Construction of Maximum Distance Separable Rhotrices using Cauchy Rhotrices over Finite Fields

P. L. Sharma
Department of Mathematics
Himachal Pradesh University,
Shimla 171005

Shalini Gupta
Bahra University, Solan, H. P.,
India

Neetu Dhiman
Department of Mathematics
Himachal Pradesh University,
Shimla 171005

ABSTRACT
Maximum distance separable (MDS) matrices are important in cryptography and particularly used in block ciphers due to their properties of diffusion. Rhotrices are represented by the coupled matrices. Therefore, maximum distance separable rhotrices are of much interest in the context of cryptography. In this paper, we define Cauchy rhotrix and then use it to construct MDS rhotrices over finite fields.

Keywords
Cauchy rhotrix, Finite field, Maximum distance separable rhotrix, Circulant rhotrix, Vandermonde rhotrix.

1. INTRODUCTION
Ajibade [1] defined a 3×3–dimensional rhotrix, which is, in some way, between 2×2–dimensional and 3×3–dimensional matrices as

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

where a, b, c, d, e are real numbers and $h(R_3) = c$ is called the heart of rhotrix R_3. He also defined the operations of addition and scalar multiplication as given below:

Let $Q_3 = \left\langle \begin{array}{ccc} & f & \\ g & h & j \\ & k & \end{array} \right\rangle$, be another 3-dimensional rhotrix, then the addition of two rhotrices is defined as

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

$$= \left\langle \begin{array}{ccc} & a+f & \\ b+g & c+h & d+j \\ & e+k & \end{array} \right\rangle,$$

and for any real number α, the scalar multiplication of a rhotrix R_3 is defined as

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

Two types of multiplication of rhotrices are discussed in the literature of rhotrices, namely, heart oriented multiplication and row-column multiplication. Ajibade discussed the heart oriented multiplication of 3-dimensional rhotrices as given below:

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

Further, it is algorithmatized for computing machines by Mohammed et al. [2]. The extended heart oriented method for rhotrix multiplication is given by Mohammed [3] and also generalized the heart oriented multiplication of 3-dimensional rhotrices to n-dimensional rhotrices. The row column multiplication of 3-dimensional rhotrices is defined by Sani [4] as follows:

$$R_3 \, o \, Q_3 = \left\langle \begin{array}{ccc} & a & \\ b & c & d \\ & e & \end{array} \right\rangle \left\langle \begin{array}{ccc} & f & \\ g & h & j \\ & k & \end{array} \right\rangle$$

$$= \left\langle \begin{array}{ccc} & af+dg & \\ bf+eg & ch & aj+dk \\ & bj+ek & \end{array} \right\rangle.$$

Sani [5] also discussed the row-column multiplication of high dimension rhotrices as follows:

Consider a n -dimensional rhotrix

$$P_n = \left\langle \begin{array}{ccccccc} & & & a_{11} & & & \\ & & a_{21} & c_{11} & a_{12} & & \\ & a_{31} & c_{21} & a_{22} & c_{12} & a_{13} & \\ . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{t1} & \cdots & \cdots & \cdots & \cdots & \cdots & a_{1t} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & a_{tt-2} & c_{t-1t-2} & a_{t-1t-1} & c_{t-2t-1} & a_{t-2t} & \\ & & a_{tt-1} & c_{t-1t-1} & a_{t-1t} & & \\ & & & a_{tt} & & & \end{array} \right\rangle,$$

where $t = (n+1)/2$ and denote it as $P_n = \langle a_{ij}, c_{lk} \rangle$ with $i, j = 1, 2, ..., t$ and $l, k = 1, 2, ..., t-1$. Then the multiplication of two rhotrices P_n and Q_n is defined as follows:

$$P_n \; o \; Q_n = \langle a_{i_1 j_1}, c_{l_1 k_1} \rangle o \langle b_{i_2 j_2}, d_{l_2 k_2} \rangle$$
$$= \left\langle \sum_{i_2 j_1 = 1}^{t} \left(a_{i_1 j_1} \, b_{i_2 j_2} \right), \sum_{l_2 k_1 = 1}^{t-1} \left(c_{l_1 k_1} \, d_{l_2 k_2} \right) \right\rangle.$$

Rhotrices over finite fields were discussed by Tudunkaya et al. [6]. Aminu [7, 8] investigated rhotrices over matrix theory and polynomials ring theory. Algebra and analysis of rhotrices is discussed in the literature, see [9, 10, 11]. Adjoint of a rhotrix, inner product spaces, bilinear forms and Caylay-Hamilton theorem are discussed by Sharma and Kanwar [12, 13, 14, 15, 16]. Different constructions of MDS rhotrices from companion matrices and Vandermonde matrices are given by Sharma et al. [17, 18, 19, 20, 21, 22, 23]. Sharma et al. [24] introduced circulant rhotrices in the literature of rhotrices and construct some MDS rhotrices using special type of circulant rhotrices, see [25].

