SCIENCE CHINA
Information Sciences

• **RESEARCH PAPER** •

On the Efficient Construction of Lightweight Orthogonal MDS Matrices

Lijing Zhou[1], Licheng Wang[1]* & Yiru Sun[1]

[1]*State Key Laboratory of Networking and Switching Technology,*
Beijing University of Posts and Telecommunications, Bei Jing 100876*, P.R. China*

Abstract In present paper, we mainly investigate the problem of efficiently constructing lightweight orthogonal MDS matrices over the matrix polynomial residue ring. Surprisingly, this problem did not receive much attention previously. We propose a necessary-and-sufficient condition, which is more efficient than the traditional method, about judging whether an orthogonal matrix is MDS. Although it has been proved that the circulant orthogonal MDS matrix does not exist over the finite field, we discuss anew this problem and get a new method to judge which polynomial residue ring can be used to construct the circulant orthogonal MDS matrix. According to this method, the minimum polynomials of non-singular matrices over $\mathbb{F}_2$ are factorized. With these results of factorizations, finally, we propose an extremely efficient algorithm for constructing lightweight circulant orthogonal MDS matrices. By using this algorithm, a lot of new lightweight circulant orthogonal MDS matrices are constructed for the first time.

Keywords MDS matrix, XOR count, polynomial residue ring, orthogonal matrix, circulant matrix

Citation Lijing Zhou, Licheng Wang and Yiru Sun. On the Efficient Construction of Lightweight Orthogonal MDS Matrices. Sci China Inf Sci, for review

1 Introduction

In block cipher, the linear diffusion layer is a significant component. For the linear diffusion layer, the branch number is a very important index. The linear diffusion layer with bigger branch number can more effectively resist linear and differential cryptanalysis. The linear diffusion layer is often expressed by a matrix. For a $n \times n$ matrix, its branch number is not greater than $n + 1$. The maximum distance separable (MDS) matrix is a matrix reaching the optimal branch number and is broadly used in many ciphers like SQUARE [2], PHOTON [1], AES [4], LED [3].

For the lightweight cryptography, the efficiency of a linear diffusion layer will influence the efficiency of cryptography largely. Therefore, constructions of lightweight MDS matrices are meaningful works for designing a lightweight cryptography. Considering that the sum of XORs [6] is the most important index for measuring the efficiency of MDS matrices, MDS matrices with fewer sum of XORs are more efficient.

Most constructions of lightweight MDS matrices are researched over $\mathbb{F}_{2^m}$ [8, 10, 11, 13]. At CRYPTO 2016, Beierle et al. [13] investigate the lightest circulant MDS matrices over $\mathbb{F}_{2^m}$. Currently, lightweight MDS matrices are investigated over $GL(m, \mathbb{F}_2)$ [9, 14]. At FSE 2016, Li et al. [9] construct 4×4 MDS

* Corresponding author (email: wanglc2012@126.com)

matrices over $GL(4,\mathbb{F}_2)$ with 13 XORs and 4×4 MDS matrices over $GL(8,\mathbb{F}_2)$ with 10 XORs. Li T. et al. [14] construct 4×4 MDS matrices over $GL(4,\mathbb{F}_2)$ with 10 XORs. Although constructing over $\mathbb{F}_{2^m}$ is efficient, the sum of XORs of the MDS matrix is larger. Although the sum of XORs of MDS matrices over $GL(m,\mathbb{F}_2)$ can achieve the minimum value, because of search space being too large, the construction is inefficient.

Motivations. The construction of the orthogonal MDS matrix is an important research direction. Most constructions of orthogonal MDS matrices are researched over $\mathbb{F}_{2^m}$. Recently, lightweight 4×4 orthogonal circulant MDS matrices over $GL(4,\mathbb{F}_2)$ are constructed in [9]. At present, 4×4 orthogonal MDS matrices over $GL(8,\mathbb{F}_2)$ have not been constructed. At present paper, we mainly solve problems as follows

(I) There is no efficient method to decide whether an orthogonal matrix is MDS.

(II) For orthogonal MDS matrices, if construct over $\mathbb{F}_{2^m}$, the sum of XORs is larger. If construct over $GL(m,\mathbb{F}_2)$, constructing is inefficient.

(III) One fact is that the finite field is a subset of the polynomial residue ring. Although it has been proved that the $2^d\times2^d$ circulant orthogonal matrix over $\mathbb{F}_{2^m}$ can not be MDS [7], there is no method to decide which polynomial residue ring can be used to construct $2^d\times2^d$ circulant orthogonal MDS matrices.

(IV) There is no efficient method for constructing lightweight orthogonal MDS matrices and lightweight circulant orthogonal MDS matrices.

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

- We propose a new necessary-and-sufficient condition, which is more efficient than the traditional method [9], about judging whether an orthogonal matrix is MDS. Besides, an efficient algorithm of constructing the lightweight orthogonal MDS matrix is given.
- Considering that finite fields is the subset of polynomial residue rings, we propose a method to judge which polynomial residue ring can be used to construct $2^d\times2^d$ circulant orthogonal MDS matrices. Moreover, an efficient necessary-and-sufficient condition for judging whether a 4×4 circulant matrix is an orthogonal matrix is given. An extremely efficient algorithm for constructing lightweight 4×4 circulant orthogonal MDS matrices is given.
- We search all the minimum polynomials of non-singular $m\times m$(m=4 or 8) matrices with 1 XOR over $\mathbb{F}_2$. According to factorizations of these minimum polynomials, only a part of them can be used to construct 4×4 circulant orthogonal MDS matrices. With theorems and methods mentioned in present paper, a lot of new lightweight circulant orthogonal MDS matrices are constructed for the first time.

