# Generating efficient circulant-like MDS matrices for implementation

DOI: https://doi.org/10.54654/isj.v2i22.1049

**Tran Thi Luong*, Truong Minh Phuong**

***Abstract*— The exploration of maximal distance separable codes (MDS codes) has been a longstanding focus in error-correcting code theory and holds significant relevance in cryptography. Numerous approaches have been investigated for constructing MDS matrices, including deriving them from MDS codes, utilizing Hadamard matrices, Cauchy matrices, Vandermonde matrices, circulant matrices, circulant-like matrices, among others. However, a major challenge for cryptography designers is finding MDS matrices with low implementation cost. In this paper, we propose algorithms for generating efficient circulant-like MDS matrices of size $4 \times 4$, and $8 \times 8$ for implementation. Subsequently, we evaluate the fixed points, the number of XOR operations of the proposed MDS matrices, and compare them with MDS matrices of other well-known ciphers. These proposed MDS matrices can become promising candidates for many cryptographic algorithms in the future.**

***Tóm tắt*— Việc sử dụng các mã tách có khoảng cách cực đại (mã MDS) đã là một trọng tâm lâu dài trong lý thuyết mã sửa sai và có ý nghĩa quan trọng trong mật mã học. Nhiều phương pháp đã được nghiên cứu để xây dựng các ma trận MDS, bao gồm việc xây dựng từ mã MDS, sử dụng các ma trận Hadamard, ma trận Cauchy, ma trận Vandermonde, ma trận dịch vòng, ma trận tựa vòng và những phương pháp khác. Tuy nhiên, một thách thức lớn đối với các nhà thiết kế mật mã là tìm ra các ma trận MDS có chi phí thực thi thấp. Trong bài báo này, nhóm tác giả đề xuất các thuật toán để tạo ra các ma trận MDS tựa vòng hiệu quả cho thực thi cỡ $4 \times 4$ và $8 \times 8$. Sau đó sẽ đánh giá số điểm bất động, số phép XOR của các ma trận MDS được đề xuất và so sánh chúng với các ma trận MDS của các mã nổi tiếng khác. Những ma trận MDS được đề xuất này có thể trở thành những ứng viên tiềm năng cho nhiều thuật toán mật mã trong tương lai.**

***Keywords*— component; formatting; style; insert.**

***Từ khóa*— các phần; định dạng; kiểu; chèn.**

## I. INTRODUCTION

MDS matrices [1, 2] play a crucial role in various areas of mathematics and computer science, particularly in the field of error-correcting codes and cryptography. In the realm of cryptography, MDS matrices find applications in the design of block ciphers [4, 5] and hash functions [6, 7]. These matrices are employed in the diffusion layer of block ciphers, contributing to the spread and mixing of input data to enhance security against various cryptographic attacks. The study and development of MDS matrices remain an active area of research, with implications for enhancing the reliability and security of communication systems, data storage, and information transmission in various technological domains.

Researchers continually explore novel methods for generating efficient MDS matrices with lower implementation costs to improve the performance and security of cryptographic algorithms. Currently, there are several commonly used methods for constructing MDS matrices, such as Hadamard matrices [8, 9], Vandermonde matrices [10], Cauchy matrices [11, 12], recursive MDS matrices [13, 14], Circulant matrices [15-18], circulant-like matrix [2, 19, 20].

The methods constructed from Hadamard [28] matrices are of significant interest because these matrices have the advantage of having

The paper was reviewed, accepted and introduced by the XXVII National Conference "Some Selected Issues on Information and Communication Technology" to be published in the Journal on September 10, 2024, revised on September 17, 2024 and accepted on September 29, 2024.

* Corresponding author

some distinct elements in the matrix, small equal to the size of the matrix. On the other hand, they can be self-inverse, making them highly advantageous for implementation. With construction methods based on Cauchy and Vandermonde matrices, their advantage lies in the ability to build large-sized MDS matrices. However, the elements in these matrices often have high Hamming weights, leading to increased implementation costs. Recursive matrices have the advantage of saving implementation costs in hardware as they can utilize very sparse companion matrices.

Matrices with properties resembling circulants and circulant-like were initially introduced by P. Junod and colleagues in their publication presented at the Selected Areas in Cryptography (SAC) conference in 2004 [2]. Circulant matrices and circulant-like matrices have the advantage of having a small number of distinct elements and can potentially contain a large number of ones, making them effective in implementation.

In [15], the researchers introduced effective circulant MDS matrices tailored for lightweight cryptography. They delved into the advantageous and intriguing characteristics of circulant matrices following the structure $B^k = I$. Regrettably, certain findings in [15] proved to be inaccurate, notably the suggested efficient circulant matrices with a size of 8, which were not MDS matrices. In [16], the authors provided a fresh algebraic demonstration outlining the absence of circulant involutory MDS matrices when working within fields of characteristic 2. For characteristics of an odd nature, they delineated parameters that might allow for potential existence. By extending the notion from circulance to θ-circulance, the limitations on the existence of θ-circulant involutory MDS matrices were eliminated, even within fields of characteristic 2. Ultimately, they expanded the definition of involutory and introduced a novel direct approach to constructing nearly involutory θ-circulant MDS matrices. In [17], the researchers calculated the reciprocal of circulant matrices with dimensions $2^n \times 2^n$, where the entries belong to the $GF(2^m)$, and this holds true for cases where $n \geq 3$. The computational process initiates with a software application that produces the cofactors of an $8 \times 8$ circulant matrix. Building upon these findings, the recursive construction of a circulant matrix's inverse becomes feasible. In [18], the researchers established the absence of specific orthogonal circulant MDS matrices. Following this, they provided a condition that is both necessary and sufficient for orthogonal θ-circulant matrices, employing $q$-polynomial rings. Furthermore, they delved into the exploration of orthogonal circulant MDS matrices across Galois rings.