Maximum distance separable (MDS) matrices have diffusion properties that are used in block ciphers and cryptographic hash functions, as discussed in [26, 27]. There are several methods to construct MDS matrices. Sajadieh et al. [28] and Lacan and Flimes [29] used Vandermonde matrices for the construction of MDS matrices. Gupta and Ray construct MDS rhotrices from companion matrices and circulant like matrices , see [30, 31]

Cauchy matrices have applications in coding theory such as in Goppa codes as discussed in [32]. Nakahara and Abraho [33] constructed an involutory MDS matrix of 16- order by using a Cauchy matrix which was used in MDS-AES design.

Definition 1.1. The matrix of the form $A = (a_{ij})_{mn}$ where

$$a_{ij} = \frac{1}{x_i - x_j}, \; x_i - x_j \neq 0, \; 1 \leq i \leq m, \; 1 \leq j \leq n$$

is called a Cauchy matrix and x_i, x_j are the elements from F_{2^n}.

For example, a Cauchy matrix of n-order can be written as

$$A_n = \begin{bmatrix} \frac{1}{x_1 - y_1} & \frac{1}{x_1 - y_2} & \cdots & \frac{1}{x_1 - y_n} \\ \frac{1}{x_2 - y_1} & \frac{1}{x_2 - y_2} & \cdots & \frac{1}{x_2 - y_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{x_n - y_1} & \frac{1}{x_n - y_2} & \cdots & \frac{1}{x_n - y_n} \end{bmatrix}$$

In the present paper we denote the (i,j)th element of ith row and jth column by A[i][j].

Definition 1.2. A 5- dimensional Cauchy rhotrix C_5 is defined as

$$C_5 = \left\langle \begin{array}{ccccc} & & \frac{1}{x_1 - y_1} & & \\ & \frac{1}{x_2 - y_1} & \frac{1}{s_1 - t_1} & \frac{1}{x_1 - y_2} & \\ \frac{1}{x_3 - y_1} & \frac{1}{s_2 - t_1} & \frac{1}{x_2 - y_2} & \frac{1}{s_1 - t_2} & \frac{1}{x_1 - y_3} \\ & \frac{1}{x_3 - y_2} & \frac{1}{s_2 - t_2} & \frac{1}{x_2 - y_3} & \\ & & \frac{1}{x_3 - y_3} & & \end{array} \right\rangle,$$

where $x_i, y_j \, (i, j = 1, 2, 3)$ and $s_l, t_m \, (l, m = 1, 2)$ are elements from a finite field. Two coupled matrices of C_5 are [35]

$$U = \begin{bmatrix} \frac{1}{x_1 - y_1} & \frac{1}{x_1 - y_2} & \frac{1}{x_1 - y_3} \\ \frac{1}{x_2 - y_1} & \frac{1}{x_2 - y_2} & \frac{1}{x_2 - y_3} \\ \frac{1}{x_3 - y_1} & \frac{1}{x_3 - y_2} & \frac{1}{x_3 - y_3} \end{bmatrix} \text{ and}$$

$$V = \begin{bmatrix} \frac{1}{s_1 - t_1} & \frac{1}{s_1 - t_2} \\ \frac{1}{s_2 - t_1} & \frac{1}{s_2 - t_2} \end{bmatrix}.$$

Definition 1.3. Let F be a finite field, and p, q be two positive integers. Let $x \to M \times x$ be a mapping from F^p to 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 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 nonzero.

Definition 1.4. 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 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.

The construction of the MDS rhotrices is discussed by Sharma and Kumar [17]. The following Lemma 1.5 is also discussed in [17].

Lemma 1.5. Any rhotrix R_5 over GF(2^n) with all non zero entries is an MDS rhotrix iff its coupled matrices $M_1 = 3\times 3$ and $M_2 = 2\times 2$ are non-singular and all their entries are non zero.

Now, we construct maximum distance separable rhotrices by using Cauchy rhotrices.

2. MDS RHOTRICES FROM CAUCHY RHOTRICES OVER F_{2^3}

In this section, we constructed some maximum distance separable rhotrices from 5- dimensional Cauchy rhotrices using the elements of finite field F_{2^3}.

Theorem 2.1. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times 3}$ and $B = (b_{lm})_{2\times 2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j}$,

$x_i = y_j^{\,j+1} + y_j + 1$, $i, j = 1,2,3$ and

$s_l = \alpha^{2l} + \alpha^l ; t_m = \alpha^{2^m} + 1; l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^3 + x + 1$ in the extension field of GF$\left(2^3\right)$. Then A and B form MDS rhotrix R_5.

