Construction and Filtration of Lightweight Formalized MDS Matrices

Zhang Shi-Yi, Wang Yong-juan, Gao Yang, Wang Tao

Corresponding author: Wang Yong-juan, E-mail: pinkywyj@163.com

Abstract: The 4×4 MDS matrix over F_2 is widely used in the design of block cipher's linear diffusion layers. However, considering the cost of a lightweight cipher's implementation, the sum of XOR operations of a MDS matrix usually plays the role of measure. During the research on the construction of the lightweight 4×4 MDS matrices, this paper presents the concept of formalized MDS matrix: some of the entries that make up the matrix are known, and their positions are determined, and the criterions of the MDS matrix is satisfied. In this paper, using the period and minimal polynomial theory of entries over finite fields, a new construction method of formalized MDS matrices is proposed. A large number of MDS matrices can be obtained efficiently by this method, and their number distribution has significant structural features. However, the algebraic structure of the lightest MDS matrices is also obvious. This paper firstly investigates the construction of 4×4 lightweight MDS matrices, analyzes the distribution characteristics of the them, and the feasibility of the construction method. Then, for the lightest MDS matrices obtained from the method above, the algebraic relations in themselves and between each other are studied, and the important application of the alternating group A_4 and it's subgroup, the Klein four-group is found.

Key words: block cipher; linear diffusion layer; MDS matrix; the alternating group; minimal polynomial;

1 Introduction

As a mainstream design method of block ciphers' linear diffusion layers[1-2], 4×4 MDS matrices have a wide application in many excellent cryptographic algorithms, such as AES[3] , SQUARE[4] . How to construct MDS matrices with XORs as few as possible efficiently is the focus of nowadays research. There are three main methods of constructing a MDS matrix. First is to extract MDS matrices via MDS codes over finite fields[3-6]. Considering the efficiency of implementation, the method requires the use of as many "1" and entries with as low Hamming weight as possible. The second way is to search MDS matrices in particular matrices, such as circulant matrices and Hadamard matrices[8] . The third technique is to use iteration[9-11]. For example, Photon[12] , which designed by LFSR(Linear Feedback Shift Register), is a representative.

Unlike the methods above, this paper presents a brand new traversal scheme. Using formalized MDS matrices, along with the period and minimal polynomial theory of the elements in the finite field, the construction of lightweight MDS matrices is realized. Then the distribution of these matrices is analyzed, and the mathematical proof of construction feasibility is also given. Besides, we find the important applications of the alternating group A_4, especially the Klein four-group in constructing MDS matrices with the fewest XORs.

Table 1 Symbol Description

Symbol	Description
$GL(m,S)$	set of all $m \times m$ non-degenerative matrices whose entries fall in S
I	identity matrices over $GL(4,F_2)$
$\#A$	XORs of matrix A
$\omega(a)$	Hamming weight of vector a, $a \in F_2^n$
L_i	formalized MDS matrix of i identity matrices
$\circ(A)$	period of matrix A over finite filed, that is $A^{15} = I$
$(v)_{(k)}$	k -expansions of vector v
$<a,<b,c>,d,e>$	positions of the non-zero entries in the matrix
$R(ab)$	perform a row permutation (ab) on a matrix
$C(ab)$	perform a column permutation (ab) on a matrix
$(ab) \circ i$	perform a permutation (ab) on i

Example 1 <4,2,<1,3>,3> is the representation of the following matrix: $\begin{pmatrix} 0&0&0&1 \\ 0&1&0&0 \\ 1&0&1&0 \\ 0&0&1&0 \end{pmatrix}$.

2 Preliminaries

Definition 1 ([7]　, XOR) For $A \in GL(m, F_2)$, $x \in F_2^n$. Then $\#A$ is the direct counting of XORs of $A \cdot x$, which represented as $\#A = \sum_{i=1}^{m}(\omega(A[i]-1))$, and $\omega(A[i])$ is the count of non-zero entries in the *i*-th row of matrix A.

Theorem 1 ([13]　, determinant conditions of a MDS matrix) Let $L=(L_{i,j})$, $1 \le i,j \le n$. The entries in L are all $m \times m$ matrices over F_2, then L can be represented as follows:

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix}. \qquad (1)$$

Then L is a MDS matrix if and only if every sub-matrix of order $t(1 \le t \le n)$ in L is full rank.

Definition 2 ([7]　) For MDS matrix as (1), its XORs is defined as $\#L = \sum_{i=1,j=1}^{n} \#L_{i,j}$.

Theorem 2([14]　) In a 4×4 MDS matrix over finite fields, the highest possible number of "1" is 9 and the lowest possible number of different entries is 3.

Based on the theorems above, this paper presents the concept of formalized MDS matrix.

Definition 3 A matrix *L* is called as a formalized MDS matrix if it satisfies the following two conditions:

1) some entries which make up *L* are known and their positions in *L* are determined;

2) *L* satisfies the determinant conditions of **Theorem 1**.

For **Example 2**, **3** and **4**, please see **Appendix I**.

Definition 4 Matrices A and B are equivalent if A can be obtained from B through a series of elementary transformations.

Definition 5 ([15]　) Let *G* be a group and let *S* be a set. Given a mapping $G \times S \to S$, denoted by $(x,s) \mapsto xs$. If for any $x, y \in G$, $s \in S$,

1) $x(ys) = (xy)s$,

2) $es = s$, *e* is the unit element of *G*.

Then we call *G* has an operation on *S*, also call *S* a *G*-set.

