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

Applications and Applied Mathematics:
An International Journal
(AAM)

Vol. 12, Issue 1 (June 2017), pp. 506 - 520

On Circulant-Like Rhotrices over Finite Fields

P. L. Sharma[1], Shalini Gupta[2] and Mansi Rehan[3]

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

[2]Department of Mathematics
Bahra University
Waknaghat, Solan, (H.P.), India

[3] Government College
Nahan (H.P.), India

Received August 5, 2016; Accepted March 21, 2017

Abstract

Circulant matrices over finite fields are widely used in cryptographic hash functions, Lattice based cryptographic functions and Advanced Encryption Standard (AES). Maximum distance separable codes over finite field $GF(2)$ have vital a role for error control in both digital communication and storage systems whereas maximum distance separable matrices over finite field $GF(2)$ are used in block ciphers due to their properties of diffusion. Rhotrices are represented in the form of coupled matrices. In the present paper, we discuss the circulant- like rhotrices and then construct the maximum distance separable rhotrices over finite fields.

Keywords: Circulant rhotrix; Vandermonde matrices; Finite field; Maximum distance separable rhotrices

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

1. Introduction

Ajibade (2003) introduced the concept of rhotrix as a mathematical object which is, in some way, between 2×2–dimensional and 3×3–dimensional matrices. He introduced a 3×3-dimensional rhotrix defined as

$$Q_3 = \left\langle \begin{array}{ccc} & f & \\ g & h & j \\ & k & \end{array} \right\rangle,$$

where a, b, c, d, e are real numbers and $h(R_3) = c$ is called the heart of rhotrix R_3. He defined the operations of addition and scalar multiplication, respectively for a rhotix of size three 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

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

and for any real number α,

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

In the literature of rhotrices, there are two types of multiplication of rhotrices namely heart oriented multiplication and row-column multiplication. In the present paper, we use the row-column multiplication. Ajibade discussed the heart oriented multiplication of 3-dimensional rhotrices as given below:

$$R_3 \, o \, Q_3 = \left\langle \begin{array}{ccc} & ah(Q_3) + fh(R_3) & \\ bh(Q_3) + gh(R_3) & h(R_3)h(Q_3) & dh(Q_3) + jh(R_3) \\ & eh(Q_3) + kh(R_3) & \end{array} \right\rangle.$$

Further, it is algorithmatized for computing machines by Mohammed et al. (2011) and also generalized the heart oriented multiplication of 3-dimensional rhotrices to an *n*-dimensional rhotrices in (2011). The row –column multiplication of 3-dimensional rhotrices is defined by Sani (2004) as follows:

$$R_3 \, o \, Q_3 = \left\langle \begin{array}{ccc} & af + dg & \\ bf + eg & ch & aj + dk \\ & bj + ek & \end{array} \right\rangle.$$

Sani (2007) also discussed the row-column multiplication of high dimension rhotrices as follows: Consider an 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:

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

Rhotrices and construction of finite fields were discussed by Tudunkaya et al. (2010). The investigations of rhotrices over matrix theory and polynomials ring theory were given by Aminu (2009, 2012). The extended heart oriented method for rhotrix multiplication was given by Mohammed (2011). Algebra and analysis of rhotrices is discussed in the literature by Ajibade (2003), Sani (2004, 2007), Tudunkaya and Makanjuola (2010), Absalom et al. (2011), Sharma and Kanwar (2012, 2013), Sharma and Kumar (2013, 2014a, 2014b) and Sharma et al. (2013a, 2013b, 2014). Sharma et al. (2015) introduced circulant rhotrices in the literature of rhotrices.

Circulant matrices are widely used in different areas of cryptography such as cryptographic hash function WHIRLPOOL, Lattice based cryptography and at the diffusion layer in Advanced Encryption Standard (AES) as discussed by Menezes et al. (1996).

