On the Construction of the Lightest 4×4 Circulant MDS Matrices

Shiyi Zhang[a], Yongjuan Wang[b], Yang Gao[a,b], and Tao Wang[a,b]

[a]xxxx; e-mail: syzhang1352@163.com.cn.
[b]xxxx; e-mail: pinkywyj@163.com.cn.

December 8, 2016

Abstract

4×4 MDS matrices with few XORs have a wide range of applications in plenty of mainstream lightweight ciphers. For 4×4 circulant MDS matrices over $GL(4, \mathbb{F}_2)$, they have at least 12 XOR operations. In this paper, by traversing their structure characteristics, we firstly investigate the utterly construction and the numeration of the lightest circulant MDS matrices. Then the overall structure and the diagrams of these matrices are given. Finally we find the characteristics of permutation group in the lightest circulant MDS matrices above: they possess characteristics of symmetric group S_4, and for a kind of particular MDS matrices, they can even form a Klein four-group in some ways.

Keywords : MDS matrix, circulant matrix, XOR operation, permutation group, lightweight cipher.

1 Introduction

In block ciphers, MDS matrices are widely used in designing linear diffusion layers, such as AES [1]. Constructing MDS matrices with XORs as few as possible helps decrease the implementation cost and promote the development of lightweight cipher. Due to the fixed form, it is one of the most common methods to search MDS matrices by traversing particular matrices, such as circulant matrices and Hadamard matrices. Unfortunately, it is also the fixed form that limits the lower bound of XORs which these particular matrices can reach. For example, 4×4 circulant MDS matrices over $GL(4, \mathbb{F}_2)$ have at least 12 XOR operations [2], and it is also the least XORs we had known before [3] came out. Recently, [3]searched all the 4×4 lightweight matrices over $GL(4, \mathbb{F}_2)$ with XORs less than 12 and got matrices with 10 XORs. In the process of investigating 4×4 circulant MDS matrices over $GL(4, \mathbb{F}_2)$ with 12 XORs, we find the characteristics of permutation group they have, meanwhile, the utterly construction and the numeration of these matrices are given. These conclusions may provide some theoretical references for future construction.

2 Preliminaries

2.1 Symbol and Description

Table 1: Symbol and Description

Symbol	Description
$GL(m, S)$	set of all $m \times m$ non-degenerative matrices whose entries fall in S
I^0	matrices coming from elementary transformation of identity matrices, whose XOR is zero
$\#A$	XORs of matrix A
$\sim$	matrices equivalent
$< a, < b, c >, d, e >$	positions of the non-zero entries in a matrix

Example 1. $< 4, 2, < 1, 3 >, 3 >$ is the representation of the following matrix

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

2.2 Definitions and Notations

Definition 1. For $A \in GL(4, \mathbb{F}_2), x \in \mathbb{F}_2$. Then $\#A$ is the direct counting of XORs of $A \cdot x$, which represented as $\#A = \sum_{i=1}^{m}(\omega(A[i] - 1))$. $\omega(A[i])$ is the count of non-zero entries in the i-th row of matrix A.

Definition 2. A 4×4 circulant matrix is shaped like

$$Circ(A, B, C, D) = \begin{pmatrix} A & B & C & D \\ D & A & B & C \\ C & D & A & B \\ B & C & D & A \end{pmatrix}$$

where $A, B, C, D \in GL(m, \mathbb{F}_2)$, and (A, B, C, D) is called as its representation row.

Theorem 1. Let $L = (L_{i,j}), 1 \leq i, j \leq n$, The entries in L are all $m \times m$ matrices over $\mathbb{F}_2$, then L can be represented as follows:

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix} \tag{1}$$

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

Definition 3. For MDS matrix shaped like (1), its XORs is defined as

$$\#L = \sum_{i=1,j=1}^{n} \#L_{i,j}.$$

Theorem 2. Let $A_i \in GL(4, \mathbb{F}_2)$,$A = \sum_{i=1}^{4} \#A_i$. If $Circ(A_1, A_2, A_3, A_4)$ is a circulant MDS matrix, then $A \geq 3$.

