AIMS Mathematics, 9(11): 30529–30547.
DOI: 10.3934/math.20241474
Received: 31 July 2024
Revised: 02 October 2024
Accepted: 18 October 2024
Published: 28 October 2024

https://www.aimspress.com/journal/Math

Research article

XOR count and block circulant MDS matrices over finite commutative rings

Shakir Ali[1,4], Amal S. Alali[2], Atif Ahmad Khan[1,*], Indah Emilia Wijayanti[3] and Kok Bin Wong[4]

[1] Department of Mathematics, Aligarh Muslim University, Aligarh-202002, India

[2] Department of Mathematical Sciences, College of Science, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh-11671, Saudi Arabia

[3] Department of Mathematics, Universitas Gadjah Mada, Yogyakarta-55598, Indonesia

[4] Institute of Mathematical Sciences, Faculty of Science, Universiti Malaya, Kuala Lumpur-50603, Malaysia

* **Correspondence:** Email: atifkhanalig1997@gmail.com.

Abstract: Block circulant MDS matrices are used in the design of linear diffusion layers for lightweight cryptographic applications. Most of the work on construction of block circulant MDS matrices focused either on finite fields or $GL(m, \mathbb{F}_2)$. The main objective of this paper is to extend the above study of block circulant MDS matrices to finite commutative rings. Additionally, we examine the behavior of the XOR count distribution under different reducible polynomials of equal degree over $\mathbb{F}_2$. We show that the determinant of a block circulant matrix over a ring can be expressed in a simple form. We construct 4×4 and 8×8 block circulant matrices over a ring. Furthermore, for non-negative integer l, we identify the conditions under which a ring $\Re_l = \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}$, contains a finite field of order 2^m, where $f(x)$ is an irreducible polynomial of degree m. To facilitate efficient implementation, we analyze XOR distributions within specific rings, such as $R_1 = \frac{\mathbb{F}_2[x]}{\langle (1+x^2+x^6) \rangle}$ and $R_2 = \frac{\mathbb{F}_2[x]}{\langle (1+x^4+x^6) \rangle}$. Our calculations reveal distinct XOR distributions when utilizing two reducible polynomials of equal degree, with XOR count distributions 776 and 764, respectively. However, when using irreducible polynomials of the same degree, the XOR count distributions remain the same. This difference is advantageous for applications in lightweight cryptography.

Keywords: MDS matrix; finite commutative ring; circulant matrix; block circulant matrix; XOR count; diffusion layer
Mathematics Subject Classification: 15A99, 94A60, 15B33, 68R99, 11T71

1. Introduction

The linear diffusion layer is widely used in the design of symmetric-key cryptography. It takes a crucial part in providing resistance against differential and linear cryptanalysis. If all square submatrices of a linear diffusion matrix are non-singular, then it is called a Maximum Distance Separable (MDS) matrix, and in other words, a perfect diffusion matrix with optimal diffusion property is called an MDS matrix. A typical application is in the MixColumns operation of AES [8]. Furthermore, except for block ciphers, MDS matrices are also broadly used in many other ciphers, such as Maelstrom-0 [11], PHOTON [12], SHARK [23], and Grϕstl [10]. There are several approaches to constructing MDS matrices, which can be applied as diffusion layers for block ciphers and hash functions. The first method is based on the algebraic structures such as Cauchy, Vandermonde, and Hadamard matrices (cf.; [13, 18, 20]). The next efficient method to be used in constructing MDS matrices is based on recursive construction (see [18, 24, 27], for more details). Also, a brief survey of various theories in the construction of MDS matrices is provided in [15].

Circulant matrices have attracted significant attention for the efficient construction of MDS matrices. A circulant matrix is a unique type of matrix in which each row vector is a cyclic shift of the previous row vector, rotated one element to the right. In the diffusion layer, circulant matrices are utilized by the Advanced Encryption Standard (AES) [8]. The advantage of circulant matrices is that they can be fully described by just n elements, instead of requiring storage of all n^2 elements. In the study of circulant MDS matrices over finite fields, significant contributions have been made, as referenced in [1, 14, 15, 21]. Han et al. [16] introduced a special generalization called block circulant matrices with circulant blocks. The authors demonstrated that block circulant matrices can perform better than circulant matrices in the implementation of the InvMixColumn operations. In 2021, Cui et al. [4] demonstrated that a Galois field is a subclass of a commutative ring, suggesting the possibility of finding more cost-effective MDS matrices within commutative rings rather than Galois fields. Taking this into account, Ali et al. [2] provided key insights into circulant MDS matrices over finite commutative rings of characteristic 2 and proved several important results regarding the non-existence of certain circulant MDS matrices over rings.

Inspired by the work of Han et al. [16] and Cui et al. [4], in the present article, we first derive the expression for the determinant of block circulant matrices over a finite commutative ring of characteristic 2. It is known that block circulant matrices can produce more efficient MDS matrices compared to circulant matrices. Using this expression, we construct block circulant MDS matrices of order 4×4 and 8×8 over rings. Furthermore, we examine the work of Khoo et al. [9], where they proposed analyzing the number of XOR operations required to compute the multiplication of a fixed element. For more studies related to implementation and d-XOR count, see the references [7, 19, 25]. In 2015, Sim et al. [26] proved the following result about the XOR-count:

Theorem A. [26, Theorem 1] The total XOR-count for a field $GF(2^n)$ is

$$n \sum_{i=2}^{n} 2^{i-2}(i-1), \quad \text{where } n \geq 2.$$

This theorem proved that the sum of XORs of the elements of the finite field is invariant under the change of an irreducible polynomial of the same degree. Further, Sarkar and Sim [25] studied the

XOR-count distribution under different bases of a finite field and proved the following:
Theorem B. [25, Proposition 2] The total XOR-count of the elements in $GF(2^n)$ is

$$n\sum_{i=2}^{n}\binom{n}{i}(i-1), \text{ where } n \geq 2,$$

and it is invariant under the choice of basis.

In 2021, Kesarwani et al. [18] extended the study of XOR count over a local rings. Using this result, we explore the XOR count distributions for two rings associated with two distinct reducible polynomials of the same degree and compare their corresponding XOR distributions. We obtain distinct XOR count distributions, which increase the probability of finding lightweight MDS matrices.

The organization of the paper is as follows: In Section 2, we start by explaining important terms like MDS matrices, circulant matrices, and block circulant matrices. Then, we show some interesting results about circulant matrices over finite commutative rings. We even figure out how to find the determinant of a circulant matrix over a ring of characteristic 2. In Section 3, we prove one of the main results about block circulant matrices in which we calculate their determinants. We even show how to make special 4×4 and 8×8 block circulant MDS matrices over ring. Further, we find out the condition when a ring $\frac{\mathbb{Z}_2[x]}{\langle (f(x))^{2^l}\rangle}$ contains a copy of finite field of order 2^m, where m is the degree of irreducible polynomial $f(x)$, and by using this result, we prove some results on MDS matrices over the ring $\frac{\mathbb{F}_2[x]}{\langle (1+x+x^3+x^4+x^8)^{2^l}\rangle}$. We start Section 4, from the definition of XOR count of a finite field, and then we calculate the XOR count distribution of two rings, $R_1 = \frac{\mathbb{F}_2[x]}{\langle (1+x^2+x^6)\rangle}$ and $R_2 = \frac{\mathbb{F}_2[x]}{\langle (1+x^4+x^6)\rangle}$. In the last section, we wrap our study with some examples of MDS matrices and their XOR counts.

