A Note on the Construction of Lightweight Cyclic MDS Matrices

Akbar Mahmoodi Rishakani[1], Yousef Fekri Dabanloo[1], Seyed Mojtaba Dehnavi[2], Mohammad Reza Mirzaee Shamsabad[3], Nasour Bagheri[4]

(Corresponding author: Akbar Mahmoodi Rishakani)

Department of Mathematics, Shahid Rajaee Teacher Training University, Tehran, Iran[1]
Shabanlou, Lavizan, Tehran, Iran
Department of Mathematical and Computer Sciences, University of Kharazmi, Tehran, Iran[2]
Department of Mathematics, Shahid Beheshti University, Tehran, Iran[3]
Department of Electrical Engineering, Shahid Rajaee Teachers Training University[4]
(Email: am.rishakani@sru.ac.ir)

(Received Aug. 22, 2017; revised and accepted Jan. 12, 2018)

Abstract

Modern lightweight block ciphers and hash functions apply linear layers for the diffusion purpose. In this paper, we characterize a class of lightweight MDS matrices decomposed into two cyclic matrices. As the main contribution, we presents a class of lightweight 4×4 cyclic MDS matrices lighter than the state-of-the-art which reduces the implementation cost (in terms of number of XOR gates required) of linear diffusion layers for hardware-oriented cryptographic primitives.

Keywords: Branch Number; Cyclic Matrix; Diffusion Layer; Lightweight Cryptographic Primitive; MDS Matrix

1 Introduction

Many modern lightweight block ciphers and hash functions apply MDS or almost MDS matrices as diffusion layers. For example, Midori [3] and QARMA [1, 9] families of block ciphers use almost MDS matrices and LED block cipher [10] and PHOTON hash function [11] use MDS matrices as diffusion layers. The performance of a diffusion layer depends on its branch number and implementation cost which is usually measured by the number of XORs required. Since the branch number of an MDS matrix is already maximum, for constrained applications like RFID and IoT [7, 8, 19, 21, 22], the implementation cost remains the main concern. For this purpose, we provide a hardware-efficient class of lightweight 4×4 cyclic MDS matrices.

1.1 Related Works

Providing MDS matrices that can be implemented with as few XOR operations as possible is one of the essentials in the design of lightweight symmetric primitives.

The XOR metric for measuring the efficiency of hardware implementations was first presented in [13] and later improved in [4] and [12]. Based on results from [18], many publications tried to find as efficient MDS matrices as possible.

In [4], the authors present lightweight cyclic MDS matrices by the use of lightweight multiplication in $\mathbb{F}_{2^m}$ (the field with 2^m elements). The cost of their presented 4×4 MDS matrices is $12m + 12$ XORs, $4 \leq m \leq 8$. Here, m is the size of input words. The authors of [15] construct lightweight 4×4 cyclic MDS matrices with implementation cost of 60 and 108 XORs for 4-bit and 8-bit input words, respectively.

Bai and Wang [2] characterize lightweight 4×4 MDS matrices with 4-bit input words for which the entries implementation needs 10 XORs and overall, the entire matrix requires $4 \times 12 + 10 = 58$ XORs for implementation. Then, a class of 4×4 MDS matrices proposed with the help of Toeplitz matrices with 58 XORs for 4-bit and 123 XORs for 8-bit input words by Sarkar *et al.* in [17]. Later, in [6] Cauchois *et al.* constructed quasi-involutory recursive-like MDS matrices from 2-cyclic codes for which the implementation cost of 4×4 MDS matrices with 4-bit input words is 72 XORs. Zhang *et al.* in [23] provide cyclic 4×4 MDS matrices with 4-bit input words and 12 XORs for entries which overall requires $4 \times 12 + 12 = 60$ XORs for implementation. Recently, Zhou *et al.* [20] proposed two kinds of lightweight 4×4 MDS matrices over 4-bit and 8-bit input words which require $4 \times 12 + 10 = 58$ and $8 \times 12 + 10 = 106$ XORs, respectively.

