Bulletin of Pure and Applied Sciences
Section - E - Mathematics & Statistics
Vol. 41E, No.2, July-December 2022.P.184-198

Print version ISSN 0970 6577
Online version ISSN 2320 3226
DOI: 10.5958/2320-3226.2022.00025.X

Original Article

Content Available online at: https://bpasjournals.com/math-and-stat/

MDS Block Hankel-like Rhotrices using Conjugate Elements and Self-Dual Bases of Finite Fields

[1]Shalini Gupta*, [2]Ruchi Narang, [3]Mansi Harish and [4] Neetu Dhiman

Author's Affiliation:
[1,2,3]Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, Himachal Pradesh 171005, India.
[4]University Institute of Technology, Himachal Pradesh University, Shimla, Himachal Pradesh 171005, India.
[1]Email: shalini.garga1970@gmail.com, [2]Email: ruchinarang8878@gmail.com, [3]Email: mansihverma16@gmail.com
[4]Email: dhimanneetu.278@gmail.com

***Corresponding Author: Shalini Gupta**, Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, Himachal Pradesh 171005, India.
E-mail: shalini.garga1970@gmail.com

How to cite this article: Gupta S., Narang R., Harish M., Dhiman N. (2022). MDS Block Hankel- like Rhotrices using Conjugate Elements and Self-Dual Bases of Finite Fields. *Bull. Pure Appl. Sci. Sect. E Math. Stat.* 41E(2), 184-198.

ABSTRACT

Maximum Distance Separable (MDS) matrices offer ideal diffusion properties and are of great importance in design of block ciphers and hash functions. A rhotrix as defined by Sani, is a coupled matrix which when used in a cryptosystem provides double security. Many authors constructed MDS Rhotrices over finite fields using matrices which are cryptographically significant. Hankel matrices have wide range of applications in engineering, coding theory and cryptography. In the present paper, we define block rhotrix and block Hankel- like rhotrix. Further, we construct MDS block Hankel-like rhotrices using self-dual basis and conjugate elements of F_{p^n}.

KEYWORDS: Finite Fields, MDS Rhotrix, Block Rhotrix, Hankel matrix, Hankel Rhotrix, Block Hankel- like Rhotrix.

1. Introduction

Rhotrix is a rhomboidal structure introduced by Ajibade [1] in 2006. A rhotrix is an extension of matrix tertions and matrix noitrets given by Attanassov and Shannon [3]. A 3–dimensional rhotrix as given by Ajibade is

$$R_3 = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle,$$

where a, b, c, d, e are real numbers and c is called the heart of rhotrix R_3. He has also shown that there are many similarities in the operations of rhotrices and matrices. He introduced operations of addition and scalar multiplication.

In the literature of rhotrix theory, two methods of multiplication of rhotrices are defined. First method of multiplication of rhotrices is known as heart-oriented multiplication, which was discussed by Ajibade and further its

generalisation was given by Mohammad et al. [10] and second method of multiplication is row column multiplication of rhotrices which was discussed by Sani [12]. These two methods of multiplication characterised the rhotrices into commutative and non-commutative rhotrices. Ajibade's heart- oriented method for rhotrix multiplication corresponds to commutative rhotrix and row column multiplication method corresponds to non-commutative rhotrix.

MDS matrices play a vital role in cryptography, hash functions and in the design of block ciphers. MDS matrix is an indispensable part for AES [5], SHARK [17], Khazad [4] and in the stream cipher MUGI. The use of a rhotrix in a cryptosystem doubles the security. Many authors constructed MDS rhotrices over finite fields using matrices which are cryptographically significant, see [2, 7- 9, 11, 13-15]. Hankel matrices were discussed by Fazel et. al in [6]. Sharma et. al. [16] defined Hankel rhotrices and used Hankel matrices for the construction of MDS Hankel rhotrices.

In the present paper, we define block rhotrix and block Hankel- like rhotrix. Further, we construct MDS block Hankel-like rhotrices using self-dual bases and conjugate elements of F_{p^n}.

The paper is organised in five sections. The following section provides preliminaries and definitions necessary for the understanding of the paper. In Section 3, we construct MDS block Hankel-like rhotrices using conjugate elements of finite fields. In section 4, self-dual bases of some finite fields are used to construct MDS block Hankel-like rhotrices. Section 5, concludes the results presented in this paper.

2. Preliminaries

Definition 2.1: [10] Finite field A commutative division ring is called a field. A field which contains finite number of elements is called a finite field. It is also called Galois field (GF) named after Evariste Galois.

Definition 2.2: [10] Prime field Prime field is a finite field, which does not contain any proper subfield. For example: $F_2 = \{0,1\}, F_3 = \{0,1,2\}$ are prime fields of order 2 and 3 respectively.

Remark 1: Every finite field has prime order.

Remark 2: For a finite field, every multiplicative group $(F, \times)$ is cyclic, but additive group $(F, +)$ is usually not cyclic.

Remark 3: For every prime power p^n, a field of prime power exists.

Remark 4: All finite fields of same size are isomorphic to each other.

Definition 2.3: [10] Self dual basis A basis $a = \{a_1, a_2, \dots, a_n\}$ of F_{q^n} over F_q is called self-dual if $\mathrm{tr}(a_i a_j) = \delta_{ij}$. A self-dual basis exists in an extension field F_{q^n} of the field F_q if q is even or both q and n are odd.

Definition 2.4: [10] Conjugates Let F_{q^n} be an extension of F_q and let $\alpha \in F_{q^n}$. Then, the conjugate elements of α over extension field F_{q^n} are the roots of the minimal polynomial of α over of F_q. Conjugate elements are known as conjugates.

Definition 2.5: Hankel Matrix A matrix of the form

$$V = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_5 \end{bmatrix}$$

is a Hankel matrix of dimension 3×3. It is denoted by Hank $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$.