2. Preliminaries

Some notations used throughout the paper are presented as follows:

R	Finite commutative ring of characteristic 2.
$U(R)$	Set of all unit elements of R.
$N(R)$	Set of all nilpotent elements of R.
$\mathcal{B}_{(s,t)}(R)$	Set of all block circulant matrices over a ring R.
I_n	Identity matrix of order n.
$\oplus$	Addition modulo 2.
$\mathbb{F}_{2^n}$	Finite field of cardinality 2^n with characteristic 2.
$GL(k,\ R)$	Set of all non-singular matrices of order k over a ring R.
$M(k,\ R)$	Set of all matrices of order k over a ring R.

In this section, we discuss some useful definitions such as MDS code, MDS matrix, circulant matrix, block circulant matrix and some important results. Throughout our paper, m, n, l, k, d, s, and t are positive integers.

Definition 1. *[6] A linear code $C(n,k)$ of length n and dimension k over R with minimum Hamming distance d satisfying $d = n - k + 1$ is said to be a maximal distance separable (MDS) code.*

Definition 2. *A matrix $M_{n\times n}$ is an MDS matrix if and only if all its square submatrices are non-singular.*

In 1997, Dong et al. [5] gave a matrix characterization of MDS codes over modules, which we state as follows:

Lemma 1. *[5, Theorem 2.1] Let $C(n,k)$ be a linear code over R with a parity check matrix H of the form $H = (B|I_{n-k})$. Then, $C(n,k)$ is an MDS code if and only if the determinants of every $t\times t$ submatrix, $t \in \{1,2,\ldots,min\{k,n-k\}\}$ of B is an element of $U(R)$.*

Note that MDS matrices are perfect diffusion matrices with maximum branch number. A permutation layer with a good diffusion matrix in block cipher can improve the avalanche characteristics of the block cipher, which increases the cipher's resistance to differential and linear cryptanalysis [17]. The MDS matrices are extensively used in designing block ciphers and hash functions that provide security against differential and linear cryptanalysis.

Definition 3. *Let R be a ring and $b_i \in R$ for all $i = 0,\ 1,\ldots,\ d-1$. Then, any $d\times d$ matrix of the form*

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

is called a circulant matrix of order d, and it is denoted by $circ(b_0, b_1, b_2, \ldots, b_{d-1})$.

Since a circulant matrix can also be written as a polynomial in some suitable permutation matrix, we have the following result:

Lemma 2. *[22, page 290] Let $d \geq 1$ be a fixed integer. Then, any circulant matrix $B = circ(b_0, b_1, \ldots, b_{d-1})$ of order d can be written in the form*

$$B = b_0 I + b_1 T + b_2 T^2 + \cdots + b_{d-1}T^{d-1},\ \text{where } T = circ(0,1,0,\ldots,0) \text{ of order } d.$$

Lemma 3. *[21, Theorem 3.1.1] Let A be a matrix of order d and $T = circ(0,1,0,\ldots,0)$ be a matrix of order d. Then, A is a circulant if and only if $AT = TA$, where it follows that all circulant matrices of the same order commute.*

Lemma 4. *[2, Lemma 7] Let $B = circ(b_0, b_1, \ldots, b_{2d-1})$ be a circulant matrix of order $2d$ where $b_0, b_1, \ldots, b_{2d-1} \in R$. Then,*

$$B^2 = circ(b_0^2 + b_d^2,\ 0,\ b_1^2 + b_{d+1}^2,\ 0,\ \ldots, b_{d-1}^2 + b_{2d-1}^2,\ 0).$$

Definition 4. *An (s,t)-block circulant matrix of order st is a matrix of the form*

$$bCirc(A_1,\ A_2,\ \ldots, A_s) = \begin{bmatrix} A_1 & A_2 & \ldots & A_s \\ A_s & A_1 & \ldots & A_{s-1} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & \ldots & A_1 \end{bmatrix},$$

where $A_1, A_2, A_3, \ldots, A_s$ are square matrices of order t and $bCirc(A_1, \ldots, A_s)$ represent a block circulant matrix.

It is clear that if $s = 1$ or $t = 1$, an (s, t)-block circulant degenerates to an ordinary circulant matrix. But a block circulant is not necessarily a circulant. For example, the matrix

$$\begin{bmatrix} a & b & e & f \\ c & d & g & h \\ e & f & a & b \\ g & h & c & d \end{bmatrix},$$

is a block circulant matrix but fails to be a circulant if $a \neq d$.

Definition 5. *Let $D = bCirc(A_1, A_2, \ldots, A_s)$ be an (s, t)-block circulant, if each block A_i is a circulant, D is called an (s, t)-block circulant with circulant blocks. The class of such types of matrices is denoted by $\mathcal{B}_{s,t}(R)$.*

For example, the matrix of type

$$bCirc\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}, \begin{bmatrix} c & d \\ d & c \end{bmatrix}, \begin{bmatrix} e & f \\ f & e \end{bmatrix}\right) = \begin{bmatrix} a & b & c & d & e & f \\ b & a & d & c & f & e \\ e & f & a & b & c & d \\ f & e & b & a & d & c \\ c & d & e & f & a & b \\ d & c & f & e & b & a \end{bmatrix},$$

is in $\mathcal{B}_{3,2}(R)$.
In [2], first and third authors calculated the determinant of the circulant matrix over a finite commutative ring of characteristic 2.

Lemma 5. *[2, Proposition 10] Let $circ(b_0, b_1, \ldots, b_{2^d-1})$ be a circulant matrix over R. Then,*

$$circ(b_0, b_1, \ldots, b_{2^d-1})^{2^d} = \Big(\sum_{j=0}^{2^d-1} b_j^{2^d}\Big) I_{2^d}, \text{ where } b_j \in R.$$

Corollary 6. *[2, Corollary 11] For any positive integer d, we have*

$$\det(circ(b_0, b_1, \ldots, b_{2^d-1})) = \sum_{j=0}^{2^d-1} b_j^{2^d} + x, \text{ where } b_j \in R \text{ and for some } x \in N(R).$$

3. The main results

The significance of MDS matrices of order 2^d is paramount in the development of block ciphers and primarily owing to their ease of implementation. Our particular emphasis is directed towards matrices within $\mathcal{B}_{s,t}(R)$, with the underlying assumption that $s = 2^{d_1}$ and $t = 2^{d_2}$ throughout the subsequent sections, where d, d_1, and d_2 are positive integers.

Now, we state and prove the first main result of this paper:

Theorem 7. *Let $D = bCirc(A_1, A_2, \ldots, A_s) \in \mathcal{B}_{s,t}(R)$, where $A_i = Circ(a_{i,1}, a_{i,2}, \ldots, a_{i,t})$, $1 \leq i \leq s$, $s = 2^{d_1}$, $t = 2^{d_2}$. Then,*

$$D^{\max\{s,t\}} = \sum_{i=1}^{s} \Big(\det(A_i) + z_i \Big)^{\frac{s}{\min\{s,t\}}} I_{st}, \text{ and } \det(D) = \sum_{i=1}^{s} \det(A_i)^s + z,$$

for some z, $z_i \in N(R)$.

Proof. Let $D = bCirc(A_1, A_2, \ldots, A_s)$ be a block circulant matrix of order $st \times st$ over the ring $\mathcal{B}_{s,t}(R)$. In view of Lemmas 3 and 5, we have

$$D^s = \begin{bmatrix} \sum\limits_{i=1}^{s} A_i^s & 0 & \ldots & \ldots & 0 & 0 \\ 0 & \sum\limits_{i=1}^{s} A_i^s & \ldots & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & 0 & \sum\limits_{i=1}^{s} A_i^s \end{bmatrix} \tag{3.1}$$

and $A_i^t = \sum\limits_{j=1}^{t} a_{i,j}^t I_t$.

