Utilitas Mathematica, 120: 19–25
DOI:10.61091/um120-03
http://www.combinatorialpress.com/um
Received 09 May 2024, Accepted 23 September 2024, Published 30 September 2024

Combinatorial Press

Article

Key Pre-distribution Schemes via Certain Resolvable Block Designs

Shyam Saurabh[1,*]

[1] Department of Mathematics, Tata College, Kolhan University, Chaibasa, India

* **Correspondence:** shyamsaurabh785@gmail.com

Abstract: Earlier optimal key pre−distribution schemes (KPSs) for distributed sensor networks (DSNs) were proposed using combinatorial designs via transversal designs, affine and partially affine resolvable designs. Here nearly optimal KPSs are introduced and a class of such KPSs is obtained from resolvable group divisible designs. These KPSs are nearly optimal in the sense of local connectivity. A metric for efficiency of KPSs is given. Further an optimal KPS has also been proposed using affine resolvable L_2−type design.

Keywords: Resolvable and affine resolvable designs, Optimal configuration, Group divisible design, L_2−type design, Hadamard product
Mathematics Subject Classification: 94C30, 68R05, 62K10

1. Introduction

Distributed Sensor Networks (DSNs) are ad–hoc mobile networks that include sensor nodes with limited computation and communication capabilities. Lee and Stinson [1, 2] and Saurabh and Sinha [3] obtained optimal key pre−distribution schemes (KPSs) for DSNs from transversal designs, affine and partially affine resolvable designs which are classes of optimal $(v,\ b,\ r,\ k)$−configurations. Those KPSs are optimal in the sense of local connectivity. Here nearly optimal KPSs are obtained from resolvable group divisible designs which are not affine. A metric for efficiency of KPSs is given and an optimal KPS has also been proposed using affine resolvable L_2−type Latin square design. A correspondence between combinatorial designs and KPSs for DSNs may be found in [1, 3].

Eschenauer and Gligor [4] proposed a randomized KPS. Their scheme consists of three phases: *key pre–distribution*, *shared–key discovery* and *path–key establishment*. Lee and Stinson [1] used this framework in the constructions of deterministic KPSs from certain combinatorial designs. In the key pre–distribution phase, a large pool of keys and their key identifiers are generated. Every sensor node is loaded with a fixed number of keys chosen from the key pool, along with their key identifiers. After deployment of the DSNs, any two nodes in the same neighborhood of DSNs look for common keys in order to communicate; this is the shared-key discovery phase. If any two sensor nodes have no common keys, then they try to establish a secure two–hop path for communication which is the *path–key establishment phase* [5].

In this paper, some combinatorial constructions are presented for deterministic optimal and nearly optimal KPSs. The present construction is useful when an optimal $(v,\ b,\ r,\ k)$−configuration is not available for the given $v,\ b,\ r,\ k$. A recent survey on the constructions of KPSs for DSNs using some combinatorial designs may be found in [3].

2. Preliminaries

2.1. Resolvable and Affine Resolvable Designs

A block design $D(v,\ b,\ r,\ k)$ or $(X,\ \mathcal{B})$ is an arrangement of the v elements of a set X into b subsets (blocks) of size k each such that each element of X occurs in exactly r blocks. For $1 \leq i \leq v; 1 \leq j \leq b$, D can be represented by a $v \times b$ incident matrix N defined by $N = \left(n_{ij}\right)_{v\times b}$, where $n_{ij} = \begin{cases} 1 \text{ if } x_i \in B_j \\ 0 \text{ otherwise} \end{cases}$, for $B_j \in \mathcal{B}$. Clearly each row and column sum of N are r and k respectively.

A block design $D(v,\ b,\ r,\ k)$ is said to be resolvable if the b blocks, each of size k can be partitioned into r resolution classes of $\frac{b}{r}$ blocks each such that in each resolution class every point is replicated exactly once. Clearly a necessary condition for a design $D(v,\ b,\ r,\ k)$ to be resolvable is that r divides b. Alternatively, if the incidence matrix N of a block design $D(v, b, r, k)$ may be partitioned in to sub matrices as: $N = (N_1|N_2|\cdots|N_t)$ where each $N_i (1 \leq i \leq t)$ is a $v \times \frac{(v}{k})$ matrix such that each row sum of N_i is one, then the design is resolvable.