1.2 Our Contribution

In most of recently presented lightweight primitives, *e.g.* QARMA [1] and Midori [3] block ciphers, almost MDS matrices are used due to the low implementation cost, *i.e.* 24 XORs for 4-bit input words; while the lightest MDS ones take 58 XORs (before this paper). Hence, there is a significant gap between the implementation cost of almost MDS matrices and MDS matrices. On the other hand, employing an almost MDS matrix as diffusion layer, in general, provides lower security bounds for the same number of rounds. Thus, in this paper, we took a step forward to reduce the gap between the implementation cost of almost MDS matrices and MDS ones, to motivate designers to use MDS matrices.

Our concern in this paper is to construct lightweight 4×4 cyclic MDS matrices with efficient implementation in hardware, measured by the number of XOR gates required. We construct 4×4 lightweight MDS matrices by the multiplication of two cyclic matrices. More precisely, one of its multiplicands is a 4×4 cyclic matrix whose entries are binary permutation matrices (which have no implementation cost in hardware) and the other is a cyclic matrix with two non-zero entries per row. We characterize the MDS property of this type of matrices. As a result, we provide lightweight 4×4 cyclic MDS matrices on m-bit input words with the implementation cost of $10m + 4$ XORs for $4 \leq m \leq 8$.

Note that our results would be infeasible without our new approach of representing the MDS matrix as a product. This is because of the fact that an MDS matrix cannot have zero entries. So, a 4×4 MDS matrix over m-bit input words would need already $12m$ XORs only for the additions within the matrix multiplication, which exceeds our results. That is, we benefit from being able to use matrices with many zero entries.

We believe that, it is irrelevant to compare the implementation cost of cyclic MDS matrices with non-cyclic ones, but since cyclic MDS matrices are less studied, we compare our results with cyclic and non-cyclic matrices in Table 1 for m-bit input words, $m = 4, 8$ (details are given in sections 3 and 4). Note that, in Table 1, by $\#A = \#A^{-1}$ we mean the matrices A for which the implementation cost of A and A^{-1} are equal.

1.3 Outline of the Paper

In Section 2, we give the preliminary notations and definitions. Section 3 presents new criteria for constructing cyclic MDS matrices. In Section 4, we verify the implementation cost of our constructions and their inverses. Section 5 concludes the paper.

2 Preliminaries

In this paper, n and m are natural numbers. By $|A|$ we denote the number of elements of a finite set A. We denote the set of all $n \times n$ matrices with entries in R by $\mathcal{M}_n(R)$ and the determinant of a matrix A in $\mathcal{M}_n(R)$ by $det_R(A)$. The XOR of two binary vectors or matrices v and w is denoted by $v \oplus w$, a zero vector or matrix by $\mathbf{0}$ and an identity matrix by I. We represent the finite field with 2 elements by $\mathbb{F}_2$ and use $\mathbb{F}_2^m$ to represent the set of all m-bit vectors. We denote by $\#A$, the number of XORs needed to implement the binary matrix $A \in \mathcal{M}_n(\mathbb{F}_2)$.

By the notation $A = cycl(a_1, a_2, a_3, \ldots, a_n)$ we mean the cyclic matrix

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}$$

For a vector $v = (v_3, v_2, v_1, v_0) \in \mathbb{F}_2^4$ we correspond a number $\bar{v} = \sum_{v_i \neq 0} 2^i$ in hexadecimal representation. So, a matrix $M \in \mathcal{M}_4(\mathbb{F}_2)$ could be represented by four numbers (in hexadecimal representation) corresponding to its rows. For instance, the following matrix is represented by $7bde$:

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad (1)$$

The set of all invertible binary matrices of order m that have exactly one non-zero entry in each row is denoted by $\mathcal{PM}_m(\mathbb{F}_2)$ and called binary permutation matrices. For example, by our notations, the matrix $2814 \in \mathcal{PM}_4(\mathbb{F}_2)$ maps the vector $x = (x_3, x_2, x_1, x_0) \in \mathbb{F}_2^4$ to (x_2, x_0, x_3, x_1). So, for any $A \in \mathcal{PM}_m(\mathbb{F}_2)$ and $x \in \mathbb{F}_2^m$, $y = xA$ is a vector whose components are a permutation of the components of x and $\#A = 0$.