In [19], the researchers introduced effective MDS matrices with a circulant-like structure in both $4 \times 4$ and $8 \times 8$ dimensions. They referred to these matrices as Type-I circulant-like matrices. They demonstrated that circulant-like MDS matrices of size $l \times l$ cannot possess involution or orthogonality properties, which are advantageous for designing SPN networks. Despite the efficiency of these matrices, there is no guarantee that their inverses will also be efficient. The authors investigated the creation of $2l \times 2l$ involutory MDS matrices, commencing with a $l \times l$ submatrix that is itself an MDS matrix. They regarded the $l \times l$ submatrix as circulant MDS matrices. They presented proof indicating the absence of circulant-like MDS matrices of size $2l \times 2l$ when $l$ is an even number. In [20], a novel category of matrices resembling circulants was introduced by the authors. These matrices possess involutory characteristics by design, denoted as Type-II circulant-like matrices. Their investigation delved into the MDS attributes of $l \times l$ circulant matrices, as well as Type-I and Type-II circulant-like matrices, leading to the development of new, efficient MDS matrices tailored for lightweight cryptography, particularly when $l$ is limited to 8. Additionally, the study encompassed the exploration of orthogonal and involutory features of such matrices, aiming to create MDS matrices with both efficient computation and inverse properties. The authors also examined the compelling properties of

circulant matrices, Type-I, and Type-II circulant-like matrices, unveiling insights applicable across diverse realms of mathematics and computer science.

Unfortunately, when we examined the proposed Type-I circulant-like MDS matrices of size $4 \times 4$ and $8 \times 8$ in [19, 20], these matrices did not satisfy the conditions of being MDS matrices.

MDS matrices [27, 29, 30] with maximum branches [21, 22] enable them to achieve maximum diffusion capability. Additionally, the number of fixed points [23] is also a crucial criterion for MDS matrices as it can impact the security of future cryptographic algorithms. The aforementioned works propose the construction of circulant or circulant-like matrices; however, they have not addressed the matrices' fixed point counts.

In this paper, we propose algorithms for generating efficient circulant-like MDS matrices of size $4 \times 4$ and $8 \times 8$ for implementation. Subsequently, we evaluate the fixed points, and the number of XOR operations of the proposed MDS matrices, and compare them with MDS matrices of other well-known ciphers. These proposed MDS matrices can become promising candidates for many cryptographic algorithms in the future.

The structure of the paper is outlined as follows. Section 2 provides the preliminaries. Section 3 introduces algorithms for producing effective circulant-like MDS matrices for practical use. The experimental outcomes and comparative analyses are detailed in Section 4. Finally, Section 5 encapsulates the conclusions.

## II. PRELIMINARIES

### *A. Circulant-like MDS matrix*

The MDS matrices are derived from the principles of error correction codes [24], specifically using codes with maximal distance separable or MDS properties. Observing the MDS matrix reveals its unique nature, characterized by the property that every square sub-matrix is invertible.

Definition 1 [24]. A matrix is an MDS matrix if and only if every sub-matrix is non-singular.

Circulant and Type-I circulant-like matrices are defined as follows.

Definition 2 [26]. The matrix of size $n \times n$ represented as

$$\begin{bmatrix} b_0 & b_1 & \cdots & b_{n-1} \\ b_{n-1} & b_0 & \cdots & b_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ b_1 & b_2 & \cdots & b_0 \end{bmatrix}$$

is termed a circulant matrix and denoted as $Circ(b_0, \ldots, b_{n-1})$.

Definition 3. (Type-I circulant-like Matrix) [2,19].

The matrix of size $m \times m$*:*

$$\begin{bmatrix} b & 1 \\ 1^T & B \end{bmatrix}$$

is referred to as a Type-I circulant-like matrix, where $B = Circ(1, b_1, \ldots, b_{m-2})$, $1 = \underbrace{(1, \ldots, 1)}_{m-1\ times}$, $1$ represents the unit element, and $b_i$*'s* and $b$ are any nonzero elements of the underlying field other than 1.

Example. Choosing $b = 02$, $B = Circ(02, 01, 03)$, we have a Type-I circulant-like matrix of size 4 as follows.

Selecting $b = 02$, and $B = Circ(02, 01, 03)$, results in the creation of a $4 \times 4$ Type-I circulant-like matrix.

$$B = \begin{bmatrix} 02 & 01 & 01 & 01 \\ 01 & 02 & 01 & 03 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{bmatrix}$$

A circulant-like matrix that satisfies the MDS condition is referred to as a circulant-like MDS matrix.

### *B. Introduction to Fixed Points and XOR Operations*

A fixed point [23] of a linear transformation $T: GF(2^q)^n \to GF(2^q)^n$ with the representation non-singular matrix $B = [b_{i,j}]_{m \times m}$ over $GF(2^q)$ is the vector $X$ satisfies: $B.X = X$. This means that when $X$ undergoes the linear transformation $T$, it remains unchanged, without any alteration.

There is no diffusion at the fixed points because the linear layer does not affect these input blocks. Therefore, an attacker can exploit this vulnerability to easily conduct a straightforward plaintext attack. In practice, the expected number of fixed points for a linear transformation is 1 since $B.0 = 0$ always holds.