Case (i): When $s > t$, *i.e.*, $d_1 > d_2$. Then, we have

$$\begin{aligned} A_i^s = A_i^{2^{d_1}} &= (A_i^{2^{d_2}})^{2^{d_1-d_2}} = (A_i^t)^{\frac{s}{t}} \\ &= \Big(\sum_{j=1}^{t} a_{i,j}^t I_t \Big)^{\frac{s}{t}} \\ &= \Big(\sum_{j=1}^{t} a_{i,j}^t \Big)^{\frac{s}{t}} I_t. \end{aligned}$$

From Corollary 6, we obtain, $\det(A_i) = z_i + \sum\limits_{j=1}^{t} a_{i,j}^t$, for some $z_i \in N(R)$. This gives,

$$A_i^s = (\det(A_i) + z_i)^{\frac{s}{t}} I_t. \tag{3.2}$$

Using Eq (3.2) in Eq (3.1), we obtain

$$D^s = \begin{bmatrix} \sum\limits_{i=1}^{s} (\det(A_i) + z_i)^{\frac{s}{t}} I_t & 0 & \ldots & \ldots & 0 & 0 \\ 0 & \sum\limits_{i=1}^{s} (\det(A_i) + z_i)^{\frac{s}{t}} I_t & \ldots & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & 0 & \sum\limits_{i=1}^{s} (\det(A_i) + z_i)^{\frac{s}{t}} I_t \end{bmatrix}$$

$$= \sum_{i=1}^{s} (\det(A_i) + z_i)^{\frac{s}{t}} I_{st}.$$

This yields that,

$$\det(D)^s = \det(D^s) = \left(\sum_{i=1}^{s} (\det(A_i) + z_i)^{\frac{s}{t}} \right)^{st}$$
$$= \sum_{i=1}^{s} (\det(A_i) + z_i)^{s^2}.$$

The last relation gives

$$\Big(\det(D) + \sum_{i=1}^{s} (\det(A_i) + z_i)^s \Big)^s = 0.$$

Thus, we obtain

$$\det(D) = \sum_{i=1}^{s} (\det(A_i) + z_i)^s + z, \text{ for some } z,\ z_i \in N(R)$$
$$= \sum_{i=1}^{s} (\det(A_i))^s + z, \text{ for some } z \in N(R),$$

and

$$D^s = \sum_{i=1}^{t} (\det(A_i) + z_i)^{\frac{s}{t}} I_{st}.$$

Case (ii): When $s \leq t$, *i.e.*, $d_1 \leq d_2$. Then, we have

$$D^t = D^{2^{d_2}} = (D^{2^{d_1}})^{2^{d_2 - d_1}} = (D^s)^{\frac{t}{s}}$$
$$= \begin{bmatrix} \sum\limits_{i=1}^{s} A_i^s & 0 & \dots & \dots & 0 & 0 \\ 0 & \sum\limits_{i=1}^{s} A_i^s & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & 0 & \sum\limits_{i=1}^{s} A_i^s \end{bmatrix}^{\frac{t}{s}}$$

$$= \begin{bmatrix} \sum_{i=1}^{s}(\det(A_i)+z_i)I_t & 0 & \dots & \dots & 0 & 0 \\ 0 & \sum_{i=1}^{s}(\det(A_i)+z_i)I_t & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & 0 & \sum_{i=1}^{s}(\det(A_i)+z_i)I_t \end{bmatrix}$$

$$= \sum_{i=1}^{s}(\det(A_i)+z_i)I_{st}.$$

This implies that,

$$\begin{aligned} \det(D)^t &= \det(D^t) \\ &= \left(\sum_{i=1}^{s}(\det(A_i)+z_i)\right)^{st}. \end{aligned}$$

The above relation yields

$$\left(\det(D) + \Big(\sum_{i=1}^{s}(\det(A_i)+z_i)\Big)^s\right)^t = 0.$$

This implies,

$$\det(D) = \Big(\sum_{i=1}^{s}(\det(A_i)+z_i)\Big)^t + \xi; \text{ for some } \xi \in N(R).$$

That is,

$$\det(D) = \sum_{i=1}^{s}(\det(A_i))^s + \xi; \text{ for some } \xi \in N(R).$$

This completes the proof. □

As an application of Theorem 7, we derive the following results. Precisely, if we take finite field of characteristic 2 in Theorem 7, then we obtain

Corollary 8. *[16, Theorem 4.4] Let* $D = bCirc(A_1, A_2, \dots, A_s) \in \mathcal{B}_{s,t}(\mathbb{F}_{2^n})$, *where* $A_i = Circ(a_{i,1}, a_{i,2}, \dots, a_{i,t})$, $1 \le i \le s$, $s = 2^{d_1}$, $t = 2^{d_2}$. *Then*

$$D^{\max\{s,t\}} = \left(\sum_{i=1}^{s}\det(A_i)^s\right)^{\frac{1}{\min\{s,t\}}} I_{st},$$

and

$$\det(D) = \sum_{i=1}^{s}\det(A_i)^s.$$

In the following propositions, we construct 4×4 and 8×8 block circulant MDS matrices over the ring $\mathbb{F}_{2^8} \times \mathbb{F}_{2^8}$, where $h(x) = x^8 + x^4 + x^3 + x + 1$ is the generating polynomial of $\mathbb{F}_{2^8}$, α and β are the roots of this generating polynomial, and $\overline{\gamma} = (\alpha, \beta)$, $\bar{\mathbf{1}} = (1, 1) \in \mathbb{F}_{2^8} \times \mathbb{F}_{2^8}$.

Proposition 9. *Let α and β be the roots of the polynomial $h(x)$. Then, $D = bCirc(circ(\bar{\boldsymbol{I}}, \bar{\gamma}), circ(\bar{\gamma}^{-1}, \bar{\gamma} + \bar{\boldsymbol{I}})) \in \mathcal{B}_{2,2}(\mathbb{F}_{2^8} \times \mathbb{F}_{2^8})$ is an MDS matrix, and $D^{-1} = \gamma^2 D$.*

Proof. Application of [16, Proposition 5.3], makes it clear that D is an MDS matrix. By employing Theorem 7, we can write

$$D^{max\{2,2\}} = D^2 \quad = \quad \sum_{i=1}^{2} (det(A_i) - z_i)^{\frac{2}{min\{2,2\}}},$$

where $A_1 = circ(\bar{\mathbf{1}}, \bar{\gamma})$, $B = circ(\bar{\gamma}^{-1}, \bar{\gamma} + \bar{\mathbf{1}})$. By Corollary 6, we obtain $\det(A_1) = \bar{\gamma}^2 + \bar{\mathbf{1}}$ and $\det(A_2) = \bar{\gamma}^2 + \bar{\mathbf{1}} + (\bar{\gamma}^{-1})^2$, and hence

$$\begin{aligned} D^{max\{2,2\}} = D^2 &= \sum_{i=1}^{2} (det(A_i) - z_i)^{\frac{2}{min\{2,2\}}} \\ &= det(A_1) + det(A_2) + z_1 + z_2, \ \ where\ z_1,\ z_2 \in N(\mathbb{F}_{2^8} \times \mathbb{F}_{2^8}) \\ &= (\alpha^2, \beta^2) + (1, 1) + (\alpha^2 + 1, \beta^2 + 1) + (\alpha^2, \beta^2)^{-1} \\ &= (\alpha^2, \beta^2)^{-1} I = (\gamma^2)^{-1} I \\ D^{-1} &= \gamma^2 D. \end{aligned}$$