Lemma 1. There are 48 pairs of (A, B) such that $Circ(I, I, A, B)$ are MDS matrices with $\#A + \#B = 3$. These 48 matrices are of the type $Circ(I, I, A, A^{-2})$ and $Circ(I, I, A^{-2}, A)$ for 24 different A.

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

Theorem 3. Let a block matrix $T = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, if A is reversible and $AC = CA$, then $|T| = |AD - CB|$.

3 Construction of Circulant MDS Matrices

3.1 Construct the lightest Circulant MDS Matrices

For a circulant matrix $Circ(A, B, C, D)$, when doing row circulant transformations, we have $Circ(A, B, C, D) \sim Circ(B, C, D, A) \sim Circ(C, D, A, B) \sim Circ(D, A, B, C)$, thus this paper only discusses one form. Obviously, the number of 4×4 matrices with 0 XOR over $\mathbb{F}_2$ is 24. Moreover, the inverse of these matrices are themselves.

According to **Theorem 2**, the minimum XORs of circulant matrix is 12. To make a $Circ(A, B, C, D)$ reach it, there must be $\#A + \#B + \#C + \#D = 3$. All possible cases are listed below:

Case 1. There are three matrices with 0 XOR among A, B, C, D, and the remaining one is with 3 XORs.

Case 2. There are two matrices with 0 XOR among A, B, C, D, and for the remaining two matrices, one has 1 bit XOR and the other has 2 XORs.

Case 3. There is only one matrix with 0 XOR among A, B, C, D, and the remaining three have 1.

First we present a proposition found during our research.

Proposition 1. If a matrix $Circ(A, B, C, D)$ is a MDS matrix, then both $Circ(B, A, D, C)$ and $Circ(A, D, C, B)$ are also MDS matrices.

Proof. It's easy to see that all the sub-matrices of order 2 of $Circ(B, A, D, C)$ or $Circ(A, D, C, B)$ are equivalent to $Circ(A, B, C, D)$'s. They are

$$\begin{pmatrix} A & B \\ B & C \end{pmatrix}, \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \begin{pmatrix} A & B \\ D & A \end{pmatrix}, \begin{pmatrix} A & C \\ C & A \end{pmatrix},$$

$$\begin{pmatrix} A & C \\ D & B \end{pmatrix}, \begin{pmatrix} A & D \\ D & C \end{pmatrix}, \begin{pmatrix} B & C \\ C & D \end{pmatrix}, \begin{pmatrix} B & D \\ D & B \end{pmatrix}$$

or their transposition matrices.#

For **Case 1**, there exists no MDS matrix.

Proof. Assume these matrices have form as $Circ(I_1, I_2, I_3, A)$ where $\#I_1 = \#I_2 = \#I_3 = 0$, $\#A = 3$. And a sub-matrix whose order is 2 can always be found, such as $\begin{pmatrix} I_1 & I_3 \\ I_3 & I_1 \end{pmatrix}$, and its determinant $\begin{vmatrix} I_1 & I_3 \\ I_3 & I_1 \end{vmatrix} = |I_1 + I_3||I_1 - I_3|$, we could just consider whether the determinant $|I_1 + I_3|$ equals to zero.

1) If there exists some row where locations of entry 1 in I_1, I_3 are the same, then this very row's entries are all 0. We have $|I_1 + I_3| = 0$.

2) If in I_1, I_3, the locations of entry 1 are different in arbitrary rows, we also have $|I_1+I_3| = 0$. Under this assumption, I_1+I_3 constitutes 4 row vectors whose weight are 2. And on the other hand, the Maximal Linearly Independent group in four-dimensional linear space whose Hamming weight is 2 has at most 3 linearly independent vectors. Then the 4 row vectors formed by $I_1 + I_3$ are linearly dependent. In summary, sub-matrix $\begin{pmatrix} I_1 & I_3 \\ I_3 & I_1 \end{pmatrix}$ of order 2 is singular, through this method we can not get a MDS matrix. #

For **Case 2**, let these matrices might be $Circ(I_1, I_2, A, B)$ where $\#I_1 = \#I_2 = 0$, $\#A + \#B = 3$.