Definition 2.6: Hankel Rhotrix A rhotrix of the form

$$R_5 = \left\langle \begin{matrix} & & \alpha_1 & & \\ & \alpha_2 & \alpha_2 & \alpha_2 & \\ \alpha_3 & \alpha_3 & \alpha_3 & \alpha_3 & \alpha_3 \\ & \alpha_4 & \alpha_4 & \alpha_4 & \\ & & \alpha_5 & & \end{matrix} \right\rangle$$

is a Hankel rhotrix. It is denoted by Hank $\{(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5), (\alpha_2, \alpha_3, \alpha_4)\}$.

Definition 2.7: Block Matrix A matrix that can be broken into sections called submatrices or blocks is called a block matrix.

Definition 2.8: Block Rhotrix Let $R = \langle C, D \rangle$ be a rhotrix of dimension $2n-1$, where C and D are coupled block matrices. Here the even ordered coupled matrix is always taken as $(\frac{n}{2} \times \frac{n}{2})$ block matrix and odd ordered coupled matrix is taken as $\left(\frac{n+1}{2} \times \frac{n+1}{2}\right)$ block matrix when n is odd. When n is even, the odd ordered coupled matrix is taken as $\left(\frac{n-2}{2} \times \frac{n-2}{2}\right)$ block matrix. The even ordered matrix is always divided into blocks of (2×2) matrices and the odd ordered matrix is divided into blocks in such a way that the even ordered and odd ordered coupled matrices are of consecutive orders.

Example: $R_7 = \langle C, D \rangle$ is a block rhotrix of dimension 7, where C is a block matrix of order $\frac{4}{2} \times \frac{4}{2}$ whose elements are matrices of order 2×2 and D is a matrix of order 1×1.
$R_9 = \langle C, D \rangle$ is a block rhotrix of dimension 9, where C is a block matrix of order $\frac{5+1}{2} \times \frac{5+1}{2}$ given by

$$C = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix}$$

whose elements are matrices of orders as given below:

$$[C_{11}]_{2\times2}, [C_{12}]_{2\times2}, [C_{13}]_{2\times1}, [C_{21}]_{2\times2}, [C_{22}]_{2\times2}, [C_{23}]_{2\times1}, [C_{31}]_{1\times2}, [C_{32}]_{1\times2}, [C_{33}]_{1\times1}.$$

The coupled block matrix D is of order 2×2 whose elements are matrices of order 2×2.

Lemma 2.9: [16] Any rhotrix $R_{2n+1} = \langle M, N \rangle$ over GF with all non-zero entries is an MDS rhotrix iff its coupled matrices M of order $n+1$ and N of order n are non-singular and all their entries are non-zero.

3. Construction of MDS Block Hankel-like Rhotrices using Conjugate Elements of Finite Fields

In this section, we define block Hankel- like matrix and block Hankel- like rhotrix. Further, we construct MDS block Hankel like rhotrices using the conjugates elements of F_{p^n}.

Definition 3.1: Block Hankel- like Matrix A matrix of the form

$$M = \begin{bmatrix} A & B & C \\ B & C & D \\ C & D & E \end{bmatrix}$$

is a block Hankel matrix of dimension 3×3, where A, B, C, D and E are Hankel matrices.

Definition 3.2: Block Hankel- like Rhotrix Let $R = < M, N >$ be a rhotrix of dimension $2n-1$, where M and N are coupled matrices of order $t \times t$ and $(t-1) \times (t-1)$ respectively. Then, we say that R is a block Hankel - like rhotrix when the coupled matrices $M$and N are block Hankel – like matrices. Here, t is taken in accordance with the definition of block rhotrix given in Section-2.

Theorem 3.3: Let $H_7 = \langle C, D \rangle$ be the block Hankel-like rhotrix of dimension 7, whose coupled block matrices are C and D, defined over F_{3^n}, where elements of C and D are conjugate elements of F_{3^n} i.e. $\{\alpha^{3^i}\}$, $i = 0,1,2, \ldots, n-1$ and $i = 0,1,2, \ldots, n-2$ respectively. Then, $H_7 = \langle C, D \rangle$ forms MDS block Hankel-like rhotrix for $n \geq 5$.

Proof: Consider

$$C = \begin{bmatrix} C_1 & C_2 \\ C_2 & C_3 \end{bmatrix}_{2\times 2}$$

and

$$D = [D_1]_{1\times 1},$$

where C_1, C_2, C_3 are Hankel matrices of 2×2 order given by

$$C_1 = \begin{bmatrix} \alpha & \alpha^3 \\ \alpha^3 & \alpha^9 \end{bmatrix}, \qquad C_2 = \begin{bmatrix} \alpha^9 & \alpha^{27} \\ \alpha^{27} & \alpha^{81} \end{bmatrix}, \qquad C_3 = \begin{bmatrix} \alpha^{81} & \alpha^{243} \\ \alpha^{243} & \alpha^{729} \end{bmatrix}.$$

And D_1 is a 3×3 Hankel matrix given by

$$D_1 = \begin{bmatrix} \alpha^3 & \alpha^9 & \alpha^{27} \\ \alpha^9 & \alpha^{27} & \alpha^{81} \\ \alpha^{27} & \alpha^{81} & \alpha^{243} \end{bmatrix}.$$

Case I: When $n = 5$, let α be the root of irreducible polynomial

$$x^5 + 2x^4 + 1 \in F_{3^5}.$$

Then, using conjugate elements $\{\alpha, \alpha^3, \alpha^9, \alpha^{27}, \alpha^{81}\}$, we show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix.
Here,

$$\begin{aligned} det\ C_1 &= \begin{vmatrix} \alpha & \alpha^3 \\ \alpha^3 & \alpha^9 \end{vmatrix} = \alpha^{11} \neq 0, \\ det\ C_2 &= \begin{vmatrix} \alpha^9 & \alpha^{27} \\ \alpha^{27} & \alpha^{81} \end{vmatrix} = \alpha^{99} \neq 0, \\ det\ C_3 &= \begin{vmatrix} \alpha^{81} & \alpha \\ \alpha & \alpha^3 \end{vmatrix} = \alpha^{165} \neq 0, \\ det\ C &= \det(C_1 C_3 - {C_2}^2) = \alpha^{138} \neq 0. \end{aligned}$$

Therefore, C is an MDS block Hankel matrix.
Likewise,

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^3 & \alpha^9 & \alpha^{27} \\ \alpha^9 & \alpha^{27} & \alpha^{81} \\ \alpha^{27} & \alpha^{81} & \alpha \end{vmatrix} = \alpha^{188} \neq 0.$$

This implies that D is an MDS block Hankel matrix.