Roadmap. In Section 2, introduce necessary preliminaries about the lightweight MDS matrix. In Section 3, propose a new necessary-and-sufficient condition for judging whether an orthogonal matrix is MDS. According to this condition, the efficient Algorithm 1 for constructing lightweight orthogonal MDS matrices is proposed. In Section 4, discuss the existence of circulant orthogonal. The extremely efficient Algorithm 2 for constructing 4×4 circulant orthogonal MDS matrices is given. In Section 5, by investigating the minimum polynomials of element-matrices, construct a lot of new lightweight circulant orthogonal MDS matrices. A short conclusion is given in Section 6.

2 Preliminaries

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

2.1 MDS Matrices

Let R be a ring with identity, $x\in R^m$. The *bundle weight* of x is defined as the number of nonzero entries of x and is expressed by $\omega_b(x)$. Let M be a $n\times n$ matrix over R. 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 search all nonzero $v\in R^n$. I.e. the branch number of $n\times n$ matrix M is $B_M=min_{v\neq0}\{\omega_b(v)+\omega_b(Mv)\}$, and

$B_M \leqslant n+1$. A *maximum distance separable* (MDS) $n \times n$ matrix is a matrix that has the maximum branch number n+1. $GL(n, \mathbb{F}_2)$ denotes the set of all non-singular $n \times n$ matrices over $\mathbb{F}_2$.

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 $L_{i,j} \in GL(m, \mathbb{F}_2)$ $(1 \leqslant i, j \leqslant n)$. $M(n,m)$ denotes all $n \times n$ 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 $1 \leqslant i, j \leqslant n, 1 \leqslant k \leqslant n$.

Theorem 1. [9] Let L is a $n \times n$ matrix over the commutative ring with identity, then L is MDS if and only if all square sub-matrices of L are of full rank.

In present paper, we construct MDS matrices in $M(n,m)$. So the above theory can be expressed as following two theorems:

Theorem 2. [9] Let $L \in M(n,m)$, then L is MDS if and only if all square sub-matrices of L are of full rank.

Theorem 3. [9] Let $L \in M(n,m)$, L is MDS if and only if all sub-determinant of L are non-singular.

2.2 XOR Count

Let $a, b \in \mathbb{F}_2$, $a+b$ is called a bit XOR operation. Let $A \in GL(m, \mathbb{F}_2)$, $x = (x_1, x_2, ..., x_m)^T \in {\mathbb{F}_2}^m$, $\#A$ denotes the number of XOR operations required to evaluate Ax. Let $\omega(A)$ is the number of 1 in A. $\#A = \omega(A) - m$, $\#A$ is also called by *XOR count* of A. For $L \in M(n,m)$, $\#(L)$ denotes *the sum of XORs* of L and $\#(L) = \sum_{i,j=1}^n \#(L_{ij})$. For example, let $x = (a,b,c,d)^T \in {\mathbb{F}_2}^4$, and the following matrix with 3 XOR count.

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

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

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, [4,3,2,[1,2]] is the representation of the following matrix with 1 XOR count.

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

2.3 Matrix Polynomial Residue Ring

The key contribution of present paper is that construct lightweight orthogonal MDS matrices over the matrix polynomial residue ring. In this subsection, we introduce the matrix polynomial residue ring.

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

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

$$\begin{aligned}
B &= b_{k-1}T^{k-1} + \cdots + b_1T + b_0I, \\
C &= c_{k-1}T^{k-1} + \cdots + c_1T + c_0I, \\
b(x) &= b_{k-1}x^{k-1} + \cdots + b_1x + b_0, \\
c(x) &= c_{k-1}x^{k-1} + \cdots + c_1x + c_0.
\end{aligned}$$

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

3 Orthogonal MDS Matrices

In this section, we propose a new necessary-and-sufficient condition for judging whether an orthogonal matrix is MDS. Then with this condition, we construct lightweight orthogonal MDS matrices.

3.1 Efficient Necessary-And-Sufficient Condition About Orthogonal MDS Matrices

Theorem 4. A is an orthogonal matrix of degree n over the commutative ring with identity. $|B|$ is a minor of $|A|$, and $|E|$ is the complementary minor of $|B|$. Then $|B| = 0$ if and only if $|E| = 0$.

Proof. R is a commutative ring with identity. A is an orthogonal matrix over R. $|B|$ is a minor of $|A|$. $|E|$ is the complement minor of $|B|$. Without loss of generality, let A be as follow

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} B & C \\ D & E \end{pmatrix}$$

For proving this theory, we only need to prove that $|B| = 0$ if and only if $|E| = 0$.

First, we prove that if $|B| = 0$ then $|E| = 0$.

