Applications and Applied Mathematics: An International Journal (AAM)

Volume 14 | Issue 2 | Article 38

12-2019

Hankel Rhotrices and Constructions of Maximum Distance Separable Rhotrices over Finite Fields

P. L. Sharma
Himachal Pradesh University

Arun Kumar
Himachal Pradesh University

Shalini Gupta
Bahra University

Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Applications and Applied Mathematics:
An International Journal
(AAM)

Vol. 14, Issue 2 (December 2019), pp. 1197 - 1214

Hankel Rhotrices and Constructions of Maximum Distance Separable Rhotrices over Finite Fields

[1*]P. L. Sharma, [2]Arun Kumar and [3]Shalini Gupta

[1,2]Department of Mathematics & Statistics
Himachal Pradesh University
Shimla - 5, India
[1]plsharma1964@gmail.com;

[3]Bahra University
Solan, H.P., India

[*]Corresponding Author

Received: May 31, 2018; Accepted: May 31, 2019

Abstract

Many block ciphers in cryptography use Maximum Distance Separable (MDS) matrices to strengthen the diffusion layer. Rhotrices are represented by coupled matrices. Therefore, use of rhotrices in the cryptographic ciphers doubled the security of the cryptosystem. We define Hankel rhotrix and further construct the maximum distance separable rhotrices over finite fields.

Keywords: Hankel matrix; Hankel rhotrix; Finite field; Maximum distance separable rhotrix

MSC 2010 No.: 15A09, 20H30, 11T71

1. Introduction

Cryptography is the science of converting plaintext into ciphertext and vice versa. Many encrypting and decrypting algorithms make use of matrices. Those matrices, which are contributing in the field of cryptography, have been extended by many researchers in the framework of rhotrices. Rhotrices are represented in the form of coupled matrices. The use of one rhotrix in any algorithm of cryptosystem means the use of two matrices of different dimensions. Therefore, rhotrices double the security and hence rhotrices can help to provide more security in the existing available cryptographic algorithms.

Maximum Distance Separable (MDS) matrices have applications in coding theory and cryptography, particularly in the design of block ciphers and hash functions, see Alfred et al. (1996). It is highly non-trivial to find MDS matrices, which could be used in light weight cryptography. An MDS matrix offer diffusion properties and is one of the important constituents of modern age ciphers like Advanced Encryption Standard (AES), Twofish, Shark etc….
The concept of rhotrix was developed by Ajibade (2003).

Sani (2008) introduced the concept of coupled matrices in rhotrices. This representation is useful in cryptography to improve the security, see Sharma and Kumar (2014a, 2014b and 2014c) and Sharma et al. (2013). Tudunkaya et al. (2010) discussed rhotrices over finite fields. The investigations of rhotrices over matrix theory and polynomials ring theory are discussed by Aminu (2012) and Tudunkaya (2013). The algebra and analysis of rhotrices is discussed in the literature by Absalom et al. (2011), Aminu (2009), Mohammed (2011), Sharma and Kanwar (2011, 2012a, 2012b, 2012c, 2013) and Sharma et al. (2015, 2017). Sylvester rhotrices and their properties are discussed in Sharma et al. (2017b). Nakahara and Abraho (2009) constructed an involutory MDS matrix of 16- order by using a Cauchy matrix which was used in MDS-AES design. There are several methods to construct MDS matrices. Sajadieh et al. (2012) used Vandermonde matrices for the construction of MDS matrices. The constructions of MDS rhotrices using Cauchy rhotrices are discussed by Sharma et al. (2017a).

Toeplitz matrices are useful in light weight cryptography. The maximum distance separable matrices achieve the minimum XOR count when it is constructed through Toeplitz matrices, see Sarkar and Habeeb (2016). The constructions of MDS rhotrices using Toeplitz rhotrices are discussed by Sharma and Gupta (2017). Hankel matrices arise naturally in a wide range of applications in science, engineering and other related areas such as signal processing and control theory, see Fazel et al. (2013).

2. Formulation of the Problem

A rhotrix is defined as a mathematical array, which is in some way between a 2×2 matrix and 3×3 matrix and is given as

$$R_3 = \left\{ \left\langle \begin{array}{ccc} & a & \\ b & c & d \\ & e & \end{array} \right\rangle : a, b, c, d, e \in \Re \right\}.$$

Two types of multiplication methods of rhotrices are discussed in the literature. The heart oriented multiplication of rhotrices

$$R_3 = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle \text{ and } Q_3 = \left\langle \begin{matrix} & f & \\ g & h & j \\ & k & \end{matrix} \right\rangle$$

is defined by Ajibade (2003) as

$$R_3 \, o \, Q_3 = \left\langle \begin{matrix} & ah + fc & \\ bh + gc & ch & dh + jc \\ & eh + kc & \end{matrix} \right\rangle.$$

The row-column multiplication of rhotrices is defined by Sani (2004) as

$$R_3 \, o \, Q_3 = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle \left\langle \begin{matrix} & f & \\ g & h & j \\ & k & \end{matrix} \right\rangle = \left\langle \begin{matrix} & af + dg & \\ bf + eg & ch & aj + dk \\ & bj + ek & \end{matrix} \right\rangle.$$

It is also extended for high dimensional rhotrices by Sani (2007). A generalized algorithm of heart oriented multiplication of rhotrices is discussed by Mohammed et al. (2011). The concept of coupled matrices in rhotrices is introduced by Sani (2008). For n odd, an n-dimensional rhotrix R_n can be written in the form of coupled matrices as follows:

$$R_n = \langle A_d, B_{d-1} \rangle, \text{ where } d = \frac{n+1}{2}.$$

Now, we first define Hankel rhotrix. The aim is to construct MDS rhotrices over finite fields using Hankel rhotrices.