Using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & & \\ & & \alpha^3 & \alpha^3 & \alpha^3 & & \\ & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \\ \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} \\ & \alpha^{81} & \alpha^{81} & \alpha^{81} & \alpha^{81} & \alpha^{81} & \\ & & \alpha & \alpha & \alpha & & \\ & & & \alpha^3 & & & \end{matrix} \right\rangle.$$

is an MDS block Hankel- like rhotrix.

Case II: When $n = 6$, let α be a root of irreducible polynomial

$$x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 2 \in F_{3^6}.$$

Then, using conjugate elements $\{\alpha, \alpha^3, \alpha^9, \alpha^{27}, \alpha^{81}, \alpha^{243}\}$, we will show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix.
Here,

$$\begin{aligned} det\ C_1 &= \begin{vmatrix} \alpha & \alpha^3 \\ \alpha^3 & \alpha^9 \end{vmatrix} = \alpha^{439} \neq 0, \\ det\ C_2 &= \begin{vmatrix} \alpha^9 & \alpha^{27} \\ \alpha^{27} & \alpha^{81} \end{vmatrix} = \alpha^{311} \neq 0, \end{aligned}$$

$$det\ C_3 = \begin{vmatrix} \alpha^{81} & \alpha^{243} \\ \alpha^{243} & \alpha \end{vmatrix} = \alpha^{659} \neq 0,$$
$$det\ C = det\ (C_1C_3 - {C_2}^2) = \alpha^{365} \neq 0.$$

This shows, C is an MDS block Hankel matrix.
Similarly,

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^3 & \alpha^9 & \alpha^{27} \\ \alpha^9 & \alpha^{27} & \alpha^{81} \\ \alpha^{27} & \alpha^{81} & \alpha^{243} \end{vmatrix} = \alpha^{25} \neq 0,$$

which implies, D is an MDS block Hankel matrix.
Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & & \\ & & & \alpha^3 & \alpha^3 & \alpha^3 & \\ & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \\ \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} \\ & \alpha^{81} & \alpha^{81} & \alpha^{81} & \alpha^{81} & \alpha^{81} & \\ & & \alpha^{243} & \alpha^{243} & \alpha^{243} & & \\ & & & \alpha & & & \end{matrix} \right\rangle.$$

is an MDS block Hankel- like rhotrix.

Case III: When $n = 7$ and α be a root of irreducible polynomial

$$x^7 + 2x^6 + x^5 + 1 \in F_{3^7}.$$

The conjugate elements of F_{3^7} are given by $\{\alpha, \alpha^3, \alpha^9, \alpha^{27}, \alpha^{81}, \alpha^{243}, \alpha^{729}\}$, we will show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix.
In C, we have

$$det\ C_1 = \begin{vmatrix} \alpha & \alpha^3 \\ \alpha^3 & \alpha^9 \end{vmatrix} = \alpha^{1889} \neq 0,$$
$$det\ C_2 = \begin{vmatrix} \alpha^9 & \alpha^{27} \\ \alpha^{27} & \alpha^{81} \end{vmatrix} = \alpha^{1699} \neq 0,$$
$$det\ C_3 = \begin{vmatrix} \alpha^{81} & \alpha^{243} \\ \alpha^{243} & \alpha^{729} \end{vmatrix} = \alpha^{2175} \neq 0,$$
$$det\ C = det\ (C_1C_3 - {C_2}^2) = \alpha^{1234} \neq 0.$$

Since the determinant of all the elements of C are non-zero, therefore, we can say that C is a MDS block Hankel matrix.
Similarly, we have

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^3 & \alpha^9 & \alpha^{27} \\ \alpha^9 & \alpha^{27} & \alpha^{81} \\ \alpha^{27} & \alpha^{81} & \alpha^{243} \end{vmatrix} = \alpha^{775} \neq 0.$$

This implies that D is an MDS matrix.
Then, from Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & & \\ & & & \alpha^3 & \alpha^3 & \alpha^3 & \\ & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \\ \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} & \alpha^{27} \\ & \alpha^{81} & \alpha^{81} & \alpha^{81} & \alpha^{81} & \alpha^{81} & \\ & & \alpha^{243} & \alpha^{243} & \alpha^{243} & & \\ & & & \alpha^{729} & & & \end{matrix} \right\rangle.$$

is a MDS block Hankel- like rhotrix.

Similarly, it can be shown that H_7 is a MDS block Hankel- like rhotrix for all values of n.
Hence, H_7 is a MDS block Hankel- like rhotrix over F_{3^n}.

Theorem 3.4: Let $H_7 = \langle C, D \rangle$ be the block Hankel-like rhotrix of dimension 7, whose coupled block matrices are C and D, defined over prime field F_{2^n}, where elements of $H_7 = \langle C, D \rangle$ are conjugate elements of F_{2^n} i.e.$\{\alpha^{2^i}\}$, $i = 0,1,2,\dots,n-1$ for matrix C and $i = 0,1,2,\dots,n-2$ for matrix D respectively. Then, $H_7 = \langle C, D \rangle$ forms MDS block Hankel-like rhotrix for $n \geq 5$.