Let B is as follow

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,k} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k,1} & b_{k,2} & \cdots & b_{k,k} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_k \end{pmatrix}$$

Because $|B| = 0$, so vectors $\beta_1, \beta_2, \cdots, \beta_k$ are linear dependent, so there exist not all zero k entries $m_1, m_2, \cdots, m_k \in R$ satisfying

$$m_1\beta_1 + m_2\beta_2 + \cdots + m_k\beta_k = (0, 0, \cdots, 0)$$

Then

$$m_1\alpha_1 + m_2\alpha_2 + \cdots + m_k\alpha_k = (0, 0, \cdots, 0, t_{k+1}, t_{k+2}, \cdots, t_n)$$

Because vectors $\alpha_1, \alpha_2, \cdots, \alpha_n$ are linear independent, so $t_{k+1}, t_{k+2}, \cdots, t_n$ not all are zero. Because A is orthogonal, so $(0, \cdots, 0, t_{k+1}, t_{k+2}, \cdots, t_n)$ is orthogonal with $\alpha_{k+1}, \alpha_{k+2}, \cdots, \alpha_n$. Then

$$(0,0,\cdots,0,t_{k+1},t_{k+2},\cdots,t_n)\begin{pmatrix}\alpha_{k+1}\\ \alpha_{k+2}\\ \vdots\\ \alpha_n\end{pmatrix}^T$$

$$=(0,0,\cdots,0,t_{k+1},t_{k+2},\cdots,t_n)\begin{pmatrix}a_{k+1,1} & a_{k+1,2} & \cdots & a_{k+1,n}\\ a_{k+2,1} & a_{k+2,2} & \cdots & a_{k+2,n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n,1} & a_{n,2} & \cdots & a_{n,n}\end{pmatrix}^T$$

$$=(t_{k+1},t_{k+2},\cdots,t_n)\begin{pmatrix}a_{k+1,k+1} & a_{k+1,k+2} & \cdots & a_{k+1,n}\\ a_{k+2,k+1} & a_{k+2,k+2} & \cdots & a_{k+2,n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n,k+1} & a_{n,2} & \cdots & a_{n,n}\end{pmatrix}^T$$

$$=(t_{k+1},t_{k+2},\cdots,t_n)E^T=(0,0,\cdots,0)$$

According the above equality, row vectors of E are linear independent. Then $|E|=0$.

Second, if $|E|=0$ then $|B|=0$. The process of proof is similar to the above process. So $|B|=0$ if and only if $|E|=0$.

□

Corollary 1. Let A be a $n\times n$ orthogonal matrix over the commutative ring with identity. $|B|$ is a minor of $|A|$, and $|E|$ is the complementary minor of $|B|$. Then $|B|\neq 0$ if and only if $|E|\neq 0$.

Theorem 5. Let A be a $n\times n$ orthogonal matrix over the commutative ring with identity. All minors of degree k of $|A|$ are non-zero if and only if all the complement minors of degree $n-k$ are non-zero.

Proof. Every minor of degree k must have a corresponding single complement minor of degree $n-k$. The number of all minors of degree k is equal to the number of all minors of degree $n-k$. So complement minors of all minors of degree k just are all minors of degree $n-k$. According to the Theorem 1, it is obvious that all minors of degree k are non-zero if and only if all minors of degree $n-k$ are non-zero.

□

According to Theorem 5, we propose a necessary-and-sufficient condition, which is more efficient than Theorem 2, for judging whether an orthogonal matrix is MDS as follow

Theorem 6. Let A be an orthogonal matrix of degree n over the commutative ring with identity. Then A is MDS if and only if all minors of degree between from 1 to $\lfloor\frac{n}{2}\rfloor$ are non-zero.

Proof. According to Theory 1, matrix A is MDS if and only if all minors of degree from 1 to n are non-zero. According to the Theorem 5, for orthogonal matrices, if minors of degree 1 are non-zero, then minors of degree $n-1$ must be non-zero. Similarly, if minors of degree 2 are non-zero, then minors of degree $n-2$ must be non-zero. And so on, an orthogonal matrix is MDS if and only if all minors of degree between from 1 to $\lfloor\frac{n}{2}\rfloor$ are non-zero. $\lfloor t\rfloor$ denotes the greatest integer being not greater than t.

□

3.2 Algorithm for Efficiently Constructing Lightweight Orthogonal MDS Matrices

In this subsection, we propose an efficient algorithm for constructing orthogonal MDS matrices over the $m\times m$ matrix polynomial residue ring.

Table 1 Comparison between Theorem 6 and Theorem 2

Degree of the Matrix	Degree of Minors Calculated	Method of Deciding MDS
4	1,2,3,4	Theorem 2
4	1,2	Theorem 6
5	1,2,3,4,5	Theorem 2
5	1,2	Theorem 6

3.2.1 *Entries Expression*

In present paper, we investigate 4×4 matrices with entries in the $m \times m$ matrix polynomial residue ring. For example as follow

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

In such Optimal matrix, T is a non-singular $m \times m$ matrix, $\#T$=1, and $f(x)$ is the minimum polynomial of T. $A, B \in \mathbb{F}_2[T]$ and $a(x), b(x) \in \mathbb{F}_2[x]/(f(x))$ satisfying $A = a(T)$ and $B = b(T)$. In our algorithm, x replaces T, 1 replaces I, $a(x)$ replaces A and $b(x)$ replaces B. 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 Algorithm 1, we first select non-singular matrix T, which satisfies that $\#T = 1$, T and $T + I$ are non-singular. Find the minimum polynomial $f(x)$ of T. Then all entries of matrix are chosen from $\mathbb{F}_2[T]$. The original matrix is replaced by a matrix with entries in $\mathbb{F}_2[x]/(f(x))$.