Maximum distance separable (MDS) matrices have diffusion properties that are used in block ciphers and cryptographic hash functions. There are several methods to construct MDS matrices. Sajadieh et al. (2012) and Lacan and Fimes (2004) used Vandermonde matrices for the construction of MDS matrices. Sajadieh et al. (2012) proposed the construction of involutry MDS matrices from Vandermonde matrices. Circulant matrices are also used for the construction of MDS matrices. Gupta and Ray (2013, 2014) used companion matrices and circulant-like matrices, respectively for the construction of MDS matrices. Junod et al. (2004) constructed new class of MDS matrices whose submatrices were circulant matrices. Circulant matrices are used to improve the efficiency of Lattice-based cryptographic functions.

Definition 1.1.

The $d \times d$ matrix of the form

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{d-1} \\ a_{d-1} & a_0 & a_1 & \cdots & a_{d-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix}$$

is called a circulant matrix and is denoted by $cir\left(a_0, a_1, ..., a_{d-1}\right)$.

Definition 1.2.

A circulant rhotrix C_n is defined as

$$C_n = \left\langle \begin{array}{c} a_0 \\ a_d \quad b_0 \quad a_1 \\ a_{d-1} \quad b_{d-1} \quad a_0 \quad b_1 \quad . \\ . \quad . \quad a_d \quad b_0 \quad . \quad . \quad . \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_1 \quad b_1 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad b_{d-1} \quad a_d \\ a_2 \quad b_2 \quad . \quad . \quad . \quad . \quad . \quad b_{d-2} \quad a_{d-1} \\ . \quad . \quad . \quad . \quad . \quad . \quad a_{d-2} \\ . \quad . \quad . \quad . \quad . \\ . \quad b_0 \quad . \\ a_0 \end{array} \right\rangle,$$

where $a_i, b_j \left(i = 0,1,2, ..., d\,;\, j = 0,1,2, ..., d-1\right)$ are real numbers, n is an odd positive integers and it is denoted by $cir\left(\left(a_0, ..., a_d\right), \left(b_0, ..., b_{d-1}\right)\right)$. Two coupled circulant matrices of C_n are

$$U = \begin{bmatrix} a_0 & a_1 & . & . & . & a_d \\ a_d & a_0 & . & . & . & a_{d-1} \\ a_{d-1} & a_d & . & . & . & a_{d-2} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_1 & a_2 & . & . & . & a_0 \end{bmatrix} \quad \text{and} \quad V = \begin{bmatrix} b_0 & b_1 & . & . & b_{d-1} \\ b_{d-1} & b_0 & . & . & b_{d-2} \\ . & . & . & . & . \\ . & . & . & . & . \\ b_1 & b_2 & . & . & b_0 \end{bmatrix}.$$

Definition 1.3.

Let F be a finite field, and p, q be two 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 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 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 MDSR is that all its sub-rhotrices are non-singular.

The construction of the MDS rhotrices is discussed by Sharma and Kumar in (2013). The following Lemma 1.5 is also discussed in (2013).

Lemma 1.5.

Any rhotrix R_7 over $\mathrm{GF}(2^n)$ with all non-zero entries is an MDS rhotrix iff its coupled matrices $M_1 = 4 \times 4$ and $M_2 = 3 \times 3$ are non-singular and all their entries are non-zero.

Now, we discuss two different types of circulant-like rhotrices. We also construct the maximum distance separable rhotrices by using the circulant- like rhotrices.

2. MDS Rhotrices from Type-I Circulant-Like Rhotrices

Circulant-like matrices are used in block ciphers and hash functions. Rhotrices are represented by the coupled matrices and hence the circulant rhotrices. Therefore, circulant- like rhotrices can play an important role in the designing of block ciphers and hash functions. We discuss here Type-I circulant- like rhotrices and then construct maximum distance separable rhotrices.

The $d \times d$ matrix

$$\begin{bmatrix} a & B \\ B^T & A \end{bmatrix}$$

is called Type-I circulant- like matrix, where $A = cir(a_0, a_1, ..., a_{d-2})$, $B = \underbrace{(b, ..., b)}_{d-1\ times}$, a_i's and a are any non-zero elements of the underlying field. This matrix is denoted as Type-I $(a, b, cir(a_0, a_1, ..., a_{d-2}))$.

Definition 2.1.

