On the Construction of Involutory MDS Matrices over $\mathbb{F}_{2^m}$*

BAI Jian · SUN Yao · WANG Dingkang

DOI: 10.1007/s11424-019-8125-0
Received: 18 April 2018 / Revised: 11 July 2018

Abstract This paper studies the problem of constructing lightweight involutory maximal distance separable (MDS) matrices. The authors find the exact lower bound of the XOR counts for 4 × 4 involutory MDS matrices over $\mathbb{F}_{2^4}$. Further, some new structures of 4 × 4 involutory MDS matrices over $\mathbb{F}_{2^m}$ are provided to construct involutory MDS matrices and the authors constructed the lightest 4 × 4 involutory MDS matrices over $\mathbb{F}_{2^8}$ so far by using these structures.

Keywords Diffusion layer, involutory MDS matrix, lightweight.

1 Introduction

With the development of science and technology, we have entered the information age. A large number of data provide convenient services to our lives, but at the same time information security has become particularly important. Symmetric ciphers have become the first choice to encrypt a large number of data for their fast speed. Confusion and diffusion are two basic methods to design symmetric ciphers[1]. In order to perform better against linear and differential attacks, the linear branching number and differential branch number of the diffusion matrix should be as large as possible. A matrix which achieves the maximum branch number is an maximal distance separable (MDS) matrix. These matrices ensure the designers perfect linear

BAI Jian
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China; School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China.*
Email: baijian@amss.ac.cn.
SUN Yao
SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093*, China.*
Email: sunyao@iie.ac.cn.
WANG Dingkang
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China; School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China.*
Email: dwang@mmrc.iss.ac.cn.

*This research was supported in part by the National Natural Science Foundation of China under Grant No. 11371356 & 61877058, CAS Project QYZDJ-SSW-SYS022 and the Strategy Cooperation Project AQ-1701.
◇ *This paper was recommended for publication by Editor-in-Chief GAO Xiao-Shan.*

diffusion layers, but the implementation cost can be heavy. Since the inverse of an MDS matrix is required to be implemented in most cases of decryption, one way to save area is to use an involutory MDS matrix.

The general method to construct involutory MDS matrices over finite fields is based on special matrices, such as Hadamard matrices and Cauchy matrices. In 2012, Sajadieh, et al.[2] proposed a method to construct involutory MDS matrices by multiplying one Vandermonde matrix and the inverse of another Vandermonde matrix. Gupta and Ray[3] in 2013 used Cauchy matrices to construct involutory MDS matrices. They both constructed involutory Hadamard MDS matrices over finite fields in different ways. Further, Gupta and Ray provided an equivalence of Cauchy-Hadamard involutory MDS matrices and Vandermonde-Hadamard involutory MDS matrices.

Circulant matrices are often used to construct MDS matrices, but Nakahara and Abrah$\widetilde{\text{a}}$o[4] found that 4×4 circulant matrices over any finite field could never be involutory MDS matrices. In 2014, Gupta and Ray[5] proved that circulant matrices of arbitrary order over finite fields must not be both involutory and MDS. In 2016, Liu and Sim[6] generalized the circulant structures and constructed involutory MDS matries over finite fields with left-circulant matrices. However, they found that any $2^d \times 2^d$ left-circulant matrix over finite fields is not an involutory MDS matrix.

There are mainly two kinds of methods to reduce the number of XOR operations. First, Beierle, et al.[7] and Jean, et al.[8] have relooked at the XOR count of an element and allowed reuse of repeating terms in the product vector. Second, by applying the heuristic algorithms to find a short linear straight-line program to the case of MDS matrices, Kranz, et al.[9] optimized the previous constructions globally. They found that the known constructions, such as Cauchy matrices, circulant matrices and Hadamard matrices, seem to be the same for all randomized constructions. However, we do not consider such optimization and regard XOR count in its simplified form as given by [10] and many subsequent works[11–13].

In this paper, we study the constructions of involutory MDS matrices and present some new results on the lower bound of the XOR counts for the 4×4 involutory matrices. First, we prove for the first time that $16 + 4 \times 3 \times 8$ is the exact lower bound of the XOR counts of 4×4 involutory matrices over $\mathbb{F}_{2^4}$. Second, we propose some new approaches to construct lightweight involutory MDS matrices over $\mathbb{F}_{2^m}$ and find the lightest involutory MDS matrices with $44 + 4 \times 3 \times 8$ XOR counts so far. Our method can also provide new structures to search for global optimization MDS matrices using the way in [9].

We first give some necessary notations in Section 2. A way to search for the lightest 4×4 involutory MDS matrices over $\mathbb{F}_{2^4}$ is given in Section 3. In Section 4, we give some theoretical results on constructing involutory MDS matrices. In Section 5, we construct some involutory MDS matrices over $\mathbb{F}_{2^8}$. The conclusion comes in Section 6.

2 Preliminaries

Let $\mathbb{F}_{2^m}$ be the finite field of 2^m elements. Let $E_{i,j}, i, j = 1, 2, \cdots, n$ be the $n \times n$ matrix over $\mathbb{F}_{2^m}$ whose entries are all zeros except that the i-th row and the j-th column is 1. Denote by $GL(\mathbb{F}_{2^m}, n)$ the set of all the $n \times n$ non-singular matrices with entries in the finite field $\mathbb{F}_{2^m}$. A matrix $L \in GL(\mathbb{F}_{2^m}, n)$ is called involutory, if $L = L^{-1}$. A matrix $L \in GL(\mathbb{F}_{2^m}, n)$ is called MDS, if all the minors of L are nonzero.

