Construction of Lightweight MDS Matrices over the Matrix Polynomial Residue Ring

Lijing Zhou, Licheng Wang, and Yiru Sun

Beijing University of Posts Telecommunications,Bei Jing, China

Abstract. In this article, we investigate the construction of lightweight MDS matrices over the matrix polynomial residue ring. According to distributions of the minimum polynomial, distributions of XOR count and equivalence classes of MDS matrices, we propose an algorithm, which not only can construct lightest MDS matrices, but also is evidently more efficient than previous methods. Moreover, we investigate existences of involutory MDS matrices over the matrix polynomial residue ring. According to quadratic congruence, over the matrix polynomial residue ring, we propose a simplified necessary-and-sufficient condition for deciding whether a Hadamard matrix is invorlutory. With this method, we propose another efficient and special algorithm to construct lightweight Hadamard involutory MDS matrices. Over the 8×8 matrix polynomial residue ring, we construct vast 4×4 Hadamard involutory MDS matrices with 20 XORs, which are much lighter than previous results. In addition, we obtain a series of propositions about the parity of XOR count.

Keywords: MDS matrix, XOR count, matrix polynomial residue ring, lightweight, involutory

1 Introduction

In block cipher, the non-linear confusion layer and the linear diffusion layer are two significant components required for the security of the cipher. The linear diffusion layer with bigger branch number can more effectively resist differential and linear cryptanalysis. The diffusion layer is often constructed by a matrix. For any $n \times n$ matrix, the maximum branch number is $n+1$. Maximum distance separable (MDS) matrix has the maximum branch number. MDS matrices are broadly used in many ciphers like PHOTON [1], SQUARE [2], LED [3], AES [4]. For lightweight cryptography, the cost of implementing a linear diffusion layer will influence the efficiency of cryptography largely. Therefore constructing lightweight MDS matrices is a meaningful work. Recently, the improving and designing hardware efficiency become a significant research trend. Some lightweight block ciphers [3, 5–7] and lightweight hash functions [1, 8, 9] are proposed to reduce the implementation cost. An efficient lightweight MDS matrix is extremely useful for improving the hardware efficiency. The sum of XORs [15] is the most important index for measuring the efficiency of MDS matrices, and a MDS matrix constructed with fewer sum of XORs can perform more efficiently.

Currently, a major method to construct lightweight MDS matrices is using recursive matrices. The main way is that firstly choosing a special non-singular matrix, and then composing it k times to get an MDS matrix A^k, so-called serial matrices. This method was first proposed in hash function PHOTON [1]. Such matrices later used in block cipher LED [3] and authenticated encryption scheme PRIMATEs [10], and were further investigated in [11–15]. However, this method is not suitable for low-latency implementations since it has to run several rounds to get results. Another main researching point is constructing involutory (self-inverse) lightweight MDS matrices. Nakahara et al.[16] prove that circulant MDS matrices of order 4 can not be involutory over finite field. Chand Gupta et al.[17] further prove that circulant MDS can not be involutory over finite field. Sim et al.[18] constructs lightweight Hadamard involutory MDS matrices and Hadamard-Cauchy MDS matrices over finite field. Li et al.[19] further investigated constructions of involutory MDS matrices, and they constructs lightest MDS matrices over $GL(m, \mathbb{F}_2)$, which are the optimal results at present.

In brief, all previous methods for building lightweight MDS matrices can be classified into two categories: One is to select entry matrices from $GF(2^m)$, i.e. finite filed, while another is to select entry matrices from $GL(m, \mathbb{F}_2)$, i.e. the set of all non-singular matrices. However, lightest MDS matrices can not be constructed over $GF(2^8)$ when m=8. There are two major reasons. First, $GF(2^8)$ is too small. This lead to losing a lot of MDS matrices. Second, if we want to construct lightest MDS matrices, non-singular matrices with 1 XOR count must be used to be entries of MDS matrix. But there does not exist non-singular matrix with 1 XOR operation in $GF(2^8)$. Therefore, $GF(2^8)$ is not suite for constructing lightest MDS matrices. Although $GL(m, \mathbb{F}_2)$ overcomes this limitations, the searching space is too huge and exhaustible. Therefore, designing an efficient algorithm, which can construct the lightest MDS matrices, is a meaningful work.

For improving the efficiency of constructing lightweight MDS matrices, there are two major ways: (a) reduce the search space. Researchers usually use Hadamard matrix, circulant matrix and Optimal matrix[28] to be the structures of MDS matrices. The reason is that the elements of these structures are repeatedly used, so search space can be reduced obviously. As well researchers can let some elements with 0 XORs and others with as few XORs as possible. For example, $n \times n$ identity matrix over $\mathbb{F}_2$ has 0 XOR count. In this way, the search space is reduced again, and at the same time the upper bound of the sum of XORs is greatly restricted. Choosing elements from a small set is another direct way to reduce the search space. Recently, [22, 18] use the equivalence of matrices to reduce the search space. (b) Simplify the computation of construction. Many papers construct MDS matrices over finite field [18, 24, 20, 21, 23]. By investigating the multiplication of special element in $GF(2^m)$, Christof Beierle et al.[24]get lightweight circulant MDS matrices over $GF(2^m)$. In [23], authors propose that choosing special elements from finite field constructed by some special irreducible polynomial can improve the multiplication efficiency. [18] proposes that choosing irreducible polynomial has a significant impact on the lightweightness. Although

the finite field is suitable to construct MDS matrices, it is not suitable to construct lightest-weight MDS matrices. We will intensively discuss and solve this problem in present paper.

Our Contributions In present paper, we construct lightweight MDS matrices over the matrix polynomial residue ring. To our best knowledge, it is the first time to construct MDS matrices over the matrix polynomial residue ring. Our results can be summaries as follows.

- First, over the matrix polynomial residue ring, we range over all $T \in GL(m, \mathbb{F}_2)$ that satisfies $\#T$=1 and $T + I$ is non-singular. For each of such T, we find its minimum polynomial. Then we find all elements in $\mathbb{F}_2[T]$, which have less than 4 XORs. We also analyze the distribution of the minimum polynomial and the distribution of XOR count.
- Second, we we find that, for those 4×4 MDS matrices containing at least 8 identity matrices, there exist only 5 kinds of structures.
- Third, an efficient algorithm for constructing lightest MDS matrices over the matrix polynomial residue ring are given. We obtain some good results as follows
  (1) For 4×4 MDS matrices over the 4×4 matrix polynomial residue ring. We use 1 minute 42 seconds to construct 288 MDS matrices with 10 XORs.
  (2) For 4×4 MDS matrices over the 8×8 matrix polynomial residue ring. We use 1 minute 16 seconds to construct 40320 Optimal MDS matrices with 10 XORs. We use about 14 hours to construct 1128960 MDS matrices with 10 XORs.
  (3) For 4×4 MDS matrices over the 16×16 matrix polynomial residue ring. We construct MDS matrices with 10 XORs.
- Fourth, we prove some theories about existences of involutory MDS matrices as follows
  (1) Over the matrix polynomial residue ring, $n \times n (n \geq 3)$ circulant MDS matrices can not be involutory.
  (2) Over $GL(m, \mathbb{F}_2)$, $n \times n (n \geq 2)$ special MDS matrices as mentioned in Section 7 can not be involutory.
  Besides, we prove a simplified necessary-and-sufficient condition for judging whether Hadamard matrix is involutory. With this condition, we design another efficient algorithm for constructing lightweight Hadamard involutory MDS matrices. Over 8×8 matrix over $\mathbb{F}_2$, we construct vast 4×4 Hadamard involutory MDS matrices with 20 XORs, which are much lighter than known results.
- Finally, we get a series of properties about the parity of XOR count. These properties might have independent interests.