It can be observed that the number of XOR operations is a simple and manageable metric. However, the coefficients of MDS matrices are often chosen to have a small number of XOR operations, for instance, with low Hamming weight. As highlighted in [25], a small number of XOR operations significantly reduces hardware area. On the other hand, when MDS matrices have a small number of XOR operations, it also enhances the software execution speed.

Definition 4. The XOR count of an element α in the field $GF(2^q)/g(X)$ is the number of XOR operations required to perform the multiplication of α with any given element $\beta$ in $GF(2^q)/g(X)$.

## III. PROPOSING ALGORITHMS FOR EFFICIENT GENERATION OF TYPE-I CIRCULANT-LIKE MATRICES FOR IMPLEMENTATION

In this section, we present two algorithms for the efficient generation of Type-I circulant-like MDS matrices for implementation, with sizes $4 \times 4$ and $8 \times 8$.

We select the elements of these matrices from the sets $\{0x01, \dots, 0x07\}$ and $\{0x01, \dots, 0x09\}$ because these elements have low Hamming weight and they have a lower number of XOR operations compared to other elements in the field $GF(2^8)$, resulting in low implementation costs. Therefore, this contributes to making the XOR operations of the obtained matrices small.

Consider a Type-I circulant-like matrix of size $4 \times 4$ in the following form.

$$\begin{pmatrix} m_0 & 01 & 01 & 01 \\ 01 & 01 & m_1 & m_2 \\ 01 & m_2 & 01 & m_1 \\ 01 & m_1 & m_2 & 01 \end{pmatrix} \quad (1)$$

where $m_0, m_1, m_2 \in \{0x01, \dots, 0x07\}$

Algorithm 1. Generate efficient $4 \times 4$ Type-I circulant-like matrices for implementation

Input: An empty $4 \times 4$ matrix $M$ over $GF(2^8)$; Set $\mathcal{J}$ consists of a list of elements in the form $(m_0, m_1, m_2)$, $\mathcal{J} = \emptyset$.

Output: Efficiently implementable Type-I circulant-like MDS matrices of size $4 \times 4$ with elements from $GF(2^8)$.

Step 1: Generate matrix $M$ in the form of a Type-I circulant-like matrix as shown in (1) with 3 symbolic elements $m_i \in GF(2^8), 0 \le i \le 2$.

Step 2: Choose a combination of three elements $(m_0, m_1, m_2)$ for $m_i \in \{0x01, \dots, 0x07\}$ $(0 \le i \le 2)$.

Step 3: In case the tuple $(m_0, m_1, m_2)$ is not part of $\mathcal{J}$, then:

- Fill in these elements into matrix $M$.

- Check if the obtained matrix $M$ is MDS.

+ If this statement holds, store the matrix $M$ in the file and add this tuple $(m_0, m_1, m_2)$ to $\mathcal{J}$.

Step 4: If $|\mathcal{J}| < 343$, return to Step 2.

Return: File of Type-I circulant-like MDS matrices of size $4 \times 4$ with elements in set $\{0x01, \dots, 0x07\}$.

Remark 1. Algorithm 1 is executed when all possibilities of $(m_0, m_1, m_2)$ for $m_i \in \{0x01, \dots, 0x07\}$, $(0 \le i \le 2)$ have been exhausted. In this case, the number of Type-I circulant-like matrices to be checked is 343.

Note that the MDS property of the matrices in Algorithm 1 and Algorithm 2 is verified according to Definition 1. We developed a custom program to check whether all submatrices of any given input matrix have non-zero determinants.

For Type-I circulant-like matrices of size $8 \times 8$, to find efficient matrices for execution with many 1's, we examine these matrices as follows:

$$\begin{pmatrix} m_0 & 01 & 01 & 01 & 01 & 01 & 01 & 01 \\ 01 & 01 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ 01 & m_6 & 01 & m_1 & m_2 & m_3 & m_4 & m_5 \\ 01 & m_5 & m_6 & 01 & m_1 & m_2 & m_3 & m_4 \\ 01 & m_4 & m_5 & m_6 & 01 & m_1 & m_2 & m_3 \\ 01 & m_3 & m_4 & m_5 & m_6 & 01 & m_1 & m_2 \\ 01 & m_2 & m_3 & m_4 & m_5 & m_6 & 01 & m_1 \\ 01 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & 01 \end{pmatrix} \quad (2)$$

Where $m_0, m_1, \dots, m_6 \in \{0x01, \dots, 0x09\}$.

Algorithm 2. Generate efficient $8 \times 8$ Type-I circulant-like matrices for implementation

Input: An empty matrix $M$ of size $8 \times 8$ over $GF(2^8)$; Set $\mathcal{J}$ consisting of a list of tuples $(m_0, m_1, \dots, m_6)$, $\mathcal{J} = \emptyset$.

Output: Efficiently implementable Type-I circulant-like MDS matrices of size $8 \times 8$ with elements from $GF(2^8)$.

Step 1: Generate matrix $M$ in the form of a Type-I circulant-like matrix as shown in (2) with 7 symbolic elements $m_i \in GF(2^8), 0 \leq i \leq 6$.

Step 2: Choose a combination of seven elements $(m_0, m_1, \dots, m_6)$ for $m_i \in \{0x01, \dots, 0x09\}$ $(0 \leq i \leq 6)$.

Step 3: In case the tuple $(m_0, m_1, \dots, m_6)$ is not part of $\mathcal{J}$, then:

- Fill in these elements into matrix $M$.

- Check if the obtained matrix $M$ is MDS.

+ If this statement holds, store the matrix $M$ in the file and add this tuple $(m_0, m_1, \dots, m_6)$ to $\mathcal{J}$.