The i-th component of a vector $x \in (\mathbb{F}_2^m)^n$ is denoted by x_i, *i.e.* $x = (x_{n-1}, ..., x_0)$. The weight of a vector $x \in (\mathbb{F}_2^m)^n$ with respect to m-bit input words is denoted by $wt_m(x)$ and defined as

$$wt_m(x) = |\{\, x_i : x_i \neq 0, 0 \leq i \leq n-1\}|.$$

For example, let

$$x = 1001110000101110,$$

we have, $wt_1(x) = 8$, $wt_2(x) = 6$ and $wt_4(x) = 4$.

Definition 1. *[5] Let $M \in \mathcal{M}_n(\mathcal{M}_m(\mathbb{F}_2))$. The (differential) branch number of M with respect to m-bit input words is defined as*

$$\mathcal{B}_m(M) = \min_{x \neq \mathbf{0}} \{wt_m(x) + wt_m(xM) : x \in (\mathbb{F}_2^m)^n\}.$$

For the matrix M defined in Equation (1), we have $\mathcal{B}_1(M) = 4$, i. e. $wt_1(x) + wt_1(xM) \geq 4$ for any non-zero $x \in \mathbb{F}_2^4$. On the other hand, the matrix M could be considered as a 2×2 matrix with entries in $\mathcal{M}_2(\mathbb{F}_2)$, i. e.

$$M = \left(\begin{array}{cc|cc} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ \hline 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{array}\right) \in \mathcal{M}_2(\mathcal{M}_2(\mathbb{F}_2))$$

Table 1: Comparison between the implementation cost of 4×4 MDS matrices, for m-bit input words

Source	Cyclic	$\#A = \#A^{-1}$	XOR count (m=4 / m=8)
[4]	√	X	60 / 108
[2]	X	X	58 / -
[15]	√	X	60 / 108
[15]	√	√	68 / -
[17]	X	X	58 / 123
[12]	X	X	58 / 116
[16]	√	√	60 / 128
[20]	√	X	58 / 106
[23]	√	X	60 / -
This paper	√	X	44 / 84

In this case, one can check that $\mathcal{B}_2(M) = 2$.

It is straightforward to verify that for a matrix $M \in \mathcal{M}_n(\mathcal{M}_m(\mathbb{F}_2))$ we have $\mathcal{B}_m(M) \leq n + 1$.

Definition 2. *[5] A matrix $M \in \mathcal{M}_n(\mathcal{M}_m(\mathbb{F}_2))$ is called MDS with respect to m-bit input words if*

$$\mathcal{B}_m(M) = n + 1.$$

It is worth noting that, with the help of an $n \times n$ MDS matrix with respect to m-bit input words, we can construct an MDS code of length $2n$ over m-bit alphabets [5].

3 Constructing Lightweight 4×4 Cyclic MDS Matrices

In this section we verify a class of cyclic 4×4 matrices to give sufficient conditions when they are MDS. The proposed matrices are the product of two cyclic matrices such that the non-zero entries of the first factor are in $\mathcal{PM}_m(\mathbb{F}_2)$ and the non-zero entries of the second factor belong to $\mathcal{M}_m(\mathbb{F}_2)$.

For the mentioned verification, we need the following theorems.

Theorem 1. *[5] For $M \in \mathcal{M}_n(\mathcal{M}_m(\mathbb{F}_2))$, M is MDS with respect to m-bit input words if and only if every square submatrix of M of order t, $1 \leq t \leq n$, is invertible.*

Theorem 2. *[14] For $M \in \mathcal{M}_n(\mathcal{M}_m(\mathbb{F}_2))$, if the entries of M in $R = \mathcal{M}_m(\mathbb{F}_2)$ are pairwise commuting, then*

$$det_{\mathbb{F}_2}(M) = det_{\mathbb{F}_2}(det_R(M)).$$

The following lemma is a straightforward result of Theorem 1.