Outline of This Paper The present paper is organized as follows. In Sect.2, we give basic definitions and theorems about MDS matrix and XOR count. In Sect.3, we investigate the distribution of the minimum polynomial and the distribution of XOR count on the matrix polynomial residue ring. In Sect.4, we

investigate the equivalence classes of lightweight MDS matrices over the matrix polynomial residue ring. When MDS matrices have at least 8 identity matrices being entries, MDS matrices only have 5 equivalence classes. In Sect.5, we design a general algorithm for constructing lightweight MDS matrices. In Sect.6, we use the general algorithm to construct lightest non-involutory MDS matrices. In Sect.7, we investigate existences of involutory MDS matrices and the quadratic congruence of the minimum polynomials. Besides, we investigate the Hadamard involutory MDS matrices and design an efficient and special algorithm to construct vast lighter Hadamard involutory MDS matrices. In Sect.8, we propose and prove a series of propositions about the parity of XOR count. A short conclusion is given in Sect.9.

2 Preliminaries

In this section, we introduce the basic definitions and theorems about lightweight MDS matrices.

2.1 MDS Matrices

$GL(n, S)$ denotes the set of all non-singular $n \times n$ matrices with entries in set S. The bundle weight of x is defined as the number of nonzero entries of x and is expressed by $\omega_b(x)$. For $M \in GL(n, S)$, the branch number of M is the minimum number of nonzero components in the input vector v and output vector $u = M \cdot v$ as we range over all nonzero $v \in S^n$. I.e., the branch number of $n \times n$ matrix M is $B_M = min_{v \neq 0}\{\omega_b(v) + \omega_b(Mv)\}$,and $B_M \leq n + 1$. A maximum distance separable (MDS) $n \times n$ matrix is a matrix that has the optimal branch number n+1.

Eevry linear diffusion layer is a linear map and can be represented by a matrix as follows

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

where $L_{i,j}$ $(1 \leq i, j \leq n)$ is an $m \times m$ non-singular matrix over $\mathbb{F}_2$, and denote $M(n, m)$ be the set of all matrices, which are $n \times n$ matrices with entries in $GL(m, \mathbb{F}_2)$. For $X = (x_1, x_2, ..., x_n)^T \in (F_2^m)^n$,

$$L(X) = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} L_{1,i}(x_i) \\ \sum_{i=1}^{n} L_{2,i}(x_i) \\ \vdots \\ \sum_{i=1}^{n} L_{n,i}(x_i) \end{pmatrix},$$

where $L_{i,j}(x_k) = L_{i,j} \cdot x_k$, for $1 \leq i, j \leq n, 1 \leq k \leq n$.

Theorem 1 *Let $L \in M(n, m)$, then L is MDS if and only if all square submatrices of L are of full rank.*

2.2 XOR Count

Let $a, b \in \mathbb{F}_2$, $a + b$ is called a bit XOR operation. Let $A \in GL(m, \mathbb{F}_2)$, $x = (x_1, x_2, ..., x_m)^T \in F_2^m$, $\#A$ denotes the number of XOR operations required to evaluate Ax directly. Let $\omega(A)$ is the number of 1 in A. Therefore $\#A = \omega(A) - m$, and $\#A$ is also called by XOR count of A. For $L \in M(n, m)$, we denote $\#(L) = \sum_{i,j=1}^{n} \#(L_{ij})$. For instance, let $x = (a, b, c, d)^T \in F_2^4$, and the following matrix with 4 XOR count.

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

$$Ax = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} d \\ c + d \\ b + c + d \\ a + c \end{pmatrix}.$$

For $A \in GL(m, \mathbb{F}_2)$, a simplified representation of A is given by extracting the non-zero positions in each of row of A. For example, [3,2,4,[1,3]] is the representation of the following matrix with 1 XOR count.

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

3 Matrix Polynomial Residue Ring

In this section, we investigate the distribution of the minimum polynomial and the distribution of XOR count on the matrix polynomial residue ring.

Let T be an $n \times n$ matrix over F_2, and $f(x)$ be the minimum polynomial of T. Let the order of $f(x)$ be k, then $k \leq n$. $\mathbb{F}_2[T] \cong \mathbb{F}_2[x]/(f(x))$ since T satisfies $f(T) = 0$, where $\mathbb{F}_2[T]$ denotes the matrix polynomial residue ring generated by T. Therefore matrix computations is equivalent to polynomial computations in $\mathbb{F}_2[T]$.

For example, let $B, C \in \mathbb{F}_2[T]$,

$$\begin{aligned} B &= b_{k-1}T^{k-1} + \cdots + b_1 T + b_0 I, \\ C &= c_{k-1}T^{k-1} + \cdots + c_1 T + c_0 I, \\ b(x) &= b_{k-1}x^{k-1} + \cdots + b_1 x + b_0, \\ c(x) &= c_{k-1}x^{k-1} + \cdots + c_1 x + c_0. \end{aligned}$$

Then $B + C = b(x) + c(x)|_{x=T}$, $BC = b(x)c(x)|_{x=T}$.

3.1 Analyzing the 4×4 Matrix Polynomial Residue Ring

In this subsection, we analyze the distribution of the minimum polynomial and the distribution of XOR count on the 4×4 matrix polynomial residue ring.

We range over all matrix T, which satisfies $T \in GL(4, \mathbb{F}_2)$, $\#T$=1 and $I+T$ is non-singular. The number of T is 72. Let $f(x)$ be the minimum polynomial of T, $b(x) \in \mathbb{F}_2[x]/(f(x))$. We search every T to find every $f(x)$ and all $b(x)$, where $b(x)$ satisfies $1 \leq \#b(T) \leq 3$.

Theorem 2 *Let $T \in GL(4, \mathbb{F}_2)$, $\#T$=1, $T+I$ is non-singular and $f(x)$ is the minimum polynomial of T, $b(x) \in \mathbb{F}_2[x]/(f(x))$. Then*
(1) $f(x)$ must be one of the following polynomials

$$x^4+x+1, x^4+x^2+1, x^4+x^3+1.$$

(2) if $\#b(T)$=1, $b(x)$ must be one of the following polynomials

$$x, x^3+1, x^3+x, x^3+x^2.$$

(3) if $\#b(T)$=2, $b(x)$ must be one of the following polynomials

$$x^2, x^2+1, x^2+x, x^3.$$

(4) if $\#b(T)$=3, $b(x)$ must be one of the following polynomials

$$x+1, x^2, x^3, x^3+x^2+1.$$

The distributions of $f(x)$ and $b(x)$ are as follows

Table 1: Distributions of Polynomials about 4×4 Matrix

Minimum Polynomial		
	$f(x)$	Number
MP_4	x^4+x+1	24
	x^4+x^2+1	24
	x^4+x^3+1	24

2 XORs		
	$b(x)$	Number
$X2_4$	x^2	48
	x^2+1	24
	x^2+x	24
	x^3	24

1 XOR		
	$b(x)$	Number
$X1_4$	x	72
	x^3+1	24
	x^3+x	24
	x^3+x^2	24

3 XORs		
	$b(x)$	Number
$X3_4$	$x+1$	24
	x^2	24
	x^3	24
	x^3+x^2+1	24

For any fixed T, which satisfies $T \in GL(4, \mathbb{F}_2)$, $\#T$=1 and $I + T$ is non-singular. In $\mathbb{F}_2[T]$, every element has less than and equal to 9 XORs. At most 5 elements, which are not identity matrix or 0 matrix over $\mathbb{F}_2$, with 1, 2 or 3 XORs. At most 2 elements have 1 XOR count. At most 3 elements have 2 XORs. At most 2 elements have 3 XORs.

3.2 Analyzing the 8×8 Matrix Polynomial Residue Ring

In this subsection, we analyze the distributions of minimum polynomial and XOR count in the 8×8 matrix polynomial residue ring.

We range over all matrix T, which satisfy $T \in GL(8, \mathbb{F}_2)$, $\#T$=1 and $I+T$ is non-singular. The number of T is 241920. Let $f(x)$ be the minimum polynomial of T, $b(x) \in \mathbb{F}_2[x]/(f(x))$. We range over every T to find every $f(x)$ and all $b(x)$, where $b(x)$ satisfies $1 \leq \#b(T) \leq 3$.