Type-I circulant-like rhotrix:

The Type-I circulant rhotrix R_n is defined as

$$R_n = \left\langle \begin{array}{ccccccccccc}
 & & & & & a & & & & & \\
 & & & & b & b_0 & b & & & & \\
 & & & b & b_{d-1} & a_0 & b_1 & b & & & \\
 & & . & . & a_{d-1} & b_0 & . & . & . & & \\
 & . & . & . & . & a_0 & . & . & . & . & \\
b & b_1 & . & . & . & . & . & . & . & b_{d-1} & b \\
 & a_1 & b_2 & . & . & . & . & . & b_{d-2} & a_{d-1} & \\
 & & . & . & . & . & . & . & a_{d-2} & & \\
 & & & . & . & . & . & . & & & \\
 & & & & . & b_0 & . & & & & \\
 & & & & & a_0 & & & & &
\end{array} \right\rangle, \tag{2.1}$$

where $a, b, a_i, b_i\ (i = 0,1,2,...,d-1;\ j = 0,1,2,...,d-1)$ are real numbers, n is an odd positive integer and is denoted by $[(a, b, cir(a_0, ..., a_{d-1})), cir(b_0, ..., b_{d-1})]$. Conversion of a rhotrix to a coupled matrix is discussed by Sani (2008) and had shown that the rhotrix R_n consists of two coupled matrices

$$A = \begin{bmatrix} a & b & \cdots & \cdots & b \\ b & a_0 & a_1 & \cdots & a_{d-1} \\ b & a_{d-1} & a_0 & \cdots & a_{d-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & a_1 & \cdots & \cdots & a_0 \end{bmatrix}$$

and

$$B=\begin{bmatrix} b_0 & b_1 & \cdots & b_{d-1} \\ b_{d-1} & b_0 & \cdots & b_{d-2} \\ \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \cdots & b_0 \end{bmatrix},$$

which are denoted as $A=\left(a,b,cir\left(a_0,\ldots,a_{d-1}\right)\right)$ and $B=cir\left(b_0,\ldots,b_{d-1}\right)$.

Theorem 2.2.

Let R_7 be Type-I circulant-like rhotrix and $A=\left(a,a^2+1,cir\left(1,a+1,a^{-1}\right)\right)$ and $B=cir\left(a,1+a,a^2\right)$ be defined over $\mathrm{GF}(2)$, where a is the root of irreducible polynomial $p(x)=x^8+x^7+x^5+x^4+1$ in the extension field of $\mathrm{GF}\left(2^8\right)$. Then, A^3 and B^3 form MDS rhotrix R_7^3 of order 7.

Proof:

For given $A=\left(a,a^2+1,cir\left(1,a+1,a^{-1}\right)\right)$, we have

$$A^3=\begin{bmatrix} a+a^5+a^{-1} & a^6+a^2+a^{-2}+1 & a^6+a^2+a^{-2}+1 & a^6+a^2+a^{-2}+1 \\ a^6+a^2+a^{-2}+1 & a^5+a^3+a^{-3}+a^2 & a^5+a^{-2}+a^{-1}+a+1 & a^5+a^2+a^{-2}+a+1 \\ a^6+a^2+a^{-2}+1 & a^5+a^2+a^{-2}+a+1 & a^5+a^3+a^{-3}+a^2 & a^5+a^{-2}+a^{-1}+a+1 \\ a^6+a^2+a^{-2}+1 & a^5+a^{-2}+a^{-1}+a+1 & a^5+a^2+a^{-2}+a+1 & a^5+a^3+a^{-3}+a^2 \end{bmatrix}. \quad (2.2)$$

Since, a is the root of $x^8+x^7+x^5+x^4+1$, therefore

$$a^8+a^7+a^5+a^4+1=0,$$

that is,

$$a\left(a^7+a^6+a^4+a^3\right)=1,$$

it gives,

$$a^{-1}=a^7+a^6+a^4+a^3,$$
$$a^{-2}=a^6+a^5+a^3+a^2$$

and

$$a^{-3}=a^5+a^4+a^2+a.$$

Therefore,

$$A^3[1][1]=a+a^5+a^{-1}=a^7+a^6+a^5+a^4+a^3+a\neq 0;$$
$$A^3[1][2]=A^3[1][3]=A^3[1][4]=a^6+a^2+a^{-2}+1=a^5+a^3+1\neq 0;$$
$$A^3[2][1]=A^3[3][1]=A^3[4][1]=a^6+a^2+a^{-2}+1=a^5+a^3=1\neq 0;$$
$$A^3[2][2]=A^3[3][3]=A^3[4][4]=a^5+a^3+a^{-3}+a^2=a^4+a^3+a\neq 0;$$