Proof: For given

$$A = (a_{ij})_{3\times 3};\ a_{ij} = \frac{1}{x_i + y_j},\ x_i + y_j \neq 0;$$

$$y_j = \alpha^{2^j},\ x_i = y_j^{\,j+1} + y_j + 1;\ i, j = 1,2,3$$

we have

$$y_1 = \alpha^2,\ y_2 = \alpha^2 + \alpha,\ y_3 = \alpha$$

and

$$x_1 = \alpha + 1,\ x_2 = 0,\ x_3 = \alpha^2 + 1.$$

Therefore,

$$A = \begin{bmatrix} \dfrac{1}{\alpha^2+\alpha+1} & \dfrac{1}{\alpha^2+1} & 1 \\ \dfrac{1}{\alpha^2} & \dfrac{1}{\alpha^2+\alpha} & \dfrac{1}{\alpha} \\ 1 & \dfrac{1}{\alpha+1} & \dfrac{1}{\alpha^2+\alpha+1} \end{bmatrix}. \quad (2.1)$$

Since, α is the root of $x^3 + x + 1 = 0$. Therefore, $\alpha^2 + \alpha + 1 \neq 0$, $\alpha^2 + \alpha \neq 0$, $\alpha^2 + 1 \neq 0$, $\alpha^2 \neq 0$, $\alpha + 1 \neq 0$, $\alpha \neq 0$.

Also, det $A = \dfrac{\alpha^2 + 1}{\alpha^2 + \alpha + 1} \neq 0$. So, A is non-singular.

Also all the sub matrices of A are non-singular. From (2.1), we have

$$A[1][1] = A[3][3] = \frac{1}{\alpha^2 + \alpha + 1} \neq 0,$$

$$A[1][2] = \frac{1}{\alpha^2 + 1} \neq 0,$$

$$A[1][3] = A[3][1] = 1 \neq 0,$$

$$A[2][1] = \frac{1}{\alpha^2} \neq 0,$$

$$A[2][2] = \frac{1}{\alpha^2 + \alpha} \neq 0,$$

$$A[2][3] = \frac{1}{\alpha} \neq 0,$$

$$A[3][2] = \frac{1}{\alpha + 1} \neq 0.$$

This implies that A is MDS matrix.

Similarly, we can prove that

$$B = \begin{bmatrix} \dfrac{1}{\alpha+1} & 1 \\ \dfrac{1}{\alpha^2+\alpha+1} & \dfrac{1}{\alpha^2+1} \end{bmatrix} \quad (2.2)$$

is MDS matrix. From (2.2), we have

$$B[1][1] = \frac{1}{\alpha + 1} \neq 0,$$

$$B[1][2] = 1 \neq 0,$$

$$B[2][1] = \frac{1}{\alpha^2 + \alpha + 1} \neq 0,$$

$$B[2][2] = \frac{1}{\alpha^2 + 1} \neq 0.$$

The rhotrix of the coupled matrices A and B is

$$R_5 = \left\langle \begin{array}{ccccc} & & A[1][1] & & \\ & A[2][1] & B[1][1] & A[1][2] & \\ A[3][1] & B[2][1] & A[2][2] & B[1][2] & A[1][3] \\ & A[3][2] & B[2][2] & A[2][3] & \\ & & A[3][3] & & \end{array} \right\rangle$$

(2.3)

that is,

$$R_5 = \left\langle \begin{array}{ccccc} & & \frac{1}{\alpha^2+\alpha+1} & & \\ & \frac{1}{\alpha^2} & \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} & \\ 1 & \frac{1}{\alpha^2+\alpha+1} & \frac{1}{\alpha^2+\alpha} & 1 & 1 \\ & \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} & \frac{1}{\alpha} & \\ & & \frac{1}{\alpha^2+\alpha+1} & & \end{array} \right\rangle.$$

Therefore, from Lemma 1.5, it is clear that R_5 is maximum distance separable rhotrix (MDSR).

On the similar arguments we can prove the following Theorems 2.2 to 2.4.

Theorem 2.2. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times3}$ and $B = (b_{lm})_{2\times2}$ are defined as $a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and $b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + \alpha^j + 1;\ x_i = y_j^{\ j+1} + \ y_j + 1$, $i, j = 1,2,3$ and $s_l = \alpha^{2^l}\ ;\ t_m = \alpha^m + \alpha + 1; l, m = 1,2,$ where α is the root of irreducible polynomial $p(x) = x^3 + \ x + 1$ in the extension field of GF (2^3). Then A and B form MDS rhotrix R_5.

Theorem 2.3. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times3}$ and $B = (b_{lm})_{2\times2}$ are defined as $a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and $b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + \alpha^j$; a $x_i = y_j^{\ j+1} + 1$, $i, j = 1,2,3$ and $s_l = \alpha^l + 1; t_m = \alpha^{2^m} + \alpha;\ l, m = 1,2,$ where α is the root of irreducible polynomial $p(x) = x^3 + \ x + 1$ in the extension field of GF (2^3). Then A and B form MDS rhotrix R_5.