Lemma 1. *Let $A \in \mathcal{M}_m(\mathbb{F}_2)$ and $P_1, P_2, P_3, P_4 \in \mathcal{PM}_m(\mathbb{F}_2) \bigcup \{\mathbf{0}\}$. If the matrix*

$$M = cycl(P_1, P_2, P_3, P_4) \times cycl(I, A, \mathbf{0}, \mathbf{0}),$$

is MDS with respect to m-bit input words, then at most one of P_i's, $1 \leq i \leq 4$, could be zero.

According to Lemma 1, we verify the following class of matrices in more details:

$$M = cycl(P_1, P_2, P_3, \mathbf{0}) \times cycl(I, A, \mathbf{0}, \mathbf{0}). \quad (2)$$

It is easy to verify that, the matrix defined in Equation (2) is MDS if and only if the matrix

$$M' = cycl(I, P_1^{-1}P_2, P_1^{-1}P_3, \mathbf{0}) \times cycl(I, A, \mathbf{0}, \mathbf{0}),$$

is MDS. As $\mathcal{PM}_m(\mathbb{F}_2)$ is closed under multiplication and inversion, we have $p_1 = P_1^{-1}P_2, p_2 = P_1^{-1}P_3 \in \mathcal{PM}_m(\mathbb{F}_2)$. Now if we assume that p_1, p_2 and A are pairwise commuting, then the determinants of the square submatrices of

$$\begin{aligned} M' &= cycl(I, p_1, p_2, \mathbf{0}) \times cycl(I, A, \mathbf{0}, \mathbf{0}) \\ &= cycl(I, A \oplus p_1, p_1A \oplus p_2, p_2A), \end{aligned}$$

are as following.

(a) 1×1 submatrices:

$$I, A \oplus p_1, p_1A \oplus p_2, p_2A.$$

(b) 2×2 submatrices:

$$\begin{aligned} &p_1p_2A \oplus I, p_1(A^2 \oplus p_1A \oplus p_2), \\ &A^2 \oplus p_1A \oplus p_1^2 \oplus p_2, p_2^2A^2 \oplus p_1A \oplus p_2, \\ &p_1p_2A^2 \oplus (p_2^2 \oplus I)A \oplus p_1, p_1^2A^2 \oplus p_2^2 \oplus I, \\ &(p_1^2 \oplus p_2)A^2 \oplus p_1p_2A \oplus p_2^2, (p_2^2 \oplus I)A^2 \oplus p_1^2, \\ &p_2A^2 \oplus p_1p_2A \oplus I. \end{aligned}$$

(c) 3×3 submatrices:

$$\begin{aligned} &(p_1 \oplus p_1p_2^2)A^3 \oplus (p_2 \oplus p_1^2 \oplus p_2^3)A^2 \oplus p_1^3A \\ &\qquad \oplus p_2^2 \oplus p_1^2p_2 \oplus I, \\ &(p_2 \oplus p_1^2 \oplus p_2^3)A^3 \oplus p_1^3A^2 \oplus (p_1^2p_2 \oplus p_2^2 \oplus I)A \\ &\qquad \oplus p_1 \oplus p_1p_2^2, \\ &p_1^3A^3 \oplus (p_1^2p_2 \oplus p_2^2 \oplus I)A^2 \oplus (p_1 \oplus p_1^2p_2)A \\ &\qquad \oplus p_1^2 \oplus p_2^3 \oplus p_2, \\ &(p_2^2 \oplus p_1^2p_2 \oplus I)A^3 \oplus (p_1 \oplus p_1p_2^2)A^2 \\ &\qquad \oplus (p_1^2 \oplus p_2 \oplus p_2^3)A \oplus p_1^3. \end{aligned}$$

(d) 4×4 submatrices:

$$(I \oplus p_1^2 p_2 \oplus p_2 p_1^2 \oplus p_1^4 \oplus p_2^4)(I \oplus A^4).$$

According to Theorem 1 and Theorem 2, M' is MDS with respect to m-bit input words if and only if the aforementioned submatrices are invertible.

In the special case of $p_1 = p_2 = I$, we have the following theorem.