3.2.2 *Construct Orthogonal Matrices*

T is a $m \times m$ non-singular matrix over $\mathbb{F}_2$ and $f(x)$ is the minimum polynomial of T. Let L be a 4×4 matrix over $\mathbb{F}_2[x]/(f(x))$ as follow

$$L = \begin{pmatrix} l_{1,1}(x) & l_{1,1}(x) & l_{1,3}(x) & l_{1,1}(x) \\ l_{2,1}(x) & l_{2,2}(x) & l_{2,3}(x) & l_{2,4}(x) \\ l_{3,1}(x) & l_{3,2}(x) & l_{3,3}(x) & l_{3,4}(x) \\ l_{4,1}(x) & l_{4,2}(x) & l_{4,3}(x) & l_{4,4}(x) \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix}.$$

If L is an orthogonal matrix, L should satisfy following two conditions
(1)$\alpha_k \alpha_k^T = l_{k,1}^2(x) + l_{k,2}^2(x) + l_{k,3}^2(x) + l_{k,4}^2(x) = 1 \pmod{f(x)}$ $(k = 1, 2, 3\ or\ 4)$
(2)$\alpha_i \alpha_j^T = 0$ ($i \neq j$ and $1 \leqslant i, j \leqslant 4$)

3.2.3 *MDS Judgment*

For judging whether a 4×4 orthogonal matrix over the matrix polynomial residue ring is MDS, according to Theorem 6, all minors of degree 1 and 2 of this orthogonal matrix should be non-singular. If one of these minors is singular, then this orthogonal matrix is not MDS. According to the polynomial residue ring theory, a matrix over $\mathbb{F}_2[x]/(f(x))$ is non-singular if and only if the determinant of this matrix is relatively prime with $f(x)$.

For instance, T is a non-singular matrix over $\mathbb{F}_2$, and $f(x)$ is the minimum polynomial of T. Let H be a matrix with entries in $\mathbb{F}_2[T]$. Because entries of H are expressed by polynomials in our algorithms, so H can be expressed as follow

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

Every minor is calculated according to the determinant complete expansion formula. For example, a minor of order 3 in H can be calculated as follow

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

If x^4+1 is relatively prime with $f(x)$, this sub-matrix is non-singular.

According to above contents, we propose the Algorithm 1 to construct $n \times n$ lightweight orthogonal MDS matrices as follow

Algorithm 1 Construct Lightweight Orthogonal MDS matrices

1: **for** Search all T with as few XORs as possible. T and $T+I$ are non-singular. **do**
2: Find the minimum polynomial $f(x)$ of T.
3: **for** Construct orthogonal matrices over $\mathbb{F}_2[x]/(f(x))$. **do**
4: Calculate all minors of degree from 1 to $\lfloor \frac{n}{2} \rfloor$ of every orthogonal matrix. If all minors are relative prime with the minimum polynomial $f(x)$, then this orthogonal matrix is MDS. Otherwise this orthogonal matrix is not MDS and search next orthogonal matrix.
5: Let T be substituted into this orthogonal MDS matrix and compute the sum of XORs of this MDS matrix.
6: **end for**
7: **end for**

Remark 1. Algorithm 1 improves the efficiency of constructing orthogonal MDS matrices as follows

(I) *By using Theory 6, largely reduce computation of MDS judgment. Improve the efficiency of judging whether an orthogonal matrix is MDS.*

(II) *By using the matrix polynomial residue ring to express entries of MDS matrices, improve the efficiency of calculating minors of MDS matrices.*

By using Algorithm 1, over the 4×4 matrix polynomial residue ring, constructing 288 4×4 circulant orthogonal MDS matrices with 24 XORs takes 51 seconds. The experiment platform is Intel i5-5300, 2.30GHz with 4GB memory, running Windows 10. Programming language is the C language. One example is given as follow:

Let $T = [[1,2],3,4,1]$. The following matrix is a circulant orthogonal MDS matrix with 24 XORs.

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

4 Analyzing Circulant Orthogonal MDS Matrices

In this section, we discuss the existence of the $2^d \times 2^d$ circulant orthogonal MDS matrix. We propose an efficient necessary-and-sufficient condition for judging whether a 4×4 circulant matrix is an orthogonal matrix. We give a method to judge which polynomial residue ring can be used to construct $2^d \times 2^d$

circulant orthogonal MDS matrices. With this method, an extremely efficient algorithm for building lightweight 4×4 circulant orthogonal MDS matrices is given.

4.1 Existence of Circulant Orthogonal MDS matrices

Theorem 7. Let $g(x)$ be an irreducible polynomial over $\mathbb{F}_2$, and $f(x) = g(x)^k$ $(k \geqslant 1)$. If $(a_1, a_2, \cdots, a_{2^d})$ is a $2^d \times 2^d$ circulant orthogonal matrix over $\mathbb{F}_2[x]/(f(x))$, then $(a_1, a_2, \cdots, a_{2^d})$ is not MDS.

Proof. Let $(a_1, a_2, \cdots, a_{2^d})$ is as follow

$$(a_1, a_2, \cdots, a_{2^d}) = \begin{pmatrix} a_1 & a_2 & \cdots & a_{2^d} \\ a_{2^d} & a_1 & \cdots & a_{2^d-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^d-1} \\ \alpha_{2^d} \end{pmatrix}$$

Because $(a_1, a_2, \cdots, a_{2^d})$ is an orthogonal matrix, so

$$a_1^2 + a_2^2 + \cdots + a_{2^d}^2 = (a_1 + a_2 + \cdots a_{2^d})^2 = 1. \tag{1}$$

Then $a_1 + a_2 + \cdots a_{2^d}$ is relatively prime with $f(x)$.