Step 4: If $|\mathcal{J}| < 4{,}782{,}969$, return to Step 2.

Return: File of Type-I circulant-like MDS matrices of size $8 \times 8$ with elements in set $\{0x01, \dots, 0x09\}$.

Remark 2. Algorithm 2 is executed when all possibilities of $(m_0, m_1, \dots, m_6)$ for $m_i \in \{0x01, \dots, 0x09\}$, $(0 \leq i \leq 6)$ have been exhausted. In this case, the number of Type-I circulant-like matrices to be checked is $4{,}782{,}969$.

The experimental section is presented in Section 4.

## IV. EXPERIMENT AND COMPARISON

Conducting experiments with Algorithm 1 and Algorithm 2 with C using a computer configured as follows: VivoBook_ASUSLaptop X513EP_X515EP (Core i5-10210U, 8GB RAM).

For Algorithm 1, the input data is an empty $4 \times 4$ Type-I circulant-like matrix over the field $GF(2^8)$ with the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$.

For Algorithm 2, the input data is an empty $8 \times 8$ Type-I circulant-like matrix over the field $GF(2^8)$ with the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$.

For calculating the number of XOR operations for the matrices, we based our approach on Definition 4 and the method for calculating the number of XOR operations outlined in [25].

After experimenting to find a set of Type-I circulant-like MDS matrices of size $4 \times 4$ from Algorithm 1 and $8 \times 8$ matrices from Algorithm 2, we proceeded to calculate the fixed points of these matrices. Then, we selected only those matrices with exactly one fixed point. Subsequently, we calculated the number of XOR operations for each obtained matrix and chose matrices with the minimum number of XOR operations among them. The summarized results are presented in Table 1.

After the experimental process, we obtained two Type-I circulant-like MDS matrices of size $4 \times 4$ with a minimum XOR count of 147. These matrices are presented in Table 2. For the $8 \times 8$ matrices, we obtained six Type-I circulant-like MDS matrices with a minimum XOR count of 948. These matrices are presented in Table 3.

TABLE 1. SUMMARY OF THE NUMBER OF EFFECTIVE TYPE-I CIRCULANT-LIKE MDS MATRICES OBTAINED

| **Type of Matrix** | ***Total matrices in the search space*** | ***Run time*** | ***Number of obtained MDS matrices*** | ***Number of MDS matrices with a fixed point count of 1*** | ***Number of matrices with the minimum XOR count*** |
|---|---|---|---|---|---|
| Circulant-like matrices of size $4 \times 4$ | $7^3 = 343$ | 4,6 minutes | 71 | 71 | 2 (with XOR count = 147) |
| Circulant-like matrices of size $8 \times 8$ | $9^7 = 4{,}782{,}969$ | 102,2 hours | 24 | 24 | 6 (with XOR count =948) |

From the results obtained in Table 2, we proceed to compare our proposed circulant-likeMDS matrices of size $4 \times 4$ with MDS matrices from some well-known codes. Table 4 presents the comparison of $4 \times 4$ MDS matrices, while Table 5 compares their inverses.

TABLE 2. TWO PROPOSED TYPE-I CIRCULANT-LIKE MDS MATRICES OF SIZE $4\times4$ WITH THE MINIMUM XOR COUNT FOR THE PRIMITIVE POLYNOMIAL $X^8 + X^4 + X^3 + X^2 + 1$

| **No.** | ***Set*** $(m_0, m_1, m_2)$ | ***Type-I Circulant-Like Matrix*** $(4 \times 4)$ | ***Number of Fixed Points*** | ***Number of XORs*** |
|---|---|---|---|---|
| 1 | (02,02,06) | $A_1 = \begin{bmatrix} 02 & 01 & 01 & 01 \\ 01 & 01 & 02 & 06 \\ 01 & 06 & 01 & 02 \\ 01 & 02 & 06 & 01 \end{bmatrix}$ | $2^0$ | 147 |
| 2 | (02,06,02) | $A_2 = \begin{bmatrix} 02 & 01 & 01 & 01 \\ 01 & 01 & 06 & 02 \\ 01 & 02 & 01 & 06 \\ 01 & 06 & 02 & 01 \end{bmatrix}$ | $2^0$ | 147 |

TABLE 3. SIX PROPOSED TYPE-I CIRCULANT-LIKE MDS MATRICES OF SIZE $8 \times 8$ WITH THE MINIMUM XOR COUNT FOR THE PRIMITIVE POLYNOMIAL $X^8 + X^4 + X^3 + X^2 + 1$

| **No.** | **Set** $(m_0, m_1, \dots, m_6)$ | **Type-I Circulant-Like Matrix** $(8 \times 8)$ | **Number of Fixed Points** | **Number of XORs** |
|---|---|---|---|---|
| 1 | (2,9,7,6,3,2,4) | $\begin{bmatrix} 2 & 1 \\ 1^T & Circ(1,9,7,6,3,2,4) \end{bmatrix}$ | $2^0$ | 948 |
| 2 | (2,3,9,2,7,4,6) | $\begin{bmatrix} 2 & 1 \\ 1^T & Circ(1,3,9,2,7,4,6) \end{bmatrix}$ | $2^0$ | 948 |
| 3 | (2,2,6,9,4,3,7) | $\begin{bmatrix} 2 & 1 \\ 1^T & Circ(1,2,6,9,4,3,7) \end{bmatrix}$ | $2^0$ | 948 |
| 4 | (2,7,3,4,9,6,2) | $\begin{bmatrix} 2 & 1 \\ 1^T & Circ(1,7,3,4,9,6,2) \end{bmatrix}$ | $2^0$ | 948 |
| 5 | (2,6,4,7,2,9,3) | $\begin{bmatrix} 2 & 1 \\ 1^T & Circ(1,6,4,7,2,9,3) \end{bmatrix}$ | $2^0$ | 948 |
| 6 | (2,4,2,3,6,7,9) | $\begin{bmatrix} 2 & 1 \\ 1^T & Circ(1,4,2,3,6,7,9) \end{bmatrix}$ | $2^0$ | 948 |