3 Construction of Formalized MDS Matrices

Let $L_i[I, A, B]$ denote a formalized MDS matrix in which *i* represents the number of elementary matrices, and $A, B \in GL(m, F_2)$ represent formal elements in the matrix. In this paper, the value of *i* limited to 7, 8, 9, thus the specific process of construction is shown in Figure 1.

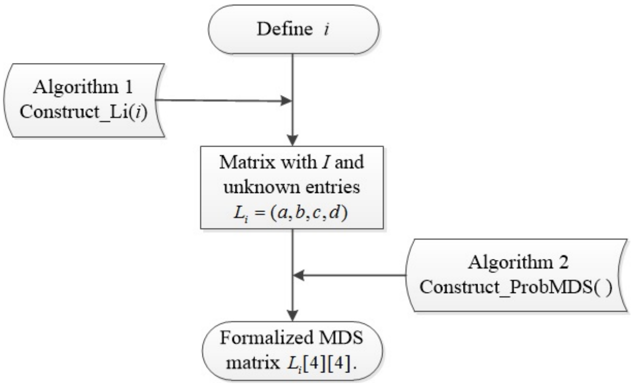

Figure 1 Construction Process of Formalized MDS Matrix

First, the number of identity matrices should be determined. **Algorithm 1**, Construct_Li (*i*) constructs a 4×4 matrix containing *i I*, and entries of other remaining positions are unknown. The matrix in this step satisfies any sub matrix of order 2 formed entirely by *I* would not appear. Next, **Algorithm 2** assigns the unknown positions of the matrix, and completes the construction.

Algorithm 1: Construct_Li(int i), to construct a 4×4 MDS matrix with *i I*
Input: number of identity matrices, *i* (*i*=7,8,9)
Output: a file with a decimal 4-dimensional vector $L_i=(a,b,c,d)$ //when (a,b,c,d) is converted to binary number, they represents the positions of *I* in the first row to the last row respectively

```
int $N$=$2^4-1$;
int A[4]; // an inter array which stores the results
fill $[0,N-1]$ into A[4] in dictionary order
for each A[4], $p,q\in[0,3], p\neq q$ do
    $(A[p])_{(2)}+(A[q])_{(2)}=(a',b',c',d')_{(3)}$
    If at least two numbers in $a',b',c',d'$ equal to 2, then
        return 4; // There is at least a matrix formed entirely by $I$
    else
        Save (A[0], A[1], A[2], A[3]) to text;//make it, save the result
    end if;
end for
end;
```

For example of **Algorithm 1**, **Example 5**, **Example 6** and **Example 7** , please see **Appendix II**.

Algorithm 2: Construct_ProbMDS(int $L_i[4]$), to construct a 4×4 formalized MDS matrix
Input: output of **Algorithm 1**, $L_i[4]=(a,b,c,d)$
Output: formalized MDS matrices $L_i[4][4]$ saved in file

```
1:  $L_i[4][4]\Leftarrow L_i[4]$;  //fill $I$ into the matrix
2: Find a position of an unknown entry and record the space's coordinates $w=(k,t), k,t=0,1,2,3$
3: if($w$==(3, 3)) then
4:     go to step 21;     // The space has been filled, save the result
5: else
6:     Fill_In( $L_i[4][4], w$);   // Fill the formalized entry $A$ in this space
7:     If there is a $2\times 2$ singular sub-matrix then
8:         $A\leftarrow B$;
9:     end if;
8:     Find an unknown entry's position $w'$ which is in the same row or column with $w$
9:     if $w'$==(3, 3) then
10:        $w'\Leftarrow w$;  // There is no entry in the same row or column with $w$, return to the last saved $w$
11:        if $w==w_0$ then       // when return to the starting position, still can not find a $w'$, replace the
                                   starting position and then re-search
12:            go to step 2;
13:        end if;
14:    else
15:        There is at least one vacancy in the same row or column with $w$, fill in the formalized entry $A$
16:        If there is a $2\times 2$ singular sub-matrix then
17:            $A\leftarrow B$;
18:        end if;
19:        go to step 8;
20:    end if;
21. Save ( $L_i[4][4]$ ) to text;    //Save the result to a file
22: end if;
23: end;
```

It should be noted that in a formalized MDS matrix, the positions of *A*, *B* are interchangeable.

Example 8 Assume the input

$$\begin{pmatrix} \mathrm{I} & \mathrm{I} & & \\ & \mathrm{I} & \mathrm{I} & \\ & & \mathrm{I} & \mathrm{I} \\ \mathrm{I} & & & \mathrm{I} \end{pmatrix},$$

then the construction process is shown in Figure 2 below:

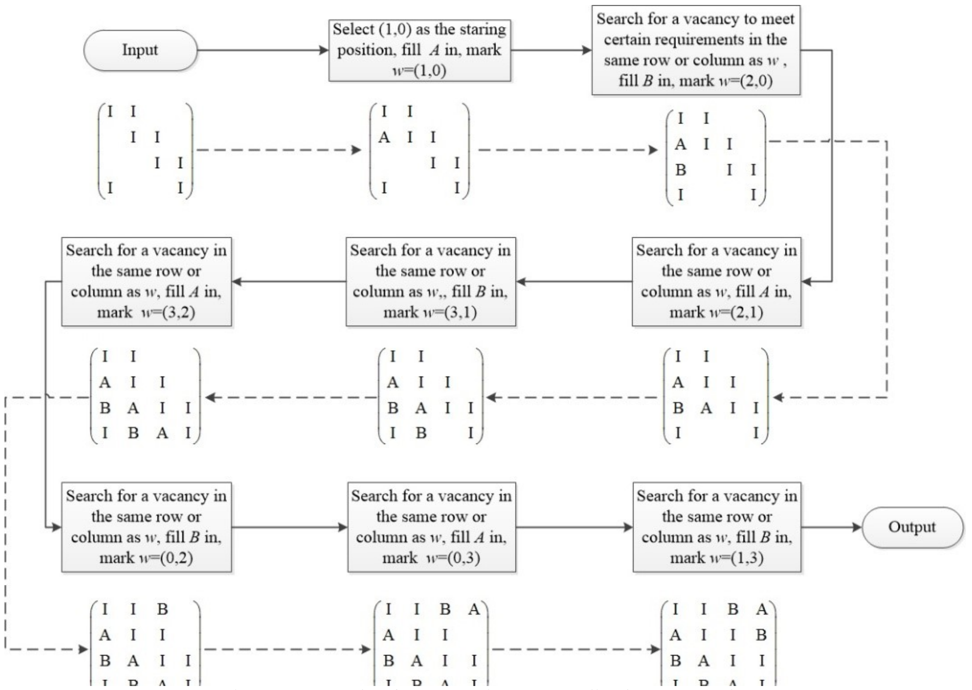
Input
Select (1,0) as the staring position, fill A in, mark w=(1,0)
Search for a vacancy to meet certain requirements in the same row or column as w , fill B in, mark w=(2,0)
Search for a vacancy in the same row or column as w, fill A in, mark w=(2,1)
Search for a vacancy in the same row or column as w,, fill B in, mark w=(3,1)
Search for a vacancy in the same row or column as w, fill A in, mark w=(3,2)
Search for a vacancy in the same row or column as w, fill B in, mark w=(0,2)
Search for a vacancy in the same row or column as w, fill A in, mark w=(0,3)
Search for a vacancy in the same row or column as w, fill B in, mark w=(1,3)
Output

Figure 2 Example of Constructing a Formalized MDS Matrix

The number of formalized MDS matrices constructed by this paper is summed up as Table 2.

Table 2 Categories of Formalized MDS Matrices

i	Formalized MDS matrices	Actual MDS matrices
9	384	192
8	1296	720
7	3456	576

4 Filtration of MDS Matrices

Not all the formalized MDS matrices in Table 2 are assigned to be MDS matrices, this is because elements over a finite field always have the minimal polynomial. For a particular form matrix, it can not be a MDS matrix when the determinant of its sub-matrices contain an annihilation polynomial of *A*. See Section 4.1 for details.

After obtaining a formalized MDS matrix, then the assignments of *A* and *B* are completed. Without loss of generality, when $i = 7,8,9$ respectively, three formalized MDS matrices $L_i[I, A, B]$ of the lightest XORs are chosen as the traversing objects. Let *A* traverse all the 2688 matrices whose period is 15. Let $B = A^d$, $B = A^d$, $d = 2,3,\ldots,14$. Then **Theorem 1** is used to filtrate the MDS matrices.

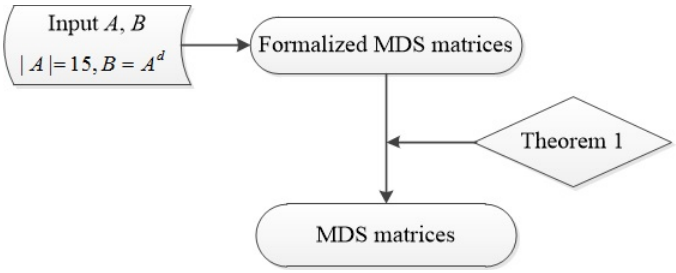

Figure 3 Filtration of MDS Matrices

4.1 Filtration of MDS matrices with 9 *I*

Might as well select the MDS matrix form in [7] :

$$L_9 = \begin{pmatrix} A\,I\,I\,I \\ I\,I\,B\,A \\ I\,A\,I\,B \\ I\,B\,A\,I \end{pmatrix},$$

where $A,B \in GL(m,F_2)$. When $m=4$, [7] has obtained 24 MDS matrices with the fewest XORs 13 for $m=4$, and 40320 MDS matrices with 10 XORs for $m=8$, where $B=A^{-2}$.

In fact, if L is an MDS matrix, then the period of these A is 15, that is $B=A^{-2}=A^{13}$. Using the traversal method proposed in this paper, the results is shown in Table 3:

Table 3 Filtration of MDS Matrices with 9 I

Relation between A、B	Number of MDS matrices
$B=A^2$	0
$B=A^3$	0
$B=A^4$	1344
$B=A^5$	2688
$B=A^6$	2688
$B=A^7$	0
$B=A^8$	0
$B=A^9$	1344
$B=A^{10}$	1344
$B=A^{11}$	2688
$B=A^{12}$	0
$B=A^{13}$	1344
$B=A^{14}$	0

When d=13, there is a MDS matrix with 13 XORs of 24 values, which is consistent with [7] .

Analysis

The annihilation polynomial of A is $x^{15}+1$, to factorize it over F_2,

$$x^{15}+1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

For 2688 A of period 15, the results show that these A can be divided into two groups of the same number, half of them take x^4+x^3+1 as minimal polynomial, and the other take x^4+x+1.

1. Apparently, in the premise of $|A|=15$, when d equals to 2, 8, 14 respectively, their corresponding sub-matrices $\begin{pmatrix} I & A \\ A & B \end{pmatrix}, \begin{pmatrix} B & A \\ I & B \end{pmatrix}, \begin{pmatrix} A & I \\ I & B \end{pmatrix}$ are singular.

