Sigma J Eng Nat Sci, Vol. 43, No. 3, pp. 955−961, June, 2025

Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2025.00083

Research Article

Applications of 4x4 involutive MDS matrix on finite fields F_{2^4}, F_{2^6}, F_{2^7}

Mehmet ÖZEN[1,*], Serra SAZOĞLU[1], Tuğçe TUFANÇLI[1], Osama A. NAJI[1]

[1]Department of Mathematics, Sakarya University, Sakarya, 54050, Türkiye

ARTICLE INFO

Article history
Received: 02 May 2024
Revised: 03 July 2024
Accepted: 08 July 2024

Keywords:
Cauchy Matrices; Hadamard Matrices; Involutive MDS Matrices; Lightweight Cryptology; Xor Numbers

ABSTRACT

In today's digital environment, a major amount of information is exchanged over insecure communication channels. In such an environment, cryptology plays a crucial role in ensuring that data is transmitted accurately and secure. Maximum distance separable (MDS) matrices which are derived from MDS codes, enhance the strength of cryptographic systems and contribute significantly to durability against different types of attacks. MDS matrices are widely used in the diffusion layers of lightweight block ciphers due to their easy usage and security. In addition, involutive MDS matrices with a minimum XOR number have lower costs and less memory because they allow the same matrix in encryption and decryption. For this reason, MDS matrices have been an area of interest. In this study, it is aimed to obtain 4*x*4 involutive MDS matrices on F_{2^4}, F_{2^6} and F_{2^7} finite fields that have not been studied before. After that, we have determined the matrices that have minimum XOR numbers. Thus, we have obtained 4*x*4 involutive MDS matrices with good properties to be used in block ciphers.

Cite this article as: Özen M, Sazoğlu S, Tufançli T, Naji OA. Applications of 4x4 involutive MDS matrix on finite fields F_{2^4}, F_{2^6}, F_{2^7}. Sigma J Eng Nat Sci 2025;43(3):955−961.

INTRODUCTION

Maximum Distance Separable (MDS) matrices have gained considerable interest, particularly because of their application in the diffusion layers of cryptographic algorithms. Their use enhance encryption strength and improve resistance against a wide range of cryptanalytic attacks [1]. Therefore, MDS matrices derived from MDS codes are used in most block ciphers such as Advanced Encryption Standard (AES) [2] and they are also used in hash functions such as Whirlpool [3], Photon family [4] and Whirlwind [5].

MDS matrices also prove the security of differential and linear cryptanalysis because block ciphers which use MDS matrix are secure. For this reason, it is important to find MDS matrices with good application properties [6]. On the other hand, MDS matrices have great advantages in block encryption. Thanks to involutive MDS matrices, lower costs are obtained by using the same matrix in encryption and decryption. In addition, one of these advantages is that involutive MDS matrices use less memory in encryption [7].

The methods of creating MDS matrices can be divided into two groups. These are direct creation methods and search-based methods. The first group includes methods based on Cauchy matrices [8], complementary matrices [4, 9], Vandermonde matrices [10, 11], abbreviated BCH codes [12, 13] and skew recursive structures [14]. The second

***Corresponding author.**
*E-mail address: ozen@sakarya.edu.tr

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

Published by Yıldız Technical University Press, İstanbul, Turkey

group consists of some interesting ideas. These are made using recursive structures [15, 16], hybrid structures [17] and special matrix forms [9, 18, 19]. There are hybrid methods (Generalized Hadamard Matrices) that combine direct generation methods with search-based methods. For one of the easiest construction methods that provides effectiveness, Hadamard matrices-like matrix forms are also used in circular and finite fields [6].

When examining methods for constructing MDS matrices, it is observed that the search-based approach requires verifying that all square submatrices of the generated matrix also satisfy the MDS property. This significantly increases the computational cost of the search process. Moreover, due to the vast search space for potential matrix elements, the practicality of this method becomes highly limited, particularly in environments with constrained system resources making it inefficient in terms of memory, speed, and overall performance under certain conditions. In contrast, the direct generation method enforces specific matrix structures and coding techniques to construct MDS matrices, thereby significantly reducing the search space and eliminating the need for an exhaustive search. However, when employing structured matrices such as Hadamard, Circulant, Toeplitz, or Circulant-like forms, additional search efforts are still required, as these forms do not inherently guarantee the MDS property. Consequently, despite their structural advantages, such matrices must still undergo verification processes to ensure they satisfy MDS criteria.