Theorem 3. *Let $A \in \mathcal{M}_m(\mathbb{F}_2)$. The matrix*

$$M = cycl(I, I, I, \mathbf{0}) \times cycl(I, A, \mathbf{0}, \mathbf{0}) \tag{3}$$

is MDS with respect to m-bit input words if and only if $A, A^3 \oplus I, A^7 \oplus I$ are invertible.

Proof. By replacing p_1 and p_2 with I in matrices of (a),(b),(c) and (d), it results that M is MDS if and only if the following matrices are invertible.

$$\begin{array}{c} I,\ A,\ I \oplus A,\ A^2,\ (I \oplus A)^2, \\ A(I \oplus A),\ I \oplus A \oplus A^2,\ I \oplus A \oplus A^3, \\ I \oplus A^2 \oplus A^3,\ A(I \oplus A \oplus A^2), \\ A^3 \oplus A^2 \oplus A \oplus I,\ (I \oplus A)^4. \end{array} \tag{4}$$

Given that $I \oplus A^3 = (I \oplus A)(I \oplus A \oplus A^2)$, $I \oplus A^7 = (I \oplus A)(I \oplus A \oplus A^3)(I \oplus A^2 \oplus A^3)$, $(I \oplus A)^4 = (I \oplus A)(A^3 \oplus A^2 \oplus A \oplus I)$ and regarding (4), all submatrices of M are invertible if and only if $A, I \oplus A^3, I \oplus A^7$ are invertible, which completes the proof. □

Similar to Theorem 3, the next theorem could be proved.

Theorem 4. *Let $A \in \mathcal{M}_m(\mathbb{F}_2)$. The matrix*

$$M = cycl(I, I, I, \mathbf{0}) \times cycl(I, \mathbf{0}, \mathbf{0}, A)$$

is MDS with respect to m-bit input words if and only if $A, A^3 \oplus I, A^7 \oplus I$ are invertible.

Similarly, we verified the MDS property of matrices

$$M = cycl(I, I, I, \mathbf{0}) \times cycl(I, \mathbf{0}, A, \mathbf{0}).$$

We found out that, there is no matrix $A \in \mathcal{M}_m(\mathbb{F}_2)$ such that M is MDS.

4 Implementation and Experimental Results

In this section, we discuss the implementation cost of the 4×4 cyclic MDS matrices given in Theorem 3 and Theorem 4 and their corresponding inverses. For the matrix M in Equation (3), we have

$$\#M = 10m + 4\#A. \tag{5}$$

This is because the implementation cost of $C = cycl(I, A, \mathbf{0}, \mathbf{0})$ would be $4m + 4\#A$ XORs; since, for the action of C on input words, we should apply A four times plus extra $4m$ XORs for the additions within matrix multiplication. On the other hand, to implement $B = cycl(I, I, I, \mathbf{0})$, we use the following procedure:

$$\begin{array}{rcl} (X_3, X_2, X_1, X_0)B & = & (Y_3, Y_2, Y_1, Y_0), \\ Z_0 = X_1 \oplus X_2, Z_1 & = & X_0 \oplus X_3, \\ Y_0 = X_0 \oplus Z_0, Y_1 & = & X_3 \oplus Z_0, \\ Y_2 = X_2 \oplus Z_1, Y_3 & = & X_1 \oplus Z_1, \end{array}$$

which shows that B needs $6m$ XORs. By the same calculations, the implementation cost of matrices M verified in Theorem 4 equals to $10m + 4\#A$ XORs.

Now according to Equation (5), the construction of lightweight 4×4 MDS matrices with respect to m-bit input words, $4 \leq m \leq 8$, given in Theorem 3 and Theorem 4, would be reduced to finding invertible matrices $A \in \mathcal{M}_m(\mathbb{F}_2)$ with as low implementation cost as possible such that $I \oplus A^3$ and $I \oplus A^7$ are invertible. Every invertible matrix A with $\#A = 0$ belongs to $\mathcal{PM}_m(\mathbb{F}_2)$; so, at least one of the non-zero entries of A would be on its principal diagonal, i. e. one of the rows of A equals to the corresponding row of I. This means that $I \oplus A$ could not be invertible. Thus, we should search for matrices A with $\#A = 1$.