2. When d equals to 3, 7, 12 respectively, the following 3×3 sub-matrices are singular for A:

$$\text{when } d=3, \quad \begin{pmatrix} A & I & I \\ I & A^3 & A \\ I & I & A^3 \end{pmatrix}, \begin{pmatrix} I & I & I \\ I & A^3 & A \\ A & I & A^3 \end{pmatrix};$$

$$\text{when } d=7, \quad \begin{pmatrix} A & I & I \\ I & I & A \\ I & A & A^7 \end{pmatrix}, \begin{pmatrix} I & I & I \\ I & A^7 & A \\ A & I & A^7 \end{pmatrix};$$

$$\text{when } d=12, \quad \begin{pmatrix} A & I & I \\ I & A^{12} & A \\ I & I & A^{12} \end{pmatrix}, \begin{pmatrix} I & A^{12} & A \\ A & I & A^{12} \\ A^{12} & A & I \end{pmatrix}.$$

For example, when $d=3$, the determinant of the singular sub-matrices are

$$\begin{vmatrix} A & I & I \\ I & A^3 & A \\ I & I & A^3 \end{vmatrix} = | A^7 + A^2 + A + I | = | A + I |^3 | A^4 + A^3 + I | \,(1),$$

$$\begin{vmatrix} I & I & I \\ I & A^3 & A \\ A & I & A^3 \end{vmatrix} = | A^6 + A^4 + A^3 + A^2 + A + I | = | A + I |^2 | A^4 + A + I | \quad (2);$$

In (1), polynomial $x^4 + x^3 + 1$ can annihilate 1344 A whose period is 15; in (2), polynomial $x^4 + x + 1$ can annihilate the remaining 1344 A. Thus when $d = 3$, for all the A of period 15, a matrix like L could not be a MDS matrix. The same reason goes for $d = 7,12$.

3. When d equals to 4, 9, 10, 13 respectively, these 3×3 sub-matrices below are singular:

$$\text{when } d=4, \begin{pmatrix} I & A^4 & A \\ A & I & A^4 \\ A^4 & A & I \end{pmatrix}; \text{when } d=9, \begin{pmatrix} I & I & I \\ I & A^9 & A \\ A & I & A^9 \end{pmatrix};$$

$$\text{when } d=10, \begin{pmatrix} A & I & I \\ I & A^{10} & A \\ I & I & A^{10} \end{pmatrix}; \text{when } d=13, \begin{pmatrix} I & I & I \\ I & A^{13} & A \\ A & I & A^{13} \end{pmatrix}.$$

Take as $d=4$ an example, the determinant of the singular 3×3 sub-matrices are $| A^{12} + A^5 + A^3 + I | = |A + I|^2 | A^4 + A + I || A^6 + A^4 + A^3 + A + I |$, it contains polynomial $x^4 + x + 1$ which can annihilate 1344 A. Therefore when $d = 4$, there is only 1344 MDS matrices. Same goes for $d = 9,10,13$.

Further, let B be a linear combination of some power of A. It is the form $B = A^{d_1} + A^{d_2}$ that only need to be considered, where $d_1 \neq d_2, 1 \leq d_1, d_2 \leq 14$. When $m = 4$, let A traverse all the 2688 matrices whose period is 15. We also get 24 MDS matrices with 13 XORs, they are exactly the same as these MDS matrices obtained when $B = A^{-2}$, and when

$$B = A + A^{12}, B = A^2 + A^{14}, B = A^3 + A^8,$$
$$B = A^4 + A^{11}, B = A^5 + A^7, B = A^9 + A^{10},$$

we get them.

4.2 Filtration of MDS matrices with 8, 7 *I*

When $i = 8,7$, consider the following two matrices:

$$L_8 = Circ(I, I, A, B) = \begin{pmatrix} I\,I\,A\,B \\ B\,I\,I\,A \\ A\,B\,I\,I \\ I\,A\,B\,I \end{pmatrix}, \quad L_7 = \begin{pmatrix} A\,I\,A\,B \\ I\,A\,B\,I \\ A\,B\,I\,I \\ B\,I\,I\,A \end{pmatrix},$$

when $\#A = 1, \#B = 2$, $B = A^{13}$, they each have 24 MDS matrix with fewest XORs, and their values of (A, B) are exactly the same. For details of the traversal, please refer to **Appendix III**.

4.3 Feasibility Proof

From the above analysis it can be seen that as long as the determinant of the sub-matrices of a formalized MDS matrix does not contain the minimal polynomial of A, then the matrix must be an MDS matrix. And the number of these matrices is closely related to d.

Theorem 3 $A, B \in GL(m, F_2)$, $\circ(A) = 15$, $B = A^{d_1} + A^{d_2} + \cdots + A^{d_k}$, $d_1, d_2, \ldots, d_k$ are pairwise different, $k = 1,2,\ldots,14$, $d_1, d_2, \ldots, d_k = 1,2,\ldots,14$. Using the construction method in chapter 4, MDS can be obtained, and the number of them is related to the values of $d_1, d_2, \ldots, d_k$. For each group $(d_1, d_2, \ldots, d_k)$, their number can only be classified into three different cases:

1) for all A, all the matrices are MDS matrices;

2) for all A, half of the matrices are MDS matrices;

3) for all A, none of the matrices are MDS matrices.

