

## Optimizing traceable codes with Latin squares and projective planes

Anu Kathuria

*Department of Mathematics*

*The Technological Institute of Textile and Sciences*

*Bhiwani 127021*

*Haryana*

*India*

---

### Abstract

Traitor tracing is indeed a significant concept in cryptography, introduced by Chor, Fiat and Naor [7] in 1994. Combinatorial designs are Mathematical Structures that are highly suitable for creating traceable codes. They offer systematic methods for code construction, ensuring properties like traceability and resistance to collusion. Here in this paper we intend a novel method to make 3 –TA codes. No such Example of 3-TA code is available in Literature. We also take into consideration one more Combinatorial Design that is Projective Plane which even always proves to be 2-Frameproof Code.

---

**Subject Classification:** 12F05, 12F06, 12G15.

**Keywords:** Latin square, Traceable code, Frameproof code, Projective plane.

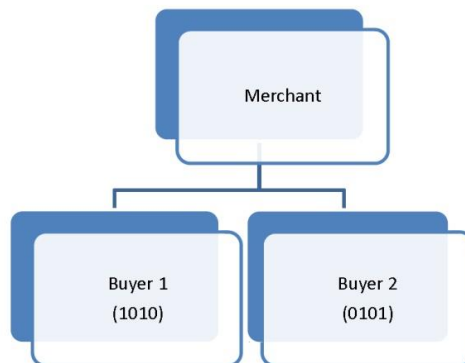
### 1. Introduction

The rise of computer networks, particularly the global internet, has indeed revolutionized the distribution of electronic documents but has also introduced significant challenges in the protection of Copyrighted Materials. While network distribution enables the reach to a vast number of recipients and allows for the customization and preprocessing of information to meet individual needs. But the extensive use of computer networks like the global internet for distributing electronic documents does indeed pose a significant business threat to information providers. This problem relates to digital watermarking and fingerprinting techniques used for tracking and protecting the redistribution of copyrighted materials. The distinction between pages A and B hinges on imperceptible differences, such as slight shifts in text word positions. The challenge is to determine whether a given copy was derived from A or B after

---

E-mail: [anu\\_sept24@rediffmail.com](mailto:anu_sept24@rediffmail.com)

potential recursive reproduction. In the digital age, protecting the ownership and integrity of electronic data has become a critical challenge. A digital watermark is an invisible structure embedded within a host signal, used to "mark" ownership and provide a means of authentication. Digital watermarks serve multiple purposes, including digital signal tagging, authentication, and the anticipation of unauthorized copying and distribution of electronic data. One of the key applications of digital watermarking is fingerprinting, which allows for the tracking and identification of unauthorized copies. With digital fingerprinting, a publisher embeds a unique fingerprint pattern into each distributed copy of a document, keeping a database of sold copies and their corresponding fingerprints. If an illegally distributed copy is later discovered, it can be traced back to the offending user by comparing its unique fingerprint to a database. Due to the marking process, no two copies will be identical, resulting in slight marking distortions in the documents. To be acceptable, these distortions must be negligible to users. A pirate, or offending user, may attempt various methods to remove the fingerprint in order to distribute illegal copies anonymously. Assuming that the pirate has an access to a single marked copy, that has been marked for him, he may try to restore the original document by identifying and removing that fingerprint, or try to corrupt the fingerprint by distorting the document. A stronger attack results if several pirates collude and compare their independently marked copies. Then they can detect and locate the differences and combine their copies into a new one whose fingerprint differs from all the pirates.



In that case if merchant embeds these two codewords (1010) and (0101) in the copies of different customers, then both of the buyers can collude together and generate a new copy with different codeword (0001). If that copy has already been assigned to the third user then an innocent user can be framed in that case although he is not a part of this conspiracy.