Theorem 2.4. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times3}$ and $B = (b_{lm})_{2\times2}$ are defined as $a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and $b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + 1;$ $x_i = y_j + 1$, $i, j = 1,2,3$ and $s_l = \alpha^{2l} + \alpha + 1; t_m = \alpha^{2^m} + \alpha;\ l, m = 1,2,$ where α is the root of irreducible polynomial $p(x) = x^3 + \ x + 1$ in the extension field of GF (2^3). Then A and B form MDS rhotrix R_5.

3. MDS RHOTRICES FROM CAUCHY RHOTRICES OVER F_{2^4}

Theorem 3.1. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times3}$ and $B = (b_{lm})_{2\times2}$ are defined as $a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and $b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j}$; $x_i = y_j^{\ j+1} + y_j + 1$, $i, j = 1,2,3$ and $s_l = \alpha^{2l} + \alpha^l\ ; t_m = \alpha^{2^m} + 1; l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^4 + \ x + 1$ in the extension field of GF (2^4). Then A and B form MDS rhotrix R_5.

Proof: For given

$A = (a_{ij})_{3\times3}$; $a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0;\ y_j = \alpha^{2^j}$, $x_i = y_j^{\ j+1} + y_j + 1;\ i, j = 1,2,3,$

we have

$$y_1 = \alpha^2,\ y_2 = \alpha + 1,\ y_3 = \alpha^2 + 1$$

and

$$x_1 = \alpha^2 + \alpha,\ x_2 = \alpha^3 + \alpha^2 + 1,\ x_3 = 0.$$

Therefore,

$$A=\begin{bmatrix} \frac{1}{\alpha} & \frac{1}{\alpha^2+1} & \frac{1}{\alpha+1} \\ \frac{1}{\alpha^3+1} & \frac{1}{\alpha^3+\alpha^2+\alpha} & \frac{1}{\alpha^3} \\ \frac{1}{\alpha^2} & \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} \end{bmatrix}. \quad (3.1)$$

Since, α is the root of $x^4+x+1=0$. Therefore, $\alpha^3+\alpha^2+\alpha\neq 0,\ \alpha^2+1\neq 0,\ \alpha^3+1\neq 0,$ $\alpha^2\neq 0,\ \alpha^3\neq 0,\ \alpha+1\neq 0,\ \alpha\neq 0.$

Also, $\det A=\frac{\alpha+1}{\alpha^3+\alpha+1}\neq 0$. So, A is non-singular.

Also all the sub matrices of A are non-singular. From (3.1), we have

$$A[1][1]=\frac{1}{\alpha}\neq 0,$$

$$A[1][2]=A[3][3]=\frac{1}{\alpha^2+1}\neq 0,$$

$$A[1][3]=A[3][2]=\frac{1}{\alpha+1}\neq 0,$$

$$A[2][1]=\frac{1}{\alpha^3+1}\neq 0,$$

$$A[2][2]=\frac{1}{\alpha^3+\alpha^2+\alpha}\neq 0$$

$$A[2][3]=\frac{1}{\alpha^3}\neq 0,$$

$$A[3][1]=\frac{1}{\alpha^2}\neq 0.$$

Therefore, A is MDS matrix.

Similarly, we can prove that

$$B=\begin{bmatrix} \frac{1}{\alpha+1} & \frac{1}{\alpha^2} \\ \frac{1}{\alpha} & \frac{1}{\alpha^2+1} \end{bmatrix} \quad (3.2)$$

is MDS matrix. From (3.2),we have

$$B[1][1]=\frac{1}{\alpha+1}\neq 0,$$

$$B[1][2]=\frac{1}{\alpha^2}\neq 0,$$

$$B[2][1]=\frac{1}{\alpha}\neq 0,$$

$$B[2][2]=\frac{1}{\alpha^2+1}\neq 0.$$

The rhotrix of the coupled matrices A and B is

$$R_5=\left\langle \begin{array}{ccccc} & & A[1][1] & & \\ & A[2][1] & B[1][1] & A[1][2] & \\ A[3][1] & B[2][1] & A[2][2] & B[1][2] & A[1][3] \\ & A[3][2] & B[2][2] & A[2][3] & \\ & & A[3][3] & & \end{array} \right\rangle, \quad (3.3)$$

that is,

$$R_5=\left\langle \begin{array}{ccccc} & & \frac{1}{\alpha} & & \\ & \frac{1}{\alpha^3+1} & \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} & \\ \frac{1}{\alpha^2} & \frac{1}{\alpha} & \frac{1}{\alpha^3+\alpha^2+\alpha} & \frac{1}{\alpha^2} & \frac{1}{\alpha^3} \\ & \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} & \frac{1}{\alpha^3} & \\ & & \frac{1}{\alpha^2+1} & & \end{array} \right\rangle.$$

Therefore, from Lemma 1.5, it is clear that R_5 is maximum distance separable rhotrix (MDSR).