We aim to search the involutory MDS matrices over $\mathbb{F}_{2^m}$ and we define the following notation to decrease the complexity.

Definition 2.1 Let $L \in GL(\mathbb{F}_{2^m}, n)$. For any permutation matrix P such that $P \in GL(\mathbb{F}_{2^m}, n)$ and $\omega(P) = n$, we call L is equivalent to PLP^{-1}.

Proposition 2.2 *Under Definition* 2.1, *if two matrices are equivalent, their involutory property, MDS property and XOR counts are all invariant.*

It is easy to verify this property by the definition and this property will be used throughout this paper.

Particularly, we denote $P(i, j) \in GL(\mathbb{F}_{2^m}, n)$ the permutation matrix acquired from the identity matrix by swapping the i-th row and the j-th row, and we call it the elementary permutation transformation. It is obvious that $P(i, j)^{-1} = P(i, j)$. We can prove the following proposition by using the elementary permutation transformations.

Proposition 2.3 *Let* L, $L' \in GL(\mathbb{F}_{2^m}, n)$. *If* L *is equivalent to* L', *then there exists* $i \in \{1, 2, \cdots, n\}$ *such that* $L'_{1,1} = L_{i,i}$ *and the other entries of the first row of* L' *is a permutation of the other entries of the* i*-th row of* L.

Proof Since L is equivalent to L', there exists a permutation matrix P s.t. $PLP^{-1} = L'$. Let $P = \sum_{i=1}^{n} E_{i,\sigma(i)}$, where σ is a permutation of $1, 2, \cdots, n$. Then $L'_{1,1} = L_{\sigma(1),\sigma(1)}$. The equivalent transformation does not change entries of one whole row for any matrix, therefore the other entries of the first row of L' is a permutation of the other entries of the $\sigma(1)$-th of L. The proof is finished. ▮

Remark 2.4 Under a well order in the finite field $\mathbb{F}_{2^m}$, we can choose the largest element $L_{i,j}$ among all the non-diagonal entries of a matrix $L \in GL(\mathbb{F}_{2^m}, n)$. By Proposition 2.3, there exists a matrix L' which is equivalent to L satisfied $L'_{1,2} = L_{i,j}$. It is obvious that $L'_{1,2}$ is the largest non-diagonal entry of L'. In this way, we can save the searching time by only considering the matrices with the largest entry located at position $(1, 2)$.

2.1 XOR Counts of MDS Matrices

It is easy to see that, $\mathbb{F}_{2^m}$ is also an m-dimensional vector space over the field $\mathbb{F}_2$. If a linear basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ is fixed, the linear map $\sigma_a : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}, \sigma_a(x) = ax, a \in \mathbb{F}^*_{2^m}, x \in \mathbb{F}_{2^m}$ can always be equivalently described as $X \mapsto AX$, where $A \in GL(\mathbb{F}_2, m)$ and $X \in \mathbb{F}_2^m$.

The XOR count of an element $a \in \mathbb{F}_{2^m}$ is the number of XOR operations needed to be implement the multiplication of a with arbitrary element $x \in \mathbb{F}_{2^m}$. Theoretically, choose any linear basis of the field $\mathbb{F}_{2^m}$, the representation matrix of $a \in \mathbb{F}_{2^m}$ could implement its multiplication. For $A \in GL(\mathbb{F}_2, m)$, we denote $\omega(A)$ the number of nonzero entries in A. It is easy to know that the number of XOR operations that required to evaluate AX is $\omega(A) - m$, denoted by $\#A$. For example,

$$AX = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_4 \\ x_1 + x_4 \\ x_2 \\ x_3 \end{pmatrix}.$$

Hence, $\#A = 1 = \omega(A) - 4$. For briefness, we write down the nonzero positions in each row of A. We view $[4, [1, 4], 2, 3]$ as A.

The XOR counts of an MDS matrix is the total number of the XOR operations needed to be implemented. Such a matrix L can be implemented in a straightforward way with $\sum_{i,j=1}^{n}(\#L_{i,j}) + m \times (m-1) \times n$ XOR operations. In this paper, we mainly consider the MDS matrices for the case $n = 4$.

3 The Lower Bound of the XOR Counts of Involutory MDS Matries over $\mathbb{F}_{2^4}$

In this section, we prove for the first time that the lower bound of the XOR counts of involutory MDS matries over $\mathbb{F}_{2^4}$ is $16 + 4 \times 3 \times 4$. This lower bound can be found by Algorithm 3.3.

Theorem 3.1 *The lightest 4×4 involutory MDS matrix over $\mathbb{F}_{2^4}$ has $16 + 4 \times 3 \times 4$ XOR operations. Furthermore, all the involutory MDS matrices with XOR counts $\mathbb{F}_{2^4}$ must be equivalent to one of the following three matrices:*

$$A_1 = \begin{pmatrix} 1 & \alpha & \alpha^3 & \alpha^2 \\ 1 & 1 & \alpha & \alpha^3 \\ \alpha^2 & \alpha & 1 & \alpha \\ 1 & \alpha^2 & 1 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} \alpha & \alpha^3 & 1 & \alpha \\ \alpha^2 & \alpha & 1 & 1 \\ 1 & \alpha & \alpha & \alpha^3 \\ 1 & 1 & \alpha^2 & \alpha \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & \alpha & \alpha & \alpha^3 \\ 1 & 1 & \alpha^2 & \alpha \\ \alpha & \alpha^3 & 1 & \alpha \\ \alpha^2 & \alpha & 1 & 1 \end{pmatrix},$$

where α is a root of the irreducible polynomial $X^4 + X + 1$.