Proof It's known that there are 2688 matrices *A* of period 15 over F_2, and their minimal polynomials are $f_1 = x^4 + x + 1$ and $f_2 = x^4 + x^3 + 1$, which can annihilate distinct 1344 matrices *A* respectively. For matrices *L* with only three entries, I, A, A^d, its determinants of each sub-matrices are a polynomial about *A*, denote $f(A)$. We uniquely factorize $f(x)$ over F_2 and get $f = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, where $p_1, p_2, \cdots, p_k$ are irreducible polynomials and $t_1, t_2, \cdots, t_k \in N$. Then either there exists m to make $p_m = f_1$ or $p_m = f_2$, or for all m there exists no $p_m = f_1$ or $p_m = f_2$, where $m = t_1, t_2, \cdots, t_k$. When f has f_1 and f_2 as its factors, all *L* are not MDS matrices; when f has only f_1 or f_2 as its factor, half of *L* are MDS matrices; when f has neither f_1 nor f_2 as its factor, all *L* are MDS matrices. #

4.4 Numeration

For the following three formalized MDS matrices over $GL(4, F_2)$ discussed in this chapter:

$$L_9 = \begin{pmatrix} A\,I\,I\,I \\ I\,I\,B\,A \\ I\,A\,I\,B \\ I\,B\,A\,I \end{pmatrix},\ L_8 = \begin{pmatrix} I\,I\,A\,B \\ B\,I\,I\,A \\ A\,B\,I\,I \\ I\,A\,B\,I \end{pmatrix},\ L_7 = \begin{pmatrix} A\,I\,A\,B \\ I\,A\,B\,I \\ A\,B\,I\,I \\ B\,I\,I\,A \end{pmatrix},$$

the results are summarized in Table 4 below:

Table 4 Construction results of MDS matrices L_9, L_8, L_7

i	Least XORs	Number of the lightest MDS matrices	Total number of MDS matrices in this form
9	13	24	$2688 \times 3 + 1344 \times 4 = 13440$
8	12	24	$2688 \times 5 + 1344 \times 4 = 18816$
7	13	24	$1344 \times 5 = 6720$

Note: Table 4 shows the traversal results of some particular formalized MDS matrices, and it is feasible to apply the above method to other formalized MDS matrices. Thus it can be seen that a large number of MDS matrices can be obtained through this paper's method. Next, we carry out a further research and analysis for the lightest MDS matrices.

5 Algebraic Structure of the Lightest MDS matrices

This chapter discusses the relation between L_9, L_8, L_7 and also their algebraic structures when they reach the fewest XORs. Because in these matrices, $B = A^{13}$, we only need to consider *A*.

5.1 Internal Algebraic Relations

When $i = 7, 8$, *A* in $L_i[I, A, B]$ are exactly the same, and these *A* can be numbered in 4 rows and 6 columns as the following Table 5:

Table 5 when $i = 7, 8$, groups of *A* in the lightest MDS matrix

Generic system	A_1	A_2	A_3	A_4
Row1	1. <<1,4>,3,1,2>	7. <4,<2,3>,1,2>	13. <3,4,<2,3>,1>	19. <3,4,2,<1,4>>
Row2	2. <<1,2>,4,1,3>	8. <3,<1,2>,4,2>	14. <3,1,<3,4>,2>	20. <2,4,1,<3,4>>
Row3	3. <<1,2>,3,4,1>	9. <4,<1,2>,2,3>	15. <2,3,<3,4>,1>	21. <4,1,2,<3,4>>
Row4	4. <<1,3>,4,2,1>	10. <3,<2,4>,2,1>	16. <4,3,<1,3>,2>	22. <4,3,1,<2,4>>
Row5	5. <<1,3>,1,4,2>	11. <2,<2,4>,1,3>	17. <2,4,<1,3>,3>	23. <3,1,4,<2,4>>
Row6	6. <<1,4>,1,2,3>	12. <2,<2,3>,4,1>	18. <4,1,<2,3>,3>	24. <2,3,4,<1,4>>

Using *R*( ) to represent the row permutation of a matrix, *C*( ) to represent the column permutation of a matrix. Considering the columns in Table 5, the algebraic relation in A_1, A_2, A_3, A_4 can be obtained, as it shown in Figure 4.

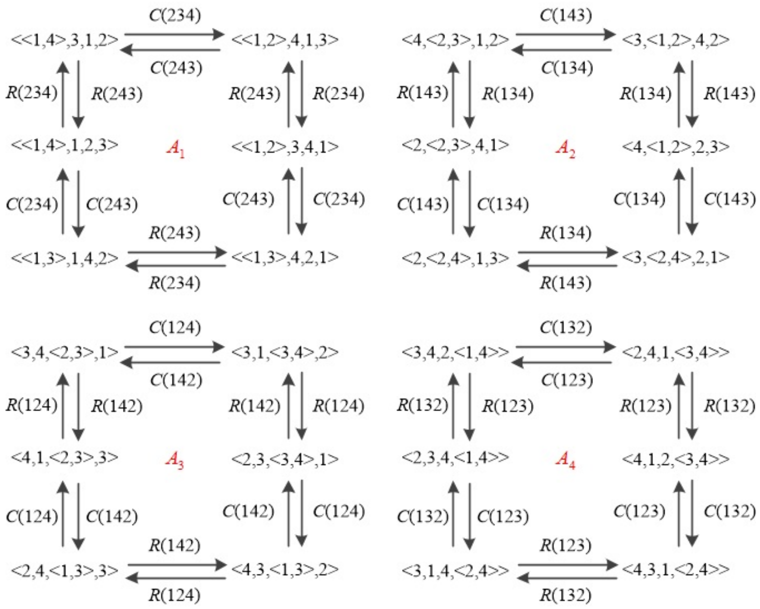

Figure 4 when $i=7,8$, generation relations of *A* in the MDS matrix with the least XORs

From Figure 4, we can derive some criteria for constructing an MDS matrix of the fewest XORs.