On the similar arguments we can prove the following theorems.

Theorem 3.2. Let R_5 be a Cauchy rhotrix whose coupled matrices $A=(a_{ij})_{3\times 3}$ and $B=(b_{lm})_{2\times 2}$ are defined as

$a_{ij}=\frac{1}{x_i+y_j},\ x_i+y_j\neq 0$ and

$b_{lm}=\frac{1}{s_l+t_m},\ s_l+t_m\neq 0$. Let

$y_j=\alpha^{2^j}+\alpha^j+1;\ x_i=y_j{}^{j+1}+\ y_j+1,$ $i,j=1,2,3$ and

$s_l=\alpha^{2^l};\ t_m=\alpha^m+\alpha+1; l,m=1,2,$ where α is the root of irreducible polynomial $p(x)=x^4+x+1$ in the extension field of GF$\left(2^4\right)$. Then A and B form MDS rhotrix R_5.

Theorem 3.3. Let R_5 be a Cauchy rhotrix whose coupled matrices $A=(a_{ij})_{3\times 3}$ and $B=(b_{lm})_{2\times 2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + \alpha^j$; a

$x_i = y_j^{\,j+1} + 1$, $i, j = 1,2,3$ and

$s_l = \alpha^l + 1; t_m = \alpha^{2^m} + \alpha; l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^4 + x + 1$ in the extension field of GF(2^4). Then A and B form MDS rhotrix R_5.

Theorem 3.4. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times3}$ and $B = (b_{lm})_{2\times2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + 1$;

$x_i = y_j + 1$, $i, j = 1,2,3$ and

$s_l = \alpha^{2l} + \alpha + 1; t_m = \alpha^{2^m} + \alpha; l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^4 + x + 1$ in the extension field of GF(2^4). Then A and B form MDS rhotrix R_5.

4. MDS RHOTRICES FROM CAUCHY RHOTRICES OVER F_{2^5}

In this section, we have construct some maximum distance separable rhotrices from 5- dimensional Cauchy rhotrices using the elements of finite field F_{2^5}.

Theorem 4.1. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times3}$ and $B = (b_{lm})_{2\times2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j}$,

$x_i = y_j^{\,j+1} + y_j + 1$, $i, j = 1,2,3$ and

$s_l = \alpha^{2l} + \alpha^l; t_m = \alpha^{2^m} + 1; l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^5 + x^2 + 1$ in the extension field of GF(2^5). Then A and B form MDS rhotrix R_5.

Proof: For given

$A = (a_{ij})_{3\times3}$; $a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$;

$y_j = \alpha^{2^j}$, $x_i = y_j^{\,j+1} + y_j + 1$; $i, j = 1,2,3$

we have

$$y_1 = \alpha^2, y_2 = \alpha^4, y_3 = \alpha^3 + \alpha^2 + 1$$

and

$x_1 = \alpha^4 + \alpha^2 + 1$, $x_2 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$, $x_3 = \alpha^3 + \alpha^2 + \alpha$.

Therefore,

$$A = \begin{bmatrix} \dfrac{1}{\alpha^4+1} & \dfrac{1}{\alpha^2+1} & \dfrac{1}{\alpha^4+\alpha^3} \\ \dfrac{1}{\alpha^4+\alpha^3+\alpha+1} & \dfrac{1}{\alpha^4+\alpha^2+\alpha+1} & \dfrac{1}{\alpha^4+\alpha} \\ \dfrac{1}{\alpha^4+\alpha} & \dfrac{1}{\alpha^4+\alpha^3+\alpha^2+\alpha} & \dfrac{1}{\alpha+1} \end{bmatrix}. \tag{4.1}$$

Since, α is the root of $x^5 + x^2 + 1 = 0$. Therefore, $\alpha^4 + \alpha^3 + \alpha^2 + \alpha \neq 0$, $\alpha^4 + \alpha^3 + \alpha + 1 \neq 0$, $\alpha^4 + \alpha^2 + \alpha + 1 \neq 0$, $\alpha^4 + \alpha^3 \neq 0$, $\alpha^4 + \alpha \neq 0$, $\alpha^4 + 1 \neq 0$, $\alpha^2 + 1 \neq 0$ and $\alpha + 1 \neq 0$.