$$A^3[2][3] = A^3[3][4] = A^3[4][2] = a^5 + a^{-2} + a + a^{-1} + 1 = a^7 + a^4 + a^2 + a + 1 \neq 0;$$
$$A^3[2][4] = A^3[3][2] = A^3[4][3] = a^5 + a^{-2} + a^2 + a + 1 = a^6 + a^3 + a + 1 \neq 0.$$

Clearly A^3 is MDS matrix. Now, for

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

we have,

$$B^3 = \begin{bmatrix} a^6+a^2+a+1 & a^5+a^4+a^3 & a^5+a^3+a \\ a^5+a^3+a & a^6+a^2+a+1 & a^5+a^4+a^3 \\ a^5+a^4+a^3 & a^5+a^3+a & a^6+a^2+a+1 \end{bmatrix}. \qquad (2.3)$$

Therefore,

$$B^3[1][1] = B^3[2][2] = B^3[3][3] = a^6 + a^2 + a + 1 \neq 0;$$
$$B^3[1][2] = B^3[2][3] = B^3[3][1] = a^5 + a^4 + a^3 \neq 0;$$
$$B^3[1][3] = B^3[3][2] = B^3[2][1] = a^5 + a^3 + a \neq 0.$$

Clearly B^3 is MDS matrix. The rhotrix of the coupled matrices A^3 and B^3 is

$$R_7^3 = \left\langle \begin{array}{ccccccc} & & & A^3[1][1] & & & \\ & & A^3[2][1] & B^3[1][1] & A^3[1][2] & & \\ & A^3[3][1] & B^3[2][1] & A^3[2][2] & B^3[1][2] & A^3[1][3] & \\ A^3[4][1] & B^3[3][1] & A^3[3][2] & B^3[2][2] & A^3[2][3] & B^3[1][3] & A^3[1][4] \\ & A^3[4][2] & B^3[3][2] & A^3[3][3] & B^3[2][3] & A^3[2][4] & \\ & & A^3[4][3] & B^3[3][3] & A^3[3][4] & & \\ & & & A^3[4][4] & & & \end{array} \right\rangle, \qquad (2.4)$$

that is,

$$
R_7^3 = \left\langle \begin{array}{cccc}
 & & & a^7+a^6+a^5+a^4+a^2+a \\
 & & a^5+a^3+1 & a^6+a^2+a+1 \\
 & a^5+a^3+1 & a^5+a^3+a & a^4+a^3+a \\
a^5+a^3+1 & a^5+a^4+a^3 & a^6+a^3+a+1 & a^6+a^2+a+1 \\
 & a^7+a^4+a^2+a+1 & a^5+a^3+a & a^4+a^3+a \\
 & & a^6+a^3+a+1 & a^6+a^2+a+1 \\
 & & & a^4+a^3+a
\end{array} \right.
$$

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

Therefore, from Lemma 1.5, it is clear that R_7^3 is maximum distance separable rhotrix (MDSR). On the similar arguments we can prove the following theorems.

Theorem 2.3.

Let R_7 be Type-I circulant-like rhotrix. $A=\left(a,a^{-1},cir\left(1,a^{-1}+1,a^{-2}\right)\right)$ and $B=cir\left(a,a^{-2},a^{-1}\right)$ be defined over $\mathrm{GF}(2)$, where a is the root of irreducible polynomial $p(x)=x^8+x^7+x^5+x^4+1$ in the extension field of $\mathrm{GF}\left(2^8\right)$. Then, A^3 and B^3 form MDS rhotrix R_7^3 of order 7.

Theorem 2.4.