Remark 3.2 Sarkar and Syed[12] constructed a matrix which is equivalent to A_3. But the above theorem shows that there are no involutory MDS matrices with fewer XOR counts and every lightest involutory MDS matrices must be equivalent to one of A_1, A_2 and A_3.

The polynomial $x^4 + x + 1$ is primitive over $\mathbb{F}_2$. Let α be a root of $x^4 + x + 1 = 0$, then any element of $\mathbb{F}_{2^4}$ can be represented as the power of α. During the search, we find that choosing a basis first and then traversing matrices is much faster than traversing matrices over the field $\mathbb{F}_{2^m}$ directly. In this way, we enumerate all the bases to search for all the involutory MDS matrices whose XOR count is at most $16 + 4 \times 3 \times 4$. It takes only in a few minutes. During the search, we also find the following facts:

1) There are 2^{16} matrices of 4×4 over $\mathbb{F}_2$. Among them, there are 1344 matrices whose minimal polynomial is $x^4 + x + 1$. For $A \in GL(\mathbb{F}_2, 4)$ with minimal polynomial $x^4 + x + 1$, we

call $(\#A, \#A^2, \cdots, \#A^{15})$ an XOR count sequence of the whole field. Then there are only 35 different XOR counts sequences of the whole field.

2) Assume that L is an involutory matrix to search. If we know the values of $L_{1,1}, L_{1,2}, L_{1,3}$, $L_{1,4}$, $L_{2,1}, L_{2,2}$, $L_{3,1}, L_{3,2}$, then the other 8 entries of L can be derived by the involutory and MDS property. First, $L_{4,1}$ is obtained since the product of first row and the first column equals one. Second, $L_{4,2}$ is obtained since the first row is orthogonal to the second column. Because L is an MDS matrix, $L_{3,1}L_{4,2}+L_{3,2}L_{4,1}$ is invertible. Then the other six entries can be obtained by the involutory property. Finally, $L_{3,3}$ and $L_{3,4}$ can be obtained by solving two linear equations, these equations are obtained by products of the third row of L and the first two columns of L. $L_{4,3}$ and $L_{4,4}$ are computed similarly. $L_{2,3}$ and $L_{2,4}$ can be computed directly.

Algorithm 3.3 (The 4×4 Searching Algorithm)
Input The finite field $\mathbb{F}_{2^4}$ with a primitive element α s.t. $\alpha^4 + \alpha = 1$.
Output The set of 4×4 involutory MDS matrices $L \in GL(\mathbb{F}_{2^4}, 4)$.

```
begin
    $LS \longleftarrow \varnothing, S \longleftarrow \varnothing$
    for every matrix $A \in GL(4, F_2)$ do
        if the minimal polynomial of $A$ is $x^4 + x + 1$ then
            $S \longleftarrow S \cup (\#A, \#A^2, \cdots, \#A^{15})$
    for $L_{1,1}, L_{1,2}, L_{1,3}, L_{1,4}, L_{2,1}, L_{2,2}, L_{3,1}, L_{3,2} \in \mathbb{F}_{2^4}^*$ do
        $L_{4,1} \longleftarrow L_{1,4}^{-1}(L_{1,1}^2 + L_{1,2}L_{2,1} + L_{1,3}L_{3,1} + 1)$            $(*)$
        $L_{4,2} \longleftarrow L_{1,4}^{-1}(L_{1,1}L_{1,2} + L_{1,2}L_{2,2} + L_{1,3}L_{3,2})$            $(*)$
        if $L_{3,1}L_{4,2}$ equals $L_{3,2}L_{4,1}$ then
            continue to the next loop of for
        $M \longleftarrow (L_{3,1}L_{4,2} + L_{3,2}L_{4,1})^{-1}$            $(**)$
        $L_{3,3} \longleftarrow M(L_{4,2}(L_{1,1}L_{3,1} + L_{2,1}L_{3,2}) + L_{4,1}(L_{1,2}L_{3,1} + L_{2,2}L_{3,2}))$            $(**)$
        $L_{3,4} \longleftarrow M(L_{3,2}(L_{1,1}L_{3,1} + L_{2,1}L_{3,2}) + L_{3,1}(L_{1,2}L_{3,1} + L_{2,2}L_{3,2}))$            $(**)$
        $L_{4,3} \longleftarrow M(L_{4,2}(L_{1,1}L_{4,1} + L_{2,1}L_{4,2}) + L_{4,1}(L_{1,2}L_{4,1} + L_{2,2}L_{4,2}))$            $(**)$
        $L_{4,4} \longleftarrow M(L_{3,2}(L_{1,1}L_{4,1} + L_{2,1}L_{4,2}) + L_{3,1}(L_{1,2}L_{4,1} + L_{2,2}L_{4,2}))$            $(**)$
        $L_{2,3} \longleftarrow L_{1,2}^{-1}(L_{1,1}L_{1,3} + L_{1,3}L_{3,3} + L_{1,4}L_{4,3})$            $(**)$
        $L_{2,4} \longleftarrow L_{1,2}^{-1}(L_{1,1}L_{1,4} + L_{1,3}L_{3,4} + L_{1,4}L_{4,4})$            $(**)$
        $L \longleftarrow \begin{pmatrix} L_{1,1} & L_{1,2} & L_{1,3} & L_{1,4} \\ L_{2,1} & L_{2,2} & L_{2,3} & L_{2,4} \\ L_{3,1} & L_{3,2} & L_{3,3} & L_{3,4} \\ L_{4,1} & L_{4,2} & L_{4,3} & L_{4,4} \end{pmatrix}$            $(***)$
        for every sequence $seq \in S$ do
            compute $\#L$ with XOR counts in $seq$
        if the minimum value of $\#L$ is less than 16 then
            continue to the next loop of for
        if $L$ is involutory and MDS then
            $LS \longleftarrow LS \cup \{L\}$
    return $LS$
end
```