Also, $\det A = \dfrac{\alpha^4}{\alpha^4 + \alpha^3 + a^2} \neq 0$. So, A is non-singular. Also all the sub matrices of A are non-singular. From (4.1), we have

$A[1][1] = \dfrac{1}{\alpha^4 + 1} \neq 0$,

$A[1][2] = \dfrac{1}{\alpha^2 + 1} \neq 0$,

$A[1][3] = A[3][1] = \dfrac{1}{\alpha^4 + \alpha^3} \neq 0$,

$A[2][1] = \dfrac{1}{\alpha^4 + \alpha^3 + \alpha + 1} \neq 0$,

$A[2][2] = \dfrac{1}{\alpha^3 + \alpha^2 + \alpha + 1} \neq 0$,

$$A[2][3] = \frac{1}{\alpha^4 + \alpha} \neq 0,$$

$$A[3][1] = \frac{1}{\alpha^3 + \alpha} \neq 0,$$

$$A[2][2] = \frac{1}{\alpha^3 + \alpha^2 + \alpha + 1} \neq 0,$$

$$A[3][3] = \frac{1}{\alpha + 1} \neq 0.$$

Therefore, A is MDS matrix.

Similarly, we can prove that

$$B = \begin{bmatrix} \frac{1}{\alpha + 1} & \frac{1}{\alpha^4 + \alpha^2 + \alpha + 1} \\ \frac{1}{\alpha^4 + 1} & \frac{1}{\alpha^2 + 1} \end{bmatrix} \quad (4.2)$$

is MDS matrix. From (4.2), we have

$$B[1][1] = \frac{1}{\alpha + 1} \neq 0,$$

$$B[1][2] = \frac{1}{\alpha^4 + \alpha^2 + \alpha + 1} \neq 0,$$

$$B[2][1] = \frac{1}{\alpha^4 + 1} \neq 0,$$

$$B[2][2] = \frac{1}{\alpha^2 + 1} \neq 0.$$

The rhotrix of the coupled matrices A and B is

$$R_5 = \left\langle \begin{array}{ccccc} & & A[1][1] & & \\ & A[2][1] & B[1][1] & A[1][2] & \\ A[3][1] & B[2][1] & A[2][2] & B[1][2] & A[1][3] \\ & A[3][2] & B[2][2] & A[2][3] & \\ & & A[3][3] & & \end{array} \right\rangle. \quad (4.3)$$

Using (4.1) and (4.2) in (4.3), we have

$$R_5 = \left\langle \begin{array}{ccccc} & & \frac{1}{\alpha^4+1} & & \\ & \frac{1}{\alpha^4+\alpha^3+\alpha+1} & \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} & \\ \frac{1}{\alpha^3+\alpha} & \frac{1}{\alpha^4+1} & \frac{1}{\alpha^3+\alpha^2+\alpha+1} & \frac{1}{\alpha^4+\alpha^2+\alpha+1} & \frac{1}{\alpha^4+\alpha^3} \\ & \frac{1}{\alpha^4+\alpha^3+\alpha^2+\alpha} & \frac{1}{\alpha^2+1} & \frac{1}{\alpha^4+\alpha} & \\ & & \frac{1}{\alpha+1} & & \end{array} \right\rangle.$$

Therefore, from Lemma 1.5, it is clear that R_5 is maximum distance separable rhotrix (MDSR).

In the similar ways we can prove the following theorems.

Theorem 4.2. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times 3}$ and $B = (b_{lm})_{2\times 2}$ are defined as

$a_{ij} = \frac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \frac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let

$y_j = \alpha^{2^j} + \alpha^j + 1;\ x_i = y_j{}^{j+1} + \ y_j + 1,$

$i, j = 1, 2, 3$ and

$s_l = \alpha^{2^l};\ t_m = \alpha^m + \alpha + 1; l, m = 1, 2,$ where α is the root of irreducible polynomial $p(x) = x^5 + x^2 + 1$ in the extension field of GF(2^3). Then A and B form MDS rhotrix R_5.

Theorem 4.3. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times 3}$ and $B = (b_{lm})_{2\times 2}$ are defined as

$a_{ij} = \frac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \frac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + \alpha^j$; a

$x_i = y_j{}^{j+1} + 1$, $i, j = 1, 2, 3$ and

$s_l = \alpha^l + 1; t_m = \alpha^{2^m} + \alpha;\ l, m = 1, 2,$ where α is the root of irreducible polynomial $p(x) = x^5 + x^2 + 1$ in the extension field of GF(2^3). Then A and B form MDS rhotrix R_5.

Theorem 4.4. Let R_5 be a Cauchy rhotrix whose coupled matrices $A = (a_{ij})_{3\times 3}$ and $B = (b_{lm})_{2\times 2}$ are defined as

$a_{ij} = \frac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \frac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + 1;$

$x_i = y_j + 1$, $i, j = 1, 2, 3$ and

$s_l = \alpha^{2l} + \alpha + 1; t_m = \alpha^{2^m} + \alpha;\ l, m = 1, 2,$ where α is the root of irreducible polynomial $p(x) = x^5 + x^2 + 1$ in the extension field of GF(2^3). Then A and B form MDS rhotrix R_5.