## 2. Literature Review

This detailed description provides an overview of various fingerprinting codes and their roles in addressing the problem of traitor tracing and protection

against unauthorized redistribution of copyrighted materials. Below, we summarize the key types of fingerprinting codes and their significance, along with some observations on their properties and Applications. Frameproof (FP) Codes were introduced by Boneh and Shaw [5] to prevent colluding users from framing an innocent party. If a group of up to “c” colluders generate a new codeword, it cannot correspond to a codeword of an innocent user. Boneh and Shaw used Error Correcting Codes (ECC) to construct c-frameproof codes. A code with minimum distance  $d > (1-1/c)n$ , where  $n$  is the length and  $c$  is the number of colluders, can serve as a c-frameproof code. Identifiable Parent Property (IPP) Codes were introduced by Hollman et al. [6] to identify at least one colluder from the codeword of a pirated copy. IPP codes are a generalization and can identify the origin of the codeword, unlike FP codes, which only prevent framing. One more family of robust codes i.e. Traceable (TA) Codes were introduced by Chor, Fiat, and Naor [7, 14]. TA Codes are stronger than IPP codes; can trace traitors with fewer restrictive conditions but may not have efficient tracing algorithms. Traceable (TA) Codes were studied extensively by Staddon, Stinson, and Wei [4]. Necessary and Sufficient conditions for equidistant 2-TA codes have been derived for their use. Infinite classes of nonlinear equidistant 2-TA codes of length  $n$  and distance  $d$  with  $2n/3 < d \leq 3n/4$  have also been studied in [1, 2, 3, 10]. Al-Seraji, Alnussary, and Jafar [15, 16] have also explained finite Projective Planes of order 53, 61 and 64. These Projective Planes can also be used in different fingerprinting schemes as traceable codes. Different types of traceable codes can also be designed using Lexicographic codes which are discussed in [17]. A few authors have also suggested construction of different fingerprinting codes using the Designs of Oligo Arrays in [11, 12, 13]

## 2.1 Some Preliminaries

Throughout this paper we will apply these basic definitions and terminology from [1, 3, 4, 5, 6, 9] and  $G_q$  denotes a finite field with  $q$  elements.

- (i) **Code and Codewords** : “Let  $Q$  be a finite set of alphabets. Then a subset  $C \subset Q^n$  is called a code of length  $n$  over  $Q$ . The elements of  $Q^n$  are called words and the elements of Code are called codewords of length  $n$ ”.
- (ii) **Hamming Distance**: “Let  $a$  and  $b$  be two codewords, then the hamming distance between  $a$  and  $b$  i.e.  $d(a, b)$  is the number of coordinates in which they differ and the number of non zero coordinates of a word  $c$  is called the weight of  $c$ . The minimum distance  $d$  of  $C$  is  $d = \min.\{d(a, b) \mid a, b \in C\}$ .”
- (iii) **Similar Positions**: “ $I(x, y) = \{i: x_i = y_i\}$  for  $x = \{x_1, x_2, \dots, x_n\}$ ,  $y = \{y_1, y_2, \dots, y_n\} \in Q^n$ . Similarly we can define  $I(x, y, z, \dots)$  for any number of words  $x, y, z, \dots$ ”
- (iv) **Dimension and Minimum Distance**: “A subspace  $C$  of  $F_q^n$  is called a linear code over  $F_q$ . The dimension of the code is defined as the dimension of the subspace. A linear code with length  $n$ , dimension  $k$  and minimum distance  $d$  is denoted as  $[n, k, d]$  code.”

- (v) **Maximum Distance Separable Code:** “A linear code  $C [n, k, d]$  is a Maximum Distance Separable code if  $d = n - k + 1$ ”.
- (vi) **Latin Square:** A Latin Square of order  $n$  is  $n \times n$  array whose entries are from a set  $S_q$  of distinct symbols  $\{0, 1, 2, 3, 4, \dots, q - 1\}$  such that each row and each column of the array contains each symbol exactly once.