□

Proposition 10. *Let α and β be the roots of the polynomial $h(x)$. Then, $D = bCirc(circ(\bar{\boldsymbol{I}}, \bar{\boldsymbol{I}}, \bar{\gamma}^{-1} + \bar{\gamma}, \bar{\gamma}), cir(\bar{\boldsymbol{I}} + \bar{\gamma} + \bar{\gamma}^{-1}, \bar{\boldsymbol{I}} + \bar{\gamma}, \bar{\gamma}^{-1}, \bar{\gamma}^{-1} + \bar{\gamma})) \in \mathcal{B}_{2,4}(\mathbb{F}_{2^8} \times \mathbb{F}_{2^8})$ is an MDS matrix, and $D^{-1} = \gamma^{-4} D \times D^2$.*

Proof. In view of [16, Proposition 5.4], we can easily see that D is an MDS matrix. With the help of Theorem 7, we can write

$$D^{\max\{4,2\}} = D^4 = \quad = \quad \sum_{i=1}^{2} (\det(A_i))^2 I,$$

where $A_1 = circ(\bar{\mathbf{1}}, \bar{\mathbf{1}}, \bar{\gamma}^{-1} + \bar{\gamma}, \bar{\gamma})$, $A_2 = cir(\bar{\mathbf{1}} + \bar{\gamma} + \bar{\gamma}^{-1}, \bar{\mathbf{1}} + \bar{\gamma}, \bar{\gamma}^{-1}, \bar{\gamma}^{-1} + \bar{\gamma}))$. Application of Corollary 6 yields, $\det(A_1) = (\bar{\gamma}^{-1})^2$ and $\det A_2 = (\bar{\gamma}^{-1})^2 + (\bar{\gamma})^2$

$$\begin{aligned} D^{\max\{4,2\}} &= \sum_{i=1}^{2} (\det(A_i))^2 I \\ D^4 &= ((\bar{\gamma}^{-1})^4 + (\bar{\gamma}^{-1})^4 + (\bar{\gamma})^4) I = ((\bar{\gamma})^4) I. \end{aligned}$$

This implies,

$$D^{-1} \quad = \quad (\bar{\gamma}^{-1})^4 D \times D^2.$$

□

Proposition 11. *Let α and β be the roots of the polynomial $h(x)$. Then, $D = bCirc(circ(\bar{\boldsymbol{1}}, \bar{\gamma}^{-1}), circ(\bar{\gamma}^{-1} + \bar{\boldsymbol{1}}, \bar{\gamma}^2), circ(\bar{\gamma}, \bar{\gamma}^{-1} + \bar{\boldsymbol{1}}), circ(\bar{\gamma}^2 + \bar{\boldsymbol{1}}, \bar{\boldsymbol{1}} + \bar{\gamma} + \bar{\gamma}^{-1})) \in \mathcal{B}_{4,2}(\mathbb{F}_{2^8} \times \mathbb{F}_{2^8})$ is an MDS matrix.*

Proposition 12. *Let $D = bCirc(circ(a_1, a_2),\ circ(a_3, a_4))$ be an MDS matrix over R. Then, $a_i \neq a_j + \eta$ $(1 \leq i,\ j \leq 4)$, for any $\eta \in N(R)$.*

Proof. Since $D = bCirc(circ(a_1, a_2),\ circ(a_3, a_4))$. So, we have

$$D = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \\ a_3 & a_4 & a_1 & a_2 \\ a_4 & a_3 & a_2 & a_1 \end{bmatrix}.$$

Let us suppose on the contrary, $a_i = a_j + \eta$, where $1 \leq i,\ j \leq 4$. Since $C = circ(a_i,\ a_j) = circ(a_i,\ a_i + \eta)$ is a submatrix of D, so $\det(C) = a_i^2 + a_i^2 + \eta^2 = \eta^2$. This implies that $\det(C) \in N(R)$. Hence, we obtained a contradiction as D is an MDS matrix. Therefore $a_i \neq a_j + \eta$ $(1 \leq i,\ j \leq 4)$, for any $\eta \in N(R)$. □

In the following lemma, we prove that the ring $\Re_l = \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}$ contains a finite field of order 2^m, where $f(x)$ is any irreducible polynomial of degree m.

Lemma 13. *Let $f(x)$ be any irreducible polynomial of degree m over $\mathbb{F}_2$ and $\Re_l = \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}$ be a ring. Then, $\Re_l$ has a field of order 2^m.*

Proof. Let $f(x)$ be an irreducible polynomial of degree m over $\mathbb{F}_2$. Now, we define a map $\phi : \frac{\mathbb{F}_2[x]}{\langle f(x) \rangle} \longrightarrow \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}$ as $\phi(h(x) + \langle f(x) \rangle) = (h(x))^{2^l} + \langle (f(x))^{2^l} \rangle$ for all $h(x) \in \mathbb{F}_2[x]$. First, we prove that ϕ is well defined. Let $h_1(x) + \langle f(x) \rangle$ and $h_2(x) + \langle f(x) \rangle \in \frac{\mathbb{F}_2[x]}{\langle f(x) \rangle}$ such that $h_1(x) + \langle f(x) \rangle = h_2(x) + \langle f(x) \rangle$. This implies that $h_1(x) - h_2(x) \in \langle f(x) \rangle$, that is, $h_1(x) - h_2(x) = g(x) \cdot f(x)$ for some $g(x) \in \mathbb{F}_2[x]$. Therefore, we write $(h_1(x) - h_2(x))^{2^l} = (g(x) \cdot f(x))^{2^l}$, that is, $(h_1(x) - h_2(x))^{2^l} = (g(x))^{2^l} (f(x))^{2^l} = 0 \mod (f(x))^{2^l}$. Hence, $\phi(h_1(x) + \langle f(x) \rangle) = \phi(h_2(x) + \langle f(x) \rangle)$.

Next, we want to prove that ϕ is a ring homomorphism. For any $h_1(x) + \langle f(x) \rangle,\ h_2(x) + \langle f(x) \rangle \in \frac{\mathbb{F}_2[x]}{\langle f(x) \rangle}$, we have

$$\begin{aligned} \phi(h_1(x) + \langle f(x) \rangle + h_2(x) + \langle f(x) \rangle) &= (h_1(x) + h_2(x))^{2^l} + \langle (f(x))^{2^l} \rangle \\ &= (h_1(x))^{2^l} + (h_2(x))^{2^l} + \langle (f(x))^{2^l} \rangle \\ &= \phi(h_1(x) + \langle f(x) \rangle) + \phi(h_2(x) + \langle f(x) \rangle). \end{aligned}$$

Also, we have

$$\begin{aligned} \phi((h_1(x) + \langle f(x) \rangle) \cdot (h_2(x) + \langle f(x) \rangle)) &= \phi(h_1(x)h_2(x) + \langle f(x) \rangle) \\ &= (h_1(x)h_2(x))^{2^l} + \langle (f(x))^{2^l} \rangle \\ &= ((h_1(x))^{2^l} + \langle (f(x))^{2^l} \rangle) \cdot ((h_2(x))^{2^l} + \langle (f(x))^{2^l} \rangle) \\ &= \phi(h_1(x) + \langle f(x) \rangle) \cdot \phi(h_2(x) + \langle f(x) \rangle). \end{aligned}$$

Hence, ϕ is a ring homomorphism. To show that ϕ is an embedding, we prove that ϕ is injective. Let $h(x) + \langle f(x) \rangle \in \mathrm{Ker}(\phi)$. Therefore, we have $\phi(h(x) + \langle f(x) \rangle) = \langle (f(x))^{2^l} \rangle$, which implies

$(h(x))^{2^l} + \langle (f(x))^{2^l} \rangle = \langle (f(x))^{2^l} \rangle$. Thus, $(h(x))^{2^l} \in \langle (f(x))^{2^l} \rangle$, $f(x) \mid h(x)$. That is, $h(x) + \langle f(x) \rangle = \langle f(x) \rangle$. Henceforth, we conclude that $\text{Ker}(\phi) = \{\langle f(x) \rangle\}$.

