The Lightest 4×4 MDS Matrices over $GL(4, \mathbb{F}_2)$

Ting Li[1], Jian Bai[2], Yao Sun[1], Dingkang Wang[2], and Dongdai Lin[1]

[1] SKLOIS, Institute of Information Engineering, CAS, Beijing 100093,China
[2] KLMM, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China

Abstract. Maximal Distance Separable (MDS) matrices are important components for block ciphers. In this paper, we present an algorithm for searching 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$. By this algorithm, we find that all the lightest MDS matrices have only 10 XOR counts. Besides, all these lightest MDS matrices can be classified to 3 types, and some necessary and sufficient conditions are presented for them as well. Some theoretical results can be generalized to the case $GL(m, \mathbb{F}_2)$, and 4×4 MDS matrices with 10 XOR counts can be constructed directly.

Keywords: MDS matrix, lightweight, diffusion layer.

1 Introduction

Diffusion and confusion are fundamental properties when designing symmetric-key ciphers [1]. They are required for the security of the cipher. Generally, the confusion property is to spread the internal dependencies as much as possible [2]. While the diffusion layer is obtained by a linear diffusion matrix which transforms an input vector to some output vectors via diffusion operations. To resist linear and differential attacks, it is necessary to maximize the diffusion power of the matrix. That is to say, increasing the branch number is helpful to achieve a better performance. The matrix with the maximum branch number is a perfect diffusion layer, and we call the matrix a *Maximal Distance Separable* (MDS) matrix.

MDS matrices are widely used in many ciphers like AES [3], LED [4], SQUARE [5]. In the view of computation efficiency, not all of the MDS matrices are appropriate for diffusion layer in practice. Thus, it is necessary to reduce the implementation costs when designing the diffusion layer. Recently, several lightweight block cipher such as SIMON [6] and SPECK [6], PRESENT [7], SIMECK [8] and lightweight function such as QUARK [9] and PHOTON [10] are designed to minimize the implementation costs. For MDS matrices, the construction of lightweight MDS matrix becomes a popular topic, where *lightweight MDS matrix* means the MDS matrix with small XOR counts.

The common method of constructing lightweight MDS matrices is to use some specific structure of matrices, then choose the elements of finite fields with lower Hamming weights. Thus, circulant matrix and Hadamard matrix are preferred due to their limited elements. Circulant-like MDS matrices were constructed and the lightest MDS circulant-like matrices were found [11,12]. Hadamard-Cauchy like MDS and involutory MDS matrices were studied as well [13]. Li and Wang [14] first constructed (non-commutative) circulant involutory MDS matrices and gave some lower bounds on XOR counts of circulant and Hadamard MDS matrices. Liu and Sim [15] generalized the circulant structures and proposed a new class of matrices, called cyclic matrices. They also obtained the lightest cyclic matrices. Sarkar and Syed [16] gave theoretical constructions of Toeplitz MDS matrices and reported the minimum value of XOR counts of 4×4 MDS matrices over $\mathbb{F}_2^4$ and $\mathbb{F}_2^8$, respectively.

Another way to construct lightweight MDS matrices is by recursive construction. This method was first used in the design of PHOTON lightweight hash family [10] and LED lightweight block cipher [4]. Sajadieh et al. [17] extended the recursive method by using linear transformations instead of multiplications of elements in finite fields. Then Wu et al. [18] improved it by using linear transformations with fewer XOR counts and gave some extreme lightweight MDS matrices.

Although these methods are efficient for finding lightweight MDS matrices, the matrices found are optimal among the subclasses rather than the whole population of the matrix type. And the lower bound of XOR counts is not confirmed yet. To the best of our knowledge, the lightest 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$ have the weight of 10 counted by XOR operators [16]. For 4×4 MDS matrices over $GL(8, \mathbb{F}_2)$ the lightest weight is reported as 27 [16].

In this paper, we present an algorithm for searching MDS matrices without any particular structures. We find all the lightest 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$ have 10 XOR counts, including the Toeplitz MDS matrices presented in [16]. We classify all these lightest MDS matrices to 3 types, and give some sufficient and necessary conditions for these 3 types matrices being MDS matrices. Using these conditions, we directly construct some 4×4 MDS matrices over $GL(m, \mathbb{F}_2)$ with 10 XOR counts where $m \geq 4$.

We summarize our contributions of this paper below.