Theorem 3 *Let $T \in GL(8, \mathbb{F}_2)$, $\#T$=1, $T + I$ is non-singular and $f(x)$ is the minimum polynomial of T,$b(x) \in \mathbb{F}_2[x]/(f(x))$. Then*
(1) $f(x)$ must be one of the following polynomials

$$x^8 + x + 1, x^8 + x^2 + 1, x^8 + x^3 + 1, x^8 + x^4 + 1, x^8 + x^5 + 1, x^8 + x^6 + 1.$$

(2) for $\#b(T)$=1, $b(x)$ must be one of the following polynomials

$$x, x^7 + 1, x^7 + x, x^7 + x^2, x^7 + x^3, x^7 + x^4, x^7 + x^5.$$

(3) for $\#b(T)$=2, $b(x)$ must be one of the following polynomials

$$x^2, x^6 + 1, x^6 + x, x^6 + x^2, x^6 + x^3, x^6 + x^4.$$

(4) for $\#b(T)$=3, $b(x)$ must be one of the following polynomials

$$x^3, x^5 + 1, x^5 + x, x^5 + x^2, x^5 + x^3, x^7 + x^6 + 1$$

The distributions of $f(x)$ and $b(x)$ are as follows

For any fixed T, which satisfies $T \in GL(8, \mathbb{F}_2)$, $\#T$=1 and $I + T$ is non-singular. In $\mathbb{F}_2[T]$, every element has less than and equal to 44 XORs. At most 4 elements, which are not identity matrix or 0 matrix over $\mathbb{F}_2$, with 1 or 2 XORs. At most 6 elements, which are not identity matrix or 0 matrix over $\mathbb{F}_2$, with 1, 2 or 3 XORs. At most 2 elements have 1 XOR count. At most 2 elements have 2 XORs. At most 2 elements have 3 XORs.

Theorem 4 *Let $T \in GL(m, \mathbb{F}_2)$, $\#T$=1, $T + I$ is non-singular. Then $T^{-1} \in \mathbb{F}_2[T]$.*

Proof. Because $T \in GL(m, \mathbb{F}_2)$, $\#T$=1, $T + I$ is non-singular.

For m=4. The minimum polynomial of T must one of the following polynomials

$$x^4 + x + 1, x^4 + x^2 + 1, x^4 + x^3 + 1.$$

Table 2: Distributions of Polynomials about 8×8 Matrix

Minimum Polynomial		
	$f(x)$	Number
MP_8	x^8+x+1	40320
	x^8+x^2+1	40320
	x^8+x^3+1	40320
	x^8+x^4+1	40320
	x^8+x^5+1	40320
	x^8+x^6+1	40320

2 XORs		
	$b(x)$	Number
$X2_8$	x^2	241920
	x^6+1	40320
	x^6+x	40320
	x^6+x^2	40320
	x^6+x^3	40320
	x^6+x^4	40320

1 XOR		
	$b(x)$	Number
$X1_8$	x	241920
	x^7+1	40320
	x^7+x	40320
	x^7+x^2	40320
	x^7+x^3	40320
	x^7+x^4	40320
	x^7+x^5	40320

3 XORs		
	b(x)	Number
$X3_8$	x^3	201600
	x^5+1	40320
	x^5+x	40320
	x^5+x^2	40320
	x^5+x^3	40320
	x^7+x^6+1	40320

For m=8. The minimum polynomial of T must one of the following polynomials

$$x^8+x+1, x^8+x^2+1, x^8+x^3+1, x^8+x^4+1, x^8+x^5+1, x^8+x^6+1.$$

For example, the minimum polynomial of T is x^8+x^3+1. It has that

$$\begin{aligned} & T^8+T^3+I=0 \\ \Rightarrow\ & T^8+T^3=I \\ \Rightarrow\ & T(T^7+T^2)=I \\ \Rightarrow\ & T^{-1}=T^7+T^2 \\ \Rightarrow\ & T^{-1}\in \mathbb{F}_2[T] \end{aligned}$$

Similarly, other situations have the same results. Above all, let $T \in GL(m, \mathbb{F}_2)$, $\#T$=1, $T+I$ is non-singular, then $T^{-1} \in \mathbb{F}_2[T]$.
□

3.3 Advantages of the Matrix Polynomial Residue Ring for Constructing Lightweight MDS Matrices

Let $T \in GL(m, \mathbb{F}_2)$, $\#T$=1, $T+I$ is non-singular and $f(x)$ is the minimum polynomial of T. Advantages of the matrix polynomial residue ring for constructing lightweight MDS matrices are as follows

(I) *Matrix with 1 XOR count can be used to construct MDS matrix.*

If we want to use matrix T with 1 XOR count to construct MDS matrix, we just need to let T to be an entry of MDS matrix, and other entries are chosen from $\mathbb{F}_2[T]$. In this way, T is successfully used to construct MDS matrix.

(II) *Computation of the matrix polynomial residue ring is more efficient than general matrix.* Computation of the matrix polynomial residue ring is equivalent to polynomial residue ring since the matrix polynomial residue ring is isomorphic to polynomial residue ring. Therefore computation of the matrix polynomial residue ring is more efficient than general matrix.

4 Equivalence Classes of Lightweight MDS Matrix

In this section, we investigate the abstract equivalence classes of 4×4 lightweight MDS matrix over the matrix polynomial residue ring.

Let $L_1, L_2 \in M(n, m)$, if L_1 can be transformed to become L_2 by exchanging rows or columns, then L_1 is equivalent to L_2.

For constructing lightest MDS matrix, the lightest MDS matrix should have as many identity matrices to be entries as possible since identity matrix over $\mathbb{F}_2$ has 0 XOR count. However, any sub-matrix of order 2, in MDS matrix, must not be $\begin{pmatrix} I & I \\ I & I \end{pmatrix}$.Otherwise, such matrix is not MDS. By using such point, we investigate the equivalence classes of lightweight 4×4 MDS matrices. We propose the following theorem.

Theorem 5 *Let $L \in M(4, m)$, if L is MDS and L has at least 8 identity matrices to be entries, L must take one of the following structures*

$$S_1 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ I & & & I \end{pmatrix}, S_2 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ & & & I \end{pmatrix}, S_3 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ & & I & \end{pmatrix},$$

$$S_4 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ I & & & \end{pmatrix}, S_5 = \begin{pmatrix} I & I & & \\ & I & I & \\ & & I & I \\ I & & & I \end{pmatrix},$$

where I is identity matrix over $\mathbb{F}_2$ and white positions can be any other non-singular matrices over $\mathbb{F}_2$.

According to [28], in a MDS matrix of degree n, there exist at most $3(n-1)$ identity matrices to be entries. This kind of matrix is called the *Optimal matrix*. For example, the following matrix is an Optimal matrix.

$$\begin{pmatrix} A_{1,1} & I & I & \cdots & I \\ I & I & A_{2,3} & \cdots & A_{2,n} \\ I & A_{3,2} & I & \cdots & A_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I & A_{n,2} & A_{n,3} & \cdots & I \end{pmatrix}$$

In previous papers, circulant matrix, Hadamard matrix and Optimal matrix are usually used to construct lightweight MDS matrices. They are as follows

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

$$Optimal\ matrix = \begin{pmatrix} A & I & I & I \\ I & I & A & B \\ I & B & I & A \\ I & A & B & I \end{pmatrix}.$$

It should be pointed that $Circ(I,I,A,B)$ is the special situation of S_5 and the Optimal matrix is the special situation of S_1.

Generally, when we construct lightest MDS matrices, if A, which is not identity matrix, is an entry in one of 5 equivalence classes, then $A+I$ should be non-singular. The reason is that there must exists a sub-determinant of order 2 like $\begin{vmatrix} I & I \\ I & A \end{vmatrix} = A + I$ in such matrix. Because of the requirement of MDS, $A+I$ should be non-singular.

5 General Algorithm of Constructing Lightweight MDS Matrices

In this section, we investigate the general algorithm for constructing lightweight MDS matrices over the matrix polynomial residue ring.

5.1 Entries Expression

In this subsection, we investigate entry expression in our algorithm.