1) When $I_1 = I_2$, by traversing all the matrices over $\mathbb{F}_2$ that satisfy $\#I_1 = \#I_2 = 0, \#A = 1, \#B = 2$ or $\#A = 2, \#B = 1$, finally we get 1152 MDS matrices shaped like $Circ(I_1, I_1, A, B)$ with 12 XORs.

2) When $I_1 \neq I_2$, using the same strategy above, we get 1152 MDS matrices as well.

Note that if $Circ(I_1, I_2, A, B)$ is a MDS matrix, then $Circ(I_2, I_1, B, A)$is also a MDS matrix.

For **Case 3**, suppose this kind of matrix as $Circ(I_1, A, B, C)$, where $\#I_1 = 0, \#A = \#B = \#C = 1$, we get 1152 MDS matrices with 12 XORs in total. Note : if $Circ(I_1, A, B, C)$ is a MDS matrix, then according to **Propsition 1**, $Circ(I_1, C, B, A)$ is also a MDS matrix.

3.2 Structure of MDS Matrices like $Circ(I_1^0, I_2^0, A, B)$

For matrices of the form $Circ(I_1, I_2, A, B)$, where $\#I_1 = \#I_2 = 0$, $\#A + \#B = 3$, we find that there are each 1152 MDS matrices with 12 XORs no matter I_1 equals to I_2 or not.

Known from **Lemma 1**, $I_1 = I_2 = I$ is a particular case of this condition. The number of MDS matrices like $Circ(I, I, A, B)$ are totally 48. On the other hand, the number of 4×4 matrices with 0 XOR over $\mathbb{F}_2$ is 24. Using elementary transformations, when $I_1 = I_2$, we get $24 \times 48 = 1152$ matrices shaped like $Circ(I_1, I_1, A, B)$. Meanwhile, if we have already known the forms of these 48 matrices $Circ(I, I, A, B)$, we

can easily get the others', and these matrices like $Circ(I_1, I_1, A, B)$ are determined by the transformations from I to I_1.

For example, assume we have known the form of $Circ(I, I, A, B)$, and we need to learn the form of $Circ(I_i, I_i, A_i, B_i), i = 1, 2, \ldots, 23$, where $I_i = IT_i$, and T_i is the linearly transformation matrix from I to I_i, thus we have $A_i = AT_i, B_i = BT_i$.

Example 2. For $I =< 1, 2, 3, 4 >$, if we have MDS matrix

$$Circ(I, I, < 2, 3, 4, < 1, 4 >>, << 2, 3 >, < 3, 4 >, 1, 2 >),$$

then for $I_1 =< 4, 3, 2, 1 >$ and $I_2 =< 3, 1, 4, 2 >$, these matrices below are also MDS matrices:

1) $Circ(I_1, I_1, << 1, 4 >, 4, 3, 2 >, < 2, 1, < 3, 4 >, < 2, 3 >>)$,

2) $Circ(I_2, I_2, < 4, 2, < 1, 4 >, 3 >, < 1, < 2, 3 >, 2, < 3, 4 >>)$.

Proposition 2. Taken 48 lightest circulant MDS matrices $Circ(I, I, A, B)$ as a whole, let it be a generator g. Then, using the structure features of symmetric group S_4 and g we can get all the 1152 lightest circulant MDS matrices like $Circ(I_1, I_1, A, B)$.

When $I_1 \neq I_2$, let $I_1 = (R_1, R_2, R_3, R_4)^T$ where R_1, R_2, R_3, R_4 are four-dimensional row vectors with 1 Hamming weight over $\mathbb{F}_2$. It is presented that in the MDS matrices with 12 XORs we construct, the form of I_2 must be one of the three as follows:

$$(R_3, R_4, R_1, R_2)^T, (R_2, R_1, R_4, R_3)^T, (R_4, R_3, R_2, R_1)^T.$$

Meanwhile, if given I_1, I_2, then for $\#A = 1, \#B = 2$ and $\#A = 2, \#B = 1$, there are 8 MDS matrices $Circ(I_1, I_2, A, B)$ and $Circ(I_2, I_1, B, A)$ for each case. Thus, for different I_1, when $I_1 \neq I_2$, $24 \times [(8 + 8) \times 3] = 1152$ MDS matrices like $Circ(I_1, I_2, A, B)$ can be constructed.