Thus, ϕ is injective. Hence, $\frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}$ contains a field of order 2^m which is isomorphic to $\frac{\mathbb{F}_2[x]}{\langle f(x) \rangle}$. □

Lemma 14. *Let $\psi : M\left(d, \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right) \longrightarrow M\left(d, \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$ be a map, for any $A = (a_{i,j}) \in M\left(d, \frac{\mathbb{F}_2[x]}{\langle ((f(x))^{2^l} \rangle}\right)$ define ψ as $\psi((a_{ij})) = (a_{ij} + \eta_{ij}) = A'$, where $\eta_{ij} \in N\left(\frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$ for $1 \leq i,\ j \leq d$. Then, A is invertible if and only if A' is invertible.*

Proof. Let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{bmatrix} \in M\left(d, \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$$

be an invertible matrix. Since,

$$\psi : M\left(d, \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right) \longrightarrow M\left(d, \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$$

be a map defined by $\psi((a_{ij})) = (a_{ij} + \eta_{ij}) = A'$. That is,

$$A' = \psi(A) = \begin{bmatrix} a_{11} + \eta_{11} & a_{12} + \eta_{12} & \cdots & a_{1d} + \eta_{1d} \\ a_{21} + \eta_{21} & a_{22} + \eta_{22} & \cdots & a_{2d} + \eta_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} + \eta_{d1} & a_{d2} + \eta_{d2} & \cdots & a_{dd} + \eta_{dd} \end{bmatrix}.$$

We now prove that A' is invertible in $M\left(d, \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$. For this, we calculate the determinant of A' as

$$\begin{aligned} \det(A') &= \begin{vmatrix} a_{11} + \eta_{11} & a_{12} + \eta_{12} & \cdots & a_{1d} + \eta_{1d} \\ a_{21} + \eta_{21} & a_{22} + \eta_{22} & \cdots & a_{2d} + \eta_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} + \eta_{d1} & a_{d2} + \eta_{d2} & \cdots & a_{dd} + \eta_{dd} \end{vmatrix} \\ &= \begin{vmatrix} a_{11} & a_{12} + \eta_{12} & \cdots & a_{1d} + \eta_{1d} \\ a_{21} & a_{22} + \eta_{22} & \cdots & a_{2d} + \eta_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} & a_{d2} + \eta_{2d} & \cdots & a_{dd} + \eta_{dd} \end{vmatrix} + \begin{vmatrix} \eta_{11} & a_{12} + \eta_{12} & \cdots & a_{1d} + \eta_{1d} \\ \eta_{21} & a_{22} + \eta_{22} & \cdots & a_{2d} + \eta_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ \eta_{d1} & a_{d2} + \eta_{d2} & \cdots & a_{dd} + \eta_{dd} \end{vmatrix} \\ &= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{vmatrix} + t, \end{aligned}$$

where

$$t = \begin{vmatrix} \eta_{11} & a_{12}+\eta_{12} & \cdots & a_{1d}+\eta_{1d} \\ \eta_{21} & a_{22}+\eta_{22} & \cdots & a_{2d}+\eta_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ \eta_{d1} & a_{d2}+\eta_{d2} & \cdots & a_{dd}+\eta_{dd} \end{vmatrix} + \cdots + \begin{vmatrix} a_{11} & a_{12} & \cdots & \eta_{1d} \\ a_{21} & a_{22} & \cdots & \eta_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} & a_{d2} & \cdots & \eta_{dd} \end{vmatrix} \in N\left(\frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right).$$

Since A is invertible, $\det(A)$ is a unit in $\frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}$. Therefore, $\det(A') = \det(A)+t$, where $t \in N\left(\frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$, which implies that $\det(A')$ is also a unit element in $\frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}$. Hence, A' is invertible.
Similarly, we can prove the converse of this theorem. □

Theorem 15. *Let $A = (a_{ij}) \in GL\left(d, \frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$ be an MDS matrix, and $\eta_{ij} \in N\left(\frac{\mathbb{F}_2[x]}{\langle (f(x))^{2^l} \rangle}\right)$. Then, $A' = (a_{ij} + \eta_{ij})$ is an MDS matrix.*

Proof. The proof of this theorem directly follows from Lemma 14. □

Theorem 16. *Let $\mathcal{R}_t = \frac{\mathbb{F}_2[x]}{\langle (1+x+x^3+x^4+x^8)^{2^t} \rangle}$ be a ring with a positive integer t and β be a root of the irreducible polynomial $1+x+x^3+x^4+x^8$, and $\alpha = \beta^{2^t}$. Then, $D = bCirc(circ(1+\eta_1, \alpha+\eta_2),\ circ(\alpha^{-1}+\eta_3, \alpha+1+\eta_4))$ is an MDS matrix, where η_1, η_2, η_3 and $\eta_4 \in N(\mathcal{R}_t)$.*

Proof. The proof of this theorem follows from Lemma 13 and Theorem 15. □

Corollary 17. *In particular, if we take $\eta_1 = \eta_2 = \eta_3 = \eta_4 = \eta$ in Theorem 16, then $D^2 = \frac{1}{\alpha^2} I_4$.*

Proof. We have

$$D = \begin{bmatrix} 1+\eta & \alpha+\eta & \alpha^{-1}+\eta & 1+\alpha+\eta \\ \alpha+\eta & 1+\eta & 1+\alpha+\eta & \alpha^{-1}+\eta \\ \alpha^{-1}+\eta & 1+\alpha+\eta & 1+\eta & \alpha+\eta \\ 1+\alpha+\eta & \alpha^{-1} & \alpha+\eta & 1+\eta \end{bmatrix}. \text{ Then, we obtain}$$

$$D^2 = \begin{bmatrix} 1+\eta & \alpha+\eta & \alpha^{-1}+\eta & 1+\alpha+\eta \\ \alpha+\eta & 1+\eta & 1+\alpha+\eta & \alpha^{-1}+\eta \\ \alpha^{-1}+\eta & 1+\alpha+\eta & 1+\eta & \alpha+\eta \\ 1+\alpha+\eta & \alpha^{-1} & \alpha+\eta & 1+\eta \end{bmatrix} \begin{bmatrix} 1+\eta & \alpha+\eta & \alpha^{-1}+\eta & 1+\alpha+\eta \\ \alpha+\eta & 1+\eta & 1+\alpha+\eta & \alpha^{-1}+\eta \\ \alpha^{-1}+\eta & 1+\alpha+\eta & 1+\eta & \alpha+\eta \\ 1+\alpha+\eta & \alpha^{-1} & \alpha+\eta & 1+\eta \end{bmatrix}$$

$$= \begin{bmatrix} (1+\eta)^2+(\alpha+\eta)^2+ & 0 & 0 & 0 \\ (\alpha^{-1}+\eta)^2+(\alpha+1+\eta)^2 & & & \\ 0 & (1+\eta)^2+(\alpha+\eta)^2+ & 0 & 0 \\ & (\alpha^{-1}+\eta)^2+(\alpha+1+\eta)^2 & & \\ 0 & 0 & (1+\eta)^2+(\alpha+\eta)^2+ & 0 \\ & & (\alpha^{-1}+\eta)^2+(\alpha+1+\eta)^2 & \\ 0 & 0 & 0 & (1+\eta)^2+(\alpha+\eta)^2+ \\ & & & (\alpha^{-1}+\eta)^2+(\alpha+1+\eta)^2 \end{bmatrix}$$

$$= \begin{bmatrix} (\alpha^{-1})^2 & 0 & 0 & 0 \\ 0 & (\alpha^{-1})^2 & 0 & 0 \\ 0 & 0 & (\alpha^{-1})^2 & 0 \\ 0 & 0 & 0 & (\alpha^{-1})^2 \end{bmatrix} = (\alpha^{-1})^2 I = \frac{1}{\alpha^2} I.$$