Let R_7 be Type-I circulant-like rhotrix. $A=\left(a^{-1},a^2,cir\left(1,a^{-1}+1,a+1\right)\right)$ and $B=cir\left(a,a^{-1}+1,a^{-1}\right)$ be defined over $\mathrm{GF}(2)$, where a is the root of irreducible polynomial $p(x)=x^8+x^7+x^5+x^4+1$ in the extension field of $\mathrm{GF}\left(2^8\right)$. Then, A^3 and B^3 form MDS rhotrix R_7^3 of order 7.

Theorem 2.5.

Let R_7 be Type-I circulant-like rhotrix. $A=\left(a+1,a^{-1},cir\left(1,a,a^2+1\right)\right)$ and $B=cir\left(a,1,a+a^{-1}\right)$ be defined over $\mathrm{GF}(2)$, where a is the root of irreducible polynomial $p(x)=x^8+x^7+x^5+x^4+1$ in the extension field of $\mathrm{GF}\left(2^8\right)$. Then, A^3 and B^3 form MDS rhotrix R_7^3 of order 7.

3. MDS Rhotrices from Type-II Circulant-Like Rhotrices

Circulant- like matrices of Type-II are useful in block ciphers and also used to construct maximum distance separable matrices for diffusion layers in Adnanced Encryption Standard (AES). Therefore, we introduce circulant-like rhotrices and then use them to construct the maximum distance separable rhotrices.

The $2d \times 2d$ matrix

$$\begin{bmatrix} S & S^{-1} \\ S^3 + S & S \end{bmatrix}$$

is called Type-II circulant- like matrix, where $S = cir\left(a_0, ..., a_{d-1}\right)$. This matrix is denoted as Type II $\left(cir\left(a_0, ..., a_{d-1}\right)\right)$.

Definition 3.1.

Type-II circulant-like rhotrix:

Two coupled matrices

$$\mathrm{A} = \begin{bmatrix} \mathrm{P} & \mathrm{P}^{-1} \\ \mathrm{P}^3 + \mathrm{P} & \mathrm{P} \end{bmatrix}, B = \begin{bmatrix} a & I \\ I^T & \mathrm{P} \end{bmatrix}$$

form Type-II circulant rhotrix, where P is even ordered circulant matrix $cir\left(a_0, \ldots, a_{d-1}\right)$ and $a, a_0, \ldots, a_{d-1}$ are real numbers. It is denoted by Type-II $\left[cir\left(\left(a_0, \ldots, a_{d-1}\right)\right), \left(a, 1, cir\left(a_0, ..., a_{d-1}\right)\right)\right]$.

Example.

Let $\mathrm{P} = cir\left(1, b\right)$, then

$$\mathrm{P} = \begin{bmatrix} 1 & b \\ b & 1 \end{bmatrix}$$

$$\mathrm{P}^{-1} = \begin{bmatrix} \dfrac{-1}{b^2-1} & \dfrac{b}{b^2-1} \\ \dfrac{b}{b^2-1} & \dfrac{-1}{b^2-1} \end{bmatrix},$$

$$\mathrm{P}^3 = \begin{bmatrix} 3b^2+1 & b\left(b^2+3\right) \\ b\left(b^2+3\right) & 3b^2+1 \end{bmatrix}$$

and

$$\mathrm{P}^3+\mathrm{P}=\begin{bmatrix} 3b^2+2 & b\left(b^2+4\right) \\ b\left(b^2+4\right) & 3b^2+2 \end{bmatrix}.$$

Thus, the coupled matrices are

$$\mathrm{A}=\begin{bmatrix} 1 & b & \dfrac{-1}{b^2-1} & \dfrac{b}{b^2-1} \\ b & 1 & \dfrac{b}{b^2-1} & \dfrac{-1}{b^2-1} \\ 3b^2+2 & b\left(b^2+4\right) & 1 & b \\ b\left(b^2+4\right) & 3b^2+2 & b & 1 \end{bmatrix}$$

and

$$\mathrm{B}=\begin{bmatrix} a & 1 & 1 \\ 1 & 1 & b \\ 1 & b & 1 \end{bmatrix}.$$

Therefore, Type-II circulant-like rhotrix is

$$R_7=\left\langle \begin{array}{ccccccc} & & & 1 & & & \\ & & b & a & b & & \\ & 3b^2+2 & 1 & 1 & 1 & \dfrac{-1}{b^2-1} & \\ b\left(b^2+4\right) & 1 & b\left(b^2+4\right) & 1 & \dfrac{b}{b^2-1} & 1 & \dfrac{b}{b^2-1} \\ & 3b^2+2 & b & 1 & b & \dfrac{-1}{b^2-1} & \\ & & b & 1 & b & & \\ & & & 1 & & & \end{array} \right\rangle.$$

Theorem 3.2.

