On Circulant-Like Rhotrices over Finite Fields

P. L. Sharma¹, Shalini Gupta² and Mansi Rehan³

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

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

³Government 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
\[ Q_3 = \begin{pmatrix} f \\ g \\ h \\ j \\ k \end{pmatrix}, \]

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

\[ Q_3 = \begin{pmatrix} f \\ g \\ h \\ j \\ k \end{pmatrix} \]

be another 3-dimensional rhotrix, then

\[ R_3 + Q_3 = \begin{pmatrix} a \\ b \quad h(R_3) \quad d \\ e \end{pmatrix} + \begin{pmatrix} f \\ g \quad h(Q_3) \quad j \\ k \end{pmatrix} = \begin{pmatrix} a + f \\ b + g \quad h(R_3) + h(Q_3) \quad d + j \\ e + k \end{pmatrix}, \]

and for any real number \( \alpha \),

\[ \alpha R_3 = \alpha \begin{pmatrix} a \\ b \quad h(R_3) \quad d \\ e \end{pmatrix} = \begin{pmatrix} \alpha a \\ \alpha b \quad \alpha h(R_3) \quad \alpha d \\ \alpha e \end{pmatrix}. \]

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:

\[ R_3 \circ Q_3 = \begin{pmatrix} ah(Q_3) + fh(R_3) \\ bh(Q_3) + gh(R_3) \\ eh(Q_3) + kh(R_3) \end{pmatrix}. \]

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:

\[ R_3 \circ Q_3 = \begin{pmatrix} af + dg \\ bf + eg \quad ch \quad aj + dk \\ bj + ek \end{pmatrix}. \]
Sani (2007) also discussed the row-column multiplication of high dimension rhotrices as follows: Consider an $n$-dimensional rhotrix

$$P_n = \begin{pmatrix}
  a_{11} & a_{21} & c_{11} & a_{12} \\
  a_{31} & c_{21} & a_{22} & c_{12} & a_{13} \\
  \vdots & \vdots & \vdots & \vdots & \vdots \\
  a_{i1} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_{1t} \\
  \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & a_{n-2} & c_{t-1t-2} & a_{t-1t-1} & c_{t-2t-1} & a_{t-2t} \\
  \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & a_{n-1} & c_{t-1t-1} & a_{t-1t} \\
  \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & a_{nt} 
\end{pmatrix},$$

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

$$P_n \diamond Q_n = \langle a_{ij}, c_{ik} \rangle \diamond \langle b_{ij}, d_{ik} \rangle = \left\langle \sum_{l_j, l_k=1}^{t} (a_{ij} b_{ij} c_{ik} d_{ik}), \sum_{l_j, l_k=1}^{t} (c_{ik} d_{ik}) \right\rangle.$$


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

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

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

Definition 1.2.

A circulant rhotrix $C_n$ is defined as

$$
C_n = \begin{bmatrix}
  a_0 & a_d & b_0 & a_1 \\
  a_{d-1} & b_{d-1} & a_0 & b_1 \\
  \vdots & \vdots & \vdots & \vdots \\
  a_1 & b_1 & \cdots & \cdots & b_{d-1} & a_d \\
  a_2 & b_2 & \cdots & \cdots & b_{d-2} & a_{d-1} \\
  \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
  \vdots & \vdots & \vdots & \vdots & a_{d-2} & \vdots \\
  \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
  b_0 & & & & & \\
  a_0 & & & & & 
\end{bmatrix}
$$

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

$$
U = \begin{bmatrix}
  a_0 & a_1 & \cdots & a_d \\
  a_d & a_0 & \cdots & a_{d-1} \\
  a_{d-1} & a_d & \cdots & a_{d-2} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_1 & a_2 & \cdots & a_0 
\end{bmatrix}
$$

and

$$
V = \begin{bmatrix}
  b_0 & b_1 & \cdots & b_{d-1} \\
  b_{d-1} & b_0 & \cdots & b_{d-2} \\
  \vdots & \vdots & \ddots & \vdots \\
  b_1 & b_2 & \cdots & b_0 
\end{bmatrix}
$$
**Definition 1.3.**

Let $F$ be a finite field, and $p$, $q$ be two integers. Let $x \rightarrow M \times x$ 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 $R_2$ over $GF(2^n)$ 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 \( A = \text{cir}(a_0, a_1, \ldots, a_{d-2}), \ B = (b, \ldots, b) \), \( a_i \)'s and \( a \)
are any non-zero elements of the underlying field. This matrix is denoted as Type-I \((a, b, \text{cir}(a_0, a_1, \ldots, a_{d-2}))\).