1. We present a searching algorithm and give the lower bound of XOR counts for 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$.
2. We classified the lightest 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$ into 3 classes by their structures.
3. We give some sufficient and necessary conditions for these 3 classes of matrices being MDS matrices. We also prove that the conditions can be generalized to 4×4 MDS matrices over $GL(m, \mathbb{F}_2)$. An instance is also provided.

Outline. We first give some notations in Sect. 2. Then we give our algorithm and results in Sect. 3, together with some theoretical results. The conclusion comes in Sect. 4.

2 Preliminary

In this section, we first state some notations which will be useful in the rest of the paper. Then two useful propositions of MDS matrices and a definition are given. Please note that all the matrices mentioned in our paper are square matrices unless otherwise stated.

The notation $GL(m, S)$ denotes the set of all $m \times m$ non-singular matrices with entries in S, where S is generally a finite field. For any $a, b \in \mathbb{F}_2$, the operation $a + b$ is called a bit XOR operation. For a matrix $A \in GL(m, \mathbb{F}_2)$, we use $\#A$ to denote the number of XOR operations that is required to calculate $A \cdot x$ where $x \in \mathbb{F}_2^m$. In the paper, we use "XOR counts" instead of "the number of XOR operations" for short. It is easy to see

$$\#A = \sum_{i=1}^{m} (\omega(A[i]) - 1),$$

where $\omega(A[i])$ means the number of nonzero entries in the i-th row of A.

We consider the matrix having the following form:

$$L := (L_{i,j}) = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix},$$

where $L_{i,j} \in GL(m, \mathbb{F}_2)$ for $1 \leq i, j \leq n$. We denote $\mathcal{M}(n, m)$ be the set of all matrices having the above form.

Generally, XOR counts is the number of all the XOR operations. Thus the total XOR operations of L is $\sum_{i,j=1}^{n} (\#L_{i,j}) + m \times (m-1) \times n$, where $m \times (m-1) \times n$ is fixed. For convenience, we define the XOR counts of the matrix $L : \#L = \sum_{i,j=1}^{n} (\#L_{i,j})$.

Square sub-matrices of L of order t means the following matrices

$$L(J, K) := (L_{j_l, k_p}, 1 \leq l, p \leq t)$$

where $J = [j_1, \cdots, j_t]$ and $K = [k_1, \cdots, k_t]$ are two sequences of length t, and $1 \leq j_1 < \cdots < j_t \leq n, 1 \leq k_1 < \cdots < k_t \leq n$.

The following tow propositions are well known.

Proposition 1 (Theorem 1 in [14]) *Let $L \in \mathcal{M}(n, m)$. Then L is a MDS matrix if and only if all square sub-matrices of L of order t are of full rank for $1 \leq t \leq n$.*

In order to speed up the search of MDS matrices, we need to define a stronger equivalent relation between MDS matrices.

Definition 2 *Consider a matrix $L = (L_{i,j}), 1 \leq i, j \leq n$ such that $L_{i,\sigma(i)} = I_m$ and $L_{i,j} = 0$ for $j \neq \sigma(i)$, where I_m is the $m \times m$ identity matrix over $\mathbb{F}_2$ and $\sigma(\cdot)$ is a permutation of $[1, 2, \cdots, n]$. Let $\mathbb{P}$ be a set of all such L's.*

Let $\mathbb{Q}$ be a set of $Diag(L_1, L_2, \cdots, L_n)$, where $L_i \in GL(m, \mathbb{F}_2)$ and $\#L_i = 0$ for $i = 1, 2, \cdots, n$.

For $M, N \in \mathcal{M}(n, m)$, we say M is equivalent to N, if there exists $P_1, P_2 \in \mathbb{P}, Q_1, Q_2 \in \mathbb{Q}$ such that $M = P_1 \cdot Q_1 \cdot N \cdot Q_2 \cdot P_2$.

For any $P \in \mathbb{P}$ and $Q = Diag(L_1, L_2, \cdots, L_n) \in \mathbb{Q}$, where $P_{i,\sigma(i)} = I_m$ and $P_{i,j} = 0$ for $j \neq \sigma(i)$, it is easy to verify that $P \cdot Q = Diag(L_{\sigma(1)}, L_{\sigma(2)}, \cdots, L_{\sigma(n)}) \cdot P$. Therefore, the relation in Definition 3 is an equivalent relation.