TABLE 4. COPARISONS OF PROPOSED TYPE-I CIRCULANT-LIKE MATRICES OF SIZE $4 \times 4$ WITH OTHER ONES

| **MDS matrices of size $4 \times 4$ ($A$)** | **Primitive polynomial** | **Number of Fixed Points** | **Number of XORs** |
|---|---|---|---|
| Circ[0xc4,0x65,0xc8,0x8b] (Hierocrypt block cipher) | $x^8 + x^6 + x^5 + x + 1$ | $2^0$ | 448 |
| Circ [0x2, 0x3, 0x1, 0x1] (AES block cipher) | $x^8 + x^4 + x^3 + x + 1$ | $2^{16}$ | 152 |
| $\begin{bmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{bmatrix}$ (Twofish block cipher) | $x^8 + x^6 + x^5 + x + 1$ | $2^0$ | 444 |
| Type-I circulant-like MDS matrices of size $4 \times 4$ in [19, 20] | They all not satisfy the conditions to be MDS matrices for the primitive polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$ in [19] and the primitive polynomial $x^8 + x^4 + x^3 + x + 1$ in [20] | | |
| Our two proposed Type-I circulant-like matrices of size $4 \times 4$ (Table 2) | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 147 |

Looking at Table 4, it can be observed that the two proposed Type-I circulant-like MDS matrices of size $4 \times 4$ in Table 2 (matrices $A_1$ and $A_2$) have the smallest and best possible number of fixed points, while the fixed-point count of AES is $2^{16}$, which is quite high and may affect security. Additionally, the number of XOR operations for our proposed matrices is smaller compared to matrices from Hierocrypt, AES, and Twofish when calculated using the same method. Therefore, it can be stated that our proposed $4 \times 4$ MDS matrices are very promising.

TABLE 5. COMPARISON OF $4 \times 4$ INVERSE MDS MATRICES

| **Inverse MDS matrices of size $4 \times 4$ ($A^{-1}$)** | **Primitive polynomial** | **Number of Fixed Points** | **Number of XORs** |
|---|---|---|---|
| $A^{-1}$ =Circ[0x82, 0xc4, 0x34, 0xf6], Inverse of the matrix Circ[0xc4,0x65,0xc8,0x8b] **(Hierocrypt block cipher)** | $x^8 + x^6 + x^5 + x + 1$ | $2^0$ | 520 |
| $A^{-1}$ =Circ[0xe, 0xb, 0xd, 0x9], Inverse of the matrix Circ [0x2, 0x3, 0x1, 0x1] **(AES block cipher)** | $x^8 + x^4 + x^3 + x + 1$ | $2^{16}$ | 440 |
| $A^{-1} = \begin{bmatrix} 63 & 7E & 6B & 92 \\ D2 & 6B & F5 & D1 \\ 75 & 92 & D1 & FE \\ AB & 63 & D2 & 75 \end{bmatrix}$ Inverse of the matrix $\begin{bmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{bmatrix}$ **(Twofish block cipher)** | $x^8 + x^6 + x^5 + x + 1$ | $2^0$ | 535 |
| ${A_1}^{-1} = \begin{bmatrix} C2 & 98 & 98 & 98 \\ 98 & 72 & 52 & 0D \\ 98 & 0D & 72 & 52 \\ 98 & 52 & 0D & 72 \end{bmatrix}$ Inverse of our proposed Type-I circulant-like matrix $A_1$ of size $4 \times 4$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 502 |
| ${A_2}^{-1} = \begin{bmatrix} C2 & 98 & 98 & 98 \\ 98 & 72 & 0D & 52 \\ 98 & 52 & 72 & 0D \\ 98 & 0D & 52 & 72 \end{bmatrix}$ Inverse of our proposed Type-I circulant-like matrix $A_2$ of size $4 \times 4$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 502 |

Through Table 5, it can be seen that the inverses of our proposed matrices $A_1$ and $A_2$ also have a very good fixed point count of 1. Meanwhile, the inverse matrix of AES still has a very large fixed point count of $2^{16}$. In terms of XOR operations, the inverses of our proposed matrices $A_1$ and $A_2$ also have fewer XOR operations compared to matrices of Hierocrypt, Twofish, and more than AES.

Recalling that in cryptography, MDS matrices with a smaller fixed point count, ideally 1, are considered better. Additionally, for efficient execution and low execution cost, fewer XOR operations in MDS matrices are preferable.

From the above observations, it can be seen that our two proposed Type-I circulant-like MDS matrices of size $4 \times 4$ are efficient matrices suitable for execution and may serve as candidates for various cryptographic algorithms.

Based on the results in Table 3, we proceed to compare our proposed six Type-I circulant-like MDS matrices of size $8 \times 8$ with MDS matrices from some well-known cryptographic schemes. Table 6 shows the comparison of the $8 \times 8$ MDS matrices, and Table 7 compares their inverses.