Further a resolvable design is said to be affine if any two blocks belonging to different resolution classes intersect in constant number of elements. Some examples of resolvable and affine resolvable designs are given in subsections 2.2–2.4.

2.2. Group Divisible Design

Let $v = mn$ elements be arranged in an $m \times n$ array. A *group divisible* (*GD*) *design* is an arrangement of the $v = mn$ elements in b blocks each of size k such that:

1) Every element occurs at most once in a block;

2) Every element occurs in r blocks;

3) Every pair of elements, which are in the same row of the $m \times n$ array, occur together in λ_1 blocks whereas every other pair of elements occur together in λ_2 blocks.

The non–negative integers: $v = mn, b, r, k,\ \lambda_1$and λ_2 are known as parameters of the GD design and they satisfy the relations: $bk = vr; (n-1)\lambda_1 + n(m-1)\lambda_2 = r(k-1)$. Furthermore, if $r - \lambda_1 = 0$ then the GD design is singular; if $r - \lambda_1 > 0$ and $rk - v\lambda_2 = 0$ then it is semi–regular (*SR*); and if $r - \lambda_1 > 0$ and $rk - v\lambda_2 > 0$, the design is regular (*R*) [6].

Transversal designs are special classes of SRGD designs having $\lambda_1 = 0,\ k = m$. Some recent constructions of GD designs using certain combinatorial matrices may be found in [7, 8].

Example 1. *Consider the following resolvable solution of an SRGD design SR9 with parameters* $v = 8, b = 16, r = 4, k = 2, \lambda_1 = 0, \lambda_2 = 1, m = 2, n = 4$ *as given in* [6]*:*

RI: [(1 5) (2 6) (3 7) (4 8)];
RII: [(2 7) (1 8) (4 5) (3 6)];
RIII: [(4 6) (3 5) (2 8) (1 7)];
RIV: [(3 8) (4 7) (1 6) (2 5)].

The arrangement of $v = 8$ *elements in* 2×4 *array is given as:* $\begin{matrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{matrix}$

2.3. $\mathbf{L_2}$–*type design*

Let $v = n^2$*elements be arranged in an* $n \times n$ *array. An* L_2*–type (Latin square) design is an arrangement of the* $v = n^2$ *elements in* b *blocks each of size* k *such that:*

1. *Every element occurs at most once in a block;*

2. *Every element occurs in* r *blocks;*

3. *Every pair of elements, which are in the same row or in the same column of the $n \times n$ array, occur together in λ_1 blocks whereas every other pair of elements occur together in λ_2 blocks.*

The non–negative integers $v = n^2, b, r, k, \lambda_1$and λ_2 are known as parameters of the L_2 *– type design and they satisfy the relations: $bk = vr; 2(n-1)\lambda_1 + (n-1)^2\lambda_2 = r(k-1)$. Some recent constructions of these designs may be found in* [9].

Example 2. *Consider an L_2−type design LS*26 *as given in* [6] *with parameters $v = b = 9, r = k = 4, n_1 = n_2 = 4, \lambda_1 = 1, \lambda_2 = 2$ whose blocks are given as:*

$$(1269); (2468); (1489); (2579); (2347); (3459); (1567); (3678); (1358)$$

The arrangement of $v = 9$ elements in 3×3 array is given as,

$$\begin{matrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{matrix}$$

2.4. Nearly Optimal KPS and Efficiency

A block design $D(v, b, r, k)$ is said to be a (v, b, r, k)−*configuration* if any two blocks intersect in at most one element. A (v, b, r, k)−configuration is a α−*common intersection design* (α – *CID*) if $\left|\{B_h \in \mathcal{B} : B_i \cap B_h \neq \phi \text{ and } B_j \cap B_h \neq \phi\}\right| \geq \alpha$, whenever $B_i \cap B_j = \phi$ where $B_i, B_j \in \mathcal{B}$ are blocks of the configuration.