The GHadamard matrix represents a hybrid construction technique that incorporates Hadamard matrices—a class of structured matrices—within its substructure to directly generate new MDS matrices without requiring an exhaustive search. The motivation for employing Hadamard matrices lies in their crucial part in the construction of involutive MDS matrices. The classical definition of Hadamard matrices is extended and refined within the GHadamard framework [20], allowing for more flexible and efficient matrix generation. This study focuses on the construction of MDS matrices suitable for lightweight block ciphers. Specifically, we explore the concept of involutive MDS matrices, the XOR count as a performance metric, and two structured approaches: the Generalized Hadamard and the Cauchy-based Hadamard matrix forms. Subsequently, practical applications of these methods are discussed. Throughout the study, matrices are studied in $4x4$ dimensions due to ease of use and security in cryptology. Using the irreducible polynomial $x^4 + x + 1$ in the finite field F_{2^4}, a $4x4$ involutive MDS matrix is constructed with the Generalized Hadamard matrix form. The $4x4$ involutive MDS matrix on the finite field F_{2^8} was studied with different method [7]. In this study, $4x4$ involutive MDS matrices are constructed using the Generalized Hadamard matrix form and the Cauchy-based Hadamard matrix form over the finite fields F_{2^6} and F_{2^7}. For F_{2^6}, the irreducible polynomials $x^6 + x + 1$ and $x^6 + x^3 + 1$ are utilized, while for F_{2^7}, the polynomials $x^7 + x + 1$ and $x^7 + x^3 + 1$ are employed. These constructions demonstrate the applicability of both matrix forms across different field sizes and irreducible polynomial selections. Subsequently, we compute the XOR counts of the generated matrices, which serve as a measure of implementation efficiency. In certain applications, we derived novel $4x4$ involutive MDS matrices by applying isomorphisms to previously constructed matrices. This approach enabled us to evaluate and compare the XOR numbers of both the original and the newly derived matrices, offering insights into their relative computational efficiency.

Preliminaries

Some important properties of MDS matrices can be given by:

1. The square matrix of A is MDS if and only if every subframe matrix of A is regular (invertible).
2. The property of an MDS matrix is preserved in permutations of rows/columns. Similarly, multiplying a row/column by a non-zero $c \in F_2m$ does not affect its property of being MDS. In general, Let A be $kx(n-k)$ matrix, minimum distance d of $[n, k, d]$ C code whose generator matrix is $G = [I|A]$ is preserved after the above operations are applied to A [6].
3. The property of an MDS matrix is preserved under transpose processing [6].

Definition 1. Let A be a matrix. Matrices with $A.A=I$ or matrices whose inverse is equal to itself are called involutive matrices [7].

Definition 2. The $4x4$ involutive MDS matrix form given below is called Generalized Hadamard.

$$\begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix}$$

where $a_0, a_1, a_2, a_3, b_1, b_2, b_3 \in F_{2^r}\backslash\{0\}$ [7].

Definition 3. A Cauchy matrix C is a kxk matrix formed by two discrete sets of elements from $\{\alpha_0, \alpha_1, \dots, \alpha_{k-1}\}$ and $\{\beta_0, \beta_1, \dots, \beta_{k-1}\}$ such that $C[i,j] = \frac{1}{\alpha_i + a_j}$ over $GF(2^r)$ [21].

Proposition 4. Let $G = \{x_0, x_1, \dots, x_{n-1}\}$ be additive subgroup of F_{2^r}. Let $y_j = I + x_j$ be elements of G where $j = 0,1, \dots, n-1$ and for $I \notin G$, $I + G$ be a coset. Then for all $0 \le i, j \le n-1$, nxn matrix $A = (a_{i,j})$ is MDS matrixx such that $a_{i,j} = \frac{1}{x_i + y_j}$ [22].

Remark 5. If matrix A is an nxn matrix in the form specified in Proposition 1, matrix $c^{-1}A$ becomes an involutive MDS matrix such that c is the sum of elements in any row here [22].

Proposition 6. Let $H = (h_{i,j})$ be a $2^n x 2^n$ matrix and its first row is $(h_0, h_1, \dots, h_2n{-}1)$. In this case, H becomes Hadamard if and only if $h_{i,j} = h_{i \oplus j}$, where $i \oplus j$ is equal to the n-bit binary of i and j [22].

Remark 7. Let $G = \{x_0, x_1, \dots, x_{2^n-1}\}$ be additive subgroup of F_{2^r} and $x_i + x_j = x_{i\oplus j}$ where $i \oplus j$ is equal to the n-bit binary of i and j. Then, for $I \in \frac{F_{2^r}}{G}$, $H' = (h'_{i,j}) = \left(\frac{1}{I+x_{i\oplus j}}\right)$ is Hadamard [22].

Proposition 8. Let $G = \{x_0, x_1, \dots, x_{2^n-1}\}$ be additive subgroup of F_2r which is linear span of n linear independent elements $\{x_0, x_1, \dots, x_{2^n-1}\}$ such that $x_i = \sum_{k=0}^{n-1} i_k x_{2^k}$ where $i_{n-1}, \dots, i_1, i_0$ is binary representation of i. For $0 \le i \le 2^n - 1$ and $l \in F_2r/G$, let $y_i = l + x_i$. $A = (a_{i,j})$ matrix is a Hadamard MDS matrix where $a_{i,j} = \frac{1}{(x_i+y_j)}$ [22].