Proposition 3 *For $M, N \in \mathcal{M}(n, m)$, if M is equivalent to N, then M is an MDS matrix if and only if N is an MDS matrix.*

Proof. Multiplication by matrices of P and Q only swaps the rows or the columns of every square sub-matrices. The invertibility of the square sub-matrices still holds. Therefore, M is an MDS matrix if and only if N is an MDS matrix.

In simple words, we say two MDS matrices, e.g. M and N, are equivalent, if M can be transformed to N by simply swapping rows and columns in some ways.

According to this equivalence, we define the *row/column-minimal form* of a matrix in $GL(m, \mathbb{F}_2)$. Given $M \in GL(m, \mathbb{F}_2)$ and let r_i be the i-th row of M, $0 < i \leq m$, where r_i can be regarded as a binary number and the most significant bit is the left-most. Thus, the rows of M are comparable. Particularly, we say the i-th row is **lighter** than the j-th row, if the binary number of the i-th row is smaller. If $r_i \leq r_j$ for all i and j such that $0 < i < j \leq m$, we say that M is the row-minimal among all the equivalent matrices. Similarly, we can defined the column-minimal form, where the most significant bit is the top-most. Either of them can be used as representative element of equivalent matrices set. Please note that we use the symbol " · " in matrices to represent 0.

Example 1. Let

$$M = \begin{pmatrix} 1 & 1 & \cdot & 1 \\ \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \end{pmatrix}.$$

Consider its rows as binary number: $r_1 = 1101$, $r_2 = 0101$, $r_3 = 0001$, $r_4 = 0010$. We have $r_3 < r_4 < r_2 < r_1$. Thus its row-minimal form is

$$M_r = \begin{pmatrix} \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & 1 \\ 1 & 1 & \cdot & 1 \end{pmatrix}.$$

In the same way, binary numbers of its columns are $c_1 = 1000$, $c_2 = 1100$, $c_3 = 0001$, $c_4 = 1110$. Then we have $c_3 < c_1 < c_2 < c_4$ and obtain its column-minimal form:

$$M_c = \begin{pmatrix} \cdot & 1 & 1 & 1 \\ \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot \end{pmatrix}.$$

3 Results on 4×4 MDS Matrices

In this section, we describe the algorithm of searching the ligthest 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$ in Sect. 3.1. In Sect. 3.2 we give the results on XOR counts, and focus on the structures of these founded MDS matrices with the minimal XOR counts. In Sect. 3.3, we present some properties of the lightweight 4×4 MDS matrices based on the founded structures.

3.1 Algorithm

To illustrate the algorithm clearly, we give a detailed description of the algorithm for searching 2×2 MDS matrices. The algorithms for $n \times n$ MDS matrices can be obtained by simple generalizations.

A matrix in $\mathcal{M}(n, m)$ is partitioned into n^2 blocks, where each block is a matrix in $GL(m, \mathbb{F}_2)$. The blocks of $\mathcal{M}(2, 4)$ are showed in Figure 1. For the sake of convenience, we write $M = (A, B, C, D)$ if M are partitioned into these 4 blocks. The symbol " $*$ " donates the binary elements in blocks, where the rows or columns with dark shade are always not smaller than the light ones in Figure 1.

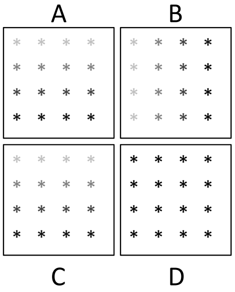

Fig. 1. $2\times$ 2 matrix.

The main idea is to loop over all matrices in $GL(4, \mathbb{F}_2)$ for block A, B, C and D. Then we check whether the 2×2 matrix is of full rank or not. To avoid repetitive search, as shown in Figure 1, for block A and C, we only need to consider the matrices in row-minimal form. As to block B, we only consider the matrices in column-minimal form. Proposition 3 shows that minimal form in this way is enough. It is obvious that any matrix can be transformed to the form in Figuer 1 only by swapping rows and columns. In this way, although we only consider the minimal form of block A,B and C, all the 2×2 matrices are checked actually.

The 2×2 Searching Algorithm searches all candidates and outputs all the 2×2 MDS matrices over $GL(4, \mathbb{F}_2)$.