□

Theorem 18. *Let $\mathcal{R}_t = \frac{\mathbb{F}_2[x]}{\langle(1+x+x^3+x^4+x^8)^{2^t}\rangle}$ be a ring and β be a root of the irreducible polynomial $1 + x + x^3 + x^4 + x^8$, and $\alpha = \beta^{2^t}$. Then, $D = bCirc(circ(1 + \eta_1, 1 + \eta_2, \alpha + \alpha^{-1} + \eta_3, \alpha + \eta_4), circ(1 + \alpha + \alpha^{-1} + \eta_1', 1+\alpha+\eta_2', \alpha^{-1}+\eta_3', \alpha+\alpha^{-1}+\eta_4'))$ is an MDS matrix, where $\eta_1, \eta_2, \eta_3, \eta_4, \eta_1', \eta_2', \eta_3'$ and $\eta_4' \in N(\mathcal{R}_t)$.*

Proof. The proof of this theorem is on similar lines as that of Lemma 13 and Theorem 15. □

Corollary 19. *If we take $\eta_1 = \eta_2 = \eta_3 = \eta_4 = \eta_1' = \eta_2' = \eta_3' = \eta_4'$ in Theorem 18, then $D^4 = (\alpha^4 + z)I$, for some $z \in N(\mathcal{R}_t)$.*

4. XOR count distribution of finite commutative rings of characteristic 2

In this section, we delve into the XOR count distribution for elements within two rings: $R_1 = \frac{\mathbb{F}_2[x]}{\langle(1+x^2+x^6)\rangle}$ and $R_2 = \frac{\mathbb{F}_2[x]}{\langle(1+x^4+x^6)\rangle}$. Employing a method delineated by Kesarwani et al. [18], which entails determining the XOR count of a local ring with characteristic 2. We apply the same method in finite fields to define the XOR count for elements within R_1 and R_2. For a more comprehensive understanding of XOR count, readers are encouraged to delve into the detailed discussions provided in [19]. Let us commence this section by outlining the definition of XOR count.

Definition 6. *[25, Definition 1] The XOR count of an element θ in the field $\mathbb{F}_{2^n}$ is the number of XORs required to implement the multiplication of θ with an arbitrary element β. XOR counts of all elements of $\mathbb{F}_{2^n}$ referred to as the XOR count distribution.*

We begin by outlining the procedure for computing the number of XOR operations needed to execute a multiplication by elements α^3 within the finite rings R_1 and R_2.

For ring $R_1 = \frac{\mathbb{F}_2[x]}{\langle(1+x^2+x^6)\rangle} = \{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4+a_5\alpha^5;\ where\ \alpha = x+\langle 1+x^2+x^6\rangle,\ a_i \in \mathbb{F}_2\}$. Consider the multiplication of α^3 with an arbitrary element $\beta = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4 + b_5\alpha^5$, where $b_i \in \mathbb{F}_2$, as

$$\begin{aligned}\alpha^3 \cdot (b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4 + b_5\alpha^5) &= b_0\alpha^3 + b_1\alpha^4 + b_2\alpha^5 + b_3\alpha^6 + b_4\alpha^7 + b_5\alpha^8\\ &= b_0\alpha^3 + b_1\alpha^4 + b_2\alpha^5 + b_3(1+\alpha^2) + b_4(\alpha\\ &\quad +\alpha^3) + b_5(\alpha^2+\alpha^4)\\ &= b_3 + b_4\alpha + (b_3+b_5)\alpha^2 + (b_0+b_4)\alpha^3\\ &\quad +(b_1+b_5)\alpha^4 + b_2\alpha^5.\end{aligned}$$

The product of α^3 and β can be expressed as

$$(b_3,\ b_4,\ b_3 \oplus b_5,\ b_0 \oplus b_4,\ b_1 \oplus b_5,\ b_2),$$

where there are three XOR operations. Consequently, the XOR count of the element α^3 in R_1 is 3.
For the ring $R_2 = \frac{\mathbb{F}_2[x]}{\langle(1+x^4+x^6)\rangle} = \{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4+a_5\alpha^5;\ where\ \alpha = x+\langle 1+x^4+x^6\rangle,\ a_i \in \mathbb{F}_2\}$. Consider the multiplication of α^3 with an arbitrary element $\beta = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4 + b_5\alpha^5$, where $b_i \in \mathbb{F}_2$ as

$$\begin{aligned}\alpha^3 \cdot (b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4 + b_5\alpha^5) &= b_0\alpha^3 + b_1\alpha^4 + b_2\alpha^5 + b_3\alpha^6 + b_4\alpha^7 + b_5\alpha^8\\ &= b_0\alpha^3 + b_1\alpha^4 + b_2\alpha^5 + b_3(1+\alpha^4) + b_4(\alpha\end{aligned}$$

$$
\begin{aligned}
& +\alpha^5) + b_5(\alpha^2 + 1 + \alpha^4) \\
= \; & (b_3 + b_5) + b_4\alpha + b_5\alpha^2 + b_0\alpha^3 + (b_1 + b_3 \\
& + b_5)\alpha^4 + (b_2 + b_4)\alpha^5.
\end{aligned}
$$

The product of α^3 and β takes the form

$$(b_3 \oplus b_5,\ b_4,\ b_5,\ b_0,\ b_1 \oplus b_3 \oplus b_5,\ b_2 \oplus b_4),$$

which contains four XORs. Hence, the XOR count for the element α^3 in R_2 is 4.

Then, we can calculate the number of XORs required for the multiplication of each element in rings R_1 and R_2 by using the same approach. Table 1 shows the number of XOR gates for each elements of the finite rings of order 2^6 defined by two reducible polynomials $(1 + x^2 + x^6)$ and $(1 + x^4 + x^6)$. The Magma computation system [3] is used to complete all of the computations in Table 1.

In Table 1, we observe that the sum of all XOR distributions of the elements in R_1 and R_2 amounts to 776 and 764, respectively. Our investigation aligns with the findings of Sarkar and Sim [25] in the realm of finite fields, where they demonstrate that there is no advantage in varying the choice of irreducible polynomials over $\mathbb{F}_2$. They proved that the total XOR count of elements in $\mathbb{F}_{2^n}$ remains constant, *i.e.*, $n\sum_{i=2}^{n}\binom{n}{i}(i-1)$. However, our exploration reveals a contrasting scenario: When employing two reducible polynomials of equal degree, distinct XOR distributions emerge. Specifically, in our investigation, we observe the XOR sums for the respective rings R_1 and R_2 to be 776 and 764.

Table 1. XOR count distribution table for the rings R_1 and R_2.

$R_1 = \frac{\mathbb{F}_2[x]}{\langle(1+x^2+x^6)\rangle} = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5;\ \alpha^6 = 1 + \alpha^2,\ a_i \in \mathbb{F}_2\}$,

$R_2 = \frac{\mathbb{F}_2[x]}{\langle(1+x^4+x^6)\rangle} = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5;\ \alpha^6 = 1 + \alpha^4,\ a_i \in \mathbb{F}_2\}$.