Proof. Let's consider the matrix $H = (h_{i,j}) = (x_i + x_j)$. Then, $h_{i,j} = x_{i\oplus j}$. From Proposition 2, H is Hadamard. So, $a_{i,j} = \frac{1}{(x_i+y_j)} = \frac{1}{(I+x_i+x_j)} = \frac{1}{I+x_{i\oplus j}}$. From Remark 2, A is Hadamard and from Proposition 1, A is MDS. Then A is Hadamard MDS matrix [22].

Remark 9. The matrix $\frac{1}{c}A$ is a Hadamard involutive MDS matrix where c is the sum of the elements in any row.

Definition 10. The XOR number of the α element over $\frac{GF(2^r)}{p(X)}$ is the number of XORs required to apply the multiplication of α with any β element on $\frac{GF(2^r)}{p(X)}$ [21].

For example; on the finite field $\frac{F_{2^6}}{x^6+x^3+1}$, let's take one element of the MDS matrix which is α. Since we are on F_{2^6} we should take polynomial of the fifth degree, then we multiply them:

$$\alpha(a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) = a_4\alpha^5 + a_3\alpha^4 + a_2\alpha^3 + a_1\alpha^2 + (a_5 + a_0)\alpha + a_5$$

When we look at the all coefficients, there is only one addition in the coefficient of the polynomial which is $a_5 + a_0$. Thus, this element of the MDS matrix have 1 XOR number. After finding XOR numbers of all elements of the MDS matrix, total XOR number is sum of the all of them.

APPLICATIONS OF 4*X*4 INVOLUTIVE MDS MATRIX OVER FINITE FIELDS F_{2^4}

Creating A 4*x*4 Involutive MDS Matrix Over Finite Field F_{2^4}

Example 11. Let's consider finite field $\frac{F_{2^4}}{x^4} + x + 1$. Let α be the root of $x^4 + x + 1$. Then,

$$M1 = Ghad(a_0, a_1, b_1, a_2, b_2, a_3, b_3) = Ghad(1, \alpha, \alpha^3 + \alpha, \alpha + 1, \alpha, 1, \alpha^2 + \alpha)$$

Let's create a 4*x*4 involutive MDS matrix.

$$M_1 = \begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & \alpha^2+\alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha \\ \alpha^3+\alpha+1 & 1 & \alpha^3+\alpha+1 & 1 \\ \alpha^3 & \alpha^2+1 & 1 & \alpha^2+\alpha \\ \alpha^2+\alpha+1 & \alpha^2+1 & \alpha^3+\alpha^2+\alpha & 1 \end{bmatrix}$$

where $b_1^{-1}.(\alpha^3 + \alpha) = 1 \Rightarrow b_1^{-1} = \alpha^6$, $b_2^{-1}.\alpha = 1 \Rightarrow b_2^{-1} = \alpha^{14}$, $b_3^{-1}.(\alpha^2 + \alpha) = 1 \Rightarrow b_3^{-1} = \alpha^{10}$. Total number of XORs = 66 + 4.3.4 = 114

Creating A 4*x*4 Involutive MDS Matrix Over Finite Field F_{2^6}

Example 12. F_{2^6} be defined by the irreducible polynomial $p_2(x) = x^6 + x^3 + 1$. Let $\alpha + 1$ be the root of the polynomial $p_2(x)$. Let $y_i = I + x_i$ and G be a additive subgroup where

$$G = \left\{\begin{matrix} x_0 = (\alpha+1)^2 = \alpha^2+1, x_1 = \alpha+1, x_2 = (\alpha+1)^3 = \alpha^3+\alpha^2+\alpha+1, \\ x_3 = (\alpha+1)^3 + (\alpha+1)^2 + \alpha + 1 = \alpha^3 + 1 \end{matrix}\right\}$$

Then the elements are $y_0 = \alpha^5 + \alpha^2 + \alpha + 1$, $y_1 = \alpha^5 + 1$, $y_2 = \alpha^5 + \alpha^3 + \alpha^2 + 1$, $y_3 = \alpha^5 + \alpha^3 + \alpha + 1$ for $0 \le i \le 3$, respectively. Accordingly, the Hadamard-Cauchy matrix can be constructed as follows:

$$M_1 = \begin{bmatrix} \frac{1}{x_0+y_0} & \frac{1}{x_0+y_1} & \frac{1}{x_0+y_2} & \frac{1}{x_0+y_3} \\ \frac{1}{x_1+y_0} & \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & \frac{1}{x_1+y_3} \\ \frac{1}{x_2+y_0} & \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & \frac{1}{x_2+y_3} \\ \frac{1}{x_3+y_0} & \frac{1}{x_3+y_1} & \frac{1}{x_3+y_2} & \frac{1}{x_3+y_3} \end{bmatrix}$$
$$= \begin{bmatrix} (\alpha+1)^3 & (\alpha+1)^{56} & (\alpha+1)^{19} & (\alpha+1)^{16} \\ (\alpha+1)^{56} & (\alpha+1)^3 & (\alpha+1)^{16} & (\alpha+1)^{19} \\ (\alpha+1)^{19} & (\alpha+1)^{16} & (\alpha+1)^3 & (\alpha+1)^{56} \\ (\alpha+1)^{16} & (\alpha+1)^{19} & (\alpha+1)^{56} & (\alpha+1)^3 \end{bmatrix}$$

But this matrix isn't involutive. To find involutive matrix from M_1, we have to calculate $\frac{1}{c}M_1$ where c is the sum of the elements of any row of the matrix or $c = \sum_{j=0}^{n-1} \frac{1}{I+x_i}$

$$c = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + \alpha^4 + \alpha + 1 = \alpha^5 + \alpha^2 = (\alpha + 1)^7$$

$$\frac{1}{c}.M_1 = \begin{bmatrix} (\alpha+1)^{59} & (\alpha+1)^{49} & (\alpha+1)^{12} & (\alpha+1)^9 \\ (\alpha+1)^{49} & (\alpha+1)^{59} & (\alpha+1)^9 & (\alpha+1)^{12} \\ (\alpha+1)^{12} & (\alpha+1)^9 & (\alpha+1)^{59} & (\alpha+1)^{49} \\ (\alpha+1)^9 & (\alpha+1)^{12} & (\alpha+1)^{49} & (\alpha+1)^{59} \end{bmatrix}$$

The matrix $\frac{1}{c}.M_1$ is 4x4 involutive Hadamard-Cauchy matrix over $\frac{F_{2^6}}{x^6+x^3+1}$. The number of XORs required for this matrix is 49 + 4.4.6 = 145.

Now let's look at the change in the XOR numbers of the matrices using isomorphism. Let's take the finite field $\frac{F_{2^6}}{p(x)}$ where $p(x) = (x^6 + x + 1)$. Let $\alpha = \beta + 1$ be the root of $p(x)$.

Is there any ${\alpha_1}^{s_1} = (\beta + 1)^{s_1}$ such that $p({\alpha_1}^{s_1}) = 0$. For $p_2(x) = x^6 + x^3 + 1$,

$$((\beta + 1)^7)^6 + (\beta + 1)^7)^3 + 1 = (\beta + 1)^{42} + (\beta + 1)^{21} + 1 = \beta^3 + \beta^3 + 1 + 1 = 0$$

Using the isomorphism $f_{7,1}$: $\alpha \rightarrow (\beta + 1)^7$, from the $\frac{1}{c}.M_1$ over the field $\frac{F_{2^6}}{p_2(x)}$, the matrix M_1' can be created over $\frac{F_{2^6}}{p_2(x)}$ as follows:

$$\frac{1}{c}.M_1 = \begin{bmatrix} (\alpha+1)^{59} & (\alpha+1)^{49} & (\alpha+1)^{12} & (\alpha+1)^{9} \\ (\alpha+1)^{49} & (\alpha+1)^{59} & (\alpha+1)^{9} & (\alpha+1)^{12} \\ (\alpha+1)^{12} & (\alpha+1)^{9} & (\alpha+1)^{59} & (\alpha+1)^{49} \\ (\alpha+1)^{9} & (\alpha+1)^{12} & (\alpha+1)^{49} & (\alpha+1)^{59} \end{bmatrix}$$

$$\xrightarrow{\alpha \rightarrow (\beta+1)^7} \begin{bmatrix} \beta^{35} & \beta^{28} & \beta^{21} & 1 \\ \beta^{28} & \beta^{35} & 1 & \beta^{21} \\ \beta^{21} & 1 & \beta^{35} & \beta^{28} \\ 1 & \beta^{21} & \beta^{28} & \beta^{35} \end{bmatrix}$$

The number of XORS required for this matrix is 39 + 4.3.6 = 111.