5. MDS RHOTRICES FROM CAUCHY RHOTRICES OVER F_{2^6}

In this section, we have construct some maximum distance separable rhotrices from 5- dimensional Cauchy rhotrices using the elements of finite field F_{2^6}.

Theorem 5.1. Let R_5 be a Cauchy rhotrix whose coupled matrices $A=\left(a_{ij}\right)_{3\times 3}$ and $B=\left(b_{lm}\right)_{2\times 2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j}$,

$x_i = y_j{}^{j+1} + y_j + 1$, $i, j = 1,2,3$ and

$s_l = \alpha^{2l} + \alpha^l ; t_m = \alpha^{2^m} + 1; l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^6 + x + 1$ in the extension field of GF$\left(2^6\right)$. Then A and B form MDS rhotrix R_5.

Proof: For given

$A=\left(a_{ij}\right)_{3\times 3}$; $a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$; , we have

$$y_j = \alpha^{2^j},\ x_i = y_j{}^{j+1} + y_j + 1;\ i, j = 1,2,3$$

$$y_1 = \alpha^2,\ y_2 = \alpha^4,\ y_3 = \alpha^3 + \alpha^2$$

and

$$x_1 = \alpha^4 + \alpha^2 + 1,\ x_2 = \alpha^4 + \alpha^2,\ x_3 = \alpha^3 .$$

Therefore,

$$A = \begin{bmatrix} \dfrac{1}{\alpha^4+1} & \dfrac{1}{\alpha^2+1} & \dfrac{1}{\alpha^4+\alpha^3+1} \\ \dfrac{1}{\alpha^4} & \dfrac{1}{\alpha^2} & \dfrac{1}{\alpha^4+\alpha^3} \\ \dfrac{1}{\alpha^3+\alpha^2} & \dfrac{1}{\alpha^4+\alpha^3} & \dfrac{1}{\alpha^2} \end{bmatrix}. \quad (5.1)$$

Since, α is the root of $x^6 + x + 1 = 0$. Therefore,

$\alpha^4 + 1 \neq 0$, $\alpha^2 + 1 \neq 0$, $\alpha^4 + \alpha^2 + \alpha + 1 \neq 0$,
$\alpha^4 + \alpha^3 + 1 \neq 0$, $\alpha^4 \neq 0$, $\alpha^2 \neq 0$,
$\alpha^4 + \alpha^3 \neq 0$, and $\alpha^3 + \alpha^2 \neq 0$.

Also, det $A = \dfrac{\alpha^2 + \alpha}{\alpha^5 + \alpha^3 + a^2} \neq 0$. So, A is non-singular. Also all the sub matrices of A are non-singular.

From (5.1), we have

$A[1][1] = \dfrac{1}{\alpha^4 + 1} \neq 0$,

$A[1][2] = \dfrac{1}{\alpha^2 + 1} \neq 0$,

$A[1][3] = \dfrac{1}{\alpha^4 + \alpha^3 + 1} \neq 0$,

$A[2][1] = \dfrac{1}{\alpha^4} \neq 0$,

$A[2][2] = A[3][3] = \dfrac{1}{\alpha^2} \neq 0$,

$A[2][3] = \dfrac{1}{\alpha^4 + \alpha^3} \neq 0$,

$A[3][1] = \dfrac{1}{\alpha^3 + \alpha^2} \neq 0$,

$A[2][2] = \dfrac{1}{\alpha^3 + \alpha^2 + \alpha + 1} \neq 0.$

Therefore, A is MDS matrix.

Similarly, we can prove that

$$B = \begin{bmatrix} \dfrac{1}{\alpha+1} & \dfrac{1}{\alpha^4+\alpha^2+\alpha+1} \\ \dfrac{1}{\alpha^4+1} & \dfrac{1}{\alpha^2+1} \end{bmatrix} \quad (5.2)$$

is MDS matrix. From (5.2), we have

$B[1][1] = \dfrac{1}{\alpha + 1} \neq 0,$

$B[1][2] = \dfrac{1}{\alpha^4 + \alpha^2 + \alpha + 1} \neq 0,$

$B[2][1] = \dfrac{1}{\alpha^4 + 1} \neq 0,\ B[2][2] = \dfrac{1}{\alpha^2 + 1} \neq 0.$

The rhotrix of the coupled matrices A and B is

$$R_5 = \left\langle \begin{array}{ccccc} & & A[1][1] & & \\ & A[2][1] & B[1][1] & A[1][2] & \\ A[3][1] & B[2][1] & A[2][2] & B[1][2] & A[1][3] \\ & A[3][2] & B[2][2] & A[2][3] & \\ & & A[3][3] & & \end{array} \right\rangle \quad (5.3)$$

.