To avoid the repetitive computations, the algorithm filters out those matrices without minimal forms of block A, B and C in line 4-5, 7-8 and 10-11. By doing

Algorithm 1: The 2 × 2 Searching Algorithm

```
   Output: The set of 2× 2 MDS matrices $L \in \mathcal{M}(2,4)$.
 1 begin
 2     $L \longleftarrow \varnothing$
 3     for every matrix $A \in GL(4,\mathbb{F}_2)$ do
 4         if $A$ is not row-minimal form then
 5             GotoLine 3
 6         for every matrix $B \in GL(4,\mathbb{F}_2)$ do
 7             if $B$ is not column-minimal form then
 8                 GotoLine 6
 9             for every matrix $C \in GL(4,\mathbb{F}_2)$ do
10                 if $C$ is not row-minimal form then
11                     GotoLine 9
12                 for every matrix $D \in GL(4,\mathbb{F}_2)$ do
13                     $D' \longleftarrow C\cdot A^{-1}\cdot B + D$
14                     if $D'$ is invertible then
15                         $M \longleftarrow (A,B,C,D)$, $L \longleftarrow L \cup \{M\}$
16     return $L$
```

computations at line 13, we only need to calculate the rank of D' instead of M. This works because that linear transformation of matrix does not change the rank. If D' is of full rank, then M is of full rank. And we pick out A, B, C and D from the matrice of full rank. Therefore, only calculating the rank of D' is sufficient when we search 2×2 MDS matrices. In practice, to accelerate the algorithm, we can add some limits by setting the maximum available XOR counts.

The algorithm can be generalized to $n \times n$ MDS matrices directly. Here we take the 3×3 Searching Algorithm for example. There are 9 for-loops in the algorithm corresponding to the blocks A-J in (a) of Figure 2. For each loop, the candidates are picked out from the non-singular matrices as well. Thus, steps of checking of sub-matrices of order 1 is omitted.

The sub-matrices of order 2 are constructed in the following sequence: $(A, B, C, D) \longrightarrow (A,B,E,F) \longrightarrow (C,D,E,F) \longrightarrow (A,G,C,H) \longrightarrow (B,G,D,H) \longrightarrow (A,G,E,J) \longrightarrow (B,G,F,J) \longrightarrow (C,H,E,J) \longrightarrow (D,H,F,J)$. The method to calculate the rank of these order 2 sub-matrices is as same as Algorithm 1.

To check whether the sub-matrix of order 3 is of full rank or not, we reduce the block C and E to 0 at first in (b). Then we calculate the rank of $(C\cdot A^{-1}\cdot B+D$, $C\cdot A^{-1}\cdot G+H$, $E\cdot A^{-1}\cdot B+F$, $E\cdot A^{-1}\cdot G+J)$ and check whether it is of full rank or not. After checking all the sub-matrices of order 2 and 3, we can determine whether it is a MDS matrix or not. Please note that block A-J skipped the use of block name I to avoid the confusion with the identity matrix.

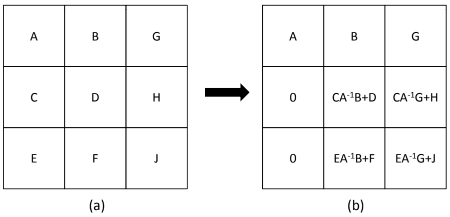

Fig. 2. 3× 3 matrix.

The method for searching 4×4 MDS matrices is similar and we only give the loop order of block in Figure 3 here. In implementation, we always suppose block A to be the identity matrix if we use the algorithm to search the lightweight MDS matrix with XOR counts less than 12. Since we set the upper bound of XOR counts to 12, there are at least 4 blocks with 0 XOR counts. By swapping rows and columns, block A can be transformed to the identity matrix. Please not that we only enumerate row-minimal form for block C, E and G and column-minimal form for block B, J and N. The others are selected from the set of all the non-singular matrices.

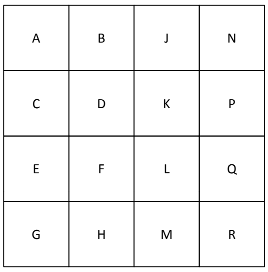

Fig. 3. 4× 4 matrix.

3.2 Structures of the Ligthest 4×4 MDS Matrices over $GL(4, \mathbb{F}_2)$

Li and Wang investigated the constructions of 4×4 lightweight MDS matrices with entries in the set of 4×4 non-singular matrices over $\mathbb{F}_2$ [14]. They found $\#L \geq 12$ and $\#L \geq 16$ for Circulant MDS matrices and Hadamard MDS matrices, respectively.