In present paper, we investigate 4×4 matrices with entries in the $m \times m$ matrix polynomial residue ring, m=4 or 8. For example, like Optimal matrix

$$Optimal\ Matrix = \begin{pmatrix} A & I & I & I \\ I & I & A & B \\ I & B & I & A \\ I & A & B & I \end{pmatrix}.$$

In such Optimal matrix, T is a non-singular matrix, $\#T$=1, and $f(x)$ is the minimum polynomial of T. $A, B \in \mathbb{F}_2[T]$ and $a(x), b(x) \in \mathbb{F}_2[x]/(f(x))$. In our algorithm, x replaces T, 1 replaces I, $a(x)$ replaces A and $b(x)$ replaces B, where $A = a(T)$ and $B = b(T)$. Therefore this Optimal matrix is replaced as the following matrix in our algorithm

$$\begin{pmatrix} a(x) & 1 & 1 & 1 \\ 1 & 1 & a(x) & b(x) \\ 1 & b(x) & 1 & a(x) \\ 1 & a(x) & b(x) & 1 \end{pmatrix}.$$

In our algorithm, we first select such matrix T, which satisfies that $\#T = 1$, T and $T + I$ are non-singular. Find $f(x)$, which is the minimum polynomial of T. Then all entries of matrix are chosen from $\mathbb{F}_2[T]$. Original matrix is replaced by a matrix, where entries belong to $\mathbb{F}_2[x]/(f(x))$.

5.2 Judging MDS

In this subsection, we investigate MDS judgement in our algorithm.

Necessary and sufficient condition of MDS According to Theorem 1, $L \in M(n, m)$, L is MDS if and only if all sub-matrix of L are full rank. Sub-matrix being full rank is equivalent to sub-determinant being non-singular since entries are $m \times m$ matrices. Therefore the necessary and sufficient condition of MDS can also be described as follows

Theorem 6 *Let $L \in M(n, m)$, L is MDS if and only if all sub-determinant of L are non-singular.*

Above theorem is the method to judge whether matrix is MDS in our algorithm.

Sub-determinant calculation For instance, because entries are expressed as polynomials in our algorithm, so matrix is expressed as follows

$$\begin{pmatrix} x & 1 & 1 & 1 \\ 1 & 1 & x & x^2+1 \\ 1 & x^2+1 & 1 & x \\ 1 & x & x^2+1 & 1 \end{pmatrix}.$$

Sub-determinants are calculated according to determinant complete expansion formula. For instance, a sub-determinant of order 3 in above matrix can be calculated as follows

$$\begin{vmatrix} x & 1 & 1 \\ 1 & 1 & x \\ 1 & x^2+1 & 1 \end{vmatrix} = x + x + (x^2+1) + 1 + (x^4+x^2) + 1 = x^4 + 1.$$

Then let T be substituted into x^4+1 to get T^4+I.

Finally, judge whether T^4+I is non-singular. T^4+I is non-singular if and only if x^4+1 is relatively prime to $f(x)$, which is the minimum polynomial of T. We just find the greatest common factor of x^4+1 and $f(x)$. If the greatest common factor equals to 1, then T^+I is non-singular. Otherwise, it is singular.

5.3 General Algorithm

In this subsection, we investigate the General Algorithm for constructing lightest 4×4 MDS matrices over the $m\times m$ matrix polynomial residue ring, where m= 4 or 8.

Algorithm 1 General Algorithm

```
for Range over all T, #T=1, T and T+I are non-singular do
    Find the minimum polynomial of T in MP_4
    Find polynomials b_1(x),...,b_k(x) in X1_m, X2_m and X3_m, which satisfy that XOR count is less than 4.
    for i from 1 to 5 do
        for In S_i, every place, which is not 1, searches in {b_1(x),...,b_k(x)} do
            if Matrix is MDS then
                Record this MDS matrix and its sum of XORs
            end if
        end for
    end for
end for
```

6 Lightweight Non-involutory MDS Matrices

In this section, we construt non-involutory lightweight MDS matrices by using General Algorithm. Our platform is Intel i5-5300, 2.30GHz with 4GB memory, running Windows 10. We programme by using C language.

6.1 Construction over the 4×4 Matrix Polynomial Residue Ring

In this section, we construct lightweight 4×4 MDS matrices over the 4×4 matrix polynomial residue ring. We quickly construct many MDS matrices with 10 XORs, which are the optimal results at present. Our results are the same with [25]. We use 1 minute 42 seconds to find 288 MDS matrices with 10 XORs by using S1 matrix structure. It takes about 13 minutes to verify that there does not exist MDS matrices with 10 XORs in $S2$, $S4$ or $S5$. The details of constructions are as follows

Example 1 $T\in GL(m,\mathbb{F}_2)$.

Table 3: Lightweight Non-involutory MDS Matrices over the 4×4 Matrix Polynomial Residue Ring

Matrix type	Sum of XORs	Number	Running time
Circ(I, I, A, B)	12	96	00:00:01
Had(I, A, B, C)	20	288	00:00:04
Optimal	13	48	00:00:01
S1	10	288	00:01:42
S3	10	48	00:05:05

(1) m=4. $T = [[1, 2], 3, 4, 1]$. The following matrix is a MDS matrix with 10 XORs.

$$\begin{pmatrix} T^2+T & I & I & I \\ I & I & T & T^2+T \\ I & T^2+T & I & T^3+T^2 \\ I & T & T^3+T^2 & I \end{pmatrix}$$

(2) m=8. $T = [[2, 4], 3, 4, 5, 6, 7, 8, 1]$. The following matrix is a MDS matrix with 10 XORs.

$$\begin{pmatrix} T^2 & I & I & I \\ I & I & T & T^2 \\ I & T & I & T^7+T \\ I & T^7+T & T^2 & I \end{pmatrix}$$

6.2 Construction over the 8×8 Matrix Polynomial Residue Ring

In this subsection, we construct lightweight 4×4 MDS matrices over the 8×8 matrix polynomial residue ring. Recently, Li et al. investigate the lightest 4×4 MDS matrices over $GL(8, \mathbb{F}_2)$[19]. We and Li et al. get the same sum of XORs, which is the optimal results at present. The details of our constructions are as follows

Table 4: Lightweight Non-involutory MDS Matrices over 8×8 the Matrix Polynomial Residue Ring

Matrix type	Sum of XORs	Number	Time
Circ(I, I, A, B)	12	96	00:01:27
Had(I, A, B, C)	20	241920	00:07:00
Optimal	10	40320	00:01:16
S1	10	1128960	14:00:00

Table 5: Comparisons with previous constructions of non-involutory MDS matrices

Matrix type	Elements	Sum of XORs	Ref.
$Circ(I, I, A, B)$	$GL(8, \mathbb{F}_2)$	12	[19]
$Had(I, A, A^T, B)$	$GL(8, \mathbb{F}_2)$	20	[19]
$Optimal$	$GL(8, \mathbb{F}_2)$	10	[19]
$Had(0 \times 01, 0 \times 02, 0 \times 04, 0 \times 91)$	$F_{2^8}/0 \times 1c3$	52	[18]
$Subfield - Had(0 \times 1, 0 \times 2, 0 \times 8, 0 \times 9)$	$F_{2^4}/0 \times 13$	40	[18]
$Circ(0 \times 02, 0 \times 03, 0 \times 01, 0 \times 01)$	$F_{2^8}/0 \times 11b$	56	[4]
$Circ(0 \times 1, 0 \times 1, 0 \times 2, 0 \times 91)$	$F_{2^8}/0 \times 1c3$	24	[22]
$Circulant$	F_{2^8}	24	[24]
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{8\times8}]$	12	Ours
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times8}]$	20	Ours
$Optimal$	$\mathbb{F}_2[T_{8\times8}]$	10	Ours
S_1	$F_2[T_{8\times8}]$	10	Ours
$Had(I, A, B, C)$	$GL(4, \mathbb{F}_2)$	16	[19]
$Optimal$	$GL(4, \mathbb{F}_2)$	13	[19]
$Circ(I, I, A, B)$	$GL(4, \mathbb{F}_2)$	12	[19]
$Had(0 \times 1, 0 \times 2, 0 \times 8, 0 \times 9)$	$F_{2^4}/0 \times 13$	20	[18]
$Circ(0 \times 1, 0 \times 1, 0 \times 9, 0 \times 4)$	$F_{2^4}/0 \times 13$	12	[22]
$Circulant$	F_{2^4}	12	[24]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{4\times4}]$	20	Ours
$Optimal$	$\mathbb{F}_2[T_{4\times4}]$	13	Ours
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{4\times4}]$	12	Ours
S_1	$\mathbb{F}_2[T_{4\times4}]$	10	Ours

6.3 Construction over the 16×16 Matrix Polynomial Residue Ring

In this subsection, we construct lightweight 4×4 MDS matrices over the 16×16 matrix polynomial residue ring. We construct Circulant MDS matrices with 12 XORs and Optimal MDS matrices with 10 XORs.