TABLE 6. COMPARISON OF OUR 8×8 TYPE-I CIRCULANT-LIKE MATRICES WITH MATRICES FROM WELL-KNOWN CIPHERS

| **MDS matrices of size $8 \times 8$ ($A$)** | **Primitive polynomial** | **Number of Fixed Points** | **Number of XORs** |
|---|---|---|---|
| **Six proposed Type-I circulant-like MDS matrices of size $8 \times 8$** (in Table 3) | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 948 |
| Circ[0x1, 0x1, 0x4, 0x1, 0x8, 0x5, 0x2, 0x9] **(Whirlpool block cipher)** | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 840 |
| Circ[0x1, 0x1, 0x5, 0x1, 0x8, 0x6, 0x7, 0x4] (**Kalyna block cipher)** | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 952 |
| Type-I circulant-like MDS matrices of size $8 \times 8$ in [19, 20], | Do not satisfy the conditions to be MDS matrices | | |

From Table 6, it can be observed that our proposed $8 \times 8$ Type-I circulant-like matrices share the same number of fixed points (1) as matrices from Whirlpool and Kalyna. In terms of XOR operations, our matrices have fewer XOR operations (better performance) compared to Kalyna and more than Whirlpool.

TABLE 7. COMPARISON OF $8 \times 8$ INVERSE MDS MATRICES

| **Inverse MDS matrices of size $8 \times 8$ ($A^{-1}$)** | **Primitive polynomial** | **Number of Fixed Points** | **Number of XORs** |
|---|---|---|---|
| The inverses of the 6 Type-I circulant-like matrices of size $8 \times 8$ proposed by us in Table 3 | | | |
| $\begin{bmatrix} E1 & DE & DE & DE & DE & DE & DE & DE \\ DE & 5C & 6A & BC & BE & DF & 0E & 44 \\ DE & 44 & 5C & 6A & BC & BE & DF & 0E \\ DE & 0E & 44 & 5C & 6A & BC & BE & DF \\ DE & DF & 0E & 44 & 5C & 6A & BC & BE \\ DE & BE & DF & 0E & 44 & 5C & 6A & BC \\ DE & BC & BE & DF & 0E & 44 & 5C & 6A \\ DE & 6A & BC & BE & DF & 0E & 44 & 5C \end{bmatrix}$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 2142 |
| $\begin{bmatrix} E1 & DE & DE & DE & DE & DE & DE & DE \\ DE & 5C & DF & 6A & 0E & BC & 44 & BE \\ DE & BE & 5C & DF & 6A & 0E & BC & 44 \\ DE & 44 & BE & 5C & DF & 6A & 0E & BC \\ DE & BC & 44 & BE & 5C & DF & 6A & 0E \\ DE & 0E & BC & 44 & BE & 5C & DF & 6A \\ DE & 6A & 0E & BC & 44 & BE & 5C & DF \\ DE & DF & 6A & 0E & BC & 44 & BE & 5C \end{bmatrix}$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 1986 |
| $\begin{bmatrix} E1 & DE & DE & DE & DE & DE & DE & DE \\ DE & 5C & 0E & BE & 6A & 44 & DF & BC \\ DE & BC & 5C & 0E & BE & 6A & 44 & DF \\ DE & DF & BC & 5C & 0E & BE & 6A & 44 \\ DE & 44 & DF & BC & 5C & 0E & BE & 6A \\ DE & 6A & 44 & DF & BC & 5C & 0E & BE \\ DE & BE & 6A & 44 & DF & BC & 5C & 0E \\ DE & 0E & BE & 6A & 44 & DF & BC & 5C \end{bmatrix}$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 2017 |

| | | | |
|---|---|---|---|
| $\begin{bmatrix} E1 & DE & DE & DE & DE & DE & DE & DE \\ DE & 5C & BC & DF & 44 & 6A & BE & 0E \\ DE & 0E & 5C & BC & DF & 44 & 6A & BE \\ DE & BE & 0E & 5C & BC & DF & 44 & 6A \\ DE & 6A & BE & 0E & 5C & BC & DF & 44 \\ DE & 44 & 6A & BE & 0E & 5C & BC & DF \\ DE & DF & 44 & 6A & BE & 0E & 5C & BC \\ DE & BC & DF & 44 & 6A & BE & 0E & 5C \end{bmatrix}$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 1976 |
| $\begin{bmatrix} E1 & DE & DE & DE & DE & DE & DE & DE \\ DE & DE & BE & 44 & BC & 0E & 6A & DF \\ DE & DF & DE & BE & 44 & BC & 0E & 6A \\ DE & 6A & DF & DE & BE & 44 & BC & 0E \\ DE & 0E & 6A & DF & DE & BE & 44 & BC \\ DE & BC & 0E & 6A & DF & DE & BE & 44 \\ DE & 44 & BC & 0E & 6A & DF & DE & BE \\ DE & BE & 44 & BC & 0E & 6A & DF & DE \end{bmatrix}$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 1884 |
| $\begin{bmatrix} E1 & DE & DE & DE & DE & DE & DE & DE \\ DE & DE & 44 & 0E & DF & BE & BC & 6A \\ DE & 6A & DE & 44 & 0E & DF & BE & BC \\ DE & BC & 6A & DE & 44 & 0E & DF & BE \\ DE & BE & BC & 6A & DE & 44 & 0E & DF \\ DE & DF & BE & BC & 6A & DE & 44 & 0E \\ DE & 0E & DF & BE & BC & 6A & DE & 44 \\ DE & 44 & 0E & DF & BE & BC & 6A & DE \end{bmatrix}$ | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 2127 |
| $A^{-1}$= Circ[0x4, 0xaf, 0xe, 0xa4, 0xc2, 0xc2, 0xcb, 0x3e]<br>Inverse of the matrix<br>Circ[0x1, 0x1, 0x4, 0x1, 0x8, 0x5, 0x2, 0x9]<br>(Whirlpool Block cipher) | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 1792 |
| $A^{-1}$ = Circ[0xad,0x95,0x76,0xa8,0x2f, 0x49, 0xd7, 0xca]<br>Inverse of the matrix<br>Circ[0x1, 0x1, 0x5, 0x1, 0x8, 0x6, 0x7, 0x4]<br>(Kalyna Block cipher) | $x^8 + x^4 + x^3 + x^2 + 1$ | $2^0$ | 2048 |