Proof: Here, we have

$$C = \begin{bmatrix} C_1 & C_2 \\ C_2 & C_3 \end{bmatrix}_{2\times 2}$$

and

$$D = [D_1]_{1\times 1},$$

where C_1, C_2, C_3 are Hankel matrices of 2×2 order given by

$$C_1 = \begin{bmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha^4 \end{bmatrix}, \qquad C_2 = \begin{bmatrix} \alpha^4 & \alpha^8 \\ \alpha^8 & \alpha^{16} \end{bmatrix}, \qquad C_3 = \begin{bmatrix} \alpha^{16} & \alpha \\ \alpha & \alpha^2 \end{bmatrix}.$$

Also, D_1 is a 3×3 Hankel matrix given by

$$D_1 = \begin{bmatrix} \alpha^2 & \alpha^4 & \alpha^8 \\ \alpha^4 & \alpha^8 & \alpha^{16} \\ \alpha^8 & \alpha^{16} & \alpha \end{bmatrix}.$$

Case I: For $n = 5$ and α be a root of irreducible polynomial

$$x^5 + x^2 + 1 \in F_{2^5}.$$

Then, using conjugate elements $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$, we will show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix. Here,

$$det\ C_1 = \begin{vmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha^4 \end{vmatrix} = \alpha^{21} \neq 0,$$
$$det\ C_2 = \begin{vmatrix} \alpha^4 & \alpha^8 \\ \alpha^8 & \alpha^{16} \end{vmatrix} = \alpha^{26} \neq 0,$$
$$det\ C_3 = \begin{vmatrix} \alpha^{16} & \alpha \\ \alpha & \alpha^2 \end{vmatrix} = \alpha^{11} \neq 0,$$
$$det\ C = det\ (C_1 C_3 - {C_2}^2) = \alpha^{31} \neq 0.$$

Therefore, we can say that C is an MDS block Hankel matrix.
Likewise, we show that

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^2 & \alpha^4 & \alpha^8 \\ \alpha^4 & \alpha^8 & \alpha^{16} \\ \alpha^8 & \alpha^{16} & \alpha \end{vmatrix} = \alpha^{27} \neq 0.$$

This implies that D is an MDS matrix.
Then, from Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle,$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & \\ & & \alpha^2 & \alpha^2 & \alpha^2 & \\ & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 & \\ \alpha^8 & \alpha^8 & \alpha^8 & \alpha^8 & \alpha^8 & \alpha^8 & \alpha^8 \\ & \alpha^{16} & \alpha^{16} & \alpha^{16} & \alpha^{16} & \alpha^{16} & \\ & & \alpha & \alpha & \alpha & & \\ & & & \alpha^2 & & & \end{matrix} \right\rangle$$

is an MDS block Hankel- like rhotrix.

Case II: When $n = 6$ and α be a root of irreducible polynomial

$$x^6 + x + 1 \in F_{2^6}.$$

Then, using conjugate elements $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}\}$, we will show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix.
Here,

$$det\, C_1 = \begin{vmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha^4 \end{vmatrix} = \alpha^{62} \neq 0,$$
$$det\, C_2 = \begin{vmatrix} \alpha^4 & \alpha^8 \\ \alpha^8 & \alpha^{16} \end{vmatrix} = \alpha^{59} \neq 0,$$
$$det\, C_3 = \begin{vmatrix} \alpha^{16} & \alpha^{32} \\ \alpha^{32} & \alpha \end{vmatrix} = \alpha^{47} \neq 0,$$
$$det\, C = det\, (C_1 C_3 - {C_2}^2) = \alpha^{23} \neq 0.$$

Therefore, we can say that C is an MDS block Hankel matrix.
In the same manner, we show that

$$det\, D = det\, D_1 = \begin{vmatrix} \alpha^2 & \alpha^4 & \alpha^8 \\ \alpha^4 & \alpha^8 & \alpha^{16} \\ \alpha^8 & \alpha^{16} & \alpha^{32} \end{vmatrix} = \alpha^{158} \neq 0.$$

Therefore, D is an MDS matrix.
Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle,$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & \\ & & \alpha^2 & \alpha^2 & \alpha^2 & \\ \alpha^8 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^8 \\ & \alpha^8 & \alpha^8 & \alpha^8 & \alpha^8 & \alpha^8 & \\ & \alpha^{16} & \alpha^{16} & \alpha^{16} & \alpha^{16} & \alpha^{16} & \\ & & \alpha^{32} & \alpha^{32} & \alpha^{32} & & \\ & & & \alpha & & & \end{matrix} \right\rangle$$

is an MDS block Hankel- like rhotrix.
In the same way, it can be shown that H_7 is an MDS block Hankel- like rhotrix for all values of n.
Hence, H_7 is an MDS block Hankel- like rhotrix over F_{2^n}.

Theorem 3.5: Let $H_7 = \langle C, D \rangle$ be the block Hankel-like rhotrix of dimension 7, whose coupled block matrices are C and D, defined over prime field F_{5^n}, where elements of $H_7 = \langle C, D \rangle$ are conjugate elements of F_{5^n} i.e $\left\{\alpha^{5^i}\right\}$, $i = 0,1,2, \ldots, n-1$ and $i = 0,1,2, \ldots, n-2$ respectively. Then, $H_7 = \langle C, D \rangle$ forms MDS block Hankel-like rhotrix for $n \geq 5$.