A matrix is called Hankel matrix if every descending diagonal from left to right is constant. The matrix of the form $H = (A_{i,j})_{n \times n}$ where $A_{i,j} = A_{j,i} = a_{i+j-2}$ is called a Hankel matrix and $A_{i,j}$ are the elements from $\mathbb{F}_{2^n}$, see Fazel et al. (2013).

For example, a Hankel matrix of order $n \times n$ can be written as

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & . & \cdots & a_{n-1} \\ a_1 & a_2 & . & . & . & . \\ a_2 & . & . & . & . & \vdots \\ . & . & . & . & . & a_{2n-4} \\ \vdots & . & . & . & a_{2n-4} & a_{2n-3} \\ a_{n-1} & . & \cdots & a_{2n-4} & a_{2n-3} & a_{2n-2} \end{bmatrix}.$$

If the $(i,j)^{th}$ element of A is denoted $A_{i,j}$, then we have

$$A_{i,j} = A_{j,i} = a_{i+j-2}.$$

Let $a_0, a_1,\ldots,a_{n-1}$ denote n real numbers and let $d = \frac{n+1}{2}$, n is odd positive integer. The Hankel rhotrix is denoted by

$$H_n = \text{H}((a_0, a_1,\ldots,a_d,\ldots,a_{2d-2}), (a_1, a_2,\ldots,a_d,\ldots,a_{2d-3}))$$

and is defined as

$$H_n = \left\langle \begin{array}{c} a_0 \\ a_1 \quad a_1 \quad a_1 \\ a_2 \quad a_2 \quad a_2 \quad a_2 \quad . \\ . \quad . \quad a_3 \quad a_3 \quad . \quad . \quad . \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{(d-1)} \quad a_{(d-1)} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad a_{(d-1)} \quad a_{(d-1)} \\ a_d \quad a_d \quad . \quad . \quad . \quad . \quad . \quad a_d \quad a_d \\ . \quad . \quad . \quad . \quad . \quad . \\ . \quad . \quad . \quad . \quad . \\ a_{(2d-3)} \quad a_{(2d-3)} \quad a_{(2d-3)} \\ a_{(2d-2)} \end{array} \right\rangle. \qquad (2.0.1)$$

Note that, all the elements of first row and last column in H_n are distinct and the horizontal diagonal elements are same. Also, $H_n = < A_{\frac{n+1}{2}}, B_{\frac{n-1}{2}} >$, where the matrices $A_{\frac{n+1}{2}}$ *and* $B_{\frac{n-1}{2}}$ are called coupled matrices.

For example, the coupled matrices of a 5-dimensional Hankel rhotrix $H_5 = \langle A_3, B_2 \rangle$ are given by

$$A_3 = \begin{bmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_3 \end{bmatrix}.$$

The MDS matrices and rhotrices are defined in literature, see Gupta and Ray (2013), Sharma and Kumar (2013), we respectively have

(1) Let $\mathbb{F}$ be a finite field and p, q be positive integers. Let $x \rightarrow M \times x$ be a mapping from $\mathbb{F}^p$ to $\mathbb{F}^q$ defined by the $q \times p$ matrix M. We say that it is an MDS matrix if the set of all pairs $(x, M \times x)$ is an MDS code, that is a linear code of dimension p, length $p+q$ and minimum

distance $q+1$. In other form, we can say that a square matrix A is an MDS matrix if and only if every square sub-matrices of A are non-singular. This implies that all the entries of an MDS matrix must be non-zero.

(2) An m$\times n$ rhotrix over a finite field K is an MDS rhotrix if it is the linear transformation $f(x) = Ax$ from K^n to K^m such that no two different $m + n$ - tuples of the form $(x, f(x))$ coincide. The necessary and sufficient condition of a rhotrix to be an MDS rhotrix is that all its sub-rhotrices are non-singular.
We need the following lemmas, which are defined by Sharma and Kumar (2013) to construct the MDS rhotrices**.**

Lemma 2.1.

Any rhotrix R_5 over GF(2^n) with all non-zero entries is an MDS rhotrix iff its coupled matrices M_1 of order 3 and M_2 of order 2 are non-singular and all their entries are non-zero.

Lemma 2.2.

Any rhotrix R_{2n+1} over GF(2^n) with all non-zero entries is an MDS rhotrix iff its coupled matrices M_1 of order $n+1$ and M_2 of order n are non-singular and all their entries are non-zero.
In the following section, we construct maximum distance separable Hankel rhotrices by using elements of finite field GF (2^n). In the further discussion, we denote the $(i, j)^{\text{th}}$ element of the rhotrix by $A[i][j]$ and $H_n =< A, B >$.

3. MDS Rhotrices from Hankel Rhotrices over $\mathbb{F}_{2^n}$

Here, we construct Maximum Distance Separable rhotrices using five and seven dimensional Hankel rhotrices. We prove that the Hankel rhotrices with the elements from $\mathbb{F}_{2^n}$ of the type $\alpha^{2^i}+1$ and $\alpha^{2^i}+\alpha^i$**,** respectively $0 \leq i \leq 4$ for 5-dimension and $0 \leq i \leq 6$ for 7- dimension, where α is the root of irreducible polynomial of degree n, are Maximum Distance Separable (MDS) Hankel rhotrices.