Through Table 7, it can be observed that the inverses of our 6 matrices all have a fixed point score of 1, matching the inverses of Whirlpool's matrix and Kalyna's one. In terms of XOR operations, our 6 matrices have a larger XOR count compared to the inverse of the Whirlpool matrix. However, they exhibit a lower XOR count (better performance) compared to Kalyna.

Please note that in this paper, we focus solely on proposing efficient circulant-like MDS matrices of size $4 \times 4$, and $8 \times 8$ for implementation. While we are capable of handling larger matrices such as $16 \times 16$ or $32 \times 32$, such large MDS matrices are rarely used in cryptography due to the significant execution costs they impose on cryptographic algorithms. On the other hand, for lightweight applications, smaller MDS matrices are more desirable to reduce execution costs.

## V. Conclusion

A significant obstacle faced by cryptographic designers involves discovering MDS matrices with a minimal implementation cost. Researching the construction of MDS matrices based on circulant-like matrices is an intriguing approach. In this article, we introduce algorithms designed to produce effective circulant-like MDS matrices of size $4 \times 4$ and $8 \times 8$ suitable for practical application. Following this, we assess the fix points and the quantity of XOR operations associated with the suggested MDS matrices. We then conduct a comparative analysis with MDS matrices from various renowned ciphers and the proposed Type-I circulant-like MDS matrices in [19, 20]. Our proposed MDS matrices exhibit potential as viable choices for numerous cryptographic algorithms in the forthcoming years.

## References

[1] Samanta, S. (2023). Design and analysis of MDS and Near-MDS Matrices and their application to lightweight cryptography (Doctoral dissertation, Indian Statistical Institute, Kolkata).

[2] Junod, P., & Vaudenay, S. (2005). Perfect diffusion primitives for block ciphers. In Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers 11 (pp. 84-99). Springer Berlin Heidelberg.

[3] Daemen, J., & Rijmen, V. (1998, September). The block cipher Rijndael. In International Conference on Smart Card Research and

Advanced Applications (pp. 277-284). Berlin, Heidelberg: Springer Berlin Heidelberg.

[4] Daemen, J., Knudsen, L., & Rijmen, V. (1997). The block cipher Square. In Fast Software Encryption: 4th International Workshop, FSE'97 Haifa, Israel, January 20–22 1997 Proceedings 4 (pp. 149-165). Springer Berlin Heidelberg.

[5] Daemen, J., & Rijmen, V. (1998, September). The block cipher Rijndael. In International Conference on Smart Card Research and Advanced Applications (pp. 277-284). Berlin, Heidelberg: Springer Berlin Heidelberg.

[6] Ayubi, P., Setayeshi, S., & Rahmani, A. M. (2023). Chaotic Complex Hashing: A simple chaotic keyed hash function based on complex quadratic map. Chaos, Solitons & Fractals, 173, 113647.

[7] O'Neill, M. (2008). Low-cost SHA-1 hash function architecture for RFID tags. RFIDSec, 8, 41-51.

[8] Samanta, S. (2023). On the Counting of Involutory MDS Matrices. arXiv preprint arXiv:2310.00090.

[9] Tuncay, G., Sakallı, F. B., Pehlivanoğlu, M. K., Yılmazgüç, G. G., Akleylek, S., & Sakallı, M. T. (2023). A new hybrid method combining search and direct based construction ideas to generate all 4× 4 involutory maximum distance separable (MDS) matrices over binary field extensions. PeerJ Computer Science, 9, e1577.

[10] Li, Q., Wu, B., & Liu, Z. (2018). Direct constructions of (involutory) MDS matrices from block vandermonde and cauchy-like matrices. In Arithmetic of Finite Fields: 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14-16, 2018, Revised Selected Papers 7 (pp. 275-290). Springer International Publishing.

[11] Mohsenifar, N., & Sajadieh, M. (2023). Introducing a new connection between the entries of MDS matrices constructed by generalized Cauchy matrices in GF (2 q). Journal of Applied Mathematics and Computing, 69(5), 3871-3891.

[12] Chatterjee, T., & Laha, A. (2023). A note on semi-orthogonal (G-matrix) and semi-involutory MDS matrices. Finite Fields and Their Applications, 92, 102279.

[13] Gupta, K. C., Pandey, S. K., & Venkateswarlu, A. (2017). On the direct construction of recursive MDS matrices. Designs, Codes and Cryptography, 82, 77-94.

[14] Gupta, K. C., Pandey, S. K., & Samanta, S. (2022, July). Construction of Recursive MDS Matrices Using DLS Matrices. In International Conference on Cryptology in Africa (pp. 3-27). Cham: Springer Nature Switzerland.

[15] Chand Gupta, K., & Ghosh Ray, I. (2014). On constructions of circulant MDS matrices for lightweight cryptography. In International Conference on Information Security Practice and Experience (pp. 564-576). Springer, Cham.

[16] Cauchois, V., & Loidreau, P. (2019). On circulant involutory MDS matrices. Designs, Codes and Cryptography, 87(2), 249-260.