3.1 Algorithm

As we know that, there are many matrix representations of elements in a finite field. when searching for light MDS matrices, it is difficult to traverse all the matrix representation. In fact, the searching depends only on the XOR counts of elements in the given finite field rather than a specific matrix representation. Thus, we compute all the XOR count sequences in the begining. Our algorithm only searches for involutory MDS matrices, not non-involutory MDS matrices. We can only loop half of the entries in the matrix while the others can be computed directly due to the property of involutory. In lines marked $(*)$ of Algorithm 3.3, $L_{4,1}$ and $L_{4,2}$ are obtained since the product of the first row of the involutory matrix L and the first two columns of L are 1 and 0 respectively. Since L is an MDS matrix, the 2×2 submatrix $\left(\begin{smallmatrix} L_{3,1} & L_{3,2} \\ L_{4,1} & L_{4,2} \end{smallmatrix}\right)$ is invertible, that is $L_{3,1}L_{4,2} \neq L_{3,2}L_{4,1}$. Once $L_{3,1}L_{4,2} \neq L_{3,2}L_{4,1}$ is satisfied, we can obtain $L_{3,3}, L_{3,4}, L_{4,3}$ and $L_{4,4}$ by solving the linear equation system, which are concluded from the product of the last two rows of the involutory matrix L and the first two columns of L. So far every entry of L has been determined except $L_{2,3}$ and $L_{2,4}$. They can be computed directly by the product of the the first row of L and the last two columns of L. In lines marked $(**)$ of Algorithm 3.3, we show the exact formula to compute all the entries mentioned above. The lightest involutory MDS matrix L must satisfy that $\#L \leq 16$ from [12]. Comparing with verifying the MDS property of L, verifying the XOR counts is much faster. There are still a lot of MDS matrices after the line marked $(***)$, while few of them are lighter than 17 in a certain matrix representation. And verifying the XOR counts is much faster than verifying the MDS property of L. Thus, we decide to verify the XOR counts first.

4 New Approaches to Construct Involutory MDS Matrices

In this section we present some theoretical results on constructing involutory MDS matrices. Unlike the common used circulant matrix and the Hadamard matrix, we find some new structures to obtain new lightweight involutory MDS matrices.

Theorem 4.1 *Let $L \in GL(\mathbb{F}_{2^m}, n)$. If L is involutory, then*

$$Trace(L) = \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 0, & \text{if } n \text{ is even.} \end{cases}$$

Proof Let $L' = L^2$. Because L is involutory, we have $L'_{i,i} = \sum_{k=1}^{n} L_{i,k}L_{k,i} = 1$. Then

$$\sum_{i=1}^{n} L'_{i,i} = \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 0, & \text{if } n \text{ is even.} \end{cases}$$

On the other hand,

$$\begin{aligned}\sum_{i=1}^{n} L'_{i,i} = \sum_{i,k=1}^{n} L_{i,k}L_{k,i} &= \sum_{1\le k<i\le n} L_{i,k}L_{k,i} + \sum_{1\le i<k\le n} L_{i,k}L_{k,i} + \sum_{1\le k=i\le n} L_{i,k}L_{k,i}\\ &= \sum_{1\le k<i\le n} L_{i,k}L_{k,i} + \sum_{1\le k<i\le n} L_{k,i}L_{i,k} + \sum_{1\le i\le n} L_{i,i}^2\\ &= \sum_{1\le k<i\le n} (L_{i,k}L_{k,i} + L_{k,i}L_{i,k}) + \Bigg(\sum_{1\le i\le n} L_{i,i}\Bigg)^2\\ &= Trace(L)^2.\end{aligned}$$

Therefore,

$$Trace(L)^2 = \begin{cases} 1, & \text{if } n \text{ is odd,}\\ 0, & \text{if } n \text{ is even.}\end{cases}$$

This means $Trace(L) \in \mathbb{F}_2$ and then

$$Trace(L) = Trace(L)^2 = \begin{cases} 1, & \text{if } n \text{ is odd,}\\ 0, & \text{if } n \text{ is even.}\end{cases}$$

∎

By Theorem 4.1, we make a more detailed analysis on the structure of involutory MDS matrices in the following theorem.

