Constructions for Key Distribution Pattern using Resolvable Designs

CHEN SHANGDI
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
11csd@163.com

WEI HUIHUI
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
weihuihui1213@gmail.com

Abstract: Key distribution patterns (KDPs) are finite incidence structures satisfying a certain property which makes them widely used in minimizing the key storage and ensuring the security of communication between users in a large network. In this paper we discuss the close connection between resolvable designs and KDPs, and convert the constructions of KDPs into the constructions of resolvable designs. Finally, we give a construction of $(q^2, q, 1)$-ARBIBD and generalize it to constructions of resolvable design with q^n (n is a integer and $n \geq 2$) points by mathematical induction.

Key–Words: Key distribution pattern, finite incidence structure, resolvable design

1 Introduction

Key distribution is one of the major problems in communication and network security. In a large network, the capability of secure communication between every pair of users is required, thus key management becomes a very significant problem.

More formally, suppose v users, P_1, P_2, ..., P_v say, are connected in a network, every pair of users $\{P_i, P_j\}$ requires a distinct cryptographic key known to them but not to the others to secure their communications. When P_i and P_j want to communicate with each other in a secure way, the key distribution centre (KDC) generates a random key to be used by them, and then sends it to P_i and P_j encrypted with their respective key encrypting keys. This type of system clearly requires each user to store $(v-1)$ keys and usually for the KDC to store $\frac{1}{2}v(v-1)$ keys. The disadvantage is that the large amount of key storage are required both at each user and at the KDC in a large network.

Key distribution patterns have been studied extensively and under different guises.

In 1988, C. Mitchell and F. Piper in [1] proposed a certain special kind of finite incidence structure called *key distribution patterns* (KDPs) for reducing the large storage requirement and gave some simple examples of $(\mathcal{G}, \mathcal{F})$-KDPs and made use of previous research in the area of design theory in order to construct KDPs.

The second approach to $(\mathcal{G}, \mathcal{F})$-KDP constructions is to construct $(\mathcal{G}, \mathcal{F})$-KDPs from other mathematical objects. C. M. O'Keefe [3] used special finite geometric structures such as Inversive, Minkowski planes and Laguerre planes to construct (t, ω)-KDPs with storage requirements lower than the trivial distribution system. K. A. S. Quinn [7, 8] constructed KDPs from finite projective planes and affine planes. Stinson [11, 12] used design theory, orthogonal and perpendicular arrays in order to construct specific $(\mathcal{G}, \mathcal{F})$-KDPs with particular properties.

The third approach to $(\mathcal{G}, \mathcal{F})$-KDP constructions uses probabilistic techniques. In 1994, Ruszink'o [9] used a combinatorial approach to give an upper bound for (t, ω)-KDPs. In 1991 and 1999, Quinn [7, 8] presented several lower bounds for (t, ω)-KDPs using combinatorics and design theory. In 1997 and 1998, Stinson [11, 12] used resilient functions for improving the efficiency of $(\mathcal{G}, \mathcal{F})$-KDPs.

Manjusri Baus [6] gave a construction of resolvable designs of order p^2, where p is a prime. S. Kageyama [10] gave an inequality about the number of b for RBIBDs which are not affine resolvable.

In this paper, we begin with Section 1 where we highlight the importance of key management and discuss previous work completed by other authors. Section 2 contains the mathematical structure necessary for this paper. Section 3 focusses upon key distribution patterns which form the basis of this thesis, presents the relationships between Resolvable designs and KDPs and discuss the bound on the number of blocks. Section 4 we examine different approaches to the construction of resolvable design with q^2, q^3

points and sets up the general situation with q^n points by mathematical induction. Section 5 summarizes the main contributions of this thesis and highlight areas of future study that follow from our work.

2 Finite Incidence Structures and Resolvable designs

The subject combinatorial design is extensively used in this paper. We begin with some definitions about design theory adopted from [1, 4].

Definition 1 *A finite incidence structure $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P}$ is a nonempty finite set of elements called points, $\mathcal{B}$ is a collection of nonempty finite subset of $\mathcal{P}$ called blocks and $\mathcal{I} \in \mathcal{P} \times \mathcal{B}$ is a binary relation between $\mathcal{P}$ and $\mathcal{B}$.*

If $(P, x) \in \mathcal{I}$, where $P \in \mathcal{P}$ and $x \in \mathcal{B}$, then we say that P is incident with x or x is incident with P.

We usually use v and b denotes the total number of points and blocks respectively, i.e., $v = |\mathcal{P}|$, $b = |\mathcal{B}|$, and call v be the order of $\mathcal{P}$.

Definition 2 *Let $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a finite incidence structure, where $\mathcal{P} = \{P_1, P_2, \cdots, P_v\}$ and $\mathcal{B} = \{B_1, B_2, \cdots, B_b\}$. For $1 \leq i \leq v$, $1 \leq j \leq b$, let*

$$a_{ij} = \begin{cases} 1, \text{ If } i \in B_j \\ 0, \text{ If } i \notin B_j \end{cases},$$

then the 0-1 matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1b} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2b} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3b} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{v1} & a_{v2} & a_{v3} & \cdots & a_{vb} \end{pmatrix}$$

called the incidence matrix of $\mathcal{K}$.

We sometimes specify an incidence structure by listing sets of points, each set incident with a block. It is possible for two blocks of a structure to be incident with the same set of points. When this happens we say that the structure has repeated blocks. When a structure has no repeated blocks, we often identify a block with the set of points with which it is incident.

A structure is said to be uniform if every block is incident with a constant number of points (which we usually denote by k), and regular if every point is incident with a constant number of blocks (usually denoted by r).

If a structure is not uniform, for $1 \leq j \leq b$, let $k_j = |(x_j)|$, where (x_j) represent the se of points incident with a block x_j. If a structure is not regular, for $1 \leq i \leq v$, let $r_i = |(P_i)|$, where (P_i) represent the set of blocks incident with a point P_i. Finally, for $1 \leq i, j \leq v$, $i \neq j$, let $\lambda(i, j) = |(P_i) \cap (P_j)|$ and $s(i, j) = |(x_i) \cap (x_j)|$, where $(P_i) \cap (P_j)$ denotes the set of blocks incident with both P_i and P_j, and $(x_i) \cap (x_j)$ denotes the set of points incident with both x_i and x_j.

A *design* is a uniform structure with no repeated blocks.