This implies that any two disjoint blocks intersect with at least α blocks in common or any two disjoint blocks can be connected through at least α blocks. In general, it is desirable to construct a (v, b, r, k)−configuration with α as large as possible for a given (v, b, r, k). This maximum value of α is denoted by $\alpha^*(v,\ b,\ r,\ k) = k(r-1)$. Such a configuration is called *optimal* [1,2]. The KPSs obtained from optimal configurations are optimal in the sense of local connectivity.

The efficiency of a KPS obtained from a (v, b, r, k)−configuration is defined here as: $E = \frac{\alpha}{k(r-1).}$ Clearly $E = 1$ for an optimal configuration. A KPS will be called nearly optimal if its efficiency $E \approx 1$ when number of nodes is very large. If an optimal KPS for a given v, b, r, k is not available, we go for nearly optimal KPS. Some examples of such KPSs are given in Section 3.

A block design $D(v, b, r, k)$ may be used to obtain a KPS having $N = b$ sensor nodes, k is the number of keys per node with efficiency $E = \frac{\alpha}{k(r-1)}$where α is determined using the corresponding series of designs and $\alpha^* = k(r-1)$ if the KPS is optimal. A nearly optimal KPS will be denoted as $(N,\ k, \alpha,\ E)$.

Example 3. *Consider an affine resolvable SRGD design SR23 as listed in* [6] *with parameters $v = b = 9, r = k = 3, \lambda_1 = 0, \lambda_2 = 1, m = n = 3$ which is a* $(9,\ 9,\ 3,\ 3)$− *configuration. The resolution classes are given as:*

RI: [(1 2 3) (4 5 6) (7 8 9)];

RII: [(1 5 9) (2 6 7) (3 4 8)];

RIII: [(1 6 8) (2 4 9) (3 5 7)].

It is easy to verify that any two disjoint blocks of this design intersect with six blocks in common, i.e., $\left|\{B_h \in \mathcal{B} : B_i \cap B_h \neq \phi \text{ and } B_j \cap B_h \neq \phi\}\right| = 6 = k(r-1) = 6$ for $B_i \cap B_j = \phi$ where $B_i, B_j \in \mathcal{B}$. Hence SR23 is an optimal $(9,\ 9,\ 3,\ 3)$− *configuration which is a 6 – CID. The arrangement of $v = 9$ elements in 3×3 array is given as,*

$$\begin{matrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{matrix}$$

3. The Constructions

3.1. Optimal KPS from Affine Resolvable $\mathbf{L_2}$*−type designs*

Let $A = \left(a_{ij}\right)$ and $B = \left(b_{ij}\right)$ be two $m \times n$ matrices. Then their Hadamard product $A \circledcirc B$ is also an $m \times n$ matrix given by $A \circledcirc B = \left(a_{ij}b_{ij}\right)$.

The following Series I of L_2−type designs may be found in [9]:

Series I: There exists an L_2−type design with parameters:

$$v = n^2,\ b = 2n,\ \ r = 2, k = n,\ \lambda_1 = 1,\ \lambda_2 = 0. \tag{1}$$

The incidence matrix of above design is given as: $N = (N_1|N_2) = \begin{pmatrix} E_1 & I_n \\ E_2 & I_n \\ \vdots & \vdots \\ E_n & I_n \end{pmatrix}$, where $E_i (1 \leq i \leq n)$ is an $n \times n$ matrix whose i^{th} column contains only +1's and 0 elsewhere. Now it is shown below that the design with parameters (1) is affine resolvable.