**Example:** Let  $Z_3 = \{0, 1, 2\}$  then Latin Square of order 3 is

|   |   |   |
|---|---|---|
| 0 | 1 | 2 |
| 2 | 0 | 1 |
| 1 | 2 | 0 |

- (vii) **Mutually Orthogonal Latin Squares** [9]: “Let  $A$  and  $B$  be two Latin Squares of order  $n$ . Let  $a_{ij}$  and  $b_{ij}$  denote the  $(i, j)$ th entries of  $A$  and  $B$  respectively. Then  $A$  and  $B$  are said to be MOLS if  $n^2$  ordered pairs  $(a_{ij}, b_{ij})$   $i, j = 1, 2, 3, 4, 5 \dots q$  are all distinct i.e. if we superimpose the two squares to form new  $n \times n$  square with ordered pairs as entries, then these  $n^2$  ordered pairs are all distinct.

**Example:** The Latin Squares

$$A = \begin{matrix} & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 2 \end{matrix}$$

and

$$B = \begin{matrix} & 1 & 2 & 3 \\ 1 & 3 & 1 & 1 \\ 2 & 2 & 3 & 1 \end{matrix}$$

are mutually orthogonal to each other.

3.1 Now let us define some terms related to fingerprinting codes.

- (i) **Detectable and Undetectable Positions:** “Let  $X \subset Q^n$ , Then we say that the position  $i \in Q^n$  is undetectable for  $X$  if  $i$ th position of each word  $x \in X$  is occupied with same alphabet, otherwise the position  $i$  is detectable”.
- (ii) **Descendant Set:** “For any two words  $a = \{a_1, a_2, \dots, a_n\}$  and  $b = \{b_1, b_2, \dots, b_n\}$  in  $Q^n$ , the set of descendants is defined as  $D(a, b) = \{x \in Q^n \mid x_i \in \{a_i, b_i\}, i=1, 2, 3, \dots, n\}$ ”

The above definition of Descendant set can be naturally extended to any finite number of words  $a, b, c, \dots$ .

- (iii) **Frameproof Code** [5]: “A code  $C$  is called  $c$ -frameproof if for every set  $W \subset C$ , of size at most  $c$ , satisfies the condition  $F(W) \cap C = W$ ”

The definition states that in a  $c$ -frameproof code, the only codewords in the feasible set of a coalition of at most  $c$  users are the codewords of the member of coalition.

**Example:** Let  $C$  be a code given by

$$C = \{(1, 0, 0), (0, 2, 0), (0, 0, 3)\} \text{ and } W = \{(1, 0, 0), (0, 2, 0)\}$$

By the definition of feasible set,

$F(W) = \{(1,2,0), (0,0,0), (1,0,0), (0,2,0)\}$  i.e. obvious  $F(W) \cap C = W$ .

- (iv) **Identifiable Parent Property Code[6]** : “A code  $C$  is c-IPP if for any  $x \in \text{Desc}(C)$  it holds that if  $C_i \subset C$  with  $|C_i| \leq c$ , then  $\cap_{\{i: x \in \text{Desc}(C_i)\}} C_i \neq \emptyset$  (Empty)”
- (v) **Traceable Code [4]**: “For  $x, y \in Q^n$ ; define  $I(x, y) = \{i : x_i = y_i\}$ .  $C$  is c-TA code provided that for all  $I$  and for all  $x \in \text{desc}_c(C_I)$  there is atleast one codeword  $y \in C_I(C \setminus C)$ ;  $|x, y| > |x, z|$  for any  $z \in C \setminus C_I$ . The condition in terms of distance is equivalent to  $d(x, y) < d(x, z)$ ”.

In the Section 4, we suggest the method of Constructing 3-TA Code using the Combinatorial Design “Latin Squares”. We also explain this method by giving an example. No any example of 3-TA code has been reported in Literature till now. Here we first discuss the basic results and theorems related to *MOLS*.

**4. Theorem 4.1** [9]: *An MDS code with  $k = 2$  is also equivalent to a set of  $(n - 2)$  Mutually Orthogonal Latin Squares of order  $n$ .*

**Definition 4.2** [9]: If  $q = p^e$  is a prime power, then  $N(Q) = q - 1$ , where  $N$  defines the number of Mutually Orthogonal Latin Squares.