3.1. MDS Hankel Rhotrices using the elements $\{\alpha^{2^i}+1\}$

In this section, we construct maximum distance separable Hankel rhotrices of dimension 5 and 7 using the elements from $\mathbb{F}_{2^n}$ of the type $\{\alpha^{2^i}+1\}$ for 5- dimension $(0 \leq i \leq 4)$, for 7- dimension $(0 \leq i \leq 6)$, where α is the root of irreducible polynomial of degree n.

Theorem 3.1.1.

Let $H_5 =< A, B >$ be the Hankel rhotrix of dimension 5, and let the coupled matrices A and B be defined over $\mathbb{F}_{2^n}$ as $A = H\left(\alpha^{2^i} + 1\right), B = H\left(\alpha^{2^j} + 1\right)$, $i = 0, 1, 2, 3, 4$ and $j = 1, 2, 3$. Then, A and B form an MDS Hankel rhotrix for $n > 3$.

Proof:

The Hankel rhotrix H_5 formed by the coupled matrices A and B is given by

$$H_5 = \left\langle \begin{array}{ccccc} & & A[1][1] & & \\ & A[2][1] & B[1][1] & A[1][2] & \\ A[3][1] & B[2][1] & A[2][2] & B[1][2] & A[1][3] \\ & A[3][2] & B[2][2] & A[2][3] & \\ & & A[3][3] & & \end{array} \right\rangle. \tag{3.1.1}$$

Since $A = H\left(\alpha^{2^i} + 1\right), i = 0, 1, 2, 3, 4$ and $B = H\left(\alpha^{2^j} + 1\right), j = 1, 2, 3$, we have

$$A = H(\alpha + 1, \alpha^2 + 1, \alpha^4 + 1, \alpha^8 + 1, \alpha^{16} + 1) = \begin{bmatrix} \alpha + 1 & \alpha^2 + 1 & \alpha^4 + 1 \\ \alpha^2 + 1 & \alpha^4 + 1 & \alpha^8 + 1 \\ \alpha^4 + 1 & \alpha^8 + 1 & \alpha^{16} + 1 \end{bmatrix}$$

and $B = H(\alpha^2 + 1, \alpha^4 + 1, \alpha^8 + 1) = \begin{bmatrix} \alpha^2 + 1 & \alpha^4 + 1 \\ \alpha^4 + 1 & \alpha^8 + 1 \end{bmatrix}$.

We find that determinant $(A) = \alpha^{21} + \alpha^{16} + \alpha^{12} + \alpha^8 + \alpha^5 + \alpha^4$ and determinant $(B) = \alpha^{10} + \alpha^2$.

For $n = 4$, we choose α to be the root of irreducible polynomial $x^4 + x + 1 = 0$, and therefore,

$$A = \begin{bmatrix} \alpha + 1 & \alpha^2 + 1 & \alpha \\ \alpha^2 + 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & \alpha + 1 \end{bmatrix}.$$

Since all the elements of A are non-zero, determinant (A) = 1 ≠ 0 and all the sub-matrices of A are non-singular, we see that A is an MDS matrix.

Similarly,

$$B = \begin{bmatrix} \alpha^2 + 1 & \alpha \\ \alpha & \alpha^2 \end{bmatrix}$$

is also MDS matrix. Thus, H_5 in (3.1.1) takes the form

$$H_5 = \left\langle \begin{array}{ccccc} & & \alpha+1 & & \\ & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \\ \alpha & \alpha & \alpha & \alpha & \alpha \\ & \alpha^2 & \alpha^2 & \alpha^2 & \\ & & \alpha+1 & & \end{array} \right\rangle. \quad (3.1.2)$$

It now follows from Lemma 2.2 and Definition of H_n as given in (2.0.1) that H_5 is Maximum Distance Separable (MDS) Hankel Rhotrix for $n = 4$.

On using similar arguments, we can prove the results for $n = 5, 6, 7$ and 8, we respectively choose α to be the root of the irreducible polynomial $x^5 + x^2 + 1 = 0, x^6 + x + 1 = 0, x^7 + x + 1 = 0$ and $x^8 + x^7 + x^6 + x + 1 = 0$. Further, for $n = 5, 6, 7$ and 8, we respectively get the following rhotrices

$$H_5 = \left\langle \begin{array}{ccccc} & & \alpha+1 & & \\ & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \\ \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 \\ & \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \\ & & \alpha^4+\alpha^3+\alpha & & \end{array} \right\rangle,$$

$$H_5 = \left\langle \begin{array}{ccccc} & & \alpha+1 & & \\ & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \\ \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 \\ & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \\ & & \alpha^4+\alpha & & \end{array} \right\rangle,$$

$$H_5 = \left\langle \begin{array}{ccccc} & & \alpha+1 & & \\ & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \\ \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 \\ & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \\ & & \alpha^4+\alpha^2+1 & & \end{array} \right\rangle,$$

$$H_5 = \left\langle \begin{array}{ccccc} & & \alpha+1 & & \\ & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \\ \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 \\ & \alpha^7+\alpha^6+\alpha & \alpha^7+\alpha^6+\alpha & \alpha^7+\alpha^6+\alpha & \\ & & \alpha^4+\alpha^3+\alpha^2+\alpha & & \end{array} \right\rangle.$$

Similarly, A and B form MDS Hankel rhotrices for $n > 8$ and hence for $n > 3$.

Theorem 3.1.2.