Example 3. When $I_1 \neq I_2$, all the 4×4 MDS matrices with 12 XORs over $\mathbb{F}_2$ like $Circ(I_1, I_2, A, B)$ are listed as follows:

Table 2: MDS matrices like $Circ(I_1, I_2, A, B)$

I_1	I_2	A	B
$<4,3,2,1>$	$<3,4,1,2>$	$<<1,3>,4,3,2>$	$<<1,3>,2,3,<2,4>>$
		$<1,4,<1,3>,2>$	$<1,<2,4>,<1,3>,4>$
		$<3,<1,4>,4,2>$	$<2,<1,4>,4,<2,3>>$
		$<3,1,<1,4>,2>$	$<<2,3>,1,<1,4>,3>$
		$<<2,3>,4,1,3>$	$<<2,3>,1,<1,4>,3>$
		$<2,4,1,<2,3>>$	$<2,<1,4>,4,<2,3>>$
		$<3,<2,4>,1,4>$	$<2,<1,4>,4,<2,3>>$
		$<3,2,1,<2,4>>$	$<<1,3>,2,3,<2,4>>$
	$<2,1,4,3>$	$<<2,3>,1,4,2>$	$<<2,3>,<1,4>,1,2>$
		$<2,<1,4>,1,3>$	$<<2,3>,<1,4>,1,2>$
		$<<1,2>,2,4,3>$	$<<1,2>,2,3,<3,4>>$
		$<1,<1,2>,4,3>$	$<1,<1,2>,<3,4>,4>$
		$<2,4,<1,4>,3>$	$<3,4,<1,4>,<2,3>>$
		$<3,1,4,<2,3>>$	$<3,4,<1,4>,<2,3>>$
		$<2,1,<3,4>,4>$	$<1,<1,2>,<3,4>,4>$
		$<2,1,3,<3,4>>$	$<<1,2>,2,3,<3,4>>$
	$<1,2,3,4>$	$<1,<2,4>,3,2>$	$<<1,3>,<2,4>,1,2>$
		$<1,2,<3,4>,3>$	$<<1,2>,1,<3,4>,3>$
		$<<1,3>,2,1,4>$	$<<1,3>,<2,4>,1,2>$
		$<<1,2>,1,3,4>$	$<<1,2>,1,<3,4>,3>$
		$<2,<1,2>,3,4>$	$<2,<1,2>,4,<3,4>>$
		$<3,2,<1,3>,4>$	$<3,4,<1,3>,<2,4>>$
		$<1,4,3,<2,4>>$	$<3,4,<1,3>,<2,4>>$
		$<1,2,4,<3,4>>$	$<2,<1,2>,4,<3,4>>$

In fact, there are only $C_2^1 \cdot C_2^1 = 4$ results after we perform twice row swaps on I_1. Then we have three distinct I_2 that are different from I_1, let them be $I_{21}^0, I_{22}^0, I_{23}^0$ respectively. It can be seen that the values of I_2 contain all even permutations of I_1, and they constitute a Klein four-group.

Theorem 4. Given a 4×4 circulant MDS matrix over $GL(4, \mathbb{F}_2)$ with 12 XORs, and it shaped like $Circ(I_1, I_2, A, B)$, where $\#I_1 = \#I_2 = 0$, $\#A + \#B = 3$. Then I_2 is an even permutation of I_1. Moreover, I_2 constitute a Klein four-group $k_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ with regard to permutations of I_1.