Example 2 $T \in GL(16, \mathbb{F}_2)$. $T = [[1, 2], 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 1]$. The minimum polynomial of T is $x^{16} + x^{15} + 1$.

(1) L_1 is a circulant MDS matrix with 12 XORs.

$$L_1 = \begin{pmatrix} I & I & T & T^{14}+T^{13} \\ T^{14}+T^{13} & I & I & T \\ T & T^{14}+T^{13} & I & I \\ IT & T^{14}+T^{13} & I & \end{pmatrix}$$

(2) L_2 is a Optimal MDS matrix with 10 XORs.

$$L_2 = \begin{pmatrix} T & I & I & I \\ I & I & T & T^{14}+T^{13} \\ I & T^{14}+T^{13} & I & T \\ I & T & T^{14}+T^{13} & I \end{pmatrix}$$

7 Lightweight Involutory MDS Matrices

In this section, we investigate existences of involutory MDS matrices and constructions of lightweight involutory MDS matrices over the matrix polynomial residue ring. Our platform is Intel i5-5300, 2.30GHz with 4GB memory, running Windows 10. We programme by using C language.

7.1 Existences of Involutory MDS Matrices

In this subsection, we investigate existences of involutory MDS matrices.

Theorem 7 *Let L be an MDS matrix of degree $n (n \geq 2)$ over $GL(m, \mathbb{F}_2)$ as the following matrix, where the number of identity matrices is greater than or equal to $2n-1$. Then L is not involutory.*

$$L = \begin{pmatrix} * \cdots * & I & * \cdots * \\ \vdots \quad \vdots & \vdots & \vdots \quad \vdots \\ * \cdots * & I & * \cdots * \\ I \cdots I & A_{i,i} & I \cdots I \\ * \cdots * & I & * \cdots * \\ \vdots \quad \vdots & \vdots & \vdots \quad \vdots \\ * \cdots * & I & * \cdots * \end{pmatrix}$$

where $A_{i,i}$ is at the ith row and the ith column.

Proof. Assume that L is involutory.

When $n = 2k$, k=1,2,3$\cdots$. Then

$$L^2 = \begin{pmatrix} * \cdots & * & \cdots * \\ \vdots & \vdots & \vdots \\ * \cdots A_{i,i}^2 + I & \cdots & * \\ \vdots & \vdots & \vdots \\ * \cdots & * & \cdots * \end{pmatrix} = \begin{pmatrix} I\ 0 \cdots 0 \\ 0\ I \cdots 0 \\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\ 0 \cdots I \end{pmatrix} \Rightarrow A_{i,i}^2 = 0 \Rightarrow A_{i,i}\ \textit{is singular.}$$

Because L is MDS, so $A_{i,i}$ is non-singular. This is a contradiction. Therefore in this case, L can not be involutory.

When $n = 2k+1$, k=1,2,3$\cdots$. Then

$$L^2 = \begin{pmatrix} * \cdots & * & \cdots * \\ \vdots & \vdots & \vdots \\ * \cdots & A_{i,i}^2 & \cdots * \\ \vdots & \vdots & \vdots \\ * \cdots & * & \cdots * \end{pmatrix} = \begin{pmatrix} I\ 0 \cdots 0 \\ 0\ I \cdots 0 \\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\ 0 \cdots I \end{pmatrix} \Rightarrow A_{i,i}^2 = I$$

$$\Rightarrow A_{i,i}^2 + I = 0 \Rightarrow (A_{i,i} + I)^2 = 0 \Rightarrow A_{i,i} + I\ \textit{is singular.}$$

In L, there must exist a sub-determinant like $\begin{vmatrix} I & I \\ I & A_{i,i} \end{vmatrix} = A_{i,i} + I$. Becuase L is MDS, so $A_{i,i} + I$ should be non-singular. This is a contradiction. Therefore in this case, L must not be involutory.

In a word, L is not involutory.
□

According above theorem, Optimal MDS matrix as the following matrix can not be involutory.

$$\begin{pmatrix} * \cdots * & I & * \cdots * \\ \vdots \quad \vdots & \vdots & \vdots \quad \vdots \\ * \cdots * & I & * \cdots * \\ I \cdots I & A_{i,i} & I \cdots I \\ * \cdots * & I & * \cdots * \\ \vdots \quad \vdots & \vdots & \vdots \quad \vdots \\ * \cdots * & I & * \cdots * \end{pmatrix}$$

where $A_{i,i}$ is at the ith row and the ith column.

Theorem 8 *Let L be a MDS matrix of degree $2k+1 (k = 1, 2, \cdots)$ over $GL(m, \mathbb{F}_2)$ as the following matrix. Then L is not involutory.*

$$L = \begin{pmatrix} * \cdots * & I & * \cdots * \\ \vdots \quad \vdots & \vdots & \vdots \quad \vdots \\ * \cdots * & I & * \cdots * \\ I \cdots I & A_{i,j} & I \cdots I \\ * \cdots * & I & * \cdots * \\ \vdots \quad \vdots & \vdots & \vdots \quad \vdots \\ * \cdots * & I & * \cdots * \end{pmatrix}$$

where $A_{i,j}$ is at the ith row and the jth column$(i \neq j)$.

Proof. Assume that L is involutory. Then

$$L^2 = \begin{pmatrix} * & * & * & * & * \\ * & \ddots & * & * & * \\ * & * & \ddots & * & * \\ * & I & * & \ddots & * \\ * & * & * & * & * \end{pmatrix} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix}$$

In L^2, at the ith row and the jth column, the entry is I. But according the above equation, at this position, this entry also should be 0. This is a contradiction. And then before assumption is wrong. Therefore L is not involutory.
□

Theorem 9 *Let $T \in GL(m, \mathbb{F}_2)$, A_1, A_2, $\cdots$, $A_n \in \mathbb{F}_2[T]$. If $Circ(A_1, A_2, ..., A_n)$ is MDS, then $Circ(A_1, A_2, ..., A_n)$ is not involutory, where $n \geq 3$.*

Proof. $L = Circ(A_1, A_2, ..., A_n)$ is a MDS matrix as the following matrix, where A_1, A_2, $\cdots$, $A_n \in \mathbb{F}_2[T]$.

$$Circ(A_1, A_2, ..., A_n) = \begin{pmatrix} A_1 & A_2 & \cdots & A_n \\ A_n & A_1 & \cdots & A_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & \cdots & A_1 \end{pmatrix}$$

Assume that L is an involutory matrix.

When $n = 2k + 1$, $k = 1, 2, 3 \cdots$. Then

$$L^2 = \begin{pmatrix} A_1 & \cdots & A_{k+1} & \cdots & A_{2k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_{k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_1 \end{pmatrix} \begin{pmatrix} A_1 & \cdots & A_{k+1} & \cdots & A_{2k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_{k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_1 \end{pmatrix}$$

$$= \begin{pmatrix} * & * & \cdots & A_{k+1}^2 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} \Rightarrow A_{k+1}^2 = 0 \Rightarrow A_{k+1} \textit{ is singular.}$$

Because L is MDS, so A_{k+1} is non-singular. This is a contradiction. Therefore in this case, L can not be involutory.