Example 3 *[7] The following structure with point set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ and block set*

$$\{1, 3, 5, 7\}, \{1, 4, 5, 8\}, \{1, 3, 6, 8\}, \{1, 4, 6, 7\},$$

$$\{2, 4, 6, 8\}, \{2, 3, 6, 7\}, \{2, 4, 5, 7\}, \{2, 3, 5, 8\},$$

$$\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\},$$

$$\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}.$$

Clearly, it is a finite incidence structure but not a design because the block set above is regular, but not uniform.

Definition 4 *Let v, k, λ and t be integers such that $v \geq k \geq 2$, $\lambda \geq 1$ and $t \geq 0$. Let X be a set of elements, called points, and let $\mathcal{B}$ be a collection of nonempty subsets of X, called blocks. The pair $(X, \mathcal{B})$ is called a t-(v, k, λ)* design *or, simply, a t-*design*, if the following properties are satisfied:*

1. *$|X| = v$.*
2. *Each block contains exactly k points.*
3. *Every subset of t distinct points is contained in exactly λ blocks.*

Remark 5 *If $t = 2$, the pair $(X, \mathcal{B})$ is called a (v, k, λ) balanced incomplete block design or, simply, a (v, k, λ)-BIBD.*

Theorem 6 *[4] In a (v, k, λ)-BIBD, the number of blocks which contain any given point is equal to*

$$r = \frac{\lambda(v-1)}{k-1}.$$

the total number of blocks is equal to

$$b = \frac{\lambda v(v-1)}{k(k-1)}.$$

Definition 7 *Let $(X, \mathcal{B})$ be a (v, k, λ)-BIBD. A parallel class in $(X, \mathcal{B})$ is a subset of disjoint blocks from $\mathcal{B}$ whose union is X. A partition of $\mathcal{B}$ into several parallel classes is called a resolution, and $(X, \mathcal{B})$ is said to be resolvable if $\mathcal{B}$ has a resolution. A resolvable (v, k, λ)-BIBD is also denoted by (v, k, λ)-RBIBD.*

Theorem 8 *[4] Let $(X, \mathcal{B})$ be a (v, k, λ)-BIBD. If $(X, \mathcal{B})$ has a parallel class, then $k|v$ and each parallel class contains v/k blocks, and if $(X, \mathcal{B})$ is resolvable then $\mathcal{B}$ is partitioned into $b/(v/k) = r$ parallel classes.*

Theorem 9 *[4](**Bose Inequality**) If there exists a nondegenerate resolvable $(v,\ b, r, k, \lambda)$-BIBD, then $b \geq v + r - 1$.*

Theorem 10 *[4] In a (v, b, r, k, λ)-BIBD, $b \geq v+r-1$ if and only if $r \geq k + \lambda$.*

Definition 11 *A resolvable BIBD with $b = v + r - 1$ (or, equivalently, $r = k + \lambda$) is called affine resolvable. Affine resolvable BIBD is abbreviated as AR-BIBD.*

Theorem 12 *[10] If there exists a resolvable (v, b, r, k, λ)-BIBD which is not affine resolvable, then $b \geq 2v + r - 2$ and $r \geq \lambda + 2k$.*

In addition, from Theorem 1.1 of [12], for a (v, b, r, k, λ)-BIBD, we know

$$b \geq \lceil \frac{(v-k)^3}{v^2} \rceil + 2r - \lambda.$$

Then for a resolvable BIBD with $v = sk$, $b = sr$, we obtain

Theorem 13 *[13] For a resolvable BIBD with parameters $v = sk, b, r, k, \lambda$, and with an integer $s \geq 2$, an inequality*

$$b \geq 2 + \lfloor \frac{(v-k)(b-r-1)^2}{b-v-r+k+(b-2r+\lambda)(v-k-1)} \rfloor$$

Theorem 14 *[13] For a resolvable BIBD with parameters $v = sk, b, r, k, \lambda$, and when $s = 2$*

$$b \geq \frac{rk(k-1)}{r-k+\lambda(k-1)} \geq 4\lambda + 2 \geq v + r - 1,$$

when $s \geq 3$

$$b \geq s^2\lambda + s \geq \frac{rk(k-1)}{r-k+\lambda(k-1)} \geq v + r - 1$$

hold. The equality signs hold at the same time when and only when the BIBD is affine resolvable in each case.

3 Key Distribution Patterns and Resolvable designs

3.1 Key Distribution Patterns

Mitchell and Piper were the first to investigate key distribution pattern and gave the definition of ω-KDP [1].

Definition 15 *Let $v \geq 3$ and let ω be an integer with $1 \leq \omega < v - 2$. A ω-KDP on v points is a finite incidence structure $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with v points such that for any pair of points P_i, P_j, we have*

$$(P_i) \bigcap (P_j) \not\subseteq \bigcup_{i=1}^{\omega} (Q_i),$$

for any points $Q_1, \cdots, Q_\omega \in \mathcal{P} \setminus \{P_i, P_j\}$.

Many other papers also use this concept, see G_n^ω-KDP in [2].

Definition 16 *A finite incidence structure $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a G_n-KDP, iff the internal structure of $\mathcal{K}$ at $P \in \mathcal{P}$ is a G_{n-1}-KDP. And a G_n-KDP has some properties which secure against collusion by up to some number ω of users, such a special G_n-KDP is called G_n^ω-KDP.*

In this paper, it also showed that any $(n+1)$-(v, k, λ) design is a G_n-KDP, and a G_{n+1}-KDP is again a G_n-KDP, that is, G_{n+1}-KDP$\subset$ G_n-KDP$\subset$$G_n$-KDP$\subset\cdots (n \geq 2)$.

Julia Novak [5] gave the definition of generalized key distribution pattern as follows. Let $2^{\mathcal{P}}$ be the set of all subset of users, then $\mathcal{G} \subseteq 2^{\mathcal{P}}$ be the collection of all privileged subsets of users who can calculate the secret key, and $\mathcal{F} \subseteq 2^{\mathcal{P}}$ be the collection of all forbidden subsets of users who are prohibited to obtain some information about key.