Because $(a_1, a_2, \cdots, a_{2^d})$ is an orthogonal matrix again, so $\alpha_1 \alpha_{2k}^T = 0$ $(k = 1, 2, \cdots, 2^{d-2})$, and these equalities can be expressed as follows

$$\sum_{i=1}^{2^d} a_i a_{i+1} = \sum_{i=1}^{2^d} a_i a_{i+3} = \cdots = \sum_{i=1}^{2^d} a_i a_{i+\cdot 2^{d-1}-1} = 0,$$

where corner marks are computed modulo 2^d. By adding above equalities, we get the following equality

$$(a_1 + a_3 + \cdots + a_{2^d-1})(a_2 + a_4 + \cdots + a_2^d) = 0.$$

Then

$$f(x) \mid (a_1 + a_3 + \cdots + a_{2^d-1})(a_2 + a_4 + \cdots + a_2^d). \tag{2}$$

First of all, we will prove that $f(x) \nmid (a_1 + a_3 + \cdots + a_{2^d-1})$ and $f(x) \nmid (a_2 + a_4 + \cdots + a_2^d)$.

If $f(x) \mid (a_1 + a_3 + \cdots + a_{2^d-1})$, then $a_1 + a_3 + \cdots + a_{2^d-1} = 0$. This will result in the following minor equals 0.

$$\begin{vmatrix} a_1 & a_3 & \cdots & a_{2^d-1} \\ a_{2^d-1} & a_1 & \cdots & a_{2^d-3} \\ \cdots & \cdots & \cdots & \cdots \\ a_5 & a_7 & \cdots & a_3 \\ a_3 & a_5 & \cdots & a_1 \end{vmatrix} = 0$$

It goes against the requirement of MDS, so $f(x) \nmid (a_1 + a_3 + \cdots + a_{2^d-1})$. It can be similar that if $f(x) \mid (a_2 + a_4 + \cdots + a_2^d)$, then the following minor equals 0.

$$\begin{vmatrix} a_2 & a_4 & \cdots & a_{2^d} \\ a_{2^d} & a_2 & \cdots & a_{2^d-2} \\ \cdots & \cdots & \cdots & \cdots \\ a_6 & a_8 & \cdots & a_4 \\ a_4 & a_6 & \cdots & a_2 \end{vmatrix} = 0$$

It also goes against the requirement of MDS, so $f(x) \nmid (a_2 + a_4 + \cdots + a_{2^d})$.

Next, for $f(x) = g(x)^k$, we prove in following two situations.

First situation, $k = 1$. According to Equality 2, then $f(x) \nmid (a_1 + a_3 + \cdots + a_{2^d-1})$ or $f(x) \nmid (a_2 + a_4 + \cdots + a_2^d)$. According to above proof, we know that this goes against the requirement of MDS. So when $k = 1$, $(a_1, a_2, \cdots, a_{2^d})$ is not MDS.

Second situation, $k \geqslant 2$. According to Equality 2 and $f(x) \nmid (a_1 + a_3 + \cdots + a_{2^d-1})$ and $f(x) \nmid (a_2 + a_4 + \cdots + a_2^d)$, we can get that $g(x) \mid (a_1 + a_3 + \cdots + a_{2^d-1})$ and $g(x) \mid (a_2 + a_4 + \cdots + a_2^d)$. It result in that $a_1 + a_2 + \cdots a_{2^d}$ is not relatively prime with $f(x)$ But according to Equality 1, $a_1 + a_2 + \cdots a_{2^d}$ is relatively prime with $f(x)$. So when $k \geqslant 2$, $(a_1, a_2, \cdots, a_{2^d})$ is not MDS.

□

Remark 2. For Theorem 7, two aspects should be pointed:

(I) *The finite field is a special case in Theorem 7.*

Only when $k = 1$, $\mathbb{F}_2[x]/(f(x))$ is a finite field. When $k > 1$, $\mathbb{F}_2[x]/(f(x))$ is a finite ring. Chand Gupta, K. et al. [7] only proved that the $2^d \times 2^d$ circulant orthogonal matrix over the finite field must not be MDS. We prove the existence of circulant the orthogonal matrix over a bigger set than [7].

(II) *The $2^d \times 2^d$ circulant orthogonal MDS matrix has the chance to be constructed.*

Let $h_1(x) \neq 1$, $h_2(x) \neq 1$. $h_1(x)$ is relatively prime with $h_2(x)$. $f(x) = h_1(x)h_2(x)$. Then $f(x)$ is not the case of Theorem 7. In this case, we have a chance to construct the $2^d \times 2^d$ circulant orthogonal MDS matrix over $\mathbb{F}_2[x]/(f(x))$. With this point, we will efficiently construct lightweight 4×4 circulant orthogonal MDS matrices later.

4.2 Efficient Necessary-And-Sufficient Condition about Deciding 4×4 Circulant Orthogonal Matrices

Theorem 8. Let $f(x)$ be a polynomial over $\mathbb{F}_2$. Let (a, b, c, d) be a 4×4 circulant matrix over $\mathbb{F}_2[x]/(f(x))$. Then (a, b, c, d) is an orthogonal matrix if and only if $(a + b + c + d)^2 \equiv 1 \pmod{f(x)}$ and $(a + c)(b + d) \equiv 0 \pmod{f(x)}$.