By our algorithm, we searched all the lightweight matrices $L \in \mathcal{M}(4, 4)$ such that $\#L < 12$, and obtain the following theorem.

Theorem 4. *Let $L \in \mathcal{M}(4, 4)$. If L is a MDS matrix, then $\#L \geq 10$.*

It takes about 1 days to verify that there is no MDS matrix L suth that $\#L \leq 9$. We use less than 2 hours to find the first MDS matrix L with $\#L = 10$, and spend about one week to find out all MDS matrices with 10 XOR counts.

Our platform is Intel i7-4790, 3.6 GHz with 16 GB memory, running Ubuntu 15.04.

We find that all the matrices in $GL(4, \mathbb{F}_2)$ and its number is 20160, where the number of minimal form is 840. In implementation of searching 4×4 MDS matrices, there are 840 candidates for block B, C, E, G, J and N and 20160 candidates for other blocks except block A. Since this experiment aims to find the lower bound of XOR counts of 4×4 MDS matrices over $GL(4, F_2)$, we set the limit of XOR counts. In each loop, we first check the total XOR counts, if it exceeds the value of limit, we ignore it and continue to the next. With the help of these techniques, computational complexity is reduced.

We find that all the MDS matrices with 10 XOR counts can be classified into 3 types with respect to the equivalent relation defined in Definition 2. We summarize the structures of the lightest MDS matrices and obtain some of their properties via direct observations. In other words, the properties given below are only necessary conditions for matrices A, B, X, and Y.

Theorem 5. *If L is a 4×4 MDS matrix over GL(4, $\mathbb{F}_2$) and $\#L = 10$, then L must be equivalent to an MDS matrix having one of the following three types. Let I be the 4×4 identity matrix over $\mathbb{F}_2$.*

1. $\begin{pmatrix} I & I & I & X \\ I & A & B & I \\ I & B & A & A \\ X & I & A & I \end{pmatrix}$, *where $AB = I$ and $X = B^2$.*

2. $\begin{pmatrix} X & I & I & I \\ I & I & A & X \\ I & A & B & I \\ I & X & I & B \end{pmatrix}$, *where $AB = I$ and $X = B^2$.*

3. $\begin{pmatrix} Y & I & I & I \\ I & I & A & B \\ I & A & I & X \\ I & B & X & I \end{pmatrix}$, *where $A + B = X$.*

Some instances are given below.

Example 2. We give one instance for each type.

$$\text{Type1:}\left(\begin{array}{cccc|cccc|cccc|cccc}
1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&1&\cdot\\
\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&1&1&\cdot&\cdot\\
\hline
1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot\\
\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&1&\cdot&\cdot&\cdot&1&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot&\cdot&1\\
\hline
1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&1&1\\
\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot\\
\hline
\cdot&1&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot\\
1&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&1&\cdot\\
1&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1
\end{array}\right)
\quad
\text{Type2:}\left(\begin{array}{cccc|cccc|cccc|cccc}
\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot\\
1&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&1&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1\\
\hline
1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&1&\cdot&\cdot\\
\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&1&\cdot\\
\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&1&1&\cdot\\
\hline
1&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot\\
\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&1\\
\hline
1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&1&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&1&\cdot
\end{array}\right)$$

$$\text{Type3:}\left(\begin{array}{cccc|cccc|cccc|cccc}
1&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot\\
1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&1&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1\\
\hline
1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1\\
\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&1\\
\cdot&\cdot&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&1&1&1&\cdot&\cdot&\cdot&1&\cdot&\cdot\\
\hline
1&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&1\\
\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&\cdot\\
\cdot&\cdot&\cdot&1&1&1&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot\\
\hline
1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&1&1&1&\cdot&\cdot&\cdot\\
\cdot&1&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&1&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&1&\cdot&1&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1
\end{array}\right)$$

Remark 1. The three examples are not the original matrices found. To illustrate that these matrices are symmetric, we rearrangle the blocks in these MDS matrices. The blocks are not in column-minimal or row-minimal form is because we swap the rows and columns to make most of the blocks with XOR counts 0 to be identity matrix.

We obtain 845 MDS matrices in minimal form through the searching algorithm, 364 of them are equivalent to Type 1, 315 of them are equivalent to Type 2 and the other 166 of them are equivalent to Type 3. In these statistic, some matrices are exactly same after swapping rows and columns and the matrices in this situation are counted as well. Please note that not all of these matrices are representatives, the number of representatives in each type should be small. There is an interesting conclusion that under the equivalent relation all the matrices with XOR counts 0 can be transformed into the identity matrix simultaneously. However, the reason is unknown.