When $n = 2k$, $k = 2, 3, 4 \cdots$. Then

$$L^2 = \begin{pmatrix} A_1 & \cdots & A_k & \cdots & A_{2k-1} & A_{2k} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_k & A_{k+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_1 & A_2 \\ * & \cdots & * & \cdots & A_{2k} & A_1 \end{pmatrix} \begin{pmatrix} A_1 & \cdots & A_k & \cdots & A_{2k-1} & A_{2k} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_k & A_{k+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_1 & A_2 \\ * & \cdots & * & \cdots & A_{2k} & A_1 \end{pmatrix}$$

$$= \begin{pmatrix} * & \cdots & A_k^2 + A_{2k}^2 & 0 \\ * & \cdots & * & * \\ \vdots & \cdots & \vdots & \vdots \\ * & \cdots & * & * \end{pmatrix} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} \Rightarrow A_k^2 + A_{2k}^2 = 0.$$

There is a 2×2 sub-matrix $\begin{pmatrix} A_k & A_{2k} \\ A_{2k} & A_k \end{pmatrix}$ in L.

$$L = \begin{pmatrix} A_1 & \cdots & A_k & \cdots & A_{2k} \\ \vdots & & \vdots & & \vdots \\ A_{k+1} & \cdots & A_{2k} & \cdots & A_k \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & * \end{pmatrix}$$

According above discussions, $A_k^2 + A_{2k}^2 = 0$. Because L is MDS, so $\begin{vmatrix} A_k & A_{2k} \\ A_{2k} & A_k \end{vmatrix} = A_k^2 + A_{2k}^2$ should be non-singular. This is a contradiction. Therefore in this case, L can not be involutory.

In a word, $Circ(A_1, A_2, ..., A_n)$ can not be an involutory MDS matrix.

□

7.2 Hadamard Involutory Matrices

Theorem 10 *Let $T \in GL(m, \mathbb{F}_2)$. $f(x)$ is the minimum polynomial of T. $a_1(x)$, $a_2(x)$, $\cdots$, $a_{2^k}(x) \in \mathbb{F}_2[x]/(f(x))$. $L = Had(a_1(T), a_1(T), \cdots, a_{2^k}(T))$ is involutory if and only if*

$$(\sum_{i=1}^{2^k} a_i(x))^2 \equiv 1 \ (mod \ f(x))$$

Proof. Because $T \in GL(m, \mathbb{F}_2)$ and $L = Had(a_1(T), a_1(T), \cdots, a_{2^k}(T))$ is involutory, so

$$L^2 = \begin{pmatrix} \sum_{i=1}^{2^k}(a_i(T))^2 & & & \\ & \sum_{i=1}^{2^k}(a_i(T))^2 & & \\ & & \ddots & \\ & & & \sum_{i=1}^{2^k}(a_i(T))^2 \end{pmatrix} = \begin{pmatrix} I & & & \\ & I & & \\ & & \ddots & \\ & & & I \end{pmatrix}$$

$$\Leftrightarrow \sum_{i=1}^{2^k}(a_i(x))^2 \equiv (\sum_{i=1}^{2^k} a_i(x))^2 \equiv 1 \ (mod \ f(x))$$

□

Deduction 1 *Let $T \in GL(m, \mathbb{F}_2)$. $f(x)$ is the minimum polynomial of T. $a(x)$, $b(x)$ and $c(x) \in \mathbb{F}_2[x]/(f(x))$. $L = Had(I, a(T), b(T), c(T))$ is involutory if and only if*

$$(a(x) + b(x) + c(x))^2 \equiv 0 \ (mod \ f(x))$$

Proof. According to Theorem 10, $Had(I, a(T), b(T), c(T))$ is involutory if and only if $(1 + a(x) + b(x) + c(x))^2 \equiv 1 \ (mod \ f(x))$. $(1 + a(x) + b(x) + c(x))^2 \equiv 1 \ (mod \ f(x)) \Leftrightarrow (a(x) + b(x) + c(x))^2 \equiv 0 \ (mod \ f(x))$

□

We construct lightweight Hadamard involutory MDS matrices as $Had(I, A, B, C)$. In our experiments, $A \in GL(8, \mathbb{F}_2)$, $\#A$=1, $A + I$ is non-singular. $f(x)$ is the minimum polynomial of A. $b(x)$, $c(x) \in \mathbb{F}_2[x]/(f(x))$ and $B = b(A)$, $C = c(A)$. According to above theorem, $Had(I, A, B, C)$ is involutory if and only if $(x + b(x) + c(x))^2 \equiv 0 \ (mod \ f(x))$. So $x^2 \equiv (b(x) + c(x))^2 (mod f(x))$. As mentioned in section 4, the minimum polynomial of A must be one of the following polynomials

$$x^8 + x + 1, x^8 + x^2 + 1, x^8 + x^3 + 1, x^8 + x^4 + 1, x^8 + x^5 + 1, x^8 + x^6 + 1.$$

We find all $g(x)$ satisfying $g^2(x) \equiv x^2 \ (mod \ f(x))$, where $f(x)$ is one of above minimum polynomials. Each of $x^8 + x + 1$, $x^8 + x^3 + 1$, *and* $x^8 + x^5 + 1$ only has one solution. Each of $x^8 + x^2 + 1$, $x^8 + x^4 + 1$, *and* $x^8 + x^6 + 1$ has 16 solutions.

Specifically, solutions of $g(x)$ satisfying $g^2(x) \equiv x^2 \ (mod \ x^8 + x^2 + 1)$ are as follows

$$x,\ x^4+1,\ x^5+x^2,\ x^5+x^4+x^2+x^1+1,\ x^6+x^3+x^2+x^1,\ x^6+x^4+x^3+x^2+1,$$

$$x^6 + x^5 + x^3,\ x^6 + x^5 + x^4 + x^3 + x^1 + 1,\ x^7 + x^3 + 1,\ x^7 + x^4 + x^3 + x^1,$$

$$x^7+x^5+x^3+x^2+x^1+1,\ x^7+x^5+x^4+x^3+x^2,\ x^7+x^6+x^2+1,\ x^7+x^6+x^4+x^2+x^1,$$

$$x^7 + x^6 + x^5 + x^1 + 1,\ x^7 + x^6 + x^5 + x^4.$$

Solutions of $g(x)$ satisfying $g^2(x) \equiv x^2 \ (mod \ x^8 + x^4 + 1)$ are as follows

$$x,\ x^4+x^2+x^1+1,\ x^5+x^3,\ x^5+x^4+x^3+x^2+1,\ x^6+x^1+1,\ x^6+x^4+x^2+x^1,$$

$$x^6 + x^5 + x^3 + 1,\ x^6 + x^5 + x^4 + x^3 + x^2,\ x^7,\ x^7 + x^4 + x^2 + 1,\ x^7 + x^5 + x^3 + x^1,$$

$$x^7 + x^5 + x^4 + x^3 + x^2 + x^1 + 1,\ x^7 + x^6 + 1,\ x^7 + x^6 + x^4 + x^2,$$

$$x^7 + x^6 + x^5 + x^3 + x^1 + 1,\ x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1.$$

Solutions of $g(x)$ satisfying $g^2(x) \equiv x^2 \ (mod \ x^8 + x^6 + 1)$ are as follows

$$x,\ x^4 + x^3 + x^1 + 1,\ x^5 + x^3 + 1,\ x^5 + x^4,\ x^6 + x^3 + x^2 + 1,\ x^6 + x^4 + x^2,$$

$$x^6+x^5+x^2+x^1,\ x^6+x^5+x^4+x^3+x^2+x^1+1,\ x^7+x^2+1,\ x^7+x^4+x^3+x^2,$$

$$x^7 + x^5 + x^3 + x^2 + x^1,\ x^7 + x^5 + x^4 + x^2 + x^1 + 1,\ x^7 + x^6 + x^3 + x^1,$$

$$x^7 + x^6 + x^4 + x^1 + 1,\ x^7 + x^6 + x^5 + 1,\ x^7 + x^6 + x^5 + x^4 + x^3.$$

7.3 Construction of Lightweight Hadamard Involutory MDS Matrices

In this subsection, we investigate constructions of lightweight Hadamard involutory 4×4 MDS matrices over the matrix polynomial residue ring.