Proof. Let (a, b, c, d) be as follow

$$(a, b, c, d) = \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix}$$

(a, b, c, d) is an orthogonal matrix if and only if

(I) $|\alpha_1| = |\alpha_2| = |\alpha_3| = |\alpha_4| = 1$ and

(II) $\alpha_i \alpha_j^T = 0$ $(i \neq j, 1 \leqslant i, j \leqslant 4)$.

For **(I)**, because (a, b, c, d) is a circulant matrix over $\mathbb{F}_2[x]/(f(x))$, so

$$|\alpha_1| = |\alpha_2| = |\alpha_3| = |\alpha_4| = a^2 + b^2 + c^2 + d^2 = (a + b + c + d)^2 \equiv 1 \pmod{f(x)}.$$

Then $|\alpha_1|$=$|\alpha_2|$=$|\alpha_3|$=$|\alpha_4| = 1$ is equivalent to $(a + b + c + d)^2 = 1$

For **(II)**, because (a, b, c, d) is a circulant matrix, so

$$\alpha_1\alpha_2^T = \alpha_2\alpha_3^T = \alpha_3\alpha_4^T = \alpha_1\alpha_4^T \textit{ and } \alpha_1\alpha_3^T = \alpha_2\alpha_4^T.$$

It is obvious that $\alpha_1\alpha_3^T$=$\alpha_2\alpha_4^T$=$ac + bd + ca + db$=0. Besides, $\alpha_1\alpha_2^T$=$ab + bc + cd + da$=$(a + c)(b + d)$. So $\alpha_i\alpha_j^T = 0$ $(i \neq j, 1 \leqslant i, j \leqslant 4)$ is equivalent to $(a + c)(b + d) = 0$.

□

4.3 The Choice of Elements

In this subsection, we introduce how to choose elements to construct 4×4 circylant orthogonal MDS matrices.

Theorem 9. Let $f(x)$ be a polynomial over $\mathbb{F}_2$. If (a, b, c, d) is a 4×4 circulant orthogonal MDS matrix over $\mathbb{F}_2[x]/(f(x))$, then there exist $g(x)$ and $t(x)$ satisfying $f(x) = g(x)t(x)$, $g(x) \neq 1$, $t(x) \neq 1$, $g(x) \mid (a + c)$, $t(x) \mid (b + d)$ and $g(x)$ is relatively prime with $t(x)$.

Proof. Let $L = (a, b, c, d)$ be a circulant orthogonal MDS matrix over $\mathbb{F}_2[x]/(f(x))$ as follow

$$L = \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}$$

According to Theorem 8, $f(x) \mid (a + c)(b + d)$. First, we prove $f(x) \nmid (a + c)$ and $f(x) \nmid (b + d)$.

Assume $f(x) \mid (a + c)$. Because of $a, c \in \mathbb{F}_2[x]/(f(x))$, then $a = c$. This results in that $L = (a, b, c, d)$=(a, b, a, d) be as follow

$$L = \begin{pmatrix} a & b & a & d \\ d & a & b & a \\ a & d & a & b \\ b & a & d & a \end{pmatrix}$$

In this matrix, there is a minor $\begin{vmatrix} a & a \\ a & a \end{vmatrix} = 0$. This does not satisfy the requirement of MDS. But (a, b, c, d) is MDS, so this is a contradiction. This assumption is wrong. Then $f(x) \nmid (a + c)$. When $f(x) \mid (b + d)$, the result is similar. So $f(x) \nmid (a + c)$ and $f(x) \nmid (b + d)$. According to $f(x) \mid (a + c)(b + d)$, there exist $g(x)$ and $t(x)$ satisfying

$$g(x) \neq 1, t(x) \neq 1, g(x) \mid (a + c), t(x) \mid (b + d) \textit{ and } f(x) = g(x)t(x).$$

Let $a + c = g(x)r_1(x)$ and $b + d = t(x)r_2(x)$.

Next we prove that $g(x)$ is relatively prime with $t(x)$.

Assume $g(x)$ is not relatively prime with $t(x)$. It means that there exists $h(x) \neq 1$ satisfying

$$g(x) = g'(x)h(x) \textit{ and } t(x) = t'(x)h(x).$$

This results in that $(a + b + c + d)^2$ is not relatively with $f(x)$. But according to Theorem 8, then

$$(a + b + c + d)^2 \equiv 1 \pmod{f(x)}.$$

This results in that $(a + b + c + d)^2$ is relatively with $f(x)$. Then this assumption is wrong. So $g(x)$ is relatively prime with $t(x)$.

□

Remark 3. According to Theorem 9,

$$a + c = g(x)r_1(x) \textit{ and } b + d = t(x)r_2(x).$$

Next we prove that $r_1(x)$ and $r_2(x)$ are well-determined.

Proof. Because of $g(x)$ being relatively prime with $t(x)$, so there are well-determined $r_1'(x)$ and $r_2'(x)$ satisfying

$$g(x)r_1'(x) + t(x)r_2'(x) = 1.$$

According to the proof of Theorem 9,

$$g(x)r_1(x)+t(x)r_2(x)=1.$$

So $r_1(x)=r'_1(x)$ and $r_2(x)=r'_2(x)$. Then $r_1(x)$ and $r_2(x)$ are well-determined.