Proof: Let us take

$$C = \begin{bmatrix} C_1 & C_2 \\ C_2 & C_3 \end{bmatrix}_{2\times 2}$$

and

$$D = [D_1]_{1\times 1}$$

where C_1, C_2, C_3 are Hankel matrices of 2×2 order given by

$$C_1 = \begin{bmatrix} \alpha & \alpha^5 \\ \alpha^5 & \alpha^{25} \end{bmatrix}, \qquad C_2 = \begin{bmatrix} \alpha^{25} & \alpha^{125} \\ \alpha^{125} & \alpha^{625} \end{bmatrix}, \qquad C_3 = \begin{bmatrix} \alpha^{625} & \alpha \\ \alpha & \alpha^5 \end{bmatrix}.$$

Also, D_1 is a 3×3 Hankel matrix given by

$$D_1 = \begin{bmatrix} \alpha^5 & \alpha^{25} & \alpha^{125} \\ \alpha^{25} & \alpha^{125} & \alpha^{625} \\ \alpha^{125} & \alpha^{625} & \alpha \end{bmatrix}.$$

Case I: When $n = 5$, let α be a root of irreducible polynomial

$$x^5 + 4x^4 + 3x^3 + x^2 + 2x + 3 \in F_{5^5}.$$

Then, the conjugate elements of $F_{5^5}$are given by $\{\alpha, \alpha^5, \alpha^{25}, \alpha^{125}, \alpha^{625}\}$.

Here,

$$det\, C_1 = \begin{vmatrix} \alpha & \alpha^5 \\ \alpha^5 & \alpha^{25} \end{vmatrix} = \alpha^{748} \neq 0,$$

$$det\, C_2 = \begin{vmatrix} \alpha^{25} & \alpha^{125} \\ \alpha^{125} & \alpha^{625} \end{vmatrix} = \alpha^{3080} \neq 0,$$

$$det\, C_3 = \begin{vmatrix} \alpha^{625} & \alpha \\ \alpha & \alpha^5 \end{vmatrix} = \alpha^{2024} \neq 0,$$

$$det\, C = det\, (C_1 C_3 - {C_2}^2) = \alpha^{3119} \neq 0.$$

Therefore, we can say that C is an MDS block Hankel matrix.

Likewise, we show that

$$det\, D = det\, D_1 = \begin{vmatrix} \alpha^5 & \alpha^{25} & \alpha^{125} \\ \alpha^{25} & \alpha^{125} & \alpha^{625} \\ \alpha^{125} & \alpha^{625} & \alpha \end{vmatrix} = \alpha^{2274} \neq 0.$$

This implies that D is an MDS matrix.

Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle,$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & \\ & & \alpha^5 & \alpha^5 & \alpha^5 & \\ & \alpha^{25} & \alpha^{25} & \alpha^{25} & \alpha^{25} & \alpha^{25} & \\ \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} \\ & \alpha^{625} & \alpha^{625} & \alpha^{625} & \alpha^{625} & \alpha^{625} & \\ & & \alpha & \alpha & \alpha & & \\ & & & \alpha^5 & & & \end{matrix} \right\rangle$$

is an MDS block Hankel- like rhotrix.

Case II: When $n = 6$, let α be a root of irreducible polynomial

$$x^6 + x^4 + x^3 + x^2 + 2 \in F_{5^6}.$$

Then, the conjugate elements of $F_{5^6}$are $\{\alpha, \alpha^5, \alpha^{25}, \alpha^{125}, \alpha^{625}, \alpha^{3125}\}$. To show that $H_7 = \langle C, D \rangle$ is a block Hankel-like rhotrix, we evaluate determinant of elements of C as given below:

$$det\, C_1 = \begin{vmatrix} \alpha & \alpha^5 \\ \alpha^5 & \alpha^{25} \end{vmatrix} = \alpha^{10462} \neq 0,$$

$$det\, C_2 = \begin{vmatrix} \alpha^{25} & \alpha^{125} \\ \alpha^{125} & \alpha^{625} \end{vmatrix} = \alpha^{11566} \neq 0,$$

$$det\ C_3 = \begin{vmatrix} \alpha^{625} & \alpha^{3125} \\ \alpha^{3125} & \alpha \end{vmatrix} = \alpha^{7918} \neq 0,$$

$$det\ C = det\ (C_1 C_3 - {C_2}^2) = \alpha^{2026} \neq 0.$$

So, we conclude that C is an MDS block Hankel matrix.

Similarly, we evaluate,

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^5 & \alpha^{25} & \alpha^{125} \\ \alpha^{25} & \alpha^{125} & \alpha^{625} \\ \alpha^{125} & \alpha^{625} & \alpha^{3125} \end{vmatrix} = \alpha^{125} \neq 0,$$

which shows that D is an MDS matrix.

Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle,$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & & \\ & & & \alpha^5 & \alpha^5 & \alpha^5 & \\ & \alpha^{25} & \alpha^{25} & \alpha^{25} & \alpha^{25} & \alpha^{25} & \\ \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} & \alpha^{125} \\ & \alpha^{625} & \alpha^{625} & \alpha^{625} & \alpha^{625} & \alpha^{625} & \\ & & \alpha^{3125} & \alpha^{3125} & \alpha^{3125} & & \\ & & & \alpha & & & \end{matrix} \right\rangle$$

is an MDS block Hankel- like rhotrix.

Similarly, it can be shown that H_7 is a MDS block Hankel- like rhotrix for all values of n.

Hence, H_7 is an MDS block Hankel- like rhotrix over field F_{5^n}.

4. Construction of MDS Block Hankel-like Rhotrices using Self-dual Bases of Finite Field

Self-dual bases are useful in many applications like the construction of devices for the arithmetic in finite fields such as multiplication, exponentiation, discrete logarithms and in applications to coding theory, cryptography and the discrete Fourier transforms. In this section, we use self-dual bases of F_{p^n} to construct MDS block Hankel -like rhotrices.

Theorem 4.1: Let $H_7 = \langle C, D \rangle$ be the block Hankel-like rhotrix of dimension 7, whose coupled block matrices are C and D, defined over F_{2^n}, where elements of C and D are given by self dual bases of F_{2^n}. Then, $H_7 = \langle C, D \rangle$ forms MDS block Hankel-like rhotrix for $n \geq 6$.