3.3 Analyses on the Ligthest 4×4 MDS Matrices

In this section, we give some sufficient and necessary conditions of the lightest 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$. Then we prove that the lower bound of XOR counts in the above structures is 10. At last, we generalize these types to $GL(m, \mathbb{F}_2)$ and give an instance of lightweight 4×4 MDS matrices over $GL(8, \mathbb{F}_2)$ with 10 XOR counts.

Theorem 6. *For the matrices of Type 1 and 2 in Theorem 5 with $AB = I$ and $X = B^2$, they are MDS matrices if and only if*

1. $|B + I| \neq 0$,
2. $|B^2 + B + I| \neq 0$,
3. $|B^3 + B^2 + I| \neq 0$,
4. $|B^3 + B + I| \neq 0$,
5. $|B^6 + B^5 + B^2 + B + I| \neq 0$,

where B is in $GL(m, \mathbb{F}_2)$, and $|B|$ means the determinate of B.

Theorem 7. *For the matrices of Type 3 in Theorem 5 with $X = A + B$, they are MDS matrices if and only if*

1. $YA^2 = I$,
2. $A^2 = B^2 = X^2$,
3. $|A + I| \neq 0$,
4. $|B + I| \neq 0$,
5. $|X + I| \neq 0$,
6. $|Y + I| \neq 0$,

where A, B, X, Y are in $GL(m, \mathbb{F}_2)$, and $|A|$ means the determinate of A.

Given matrices of 3 types, Theorems 6 and 7 are deduced directly from Proposition 1.

Next we present some useful lemmas on XOR counts. Please remember that $\#L$ refers to the XOR counts of L.

Lemma 1. *Given a matrix $B \in GL(m, \mathbb{F}_2)$ such that $|B + I| \neq 0$, then $\#B > 0$.*

Proof. We may assume that $\#B = 0$. Then rows of $\lambda I + (B + I)$ cannot be anything but $(\cdots, \lambda, \cdots)$ or $(\cdots, 1, \cdots, \lambda + 1, \cdots)/\ (\cdots, \lambda + 1, \cdots, 1, \cdots)$. We obtain $\lambda(1, 1, 1, 1, 1, 1, 1, 1)^T$ by adding all the other columns to the first column. Thus, the eigenvalue will be 0 and $|B + I|$ is singular, which is contradictory to the assumption.

Lemma 2. *Given a matrix $B \in GL(m, \mathbb{F}_2)$ with $\#B = 1$ and $X = B^2$, then $\#X \neq 1$.*

Proof. Suppose $\bar{B}$ be a non-singular matrix with $\#\bar{B} = 1$ and its diagonal elements are 1. That is to say, $\bar{B} = I + \dot{B}$, where $\dot{B}$ is a matrix having only 1 non-zero element. It is clearly that $B = P\bar{B}$, where P is a permutation matrix. Thus, we have $X = B^2 = P\bar{B}P\bar{B} = (P\bar{B}P)\cdot(I + \dot{B}) = (P\bar{B}P) + (P\bar{B}P)\dot{B}$. We assume that $\dot{B}[i:j]$(the j-th element in i-th row of $\dot{B}$) is 1 and others are 0. Then matrix X is obtained by adding the i-th columns to the j-th columns of $P\bar{B}P$. And this operation definitely will change the XOR counts of $P\bar{B}P$. Hense we have $\#X \neq 1$.

Lemma 3. *Suppose $A, B \in GL(m, \mathbb{F}_2)$ with $\#A = \#B = 1$, where $m \geq 4$. If there exists $X = A + B$ such that X is non-singular, then $\#X \geq m - 2$.*

Proof. We consider the number of nonzero entries in the i-th row of X. Since X is non-singular, all the rows should be nonzero. Thus we ignore the case that $\omega(X[i]) = 0$.

1. If $\omega(A[i]) = 1$ and $\omega(B[i]) = 1$, we have $\omega(X[i]) = 2$.
2. If $\omega(A[i]) = 1$ and $\omega(B[i]) = 2$, we have $\omega(X[i]) = 1$ or 3. And $\omega(A[i]) = 2$ and $\omega(B[i]) = 1$ is the same.
3. If $\omega(A[i]) = 2$ and $\omega(B[i]) = 2$, we have $\omega(X[i]) = 2$ or 4.