Definition 17 *Let $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a finite incidence structure and let $\mathcal{G}$ and $\mathcal{F}$ be families of non-empty subsets of $\mathcal{P}$. Then $\mathcal{K}$ is called a ($\mathcal{G}$, $\mathcal{F}$)- Key Distribution Pattern (or ($\mathcal{G}$, $\mathcal{F}$)-KDP), if for all $G \in \mathcal{G}$ and $F \in \mathcal{F}$ such that $G \cap F = \emptyset$,*

$$\bigcap_{P \in G} (P) \not\subseteq \bigcup_{Q \in F} (Q).$$

In many situations it is appropriate to define the privileged and forbidden subsets of a general ($\mathcal{G}$, $\mathcal{F}$)-KDP according to their cardinality. More specifically, we define:

1. the set of privileged subsets to be all sets of users of some maximum specified cardinality, say t;

2. the set of forbidden subsets to be all sets of users of some maximum specified cardinality, say ω.

Then using the above notations, we can rewrite the Definition 17 in the following form which are more specific.

Definition 18 *Let $\mathcal{P}$ be the set of all users in the network, then for $t, \omega \geq 1$, $\mathcal{G} = \{G \in 2^{\mathcal{P}} : 1 \leq |G| \leq t\}$ and $\mathcal{F} = \{F \in 2^{\mathcal{P}} : 1 \leq |F| \leq \omega\}$, we refer to ($\mathcal{G}$, $\mathcal{F}$)-KDP defined in this way as cardinality, or more precisely as (t, ω)-KDP.*

In this paper we use another definition of ($\mathcal{G}$, $\mathcal{F}$)-KDP, which is essentially the dual formulation of the one given in [1].

Definition 19 *Let $\mathcal{P} = \{1, 2, \cdots, v\}$ be the set of network users, $\mathcal{B} = \{B_1, B_2, \cdots, B_b\}$ be families of non-empty subsets of network users, and $\mathcal{G}$, $\mathcal{F}$ be families of non-empty subsets of network users, we say that $(\mathcal{P}, \mathcal{B})$ is a ($\mathcal{G}$, $\mathcal{F}$)-KDP if*

$$\{B_j | G \subseteq B_j, F \cap B_j = \emptyset\} \neq \emptyset$$

for all $G \in \mathcal{G}$ and $F \in \mathcal{F}$ and $G \cap F = \emptyset$.

Note that a KDP can conveniently be represented by $v \times b$ incidence matrix $A = (a_{ij})$ which is defined as follows

$$a_{ij} = \begin{cases} 1, \text{ If } i \in B_j \\ 0, \text{ otherwise} \end{cases}$$

and for any user $i \in \mathcal{P}$, we define

$$r_i = |\{B_j : i \in B_j\}|.$$

3.2 Applications of Resolvable designs to KDPs

From [2], we know that 3-design is a $(2, 1)$-KDP, so we begin with 3-design.

Theorem 20 *A resolvable $(2k, k, \lambda)$-BIBD is a $(2, 1)$-KDP.*

Proof: We just need to prove that the resolvable $(2k, k, \lambda)$-BIBD is a 3-design.

Suppose that $(X, \mathcal{B})$ is a resolvable $(2k, k, \lambda)$-BIBD with $b = 2r$ blocks and $\mathcal{B}$ is partitioned into r parallel classes. Each parallel class contains two blocks.

Let x, y, z be any three distinct points of X and let C_x be the number of blocks in $\mathcal{B}$ which contain x, but not y and z, and let C_{xy} be the number of blocks in $\mathcal{B}$ which contain x and y, but not z.

We define C_y, C_z, C_{xz}, C_{yz} in the same way. Also, denote the number of blocks in $\mathcal{B}$ which contain all x, y, z by C_{xyz}. Every pair of distinct points is contained in exactly λ blocks, then

$$C_{xy} + C_{xyz} = C_{yz} + C_{xyz} = C_{xz} + C_{xyz} = \lambda.$$

The number of blocks in $\mathcal{B}$ which contain x is equal to

$$C_x + C_{xy} + C_{xz} + C_{xyz} = r.$$

Since each parallel class contains two blocks, we obtain $C_x = C_{yz}$. Then

$$C_{yz} + C_{xy} + C_{xz} + C_{xyz} = r.$$

From the above equations, it follows that

$$C_{xyz} = \frac{3\lambda - r}{2} = \frac{\lambda(k-2)}{2(k-1)}.$$

Therefore $(X, \mathcal{B})$ is a 3-$(2k, k, \frac{\lambda(k-2)}{2(k-1)})$ design, so it is a $(2, 1)$-KDP. □

We give $(2, 1)$-KDPs derived from n-dimensional affine space $AG(n, \mathbb{F}_q)$ over $\mathbb{F}_q$, where $n \geq 2$. We first make a brief introduction of the relevant knowledge of affine space and the specific content can be found in [4]. Let

$$\mathbb{F}_q^n = \{(x_1, x_2, \cdots, x_n) : x_i \in \mathbb{F}_q\}$$

be the set of points of $AG(n, \mathbb{F}_q)$. Clearly, $\mathbb{F}_q^n = |q^n|$. $\mathbb{F}_q^n$ has an n-dimensional vector space structure if for all $(x_1, x_2, \cdots, x_n)$, $(y_1, y_2, \cdots, y_n) \in \mathbb{F}_q^n$ and $x \in \mathbb{F}_q$ we define

$$(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n)$$

$$= (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n),$$

$$x(x_1, x_2, \cdots, x_n) = (xx_1, xx_2, \cdots, xx_n).$$

Let V be an r-dimensional vector subspace of $\mathbb{F}_q^n$, where $0 \leq r \leq n$, and let $(a_1, a_2, \cdots, a_n)$ be any point of $\mathbb{F}_q^n$. The set of points in the coset $V + (a_1, a_2, \cdots, a_n)$ which is defined by

$$V + (a_1, a_2, \cdots, a_n) = \{(x_1, x_2, \cdots, x_n)$$

$$+(a_1, a_2, \cdots, a_n) : (x_1, x_2, \cdots, x_n) \in V\}$$

is called an affine r-flat, and the dimension of an r-flat is defined to be r. Clearly, $|V + (x_1, x_2, \cdots, x_n)| = |q^r|$.

In particular, 0-flats are points, 1-flats are lines, 2-flats are planes, and $(n-1)$-flats are hyperplanes. An r-flat is said to be incident with an s-flat, if the r-flat contains or is contained in the s-flat. Then the point

set $\mathbb{F}_q^n$, together with the r-flat ($0 \leq r \leq n$) and the incidence relation among them defined above called the n-dimensional affine space over $\mathbb{F}_q$ and denoted by $AG(n, \mathbb{F}_q)$.