Proof: Consider,

$$C = \begin{bmatrix} C_1 & C_2 \\ C_2 & C_3 \end{bmatrix}_{2\times 2}$$

and

$$D = [D_1]_{1\times 1},$$

where C_1, C_2, C_3 are Hankel matrices of 2×2 order and D_1 is a 3×3 Hankel matrix.

Case I: When $n = 6$, let α be a root of irreducible polynomial

$$x^6 + x + 1 \in F_{2^6}.$$

The self-dual basis of $F_{2^6}$is given by $\{\alpha^3,\ \alpha^4,\ \alpha^{53},\ \alpha^{24},\ \alpha^{32},\ \alpha^{46}\}$.

Here,

$$det\ C_1 = \begin{vmatrix} \alpha^3 & \alpha^4 \\ \alpha^4 & \alpha^{53} \end{vmatrix} = \alpha^{48} \neq 0,$$

$$det\ C_2 = \begin{vmatrix} \alpha^{53} & \alpha^{24} \\ \alpha^{24} & \alpha^{32} \end{vmatrix} = \alpha^{41} \neq 0,$$

$$det\ C_3 = \begin{vmatrix} \alpha^{32} & \alpha^{46} \\ \alpha^{46} & \alpha^{3} \end{vmatrix} = \alpha^{34} \neq 0,$$

$$det\ C = det\ (C_1 C_3 - {C_2}^2) = \alpha^{21} \neq 0.$$

This gives, C is an MDS block Hankel matrix.

Likewise, we evaluate

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^4 & \alpha^{53} & \alpha^{24} \\ \alpha^{53} & \alpha^{24} & \alpha^{32} \\ \alpha^{24} & \alpha^{32} & \alpha^{46} \end{vmatrix} = \alpha^{39} \neq 0.$$

This implies that D is an MDS matrix.

Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha^3 & & & \\ & & \alpha^4 & \alpha^4 & \alpha^4 & & \\ & \alpha^{53} & \alpha^{53} & \alpha^{53} & \alpha^{53} & \alpha^{53} & \\ \alpha^{24} & \alpha^{24} & \alpha^{24} & \alpha^{24} & \alpha^{24} & \alpha^{24} & \alpha^{24} \\ & \alpha^{32} & \alpha^{32} & \alpha^{32} & \alpha^{32} & \alpha^{32} & \\ & & \alpha^{46} & \alpha^{46} & \alpha^{46} & & \\ & & & \alpha^3 & & & \end{matrix} \right\rangle.$$

is an MDS block Hankel- like rhotrix.

Case II: For $n = 8$ and α be a root of irreducible polynomial

$$x^8 + x^6 + x^5 + x^2 + 1 \in F_{2^8}.$$

The self-dual basis of F_{2^8} is given by$\{\alpha^{32},\ \alpha^{64},\ \alpha^{240},\ \alpha,\ \alpha^{129},\ \alpha^{195},\ \alpha^{69},\ \alpha^{111}\}$.

Now, to show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix, we evaluate

$$det\ C_1 = \begin{vmatrix} \alpha^{32} & \alpha^{64} \\ \alpha^{64} & \alpha^{240} \end{vmatrix} = \alpha^{148} \neq 0,$$

$$det\ C_2 = \begin{vmatrix} \alpha^{240} & \alpha \\ \alpha & \alpha^{129} \end{vmatrix} = \alpha^{239} \neq 0,$$

$$det\ C_3 = \begin{vmatrix} \alpha^{129} & \alpha^{195} \\ \alpha^{195} & \alpha^{69} \end{vmatrix} = \alpha^{97} \neq 0,$$

$$det\ C = \det\ (C_1 C_3 - {C_2}^2) = \alpha^{98} \neq 0.$$

Since all the determinant are non-zero, therefore, we can say that C is an MDS block Hankel matrix.

Similarly, we compute

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^{64} & \alpha^{240} & \alpha \\ \alpha^{240} & \alpha & \alpha^{129} \\ \alpha & \alpha^{129} & \alpha^{195} \end{vmatrix} = \alpha^{99} \neq 0$$

which shows that D is an MDS matrix.

Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha^{32} & & & \\ & & \alpha^{64} & \alpha^{64} & \alpha^{64} & & \\ & \alpha^{240} & \alpha^{240} & \alpha^{240} & \alpha^{240} & \alpha^{240} & \\ \alpha & \alpha & \alpha & \alpha & \alpha & \alpha & \alpha \\ & \alpha^{129} & \alpha^{129} & \alpha^{129} & \alpha^{129} & \alpha^{129} & \\ & & \alpha^{195} & \alpha^{195} & \alpha^{195} & & \\ & & & \alpha^{69} & & & \end{matrix} \right\rangle.$$

is an MDS block Hankel- like rhotrix.

Similarly, it can be shown that H_7 is an MDS block Hankel- like rhotrix for all values of n.

Hence, H_7 is an MDS block Hankel- like rhotrix over F_{2^n}.

Theorem 4.2: Let $H_7 = \langle C, D \rangle$ be the block Hankel-like rhotrix of dimension 7, whose coupled block matrices are C and D, defined overF_{3^n}, where elements of C and D are given by self-dual basis of F_{3^n}. Then, $H_7 = \langle C, D \rangle$ forms MDS block Hankel-like rhotrix for $n \geq 5$.