Example 13. F_{2^6} be defined by the irreducible polynomial $p(x) = (x^6 + x + 1)$. Let α be the root of the polynomial $p(x)$. The matrix $M_3 = Ghad(a_0, a_1, b_1, a_2, b_2, a_3, b_3) = Ghad(1, \alpha^{32}, \alpha^{32}, \alpha, \alpha, \alpha^{35}, \alpha^{34})$ is 4x4 involutive MDS matrix over $\frac{F_{2^6}}{p(x)}$.

$$M_3 = \begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^{64} & \alpha^{2} & \alpha^{69} \\ \alpha^{63} & 1 & \alpha^{67} & \alpha^{66} \\ \alpha^{63} & \alpha^{129} & 1 & \alpha^{128} \\ \alpha^{64} & \alpha^{62} & \alpha^{62} & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha & \alpha^{2} & \alpha^{6} \\ 1 & 1 & \alpha^{4} & \alpha^{3} \\ 1 & \alpha^{3} & 1 & \alpha^{2} \\ \alpha & \alpha^{62} & \alpha^{62} & 1 \end{bmatrix}$$

The number of XORs required for this matrix is 24 + 4.3.6 = 96.

Creating A 4x4 Involutive MDS Matrix Over Finite Field F_{2^7}

Example 14. F_{2^7} be defined by the irreducible polynomial $r(x) = x^7 + x^3 + 1$. Let α be the root of the polynomial $r(x)$. Let $G = \{x_0 = \alpha^2 + \alpha\ , x_1 = \alpha^3\ , x_2 = \alpha^4\ , x_3 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha\}$ be additive subgroup and $I = \alpha^6 + \alpha^5$. So, $y_0 = \alpha^6 + \alpha^5 + \alpha^2 + \alpha\ , y_1 = \alpha^6 + \alpha^5 + \alpha^3\ , y_2 = \alpha^6 + \alpha^5 + \alpha^4\ , y_3 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$ where $y_i = I + x_i$ for $0 \le i \le 3$.

$$M_4 = \begin{bmatrix} \frac{1}{x_0+y_0} & \frac{1}{x_0+y_1} & \frac{1}{x_0+y_2} & \frac{1}{x_0+y_3} \\ \frac{1}{x_1+y_0} & \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & \frac{1}{x_1+y_3} \\ \frac{1}{x_2+y_0} & \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & \frac{1}{x_2+y_3} \\ \frac{1}{x_3+y_0} & \frac{1}{x_3+y_1} & \frac{1}{x_3+y_2} & \frac{1}{x_3+y_3} \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^{91} & \alpha^{69} & \alpha^{37} & \alpha^{31} \\ \alpha^{69} & \alpha^{91} & \alpha^{31} & \alpha^{37} \\ \alpha^{37} & \alpha^{31} & \alpha^{91} & \alpha^{69} \\ \alpha^{31} & \alpha^{37} & \alpha^{69} & \alpha^{91} \end{bmatrix}$$

The matrix M_4 is Cauchy based Hadamard matrix but not involutive matrix. We can make the matrix involutive by dividing the matrix by $c = \sum_{j=0}^{n-1} \frac{1}{I+x_i}$ obtained or by c by summing the elements in any row of the matrix.

$$c = \alpha^5 + \alpha^2 + \alpha^6 + 1 + \alpha^5 + \alpha^2 + \alpha^3 + 1 + \alpha^6 + \alpha^3 + 1 + \alpha + 1 = \alpha$$

$$\frac{1}{c}M_4 = \begin{bmatrix} \alpha^{90} & \alpha^{68} & \alpha^{36} & \alpha^{30} \\ \alpha^{68} & \alpha^{90} & \alpha^{30} & \alpha^{36} \\ \alpha^{36} & \alpha^{30} & \alpha^{90} & \alpha^{68} \\ \alpha^{30} & \alpha^{36} & \alpha^{68} & \alpha^{90} \end{bmatrix}$$

The matrix is now the involutive MDS matrix. The number of XORS required for this matrix is 284 + 4.4.7 = 396.

Let's consider the finite field $F_{2^7}/q(x)$ where $q(x) = x^7 + x + 1$. Let β be the root of $q(x)$. Is there any $\beta^s u$ such that $r(\beta^s u) = 0$?

$$r(\beta^{11}) = (\beta^{11})^7 + (\beta^{11})^3 + 1 = \beta^{77} + \beta^{33} + 1 = \beta^5 + \beta^3 + \beta^2 + 1 + \beta^5 + \beta^3 + \beta^2 + 1 = 0$$

Using the isomorphism $f_{11,1}$: $\alpha \rightarrow \beta^{11}$, from the matrix $\frac{1}{c}M_4$ over the field $F_{2^7}/r(x)$, the 4x4 involutive Hadamard-Cauchy MDS matrix M_4' can be created over $F_{2^7}/q(x)$ as follows:

$$\frac{1}{c}M_4 = \begin{bmatrix} \alpha^{90} & \alpha^{68} & \alpha^{36} & \alpha^{30} \\ \alpha^{68} & \alpha^{90} & \alpha^{30} & \alpha^{36} \\ \alpha^{36} & \alpha^{30} & \alpha^{90} & \alpha^{68} \\ \alpha^{30} & \alpha^{36} & \alpha^{68} & \alpha^{90} \end{bmatrix}$$