**4.3 Construction:** We begin with a description of a collection of matrices derived from *MOLS* (Mutually Orthogonal Latin Squares) whose symbols are elements in the Finite set  $S_q = \{0, 1, 2, 3, 4, 5, \dots, q - 1\}$ .

Let  $M_1, M_2, M_3, \dots, M_{q-1}$ , be a set of  $(q - 1)$  *MOLS*. The first two columns of  $(q^2 \times q + 1)$  matrix form a succession of all tuples of  $S_q$ . The third column repeats the entries of Latin Square  $M_1$  by writing it row by row from left to right. The fourth column does the same for Latin Square  $M_2$  and so on. The  $(q + 1)$ st column will be obtained by writing the entries of Latin Square  $M_{q-1}$  row by row.

Let us take  $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ . Since by definition, the number of Mutually Orthogonal Latin Squares will be 8. The construction of *MOLS* has been suggested in [9]. These *MOLS* (Mutually Orthogonal Latin Squares) of order 9 over  $Z_9$  are given as;

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 3 | 5 | 4 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |

By the steps applying and construction discussed above, the codewords of  $C$  using  $MOLS$  will be:

|   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 1 | 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 1 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |

|   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 1 | 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 1 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 1 | 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 2 | 0 | 2 | 1 | 6 | 8 | 7 | 3 | 5 | 4 |
| 2 | 1 | 0 | 2 | 7 | 6 | 8 | 4 | 3 | 5 |
| 2 | 2 | 1 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 2 | 3 | 5 | 4 | 0 | 2 | 1 | 6 | 8 | 7 |
| 2 | 4 | 3 | 5 | 1 | 0 | 2 | 7 | 6 | 8 |
| 2 | 5 | 4 | 3 | 2 | 1 | 0 | 8 | 7 | 6 |
| 2 | 6 | 8 | 7 | 3 | 5 | 4 | 0 | 2 | 1 |
| 2 | 7 | 6 | 8 | 4 | 3 | 5 | 1 | 0 | 2 |
| 2 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 3 | 0 | 3 | 6 | 4 | 7 | 1 | 8 | 2 | 5 |
| 3 | 1 | 4 | 7 | 5 | 8 | 2 | 6 | 0 | 3 |
| 3 | 2 | 5 | 8 | 3 | 6 | 0 | 7 | 1 | 4 |
| 3 | 3 | 6 | 0 | 7 | 1 | 4 | 2 | 5 | 8 |
| 3 | 4 | 7 | 1 | 8 | 2 | 5 | 0 | 3 | 6 |
| 3 | 5 | 8 | 2 | 6 | 0 | 3 | 1 | 4 | 7 |
| 3 | 6 | 0 | 3 | 1 | 4 | 7 | 5 | 8 | 2 |
| 3 | 7 | 1 | 4 | 2 | 5 | 8 | 3 | 6 | 0 |
| 3 | 8 | 2 | 5 | 0 | 3 | 6 | 4 | 7 | 1 |
| 4 | 0 | 4 | 8 | 7 | 2 | 3 | 5 | 6 | 1 |
| 4 | 1 | 5 | 6 | 8 | 0 | 4 | 3 | 7 | 2 |
| 4 | 2 | 3 | 7 | 6 | 1 | 5 | 4 | 8 | 0 |
| 4 | 3 | 7 | 2 | 1 | 5 | 6 | 8 | 0 | 4 |
| 4 | 4 | 8 | 0 | 2 | 3 | 7 | 6 | 1 | 5 |
| 4 | 5 | 6 | 1 | 0 | 4 | 8 | 7 | 2 | 3 |
| 4 | 6 | 1 | 5 | 4 | 8 | 0 | 2 | 3 | 7 |
| 4 | 7 | 2 | 3 | 5 | 6 | 1 | 0 | 4 | 8 |
| 4 | 8 | 0 | 4 | 3 | 7 | 2 | 1 | 5 | 6 |
| 5 | 0 | 5 | 7 | 1 | 3 | 8 | 2 | 4 | 6 |
| 5 | 1 | 3 | 8 | 2 | 4 | 6 | 0 | 5 | 7 |
| 5 | 2 | 4 | 6 | 0 | 5 | 7 | 1 | 3 | 8 |
| 5 | 3 | 8 | 1 | 4 | 6 | 2 | 5 | 7 | 0 |
| 5 | 4 | 6 | 2 | 5 | 7 | 0 | 3 | 8 | 1 |
| 5 | 5 | 7 | 0 | 3 | 8 | 1 | 4 | 6 | 2 |
| 5 | 6 | 2 | 4 | 7 | 0 | 5 | 8 | 1 | 3 |
| 5 | 7 | 0 | 5 | 8 | 1 | 3 | 6 | 2 | 4 |
| 5 | 8 | 1 | 3 | 6 | 2 | 4 | 7 | 0 | 5 |
| 6 | 0 | 6 | 3 | 8 | 5 | 2 | 4 | 1 | 7 |
| 6 | 1 | 7 | 4 | 6 | 3 | 0 | 5 | 2 | 8 |
| 6 | 2 | 8 | 5 | 7 | 4 | 1 | 3 | 0 | 6 |
| 6 | 3 | 0 | 6 | 2 | 8 | 5 | 7 | 4 | 1 |
| 6 | 4 | 1 | 7 | 0 | 6 | 3 | 8 | 5 | 2 |
| 6 | 5 | 2 | 8 | 1 | 7 | 4 | 6 | 3 | 0 |
| 6 | 6 | 3 | 0 | 5 | 2 | 8 | 1 | 7 | 4 |

