of edges of a graph G is denoted by $\kappa(G)$.

A clique in a graph G is a subset of vertices of G that induce a complete subgraph of G. The clique number of a graph G is denoted by $\omega(G)$. A clique is a connected sets of vertices.

We will often use the notation $G - x$ for the graph obtained from G by deleting the vertex $x$. In this case, the graph $G - x$ may have loops.

For some results in spectral graph theory, see [2]. Further results and references can be found in [3].

An upper bound for the number of edges of a simple graph with $n$ vertices is $\frac{n(n-1)}{2}$. Connected graphs have at least two edges.

JCMC