□

According to Theorem 9 and Remark 3, we give the Algorithm 2 to efficiently construct 4×4 circulant orthogonal MDS matrices.

Algorithm 2 Construct Lightweight 4×4 Circulant Orthogonal MDS matrices over $m\times m$ Matrix Polynomial Residue Rings

for Search every non-singular $m\times m$ matrix T with a few of XORs over $\mathbb{F}_2$. **do**
  Find the minimum polynomial $f(x)$ of T.
  if $f(x)=g(x)t(x)$ satisfying $g(x)\neq 1$, $t(x)\neq 1$ and $g(x)$ is relatively prime with $t(x)$. **then**
    Find $r_{i1}(x), r_{i2}$ satisfying $g(x)r_{i1}+t(x)r_{i2}=1$. Let p_{i1}=$g(x)r_{i1}$, p_{i2}=$t(x)r_{i2}=1$. Sore p_{i1} and p_{i2}.
  end if
end for
for i from 1 to k. **do**
  for Search a over $\mathbb{F}_2[x]/(f_i(x))$. **do**
    for Search b over $\mathbb{F}_2[x]/(f_i(x))$. **do**
      $c=a+p_{i1}(x), d=b+p_{i2}$.
      if The circulant orthogonal matrix (a,b,c,d) is MDS. **then**
        Store $f_i(x)$ and (a,b,c,d).
      end if
    end for
  end for
end for
for Search every $m\times m$ non-singular matrix T with a few of XORs. **do**
  for i from 1 to k. **do**
    if $f_i(T)=0$. **then**
      Substitute T into corresponding circulant orthogonal MDS matrix (a,b,c,d). Compute the sum of XORs of (a,b,c,d).
    end if
  end for
end for

Algorithm 2 can be summarized as following 3 steps:

Step 1: *Factorizing the minimum polynomials*

Find all matrices with few XORs in $GL(n,\mathbb{F}_2)$. Find all minimum polynomials $f_1(x), f_2(x), \cdots, f_k(x)$ of these matrices. Factorize $f_1(x), f_2(x), \cdots, f_k(x)$. Factorizing has two situations:

- $f_i(x)=g(x)^k$, where $g(x)$ is a irreducible polynomial over $\mathbb{F}_2$. At this case, ignore this $f_i(x)$.
- $f_i(x)=g_i(x)t_i(x)$ satisfying $g(x)\neq 1$, $t(x)\neq 1$ and $g(x)$ is relatively prime $t(x)$. At this case, store $f_i(x)$, which will be used at **Step 2**.

Step 2: *Constructing* 4×4 *circulant orthogonal matrices*

Find $r_{i1}(x)$ and $r_{i2}(x)$ satisfying $g_i(x)r_{i1}(x)+t_i(x)r_{i2}(x)=1$. Search a and b over $\mathbb{F}_2[x]/(f_i(x))$. $c=a+g_i(x)r_{i1}(x)$, $d=b+t_i(x)r_{i2}$. Construct the circulant matrix (a,b,c,d). (a,b,c,d) must be an orthogonal matrix.

Step 3: *Judging MDS*

For every (a,b,c,d), calculate all minors of (a,b,c,d). If all minors are relatively prime with $f(x)$, then (a,b,c,d) is MDS. Otherwise, it is not MDS.

Remark 4. With the traditional constructing method, only a few of circulant matrices are orthogonal matrices in vast candidate matrices. So the traditional constructing method is inefficient. With the Algorithm 2, every time constructing can certainly construct a 4×4 circulant orthogonal matrix and does not do any meaningless work. So this new method is obvious efficient.

5 Construct Lightweight 4×4 Circulant Orthogonal MDS Matrices

In this section, we factorize the minimum polynomials of $m \times m(m$=4 or 8) matrices over $\mathbb{F}_2$. According to factorizations, two efficient algorithms for constructing 4×4 lightweight circulant orthogonal MD-S matrices are given. Finally, by using such algorithms, new circulant orthogonal MDS matrices are constructed first time. The experiment platform is Intel i5-5300, 2.30GHz with 4GB memory, running Windows 10. Programming language is the C language.

5.1 Construct Over The 8×8 Matrix Polynomial Residue Ring

Let T be a 8×8 matrix over $\mathbb{F}_2$. $f(x)$ is the minimum polynomial of T. In $\mathbb{F}_2[T]$, the identity matrix I is the single matrix with 0 XOR count. When construct a MDS matrix with as few XORs as possible, there should be as many I being elements as possible in this MDS matrix. Other elements should have as few XORs as possible. Elements with 1 XOR should be used to construct lightest MDS matrix. For this purpose, let T with 1 XOR be an element of MDS matrix, and other elements are chosen from $\mathbb{F}_2[T]$.

If T is an element in a lightest MDS matrix, then there generally exists a minor in this MDS matrix as $\begin{vmatrix} I & I \\ I & T \end{vmatrix} = T + I$.

According to the requirement of MDS, T and $T+I$ should be non-singular.