[17] Wang, J. J., & Chen, Y. H. (2022). The inverse of circulant matrices over GF (2m). Discrete Mathematics, 345(3), 112741.

[18] Adhiguna, I., Arifin, I. S. N., Yuliawan, F., & Muchtadi-Alamsyah, I. (2022). On Orthogonal Circulant MDS Matrices. Computer Science, 17(4), 1619-1637.

[19] Gupta, K. C., & Ray, I. G. (2014). On constructions of MDS matrices from circulant-like matrices for lightweight cryptography. Applied Statistics Unit, Indian Statistical Institute. Calcuta. India.

[20] Gupta, K. C., & Ray, I. G. (2015). Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. Cryptography and Communications, 7(2), 257-287.

[21] Elumalai R. and Reddy A.R. (2011), "Improving diffusion power of aes rijndael with 8x8 mds matrix," International Journal of Scientific & Engineering Research, vol. 2, pp. 1-5.

[22] Rijmen V., Daemen J., Preneel B., Bosselaers A. and De Win E. (1996), "The cipher shark", in Fast Software Encryption. Springer, pp. 99-111.

[23] Z'aba M.R. (2010), "Analysis of linear relationships in block ciphers", Ph.D. Thesis, Queensland University of Technology, Brisbane, Australia.

[24] MacWilliams F.J. and Sloane N.J.A. (1977), "The theory of error-correcting codes". Elsevier.

[25] Khoo, K., Peyrin, T., Poschmann, A. Y., & Yap, H. (2014). FOAM: searching for hardware-optimal SPN structures and components with a fair comparison. In Cryptographic Hardware and Embedded Systems–CHES 2014: 16th International

Workshop, Busan, South Korea, September 23-26, 2014. Proceedings 16 (pp. 433-450). Springer Berlin Heidelberg.

[26] Rao, A. R., Bhimasankaram, P.: Linear Algebra, 2nd edn. Hindustan Book Agency.

[27] Luong, T. T., On the direct building of 8 × 8 self-reciprocal recursive MDS Matrices effective for implementation over GF(q) using Reed-Solomon codes, Journal of Discrete Mathematical Sciences & Cryptography, 26(4), pp. 1237–1248, 2023. DOI : 10.47974/JDMSC-1715.

[28] Linh, H. D., Luong, T. T. , Enhancing Block Cipher Security with Key-dependent Random XOR Tables Generated via Hadamard Matrices and Sudoku Game, Journal of Inetelligent & Fuzzy Systems, 46(4), pp. 7805-7821, 2024. DOI: 10.3233/JIFS-236998.

[29] Luong, T. T. , Linh, H. D., Generating Key-Dependent Involutory MDS Matrices through Permutations, Direct Exponentiation, and Scalar Multiplication, International Journal of Information and Computer Security, 23(4), pp. 410-432, 2024. DOI: 10.1504/IJICS.2024.10062529.

[30] Luong, T. T., Long, N. V. , Bay, V. , Efficient implementation of the linear layer of block ciphers with large MDS matrices based on a new lookup table technique, PLoS ONE, 19(6): e0304873, pp. 1-21, 2024. DOI: https://doi.org/10.1371/ journal.pone.0304873.

[31] Luong, T. T. (2022). Building the dynamic diffusion layer for SPN block ciphers based on direct exponent and scalar multiplication. Journal of Science and Technology on Information Security, 1(15), 38-45. https://doi.org/10.54654/isj.v1i15.836.

## ABOUT THE AUTHORS

**Tran Thi Luong**

Workplace: Academy of Cryptography Techniques, Vietnam Government Information Security Commission.

Email: luongtran@actvn.edu.vn

Education: Bachelor of Mathematics and Informatics of The Hanoi university of Sicence in 2006; Master degreee in Cryptographic Technique at the Academy of Cryptography Techniques in 2012; Phd degree in Cryptographic Technique at the Academy of Cryptography Techniques in 2019;
Recent research direction: Cryptogaphy, Coding theory and Information Security.

Tên tác giả: **Trần Thị Lượng**

Cơ quan công tác: Học viện Kỹ thuật mật mã, Ban Cơ yếu Chính phủ Việt Nam

Email: luongtran@actvn.edu.vn

Quá trình đào tạo: Cử nhân Toán tin ứng dụng tại Trường Đại học Khoa học Tự nhiên, Đại học Quốc gia Hà Nội năm 2006; Thạc sĩ chuyên ngành Kỹ thuật mật mã tại Học viện Kỹ thuật mật mã năm 2012; Tiến sĩ chuyên ngành Kỹ thuật mật mã tại Học viện Kỹ thuật mật mã năm 2019.

Hướng nghiên cứu hiện nay: Mật mã, lý thuyết mã, an toàn thông tin.

**Truong Minh Phuong**

Workplace: Academy of Cryptography Techniques, Vietnam Government Information Security Commission.

Email: minhphuongh19@gmail.vn

Education: Engineer of Cryptographic Technique of the Academy of Cryptography Techniques in 2012; Master degreee in Cryptographic Technique at the Academy of Cryptography Techniques in 2018.

Recent research direction: Cryptogaphy

Tên tác giả: **Trương Minh Phương**

Cơ quan công tác: Học viện Kỹ thuật mật mã, Ban Cơ yếu Chính phủ Việt Nam

Email: minhphuongh19@gmail.com

Quá trình đào tạo: Kỹ sư Kỹ thuật mật mã tại Học viện Kỹ thuật mật mã năm 2012; Thạc sĩ Kỹ thuật mật mã tại Học viện Kỹ thuật mật mã năm 2018.

Hướng nghiên cứu hiện nay: Mật mã