$$\xrightarrow{\alpha \rightarrow \beta^{11}} \begin{bmatrix} (\beta^{11})^{90} & (\beta^{11})^{68} & (\beta^{11})^{36} & (\beta^{11})^{30} \\ (\beta^{11})^{68} & (\beta^{11})^{90} & (\beta^{11})^{30} & (\beta^{11})^{36} \\ (\beta^{11})^{36} & (\beta^{11})^{30} & (\beta^{11})^{90} & (\beta^{11})^{68} \\ (\beta^{11})^{30} & (\beta^{11})^{36} & (\beta^{11})^{68} & (\beta^{11})^{90} \end{bmatrix}$$

$$= \begin{bmatrix} \beta^{101} & \beta^{113} & \beta^{15} & \beta^{76} \\ \beta^{113} & \beta^{101} & \beta^{76} & \beta^{15} \\ \beta^{15} & \beta^{76} & \beta^{101} & \beta^{113} \\ \beta^{76} & \beta^{15} & \beta^{113} & \beta^{101} \end{bmatrix} = M_4'$$

The number of XOR required for this matrix is 87 + 4.4.7 = 199.

Example 15. Let's create a 4*x*4 involutive MDS matrix on F_{2^7} according to the generalized Hadamard matrix form. $a_0 = 1$, $a_1 = \alpha + 1$, $a_2 = \alpha^2 + \alpha$, $a_3 = \alpha^2 + 1$, $b_1 = \alpha$, $b_2 = \alpha^4 + \alpha$, $b_3 = \alpha^3 + \alpha + 1$, $b_1^{-1} = \alpha^{126} = \alpha^6 + 1$, $b_2^{-1} = \alpha^{63} = \alpha^3 + 1$, $b_3^{-1} = \alpha^{96} = \alpha^6 + \alpha^3 + \alpha$. Also, if $a_0 + a_1 + a_2 + a_3 = 1$, the matrix will be involutive. Since $1 + \alpha + 1 + \alpha^2 + \alpha + \alpha^2 + 1 = 1$, the matrix we create will be involutive.

$$M_5 = \begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^8 & \alpha^{72} & \alpha^{45} \\ \alpha^6 & 1 & \alpha^{77} & \alpha^{38} \\ \alpha^{71} & \alpha^{78} & 1 & \alpha^{101} \\ \alpha^{110} & \alpha^{105} & \alpha^{40} & 1 \end{bmatrix}$$

The total number of XORs required is 245 + 4.7.3 = 329.

RESULTS AND DISCUSSION

In this study, 4*x*4 involutive MDS matrices are created on finite fields $F_{2^7}, F_{2^6}, F_{2^4}$ and which have not been studied before, using the MDS creation methods found in the literature. Then, the number of XORs required for the created matrix is calculated. New MDS matrices are produced with the help of isomorphism from the new MDS matrix we created in some of our applications, and comparison was made by calculating the XOR numbers in these matrices. The 4*x*4 involutive MDS matrices with the lowest XOR number according to the generalized Hadamard form below have been obtained by writing the code given in the sample pseudo code in Algorithm 1 in the Magma Programming Language.

Over the finite field $F_{2^6}/x^6 + x^3 + 1$

$$\begin{bmatrix} \alpha & \alpha^5+\alpha^4+\alpha^2+\alpha+1 & \alpha^4+\alpha^2 & \alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1 \\ \alpha^5+\alpha^4+\alpha^3+\alpha+1 & \alpha & \alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1 & \alpha^2+1 \\ \alpha^4+\alpha^3+\alpha^2+\alpha+1 & \alpha^5+\alpha^2 & \alpha & \alpha^5+\alpha^4+\alpha^3+\alpha+1 \\ \alpha^5+\alpha^2 & 1 & \alpha^5+\alpha^4+\alpha^2+\alpha+1 & \alpha \end{bmatrix}$$

The XOR number is 154.

$$\begin{bmatrix} 1 & \alpha^5+\alpha^3 & \alpha^5 & \alpha^5+\alpha^4+\alpha^3+\alpha \\ \alpha^4+\alpha^3+\alpha+1 & 1 & \alpha^5+\alpha^2+\alpha+1 & \alpha^5+\alpha^3+1 \\ \alpha^3+\alpha^2+1 & \alpha^4 & 1 & \alpha^4+\alpha \\ \alpha^4+\alpha^3 & \alpha^5+\alpha^4+\alpha^3 & \alpha^5+\alpha^4+\alpha^3+\alpha^2 & 1 \end{bmatrix}$$

The XOR number is 140.