1. Each $A_i(i=1,2,3,4)$ has a group permutation as it shown above, and the principle of choosing a group permutation is to ensure that after transformation, the period of *A* is still 15, as well as its minimal polynomial would not change.

2. From any position, row permutation and column permutation appear alternately.

3. Select a matrix from each A_1, A_2, A_3, A_4, such as

{<<1,4>,3,1,2>,<4,<2,3>,1,2>,<3,4,<2,3>,1>,<3,4,2,<1,4>>},

it is a generic system of these 24 *A* and it can generate all *A* by using the permutation {(123), (124), (132), (134), (142), (143), (234), (243)}, which is a subset of A_4.

4.For each row of Table 5, it is a generic system of *A*. Then for the compound operation of *R* and *C*, $R\circ C \triangleq *$ (*R*, *C* are interchangeable), Klein four-group has an operation on this generic system.

Example 9 Select the first row in Table 5, let

$$M=\{m_1=<<1,4>,3,1,2>, m_2=<4,<2,3>,1,2>, m_3=<3,4,<2,3>,1>, m_4=<3,4,2,<1,4>>\}.$$

Then according to **Definition 5**, there exists a mapping $k_4 \times M \to M$, denoted by

$$((1),m_i) \mapsto (1)*m_i = m_i,$$

$$((12)(34),m_i) \mapsto (12)(34)*m_i = m_{(12)(34)\circ i},$$

$$((13)(24),m_i) \mapsto (13)(24)*m_i = m_{(13)(24)\circ i},$$

$$((14)(23),m_i) \mapsto (14)(23)*m_i = m_{(14)(23)\circ i}.$$

So that k_4 has an operation on *M* and *M* is a k_4-set, where $i=1,2,3,4$. $(\ )(\ )\circ i$ represents a permutation of the footnote, for example, $(12)(34)\circ 1=2$, $(12)(34)\circ 3=4$.

When $i=9$, the same algebraic relation is also found in these *A* of the lightest MDS matrices. In summary, the following propositions are true for the lightest 4×4 MDS matrices $L_i[I,A,B]$, $i=7,8,9$.

Proposition 1 There are 24 *A* in total which make a certain form of $L_i[I,A,B]$ reach the fewest XORs, denote them $A_1, A_2, \ldots, A_{24}$. Using row and column permutations of a matrix, along with permutations in A_4,

$$A_4:\{(1),\ (123),\ (124),\ (132),\ (134),\ (142),\ (143),\ (234),\ (243),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

then from any $A_j(j=1,2,\ldots,24)$, it can generate all 24 *A*.

Proposition 2 For each row which is a generic system denote as *M*, it is a k_4-set, that is the Klein four-group has an operation on *M*, of which the operation multiplication is the compound operation of *R* and *C*.

5.2 Algebraic Relation between Each Other

In fact, to replace the A in the first row first column with I in L_7, the new matrix with 8 I is the equivalent form of the circulant matrix L_8, see Figure 5. Therefore, these A which make L_7 reach the fewest XORs also make L_8 reach it.

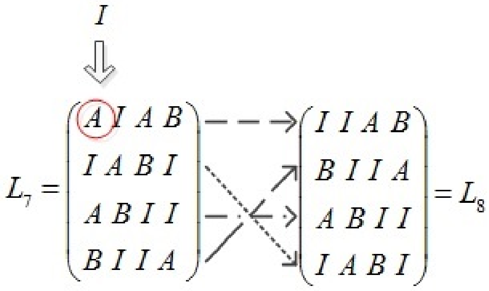
I
$L_7 = \begin{pmatrix} A\ I\ A\ B \\ I\ A\ B\ I \\ A\ B\ I\ I \\ B\ I\ I\ A \end{pmatrix}$
$\begin{pmatrix} I\ I\ A\ B \\ B\ I\ I\ A \\ A\ B\ I\ I \\ I\ A\ B\ I \end{pmatrix} = L_8$

Figure 5 construct L_8 from L_7

When $i=9$, assume A' are entries which make L_9 reach the fewest XORs in section 4.1, then there are also 24 A'. Considering row permutation and column permutation respectively, and there is a Klein four-group mapping between these A' and A. Table 6 shows the permutation of rows.

Table 6 Algebraic relation in the generic system between A' and A

A in 7I/8I	A' in 9I	Row permutation: $A \to A'$
<<1,4>,3,1,2>	<3,<1,4>,2,1>	(12)(34)
<4,<2,3>,1,2>	<<2,3>,4,2,1>	
<3,4,<2,3>,1>	<4,3,1,<2,3>>	
<3,4,2,<1,4>>	<4,3,<1,4>,2>	
<<1,3>,4,2,1>	<4,<1,3>,1,2>	
<3,<2,4>,2,1>	<<2,4>,3,1,2>	
<4,3,<1,3>,2>	<3,4,2,<1,3>>	
<4,3,1,<2,4>>	<3,4,<2,4>,1>	
<<1,2>,4,1,3>	<3,1,4,<1,2>>	(14)(23)
<3,<1,2>,4,2>	<2,4,<1,2>,3>	
<3,1,<3,4>,2>	<2,<3,4>,1,3>	
<2,4,1,<3,4>>	<<3,4>,1,4,2>	
<<1,3>,1,4,2>	<2,4,1,<1,3>>	
<2,<2,4>,1,3>	<3,1,<2,4>,2>	
<2,4,<1,3>,3>	<3,<1,3>,4,2>	
<3,1,4,<2,4>>	<<2,4>,4,1,3>	
<<1,2>,3,4,1>	<4,1,<1,2>,3>	(13)(24)
<4,<1,2>,2,3>	<2,3,4,<1,2>>	
<2,3,<3,4>,1>	<<3,4>,1,2,3>	
<4,1,2,<3,4>>	<2,<3,4>,4,1>	
<<1,4>,1,2,3>	<2,3,<1,4>,1>	
<2,<2,3>,4,1>	<4,1,2,<2,3>>	
<4,1,<2,3>,3>	<<2,3>,3,4,1>	
<2,3,4,<1,4>>	<4,<1,4>,2,3>	