We propose the Algorithm 2, which is specially designed to construct lightweight Hadamard involutory MDS matrices. Constructing 80640 Hadamard involutory MDS matrices with 20 XORs takes about 4 minutes and 14 seconds. In our experiments, when entries are 4×4 matrices over $\mathbb{F}_2$, the lightest Hadamard involutory MDS matrices with 24 XORs. When entries are 8×8 matrices over $\mathbb{F}_2$, the lightest Hadamard involutory MDS matrices with 20 XORs.

Example 3

(1) m=4. $T = [[1, 2], 3, 4, 1]$. The following matrix is a Hadamard involutory MDS matrix with 24 XORs.

$$\begin{pmatrix} I & T & T^2 & T^2+T \\ T & I & T^2+T & T^2 \\ T^2 & T^2+T & I & T \\ T^2+T & T^2 & T & I \end{pmatrix}$$

(2) m=8. $T = [4, 1, 2, 8, 6, 3, [5, 8], 7]$. The following matrix is a Hadamard involutory MDS matrix with 20 XORs.

$$\begin{pmatrix} I & T & T^6+T^4 & T^2 \\ T & I & T^2 & T^6+T^4 \\ T^6+T^4 & T^2 & I & T \\ T^2 & T^6+T^4 & T & I \end{pmatrix}$$

Table 6: Comparisons with previous constructions of involutory MDS matrices

Matrix type	Elements	Sum of XORs	Ref.
$Hadamard - Cauchy(0 \times 01, 0 \times 02, 0 \times fc, 0 \times fe)$	$F_{2^8}/0 \times 11b$	296	[17]
$Had(0 \times 01, 0 \times 02, 0 \times 04, 0 \times 06)$	$F_{2^8}/0 \times 11d$	88	[26]
$Had(0 \times 01, 0 \times 02, 0 \times b0, 0 \times b2)$	$F_{2^8}/0 \times 165$	64	[18]
$Subfield - Had(0 \times 1, 0 \times 4, 0 \times 9, 0 \times d)$	$F_{2^4}/0 \times 13$	48	[18]
$Had(I, A, A^{-1}, A + A^{-1})$	$GL(8, \mathbb{F}_2)$	40	[19]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times 8}]$	32	Ours
$Had(I, A, A^{-1}, A + A^{-1})$	$GL(4, \mathbb{F}_2)$	24	[19]
$Had(0 \times 1, 0 \times 4, 0 \times 9, 0 \times d)$	$F_{2^4}/0 \times 13$	24	[27][18]
$Had(0 \times 1, 0 \times 2, 0 \times 6, 0 \times 4)$	$F_{2^4}/0 \times 19$	24	[10]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{4\times 4}]$	24	Ours

Algorithm 2 Algorithm of Constructing Lightweight Hadamard Involutory MDS Matrices

Define matrix structure as $Had(I, A, B, C)$
for Search all $A \in GL(8, F_2)$, $\#A = 1, AandA + I$ are non-singular **do**
  x replaces A
  Find $f(x)$, which is the minimum polynomial of A in MP_8
  Find polynomials $b_1(x), \cdots, b_k(x)$ in $X1_8$, $X2_8$ and $X3_8$, which satisfy that XOR count is less than 4.
  Find all quadratic congruences of x^2 $(mod\ f(x))$.
  for i from 1 to k **do**
    $b_i(x)$ replaces B,
    for j from 1 to 16 **do** $b_i(x) + q_j(x)$ replace C, where q_j is a quadratic congruence of x^2 mod $f(x)$
      if Matrix is MDS **then**
        Record this MDS matrix and its sum of XORs
      end if
    end for
  end for
end for

Table 7: Comparisons of construction efficiency with [19]

Matrix type	Element	Sum of XORs	Number	Running time	Ref.
$Optimal$	$GL(8, \mathbb{F}_2)$	10	40320	no mentioned	[19]
$Optimal$	$\mathbb{F}_2[T_{8\times 8}]$	10	40320	1min 16sec	Ours
$S1$	$\mathbb{F}_2[T_{8\times 8}]$	10	1128960	14hours	Ours
$Circ(I, I, A, B)$	$GL(8, \mathbb{F}_2)$	12	80640	3days	[19]
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{8\times 8}]$	12	80640	1min 27sec	Ours
$Had(I, A, A^T, B)$	$GL(8, \mathbb{F}_2)$	20	622	4weeks	[19]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times 8}]$	20	241920	7min	Ours
$InvolutoryHad(I, A, A^{-1}, A + A^{-1})$	$GL(8, \mathbb{F}_2)$	40	80640	1day	[19]
$InvolutoryHad(I, A, B, C)$	$\mathbb{F}_2[T_{8\times 8}]$	32	40320	3min 22sec	Ours

8 Propositions about the Parity of XOR count

In this section, we propose propositions about the parity of XOR count.

Proposition 1 *Let A, B, $A + B \in GL(m, \mathbb{F}_2)$, then*

$$\#(A + B) \equiv \#(A) + \#(B) + m \pmod 2.$$

Proof. It is obviously that $\omega(A + B) \equiv \omega(A) + \omega(B) \pmod 2$.
Because $\#A = \omega(A) - m, \#B = \omega(B) - m$ and $\#(A + B) = \omega(A + B) - m$. Then

$$\#(A + B) \equiv \#(A) + \#(B) + m \pmod 2.$$

□

Proposition 2 *Let* $\alpha = (a_1, a_2, ..., a_m)^T$ *and* $\beta = (b_1, b_2, ..., b_m)^T$, *where* $a_i, b_i \in \mathbb{F}_2$. *Then*

$$\omega(\alpha\beta^T) = \omega(\alpha)\omega(\beta).$$

Proof. Because $\alpha = (a_1, a_2, ..., a_m)^T, \beta = (b_1, b_2, ..., b_m)^T$, then

$$\omega(\alpha\beta^T) = \omega\begin{pmatrix} a_1b_1 & a_1b_2 & \cdots & a_1b_m \\ a_2b_1 & a_2b_2 & \cdots & a_2b_m \\ \vdots & \vdots & \ddots & \vdots \\ a_mb_1 & a_mb_2 & \cdots & a_mb_m \end{pmatrix} = \sum_{i=1}^{m}\sum_{j=1}^{m} a_ib_j = \sum_{i=1}^{m} a_i \sum_{i=1}^{m} b_j = \omega(\alpha)\omega(\beta).$$

□

Proposition 3 *Let* $A, B \in GL(m, \mathbb{F}_2)$ *and* $A = (\alpha_1, \alpha_2, ..., \alpha_m)$ *and* $B = (\beta_1, \beta_2, ..., \beta_m)^T$. *Then*

$$\#(AB) \equiv \sum_{i=1}^{m} \omega(\alpha_i)\omega(\beta_i) \pmod 2.$$

Proof. Because $A = (\alpha_1, \alpha_2, ..., \alpha_m)$ and $B = (\beta_1, \beta_2, ..., \beta_m)^T$, so $AB = \sum_{i=1}^{m} \alpha_i\beta_i^T$. According to proposition 2,

$$\omega(AB) \equiv \sum_{i=1}^{m} \omega(\alpha_i\beta_i^T) \equiv \sum_{i=1}^{m} \omega(\alpha_i)\omega(\beta_i^T) \pmod 2.$$