Since each row sum of N_1 and N_2 is one, the design is resolvable. Clearly the number of resolution classes is $r = 2$ and each class contains $'n'$ blocks. The blocks corresponding to the $'n'$ columns of N_1 form one resolution class (R_1) and the blocks corresponding to the $'n'$ columns of N_2 form another resolution class (R_2). Further let B_i and B_j be two blocks from R_1 and R_2 respectively and let C_i and C_j be columns of N which represent the blocks B_i and B_j respectively. Since the Hadamard product $C_i \circledcirc C_j$ contains one exactly once and remaining entry zero in the resultant column, any two blocks from different resolution classes intersect in exactly one element. Hence the design is affine resolvable.

The above Series I of L_2−type designs can be mapped to an optimal KPS having number of nodes $N = b = 2n$, $'n'$ number of keys per node, $\alpha^* = k(r-1) = n$ and efficiency $E = 1$ [vide Lemma 1 and [3], Section 4.1.2].

Example 4. *For $n = 250$, we obtain an L_2−type design with parameters $v = 62500,\ b = 500,\ \ r = 2, k = 250,\ \lambda_1 = 1,\ \lambda_2 = 0$ which can be mapped to an optimal KPS having number of nodes $N = b = 500$, $n = 250$ keys per node, $\alpha^* = k(r-1) = 250$ and efficiency $E = 1$.*

3.2. Nearly Optimal KPS from Resolvable GD Design

Example 5. *A GD design with parameters: $v = mn, b, r, k, \lambda_1 = 0, \lambda_2 = 1$ is a $(v,\ b,\ r, k)$− configuration and the configuration is optimal if the GD design is affine resolvable and $b = kr$.*

Proof. Consider a GD design with parameters: $v = mn, b, r, k, \lambda_1 = 0, \lambda_2 = 1$. Let B_i and B_j be any two distinct blocks of the GD with above mentioned parameters. Since any pair of distinct elements occur together in either one block or no block, we have $\left|B_i \cap B_j\right| \leq 1$ and hence the above GD design is a $(v,\ b,\ r,\ k)$−configuration. The proof of second part follows from Lemma 1 of [3].

The following Series of resolvable GD designs using generalized Hadamard matrices may be found in [7]:

Series II: There exists a GD design with parameters: $v = p^t\left(p^t - 1\right), r = p^t, k = p^t - 1, b = \left(p^t\right)^2,\ \lambda_1 = 0,\ \lambda_2 = 1, m = p^t - 1, n = p^t$ where p is a prime and $t > 1$.

First, we show that any two disjoint blocks of Series II intersect with $\alpha = (p^t - 2)(p^t - 1)$ blocks in common.

Let $B_i = (\theta_1, \theta_2, \cdots, \theta_k)$ and $B_j = (\rho_1, \rho_2, \cdots, \rho_k)$ be any two disjoint blocks and $B_i \times B_j$ be their cartesian product if we consider them as sets. It is sufficient to count the blocks in which the elements (or unordered pairs) of $B_i \times B_j$ occur. In $B_i \times B_j$ there are total $k^2 = \left(p^t - 1\right)^2$ pairs out of which $'k = p^t - 1'$ pairs of elements belong to the rows of $m \times n$ array on which the GD

design is based and thus these pairs cannot be part of any block of the GD design as $\lambda_1 = 0$. Hence $\alpha = (p^t - 1)^2 - (p^t - 1) = (p^t - 2)(p^t - 1)$.

The Series I may be mapped to a nearly optimal KPS $(N,\ k, \alpha,\ E)$ having $N = b = (p^t)^2$ sensor nodes, $'k = p^t - 1'$ keys per node, $\alpha = (p^t - 2)(p^t - 1)$ and efficiency given as: $E = \frac{\alpha}{k(r-1)} = \frac{(p^t-2)(p^t-1)}{(p^t-1)^2} = 1 - \frac{1}{p^t-1}$ which tends to 1 as $t \to \infty$. □

Example 6. *Consider the following resolvable solution of an SRGD design SR26 with parameters:* $v = 12, b = 16, r = 4, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 4$ *as given in* [6],

RI: [(1 2 3) (7 8 12) (5 9 10) (4 6 11)];
RII: [(1 11 12) (3 5 7) (6 8 10) (2 4 9)];
RIII: [(1 5 6) (3 4 8) (7 9 11) (2 10 12)];
RIV: [(1 8 9) (2 6 7) (3 10 11) (4 5 12)].