The following theorem will be used in the later proof process.

Theorem 21 *[15] In $AG(n, \mathbb{F}_q)$, the Anzahl theorems as follows.*

(1) The number of m-flat in $AG(n, \mathbb{F}_q)$ for $0 \leq m \leq n$, is equal to

$$q^{n-m} \begin{bmatrix} n \\ m \end{bmatrix}_q,$$

where $\begin{bmatrix} n \\ m \end{bmatrix}_q$ is called Gaussian coefficient

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{\prod_{i=n-m+1}^{n} (q^i - 1)}{\prod_{i=1}^{m} (q^i - 1)}$$

and agree $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$ for all integer n.

(2) The number of k-flat in $AG(n, \mathbb{F}_q)$ contained in a given m-flat for $0 \leq k \leq m \leq n$, is equal to

$$q^{m-k} \begin{bmatrix} m \\ k \end{bmatrix}_q.$$

(3) The number of m-flat in $AG(n, \mathbb{F}_q)$ containing a given k-flat for $0 \leq k \leq m \leq n$, is equal to

$$\begin{bmatrix} n-k \\ m-k \end{bmatrix}_q.$$

Example 22 *Let $n \geq 2$, let X denote the set of points in $AG(n, \mathbb{F}_2)$ and $\mathcal{B}$ denote the set of hyperplanes in $AG(n, \mathbb{F}_2)$, then $(X, \mathcal{B})$ is a $(2, 1)$-KDP.*

Proof: Clearly, $(X, \mathcal{B})$ is resolvable because any subspace together with all of its cosets forms a parallel class. Then we just need to prove that the design is a BIBD.

According to Theorem 21, the number of points in $AG(n, \mathbb{F}_2)$ is equal to

$$v = 2^n \begin{bmatrix} n \\ 0 \end{bmatrix}_2 = 2^n.$$

The number of points in $AG(n, \mathbb{F}_q)$ contained in a given $(n-1)$-flat is equal to

$$k = 2^{n-1} \begin{bmatrix} n-1 \\ 0 \end{bmatrix}_2 = 2^{n-1}.$$

The number of blocks that contain two given points is the same as the number of $(n-1)$-dimensional subspace that contain one given line, which equal to

$$\lambda = \begin{bmatrix} n-1 \\ n-2 \end{bmatrix}_2 = 2^{n-1} - 1.$$

Therefore $(X, \mathcal{B})$ is a resolvable $(2^n, 2^{n-1}, 2^{n-1}-1)$-BIBD and the $b = 2(2^n - 1)$ blocks are partitioned into $r = 2^n - 1$ parallel classes. Hence $(X, \mathcal{A})$ is a $(2, 1)$-KDP.

Clearly, the $(2, 1)$-KDP given above with v nodes and $b = 2(v-1)$ keys. It's storage requirements lower than the trivial distribution system with v nodes and $b = C_v^2 = \frac{v(v-1)}{2}$ keys.

Then we generalize Theorem 20 to get ($\mathcal{G}$, $\mathcal{F}$)-KDP.

Theorem 23 *A resolvable (v, k, λ)-BIBD is a ($\mathcal{G}$, $\mathcal{F}$)-KDP for given families of privileged subsets $\mathcal{G}$ and forbidden subsets $\mathcal{F}$.*

Proof: let $v = sk$, $1 \leq t \leq s$. Suppose that a resolvable (v, k, λ)-BIBD has r parallel classes denoted by

$$\Pi_1 = \{B_1^1, \cdots, B_t^1, B_{t+1}^1, \cdots, B_s^1\},$$
$$\cdots\cdots$$
$$\Pi_i = \{B_1^i, \cdots, B_t^i, B_{t+1}^i, \cdots, B_s^i\},$$
$$\cdots\cdots$$
$$\Pi_r = \{B_1^r, \cdots, B_t^r, B_{t+1}^r, \cdots, B_s^r\}.$$

Let $i = 1, 2, \cdots, r$ and we select

$$\mathcal{G} = \{G | G \in 2^{B_1^i}, G \in 2^{B_2^i}, \cdots, \text{or } G \in 2^{B_t^i}\} \backslash \{\emptyset\},$$

and

$$\mathcal{F} = \{F | F \in 2^{B_{t+1}^i}, F \in 2^{B_{t+2}^i}, \cdots, \text{or } F \in 2^{B_s^i}\}.$$

Obviously, for any $G \in \mathcal{G}$, $F \in \mathcal{F}$, it must have $G \cap F = \emptyset$, there exists some B_j^i such that $G \subseteq B_j^i$ ($1 \leq j \leq t$) but $F \cap B_j^i = \emptyset$, it implies that

$$\{B_j^i \mid G \subseteq B_j^i, F \cap B_j^i = \emptyset\} \neq \emptyset.$$

According to definition 19, it is easy to see that a resolvable (v, k, λ)-BIBD is a ($\mathcal{G}$, $\mathcal{F}$)-KDP for given $\mathcal{G}$ and $\mathcal{F}$. □

The most important problem in our study is constructing efficient ($\mathcal{G}$, $\mathcal{F}$)-KDPs (that is, ($\mathcal{G}$, $\mathcal{F}$)-KDPs with the number of blocks is minimised) for given families of privileged $\mathcal{G}$ and forbidden subsets $\mathcal{F}$. And Julia Novak raised some questions on this.

Problem 24 *[5] Given a set of points $\mathcal{P}$ and families of non-empty subsets $\mathcal{G}$ and $\mathcal{F}$ of $\mathcal{P}$, construct an incidence structure $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, such that $\mathcal{K}$ is a ($\mathcal{G}$, $\mathcal{F}$)-KDP and*

$$|\mathcal{B}|/|(G, F) \in \mathcal{G} \times \mathcal{F} : G \cap F = \emptyset|$$

is as small as possible.

Problem 25 *[5] For a given ($\mathcal{G}$, $\mathcal{F}$)-KDP, $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, calculate a "good" lower bound for $|B|$.*

According to this, we discuss the lower bound on the number of blocks in a general ($\mathcal{G}$, $\mathcal{F}$)-KDP for given $\mathcal{G}$ and $\mathcal{F}$. Let

$$f(t) = \frac{|\mathcal{B}|}{|(G, F) \in \mathcal{G} \times \mathcal{F} : G \cap F = \emptyset|}$$

$$= \frac{b}{(2^k - 1)t \cdot 2^k(s - t)}$$

For a (v, k, λ)-BIBD, b and k are constants. It is easy to verify that the function $f(t)$ obtains the minimum when $t(s - t)$ obtains the maximum.