|   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|
| 6 | 7 | 4 | 1 | 3 | 0 | 6 | 2 | 8 | 5 |
| 6 | 8 | 5 | 2 | 4 | 1 | 7 | 0 | 6 | 3 |
| 7 | 0 | 7 | 5 | 2 | 6 | 4 | 1 | 8 | 3 |
| 7 | 1 | 8 | 3 | 0 | 7 | 5 | 2 | 6 | 4 |
| 7 | 2 | 6 | 4 | 1 | 8 | 3 | 0 | 7 | 5 |
| 7 | 3 | 1 | 8 | 5 | 0 | 7 | 4 | 2 | 6 |
| 7 | 4 | 2 | 6 | 3 | 1 | 8 | 5 | 0 | 7 |
| 7 | 5 | 0 | 7 | 4 | 2 | 6 | 3 | 1 | 8 |
| 7 | 6 | 4 | 2 | 8 | 3 | 1 | 7 | 5 | 0 |
| 7 | 7 | 5 | 0 | 6 | 4 | 2 | 8 | 3 | 1 |
| 7 | 8 | 3 | 1 | 7 | 5 | 0 | 6 | 4 | 2 |
| 8 | 0 | 8 | 4 | 5 | 1 | 6 | 7 | 3 | 2 |
| 8 | 1 | 6 | 5 | 3 | 2 | 7 | 8 | 4 | 0 |
| 8 | 2 | 7 | 3 | 4 | 0 | 8 | 6 | 5 | 1 |
| 8 | 3 | 2 | 7 | 8 | 4 | 0 | 1 | 6 | 5 |
| 8 | 4 | 0 | 8 | 6 | 5 | 1 | 2 | 7 | 3 |
| 8 | 5 | 1 | 6 | 7 | 3 | 2 | 0 | 8 | 4 |
| 8 | 6 | 5 | 1 | 2 | 7 | 3 | 4 | 0 | 8 |
| 8 | 7 | 3 | 2 | 0 | 8 | 4 | 5 | 1 | 6 |
| 8 | 8 | 4 | 0 | 1 | 6 | 5 | 3 | 2 | 7 |