Theorem 4.2 *Let $L \in GL(\mathbb{F}_{2^m}, 4)$. If L is an involutory MDS matrix, then*

$$(L_{1,1} + L_{3,3})(L_{1,1} + L_{4,4}) = L_{1,2}L_{2,1} + L_{3,4}L_{4,3}.$$

Further, given $L_{1,1}, L_{1,2}, L_{2,1}, L_{2,2}, L_{3,3}, L_{3,4}, L_{4,3}, L_{4,4}$, then

$$(L_{1,3}, L_{1,4}, L_{2,3}, L_{2,4})^{\mathrm{T}} \textit{and } (L_{4,2}, L_{3,2}, L_{4,1}, L_{3,1})^{\mathrm{T}}$$

are solutions of a linear equation system $M\widetilde{X} = 0$, where

$$M = \begin{pmatrix} L_{1,1}+L_{3,3} & L_{4,3} & L_{1,2} & 0\\ L_{3,4} & L_{1,1}+L_{4,4} & 0 & L_{1,2}\\ L_{2,1} & 0 & L_{1,1}+L_{4,4} & L_{4,3}\\ 0 & L_{2,1} & L_{3,4} & L_{1,1}+L_{3,3}\end{pmatrix}, \qquad (\star)$$

and

$$X = \begin{pmatrix} x_1 & x_2\\ x_3 & x_4\end{pmatrix}, \quad \widetilde{X} = (x_1, x_2, x_3, x_4)^{\mathrm{T}} \in \mathbb{F}_{2^m}^4.$$

And the Rank of M is 2.

Proof For simplicity, we set

$$A=\begin{pmatrix} L_{1,1} & L_{1,2} \\ L_{2,1} & L_{2,2} \end{pmatrix},\ B=\begin{pmatrix} L_{1,3} & L_{1,4} \\ L_{2,3} & L_{2,4} \end{pmatrix},\ C=\begin{pmatrix} L_{3,1} & L_{3,2} \\ L_{4,1} & L_{4,2} \end{pmatrix} \text{ and } D=\begin{pmatrix} L_{3,3} & L_{3,4} \\ L_{4,3} & L_{4,4} \end{pmatrix}.$$

Let $L' = L^2$, since L is involutory, $L'_{1,3} = L'_{1,4} = L'_{2,3} = L'_{2,4} = L'_{3,1} = L'_{3,2} = L'_{4,1} = L'_{4,2} = 0$. Then we have

$$AB = BD \tag{1}$$

and

$$CA = DC. \tag{2}$$

Since L is an MDS matrix and C is a submatrix of L, then C is invertible. From (2), we have $AC^{-1} = C^{-1}D$. Define

$$C^* = |C|\cdot C^{-1} = \begin{pmatrix} L_{4,2} & L_{3,2} \\ L_{4,1} & L_{3,1} \end{pmatrix}.$$

It is easy to see that $AC^* = C^*D$. Thus, we only need to consider $AX = XD$, that is,

$$\begin{cases} L_{1,1}x_1 + L_{1,2}x_3 = L_{3,3}x_1 + L_{4,3}x_2, \\ L_{1,1}x_2 + L_{1,2}x_4 = L_{3,4}x_1 + L_{4,4}x_2, \\ L_{2,1}x_1 + L_{2,2}x_3 = L_{3,3}x_3 + L_{4,3}x_4, \\ L_{2,1}x_2 + L_{2,2}x_4 = L_{3,4}x_3 + L_{4,4}x_4. \end{cases}$$

By Theorem 4.1, we have $L_{1,1} + L_{2,2} + L_{3,3} + L_{4,4} = 0$. Thus, we rewrite the above equations as $M\widetilde{X} = 0$, where M is consistent with $(\star)$ and $\widetilde{X} = (x_1, x_2, x_3, x_4)^{\mathrm{T}}$.

Define $\widetilde{B} = (L_{1,3}, L_{1,4}, L_{2,3}, L_{2,4})^{\mathrm{T}}$ and $\widetilde{C^*} = (L_{4,2}, L_{3,2}, L_{4,1}, L_{3,1})^{\mathrm{T}}$, they must be the solutions of $M\widetilde{X} = 0$.

Since L is an MDS matrix, $M\widetilde{X} = 0$ have nonzero solutions, that is to say $|M| = 0$. Set $E = (L_{1,1} + L_{3,3})(L_{1,1} + L_{4,4}) + L_{1,2}L_{2,1} + L_{3,4}L_{4,3}$, it is easy to see that $|M| = E^2 = 0$, i.e., $E = 0$. Further, by straight calculations, we find that E divides all the minors of order 3 of M. Thus, all the minors of order 3 of M are zero. From this, we obtain that the rank of M is at most 2. Then the rank of M is exactly 2 due to the fact that the first two rows of M are linear independent. ▌

If all the diagonal entries are equal, we have the following corollary.