For this purpose, we have exhaustively searched the proposed matrices A in $\mathcal{S}_m$, $4 \leq m \leq 8$, where, $\mathcal{S}_m$ is the set of all binary matrices $A \in \mathcal{M}_m(\mathbb{F}_2)$, for which just one of the rows has two non-zero entries and the other rows have only one non-zero entry. Clearly, $|\mathcal{S}_m| = \binom{m}{2} m^m$ and for every $A \in \mathcal{S}_m$, we have $\#A = 1$. It takes few hours to find all matrices $A \in \mathcal{S}_8$ ($|\mathcal{S}_8| = 7 \times 2^{26}$) such that A, $I \oplus A^3$ and $I \oplus A^7$ are invertible, by programming. Note that the case of $m = 8$ is the most time consuming case. As a result, we found 48, 240, 960, 480 and 25920 such matrices for $m = 4, 5, 6, 7, 8$, respectively. We present all 48 matrices for $m = 4$ as follows and give a list of five matrices for each of the other cases in Appendix.

$$\begin{array}{l} 1286, 1294, 1846, 18c2, 1942, 1a84, 214a, 2158, \\ 281c, 2854, 2948, 2a14, 3814, 3842, 418a, 41c2, \\ 421c, 4298, 4318, 4382, 5182, 5284, 6148, 6218. \\ 1285, 12a4, 1684, 1843, 1862, 1c42, 2149, 2168, \\ 2548, 2815, 2834, 2c14, 4183, 41a2, 4219, 4238, \\ 4582, 4618, 9284, 9842, a148, a814, c182, c218. \end{array} \tag{6}$$

According to Equation (5), by choosing A from the list of the matrices (6) or from the Appendix, the implementation cost of the proposed MDS matrices with respect to m-bit input words, $4 \leq m \leq 8$, derived from Theorem 3 and Theorem 4 are $10m + 4$ XORs.

Often, when aiming for the most efficient MDS matrix, the inverse of the matrix is not considered and might have much higher implementation cost. This is because of the fact that, in many applications in symmetric cryptography, we do not need to implement the inverse of components. Examples of such applications include stream ciphers, hash functions, block ciphers in CTR and OFB

modes or block ciphers with Feistel or Lai-Massy structures. Accordingly, most of the papers we are comparing with, have not verified the implementation cost of the inverse of their proposed MDS matrices [2, 4, 12, 17, 20, 23]. However, we give an upper bound for the implementation cost of the inverse of our proposed MDS matrices as following.

For $B = cycl(I, I, I, \mathbf{0})$ we have, $B^{-1} = cycl(I, \mathbf{0}, I, I)$. Therefore, $\#B^{-1} = \#B = 6m$. On the other hand, if $C = cycl(I, A, \mathbf{0}, \mathbf{0})$, then $C^{-1} = \alpha C^3$, $\alpha = (I \oplus A^4)^{-1}$. As $C^2 = cycl(I, \mathbf{0}, A^2, \mathbf{0})$, we have

$$C^{-1} = \alpha C \times cycl(I, \mathbf{0}, A^2, \mathbf{0}).$$

By this decomposition, an upper bound for the implementation cost of C^{-1} is

$$(4m + 4\#A^2) + (4m + 4\#A) + 4\#\alpha.$$

So, the implementation cost of the inverse of the matrices derived from Theorem 3 and Theorem 4 would be bounded by

$$14m + 4\#A + 4\#A^2 + 4\#\alpha.$$

For $m = 4$, we presented 48 candidates of matrix A with 1 XOR implementation cost (listed in (6)), for which the corresponding matrices M in Theorem 3 and Theorem 4 are MDS. Among them, the first 24 matrices have the property that $I \oplus A^4 = A$. In this case, $\alpha C^2 = cycl(A^{-1}, \mathbf{0}, A, \mathbf{0})$. So,

$$C^{-1} = cycl(I, A, \mathbf{0}, \mathbf{0}) \times cycl(A^{-1}, \mathbf{0}, A, \mathbf{0}).$$

This means that, if we select A from the first 24 matrices of the list (6), then the implementation cost of corresponding cyclic MDS matrix M would be 44 XORs and the implementation cost of M^{-1} would be 68 XORs. Note that, for every invertible matrix $A \in \mathcal{S}_m$, we have $A^{-1} \in \mathcal{S}_m$; i. e. $\#A^{-1} = 1$.