Let R_7 be a Type-II $[\mathrm{cir}\left(\left(1,\mathrm{a}^{-1}\right)\right),\left(a,1,cir\left(1,a^{-1}\right)\right)]$ rhotrix defined over $\mathrm{GF}(2)$, where a is the root of irreducible polynomial $p(x)=x^8+x^7+x^5+x^4+1$ in the extension field of $\mathrm{GF}(2^8)$. Then R_7^3 is an MDS rhotrix of order 7.

Proof:

Let

$$\mathrm{A}=\begin{bmatrix} \mathrm{P} & \mathrm{P}^{-1} \\ \mathrm{P}^3+\mathrm{P} & \mathrm{P} \end{bmatrix}$$

and $\mathrm{P} = cir\left(1, a^{-1}\right)$. Therefore, we have

$$\mathrm{A} = \begin{bmatrix} 1 & a^{-1} & \dfrac{a^2}{a^2-1} & \dfrac{-a}{a^2-1} \\ a^{-1} & 1 & \dfrac{-a}{a^2-1} & \dfrac{a^2}{a^2-1} \\ a^{-2} & a^{-3} & 1 & a^{-1} \\ a^{-3} & a^{-2} & a^{-1} & 1 \end{bmatrix} = A^3. \tag{3.1}$$

Here, a is the root of $p(x) = x^8 + x^7 + x^5 + x^4 + 1$. Therefore,

$$a^{-1} = a^7 + a^6 + a^4 + a^3,$$
$$a^{-2} = a^6 + a^5 + a^3 + a^2$$

and

$$a^{-3} = a^5 + a^4 + a^2 + a.$$

This gives,

$$\mathrm{A}^3[1][1] = \mathrm{A}^3[2][2] = \mathrm{A}^3[3][3] = \mathrm{A}^3[4][4] = 1 \neq 0;$$
$$\mathrm{A}^3[1][2] = \mathrm{A}^3[2][1] = \mathrm{A}^3[3][4] = \mathrm{A}^3[4][3] = a^{-1} = a^7 + a^6 + a^4 + a^3 \neq 0;$$
$$\mathrm{A}^3[1][3] = \mathrm{A}^3[2][4] = \frac{a^2}{a^2-1} = a^2\left(a^6 + a^5 + a^4\right) = a^6 + a^5 + a^4 + 1 \neq 0;$$
$$\mathrm{A}^3[1][4] = \mathrm{A}^3[2][3] = \frac{a}{a^2-1} = a\left(a^6 + a^5 + a^4\right) = a^7 + a^6 + a^5 \neq 0;$$
$$\mathrm{A}^3[3][1] = \mathrm{A}^3[4][2] = a^{-2} = a^6 + a^5 + a^3 + a^2 \neq 0;$$
$$\mathrm{A}^3[3][2] = \mathrm{A}^3[4][1] = a^{-3} = a^5 + a^4 + a^2 + a \neq 0.$$

Clearly, A^3 is MDS matrix. Now,

$$\mathrm{B} = \begin{bmatrix} a & I \\ I^T & \mathrm{P} \end{bmatrix}.$$

Therefore,

$$\mathrm{B}^3 = \begin{bmatrix} a^3 & a + a^2 + a^{-2} & a + a^2 + a^{-2} \\ a + a^2 + a^{-2} & a + 1 + a^{-2} & a + a^{-1} + a^{-3} \\ a + a^2 + a^{-2} & a + a^{-1} + a^{-3} & a + 1 + a^{-2} \end{bmatrix}. \tag{3.2}$$