Using (5.1) and (5.2) in (5.3), we have

$$R_5 = \left\langle \begin{array}{ccccc} & & \frac{1}{\alpha^4+1} & & \\ & \frac{1}{\alpha^4} & \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} & \\ \frac{1}{\alpha^3+\alpha^2} & \frac{1}{\alpha^4+1} & \frac{1}{\alpha^2} & \frac{1}{\alpha^4+\alpha^2+\alpha+1} & \frac{1}{\alpha^4+\alpha^3+1} \\ & \frac{1}{\alpha^4+\alpha^3} & \frac{1}{\alpha^2+1} & \frac{1}{\alpha^4+\alpha^3} & \\ & & \frac{1}{\alpha^2} & & \end{array} \right\rangle.$$

Therefore, from Lemma 1.5, it is clear that R_5 is maximum distance separable rhotrix (MDSR).

Theorem 5.2. Let R_5 be a Cauchy rhotrix whose coupled matrices $A=(a_{ij})_{3\times3}$ and $B=(b_{lm})_{2\times2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let

$y_j = \alpha^{2^j} + \alpha^j + 1;\ x_i = y_j^{\ j+1} + \ y_j + 1$,

$i, j = 1,2,3$ and

$s_l = \alpha^{2^l}\ ; t_m = \alpha^m + \alpha + 1; l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^6 + x + 1$ in the extension field of GF$\left(2^6\right)$. Then A and B form MDS rhotrix R_5.

Theorem 5.3. Let R_5 be a Cauchy rhotrix whose coupled matrices $A=(a_{ij})_{3\times3}$ and $B=(b_{lm})_{2\times2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + \alpha^j$; a

$x_i = y_j^{\ j+1} + 1$, $i, j = 1,2,3$ and

$s_l = \alpha^l + 1; t_m = \alpha^{2^m} + \alpha;\ l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^6 + x + 1$ in the extension field of GF$\left(2^6\right)$. Then A and B form MDS rhotrix R_5.

Theorem 5.4. Let R_5 be a Cauchy rhotrix whose coupled matrices $A=(a_{ij})_{3\times3}$ and $B=(b_{lm})_{2\times2}$ are defined as

$a_{ij} = \dfrac{1}{x_i + y_j}$, $x_i + y_j \neq 0$ and

$b_{lm} = \dfrac{1}{s_l + t_m}$, $s_l + t_m \neq 0$. Let $y_j = \alpha^{2^j} + 1;$

$x_i = y_j + 1,\ i, j = 1,2,3$ and

$s_l = \alpha^{2l} + \alpha + 1; t_m = \alpha^{2^m} + \alpha;\ l, m = 1,2$, where α is the root of irreducible polynomial $p(x) = x^6 + x + 1$ in the extension field of GF$\left(2^6\right)$.

Then A and B form MDS rhotrix R_5.

6. CONCLUSION

In the present paper, the Cauchy rhotrix is defined. The maximum distance seperable rhotrices (MDS) are of much interest in the field of cryptography. Therefore, MDS rhotrices over finite fields are also constructed in this paper.

7. ACKNOWLEDGMENTS

Author thankfully acknowledge the support of UGC SAP.

8. REFERENCES

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

[2] 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.

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

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

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

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

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

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

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

[10] Tudunkaya, S. M. (2013). Rhotrix polynomial and polynomial rhotrix, Pure and Applied mathematics Journal, Vol. 2, pp. 38-41. http://dx.doi.org/10.11648/j.pamj.20130201.16

[11] 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.

[12] 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. 30 E (Math & Stat.), No.2, pp. 333-339.

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

[14] 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.

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

[16] Sharma, P. L. and Kanwar, R. K. (2013). On involutory and pascal rhotrices, International J. of Math. Sci. & Engg. Appls. (IJMSEA), Vol. 7, No. IV, pp. 133-146.

[17] 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.

[18] 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. II, pp. 389-406.

[19] 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.

[20] 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.

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

[22] Sharma, P. L., Kumar, S. and Rehan, M. (2013a). On Hadamard rhotrix over finite field, Bulletin of Pure and Applied Sciences, Vol. 32 E (Math & Stat.), No. 2, pp. 181-190.

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

[24] 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. 03, No. 02, pp. 25-43.

[25] Sharma, P. L., Gupta, S. and Rehan, (2017). On circulant like rhotrices over finite fields, Accepted for publication in Applications and Applied Mathematics: An International Journal (AAM).

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

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

[28] 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.

[29] Lacan, J. and Fimes, J. (2004). Systematic MDS erasure codes based on Vandermonde matrices, IEEE Trans. Commun. Lett. Vol. 8, No. 9, pp. 570-572.

[30] 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, Lectures Notes in Computer Science, Vol. 8128, pp. 29-43.

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

[32] Tzeng, K. K. and Zimmermann, K. (1975). On extending Goppa codes to cyclic codes, IEEE Transactions on Information Theory, Vol. 21, pp. 721-716.

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