Since $\#A = \#B = 1$, there are at least (m-2) rows fit the situation (1).The other two rows should be nonzero, that is to say, the weight of either of the rows is at least 1. So $\#X \geq 2(m-2) + 2 = m - 2$. Particularly, when $m \geq 4$, we have $\#X \geq 2$.

From the lemmas and Theorem 6, we have the following corollary easily. The corollary gives the lower bound of XOR counts of 4 × 4 MDS matrix over $GL(m, \mathbb{F}_2)$ with $m \geq 4$ in the three types. We must emphasize that there exists 4 × 4 MDS matrix M over $GL(8, \mathbb{F}_2)$ with $\#L = 10$ for Type 1 and Type 2 but not Type 3.

Corollary 8 *Let M be a 4 × 4 MDS matrix over $GL(m, \mathbb{F}_2)$ in one of the three types given by Theorem 5, where $m \geq 4$, then the XOR counts of M is not less than 10.*

Proof. In Type 1 and 2, we observe that $X = B^2$. Then we claim that $X + I$ is non-singular, since $X + I = B^2 + I = (B + I)^2$ and from Theorem 6 we have $|B + I| \neq 0$. Thus, we have $|X + I| \neq 0$. It can be deduced from Lemma 1 and 2 that $\#X \geq 2$. Therefore, the XOR counts of M in Type 1 and 2 is not less than 10.

In Type 3, we have $YA^2 = I$ according to Theorem 7. It is obvious that $\#A^{-1} = 1$ when $\#A = 1$. Since we have $Y = (A^{-1})^2$ and $\#A = 1$, there is no doubt that $\#Y \neq 1$ according to Lemma 2. Besides, $A + I$ is required to be non-singular in Theorem 7. Consequently, the matrix of $A^{-1} + I$ is non-singular as well. So is $Y + I$. Then, we have $\#Y \neq 0$ which is proved in the first paragraph. As to $X = A + B$, we already give its XORs bound in Lemma 3. In this way, we draw the conclusion that XOR counts of M is Type 3 is also bounded by $4m + 2 \geq 10$.

Construction of MDS matrices with XOR counts 10 over $GL(m, \mathbb{F}_2)$, $m > 4$

Before we illustrate the construction of lightweight 4 × 4 MDS matrices, we give a useful proposition on the characteristic polynomial of matrix.

Proposition 9 *Suppose $f_B(\lambda) = |\lambda I - B|$ be the characteristic polynomial of matrix $B \in GL(m, \mathbb{F}_2)$ and $g(x)$ be a polynomial over $\mathbb{F}_2$, $g(B)$ is non-singular if and only if $f_B(x)$ and $g(x)$ has no common factors.*

From the above proposition, we can describe the matrix B in Type 1 and 2 more specifically. Since the characteristic polynomials of B over $GL(m, \mathbb{F}_2)$ are achieved by the conditions in Theorem 6 and Proposition 9, we can select matrix B over $GL(m, \mathbb{F}_2)$ and construct 4 × 4 MDS matrices easily.

Here we give the construction of 4×4 MDS matrix over $GL(8, \mathbb{F}_2)$ whose XOR counts is 10. All the characteristic polynomials of B satisfying the conditions in Theorem 6 are listed in Table 1.

Table 1. Possible characteristic polynomials of matrix B

$x^8 + x^6 + 1$	$x^8 + x^7 + x^6 + x^4 + 1$
$x^8 + x^2 + 1$	$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$
$x^8 + x^7 + x^5 + x^4 + 1$	$x^8 + x^6 + x^5 + x^4 + 1$
$x^8 + x^7 + x^5 + x^3 + 1$	$x^8 + x^6 + x^5 + x^3 + 1$
$x^8 + x^5 + x^4 + x^3 + 1$	$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$
$x^8 + x^7 + x^6 + x^4 + x^2 + 1$	$x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$
$x^8 + x^6 + x^5 + x^2 + 1$	$x^8 + x^7 + x^6 + x + 1$
$x^8 + x^6 + x^4 + x^2 + 1$	$x^8 + x^7 + x^5 + x + 1$
$x^8 + x^7 + x^6 + x^5 + x^2 + 1$	$x^8 + +x^6 + x^5 + x + 1$
$x^8 + x^7 + x^3 + x^2 + 1$	$x^8 + x^7 + x^3 + x + 1$
$x^8 + x^6 + x^3 + x^2 + 1$	$x^8 + x^5 + x^3 + x + 1$
$x^8 + x^5 + x^3 + x^2 + 1$	$x^8 + x^4 + x^3 + x + 1$
$x^8 + x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$
$x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^6 + x^4 + x^3 + x + 1$
$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^2 + x + 1$
$x^8 + x^4 + x^2 + x + 1$	$x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$
$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$	$x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$
$x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$	$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$