Let $H_7 =< A, B >$ be the Hankel rhotrix of dimension 7, whose coupled matrices are A and B defined over $\mathbb{F}_{2^n}$ as $A = H\left(\alpha^{2^i} + 1\right), B = H\left(\alpha^{2^j} + 1\right), i = 0,1,2,3,4,5,6$ and $j = 1,2,3,4,5$. Then, A and B form an MDS Hankel rhotrix for $n > 3$.

Proof:

The Hankel rhotrix H_7 formed by the coupled matrices A and B is given by

$$H_7 = \left\langle \begin{array}{ccccccc} & & & A[1][1] & & & \\ & & A[2][1] & B[1][1] & A[1][2] & & \\ & A[3][1] & B[2][1] & A[2][2] & B[1][2] & A[1][3] & \\ A[4][1] & B[3][1] & A[3][2] & B[2][2] & A[2][3] & B[1][3] & A[1][4] \\ & A[4][2] & B[3][2] & A[3][3] & B[2][3] & A[2][4] & \\ & & A[4][3] & B[3][3] & A[3][4] & & \\ & & & A[4][4] & & & \end{array} \right\rangle. \quad (3.1.3)$$

Since

$$A = H\left(\alpha^{2^i} + 1\right),\ i = 0,1,2,3,4,5,6 \text{ and } B = H\left(\alpha^{2^j} + 1\right),\ j = 1,2,3,4,5,$$

therefore,

$$A = H(\alpha + 1, \alpha^2 + 1, \alpha^4 + 1, \alpha^8 + 1, \alpha^{16} + 1, \alpha^{32} + 1, \alpha^{64} + 1) \text{ and}$$
$$B = H(\alpha^2 + 1, \alpha^4 + 1, \alpha^8 + 1, \alpha^{16} + 1, \alpha^{32} + 1)$$

are given by

$$A = \begin{bmatrix} \alpha+1 & \alpha^2+1 & \alpha^4+1 & \alpha^8+1 \\ \alpha^2+1 & \alpha^4+1 & \alpha^8+1 & \alpha^{16}+1 \\ \alpha^4+1 & \alpha^8+1 & \alpha^{16}+1 & \alpha^{32}+1 \\ \alpha^8+1 & \alpha^{16}+1 & \alpha^{32}+1 & \alpha^{64}+1 \end{bmatrix}$$

and

$$B = \begin{bmatrix} \alpha^2+1 & \alpha^4+1 & \alpha^8+1 \\ \alpha^4+1 & \alpha^8+1 & \alpha^{16}+1 \\ \alpha^8+1 & \alpha^{16}+1 & \alpha^{32}+1 \end{bmatrix}.$$

Now, determinant $(A) = \alpha^{85} + \alpha^{69} + \alpha^{81} + \alpha^{49} + \alpha^{84} + \alpha^{76} + \alpha^{40} + \alpha^{32}$ and determinant $(B) = \alpha^{42} + \alpha^{32} + \alpha^{24} + \alpha^{16} + \alpha^{10} + \alpha^{8}$.

For $n = 4$, we choose α to be the root of irreducible polynomial $x^4 + x + 1 = 0$, and therefore,

$$A = \begin{bmatrix} \alpha+1 & \alpha^2+1 & \alpha & \alpha^2 \\ \alpha^2+1 & \alpha & \alpha^2 & \alpha+1 \\ \alpha & \alpha^2 & \alpha+1 & \alpha^2+1 \\ \alpha^2 & \alpha+1 & \alpha^2+1 & \alpha \end{bmatrix}.$$

Since all the elements of A are non-zero, determinant (A) = 1 ≠ 0 and all the sub-matrices of A are non-singular, we see that A is an MDS rhotrix. Similarly,

$$B = \begin{bmatrix} \alpha^2+1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & \alpha+1 \\ \alpha^2 & \alpha+1 & \alpha^2+1 \end{bmatrix}$$

is an MDS rhotrix. Thus, H_7 in (3.1.3) takes the form

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & & \\ & \alpha & \alpha & \alpha & \alpha & \alpha & \\ \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ & \alpha+1 & \alpha+1 & \alpha+1 & \alpha+1 & \alpha+1 & \\ & & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & & \\ & & & \alpha & & & \end{array} \right\rangle. \tag{3.1.4}$$

It now follows from Lemma 2.2 and Definition of H_n as given in (2.0.1) that H_7 is Maximum Distance Separable (MDS) Hankel Rhotrix for $n = 4$.

On using similar arguments, we can prove the results for $n = 5, 6, 7$ and 8, we respectively choose α to be the root of the irreducible polynomial $x^5 + x^2 + 1 = 0, x^6 + x + 1 = 0, x^7 + x + 1 = 0$ and $x^8 + x^7 + x^6 + x + 1 = 0$. Further, for $n = 5, 6, 7$ and 8, we respectively get the following rhotrices

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & & \\ & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \\ \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \alpha^3+\alpha^2 \\ & \alpha^4+\alpha^3+\alpha & \alpha^4+\alpha^3+\alpha & \alpha^4+\alpha^3+\alpha & \alpha^4+\alpha^3+\alpha & \alpha^4+\alpha^3+\alpha & \\ & & \alpha+1 & \alpha+1 & \alpha+1 & & \\ & & & \alpha^2+1 & & & \end{array} \right\rangle,$$

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & & \\ & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \\ \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 \\ & \alpha^4+\alpha & \alpha^4+\alpha & \alpha^4+\alpha & \alpha^4+\alpha & \alpha^4+\alpha & \\ & & \alpha^3 & \alpha^3 & \alpha^3 & & \\ & & & \alpha+1 & & & \end{array} \right\rangle,$$