Using sector area to denote the number of MDS matrices, the distribution of circulant MDS matrices shaped like $Circ(I_1, I_2, A, B)$ is shown as Figure 1:

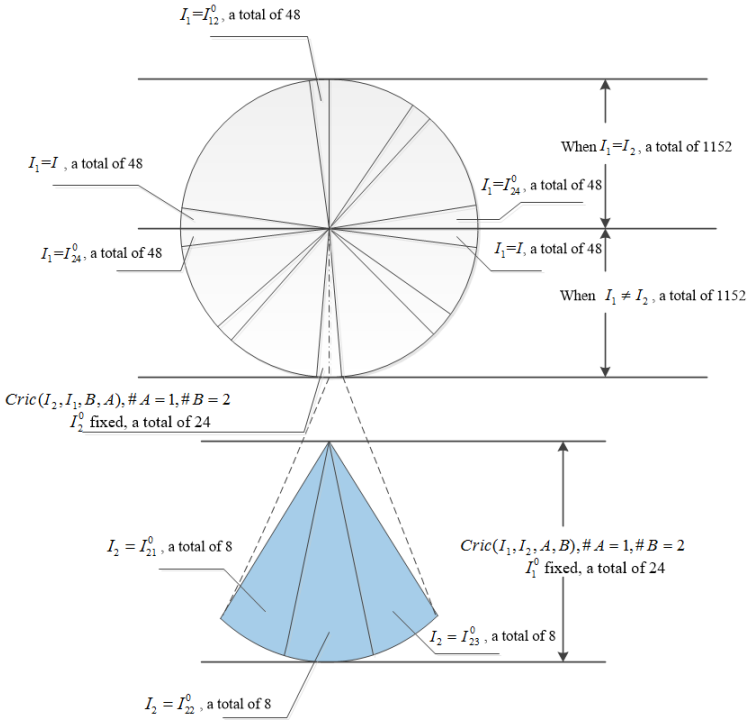

Figure 1: Structure of MDS matrices like $Circ(I_1, I_2, A, B)$

3.3 Structure of MDS Matrices like $Circ(I^0, A, B, C)$

When $I^0 = I$, we get 48 MDS matrices. Consider all the 4×4 matrices with 0 XOR over $GL(4, \mathbb{F}_2)$, $24 \times 48 = 1152$ MDS matrices with 12 XORs shaped like $Circ(I^0, A, B, C)$ can be constructed, where $\#A = \#B = \#C = 1$.

Since the positions of A, C are interchangeable, let a pair of A, C in a fixed sequence, each I^0 corresponds to 24 different MDS matrices. Moreover, these MDS matrices can be divided into 3 groups. Among the same group, each A and C has 2 values, assume they are A_1, A_2 and C_1, C_2, thus we get 4 combinations of (A, C). And each pair of (A, C) corresponds to 2 values of B, also we can get $24 \times [3 \times C_2^1 \times C_2^1 \times 2] \times 2 = 1152$ MDS matrices shaped like $Circ(I^0, A, B, C)$.

Example 4. Let $I^0 =< 4, 3, 2, 1 >$, then all the 4×4 MDS matrices shaped like $Circ(I^0, A, B, C)$ over $GL(4, \mathbb{F}_2)$ are listed below:

Table 3: MDS matrices like $Circ(I^0, A, B, C)$

I^0	A	C	B
$<4,3,2,1>$	$<<3,4>,4,2,1>$	$<4,3,<1,2>,2>$	$<<1,2>,2,4,3>$
			$<2,1,<3,4>,4>$
		$<4,3,1,<1,2>>$	$<<1,2>,1,3,4>$
			$<1,2,4,<3,4>>$
	$<3,<3,4>,2,1>$	$<4,3,<1,2>,2>$	$<1,2,<3,4>,3>$
			$<2,<1,2>,3,4>$
		$<4,3,1,<1,2>>$	$<1,<1,2>,4,3>$
			$<2,1,3,<3,4>>$
	$<4,<2,3>,3,1>$	$<<1,4>,3,2,4>$	$<3,<1,4>,4,2>$
			$<<2,3>,4,1,3>$
		$<1,3,2,<1,4>>$	$<2,<1,4>,1,3>$
			$<3,1,4,<2,3>>$
	$<4,2,<2,3>,1>$	$<<1,4>,3,2,4>$	$<<2,3>,1,4,2>$
			$<2,4,<1,4>,3>$
		$<1,3,2,<1,4>>$	$<3,1,<1,4>,2>$
			$<2,4,1,<2,3>>$
	$<<2,4>,3,4,1>$	$<4,<1,3>,2,3>$	$<<1,3>,4,3,2>$
			$<3,<2,4>,1,4>$
		$<4,1,2,<1,3>>$	$<<1,3>,2,1,4>$
			$<1,4,3,<2,4>>$
	$<2,3,<2,4>,1>$	$<4,<1,3>,2,3>$	$<1,<2,4>,3,2>$
			$<3,2,<1,3>,4>>$
		$<4,1,2,<1,3>>$	$<1,4,<1,3>,2>$
			$<3,2,1,<2,4>>$