**Definition 2.1.**

**Type-I circulant-like rhotrix:**

The Type-I circulant rhotrix \( R_n \) is defined as

\[
R_n = \begin{bmatrix}
  a & b & b_0 & b \\
  b & b_{d-1} & a_0 & b_1 & b \\
  \vdots & \vdots & a_{d-1} & b_0 & \vdots & \vdots \\
  b & b_1 & \cdots & \cdots & \cdots & b_{d-1} & b \\
  a_1 & b_2 & \cdots & \cdots & b_{d-2} & a_{d-1} \\
  \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
  \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
  b_0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
  a_0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\end{bmatrix}
\]

(2.1)

where \( a, b, a_i, b_i \ (i = 0, 1, 2, \ldots, d-1; j = 0, 1, 2, \ldots, d-1) \) are real numbers, \( n \) is an odd positive integer and is denoted by \( [(a, b, \text{cir}(a_0, \ldots, a_{d-1})), \text{cir}(b_0, \ldots, b_{d-1})] \). 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
which are denoted as  
\[ A = (a, b, cir(a_0, \ldots, a_{d-1})) \text{ and } B = cir(b_0, \ldots, b_{d-1}). \]

**Theorem 2.2.**

Let \( R_7 \) be Type-I circulant-like rhotrix and \( A = (a, a^2 + 1, cir(1, a + 1, a^{-1})) \) and \( B = cir(a, 1 + a, a^2) \) be 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, \( A^3 \) and \( B^3 \) form MDS rhotrix \( R_7^3 \) of order 7.

**Proof:**

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

\[
A^3 = \begin{bmatrix}
    a + a^5 + a^{-1} & a^6 + a^2 + a^{-2} + 1 & a^6 + a^2 + a^{-2} + 1 & a^6 + a^2 + a^{-2} + 1 \\
    a^6 + a^2 + a^{-2} + 1 & a^5 + a^3 + a^{-3} + a^2 & a^5 + a^{-2} + a^{-1} + a + 1 & a^5 + a^2 + a^{-2} + a + 1 \\
    a^6 + a^2 + a^{-2} + 1 & a^5 + a^3 + a^{-3} + a^2 & a^5 + a^3 + a^{-3} + a^2 & a^5 + a^3 + a^{-3} + a^2 \\
    a^6 + a^2 + a^{-2} + 1 & a^5 + a^3 + a^{-3} + a^2 + a + 1 & a^5 + a^3 + a^{-3} + a^2 + a + 1 & a^5 + a^3 + a^{-3} + a^2 + a + 1
\end{bmatrix}.
\] (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,

\[ a(a^7 + a^6 + a^4 + a^3) = 1, \]

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
\[
B = \begin{bmatrix}
a & 1 + a & a^2 \\
1 + a^2 & a & 1 + a \\
1 + a & a^2 & a \\
\end{bmatrix},
\]
we have,
\[
B^3 = \begin{bmatrix}
a^6 + a^2 + a + 1 & a^5 + a^4 + a^3 & a^5 + a + a^3 + a \\
a^5 + a + a^3 & a^6 + a^2 + a + 1 & a^5 + a^4 + a^3 \\
a^3 + a^2 + a^3 & a^5 + a + a^3 & a^6 + a^2 + a + 1 \\
\end{bmatrix}.
\]
(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
\[
R^3_1 = \begin{bmatrix}
\end{bmatrix},
\]
(2.4)

that is,
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. $A = (a, a^{-1}, \text{cir}(1, a^{-1} + 1, a^{-2}))$ and $B = \text{cir}(a, a^{-2}, a^{-1})$ be defined over $\text{GF}(2)$, where $a$ is the root of irreducible polynomial $p(x) = x^8 + x^7 + x^5 + x^4 + 1$ in the extension field of $\text{GF}(2^8)$. 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. $A = (a^{-1}, a^2, \text{cir}(1, a^{-1} + 1, a + 1))$ and $B = \text{cir}(a, a^{-1} + 1, a^{-1})$ be defined over $\text{GF}(2)$, where $a$ is the root of irreducible polynomial $p(x) = x^8 + x^7 + x^5 + x^4 + 1$ in the extension field of $\text{GF}(2^8)$. 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. $A = (a + 1, a^{-1}, \text{cir}(1, a, a^2 + 1))$ and $B = \text{cir}(a, a + a^{-1})$ be defined over $\text{GF}(2)$, where $a$ is the root of irreducible polynomial $p(x) = x^8 + x^7 + x^5 + x^4 + 1$ in the extension field of $\text{GF}(2^8)$. 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 Advanced 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 $S = cir(a_0,\ldots,a_{d-1})$. This matrix is denoted as Type II $(cir(a_0,\ldots,a_{d-1}))$.