The arrangement of $v = 12$ *elements in* 3×4 *array is given as,*

$$\begin{matrix} 1 & 4 & 7 & 10 \\ 2 & 5 & 8 & 11 \\ 3 & 6 & 9 & 12 \end{matrix}$$

Consider disjoint blocks $B_1 = (1\ 2\ 3)$ *and* $B_2 = (7\ 8\ 12)$ *of RI and consider the cartesian product* $B_1 \times B_2 = \{(1\ 7),\ (1\ 8),\ (1\ 12),\ (2\ 7),\ (2\ 8),\ (2\ 12),\ (3\ 7),\ (3\ 8),\ (3\ 12)\}$. *We count the number of blocks in which these pairs occur. Since the pairs* $(1\ 7)$, $(2\ 8)$ *and* $(3\ 12)$ *of elements belong to first, second and third rows respectively of the* 3×4 *array, these pairs cannot be part of any block of SR26 as* $\lambda_1 = 0$. *Clearly the disjoint blocks intersect with six blocks: (1 11 12), (3 5 7), (3 4 8), (2 10 12), (1 8 9), (2 6 7) in common. It can be also verified that any pair of remaining disjoint blocks also intersects with six blocks in common. Hence* $\alpha = 6$ *and SR26 is a* $6-CID$.

The following Table 1 lists nearly optimal KPSs using Series II having number of sensor nodes ≤1000 for different values of p and n with $\lambda_1 = 0, \lambda_2 = 1$. *The design numbers 1–6 listed below may be found in [6].*

No.	SRGD Parameters (v, r, k, b, m, n)	KPSs (N, k, α, E)
1	$(6, 3, 2, 9, 2, 3)$	$(9, 2, 2, 0.50)$
2	$(12, 4, 3, 16, 3, 4)$	$(16, 3, 6, 0.66)$
3	$(20, 5, 4, 25, 4, 5)$	$(25, 4, 12, 0.75)$
4	$(42, 7, 6, 49, 6, 7)$	$(49, 6, 30, 0.84)$
5	$(56, 8, 7, 64, 7, 8)$	$(64, 7, 42, 0.86)$
6	$(72, 9, 8, 81, 8, 9)$	$(81, 8, 56, 0.89)$
7	$(110, 11, 10, 121, 10, 11)$	$(121, 10, 90, 0.90)$
8	$(156, 13, 12, 169, 12, 13)$	$(156, 12, 132, 0.92)$
9	$(240, 16, 15, 256, 15, 16)$	$(256, 15, 210, 0.93)$
10	$(272, 17, 16, 289, 16, 17)$	$(289, 16, 240, 0.94)$
11	$(342, 19, 18, 361, 18, 19)$	$(361, 18, 306, 0.94)$
12	$(506, 23, 22, 529, 22, 23)$	$(529, 22, 462, 0.95)$
13	$(600, 25, 24, 625, 24, 25)$	$(625, 24, 552, 0.96)$
14	$(702, 27, 26, 729, 26, 27)$	$(729, 26, 650, 0.96)$
15	$(812, 29, 28, 841, 28, 29)$	$(841, 28, 756, 0.96)$
16	$(930, 31, 30, 961, 30, 31)$	$(961, 30, 870, 0.97)$

Table 1. Nearly Optimal KPSs from SRGD Designs

4. Resiliency

In a $(v,\ b,\ r,\ k)-$configuration, the compromise of $'s'$ random nodes affect a given link with probability roughly equal to: $fail(s) = 1 - \left(1 - \frac{r-2}{b-2}\right)^s$. Clearly for a larger resiliency, fail(s) should

have a smaller value [1].