Over the finite field $F_{2^7}/x^7 + x^3 + 1$

$$\begin{bmatrix} \alpha & \alpha^6+\alpha^4+1 & \alpha^4+\alpha^2+\alpha+1 & \alpha^6+\alpha^3+\alpha^2+\alpha \\ \alpha^6+\alpha^2+1 & \alpha & \alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha & \alpha^4+1 \\ \alpha^6+\alpha & \alpha^6+\alpha^3+1 & \alpha & \alpha^6+\alpha^3+\alpha+1 \\ \alpha^5+\alpha^3+\alpha^2 & \alpha^5+\alpha^4+\alpha^2 & \alpha^6+\alpha^5+\alpha^3+\alpha^2+1 & \alpha \end{bmatrix}$$

The XOR number is 206.

$$\begin{bmatrix} 1 & \alpha^5+\alpha^3+\alpha^2 & \alpha^5+\alpha^4+\alpha+1 & \alpha^6+\alpha \\ \alpha^6+\alpha^5+\alpha^4+1 & 1 & \alpha^5+\alpha^2+\alpha & \alpha^6+\alpha^5+\alpha^3+\alpha \\ \alpha^6+\alpha^4+\alpha^2+\alpha & \alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha+1 & 1 & \alpha^3+\alpha+1 \\ \alpha^5+\alpha^4+\alpha & \alpha^5+\alpha^4+\alpha^2+\alpha+1 & \alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha+1 & 1 \end{bmatrix}$$

The XOR number is 205.

Algorithm 1 Finding MDS Matrix with Low XOR Number Over F_{2^6}/x^6+x^3+1

```
P < v >:= PolynomialRing(GF(2));
f := v^6 + v^3 + 1;
R < v >:= quo < P|f >;
    Elements of the finite field is defined:
Elemanlar := [[0]];
for α in R do
    if α ne 0 then
        Append(Elemanlar,α);
    end if
end for
    The inverses of invertible elements are defined:
function FindElementsInverse()
    element-inv:=[0];
    element:=[0];
    for u in R do
        if IsInverstible(u) then
            inverse:=u^-1;
            Append( elements,u);
            Append( element-inv,inverse);
        end if
    end for
        return element-inv;
        return elements;
endfunction;
    The MDS matrix is formed with the elements in R:
function Find-ai()
        for i in [1..4]  do
            a_i := [];
            for ai in R  do
                sonuc := (a0)^2 + (a1)^2 + (a2)^2 + (a3)^2;
                if sonuc eq 1  then
                    Append( a_i,ai);
                end if
            end for
            end for
            return a_i;
endfunction;

            xy1 := x1 * y1;
            xy2 := x2 * y2;
            xy3 := x3 * y3;
            xy11 := x1 * (y1)^-1;
            x3y12 := x3 * (y1)^-1 * y2;
            x2y13 := x2 * (y1)^-1 * y3;
            x2y21 := x2 * (y2)^-1;
            x3y211 := x3 * (y2)^-1 * y1;
            x1y213 := x1 * (y2)^-1 * y3;
            x3y31 := x3 * (y3)^-1;        10
            x3y311 := x3 * (y3)^-1 * y1;
            x1y312 := x1 * (y3)^-1 * y2;
A := Matrix (R, 4, 4, [[x0, xy1, xy2, xy3] , [xy11, x0, x3y12, x2y13]]) ,
[x2y21, x3y211, x0, x1y213] , [x3y31, x3y311, x1y312, x0];
    The XOR number of the matrix is calculated:
            R < a, b, c, d, e, f >?|= PolynomialRing(R, 6);
            f := a * v^5 + b * v^4 + c * v^3 + d * v^2 + e * v + f;
            S1 := [[]];
            for i in [1..4]  do
                for j in [1..4]  do
                    result := A [i] [j] * f;
                    Append( S1,result);
                end for
                end for
```

Figure 1. The algorithm of finding MDS matrices

CONCLUSION

In this study, it is aimed to obtain 4*x*4 involutive MDS matrices on F_{2^4}, F_{2^6} and F_{2^7} fields that have not been studied before. On the finite field F_{2^4}, using the irreducible polynomial $x^4 + x + 1$, a 4*x*4 involutive MDS matrix is built with the GHadamard matrix. Over the finite field F_{2^6}, 4*x*4 involutive MDS matrices are built using the GHadamard and Cauchy Hadamard matrix forms, based on the irreducible polynomials $x^6 + x + 1$ and $x^6 + x^3 + 1$. Similarly, within the field F_{2^7}, matrices were generated using the same matrix forms in conjunction with the irreducible polynomials $x^7 + x + 1$ and $x^7 + x^3 + 1$. Following the construction, the XOR numbers of the resulting matrices were computed to evaluate their implementation efficiency. In some cases, new 4*x*4 involutive MDS matrices were further derived through isomorphisms applied to the initial matrices. In particular, some of the matrices obtained via isomorphism performed lower XOR counts compared to their original matrices. Based on these results, the matrices with minimal XOR numbers were identified. Consequently, efficient 4*x*4 involutive MDS matrices with desirable cryptographic properties were obtained, making them suitable candidates for use in lightweight block cipher designs.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

REFERENCES

[1] Akkanat K. MDS yayılım matrislerinde izomorfizmalar üzerine yeni bir çalışma [master's thesis]. Edirne Edirne: Trakya University; 2017.