Additionally, we know $a + b \geq 2\sqrt{ab}$ equivalent to the inequality

$$ab \leq \frac{(a + b)^2}{4},$$

the equality holds when $a = b$. So $f(t)$ obtains the minimum, when $s - t = t$, i.e., $t = [\frac{s}{2}]$. It implies that the ($\mathcal{G}$, $\mathcal{F}$)-KDP is more efficient where

$$\mathcal{G} = \{G | G \in 2^{B_1^i},\ G \in 2^{B_2^i},\ \cdots,\ \text{or}\ G \in 2^{B_{[\frac{s}{2}]}^i}\} \backslash \{\emptyset\},$$

and

$$\mathcal{F} = \{F | F \in 2^{B_{[\frac{s}{2}]+1}^i},\ F \in 2^{B_{[\frac{s}{2}]+2}^i},\ \cdots,\ \text{or}\ F \in 2^{B_s^i}\}.$$

Example 26 *Let q be a prime power, $1 \leq m \leq n - 1$ and $n \geq 2$. Let X denote the set of points in $AG(n, \mathbb{F}_q)$ and let $\mathcal{B}$ denote the set of m-flats in $AG(n, \mathbb{F}_q)$, then $(X, \mathcal{B})$ is a ($\mathcal{G}$, $\mathcal{F}$)-KDP where $\mathcal{G}$ and $\mathcal{F}$ defined as Theorem 23.*

Proof: The proof is similar to Example 22, we prove that $(X, \mathcal{B})$ is a resolvable $(q^n, q^m, \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q)$-BIBD and the $b = q^{n-m} \begin{bmatrix} n \\ m \end{bmatrix}_q$ blocks are partitioned into $r = \begin{bmatrix} n \\ m \end{bmatrix}_q$ parallel classes. Therefore, $(X, \mathcal{B})$ is a ($\mathcal{G}$, $\mathcal{F}$)-KDP. And the ($\mathcal{G}$, $\mathcal{F}$)-KDP is more efficient when $t = [\frac{q^{n-m}}{2}]$.

4 Constructions of resolvable designs

Next we will give some constructions of resolvable designs with q^n $(n \geq 2)$ points, where n is a integer, we begin with $n = 2$.

Construction 1 Consider a prime number q and denote the elements of $\mathbb{F}_q$ by $1, 2, \cdots, q$. Let

$$X = \mathbb{F}_q \times \mathbb{F}_q = \{(x, y) | x, y \in \mathbb{F}_q\}.$$

For convenience let a_{xy} represent the point (x, y), then consider the following steps.

Step 1 Arrange the q^2 points in a $q \times q$ matrix according to the column order, we obtain

$$\Pi_0 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1q} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2q} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3q} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{q1} & a_{q2} & a_{q3} & \cdots & a_{qq} \end{pmatrix}.$$

Regarding every row of matrix Π_0 as a block, we obtain q blocks as follows

$$B_j^0 = \{a_{j1},\ a_{j2}, \cdots, a_{jq}\}\ (1 \leq j \leq q).$$

Obviously,

$$X = \bigcup_{j=1}^{q} B_j^0,$$

it means that B_j^0 $(1 \leq j \leq q)$ can be regard as a parallel class and denote it by

$$\Sigma_0 = \{B_j^0 \mid 1 \leq j \leq q\}.$$

Step 2 For the $q \times q$ matrix Π_0, we define the sequence of elements

$$a_{11},\ a_{22},\ a_{33}, \cdots, a_{qq}$$

as the *main diagonal* or the *0-th diagonal* of matrix Π_0. Let $1 \leq i \leq q - 1$, then the sequence of elements

$$a_{i+1,1},\ a_{i+2,2},\ a_{i+3,3}, \cdots, a_{i,q}$$

as the *i-th diagonal* of matrix Π_0.

Construct new $q \times q$ matrices Π_r $(1 \leq r \leq q-1)$ and let $0 \leq i \leq q - 1$. Taking the elements of the i-th diagonal of matrix Π_{r-1} as the $(i + 1)$-th row of matrix Π_r. For every Π_r, repeat the process in Step 1, we obtain $(q - 1)$ parallel classes

$$\Sigma_r\ (1 \leq r \leq q - 1) = \{B_j^r \mid 1 \leq j \leq q\}.$$

Step 3 Finally, arrange the q^2 points in a $q \times q$ matrix according to the row order, we obtain

$$\Pi_q = \begin{pmatrix} a_{11} & a_{21} & a_{31} & \cdots & a_{q1} \\ a_{12} & a_{22} & a_{32} & \cdots & a_{q2} \\ a_{13} & a_{23} & a_{33} & \cdots & a_{q3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{1q} & a_{2q} & a_{3q} & \cdots & a_{qq} \end{pmatrix}.$$

By the same method as Step 1, we obtain a parallel class

$$\Sigma_q = \{B_j^q \mid 1 \le j \le q\},$$

where

$$B_j^q = \{a_{1j},\ a_{2j}, \cdots, a_{qj}\}\ (1 \le j \le q).$$

Thus we obtain $(q+1)$ parallel classes.

Theorem 27 *Construction 1 gives a* $(q^2, q, 1)$*-ARBIBD.*

Proof: From our construction, it is easy to see $|X| = q^2$. Each block contains q points, so $k = q$. Every pair of distinct points $(x, y), (m, n)$, where $1 \le x, y, m, n \le q$ contained exactly one block, so it is a BIBD. Let $\mathcal{B}$ be the block set, each parallel class $\Sigma_i\ (0 \le r \le q)$ contains q blocks, so the total number of blocks in $\mathcal{B}$ is $b = q(q+1)$ such that $b = v + r - 1$. Hence $(X, \mathcal{B})$ is a $(q^2, q, 1)$-ARBIBD. □

Corollary 28 *There exists a* $(q^n, q^{\frac{n}{2}}, 1)$*-ARBIB D, where* $2|n$.