For example, in L_7 let A=<<1,3>,1,4,2>. After performing once row permutation (14)(23) on A, we get its corresponding A' in L_9, <2,4,1,<1,3>>. Furthermore, the group permutation of <<1,3>,1,4,2> is (234), and after applying permutation (14)(23) on it, the group permutation of <2,4,1,<1,3>> can be obtained, that is $(234)\circ(14)(23)=(124)$. While applying column permutation (14)(23) on <<1,3>,1,4,2>, matrix <<2,4>,4,1,3> can be obtained.

It is verified that for the other 191 kinds of formalized MDS matrices with 9 I, it is always these 24 A' in Table 6 that make them reach the fewest XORs. To some extent, they are equivalent matrices.

Proposition 3 Using the Klein four-group, we can derive A' in a group of $L_j[I,A,B]$ from another A in $L_i[I,A,B]$, $i,j=7,8,9$, $i \neq j$, and the permutation relation is fixed, independent of the matrix form.

5.3 Numeration of the Lightest MDS Matrices

For other formalized MDS matrices constructed in this paper, the numeration of them is shown in Figure 6.

Figure 6 Numeration of the Lightest MDS Matrices

i	Categories of MDS matrices	Number of (A,B) in a lightest MDS matrix	Total number of the lightest MDS matrices
9	192	24	$192\times 24=4608$
8	720	24	$720\times 24=17280$
7	576	24	$576\times 24=13824$

6 Conclusions

This paper studies the construction of 4×4 lightweight MDS matrices over F_2. Firstly, the concept and construction algorithm of formalized MDS matrix are given. Secondly, a large number of MDS matrices are obtained by using matrices of period 15 and their power matrices. Then the number distribution of these MDS matrices is analyzed, and the feasibility of the construction is proved mathematically. Finally, the important application of the permutation group, especially the Klein four-group, in the construction of the lightest MDS matrix is revealed.

In this paper, the proposed method is general, and it can be further extended by flexible transformation of the parameters in the algorithms. Such as adding more entries, taking four or more different entries to construct matrices, etc. Otherwise, the algebraic relationship of the basic entries is changeable, for example, take $AB=I$. In addition, using the Klein four-group, we can get another lightest MDS matrix from a known lightest MDS, which greatly reduces the search space.

For more general cases, considering formalized MDS matrix $L_i[I,A,B]$ over $GL(m,F_2)$, this paper presents the following conjectures.

Conjecture 1 If A and B are entries that make $L_i[I,A,B]$ reach the fewest XORs, then there are $m!$ pairs (A, B) making this matrix reach the fewest XORs.

Conjecture 2 When i is a constant, regardless of the form of the matrix $L_i[I,A,B]$, the A which make it reaches the fewest XORs are fixed.

Conjecture 3 When $m=4$, under some certain conditions, permutations in Klein four-group can preserve the property of the lightest MDS matrix. That is, form a known lightest MDS matrix, another lightest MDS matrix can be obtained.

References

[1] Mac Williams F, Sloane N. The Theory of Error Correcting Codes[M]. North-Holland Publishing Company, 1978.

[2] Vaudenay, S. On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER[C]. In: 2nd International Workshop on Fast Software Encryption. Springer-Verlag, 1994: 286-297 .

[3] Daemen J, Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard[C]. Springer, 2002.

[4] Daemen J, Knudsen R, Rijmen V. The Block Cipher SQUARE[C]. In: Biham E (ed.) —FSE 1997. Springer Berlin Heidelberg, 1997(1267): 149–165.

[5] Lu X, Howard M. Hardware Design and Analysis of Block Cipher Components[C]. ICISC 2002. Springer Seoul, 2002(2587): 1-19. Springer, Seoul(2002)

[6] Augot D, Finiasz M. Direct construction of recursive MDS diffusion layers using shortened BCH codes[C]. In: Cid C, Rechberger C(eds.) — FSE 2014. 2015(8540): 3-17,

[7] Li Y Q. Wang, M S. On the Construction of Lightweight Circulant Involutory MDS Matrices[EB/OL]. FSE 2016. DOI=http://eprint.iacr.org/ 2016/406.

[8] Gupta K, Ray I G. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications[J]. Cryptogr. Commun. 2015 (7): 257-287.

[9] Guo J, Peyrin T, Poschmann A, Robshaw M. The LED Block Cipher[C]. In: Preneel B, Takagi T (eds.) —CHES 2011. Springer Heidelberg, 2011(6917): 326–341.

[10] Sajadieh M, Dakhilalian M, Mala H, Sepehrdad P. Recursive Diffusion Layers for Block Ciphers and Hash Functions[C]. In: Canteaut A (ed.) —FSE 2012. Springer Heidelberg, 2012(7549): 385–401.

[11] Wu S B, Wang M S, Wu W L. Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions[C]. In: Knudsen R and H Wu (Eds.) —SAC 2012, 2013(7707): 355-371.