**Definition 3.1.**

**Type-II circulant-like rhotrix:**

Two coupled matrices

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

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

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

**Example.**

Let $P = cir(1,b)$, then

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

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

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

and
\[
P^3 + P = \begin{bmatrix}
3b^2 + 2 & b(b^2 + 4) \\
\frac{1}{b(b^2 + 4)} & 3b^2 + 2
\end{bmatrix}.
\]

Thus, the coupled matrices are
\[
A = \begin{bmatrix}
1 & b & -1 & b \\
b & 1 & b & -1 \\
3b^2 + 2 & b(b^2 + 4) & 1 & b \\
b(b^2 + 4) & 3b^2 + 2 & b & 1
\end{bmatrix}
\]

and
\[
B = \begin{bmatrix}
a & 1 & 1 \\
1 & 1 & b \\
1 & b & 1
\end{bmatrix}
\]

Therefore, Type-II circulant-like rhotrix is
\[
R_7 = \begin{bmatrix}
1 & b & a & b \\
3b^2 + 2 & 1 & 1 & 1 \\
b(b^2 + 4) & b(b^2 + 4) & 1 & \frac{b}{b^2 - 1} \\
3b^2 + 2 & b & 1 & \frac{b}{b^2 - 1} \\
b & b & 1 & 1
\end{bmatrix}
\]

**Theorem 3.2.**

Let \( R_7 \) be a Type-II \( \text{cir} \left( \left( [1, a^{-1}] \right), \left( a, 1, \text{cir} \left( [1, a^{-1}] \right) \right) \) \) 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.

**Proof:**

Let
\[
A = \begin{bmatrix}
P & P^{-1} \\
P^3 + P & P
\end{bmatrix}
\]
and $P = cir(1, a^{-1})$. Therefore, we have

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

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,


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

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

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

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

Clearly, $A^3$ is MDS matrix. Now,

$$B = \begin{bmatrix} a & 1 \\ I & P \end{bmatrix}.$$

Therefore,

$$B^3 = \begin{bmatrix} a^3 & a + a^2 + a^{-2} & a + a^2 + a^{-2} \\ a + a^2 + a^{-2} & a + a^2 + a^{-2} & a + a^2 + a^{-2} \\ a + a^2 + a^{-2} & a + a^2 + a^{-2} & a + a^2 + a^{-2} \end{bmatrix}. \quad (3.2)$$

The matrix (3.2) gives,
Clearly $B^3$ is MDS matrix. Using (3.1) and (3.2), we obtain MDS rhotrix $R^3_7$

$$R^3_7 = \begin{pmatrix}
    a^7 + a^6 + a^4 + a^3 & a^7 + a^6 + a^4 + a^3 & 1 \\
    a^6 + a^5 + a^3 + a^2 & a^6 + a^5 + a^3 + a & 1 \\
    a^6 + a^5 + a^3 & a^6 + a^5 + a^3 + a + 1 & 1 \\
    a^7 + a^6 + a^4 + a^3 & a^6 + a^5 + a^3 + a^2 & 1 \\
    a^7 + a^6 + a^3 + a^2 & a^7 + a^6 + a^3 + a^2 + 1 & 1 \\
    a^7 + a^6 + a^4 + a^3 & a^7 + a^6 + a^4 + a^3 + a^2 + 1 & 1
\end{pmatrix}.$$

In the similar ways we can prove the following theorems.

**Theorem 3.3.**

Let $R_7$ be a Type-II $[\text{cir}\left([a,a^2]\right),\{a,1,\text{cir}(1,a^{-1})\}]$ circulant rhotrix defined over GF($2^7$), 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, $R^3_7$ is an MDS rhotrix of order 7.

**Theorem 3.4.**

Let $R_7$ be a Type-II $[\text{cir}\left([1,a+a^{-1}]\right),\{a,1,\text{cir}(1,a^{-1})\}]$ circulant rhotrix defined over GF($2^7$), 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, $R^3_7$ is an MDS rhotrix of 7.
Theorem 3.5.

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

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