Proof: Consider a prime number q and denote the elements of $\mathbb{F}_{q^{\frac{n}{2}}}$ by $1, \cdots, q, q+1, \cdots, q^{\frac{n}{2}}$. Let

$$X = \mathbb{F}_{q^{\frac{n}{2}}} \times \mathbb{F}_{q^{\frac{n}{2}}} = \{(x, y) | x, y \in \mathbb{F}_{q^{\frac{n}{2}}}\}.$$

Clearly, $|X| = q^n$. Arrange the q^n points in a $q^{\frac{n}{2}} \times q^{\frac{n}{2}}$ matrix and process the matrix with the same method as Construction 1, we can get $(q^{\frac{n}{2}}+1)$ parallel classes. Additionally, each parallel class contains $q^{\frac{n}{2}}$ blocks, every block has $q^{\frac{n}{2}}$ points, the total number of blocks is $b = q^{\frac{n}{2}}(q^{\frac{n}{2}} + 1)$ such that $b = v + r - 1$, so there exists a $(q^n, q^{\frac{n}{2}}, 1)$-ARBIBD. □

Example 29 *Let* $q = 5$.
By step 1, we get a 5×5 *matrix*

$$\Pi_0 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix}.$$

By step 2, we get $\Pi_i (1 \le i \le 4)$ *as follows.*

$$\Pi_1 = \begin{pmatrix} a_{11} & a_{22} & a_{33} & a_{44} & a_{55} \\ a_{21} & a_{32} & a_{43} & a_{54} & a_{15} \\ a_{31} & a_{42} & a_{53} & a_{14} & a_{25} \\ a_{41} & a_{52} & a_{13} & a_{24} & a_{35} \\ a_{51} & a_{12} & a_{23} & a_{34} & a_{45} \end{pmatrix},$$

$$\Pi_2 = \begin{pmatrix} a_{11} & a_{32} & a_{53} & a_{24} & a_{45} \\ a_{21} & a_{42} & a_{13} & a_{34} & a_{55} \\ a_{31} & a_{52} & a_{23} & a_{44} & a_{15} \\ a_{41} & a_{12} & a_{33} & a_{54} & a_{25} \\ a_{51} & a_{22} & a_{43} & a_{14} & a_{35} \end{pmatrix},$$

$$\Pi_3 = \begin{pmatrix} a_{11} & a_{42} & a_{23} & a_{54} & a_{35} \\ a_{21} & a_{52} & a_{33} & a_{14} & a_{45} \\ a_{31} & a_{12} & a_{43} & a_{24} & a_{55} \\ a_{41} & a_{22} & a_{53} & a_{34} & a_{15} \\ a_{51} & a_{32} & a_{13} & a_{44} & a_{25} \end{pmatrix},$$

$$\Pi_4 = \begin{pmatrix} a_{11} & a_{52} & a_{43} & a_{34} & a_{25} \\ a_{21} & a_{12} & a_{53} & a_{44} & a_{35} \\ a_{31} & a_{22} & a_{13} & a_{54} & a_{45} \\ a_{41} & a_{32} & a_{23} & a_{14} & a_{55} \\ a_{51} & a_{42} & a_{33} & a_{24} & a_{15} \end{pmatrix}.$$

By step 3, we get Π_5 *as follows.*

$$\Pi_5 = \begin{pmatrix} a_{11} & a_{21} & a_{31} & a_{41} & a_{51} \\ a_{12} & a_{22} & a_{32} & a_{42} & a_{52} \\ a_{13} & a_{23} & a_{33} & a_{43} & a_{53} \\ a_{14} & a_{24} & a_{43} & a_{44} & a_{54} \\ a_{15} & a_{25} & a_{53} & a_{45} & a_{55} \end{pmatrix}$$

Then we generalize Construction 1 to get a construction of resolvable designs with q^3 points, that is, $(q^3, q, 1)$-RBIBD.

Construction 2 Consider a prime number q and denote the elements of $\mathbb{F}_{q^i}$ by $1, \cdots, q, q+1, \cdots, q^i$, where $i = 1, 2$. Let

$$X = \mathbb{F}_{q^2} \times \mathbb{F}_q = \{(x, y) |\ x \in \mathbb{F}_{q^2},\ y \in \mathbb{F}_q\}.$$

Similarly, let a_{xy} represent the point (x, y), then consider the following steps.

Step 1 Arrange the q^3 points in a $q^2 \times q$ matrix

according to the column order, we obtain

$$\Pi_0 = \begin{pmatrix} a_{11} & \cdots & a_{1q} \\ \vdots & & \vdots \\ a_{q1} & \cdots & a_{qq} \\ a_{q+1,1} & \cdots & a_{q+1,q} \\ \vdots & & \vdots \\ a_{2q,1} & \cdots & a_{2q,q} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ a_{(q-1)q,1} & \cdots & a_{(q-1)q,q} \\ \vdots & & \vdots \\ a_{q^2,1} & \cdots & a_{q^2,q} \end{pmatrix}.$$

By the same method as Construction 1, we can get a parallel class

$$\Sigma_0 = \{B_j^0 \mid 1 \le j \le q^2\},$$

where

$$B_j^0 = \{a_{j1},\ a_{j2}, \cdots, a_{jq}\}\ (1 \le j \le q^2),$$

and

$$X = \bigcup_{j=1}^{q^2} B_j^0.$$

Step 2 For the $q^2 \times q$ matrix Π_0, let $1 \le i \le q^2$, we define the sequence of elements

$$a_{i,1},\ a_{i+1,2},\ \cdots,\ a_{i+q-2,q-1},\ a_{i+q-1,q}$$

as the i-th *skew* of matrix Π_0.