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & & \\ & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 & \\ \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 \\ & \alpha^4+\alpha^2+1 & \alpha^4+\alpha^2+1 & \alpha^4+\alpha^2+1 & \alpha^4+\alpha^2+1 & \alpha^4+\alpha^2+1 & \\ & & \alpha^4+\alpha^2+\alpha+1 & \alpha^4+\alpha^2+\alpha+1 & \alpha^4+\alpha^2+\alpha+1 & & \\ & & & \alpha^4+\alpha+1 & & & \end{array} \right\rangle,$$

$$H_7 = \left\langle \begin{array}{cccc} & & & \alpha+1 \\ & & \alpha^2+1 & \alpha^2+1 \\ & \alpha^4+1 & \alpha^4+1 & \alpha^4+1 \\ \alpha^7+\alpha^6+\alpha & \alpha^7+\alpha^6+\alpha & \alpha^7+\alpha^6+\alpha & \alpha^7+\alpha^6+\alpha \\ & \alpha^4+\alpha^3+\alpha^2+\alpha & \alpha^4+\alpha^3+\alpha^2+\alpha & \alpha^4+\alpha^3+\alpha^2+\alpha \\ & & \alpha^7+\alpha^4+\alpha^2+\alpha+1 & \alpha^7+\alpha^4+\alpha^2+\alpha+1 \\ & & & \alpha^7+\alpha^5+1 \end{array} \right.$$

$$\left.\begin{array}{ccc} \alpha^2+1 & & \\ \alpha^4+1 & \alpha^4+1 & \\ \alpha^7+\alpha^6+\alpha & \alpha^7+\alpha^6+\alpha & \alpha^7+\alpha^6+\alpha \\ \alpha^4+\alpha^3+\alpha^2+\alpha & \alpha^4+\alpha^3+\alpha^2+\alpha & \\ \alpha^7+\alpha^4+\alpha^2+\alpha+1 & & \end{array}\right\rangle.$$

Similarly, A and B form MDS Hankel rhotrices for $n > 8$ and hence for $n > 3$.

3.2. MDS Hankel Rhotrices using the elements $\{\alpha^{2^i} + \alpha^i\}$

In this section, we construct maximum distance separable Hankel rhotrices of dimension 5 and 7 using the elements from $\mathbb{F}_{2^n}$ of the type $\{\alpha^{2^i} + \alpha^i\}$ for 5-dimension $(0 \le i \le 4)$, for 7-dimension $(0 \le i \le 6)$, where α is the root of irreducible polynomial of degree n.

Theorem 3.2.1.

Let $H_5 =< A, B >$ be the Hankel rhotrix of dimension 5, whose coupled matrices are A and B defined over $\mathbb{F}_{2^n}$ which are given by $A = H\left(\alpha^{2^i} + \alpha^i\right), B = H\left(\alpha^{2^j} + \alpha^j\right),\ i = 0,1,2,3,4$ and $j = 1,2,3$. Then, A and B form an MDS Hankel rhotrix for $n > 3$.

Proof:

Since $A = H\left(\alpha^{2^i} + \alpha^i\right),\ i = 0,1,2,3,4$ and $B = H\left(\alpha^{2^j} + \alpha^j\right),\ j = 1,2,3$. Therefore, $A = H(\alpha+1, \alpha^2+\alpha, \alpha^4+\alpha^2, \alpha^8+\alpha^3, \alpha^{16}+\alpha^4)$ and $B = H(\alpha^2+\alpha, \alpha^4+\alpha^2, \alpha^8+\alpha^3)$ are given by

$$A = \begin{bmatrix} \alpha+1 & \alpha^2+\alpha & \alpha^4+\alpha^2 \\ \alpha^2+\alpha & \alpha^4+\alpha^2 & \alpha^8+\alpha^3 \\ \alpha^4+\alpha^2 & \alpha^8+\alpha^3 & \alpha^{16}+\alpha^4 \end{bmatrix} \text{and } B = \begin{bmatrix} \alpha^2+\alpha & \alpha^4+\alpha^2 \\ \alpha^4+\alpha^2 & \alpha^8+\alpha^3 \end{bmatrix}.$$

Now, determinant $(A) = \alpha^{21}+\alpha^{19}+\alpha^{17}+\alpha^{16}+\alpha^{12}+\alpha^{10}+\alpha^9+\alpha^8$ and determinant $(B) = \alpha^{10}+\alpha^9+\alpha^8+\alpha^5$.

For $n = 4$, we choose α to be the root of irreducible polynomial $x^4+x+1=0$, and therefore,

$$A = \begin{bmatrix} \alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha+1 \\ \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 \\ \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 & 1 \end{bmatrix}.$$

Since all the elements of A are non-zero, determinant (A) = 1 $\neq 0$ and all the sub-matrices of A are non-singular, we see that A is an MDS rhotrix. Similarly,

$$B = \begin{bmatrix} \alpha^2 + \alpha & \alpha^2 + \alpha + 1 \\ \alpha^2 + \alpha + 1 & \alpha^3 + \alpha^2 + 1 \end{bmatrix}$$

is an MDS rhotrix. Thus, H_5 in (3.1.1) will have the form

$$H_5 = \left\langle \begin{array}{ccccccccc} & & & & \alpha+1 & & & & \\ & & \alpha^2+\alpha & & \alpha^2+\alpha & & \alpha^2+\alpha & & \\ \alpha^2+\alpha+1 & & \alpha^2+\alpha+1 & & \alpha^2+\alpha+1 & & \alpha^2+\alpha+1 & & \alpha^2+\alpha+1 \\ & & \alpha^3+\alpha^2+1 & & \alpha^3+\alpha^2+1 & & \alpha^3+\alpha^2+1 & & \\ & & & & 1 & & & & \end{array} \right\rangle. \qquad (3.2.1)$$

It now follows from Lemma 2.2 and Definition of H_n as given in (2.0.1) that H_5 is Maximum Distance Separable (MDS) Hankel Rhotrix for $n = 4$.