When $I^0 =< 4,3,2,1 >$, these MDS matrices above in Table 3 can be divided into 3 groups according to different values of (A, C). Their relationship is shown as Figure 2.

It can be seen that in any group of (A, C) according to the same I^0, the vector of weight 2 lies in different rows in A_1, A_2, C_1, C_2. By performing once row swap and a XOR operation on some row of weight 1 and the row of weight 2 in X_1, we can determine the form of X_2, where $X \in \{A, C\}$, and the remaining two row vectors of weight 1 stay. Furthermore, every (A, C) in one group is disjoint, and the 6 swaps according to the same I^0 determined by 3 groups of (A, C) are disjoint, too.

Proposition 3. These swaps above constitute the set $\{(12), (13), (14), (23), (24), (34)\}$, and they are all the swaps of length 1 in symmetric group S_4.

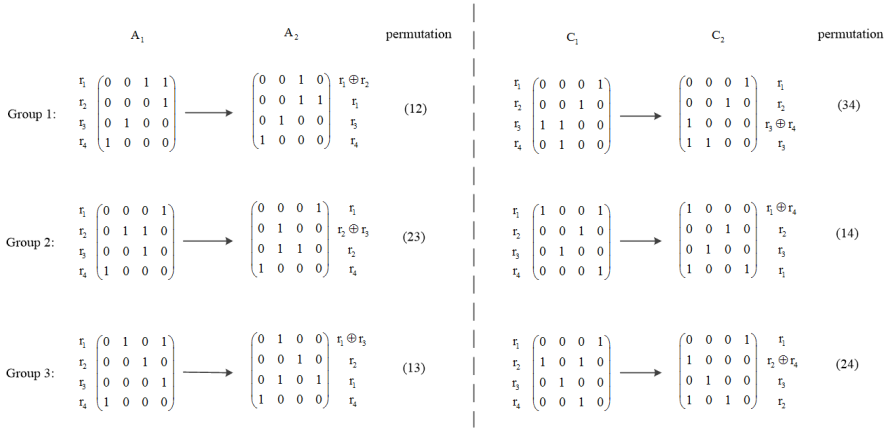

Figure 2: Permutation characteristics of MDS matrices like $Circ(I^0, A, B, C)$

For other MDS matrices like $Circ(I^0, A, B, C)$ according to different I^0, there is also a similar permutation group characteristic.

Using cubic volume to represents the number of MDS matrices, X axis and Y axis respectively represent the values of A and C, thus plane XOY represents the combination of (A, C). The number distribution of MDS matrices like $Circ(I^0, A, B, C)$ is shown as Figure 3.