To verify whether the matrices presented in Equation (2) are MDS or not, in the case of $m = 4$, we exhaustively checked P_1, P_2, P_3 and A. The total number of such matrices is $(4!)^3 2^{16} = 81 \times 2^{25}$. The result of our programming shows that for all of the resultant MDS matrices, we have $P_1 = P_2 = P_3$.

5 Conclusion

In this paper, we proposed a new class of lightweight 4×4 cyclic MDS matrices with respect to m-bit input words based on the product of cyclic matrices. The resultant MDS matrices need $10m + 4$ XORs for implementation. In comparison to the state-of-the-art, to the best of our knowledge, our proposed cyclic MDS matrices outperform the previous known cyclic MDS matrices.

References

[1] R. Avanzi, "The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes," *IACR Transactions on Symmetric Cryptology*, vol. 2017, pp. 4–44, 2017.

[2] J. Bai and D. Wang, "The lightest 4x4 MDS matrices over GL(4, $\mathbb{F}_2$)," *IACR Cryptology ePrint Archive*, vol. 2016, pp. 686, 2016.

[3] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A block cipher for low energy (Extended version)," *Cryptology ePrint Archive*, Report 2015/1142, 2015.

[4] C. Beierle, T. Kranz, and G. Leander, "Lightweight multiplication in GF(2ˆn) with applications to MDS matrices," in *Advances in Cryptology (CRYPTO'16)*, vol. 9814 of *Lecture Notes in Computer Science*, pp. 625–653, 2016.

[5] M. Blaum and R. M. Roth, "On lowest density MDS codes," *IEEE Translation Information Theory*, vol. 45, no. 1, pp. 46–59, 1999.

[6] V. Cauchois, P. Loidreau, and N. Merkiche, "Direct construction of quasi-involutory recursive-like MDS matrices from 2-cyclic codes," *Cryptology ePrint Archive*, Report 2016/1112, 2016.

[7] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[8] N. Chikouche, C. Foudil, P. L. Cayrel, and M. Benmohammed, "Improved RFID authentication protocol based on randomized mceliece cryptosystem," *International Journal Network Security*, vol. 17, no. 4, pp. 413–422, 2015.

[9] W. R. Ghanem, M. Shokir, and M. Dessoky, "Defense Against Selfish PUEA in Cognitive Radio Networks Based on Hash Message Authentication Code," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 12–21, 2016.

[10] A. P. J. Guo, T. Peyrin and M. Robshaw, "The led block cipher," *Cryptology ePrint Archive*, Report 2012/600, 2012.

[11] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Advances in Cryptology (CRYPTO'11)*, vol. 6841 of *Lecture Notes in Computer Science*, pp. 222–239, 2011.

[12] J. Jean, T. Peyrin, and S. M. Sim, "Optimizing implementations of lightweight building blocks," *Cryptology ePrint Archive*, Report 2017/101, 2017.

[13] K. Khoo, T. Peyrin, A. Y. Poschmann, and H. Yap, "Foam: Searching for hardware-optimal spn structures and components with a fair comparison," in *Cryptographic Hardware and Embedded Systems (CHES'14)*, pp. 433–450, 2014.