We select

$$B = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix},$$

where its characteristic polynomial is $x^8 + x^6 + 1$. Then by equations $AB = I$ and $X = B^2$, we can obtain A and X. Then, we construct a MDS matrix of Type 1 or 2 with 10 XOR counts. Please note that some of the characteristic polynomials in Table 1 may not appropriate for construction of lightest MDS matrix because the XOR counts of matrices corresponding to the characteristic polynomials may not be small enough.

4 Conclusion

In this paper, we find the lightest 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$ via searching all the candidates. Our results demonstrate that lower bound of XOR counts of 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$ is 10. Furthermore, we generalize these structures to $GL(m, \mathbb{F}_2)$ and directly obtain the lightweight MDS with 10 XOR counts. However, we have not applied the algorithm to 4×4 MDS matrices over $GL(8, \mathbb{F}_2)$ yet because of high complexity. We also test all the MDS matrices with 10 XOR counts, and find none is an involutory MDS matrix.

References

1. Shannon, C.E.: Communication theory of secrecy systems. The Bell System Technical Journal **28** (1949) 656–715
2. Sim, S.M., Khoo, K., Oggier, F., Peyrin, T. In: Lightweight MDS involution matrices. Springer Berlin Heidelberg, Berlin, Heidelberg (2015) 471–493
3. Daemen, J., Rijmen, V.: The design of Rijndael : AES - The Advanced Encryption Standard. Information security and cryptography : texts and monographs. Springer (2002)
4. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M. In: The LED block cipher. Springer Berlin Heidelberg, Berlin, Heidelberg (2011) 326–341
5. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher square. In: Proceedings of the 4th International Workshop on Fast Software Encryption. FSE '97, London, UK, UK, Springer-Verlag (1997) 149–165
6. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The simon and speck families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013) http://eprint.iacr.org/2013/404.
7. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C. In: PRESENT: An ultra-lightweight block cipher. Springer Berlin Heidelberg, Berlin, Heidelberg (2007) 450–466

8. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G. In: The simeck family of lightweight block ciphers. Springer Berlin Heidelberg, Berlin, Heidelberg (2015) 307–329
9. Aumasson, J.P., Henzen, L., Meier, W., Naya-Plasencia, M.: Quark: a lightweight hash. Journal of Cryptology **26** (2013) 313–339
10. Guo, J., Peyrin, T., Poschmann, A. In: The PHOTON family of lightweight hash functions. Springer Berlin Heidelberg, Berlin, Heidelberg (2011) 222–239
11. Gupta, C.K., Ray, G.I. In: On constructions of circulant MDS matrices for lightweight cryptography. Springer International Publishing, Cham (2014) 564–576
12. Junod, P., Vaudenay, S. In: Perfect diffusion primitives for block ciphers. Springer Berlin Heidelberg, Berlin, Heidelberg (2005) 84–99
13. Gupta, C.K., Ray, G.I. In: On constructions of involutory MDS matrices. Springer Berlin Heidelberg, Berlin, Heidelberg (2013) 43–60
14. Li, Y., Wang, M. In: On the construction of lightweight circulant involutory MDS matrices. Springer Berlin Heidelberg, Berlin, Heidelberg (2016) 121–139
15. Liu, M., Sim, S.M. In: Lightweight MDS generalized circulant matrices. Springer Berlin Heidelberg, Berlin, Heidelberg (2016) 101–120
16. Sarkar, S., Syed, H.: Lightweight diffusion layer: importance of toeplitz matrices. Cryptology ePrint Archive, Report 2016/835 (2016) http://eprint.iacr.org/2016/835.
17. Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P.: Efficient recursive diffusion layers for block ciphers and hash functions. Journal of Cryptology **28** (2015) 240–256
18. Wu, S., Wang, M., Wu, W. In: Recursive diffusion layers for (lightweight) block ciphers and hash functions. Springer Berlin Heidelberg, Berlin, Heidelberg (2013) 355–371