On using similar arguments, we can prove the results for $n = 5, 6, 7$ and 8, we respectively choose α to be the root of the irreducible polynomial $x^5 + x^2 + 1 = 0$, $x^6 + x + 1 = 0$, $x^7 + x + 1 = 0$ and $x^8 + x^7 + x^6 + x + 1 = 0$. Further, for $n = 5, 6, 7$ and 8, we respectively get the following rhotrices

$$H_5 = \left\langle \begin{array}{ccccccccc} & & & & \alpha+1 & & & & \\ & & \alpha^2+\alpha & & \alpha^2+\alpha & & \alpha^2+\alpha & & \\ \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 \\ & & \alpha^2+1 & & \alpha^2+1 & & \alpha^2+1 & & \\ & & & & \alpha^3+\alpha+1 & & & & \end{array} \right\rangle,$$

$$H_5 = \left\langle \begin{array}{ccccccccc} & & & & \alpha+1 & & & & \\ & & \alpha^2+\alpha & & \alpha^2+\alpha & & \alpha^2+\alpha & & \\ \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 & & \alpha^4+\alpha^2 \\ & & \alpha^2 & & \alpha^2 & & \alpha^2 & & \\ & & & & \alpha+1 & & & & \end{array} \right\rangle,$$

$$H_5 = \left\langle \begin{array}{ccccc} & & \alpha+1 & & \\ & \alpha^2+\alpha & \alpha^2+\alpha & \alpha^2+\alpha & \\ \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 \\ & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha & \\ & & \alpha^2 & & \end{array} \right\rangle,$$

$$H_5 = \left\langle \begin{array}{ccccc} & & \alpha+1 & & \\ & \alpha^2+\alpha & \alpha^2+\alpha & \alpha^2+\alpha & \\ \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 \\ & \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \\ & & \alpha^3+\alpha^2+\alpha+1 & & \end{array} \right\rangle.$$

Similarly, A and B form MDS Hankel rhotrices for $n > 8$ and hence for $n > 3$.

Theorem 3.2.2.

Let $H_7 = < A, B >$ be the Hankel rhotrix of dimension 7, whose coupled matrices are A and B defined over $\mathbb{F}_{2^n}$ as $A = H\left(\alpha^{2^i} + \alpha^i\right), B = H\left(\alpha^{2^j} + \alpha^j\right), i = 0,1,2,3,4,5,6$ and $j = 1,2,3,4,5$. Then, A and B form an MDS Hankel rhotrix for $n > 3$.

Proof:

Since

$$A = H\left(\alpha^{2^i} + \alpha^i\right),\ \ i = 0,1,2,3,4,5,6 \text{ and } B = H\left(\alpha^{2^j} + \alpha^j\right),\ \ i = 1,2,3,4,5,$$

therefore,

$$A = H(\alpha+1, \alpha^2+\alpha, \alpha^4+\alpha^2, \alpha^8+\alpha^3, \alpha^{16}+\alpha^4, \alpha^{32}+\alpha^5, \alpha^{64}+\alpha^6) \text{ and}$$
$$B = H(\alpha^2+\alpha, \alpha^4+\alpha^2, \alpha^8+\alpha^3, \alpha^{16}+\alpha^4, \alpha^{32}+\alpha^5)$$

are given by

$$A = \begin{bmatrix} \alpha+1 & \alpha^2+\alpha & \alpha^4+\alpha^2 & \alpha^8+\alpha^3 \\ \alpha^2+\alpha & \alpha^4+\alpha^2 & \alpha^8+\alpha^3 & \alpha^{16}+\alpha^4 \\ \alpha^4+\alpha^2 & \alpha^8+\alpha^3 & \alpha^{16}+\alpha^4 & \alpha^{32}+\alpha^5 \\ \alpha^8+\alpha^3 & \alpha^{16}+\alpha^4 & \alpha^{32}+\alpha^5 & \alpha^{64}+\alpha^6 \end{bmatrix}$$

and

$$B = \begin{bmatrix} \alpha^2+\alpha & \alpha^4+\alpha^2 & \alpha^8+\alpha^3 \\ \alpha^4+\alpha^2 & \alpha^8+\alpha^3 & \alpha^{16}+\alpha^4 \\ \alpha^8+\alpha^3 & \alpha^{16}+\alpha^4 & \alpha^{32}+\alpha^5 \end{bmatrix}.$$

Now, determinant $(A) = \alpha^{85}+\alpha^{81}+\alpha^{80}+\alpha^{48}+\alpha^{76}+\alpha^{73}+\alpha^{23}+\alpha^{53}+\alpha^{26}+\alpha^{27}+\alpha^{36}+\alpha^{37}+\alpha^{40}+\alpha^{67}+\alpha^{14}+\alpha^{24}+\alpha^{83}+\alpha^{34}+\alpha^{72}+\alpha^{73}+\alpha^{23}+\alpha^{49}+\alpha^{18}$

and determinant $(B) = \alpha^{42}+\alpha^{37}+\alpha^{41}+\alpha^{15}+\alpha^{34}+\alpha^{33}+\alpha^{40}+\alpha^{13}+\alpha^{24}+\alpha^{19}$.