Proof: Consider,

$$C = \begin{bmatrix} C_1 & C_2 \\ C_2 & C_3 \end{bmatrix}_{2\times 2}$$

and

$$D = [D_1]_{1\times 1},$$

where C_1, C_2, C_3 are Hankel matrices of 2×2 order and D_1 is a 3×3 Hankel matrix.
Case I: When $n = 5$ and α be a root of irreducible polynomial

$$x^5 + 2x^4 + 1 \in F_{3^5}.$$

The self-dual basis of F_{3^5} is given by $\{\alpha,\ \alpha^{18},\ \alpha^{28},\ \alpha^{39},\ \alpha^{170}\}$.

Now, to show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix, we compute

$$det\ C_1 = \begin{vmatrix} \alpha & \alpha^{18} \\ \alpha^{18} & \alpha^{28} \end{vmatrix} = \alpha^{242} \neq 0,$$

$$det\ C_2 = \begin{vmatrix} \alpha^{28} & \alpha^{39} \\ \alpha^{39} & \alpha^{170} \end{vmatrix} = \alpha^{130} \neq 0,$$

$$det\ C_3 = \begin{vmatrix} \alpha^{170} & \alpha \\ \alpha & \alpha^{18} \end{vmatrix} = \alpha^{213} \neq 0,$$

$$det\ C = det\ (C_1C_3 - {C_2}^2) = \alpha^{128} \neq 0.$$

The non-zero determinants ensure that C is an MDS block Hankel matrix.

Likewise, we show that

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^{18} & \alpha^{28} & \alpha^{39} \\ \alpha^{28} & \alpha^{39} & \alpha^{170} \\ \alpha^{39} & \alpha^{170} & \alpha \end{vmatrix} = \alpha^{121} \neq 0.$$

This implies that D is an MDS matrix.

Then, from Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha & & & \\ & & \alpha^{18} & \alpha^{18} & \alpha^{18} & & \\ & \alpha^{28} & \alpha^{28} & \alpha^{28} & \alpha^{28} & \alpha^{28} & \\ \alpha^{39} & \alpha^{39} & \alpha^{39} & \alpha^{39} & \alpha^{39} & \alpha^{39} & \alpha^{39} \\ & \alpha^{170} & \alpha^{170} & \alpha^{170} & \alpha^{170} & \alpha^{170} & \\ & & \alpha & \alpha & \alpha & & \\ & & & \alpha^{18} & & & \end{matrix} \right\rangle.$$

is an MDS block Hankel- like rhotrix.

Case II: When $n = 7$, let α be a root of irreducible polynomial

$$x^7 + 2x^6 + x^5 + 1 \in F_{3^7}.$$

The self-dual basis of $F_{3^7}$is given by $\{\alpha^{20},\ \alpha^{23},\ \alpha^{104},\ \alpha^{109},\ \alpha^{526}, \alpha^{531}, \alpha^{723}\}$.

Now, we will show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix.

Here,

$$det\ C_1 = \begin{vmatrix} \alpha^{20} & \alpha^{23} \\ \alpha^{23} & \alpha^{104} \end{vmatrix} = \alpha^{1168} \neq 0,$$

$$det\ C_2 = \begin{vmatrix} \alpha^{104} & \alpha^{109} \\ \alpha^{109} & \alpha^{526} \end{vmatrix} = \alpha^{553} \neq 0,$$

$$det\ C_3 = \begin{vmatrix} \alpha^{526} & \alpha^{531} \\ \alpha^{531} & \alpha^{723} \end{vmatrix} = \alpha^{934} \neq 0,$$

$$det\ C = det\ (C_1 C_3 - {C_2}^2) = \alpha^{1413} \neq 0.$$

Therefore, we can say that C is an MDS block Hankel matrix.

Likewise, we show that

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^{23} & \alpha^{104} & \alpha^{109} \\ \alpha^{104} & \alpha^{109} & \alpha^{526} \\ \alpha^{109} & \alpha^{526} & \alpha^{531} \end{vmatrix} = \alpha^{134} \neq 0.$$

This implies that D is an MDS matrix.

Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha^{20} & & \\ & & \alpha^{23} & \alpha^{23} & \alpha^{23} & \\ & \alpha^{104} & \alpha^{104} & \alpha^{104} & \alpha^{104} & \alpha^{104} & \\ \alpha^{109} & \alpha^{109} & \alpha^{109} & \alpha^{109} & \alpha^{109} & \alpha^{109} & \alpha^{109} \\ & \alpha^{526} & \alpha^{526} & \alpha^{526} & \alpha^{526} & \alpha^{526} & \\ & & \alpha^{531} & \alpha^{531} & \alpha^{531} & & \\ & & & \alpha^{723} & & & \end{matrix} \right\rangle.$$

is an MDS block Hankel- like rhotrix.

Similarly, it can be shown that H_7 is an MDS block Hankel- like rhotrix for all values of n.

Hence, H_7 is an MDS block Hankel- like rhotrix over F_{3^n}.

Theorem 4.3: Let $H_7 = \langle C, D \rangle$ be the block Hankel-like rhotrix of dimension 7, whose coupled block matrices are C and D, defined over F_{5^n}, where elements of C and D are given by self- dual basis of F_{5^n}. Then, $H_7 = \langle C, D \rangle$ forms MDS block Hankel-like rhotrix for $n \geq 5$.

Proof: Consider,

$$C = \begin{bmatrix} C_1 & C_2 \\ C_2 & C_3 \end{bmatrix}_{2\times 2}$$

and

$$D = [D_1]_{1\times 1},$$

where C_1, C_2, C_3 are Hankel matrices of 2×2 and D_1 is a 3×3 Hankel matrix.
Case I: When $n = 5$, let α be a root of irreducible polynomial

$$x^5 + 4x^4 + 3x^3 + x^2 + 2x \quad + 3 \in F_{5^5}.$$

The self-dual basis of F_{3^5} is given by $\{\alpha^{12},\ \alpha^{41},\ \alpha^{165},\ \alpha^{1233},\ \alpha^{1352}\}$.