Corollary 4.3 *Let $L \in GL(\mathbb{F}_{2^m}, 4)$ and all the diagonal entries are equal. L is an involutory MDS matrix if and only if there exist $p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8 \in \mathbb{F}^*_{2^m}$ such that*

$$L = \begin{pmatrix} p_1 & p_4 & p_2^{-1}p_4p_6 & p_5 \\ p_3 & p_1 & p_2^{-1}p_3p_5 & p_6 \\ p_8 & p_7 & p_1 & p_2 \\ p_2^{-1}p_3p_7 & p_2^{-1}p_4p_8 & p_2^{-1}p_3p_4 & p_1 \end{pmatrix}$$

with

$$p_1^2p_2 + p_2p_3p_4 + p_3p_5p_7 + p_4p_6p_8 = p_2, \quad p_5p_8 = p_6p_7$$

and

$$p_1p_7 \neq p_4p_8, \quad p_1^2p_2 \neq p_3p_5p_7, \quad p_1p_6 \neq p_3p_5, \quad p_3p_5^2 \neq p_4p_6^2,$$
$$p_1p_2 \neq p_5p_8, \quad p_1^2 \neq p_3p_4, \quad p_1^2p_2 \neq p_4p_6p_8, \quad p_2p_4 \neq p_5p_7, \quad p_2p_3 \neq p_6p_8.$$

Proof The sufficiency of the corollary can be proved by straight calculations. Here we only prove the necessity. Since all the diagonal entries of L are equal, the conclusion of Theorem 4.2 that $M\widetilde{X} = 0$ can be rewrite as

$$\begin{pmatrix} 0 & L_{4,3} & L_{1,2} & 0 \\ L_{3,4} & 0 & 0 & L_{1,2} \\ L_{2,1} & 0 & 0 & L_{4,3} \\ 0 & L_{2,1} & L_{3,4} & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0. \tag{3}$$

Substituting $\widetilde{X}$ by $(L_{1,3}, L_{1,4}, L_{2,3}, L_{2,4})^{\mathrm{T}}$, it is obvious that

$$L_{1,3}L_{3,4} = L_{2,4}L_{1,2}, \tag{4}$$
$$L_{1,4}L_{2,1} = L_{2,3}L_{3,4}. \tag{5}$$

Substituting $\widetilde{X}$ by $(L_{4,2}, L_{3,2}, L_{4,1}, L_{3,1})^{\mathrm{T}}$, it is obvious that

$$L_{4,2}L_{3,4} = L_{3,1}L_{1,2}, \tag{6}$$
$$L_{3,2}L_{2,1} = L_{4,1}L_{3,4}. \tag{7}$$

Further, we also have that

$$L_{1,2}L_{2,1} = L_{3,4}L_{4,3} \tag{8}$$

by the conclusion of Theorem 4.2 that $(L_{1,1} + L_{3,3})(L_{1,1} + L_{4,4}) = L_{1,2}L_{2,1} + L_{3,4}L_{4,3}$.

Set $L_{1,1} = L_{2,2} = L_{3,3} = L_{4,4} = p_1,\ L_{3,4} = p_2,\ L_{2,1} = p_3,\ L_{1,2} = p_4, L_{1,4} = p_5,\ L_{2,4} = p_6,\ L_{3,2} = p_7,\ L_{3,1} = p_8$. From (4)–(8), we can obtain

$$L_{1,3} = p_2^{-1}p_4p_6,\ L_{2,3} = p_2^{-1}p_3p_5,\ L_{4,2} = p_2^{-1}p_4p_8,\ L_{4,1} = p_2^{-1}p_3p_7,\ L_{4,3} = p_2^{-1}p_3p_4,$$

respectively.

At this time, we have

$$L^2 = \begin{pmatrix} p_1 & p_4 & p_2^{-1}p_4p_6 & p_5 \\ p_3 & p_1 & p_2^{-1}p_3p_5 & p_6 \\ p_8 & p_7 & p_1 & p_2 \\ p_2^{-1}p_3p_7 & p_2^{-1}p_4p_8 & p_2^{-1}p_3p_4 & p_1 \end{pmatrix}^2$$

$$= \begin{pmatrix} f & (p_4p_5p_8 + p_4p_6p_7)/p_2 & 0 & 0 \\ (p_3p_5p_8 + p_3p_6p_7)/p_2 & f & 0 & 0 \\ 0 & 0 & f & p_5p_8 + p_6p_7 \\ 0 & 0 & (p_3p_4p_5p_8 + p_3p_4p_6p_7)/p_2^2 & f \end{pmatrix},$$

where $f = (p_1^2p_2 + p_2p_3p_4 + p_3p_5p_7 + p_4p_6p_8)/p_2$.

Because L is an involutory MDS matrix, then

$$\begin{cases} (p_1^2p_2 + p_2p_3p_4 + p_3p_5p_7 + p_4p_6p_8)/p_2 = 1, \\ (p_4p_5p_8 + p_4p_6p_7)/p_2 = 0, \\ (p_3p_5p_8 + p_3p_6p_7)/p_2 = 0, \\ p_5p_8 + p_6p_7 = 0, \\ (p_3p_4p_5p_8 + p_3p_4p_6p_7)/p_2^2 = 0. \end{cases}$$

None of $p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8$ equals 0, thus

$$p_1^2p_2 + p_2p_3p_4 + p_3p_5p_7 + p_4p_6p_8 = p_2, \quad p_5p_8 = p_6p_7.$$

Since L is an MDS matirx, all the minors of L are invertible. We factorize all the minors of L and obtain that

$$p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8 \in \mathbb{F}_{2^m}^*, \quad p_1p_7 \neq p_4p_8, \quad p_1^2p_2 \neq p_3p_5p_7, \quad p_1p_6 \neq p_3p_5,$$
$$p_3p_5^2 \neq p_4p_6^2, \quad p_1p_2 \neq p_5p_8, \quad p_1^2 \neq p_3p_4, \quad p_1^2p_2 \neq p_4p_6p_8, \quad p_2p_4 \neq p_5p_7, \quad p_2p_3 \neq p_6p_8.$$

The proof is finished. ∎

If $p_1 = p_3 = 1, p_2 = p_4$ in Corollary 4.3, then we have the following corollary.