Total XOR count of $R_1 = 776$,

Total XOR count of $R_2 = 764$.

Elements	**XOR count of R_1**	**XOR count of R_2**	**Elements**	**XOR count of R_1**	**XOR count of R_2**
000000	0	0	000001	6	7
100000	0	0	100001	12	13
010000	1	1	010001	1	8
110000	7	7	110001	7	14
001000	2	2	001001	14	15
101000	8	4	101001	20	17
011000	9	9	011001	9	16
111000	15	11	111001	15	18
000100	3	4	000101	7	1
100100	9	10	100101	13	7
010100	8	3	010101	4	6
110100	14	9	110101	10	12
001100	11	12	001101	15	9
101100	17	14	101101	21	11
011100	16	11	011101	12	14
111100	22	13	111101	18	16
000010	4	6	000011	16	19
100010	2	8	100011	14	21
010010	11	13	010011	11	20
110010	9	15	110011	9	22
001010	8	2	001011	20	15
101010	6	8	101011	18	21
011010	15	9	011011	15	16
111010	13	15	000111	17	22
000110	13	16	100111	15	13
100110	11	18	010111	14	15
010110	18	15	110111	12	18
110110	16	17	001111	21	20
001110	17	12	101111	19	9
101110	15	8	011111	18	15
011110	22	11	111111	16	14
111110	20	17	011011	15	20

5. Examples

In this section, we present two examples of block circulant MDS matrices over the rings R_1 and R_2. Moreover, in connection with Theorem 15, we provide some additional MDS matrices.

Example 1. *Let $R_1 = \frac{\mathbb{F}_2[x]}{(\langle 1+x^2+x^6\rangle)}$ be a finite commutative ring of characteristic 2. By Lemma 13, we can say that R_1 contains a finite field of order 8. Let α be the root of the irreducible polynomial $1 + x + x^3$ over $\mathbb{F}_2$, and the matrix $A = bCirc(circ(1,\ \alpha),\ circ(1 + \alpha,\ 1 + \alpha^2))$. That is,*

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

is an MDS matrix, and $A^2 = (1+\alpha^4)I_4$. In Theorem 15, if we take $\eta_{ij} = \alpha^3 + \alpha + 1$ and $\eta'_{ij} = \alpha^5 + \alpha^4 + 1$, then we obtain two more MDS matrices A_1 and A_2, as follows:

$$A_1 = \begin{bmatrix} \alpha+\alpha^3 & 1+\alpha^3 & \alpha^3 & \alpha+\alpha^2+\alpha^3 \\ 1+\alpha^3 & \alpha+\alpha^3 & \alpha+\alpha^2+\alpha^3 & \alpha^3 \\ \alpha^3 & \alpha+\alpha^2+\alpha^3 & \alpha+\alpha^3 & 1+\alpha^3 \\ \alpha+\alpha^2+\alpha^3 & \alpha^3 & 1+\alpha^3 & \alpha+\alpha^3 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} \alpha^4+\alpha^5 & 1+\alpha+\alpha^4+\alpha^5 & \alpha+\alpha^4+\alpha^5 & \alpha^2+\alpha^4+\alpha^5 \\ 1+\alpha+\alpha^4+\alpha^5 & \alpha^4+\alpha^5 & \alpha^2+\alpha^4+\alpha^5 & \alpha+\alpha^4+\alpha^5 \\ \alpha+\alpha^4+\alpha^5 & \alpha^2+\alpha^4+\alpha^5 & \alpha^4+\alpha^5 & 1+\alpha+\alpha^4+\alpha^5 \\ \alpha^2+\alpha^4+\alpha^5 & \alpha+\alpha^4+\alpha^5 & 1+\alpha+\alpha^4+\alpha^5 & \alpha^4+\alpha^5 \end{bmatrix}.$$

Example 2. *Let $R_2 = \frac{\mathbb{F}_2[x]}{(\langle 1+x^4+x^6\rangle)}$ be a finite commutative ring of characteristic 2. In view of Lemma 13, we can say that R_2 contains a finite field of order 8. Let α be a root of the irreducible polynomial $1 + x + x^3$. Then, the matrix*

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

is an MDS matrix, and $A^2 = \alpha^4 I_4$. Moreover, if we take $\eta_{ij} = \alpha^3 + \alpha^2 + 1$ and $\eta'_{ij} = \alpha^5 + \alpha + 1$, in Theorem 15, then we obtain two MDS matrices B_1 and B_2. That is, we obtain

$$B_1 = \begin{bmatrix} \alpha^2+\alpha^3 & 1+\alpha+\alpha^2+\alpha^3 & \alpha+\alpha^2+\alpha^3 & 1+\alpha^3 \\ 1+\alpha+\alpha^2+\alpha^3 & \alpha^2+\alpha^3 & 1+\alpha^3 & \alpha+\alpha^2+\alpha^3 \\ \alpha+\alpha^2+\alpha^3 & 1+\alpha^3 & \alpha^2+\alpha^3 & 1+\alpha+\alpha^2+\alpha^3 \\ 1+\alpha^3 & \alpha+\alpha^2+\alpha^3 & 1+\alpha+\alpha^2+\alpha^3 & \alpha^2+\alpha^3 \end{bmatrix}$$

and

$$B_2 = \begin{bmatrix} \alpha+\alpha^5 & 1+\alpha^5 & \alpha^5 & 1+\alpha+\alpha^2+\alpha^5 \\ 1+\alpha^5 & \alpha+\alpha^5 & 1+\alpha+\alpha^2+\alpha^5 & \alpha^5 \\ \alpha^5 & 1+\alpha+\alpha^2+\alpha^5 & \alpha+\alpha^5 & 1+\alpha^5 \\ 1+\alpha+\alpha^2+\alpha^5 & \alpha^5 & 1+\alpha^5 & 1+\alpha+\alpha^2+\alpha^5 \end{bmatrix}.$$

5.1. XOR count of a matrix over finite commutative ring of characteristic 2

The XOR count of one row of a diffusion matrix can be computed using the following formula.

$$XOR \text{ count of one row} \quad = \quad \sum_{i=1}^{k} \gamma_i + (l-1) \cdot n, \tag{5.1}$$

where γ_i is the XOR count of the i-th entry in the row of the matrix, k is the order of the diffusion matrix, l is the number of nonzero coefficients in the row, and n is the dimension of vector space (see, [25] for more details).

Remark 1. *Using Eq (5.1) and Table 1, we calculate the XOR counts of matrices A, A_1, and A_2 in Example 1 to be 132, 212, and 264, respectively.*

Remark 2. *By employing Eq (5.1) and referring to Table 1, we compute the XOR counts for matrices B, B_1, and B_2 in Example 2 as 108, 256, and 256, respectively.*

6. Conclusions

In this paper, we studied the construction of block circulant MDS matrices over finite commutative rings with unity. Our investigation has delved into the determinant of such matrices, extending previous findings from finite fields to the ring R. Additionally, we explored conditions under which R contains a finite field of order 2^m, taking advantage of this discovery, we constructed block circulant MDS matrices of orders 4 and 8. To enhance the practical implementation of MDS matrices, we analyzed the XOR distribution within specific rings, including $R_1 = \frac{\mathbb{F}_2[x]}{\langle(1+x^2+x^6)\rangle}$ and $R_2 = \frac{\mathbb{F}_2[x]}{\langle(1+x^4+x^6)\rangle}$, providing the XOR counts distribution of these two rings. Furthermore, we presented some examples of MDS matrices alongside their corresponding XOR counts within the framework of finite commutative rings.