[12] Guo J, Peyrin T, Poschmann A. The PHOTON Family of Lightweight Hash Functions[C]. In: Rogaway P (ed.) —CRYPTO 2011. Springer Heidelberg, 2011(6841): 222–239.

[13] Blaum M and Roth R M. On Lowest Density MDS Codes[J]. IEEE Transactions on Information Theory, 1999, 45(1): 46-59.

[14] Junod P, Vaudenay S. Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices[J]. In: Handschuh H, Hasan M A (eds.) — SAC 2004. Springer Heidelberg, 2004 (3357): 84-99.

[15] Lang S. Algebra[M]. New York: Springer-Verlag, 2003.

Appendix

Appendix I

Example 2 Given a matrix

$$A=\begin{pmatrix} I & X_1\, X_2\, I \\ I & I\ \ I\ X_1 \\ X_2\, I & I\ \ I \\ X_1\, I & I\ X_2 \end{pmatrix},$$

where *I* is a identity matrix, X_1, X_2 represent some unknown entries. Then *A* satisfies condition 1) in **Definition 3**. However, there is a 2×2 sub-matrix $\begin{pmatrix} I & I \\ I & I \end{pmatrix}$ in *A*, which does not meet the determinant conditions in **Theorem 1**, thus *A* is not a formalized MDS matrix.

Example 3 Given a matrix

$$B=\begin{pmatrix} X_1 & I & I & I \\ I & I & X_2 & X_1 \\ I & X_2 & I & X_1 \\ I & X_2 & X_1 & I \end{pmatrix},$$

then *B* satisfies condition 1) in **Definition 3.** But there is a 2×2 sub-matrix $\begin{pmatrix} I & X_1 \\ I & X_1 \end{pmatrix}$ in *B*, which does not meet the determinant conditions in **Theorem 1,** thus *B* is not a formalized MDS matrix.

Example 4 Given a matrix

$$L=\begin{pmatrix} X_1 & I & I & I \\ I & I & X_2 & X_1 \\ I & X_1 & I & X_2 \\ I & X_2 & X_1 & I \end{pmatrix},$$

then *L* satisfies the condition 1) and 2) in **Definition 3** simultaneously, so *L* is the formalized MDS matrix, denote it $L_9[I, X_1, X_2]$, which indicates that *L* is composed of *I* and X_1, X_2, and the number of *I* is 9.

Appendix II

Example 5 Suppose the output $L_9(7,9,19,12)$, then the formalized MDS matrix constructed by our method is (*X* for unknown entries)

$$L_i=\begin{pmatrix} X\ I\ I\ I \\ I\ \ I\ X\,X \\ I\ X\,I\ X \\ I\,X\,X\ I \end{pmatrix}.$$

Note that the elementary row transformation of the matrix does not change the full rank of its second order sub-matrices, so the stored 4-dimensional array is disordered and it is easy to know that if a singular matrix appears in this step, it must be a matrix composed entirely of *I*.

Examples 6 and **7** give an example of the **Algorithm 1** to determine whether there is a second order sub-matrix consisting entirely of identity matrices.

Example 6 Suppose there is an intermediate result in the construction process, $A[4]=(9,14,7,10)^T$, convert it into a binary number and get the matrix

$$A[4]=\begin{pmatrix} 1\,0\,0\,1 \\ 1\,1\,1\,0 \\ 0\,1\,1\,1 \\ 0\,1\,1\,0 \end{pmatrix},$$

$A[1]+A[2]=(1,2,2,1)_{(3)}$, there are two 2 appearing, indicating that there is a 2-order sub-matrix consisting entirely of *I*, which is not feasible.

Example 7 Suppose the output of **Algorithm 1** is $(3,4,5,6)$, convert it into a binary number and get the matrix

$$\begin{pmatrix} 0\,0\,1\,1 \\ 0\,1\,0\,0 \\ 0\,1\,0\,1 \\ 0\,1\,1\,0 \end{pmatrix},$$

there is no two or more sum that equal to 2 after adding corresponding elements in any two rows. So we make it and the MDS matrix we obtained is

$$L_7 = \begin{pmatrix} X\,X\,I\;\,I \\ X\,I\,X\,X \\ X\,I\,X\,I \\ X\,I\,I\,X \end{pmatrix}.$$

Appendix III

When $i=8$, details for traversal is shown in Table 7,

Table 7 Filtration of MDS Matrices with 8 *I*

Relation between A、B	Number of MDS matrices
$B=A^2$	0
$B=A^3$	1344
$B=A^4$	2688
$B=A^5$	2688
$B=A^6$	2688
$B=A^7$	2688
$B=A^8$	0
$B=A^9$	1344
$B=A^{10}$	1344
$B=A^{11}$	0
$B=A^{12}$	1344
$B=A^{13}$	2688
$B=A^{14}$	0

When $B=A^{13}$, the lightest MDS matrices has 12 XORs, $\#A=1,\#B=2$, and there are 24 of them.

When $i=7$, details for traversal is shown in Table 8,

Table 8 Filtration of MDS Matrices with 7 *I*

Relation between A、B	Number of MDS matrices
$B=A^2$	0
$B=A^3$	1344
$B=A^4$	0
$B=A^5$	0
$B=A^6$	1344
$B=A^7$	1344
$B=A^8$	0
$B=A^9$	1344
$B=A^{10}$	0
$B=A^{11}$	0
$B=A^{12}$	0
$B=A^{13}$	1344
$B=A^{14}$	0

When $B=A^{13}$, the lightest MDS matrices has 13 XORs, $\#A=1,\#B=2$, and there are 24 of them.