Corollary 4.4 *Let*

$$L = \begin{pmatrix} 1 & p_2 & p_6 & p_5 \\ 1 & 1 & p_2^{-1}p_5 & p_6 \\ p_8 & p_7 & 1 & p_2 \\ p_2^{-1}p_7 & p_8 & 1 & 1 \end{pmatrix} \in GL(\mathbb{F}_{2^m}, 4).$$

Then L is involutory MDS if and only if $p_2^2 = p_5p_7 + p_2p_6p_8,\ p_5p_8 = p_6p_7$ and

$$p_7 \neq p_2p_8,\ p_2 \neq p_5p_7,\ p_5 \neq p_6,\ p_5^2 \neq p_2p_6^2,\ p_2 \neq p_5p_8,\ p_2 \neq 1,\ p_6p_8 \neq 1.$$

When we search for involutory MDS matrices in the shape of that in Corollory 4.4, we only need to loop three entries of that matrix and verify those inequations. This is similar to searching for involutory matrices in the shape of Hadamard matrices. However, we can find lighter involutory MDS matrices in the shape of the matrix in Collory 4.4 than Hadamard matrices. From this perspective, our construction is better than Hadamard matrices.

5 Searching for Involutory MDS Matrices with Minimum XOR Counts

To the best of our knowledge, researchers have searched for lightweight involutory MDS matrices in the shape of Hadamard matrices[14] or a general case of Hadamard matrices[12]. The latter can be viewed as a special case of L that we presented in Corollary 4.3. They have found involutory MDS matrices with XOR count $64+4\times 3\times 8$ over $\mathbb{F}_{2^8}$.

In the past, researchers used to chose the polynomial bases when searching for lightweight MDS matrices. However, irreducible polynomials with degree 8 over $\mathbb{F}_{2^8}$ have at least five terms, leading to that the matrices under the polynomial basis have at least three XOR operations. Actually, there exist matrices with two XOR operations which can be regarded as the representation of some elements in $\mathbb{F}_{2^8}$[7]. We use these matrices to search for involutory MDS matrices with the shape in Corollary 4.4 and find involutory MDS matrices with XOR count $44+4\times 3\times 8$ over $\mathbb{F}_{2^8}$.

Theorem 5.1 *Let $L_1, L_2 \in GL(\mathbb{F}_{2^m}, 4)$, such that*

$$L_1 = \begin{pmatrix} 1 & x & 1 & x^2 \\ 1 & 1 & x & 1 \\ x(x^3+1)^{-1} & x^3(x^3+1)^{-1} & 1 & x \\ x^2(x^3+1)^{-1} & x(x^3+1)^{-1} & 1 & 1 \end{pmatrix},$$

$$L_2 = \begin{pmatrix} 1 & x & x & 1 \\ 1 & 1 & x^{-1} & x \\ x^3(x^3+1)^{-1} & x^2(x^3+1)^{-1} & 1 & x \\ x(x^3+1)^{-1} & x^3(x^3+1)^{-1} & 1 & 1 \end{pmatrix}.$$

Then for all $x \in \mathbb{F}_{2^m}$, L_1, L_2 are both involutory matrices and the following conditions are equivalent:

1) *L_1 is an MDS matrix.*

2) *L_2 is an MDS matrix.*

3) *The degree of the minimal polynomial of x over $\mathbb{F}_2$ is ≥ 4 and $x^4+x^3 \neq 1$.*

Proof The conclusions in Theorem 5.1 can be obtained by the definition of involutory matrices and Corollary 4.4 directly. ∎

Here we give two matrices in the shape of L_1 and L_2 in Theorem 5.1 with XOR count $44 + 4 \times 3 \times 8$ below.

Example 5.2 If α is a root of the irreducible polynomial $X^8 + X^5 + X^3 + X^2 + 1$, then

$$\begin{pmatrix} 1 & \alpha & 1 & \alpha^2 \\ 1 & 1 & \alpha & 1 \\ \alpha^{218} & \alpha^{220} & 1 & \alpha \\ \alpha^{219} & \alpha^{218} & 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \alpha & \alpha & 1 \\ 1 & 1 & \alpha^{-1} & \alpha \\ \alpha^{220} & \alpha^{219} & 1 & \alpha \\ \alpha^{218} & \alpha^{220} & 1 & 1 \end{pmatrix}$$

are both involutory MDS matrices over $\mathbb{F}_{2^8}$. Choosing the present matrix $[[2,4],3,1,5,6,[2,7],8,4]$ for α under the basis $\alpha^5+1, \alpha^7+\alpha^2, \alpha^6+\alpha, \alpha^4, \alpha^3, \alpha^2, \alpha, 1$, then XOR counts of $1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{218}, \alpha^{219}, \alpha^{220}$ are $0, 2, 3, 4, 9, 8, 8$, respectively. So the XOR counts of these two matrices are both $44 + 4 \times 3 \times 8$.