[2] Daemen J, Rijmen V. The design of Rijndael. Vol. 2. New York: Springer-Verlag; 2002. [CrossRef]

[3] Van Tilborg HC, Jajodia S, editors. Encyclopedia of cryptography and security. New York: Springer; 2014.

[4] Guo J, Peyrin T, Poschmann A. The PHOTON family of lightweight hash functions. In: Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference; 2011 Aug 14–18; Santa Barbara, CA. Berlin: Springer; 2011. p. 222–239. [CrossRef]

[5] Barreto P, Nikov V, Nikova S, Rijmen V, Tischhauser E. Whirlwind: a new cryptographic hash function. Des Codes Cryptogr 2010;56:141–162. [CrossRef]

[6] Sakalli MT, Akleylek S, Akkanat K, Rijmen V. On the automorphisms and isomorphisms of MDS matrices and their efficient implementations. Turk J Electr Eng Comput Sci 2020;28:275–287. [CrossRef]

[7] Otal K. A generalization of the subfield construction. Int J Inf Secur Sci 2022;11:1–11.

[8] Youssef AM, Mister S, Tavares SE. On the design of linear transformations for substitution permutation encryption networks. In: Workshop on Selected Areas of Cryptography (SAC'96); 1996. p. 40–48.

[9] Chand Gupta K, Ghosh Ray I. On constructions of circulant MDS matrices for lightweight cryptography. In: Information Security Practice and Experience: 10th International Conference, ISPEC 2014; 2014 May 5–8; Fuzhou, China. Berlin: Springer; 2014. p. 564–576. [CrossRef]

[10] Lacan J, Fimes J. Systematic MDS erasure codes based on Vandermonde matrices. IEEE Commun Lett 2004;8:570–572. [CrossRef]

[11] Sajadieh M, Dakhilalian M, Mala H, Omoomi B. On construction of involutory MDS matrices from Vandermonde matrices in GF (2^q). Des Codes Cryptogr 2012;64:287–308. [CrossRef]

[12] Augot D, Finiasz M. Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: Fast Software Encryption: 21st International Workshop, FSE 2014; 2014 Mar 3–5; London, UK. Berlin: Springer; 2015. p. 3–17. [CrossRef]

[13] Berger TP. Construction of recursive MDS diffusion layers from Gabidulin codes. In: International Conference on Cryptology in India; 2013. p. 274–285. [CrossRef]

[14] Cauchois V, Loidreau P, Merkiche N. Direct construction of quasi-involutory recursive-like MDS matrices from 2-cyclic codes. IACR Trans Symmetric Cryptol 2016:80–98. [CrossRef]

[15] Sajadieh M, Dakhilalian M, Mala H, Sepehrdad P. Recursive diffusion layers for block ciphers and hash functions. In: International Workshop on Fast Software Encryption; 2012. p. 385–401. [CrossRef]

[16] Wu S, Wang M, Wu W. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In: International Conference on Selected Areas in Cryptography; 2012. p. 355–371. [CrossRef]

[17] Sim SM, Khoo K, Oggier F, Peyrin T. Lightweight MDS involution matrices. In: Fast Software Encryption: 22nd International Workshop, FSE 2015; 2015 Mar 8–11; Istanbul, Turkey. Berlin: Springer; 2015. p. 471–493. [CrossRef]

[18] Li Y, Wang M. On the construction of lightweight circulant involutory MDS matrices. In: International Conference on Fast Software Encryption; 2016. p. 121–139. [CrossRef]

[19] Liu M, Sim SM. Lightweight MDS generalized circulant matrices (full version). Cryptol ePrint Arch 2016. [CrossRef]

[20] Pehlivanoğlu MK. Maksimum uzaklıkta ayrılabilen matrislerin elde edilebilmesi için yeni bir matris formu ve bir hafif sıklet blok şifreye uygulaması [PhD thesis]. Kocaeli (Turkey): Kocaeli Univ; 2018.

[21] Sim SM, Khoo K, Oggier F, Peyrin T. Lightweight MDS involution matrices. In: Fast Software Encryption: 22nd International Workshop, FSE 2015; 2015 Mar 8–11; Istanbul, Turkey. Berlin: Springer; 2015. p. 471–493. [CrossRef]

[22] Gupta KC, Pandey SK, Ray IG, Samanta S. Cryptographically significant MDS matrices over finite fields: a brief survey and some generalized results. Adv Math Commun 2019;13. [CrossRef]