Construct new $q^2 \times q$ matrices Π_r $(1 \le r \le q^2 - 1)$ and let $1 \le i \le q^2$. Taking the elements of the i-th skew of matrix Π_{r-1} as the i-th row of matrix Π_r. For every Π_r, repeat the process in Step 1, we obtain $q^2 - 1$ parallel classes

$$\Sigma_r\ (1 \le r \le q^2 - 1) = \{B_j^r \mid 1 \le j \le q\}.$$

Step 3 Finally, arrange the q^3 points in a $q^2 \times q$ matrix according to the row order, we obtain

$$\Pi^{'} = \begin{pmatrix} a_{11} & \cdots & a_{q1} \\ \vdots & & \vdots \\ a_{q^2-q+1,1} & \cdots & a_{q^2,1} \\ a_{12} & \cdots & a_{q2} \\ \vdots & & \vdots \\ a_{q^2-q+1,2} & \cdots & a_{q^2,2} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ a_{1q} & \cdots & a_{qq} \\ \vdots & & \vdots \\ a_{q^2-q+1,q} & \cdots & a_{q^2,q} \end{pmatrix}.$$

Then partition $\Pi^{'}$ into q matrices A_i $(1 \le i \le q)$, we obtain

$$\Pi^{'} = \begin{pmatrix} A_1^{(q\times q)} \\ \\ A_2^{(q\times q)} \\ \vdots \\ \\ \vdots \\ \\ A_q^{(q\times q)} \end{pmatrix}.$$

where A_i $(1 \le i \le q)$ are $q \times q$ matrices and

$$A_i = \begin{pmatrix} a_{1i} & a_{2i} & \cdots & a_{qi} \\ a_{q+1,i} & a_{q+2,i} & \cdots & a_{2q,i} \\ \vdots & \vdots & & \vdots \\ a_{q^2-q+1,i} & a_{q^2-q+2,i} & \cdots & a_{q^2,i} \end{pmatrix}.$$

Clearly, all A_i $(1 \le i \le q)$ have q^2 elements (points) arranged in a $q \times q$ matrix, then we consider the steps of Construction 1 to all A_i at the same time, we can get $(q+1)$ parallel classes. Thus we obtain (q^2+q+1) parallel classes.

Theorem 30 *Construction 2 gives a* $(q^3, q, 1)$*-RBIBD.*

Proof: The proof of Construction 2 is a BIBD is similar to Theorem 4.1. Then let $\mathcal{B}$ be the block set, from our construction, we obtain (q^2+q+1) parallel classes and each parallel class contains q^2 blocks, so the total number of blocks is $b = q^2(q^2 + q + 1)$. So $(X, \mathcal{B})$ is a $(q^3, q, 1)$-RBIBD. □

Corollary 31 *There exists a* $(q^n, q^{\frac{n}{3}}, 1)$*-RBIBD, where* $3|n$.

Proof: Consider a prime number q and denote the elements of $\mathbb{F}_{q^i}$ by $1, \cdots, q, q+1, \cdots, q^i$, where $i = \frac{n}{3}, \frac{2n}{3}$. Let

$$X = \mathbb{F}_{q^{\frac{2n}{3}}} \times \mathbb{F}_{q^{\frac{n}{3}}} = \{(x, y) |\ x \in \mathbb{F}_{q^{\frac{2n}{3}}},\ y \in \mathbb{F}_{q^{\frac{n}{3}}}\}.$$

Clearly, $|X| = q^n$. Arrange the q^n points in a $q^{\frac{2n}{3}} \times q^{\frac{n}{3}}$ matrix and process the matrix with the same method as Construction 2, we can get $(q^{\frac{2n}{3}} + q^{\frac{n}{3}} + 1)$ parallel classes. Additionally, each parallel class contains $q^{\frac{2n}{3}}$ blocks, every block has $q^{\frac{n}{3}}$ points, the total number of blocks is $b = q^{\frac{2n}{3}}(q^{\frac{2n}{3}} + q^{\frac{n}{3}} + 1)$, so there exists a $(q^n, q^{\frac{n}{3}}, 1)$-RBIBD. □

Theorem 32 *There exists* $(q^n, q, 1)$*-RBIBD for all integers* $n \geq 2$.

Proof: We prove the statement using mathematical induction.

Base case When $n = 2$, we proved Construction 1 is a $(q^2, q, 1)$-ARBIBD.

When $n = 3$, we proved Construction 2 is a $(q^3, q, 1)$-RBIBD.

Induction step Let k be a positive integer and suppose the statement holds for $n = k$. Then consider the case $n = k + 1$ and consider the following steps.

(1) Consider a prime number q and denote the elements of $\mathbb{F}_{q^i}$ by $1, \cdots, q, q+1, \cdots, q^i$, where $i = 1, k$. Let

$$X = \mathbb{F}_{q^k} \times \mathbb{F}_q = \{(x, y) |\ x \in \mathbb{F}_{q^k},\ y \in \mathbb{F}_q\}.$$

Obviously, $|X| = q^{k+1}$. Then arrange the q^{k+1} points in a $q^k \times q$ matrix according to the column order, we obtain

$$\Pi_0 = \begin{pmatrix} a_{11} & \cdots & a_{1q} \\ \vdots & & \vdots \\ a_{q^{k-1},1} & \cdots & a_{q^{k-1},q} \\ a_{q^{k-1}+1,1} & \cdots & a_{q^{k-1}+1,q} \\ \vdots & & \vdots \\ a_{2q^{k-1},1} & \cdots & a_{2q^{k-1},q} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ a_{(q-1)q^{k-1}+1,1} & \cdots & a_{(q-1)q^{k-1}+1,q} \\ \vdots & & \vdots \\ a_{q^k,1} & \cdots & a_{q^k,q} \end{pmatrix}.$$

By the same method as Construction 1, we can get a parallel class

$$\Sigma_0 = \{B_j^0 \mid 1 \leq j \leq q^{k-1}\},$$

where

$$B_j^0 = \{a_{j1}, a_{j2}, \cdots, a_{jq}\}\ (1 \leq j \leq q^k).$$

and

$$X = \bigcup_{j=1}^{q^k} B_j^0.$$

(2) Construct new $q^{k-1} \times q$ matrices Π_r $(1 \leq r \leq q^k - 1)$ and let $1 \leq i \leq q^{k-1}$. Taking the elements of the i-th skew of matrix Π_{r-1} as the i-th row of matrix Π_r. For every Π_r, repeat the process in **(1)**, we obtain $(q^{k-1} - 1)$ parallel classes

$$\Sigma_r (1 \leq r \leq q^{k-1} - 1) = \{B_j^r \mid 1 \leq j \leq q\}.$$

(3) By the above assumption, there exists a $(q^k, q, 1)$-RBIBD. It implies that arrange q^k points in a $q^{k-1} \times q$ matrix, by the same method as Construction 2, we can get $(q^{k-1} + q^{k-2} + \cdots + 1)$ parallel classes, each parallel class contains q^{k-1} blocks, and every block has q points. Then partition Π_0 into q matrices A_i $(1 \leq i \leq q)$, we obtain

$$\Pi_0 = \begin{pmatrix} A_1^{(q^{k-1} \times q)} \\ \\ A_2^{(q^{k-1} \times q)} \\ \vdots \\ \vdots \\ A_q^{(q^{k-1} \times q)} \end{pmatrix},$$

where A_i $(1 \leq i \leq q)$ are $q^{k-1} \times q$ matrices and

$$A_i = \begin{pmatrix} a_{(i-1)q^{k-1}+1,1} & \cdots & a_{(i-1)q^{k-1}+1,q} \\ \vdots & & \vdots \\ a_{(i-1)q^{k-1}+q,1} & \cdots & a_{(i-1)q^{k-1}+q,q} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ a_{iq^{k-1}-q+1,1} & \cdots & a_{iq^{k-1}-q+1,q} \\ \vdots & & \vdots \\ a_{iq^{k-1},1} & \cdots & a_{iq^{k-1},q} \end{pmatrix}.$$