The matrix (3.2) gives,

$$
\begin{aligned}
&\mathrm{B}^3[1][1] = a^3 \neq 0;\\
&\mathrm{B}^3[1][2] = \mathrm{B}^3[1][3] = \mathrm{B}^3[2][1] = \mathrm{B}^3[3][1] = a^2 + a + a^{-2} = a^6 + a^5 + a^3 + a \neq 0;\\
&\mathrm{B}^3[2][2] = \mathrm{B}^3[3][3] = a^{-2} + a + 1 = a^6 + a^5 + a^3 + a^2 + a + 1 \neq 0;\\
&\mathrm{B}^3[2][3] = \mathrm{B}^3[3][2] = a^{-1} + a^{-3} + 1 = a^7 + a^6 + a^5 + a^3 + a^2 \neq 0.
\end{aligned}
$$

Clearly B^3 is MDS matrix. Using (3.1) and (3.2), we obtain MDS rhotrix R_7^3

$$
R_7^3 = \left\langle
\begin{array}{cccc}
 & & & 1\\
 & & a^7+a^6+a^4+a^3 & a^3\\
 & a^6+a^5+a^3+a^2 & a^6+a^5+a^3+a & 1\\
a^7+a^5+a^4+a^2+a & a^6+a^5+a^3+a & a^5+a^4+a^2+a & a^6+a^5+a^3+a^2+a+1\\
 & a^6+a^5+a^3+a^2 & a^7+a^6+a^5+a^3+a^2 & 1\\
 & & a^7+a^6+a^4+a^3 & a^6+a^5+a^3+a^2+a+1\\
 & & & 1
\end{array}
\right.
$$

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

In the similar ways we can prove the following theorems.

Theorem 3.3.

Let R_7 be a Type-II [$cir\left(\left(a,a^2\right)\right),\left(a,1,cir\left(1,a^{-1}\right)\right)$] circulant rhotrix defined over $\mathrm{GF}(2)$, where a is the root of irreducible polynomial $p(x) = x^8 + x^7 + x^5 + x^4 + 1$ in the extension field of GF $\left(2^8\right)$. Then, R_7^3 is an MDS rhotrix of order 7.

Theorem 3.4.

Let R_7 be a Type-II [$cir\left(\left(1,a+a^{-1}\right)\right),\left(a,1,cir\left(1,a^{-1}\right)\right)$] circulant rhotrix defined over $\mathrm{GF}(2)$, where a is the root of irreducible polynomial $p(x) = x^8 + x^7 + x^5 + x^4 + 1$ in the extension field of $\mathrm{GF}\left(2^8\right)$. Then, R_7^3 is an MDS rhotrix of 7.

Theorem 3.5.

Let R_7 be a Type-II [$cir((a+1,1)),(a,1,cir(1,a^{-1}))$] circulant rhotrix defined over GF(2), where a is the root of irreducible polynomial $p(x)=x^8+x^7+x^5+x^4+1$ in the extension field of GF (2^8). Then, R_7^3 is an MDS rhotrix of order 7.

4. Conclusion

Two different forms of circulant-like rhotrices are introduced which are further used to construct the MDS rhotrices with the elements $a, a+1, a^2, a^{-1}$ where a is the root of constructing irreducible polynomial $p(x)=x^8+x^7+x^5+x^4+1$ in the extension field of GF(2^8).

Acknowledgement:

We *are highly grateful to the reviewers for their valuable suggestions and comments to improve the paper substantially. We also thankfully acknowledge the support of UGC-SAP.*

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, Third Edition). Hand book of Applied Cryptography, CRC Press.

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.

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.

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

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

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.

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.
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.
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.
Sharma, P. L. and Kanwar, R. K. (2012). 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. (2013). On involutory and pascal rhotrices, International J. of Math. Sci. & Engg. Appls. (IJMSEA), Vol. 7, No. IV, 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. II, pp. 389-406.
Sharma, P. L. and Kumar, S. (2014b). 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. (2013a). On Hadamard rhotrix over finite field, Bulletin of Pure and Applied Sciences, Vol. 32 E (Math & Stat.), No. 2, pp. 181-190.
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.
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
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.