Example 7. *For $q = p^t = 31$, Series II yields nearly optimal* $(930, 961, 31, 30)-$ *configuration. This may be mapped to a KPS with 961 sensor nodes. Suppose 10 nodes are compromised, then $fail\,(s) \approx 0.26$. This implies that any given link is affected with a probability of* 26% *when 10 nodes are compromised.*

Furthermore, suppose that N_i and N_j are two neighboring nodes then the probability that N_i and N_j share a common key is: $\Pr_1 = \frac{k(r-1)}{b-1}$. Clearly $\Pr_1 = 1$ for a symmetric balanced incomplete block design having $\lambda = 1$ and $\Pr_1 < 1$ for another block designs.

Let η denote the number of nodes in the intersection of the neighborhoods of the two nodes N_i and N_j where η depends on the size of the physical area where the nodes are deployed, the distance between nodes and on the total number of sensor nodes in the DSN. The probability that N_i and N_j do not share a common key, but there exists a node N_h such that N_h shares a key with both N_i and N_j, is given as follows: $\Pr_2 = (1 - \Pr_1)\left(1 - (1 - \frac{\alpha}{b-2})^{\eta}\right)$. Then the probability that N_i is connected to N_j via a path of length one or two is approximately: $Pr = \Pr_1 + \Pr_2$ [1,3].

Example 8. *The values of $\Pr_1, \Pr_2$ and $fail(s)$ for the optimal KPS obtained from Series I are:*

$$\Pr_1 = \frac{n}{2n-1}, \Pr_2 = \frac{n-1}{2n-1}\left(1 - \left(\frac{n-2}{2(n-1)}\right)^{\eta}\right), \; fail(s) = 0.$$

Clearly the value of $fail(s)$ is the minimum which is desirable for a KPS.

5. Concluding Remarks

Earlier Lee and Stinson [1,2] and Saurabh and Sinha [3] obtained optimal KPSs from transversal designs, affine and partially affine resolvable designs. Here nearly optimal KPS has been introduced and a class of such KPS has also been proposed using resolvable group divisible designs. An optimal KPS has also been obtained using affine resolvable L_2-type design. A metric for efficiency of KPSs is given. Some other resolvable combinatorial designs (which are not affine) such as rectangular designs, balanced incomplete block designs, L_2-type designs and triangular designs may also be used to obtain nearly optimal KPSs under certain conditions. The constructions of these schemes would be taken up as a future work.

Declaration of Competing Interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Lee, J. and Stinson, D., 2005. A combinatorial approach to key pre-distribution for distributed sensor networks. In *IEEE Wireless Communications and Networking Conference, New Orleans, LA, IEEE Communication Society* (pp. 1200–1205).
2. Lee, J. and Stinson, D., 2006. Common intersection designs. *Journal of Combinatorial Designs, 14*(4), pp.251–269.
3. Saurabh, S. and Sinha, K., 2024. Optimal key pre-distribution schemes from affine resolvable and partially affine resolvable designs. *Security and Privacy, 7*(1), p.e334.
4. Eschenauer, L. and Gligor, V. D., 2002. A key-management scheme for distributed sensor networks. In *Proceedings of the 10th ACM Conference on Computer and Communications Security* (pp. 41–47).

5. Bose, M., Dey, A. and Mukerjee, R., 2013. Key predistribution schemes for distributed sensor networks via block designs. *Designs, Codes and Cryptography, 67*, pp.115–136.
6. Clatworthy, W.H., 1973. *Tables of Two-Associate-Class Partially Balanced Designs* (Vol. 63). US Government Printing Office.
7. Saurabh, S. and Sinha, K., 2023. Matrix approaches to constructions of group divisible designs. *Bulletin of the ICA, 97*, pp.83-105.
8. Saurabh, S., 2024. Some matrix constructions of non-symmetric regular group divisible designs. *Bulletin of the ICA, 102*, to appear.
9. Saurabh, S. and Sinha, K., 2022. Some matrix constructions of L_2-type Latin square designs. *Bulletin of the ICA, 95*, 93–104.