For $n=4$, we choose α to be the root of irreducible polynomial $x^4+x+1=0$, and therefore,

$$A = \begin{bmatrix} \alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 \\ \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 & 1 \\ \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 & 1 & \alpha \\ \alpha^3+\alpha^2+1 & 1 & \alpha & \alpha^3+\alpha^2+\alpha+1 \end{bmatrix}.$$

Since all the elements of A are non-zero, determinant (A) = 1 $\neq 0$ and all the sub-matrices of A are non-singular, we see that A is an MDS rhotrix. Similarly,

$$B = \begin{bmatrix} \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 \\ \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 & 1 \\ \alpha^3+\alpha^2+1 & 1 & \alpha \end{bmatrix}$$

is an MDS rhotrix. Thus, H_7 in (3.1.3) takes the form

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+\alpha & \alpha^2+\alpha & \alpha^2+\alpha & & \\ & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \\ \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+1 \\ & 1 & 1 & 1 & 1 & 1 & \\ & & \alpha & \alpha & \alpha & & \\ & & & \alpha^3+\alpha^2+\alpha+1 & & & \end{array} \right\rangle. \tag{3.2.2}$$

It now follows from Lemma 2.2 and Definition of H_n as given in (2.0.1) that H_7 is Maximum Distance Separable (MDS) Hankel Rhotrix for $n=4$.

On using similar arguments, we can prove the results for $n = 5, 6, 7$ and 8, we respectively choose α to be the root of the irreducible polynomial $x^5 + x^2 + 1 = 0$, $x^6 + x + 1 = 0$, $x^7 + x + 1 = 0$ and $x^8 + x^7 + x^6 + x + 1 = 0$. Further, for $n = 5, 6, 7$ and 8, we respectively get the following rhotrices

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+\alpha & \alpha^2+\alpha & \alpha^2+\alpha & & \\ & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \\ \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 & \alpha^2+1 \\ & \alpha^3+\alpha+1 & \alpha^3+\alpha+1 & \alpha^3+\alpha+1 & \alpha^3+\alpha+1 & \alpha^3+\alpha+1 & \\ & & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & & \\ & & & \alpha^3+\alpha^2+\alpha & & & \end{array} \right\rangle,$$

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+\alpha & \alpha^2+\alpha & \alpha^2+\alpha & & \\ & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \\ \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ & \alpha+1 & \alpha+1 & \alpha+1 & \alpha+1 & \alpha+1 & \\ & & \alpha^5+\alpha^3+1 & \alpha^5+\alpha^3+1 & \alpha^5+\alpha^3+1 & & \\ & & & 1 & & & \end{array} \right\rangle,$$

$$H_7 = \left\langle \begin{array}{ccccccc} & & & \alpha+1 & & & \\ & & \alpha^2+\alpha & \alpha^2+\alpha & \alpha^2+\alpha & & \\ & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \\ \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha^2+\alpha \\ & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \\ & & \alpha^5+\alpha^4+\alpha^2+\alpha & \alpha^5+\alpha^4+\alpha^2+\alpha & \alpha^5+\alpha^4+\alpha^2+\alpha & & \\ & & & \alpha^6+\alpha^4+\alpha & & & \end{array} \right\rangle,$$

$$H_7 = \left\langle \begin{array}{cccc} & & & \alpha+1 \\ & & \alpha^2+\alpha & \alpha^2+\alpha \\ & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \alpha^4+\alpha^2 \\ \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \alpha^7+\alpha^6+\alpha^3+\alpha+1 \\ & \alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^2+\alpha+1 \\ & & \alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha & \alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha \\ & & & \alpha^7+\alpha^6+\alpha^5 \end{array} \right.$$

$$\begin{array}{ccc} \alpha^2+\alpha & & \\ \alpha^4+\alpha^2 & \alpha^4+\alpha^2 & \\ \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \alpha^7+\alpha^6+\alpha^3+\alpha+1 & \alpha^7+\alpha^6+\alpha^3+\alpha+1 \\ \alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^2+\alpha+1 & \\ \alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha & & \end{array} \Bigg\rangle.$$

Similarly, A and B form MDS Hankel rhotrices for $n > 8$ and hence for $n > 3$.

4. Conclusion

In the present paper, we defined Hankel rhotrix. Further, we constructed the maximum distance separable (MDS) Hankel rhotrices of the dimension 5 and 7 over the finite fields $\mathbb{F}_{2^n}$ by taking the elements of the type $\alpha^{2^i}+1$ and $\alpha^{2^i}+\alpha^i$, respectively $0 \le i \le 4$ for 5 dimension and $0 \le i \le 6$ for 7 dimension, where α is the root of irreducible polynomial of degree n.

Acknowledgements

We thank the Editor-in-Chief Professor Aliakbar Montazer Haghighi and the anonymous referee for their valuable suggestions for the improvement of this paper. Also, first author thankfully acknowledge the support of UGC-SAP and second author is grateful to the UGC for granting Rajeev Gandhi National Fellowship (RGNF).

REFERENCES

Absalom, E. E., Sani, B. and Sahalu, J. B. (2011). The concept of heart-oriented rhotrix multiplication, Global J. Sci. Fro. Research, Vol. 11, No. 2, pp.35-42.

Ajibade, A. O. (2003). The concept of rhotrices in mathematical enrichment, Int. J. Math. Educ. Sci. Tech., Vol. 34, No. 2, pp.175-179.