We compare our findings with the previous results in Table 1. For $\mathbb{F}_{2^4}$, we achieve the previously known lower bound. For $\mathbb{F}_{2^8}$ we present a new lower bound of XOR count of 4×4 involutory MDS matrices which is $44 + 4 \cdot 3 \cdot 8$.

Table 1 Comparison of 4×4 involutory MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$

Matrix		Implementation	Ref.
Field/Ring	Type	XOR	
$\mathbb{F}_{2^4}/0x13$	Arbitrary	$20 + 4 \cdot 3 \cdot 4$	[8]
$\mathbb{F}_{2^4}/0x13$	Hadamard-like	$16 + 4 \cdot 3 \cdot 4$	[12]
$\mathbb{F}_{2^4}/0x13$	Hadamard	$24 + 4 \cdot 3 \cdot 4$	Joltik
$\mathbb{F}_{2^4}$	Arbitrary	$16 + 4 \cdot 3 \cdot 4$	Theorem 3.1
$\mathbb{F}_{2^8}/0x165$	Hadamard-like	$64 + 4 \cdot 3 \cdot 8$	[12]
$\mathbb{F}_{2^8}/0x11b$	Hadamard-Cauchy	$216 + 4 \cdot 3 \cdot 8$	[15]
$\mathbb{F}_{2^8}/0x11b$	Hadamard-Cauchy	$296 + 4 \cdot 3 \cdot 8$	[3]
$\mathbb{F}_{2^8}/0x11d$	Hadamard	$88 + 4 \cdot 3 \cdot 8$	Anubis
$\mathbb{F}_{2^8}/0x165$	Hadamard	$64 + 4 \cdot 3 \cdot 8$	[14]
$\mathbb{F}_{2^8}$	Arbitrary	$44 + 4 \cdot 3 \cdot 8$	Example 5.2

6 Conclusion

In this paper, we give some theoretical results on 4×4 involutory MDS matrices over $\mathbb{F}_{2^m}$. These results help us find new structures to construct involutory matrices and improve the efficiency of searching for involutory MDS matrices. We find that the exact lower bound of the XOR count of 4×4 involutory MDS matrices over $\mathbb{F}_{2^4}$ is $16 + 4 \times 3 \times 4$. We also improved the lower bound of XOR counts of involutory MDS matrices over $\mathbb{F}_{2^8}$.

The exact lower bounds of XOR counts of involutory MDS matrices over $\mathbb{F}_{2^8}$ are still unknown. We leave it for the future research.

References

[1] Shannon C E, Communication theory of secrecy systems, *The Bell System Technical Journal*, 1949, **28**(4): 656–715.

[2] Sajadieh M, Dakhilalian M, Mala H, et al., On construction of involutory MDS matrices from Vandermonde matrices in $GF(2^q)$, *Des. Codes Cryptography*, 2012, **64**(3): 287–308.

[3] Gupta K C and Ray I G, On constructions of involutory MDS matrices, *Progress in Cryptology – AFRICACRYPT* 2013, Eds. by Youssef M, Nitaj A, and Hassanien A E, Cairo, 2013.

[4] Nakahara J and Abrahão E, A new involutory MDS matrix for the AES, *International Journal of Network Security*, 2009, **9**(2): 109–116.

[5] Gupta K C and Ray I G, On constructions of circulant MDS matrices for lightweight cryptography, *ISPEC* 2014, Eds. by Huang X and Zhou J, Fuzhou, China, 2014.

[6] Liu M and Sim S M, Lightweight MDS generalized circulant matrices, *FSE* 2016, Eds. by Peyrin T, Bochum, 2016.

[7] Beierle C, Kranz T, and Leander G, Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices, *FSE* 2016, Ed. by Peyrin T, Bochum, 2016.

[8] Jean J, Peyrin T, Sim S M, et al., Optimizing implementations of lightweight building blocks, *IACR Transactions on Symmetric Cryptology*, 2017, **2017**(4): 130–168.

[9] Kranz T, Leander G, Stoffelen K, et al., Shorter linear straight-line programs for MDS matrices, *IACR Transactions on Symmetric Cryptology*, 2017, **2017**(4): 188–211.

[10] Khoo K, Peyrin P, Poschmann A, et al., Foam: Searching for hardware-optimal SPN structures and components with a fair comparison, *Cryptographic Hardware and Embedded Systems — CHES* 2014, Eds. by Batina L and Robshwa M, Busan, South Korea, 2014.

[11] Li Y and Wang M, On the construction of lightweight circulant involutory MDS matrices, *FSE* 2016, Ed. by Peyrin T, Bochum, 2016.

[12] Sarkar S and Syed H, Lightweight diffusion layer: Importance of Toeplitz matrices, *IACR Transactions on Symmetric Cryptology*, 2016, **2016**(1): 95–113.

[13] Bai J, Li T, Sun Y, et al., The lightest 4 × 4 MDS matrices over $GL(4, \mathbb{F}_2)$, *Cryptology ePrint Archive*, Report 2016/686, 2016, https: //eprint.iacr.org/2016/686.

[14] Sim S M, Khoo K, Oggier F, et al., Lightweight MDS involution matrices, *FSE* 2015, Ed. by Leander G, Istanbul, 2015.

[15] Cui T, Jin C, and Kong Z, On compact Cauchy matrices for substitution-permutation networks, *IEEE Transactions on Computers*, 2015, **64**(7): 2098–2102.