Because $\#(AB) = \omega(AB) - m$, so

$$\#(AB) \equiv \sum_{i=1}^{m} \omega(\alpha_i)\omega(\beta_i^T) + m \pmod 2.$$

□

Proposition 4 *Let* $L_1, L_2, L_1 + L_2 \in M(n, m)$. *Then*

$$\#(L_1 + L_2) \equiv \#(L_1) + \#(L_2) + nm \pmod 2.$$

Proof. It is obviously that $\omega(L_1 + L_2) \equiv \omega(L_1) + \omega(L_2) \pmod 2$.
Because $\#(L_1 + L_2) = \omega(L_1) - n^2m$, $\#(L_1) = \omega(L_1) - n^2m$, $\#(L_2) = \omega(L_2) - n^2m$, so $\#(L_1 + L_2) \equiv \#(L_1) + \#(L_1) + n^2m \equiv \#(L_1) + \#(L_1) + nm \pmod 2$.
□

Proposition 5 *Let* $A_i, B_i \in GL(m, \mathbb{F}_2)$ *and* $i = 1, 2, ..., n$. *Then*

$$\omega\left(\begin{pmatrix} A_1 & A_2 & \cdots & A_n \end{pmatrix}\begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}\right) \equiv \omega(\sum_{i=1}^{n} A_i \sum_{j=1}^{n} B_j) \pmod 2.$$

Proof.

$$\omega\left(\begin{pmatrix} A_1 & A_2 & \cdots & A_n \end{pmatrix}\begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}\right) = \omega\begin{pmatrix} A_1B_1 & A_1B_2 & \cdots & A_1B_n \\ A_2B_1 & A_2B_2 & \cdots & A_2B_n \\ \vdots & \vdots & \ddots & \vdots \\ A_nB_1 & A_nB_2 & \cdots & A_nB_n \end{pmatrix}$$

$$\equiv \omega(\sum_{i,j=1}^{n} A_iB_j) \equiv \omega(\sum_{i=1}^{n} A_i \sum_{j=1}^{n} B_j) \pmod 2.$$

□

Proposition 6 *Let* $L_1, L_2, L_1L_2 \in M(n,m)$ *and*

$$L_1 = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix},\ L_2 = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1n} \\ B_{21} & B_{22} & \cdots & B_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ B_{n1} & B_{n2} & \cdots & B_{nn} \end{pmatrix}.$$

Then

$$\#(L_1L_2) \equiv \sum_{k=1}^{n} \omega(\sum_{i=1}^{n} A_{ik} \sum_{j=1}^{n} B_{kj}) + nm \pmod 2.$$

Proof.

$$\omega(L_1L_2) \equiv \omega \sum_{k=1}^{n} \left(\begin{pmatrix} A_{1k} \\ A_{2k} \\ \vdots \\ A_{nk} \end{pmatrix}\begin{pmatrix} B_{k1} & B_{k2} & \cdots & B_{kn} \end{pmatrix}\right)$$

$$\equiv \sum_{k=1}^{n} \omega \left(\begin{pmatrix} A_{1k} \\ A_{2k} \\ \vdots \\ A_{nk} \end{pmatrix}\begin{pmatrix} B_{k1} & B_{k2} & \cdots & B_{kn} \end{pmatrix}\right) \pmod 2.$$

According to proposition 5, then

$$\omega(L_1L_2) \equiv \sum_{k=1}^{n} \omega(\sum_{i=1}^{n} A_{ik} \sum_{j=1}^{n} B_{kj}) \pmod 2.$$

Because $\#(L_1L_2) = \omega(L_1L_2) - n^2m$, so

$$\#(L_1L_2) \equiv \sum_{k=1}^{n} \omega(\sum_{i=1}^{n} A_{ik} \sum_{j=1}^{n} B_{kj}) + n^2m$$

$$\equiv \sum_{k=1}^{n} \omega(\sum_{i=1}^{n} A_{ik} \sum_{j=1}^{n} B_{kj}) + nm \pmod 2.$$

□

9 Conclutions

In the present paper, we mainly investigate constructions of 4×4 lightweight MDS matrices over the matrix polynomial residue ring, where m=4, 8 or 16. According to distributions of the minimum polynomial and distributions of XOR count, we propose an efficient algorithm to construct lightest MDS matrices. Besides, we prove that some special MDS matrices can not be involytory. According to the quadratic congruence, we propose another efficient algorithm to construct lightweight Hadamard involutory MDS matrices, which are much lighter than previous papers. Finally, we prove a series of propositions about the parity of XOR count.

References

1. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222C239. Springer, Heidelberg (2011)
2. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher SQUARE. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149C165. Springer, Heidelberg (1997)
3. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326C341. Springer, Heidelberg (2011)
4. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)
5. 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)
6. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450C466. Springer, Heidelberg (2007)
7. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The Simeck family of lightweight block ciphers. In: Guneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 307C329. Springer, Heidelberg (2015)
8. Aumasson, J.-P., Henzen, L., Meier,W., Naya-Plasencia, M.: Quark: a lightweight hash. In: Mangard, S., Standaert, F.-X. (eds.) CHES 2010. LNCS, vol. 6225, pp. 1C15. Springer, Heidelberg (2010)
9. Bogdanov, Andrey, et al. "SPONGENT: A lightweight hash function." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2011.
10. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., Wang, Q., Yasuda, K.: PRIMATEs v1. Submission to the CAESAR Competition (2014). http://competitions.cr.yp.to/round1/primatesv1.pdf
11. Augot, D., Finiasz, M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 3C17. Springer, Heidelberg (2015)
12. Augot, D., Finiasz, M.: Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In: ISIT, pp. 1551C1555 (2013)

13. Berger, T.P.: Construction of recursive MDS diffusion layers from Gabidulin codes. In: Paul, G., Vaudenay, S. (eds.) INDOCRYPT 2013. LNCS, vol. 8250, pp. 274C285. Springer, Heidelberg (2013)
14. Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P.: Recursive diffusion layers for block ciphers and hash functions. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 385C401. Springer, Heidelberg (2012)
15. Wu, S.,Wang,M.,Wu,W.: Recursive diffusion layers for (lightweight) block ciphers and hash functions. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 355C371. Springer, Heidelberg (2013)
16. Nakahara Jr., J., Abraho, I.: A new involutory mds matrix for the aes. I. J Netw. Secur. 9(2), 109C116 (2009)
17. Chand Gupta, K., Ghosh Ray, I.: On constructions of circulant MDS matrices for lightweight cryptography. In: Huang, X., Zhou, J. (eds.) ISPEC 2014. LNCS, vol. 8434, pp. 564C576. Springer, Heidelberg (2014)
18. Sim S M, Khoo K, Oggier F, et al. Lightweight MDS involution matrices[C] //International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2015: 471-493
19. Li Y, Wang M. On the construction of lightweight circulant involutory MDS matrices[C]//Fast Software Encryption. 2016
20. Berger T P, El Amrani N. Codes over mathcal L(GF (2)^m, GF (2)^m), MDS Diffusion Matrices and Cryptographic Applications[C]//International Conference on Codes, Cryptology, and Information Security Springer International Publishing, 2015: 197-214
21. Gupta K C, Ray I G. On constructions of MDS matrices from companion matrices for lightweight cryptography[C]//International Conference on Availability, Reliability, and Security. Springer Berlin Heidelberg, 2013: 29-43
22. Liu M, Sim S M. Lightweight MDS generalized circulant matrices[C]//Fast Software Encryption. 2016
23. Gupta K C, Ray I G. On constructions of MDS matrices from companion matrices for lightweight cryptography[C]//International Conference on Availability, Reliability, and Security. Springer Berlin Heidelberg, 2013: 29-43
24. Beierle C, Kranz T, Leander G. Lightweight Multiplication in GF (2^n) with Applications to MDS Matrices[J]
25. Bai J, Wang D. The Lightest 4x4 MDS Matrices over GL (4, F2)
26. Barreto, P., Rijimen, V.: The anubis block cipher. Submission to the NESSIE Project(2000)
27. Jean, J., Nikolic, I., Peyrin, T.:Joltik v1.1. Submission to the CAESAR competition(2014) http://www1.spms.ntu.edu.sg/ syllab/Joltik
28. Junod P, Vaudenay S. Perfect diffusion primitives for block ciphers[C]//International Workshop on Selected Areas in Cryptography. Springer Berlin Heidelberg, 2004: 84-99