For this case we find that the length of the code is 10 and distance between every two codewords is 9. It satisfies the condition that  $d > (1 - \frac{1}{m^2})n$ . Therefore, by the definition part (iii) of 3.1, the above code is 3-TA code. No such example has already been reported in literature till now. Suppose  $C_1, C_2$  and  $C_3$  are three codewords with numeric values

$$\begin{aligned} C_1 &= 7 \ 3 \ 1 \ 8 \ 5 \ 0 \ 7 \ 4 \ 2 \ 6 \\ C_2 &= 8 \ 8 \ 4 \ 0 \ 1 \ 6 \ 5 \ 3 \ 2 \ 7 \text{ and} \\ C_3 &= 7 \ 8 \ 3 \ 1 \ 7 \ 5 \ 0 \ 6 \ 4 \ 2 \end{aligned}$$

They if generate a new codeword  $C = 7 \ 8 \ 1 \ 1 \ 5 \ 6 \ 0 \ 4 \ 2 \ 2$   
 $d(C_1, C) = 5$ ,  $d(C_2, C) = 7$  and  $d(C_3, C) = 5$ . So, it is clear that distance  $d$  of the pirated codeword comes out to be minimum from actual codewords  $C_1$  and  $C_3$ . Even we can verify the property of traceability by taking any other three codewords. In Section 5, we also explain that how Projective Plane can be used as Frameproof code.

## 5. Projective Plane as 2-frameproof code

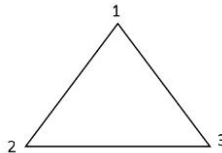
In this section we show that how Projective Plane can be used as 2-frameproof code.

**Definition 5.1** [8, 9]: A finite projective plane of order  $n$  with  $n(> 0)$  is collection of  $n^2 + n + 1$  lines and  $n^2 + n + 1$  points such that

- (a) Every line contains  $n + 1$  points.
- (b) Every point is on  $n + 1$  lines.

- (c) Any two distinct lines intersect exactly at one point.  
 (d) Any two distinct points lie on exactly one line.

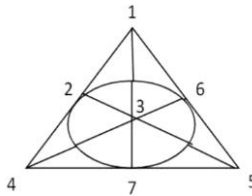
**Example 5.2:** The smallest example of a projective plane of order 1 is a triangle.



There are three lines, three points and each line contains two points.

**Example 5.3:** Projective Plane of order 2. The next nontrivial example is an example of a projective plane of order 2.

This diagram shows that there are seven points labeled from 1 to 7. There are also seven labeled  $L_1$  to  $L_7$ . Six of them are straight lines. But  $L_6$  is represented by the circle through the points 2, and 7.



The other lines are;

$L_1 = \{1, 2, 4\}$ ,  $L_2 = \{2, 3, 5\}$ ,  $L_3 = \{3, 4, 6\}$ ,  $L_4 = \{4, 5, 7\}$ ,  $L_5 = \{5, 6, 1\}$ ,  
 $L_6 = \{6, 7, 2\}$ ,  $L_7 = \{7, 1, 3\}$

#### 5.4 Incidence Matrix of Projective Plane [9]:

Let  $P$  be a finite projective plane of order  $n$ . The incidence matrix  $A$  of  $P$  is the  $(n^2 + n + 1) \times (n^2 + n + 1)$  matrix where the lines are represented by the rows and the points are represented by the columns such that row  $i$  has a 1 in column  $j$  if the line corresponding to row  $i$  contains the point corresponding to column  $j$  and 0 otherwise.

The incidence matrix of the example 5.3 is;

|       |   |   |   |   |   |   |   |
|-------|---|---|---|---|---|---|---|
| $L_1$ | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| $L_2$ | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| $L_3$ | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| $L_4$ | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| $L_5$ | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| $L_6$ | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| $L_7$ | 1 | 0 | 1 | 0 | 0 | 0 | 1 |

### 5.5 Properties of Incidence Matrix

1. Each row of this incidence matrix has constant sum  $n + 1$ .
2. Each column of this incidence matrix has constant sum  $n + 1$ .
3. The distance between every two rows is  $n^2$ .

If we take transpose of that matrix, the above properties hold simultaneously. In the next step we show that the incidence matrix of a Projective Plane is always a 2-FP code.