Clearly, all A_i $(1 \leq i \leq q)$ have q^k elements (points), then arrange the q^k points in a $q^{k-1} \times q$ matrix differ-

ent from A_i, and denote them by

$$A_i^{'} = \begin{pmatrix} a_{(i-1)q^{k-1}+1,1} & \cdots & a_{(i-1)q^{k-1}+q,1} \\ \vdots & & \vdots \\ a_{iq^{k-1}-q+1,1} & \cdots & a_{iq^{k-1},1} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ a_{(i-1)q^{k-1}+1,q} & \cdots & a_{(i-1)q^{k-1}+q,q} \\ \vdots & & \vdots \\ a_{iq^{k-1}-q+1,q} & \cdots & a_{iq^{k-1},q} \end{pmatrix}.$$

We process all A_i $(1 \leq i \leq q)$ at the same time, then we can get $(q^{k-1} + q^{k-2} + \cdots + 1)$ parallel classes. Thus we obtain $(q^k + q^{k-1} + \cdots + q + 1)$ parallel classes.

From our construction, it is clear that $|X| = q^{k+1}$. Each block contains q points, so $k^{'} = q$. Every pair of distinct points contained exactly one block, so there exists a $(q^{k+1}, q, 1)$-RBIBD. Hence the statement holds for $n = k + 1$.

By the principle of induction, there exists a $(q^n, q, 1)$-RBIBD for all integers $n \geq 2$. □

Corollary 33 *There exists a* $(q^n, q^{\frac{n}{m}}, 1)$*-RBIBD, where* m *be a positive integer and* $m|n$.

Proof: Consider a prime number q and denote the elements of $\mathbb{F}_{q^i}$ by $1, \cdots, q, q+1, \cdots, q^i$, where $i = \frac{n}{m}, n - \frac{n}{m}$. Let

$$X = \mathbb{F}_{q^{n-\frac{n}{m}}} \times \mathbb{F}_{q^{\frac{n}{m}}} = \{(x, y) |\, x \in \mathbb{F}_{q^{n-\frac{n}{m}}},\, y \in \mathbb{F}_{q^{\frac{n}{m}}}\}.$$

Clearly, $|X| = q^n$. Arrange the q^n points in a $q^{n-\frac{n}{m}} \times q^{\frac{n}{m}}$ matrix and process the matrix with the same method as Theorem 4.3, we can get $(q^{n-\frac{n}{m}} + q^{n-\frac{2n}{m}} + \cdots + 1)$ parallel classes. Additionally, each parallel class contains $q^{n-\frac{n}{m}}$ blocks, every block has $q^{\frac{n}{m}}$ points, the total number of blocks is $b = q^{n-\frac{n}{m}}(q^{n-\frac{n}{m}} + q^{n-\frac{2n}{m}} + \cdots + 1)$, so there exists a $(q^n, q^{\frac{n}{m}}, 1)$-RBIBD. □

5 Conclusion

The key point in this paper is that we discuss the relation between resolvable design and KDP, then convert the construction of KDP into the construction of resolvable design which easier to construct. Fundamental questions arising out of this work, such as finding the lower bound on the number of blocks b that holds for resolvable design and construct "good" and efficient $(\mathcal{G}, \mathcal{F})$-KDP associating with practical applications.

Acknowledgements: The research was supported by the National Natural Science Foundation of China(grant No. 61179026) and the Fundamental Research Funds for the Central Universities(grant No. 3122013K001).

References:

[1] C. J Mitchell, F. C. Piper, Key storage in secure networks, *Discrete Applied Mathematics*, 21, 1988, pp. 215-228.

[2] Seon Ho Shin, J. C. Bate, Generalization of key distribution patterns for every n-pair of users, *J. Appl. Math. Informatics*, 26, 2008, pp. 563-572.

[3] C. M. O'Keefe, Key distribution patterns using Minkowski planes, *Designs, Codes and Cryptography*, 5, 1995, pp. 261-267.

[4] Z. X. Wan, *Designs Theory*, Higher Education Press, 2009.

[5] Julia Catherine Novak, *Generalized key distribution patterns*, Doctoral Thesis, University of London, 2012.

[6] Manjusri Baus, Debabrata Kumar Ghosh, Another Construction of Resolvable Designs of Order p^2, *South Asian Journal of Mathematics*, 2, 2012, pp. 201-204.

[7] K. A. S. Quinn, Some constructions for key distribution patterns, *Designs, Codes and Cryptography*, 4, 1994, pp. 177-191.

[8] K. A. S. Quinn, Bounds for key distribution patterns, *Journal of Cryptology*, 12, 1999, pp. 227-240.

[9] M. Ruszink'o, On the upper bound of the size of the r-cover-free families, *Journal of Combinatorial Theory A*, 66, 1994, 302-310.

[10] S. Kageyama, An improved inequality for balanced incomplete block designs, *Ann. Math. Statist.*, 42, 1971, pp. 1448-1449.

[11] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer Verlag New York, 2004.

[12] D. R. Stinson, *Combinatorial designs and cryptography*, In Survey in Combinatorics, Cambridge university Press, 1993, pp. 257-287.

[13] Sanpei Kagey Ama, Improved inequalities for balanced incomplete block designs, *Discrete Mathematics*, 21, 1978, pp. 177-185.

[14] W. D. Wallis, *Combinatorial Designs*, Marcel Dekker, New York, 1988.

[15] Z. X. Wan, *Geometry of Classical Groups over Finite Field*, Lund: Student literature, 1993.