[14] I. Kovacs, D. S. Silver, and S. G. Williams, "Determinants of commuting-block matrices," *The American Mathematical Monthly*, vol. 106, no. 10, pp. 950–952, 1999.
[15] Y. Li and M. Wang, "On the construction of lightweight circulant involutory MDS matrices," in *Fast Software Encryption (FSE'16)*, pp. 121–139, 2016.
[16] M. Liu and S. M. Sim, "Lightweight MDS generalized circulant matrices," in *Fast Software Encryption (FSE'16)*, pp. 101–120, 2016.
[17] S. Sarkar and H. Syed, "Lightweight diffusion layer: Importance of toeplitz matrices," *Cryptology ePrint Archive*, Report 2016/835, 2016.
[18] S. M. Sim, K. Khoo, F. Oggier, and T. Peyrin, "Lightweight mds involution matrices," in *Fast Software Encryption (FSE'15)* , pp. 471–493, 2015.
[19] W. L. Tai and Y. F. Chang, "Comments on a secure authentication scheme for iot and cloud servers," *International Journal Network Security*, vol. 19, no. 4, pp. 648–651, 2017.
[20] L. Wang, L. Zhou and Y. Sun, "Construction of lightweight MDS matrices over matrix polynomial residue ring," Cryptology ePrint Archive, Report 2016/1173, 2016.
[21] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.
[22] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.
[23] S. Zhang, Y. Wang, Y. Gao, and T. Wang, "On the construction of the 4 x 4 lightest circulant MDS matrices," in *Proceedings of the International Conference on Cryptography, Security and Privacy, (ICCSP'17)*, pp. 1–6, 2017.

Appendix

Here, for simplicity, a matrix $A \in \mathcal{M}_m(\mathbb{F}_2)$, $5 \leq m \leq 8$, is represented by a sequence of m decimal numbers corresponding to its rows. For example, $(1, 2, 8, 16, 6)$ represents the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

List of some matrices for $m = 5$:

$(1, 2, 8, 16, 6), (2, 1, 10, 4, 16), (3, 4, 1, 8, 16),$
$(4, 2, 1, 17, 8), (12, 2, 16, 1, 4).$

List of some matrices for $m = 6$:

$(1, 2, 4, 16, 32, 10), (2, 1, 32, 20, 4, 8), (4, 2, 1, 16, 8, 34),$
$(12, 2, 1, 16, 8, 32), (33, 32, 16, 2, 8, 4).$

List of some matrices for $m = 7$:

$(1, 2, 4, 16, 32, 64, 40), (2, 8, 1, 4, 64, 16, 96),$
$(9, 1, 32, 16, 2, 64, 4), (17, 1, 4, 2, 32, 64, 8),$
$(34, 16, 8, 2, 1, 4, 64).$

List of some matrices for $m = 8$:

$(1, 2, 4, 8, 32, 64, 144, 16), (2, 1, 4, 64, 128, 8, 16, 40),$
$(20, 32, 1, 128, 16, 2, 64, 8), (80, 128, 8, 1, 4, 64, 32, 2),$
$(96, 128, 4, 8, 2, 16, 1, 64).$

Biography

Akbar Mahmoodi Rishakani received his B.S. and M.S. degrees in pure mathematics from Shahid Beheshti University in 2005 and 2008 respectively. He is now PHD student of mathematical cryptography in Shahid Rajaee Teacher Training University under the supervision of Prof. Hamid Reza Maimani and Prof. Nasour Bagheri. His current research interests include information security, cryptology and combinatorics.

Yousef Fekri Dabanloo received the B.S. degree in pure mathematics from Semnan University in 2011, Semnan, Iran. He received the M.S. degree in 2013 from Sharif University of Technology, Tehran, Iran. Now he is as a PhD student in Shahid Rajaei University, Tehran, Iran. His current research interests include information security and cryptology.

Seyed Mojtaba Dehnavi was born in 1975 in Iran. He received his BSc in applied mathematics and hardware engineering in 2001 from Iranian University of Science and Technology, his MSc in pure mathematics in 2004 from Amir Kabir University of Technology, and his PhD in mathematical cryptography in 2015 from Kharazmi University under supervision of Prof. Hamid Reza Maimani.

Mohammad Reza Mirzaee Shamsabad was born in 1983 in Iran. He received his BSc in applied mathematics in 2006 from Azad University, his MSc in pure mathematics in 2010 from Shahid Bahonar University. He is now a candidate of PhD in mathematical cryptography in Shahid Beheshti University under supervision of Prof. Hossein Hajiabolhassan.

Nasour Bagheri is an assistant professor at electrical engineering department, Shahid Rajaee Teacher Training University, Tehran, Iran. He is the author of more than 60 articles on information security and cryptology. Homepage of the author is available at: https://www.srttu.edu/english-cv-dr-bagheri/.