### 5.6 Incidence Matrix as 2-FP Code

**Theorem 5.6.1:** *The incidence matrix of a projective plane of order  $n(n > 1)$  is always 2-Frameproof Code.*

**Proof:** By the definition of frameproof code [5], as discussed above we find that an incidence matrix of a projective plane is always a Binary Code of length  $n^2 + n + 1$  with distance  $n^2$ . Since distance  $d > (\frac{n^2+n+1}{2})$ , (For  $n > 1$ ). Therefore by definition of frameproof code [5], incidence matrix of projective plane is always 2-FP Code.

## 6. Conclusion

- (i) We prove that Combinatorial Design like Latin Square can be used as 3-TA code. Here in that paper we also represent an example which comes out to be 3-TA Code.
- (ii) We also show that Projective Plane of Order  $n$  is always 2-FP Code.

## References

- [1] A. Kathuria and S. Batra, "On traceability property of equidistant codes," *J. Discrete Math.*, vol. 7, pp. 713–721 (2017).
- [2] A. Kathuria, S. Batra, and S. K. Arora, "A class of 2-FP codes," *J. Inf. Optim. Sci.*, vol. 38, no. 8, pp. 1311–1324 (Dec. 2017).
- [3] A. Kathuria and S. Batra, "On algebraic conditions of equidistant codes," *Int. J. Sci. Res. Arch.*, vol. 8, no. 2, pp. 575–588 (Apr. 2023).
- [4] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceable codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1042–1049 (2001).
- [5] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897–1905 (1998).

- [6] H. D. L. Hollmann, J. H. van Lint, and J.-P. Linnartz, "On codes with the identifiable parent property," *J. Combin. Theory Ser. A*, vol. 82, no. 1, pp. 121–133 (1998).
- [7] B. Chor, A. Fiat, and M. Naor, "Tracing traitors," in *Advances in Cryptology – CRYPTO '94*, Lecture Notes in Computer Science, vol. 839, Berlin, Germany: Springer-Verlag, pp. 257–270 (1994).
- [8] B. Victor, *Aspects of Combinatorics*, Cambridge, U.K.: Cambridge Univ. Press (1993).
- [9] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, Boca Raton, FL, USA: CRC Press (1996).
- [10] A. Kathuria, "Combinatorial properties of some fingerprinting models and linear codes," Ph.D. dissertation, Maharshi Dayanand Univ., Rohtak, India (Dec. 2013).
- [11] N. Alon, C. J. Colbourn, and A. C. H. Ling, "Equireplicate balanced binary codes for oligo arrays," *SIAM J. Discrete Math.*, vol. 14, no. 4, pp. 481–497 (2001).
- [12] T. Todorov, G. Bogdanova, and T. Yorgova, "Lexicographic constant weight equidistant codes over the alphabet of three, four and five elements," *J. Intell. Inf. Manage.*, vol. 2, pp. 183–187 (2010).
- [13] J. H. Conway and N. J. A. Sloane, "Lexicographic codes: Error-correcting codes from game theory," *IEEE Trans. Inf. Theory*, vol. 32, no. 3, pp. 337–348 (1986).
- [14] F.-W. Fu, T. Kløve, and Y. Luo, "On equidistant constant weight codes," *Discrete Appl. Math.*, vol. 128, no. 1, pp. 157–164 (2003).
- [15] R. K. Kumari, R. Arulprakasam, and V. R. Dare, "Combinatorial properties of Fibonacci partial words and arrays," *J. Discrete Math. Sci. Cryptogr.*, vol. 24, no. 4, pp. 1007–1020 (2021). [Online]. Available: <https://doi.org/10.1080/09720529.2020.179452>
- [16] M. Al-Seraji, N. A. Alnuissary, and Z. S. Jafar, "The group action on the finite projective planes of orders 53, 61, 64," *J. Discrete Math. Sci. Cryptogr.*, vol. 23, no. 8, pp. 1573–1582 (2020). [Online]. Available: <https://doi.org/10.1080/09720529.2020.1773020>
- [17] A. Kathuria, "Traceable codes constructed using certain combinatorial designs," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 8, pp. 2563–2572 (2024). [Online]. Available: <https://doi.org/10.47974/JDMSC-2072>