However, unlike previous research, our investigation has found that different XOR patterns appear when we use two reducible polynomials of the same degree. We specifically noticed different XOR distributions of rings R_1 and R_2, which are 776 and 764, respectively. This finding emphasizes how the choice of polynomials influences the way XOR behaves in specific mathematical scenarios involving certain types of rings. Our investigation has aligned with previous findings in the realm of finite fields, where they (cf.; [25]) demonstrated that there is no advantage in varying the choice of irreducible polynomials within $\mathbb{F}_{2^n}$, as they (cf.; [25]) proved that the total XOR count of elements in $\mathbb{F}_{2^n}$ remains constant.

The future work revolves around investigating the XOR count, particularly in relation to changes in the basis. We aim to determine whether altering the basis results in any modifications to the XOR distribution. Additionally, we seek to identify the conditions under which there is no variation in the XOR count distribution, particularly concerning reducible polynomials.

Author contributions

All authors have equally contributed. All authors have read and approved the final version of the manuscript for publication.

Acknowledgments

The authors thank to the anonymous reviewers for their valuable suggestions and comments which significantly improved both the quality and the presentation of this paper.

The authors extend their appreciation to Princess Nourah bint Abdulrahman University (PNU), Riyadh, Saudi Arabia, for funding this research under Researchers Supporting Project Number (PNURSP2024R231). A Substantial part of this work was done when the first and third authors were visiting Professor/Scientist at Department of Mathematics, Universitas Gadjah Mada (UGM), Indonesia (July, 2024) hosted by the Algebra Society of Indonesia and UGM. The first and third authors appreciate the gracious hospitality they received at UGM, Indonesia, during their visit. The research of the third author is financially supported by the University Grants Commission (UGC), Government of India (Ref. No.: 221610203798).

Conflicts of interest

The authors declare that they have no conflicts of interest.

References

1. I. Adhiguna, I. S. N. Arifin, F. Yuliawan, I. Muchtadi-Alamsyah, On orthogonal circulant MDS matrices, *Int. J. Math. Comput. Sci.*, **17** (2022), 1619–1637.
2. S. Ali, A. A. Khan, B. Singh, On circulant involutory and orthogonal MDS matrices over finite commutative rings, *Appl. Algebr. Eng. Comm.*, 2024. https://doi.org/10.1007/s00200-024-00656-4
3. W. Bosma, J. Cannon, *Handbook of Magma functions*, University of Sydney, 1995.
4. T. Cui, S. Chen, C. Jin, H. Zheng, Construction of higher-level MDS matrices in nested SPNs, *Inform. Sciences*, **554** (2021), 297–312. https://doi.org/10.1016/j.ins.2020.12.022
5. X. D. Dong, C. B. Son, E. Gunawan, Matrix characterization of MDS linear codes over modules, *Linear Algebr. Appl.*, **277** (1998), 57–61. https://doi.org/10.1016/S0024-3795(97)10073-8
6. S. T. Dougherty, *Algebraic coding theory over finite commutative rings*, Springer, 2017.
7. J. Jean, T. Peyrin, S. M. Sim, J. Tourteaux, Optimizing implementations of lightweight building blocks, *IACR T. Symmetric Cry.*, **4** (2017), 130–168. https://doi.org/10.46586/tosc.v2017.i4.130-168
8. D. Joan, V. Rijmen, The design of Rijndael: AES-the advanced encryption standard, *Inform. Secur. Cryptogr.*, 2002.
9. K. Khoo, T. Peyrin, A. Y. Poschmann, H. Yap, *FOAM: Searching for hardware optimal SPN structures and components with a fair comparison*, Springer, Berlin, Heidelberg, **16** (2014), 433–450. https://doi.org/10.1007/978-3-662-44709-3_24
10. P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schläffer, et al., *Grøstl-a SHA-3 candidate*, In: Dagstuhl Seminar Proceedings, Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2009.
11. F. D. Gazzoni, P. Barreto, V. Rijmen, *The Maelstrom-0 hash function*, In VI Brazilian Symposium on Information and Computer Systems Security, 2006.

12. J. Guo, T. Peyrin, A. Poschmann, The PHOTON family of lightweight hash functions, *Adv. Cry.-CRYPTO*, **6841** (2011), 222–239. https://doi.org/10.1007/978-3-642-22792-9_13
13. K. C. Gupta, I. G. Ray, *On constructions of involutory MDS matrices*, In Progress in Cryptology AFRICACRYPT, LNCS, Springer, Berlin, Heidelberg, **7918** (2013), 43–60. https://doi.org/10.1007/978-3-642-38553-7_3
14. K. C. Gupta, I. G. Ray, Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications, *Cryptogr. Commun.*, **7** (2014), 257–287. https://doi.org/10.1007/s12095-014-0116-3
15. K. C. Gupta, S. K. Pandey, I. G. Ray, S. Samanta, Cryptographically significant MDS matrices over finite fields: A brief survey and some generalized results, *Adv. Math. Commun.*, **13** (2019), 779–843. https://doi.org/10.3934/amc.2019045
16. H. Han, C. Tang, Y. Lou, M. Xu, Construction of efficient MDS matrices based on block circulant matrices for lightweight application, *Fund. Inform.*, **145** (2016), 111–124.
17. H. M. Heys, S. E. Tavares, *The design of substitution-permutation networks resistant to differential and linear cryptanalysis*, In Proceedings of the 2nd ACM Conference on Computer and Communications Security, 1994, 148–155.
18. A. Kesarwani, S. Pandey, S. Sarkar, A. Venkateswarlu, Recursive MDS matrices over finite commutative rings, *Discrete Appl. Math.*, **304** (2021), 384–396. https://doi.org/10.1016/j.dam.2021.08.016
19. L. Kölsch, *XOR counts and lightweight multiplication with fixed elements in binary finite fields*, Springer, Cham, **11476** (2019), 285–312. https://doi.org/10.1007/978-3-030-17653-2_10
20. J. Lacan, J. Fimes, Systematic MDS erasure codes based on Vandermonde matrices, *IEEE Commun. Lett.*, **8** (2004), 570–572. https://doi.org/10.1109/LCOMM.2004.833807
21. J. Philip, *Circulant matrices*, Wiley Press, New York, 1979.
22. A. R. Rao, P. Bhimasankaram, *Linear algebra*, 2 Eds., Hindustan Book Agency, 2000.
23. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, *The cipher SHARK*, In: Fast Software Encryption, LNCS, **1039** (1996), 99–111. https://doi.org/10.1007/3-540-60865-6_47
24. M. Sajadieh, M. Dakhilalian, H. Mala, P. Sepehrdad, *Recursive diffusion layers for block ciphers and Hash functions*, In: Fast Software Encryption, LNCS, Springer, Berlin, Heidelberg, **7549** (2012), 385–401.
25. S. Sarkar, S. M. Sim, *A deeper understanding of the XOR count distribution in the context of lightweight cryptography*, In Progress in Cryptology-AFRICACRYPT: 8th International Conference on Cryptology in Africa, Fes, Morocco, Springer International Publishing, **8** (2016), 167–182. https://doi.org/10.1007/978-3-319-31517-1_9
26. S. M. Sim, K. Khoo, F. Oggier, T. Peyrin, *Lightweight MDS involution matrices*, In Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, 2015.
27. S. Wu, M. Wang, W. Wu, *Recursive diffusion layers for (lightweight) block ciphers and hash functions*, In Selected Areas in Cryptography: 19th International Conference, Springer, Berlin, Heidelberg, 2013, 355–371. https://doi.org/10.1007/978-3-642-35999-6_23

AIMS Press