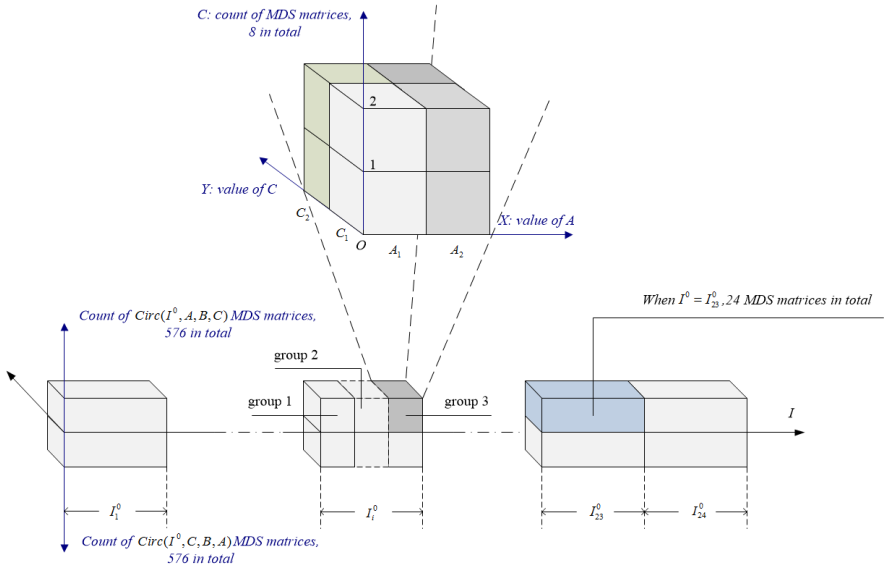

Figure 3: Numeration distribution of MDS matrices like $Circ(I^0, A, B, C)$

There are 1152 MDS matrices in total, of which type $Circ(I^0, A, B, C)$ and $Circ(I^0, C, B, A)$ are of 576 respectively. They are completely symmetrical. Take MDS matrices shaped

like $Circ(I^0, A, B, C)$ as an example, these matrices can be divided into 24 categories according to different I^0, and there are 24 MDS matrices in every category determined by $I_i^0 (i = 1, 2, \ldots, 24)$. Three groups constitute a category. For example, category I_i^0 is composed of group1, group2 and group3 as it shown in Figure 3. (A, C) has totally four combinations $(A_1, C_1), (A_1, C_2), (A_2, C_1), (A_2, C_2)$, and every $(A_j, C_j), j = 1, 2$, corresponds to 2 MDS matrices. Thus, there are 8 MDS matrices in one group.

3.4 Numeration of Circulant MDS Matrices

Let $I_1 = (R_1, R_2, R_3, R_4)^T$, to sum up, the numeration of 4×4 circulant MDS matrices with 12 XORs over $GL(4, \mathbb{F}_2)$ is listed as follows:

Table 4: Numeration of circulant MDS matrices

representation row	relationship between representation entries		matrices numeration	
$[I_1^0, I_2^0, A, B], \#A + \#B = 3$	$I_1 = I_2$		1152	
	$I_1 \neq I_2$	$I_2 = (R_2, R_1, R_4, R_3)^T$	1152	384
		$I_2 = (R_3, R_4, R_1, R_2)^T$		384
		$I_2 = (R_4, R_3, R_2, R_1)^T$		384
$[I^0, A, B, C], \#A = \#B = \#C = 1$	-		1152	

4 Conclusion

In this paper we investigate the construction, numeration and structure of the lightest 4×4 circulant MDS matrices over $GL(4, \mathbb{F}_2)$. By traversing their structure characteristics, the utterly construction and the numeration distribution of this kind of MDS matrices are given. Then from the angle of algebra, we research the interdependence of the entries in these circulant MDS matrices and go in-depth study of the permutation group characteristics within them. We find that these lightest MDS matrices possess characteristics of symmetric group S_4 and its subgroup, Klein four-group . Our work provides a new idea for further construction. For example, using the similar strategies, to construct MDS matrices through other particular matrices, such as Hadamard matrices or entries over $GL(m, F_2)$ for different m(usually $m = 8$) is feasible.

Acknowledgement The authors would like to thank xxx for many insightful comments.

References

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

[2] Li, Y,. Wang, M. : On the Construction of Lightweight Circulant Involutory MDS Matrices. *FSE 2016. IACR Cryptology ePrint Archive (http://eprint.iacr.org/)* 2016: 406 (2016)

[3] Jian Bai, Dingkang Wang. The Lightest 4×4 MDS Matrices over $GL(4, \mathbb{F}_2)$. *http://eprint.iacr.org/* 2016/686