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

Aminu, A. (2009). On the linear system over rhotrices, Notes on Number Theory and Discrete Mathematics, Vol. 15, pp.7-12.

Aminu, A. (2012). A note on the rhotrix system of equation, Journal of the Nigerian association of Mathematical Physics, Vol. 21, pp.289-296.

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., Vol. 34,
No.3, pp.946–977.

Gupta, K. C., and Ray, I. G. (2013). On constructions of MDS matrices from companion matrices

For lightweight cryptography, Cryptography Security Engineering and Intelligence Informatics, Lecture Notes in Computer Science, 8128, pp.29-43.

Mohammed, A. (2011). Theoretical development and applications of rhotrices, Ph. D. Thesis, Ahmadu Bello University, Zaria.

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, Vol. 2, pp.46-49.

Nakahara, J. and Abrahao, E. (2009). A new involutory MDS matrix for the AES, In: International Journal of Network Security, Vol. 9, pp.109-116.

Sajadieh, M., Dakhilian, M., Mala, H. and Omoomi, B. (2012). On construction of involutry MDS matrices from Vandermonde matrices, Des. Codes and Cry. Vol. 64, pp. 287-308.

Sani, B. (2004). An alternative method for multiplication of rhotrices, Int. J. Math. Educ. Sci. Tech., Vol. 35, No. 5, pp.777-781.

Sani, B. (2007). The row-column multiplication for high dimensional rhotrices, Int. J. Math. Educ. Sci. Technol, Vol. 38, pp.657-662.

Sani, B. (2008). Conversion of a rhotrix to a coupled matrix, Int. J. Math. Educ. Sci. Technol., Vol. 39, pp.244-249.

Sarkar, S. and Habeeb S. (2016). Light weight diffusion layer: Importance of Toeplitz matrices, *IACR* Trans. Symmetric Cryptol., 2016, No. 1, pp.95–113.

Sharma, P. L. and Kanwar, R. K. (2011). A note on relationship between invertible rhotrices and associated invertible matrices, Bulletin of Pure and Applied Sciences, Vol. 30E (Math & Stat.), No. 2, pp.333-339.

Sharma, P. L. and Kanwar, R. K. (2012a). Adjoint of a rhotrix and its basic properties, International J. of Mathematical Sciences, Vol. 11, No.3-4, pp.337-343.

Sharma, P. L. and Kanwar, R.K. (2012b). On inner product space and bilinear forms over rhotrices, Bulletin of Pure and Applied Sciences, Vol. 31E, No. 1, pp.109-118.

Sharma, P. L. and Kanwar, R. K. (2012c). The Cayley-Hamilton theorem for rhotrices, International Journal of Mathematics and Analysis, Vol. 4, No. 1, pp.171-178.

Sharma, P. L. and Kanwar, R.K. (2013). On involutory and Pascal rhotrices, International J. of Math. Sci. & Engg. Appls. *(IJMSEA)*, Vol. 7, No.4, pp.133-146.

Sharma P. L. and Kumar S. (2013). On construction of MDS rhotrices from companion rhotrices over finite field, International Journal of Mathematical Sciences, Vol.12, No. 3-4, pp.271-286.

Sharma, P. L. and Kumar, S. (2014a). Some applications of Hadamard rhotrices to design balanced incomplete block, International J. of Math. Sci. & Engg. Appls. (IJMSEA), Vol. 8, No. 2, pp.389-406.

Sharma, P. L. and Kumar, S. (2014b). Balanced incomplete block design (BIBD) using Hadamard rhotrices, International J. Technology, Vol. 4, No. 1, pp.62-66.

Sharma, P. L. and Kumar, S. (2014c). On a special type of Vandermonde rhotrix and its decompositions, Recent Trends in Algebra and Mechanics, Indo-American Books Publisher, New Delhi, pp. 33-40.

Sharma, P. L., Kumar, S. and Rehan, M. (2013). On Vandermonde and MDS rhotrices over GF(2^q), International Journal of Mathematics and Analysis, Vol. 5, No. 2, pp.143-160.

Sharma, P. L., Kumar, S. and Rehan, M. (2014). On construction of Hadamard codes using Hadmard rhotrices, International Journal of Theoretical & Applied Sciences, Vol. 6, No. 1, pp.102-111.

Sharma, P. L., Gupta, S. (2017). Constructions of Maximum Distance Separable Toeplitz Rhotrices over Finite Fields, J. of Combinatorics, Information & System Sciences, Vol. 42, No. 1-4, pp.89-110.

Sharma, P. L., Gupta, S. and Dhiman, N. (2017a). Construction of maximum distance separable rhotrices using Cauchy rhotrices over finite fields, International Journal of Computer Application, Vol. 168, No. 9, pp. 8-17.

Sharma, P. L., Gupta, S. and Dhiman, N. (2017b). Sylvester rhotrices and their properties over finite field, Bulletin of Pure and Applied Sciences, Vol. 36E, No. 1, pp.70-80.

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, Vol. 3, No. 2, pp.25-43.

Sharma, P. L., Gupta, S. and Rehan, M. (2017). On circulant like rhotrices over finite fields, Applications and Applied Mathematics: An International Journal (AAM), Vol. 12, No. 1, pp. 509-520.

Tudunkaya, S. M. (2013). Rhotrix polynomial and polynomial rhotrix, Pure and Applied mathematics Journal, Vol. 2, pp.38-41.

Tudunkaya, S.M. and Makanjuola, S.O. (2010). Rhotrices and the construction of finite fields, Bulletin of Pure and Applied Sciences, Vol. 29E, No. 2, pp.225-229.