To show that $H_7 = \langle C, D \rangle$ is a block Hankel- like rhotrix, we evaluate,

$$det\ C_1 = \begin{vmatrix} \alpha^{12} & \alpha^{41} \\ \alpha^{41} & \alpha^{165} \end{vmatrix} = \alpha^{2088} \neq 0,$$

$$det\ C_2 = \begin{vmatrix} \alpha^{165} & \alpha^{1233} \\ \alpha^{1233} & \alpha^{1352} \end{vmatrix} = \alpha^{1063} \neq 0,$$

$$det\ C_3 = \begin{vmatrix} \alpha^{1352} & \alpha^{12} \\ \alpha^{12} & \alpha^{41} \end{vmatrix} = \alpha^{1863} \neq 0,$$

$$det\ C = det\ (C_1C_3 - {C_2}^2) = \alpha^{1094} \neq 0.$$

The non-zero determinants show that C is an MDS block Hankel matrix.

Likewise, we show that

$$det\ D = det\ D_1 = \begin{vmatrix} \alpha^{41} & \alpha^{165} & \alpha^{1233} \\ \alpha^{165} & \alpha^{1233} & \alpha^{1352} \\ \alpha^{1233} & \alpha^{1352} & \alpha^{12} \end{vmatrix} = \alpha^{2138} \neq 0.$$

This implies that D is an MDS matrix.

Then, using Lemma 2.9, we conclude that

$$H_7 = \left\langle \begin{matrix} & A_1 & \\ A_2 & D_1 & A_2 \\ & A_3 & \end{matrix} \right\rangle$$

$$H_7 = \left\langle \begin{matrix} & & & \alpha^{12} & & \\ & & \alpha^{41} & \alpha^{41} & \alpha^{41} & \\ \alpha^{1233} & \alpha^{165} & \alpha^{165} & \alpha^{165} & \alpha^{165} & \alpha^{165} & \alpha^{1233} \\ & \alpha^{1233} & \alpha^{1233} & \alpha^{1233} & \alpha^{1233} & \alpha^{1233} & \\ & \alpha^{1352} & \alpha^{1352} & \alpha^{1352} & \alpha^{1352} & \alpha^{1352} & \\ & & \alpha^{12} & \alpha^{12} & \alpha^{12} & & \\ & & & \alpha^{41} & & & \end{matrix} \right\rangle.$$

is an MDS block Hankel- like rhotrix.

Similarly, it can be shown that H_7 is an MDS block Hankel- like rhotrix for all values of n.

Hence, H_7 is an MDS block Hankel- like rhotrix over F_{5^n}.

5. Conclusion

In this paper, we defined block rhotrix and block Hankel-like rhotrix. We constructed MDS block Hankel-like rhotrices using conjugate elements of F_{p^n} for $n \geq 5$. Further, we constructed block Hankel-like MDS rhotrices for $n \geq 5$, with the help of self-dual bases of F_{p^n}.

References

[1] Ajibade, A. O. (2003). The concept of rhotrices in mathematical enrichment, Int. J. Math. Educ. Sci. Tech., 34(2), 175-179.

[2] Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone. (1996, Third Edition). Hand book of Applied Cryptography, CRC Press.

[3] Atanassov, K. T. and Shannon, A. G. (1998). Matrix-Tertions and Matrix-Noitrets: Exercises in Mathematical Enrichment. International Journal of Mathematical Education in science and technology, 29, 898-903.

[4] Barreto P. and Rijman V. (2000). The Khazad Legacy level block cipher, NISSIE Project.

[5] Daemen J. and Rijmen V. (2000). The design of Rijndael: AES – The Advanced Data Encryption, Springer.

[6] Fazel, M., Pong, T. K., Sun, D. and Paul, T. (2013). Hankel matrix rank minimization with applications to system identification and realization, SIAM J. Matrix Anal. & Appl., 34(3), 946-977.

[7] Gupta, K. C. and Ray, I. G. (2014). On constructions of MDS matrices from circulant- like matrices for lightweight cryptography, ASU/2014/1.

[8] Junod, P. And Vaudenay, S. (2004). Perfect diffusion primitives for block ciphers building efficient MDS matrices, Lecture notes in computer science, Vol. 9-10.

[9] Lacan, J. and Fimes, J. (2004). Systematic MDS erasure codes based on Vandermonde matrices, IEEE Trans. Commun. Lett. 8(9), 570-572.

[10] Mohammed, A., Ezugwu, E.A. and Sani, B. (2011). On generalization and algorithmatization of heart-based method for multiplication of rhotrices, International Journal of Computer Information Systems, 2, 46-49.

[11] Sajadieh, M., Dakhilian, M., Mala, H. and Omoomi, B. (2012). On construction of involutory MDS matrices from Vandermonde matrices, Des. Codes and Cry, 64, 287-308.

[12] Sani, B. (2004). An alternative method for multiplication of rhotrices, Int. J. Math. Educ. Science Tech., 35(5), 777-781.

[13] Sharma P. L., Kumar Arun, Gupta Shalini (2019). Construction of MDS Hankel Rhotrices over finite fields, AAM International Journal of Applied Mathematics, 14, 1197-1214.

[14] Sharma, P. L., Gupta, S. and Rehan, M. (2015). Construction of MDS rhotrices using special type of circulant rhotrices over finite fields, Himachal Pradesh University Journal, 3(2), 25-43.

[15] Sharma, P. L. and Kumar, S. (2013). On construction of MDS rhotrices from companion rhotrices over finite field, International Journal of Mathematical Sciences, 12(3-4), 271-286.

[16] Sharma, P. L., Kumar, A. and Gupta, S. (2018). Maximum Distance Separable Hankel Rhotrices over Finite Fields, J. of Combinatorics, Information & System Sciences, 43(1-4), 13-48.

[17] Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, Erik De Win (February, 1996). The Cipher SHARK. 3rd International workshop on Fast Software Encryption.

****