Let T be a non-singular 8×8 matrix with 1 XOR over $\mathbb{F}_2$ satisfying $T+I$ non-singular. By searching all T, factorizations of minimum polynomials of these matrices are as follows

$$
\begin{aligned}
&x^8+x+1=(x^2+x+1)(x^6+x^5+x^3+x^2+1)\\
&x^8+x^2+1=(x^4+x+1)^2\\
&x^8+x^3+1=(x^3++x+1)(x^5+x^3+x^2+x+1)\\
&x^8+x^4+1=(x^2+x+1)^4\\
&x^8+x^5+1=(x^3+x^2+1)(x^5+x^4+x^3+x^2+1)\\
&x^8+x^6+1=(x^4+x^3+1)^2\\
&x^8+x^7+1=(x^2+x+1)(x^6+x^4+x^3+x+1)
\end{aligned}
$$

According to Theorem 7, only x^8+x+1, x^8+x^3+1, x^8+x^5+1 and x^8+x^7+1 can be used to construct 4×4 circulant orthogonal MDS matrices over $\mathbb{F}_2[x]/(f(x))$. While x^8+x^2+1, x^8+x^4+1 and x^8+x^6+1 can not.

According to Remark 3, x^8+x+1, x^8+x^3+1, x^8+x^5+1 and x^8+x^7+1 are investigated as follows

$$
\begin{aligned}
&f_1(x) = x^8 + x + 1 = (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1)\\
&\Rightarrow (x^2 + x + 1)(x^4 + x^2) + (x^6 + x^5 + x^3 + x^2 + 1) \cdot 1 = 1\\
&f_2(x) = x^8 + x^3 + 1 = (x^3 + +x + 1)(x^5 + x^3 + x^2 + x + 1)\\
&\Rightarrow (x^3 + +x + 1)(x^4 + x^3 + 1) + (x^5 + x^3 + x^2 + x + 1)(x^2 + x) = 1\\
&f_3(x) = x^8 + x^5 + 1 = (x^3 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1)\\
&\Rightarrow (x^3 + x^2 + 1)(x^3 + x^2 + x) + (x^5 + x^4 + x^3 + x^2 + 1)(x + 1) = 1\\
&f_4(x) = x^8 + x^7 + 1 = (x^2 + x + 1)(x^6 + x^4 + x^3 + x + 1)\\
&\Rightarrow (x^2 + x + 1)(x^4 + x^3 + x^2 + x) + (x^6 + x^4 + x^3 + x + 1) \cdot 1 = 1
\end{aligned}
\tag{3}
$$

$$
\begin{aligned}
&p_{11}(x) = (x^2 + x + 1)(x^4 + x^2) = x^6 + x^5 + x^3 + x^2,\\
&p_{12}(x) = x^6 + x^5 + x^3 + x^2 + 1,\\
&p_{21}(x) = (x^3 + +x + 1)(x^4 + x^3 + 1) = x^7 + x^6 + x^5 + x + 1,\\
&p_{22}(x) = (x^5 + x^3 + x^2 + x + 1)(x^2 + x) = x^7 + x^6 + x^5 + x,\\
&p_{31}(x) = (x^3 + x^2 + 1)(x^3 + x^2 + x) = x^6 + x^2 + x,\\
&p_{32}(x) = (x^5 + x^4 + x^3 + x^2 + 1)(x + 1) = x^6 + x^2 + x + 1,\\
&p_{41}(x) = (x^2 + x + 1)(x^4 + x^3 + x^2 + x) = x^6 + x^4 + x^3 + x,\\
&p_{42}(x) = x^6 + x^4 + x^3 + x + 1.
\end{aligned}
$$

Over 8×8 matrix polynomial residue rings, by using Algorithm 2, constructing 80640 4×4 circulant orthogonal MDS matrices with 40 XORs takes 39 minutes 19 seconds. Let $T = [[2, 8], 3, 4, 5, 6, 7, 8, 1]$. Details will be shown at Table 2. The following matrix is a circulant orthogonal MDS matrix with 40 XORs.

$$
\begin{pmatrix}
T^3 & T^3 & I & T^6 + T^4\\
T^6 + T^4 & T^3 & T^3 & I\\
I & T^6 + T^4 & T^3 & T^3\\
T^3 & I & T^6 + T^4 & T^3
\end{pmatrix}
$$

5.2 Construct Over The 4×4 Matrix Polynomial Residue Ring

By searching all non-singular 4×4 matrices over $\mathbb{F}_2$ with 1 XOR, the minimum polynomials of these matrices are as follows

$$
\begin{aligned}
&x^2 + 1 = (x + 1)^2\\
&x^3 + 1 = (x + 1)(x^2 + x + 1)\\
&x^3 + x^2 + x + 1 = (x + 1)^3\\
&x^4 + 1 = (x + 1)^4\\
&x^4 + x + 1 = x^4 + x + 1\\
&x^4 + x^2 + 1 = (x^2 + x + 1)^2\\
&x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1)\\
&x^4 + x^3 + 1 = x^4 + x^3 + 1\\
&x^4 + x^3 + x + 1 = (x + 1)(x^2 + x + 1)\\
&x^4 + x^3 + x^2 + 1 = (x + 1)(x^3 + x + 1)
\end{aligned}
$$

According to Theory 7, in above polynomials, only $x^3 + 1$, $x^4 + x^2 + x^1 + 1$, $x^4 + x^3 + x^1 + 1$ and $x^4 + x^3 + x^2 + 1$ can be used to construct circulant orthogonal matrices, but others can not.

According to Remark 3, x^3+1, x^4+x^2+x+1, x^4+x^3+x+1 and $x^4+x^3+x^2+1$ are investigated as follows

$$
\begin{aligned}
&h_1(x)=x^3+1=(x+1)(x^2+x+1)\\
&\Rightarrow (x+1)\cdot x+(x^2+x+1)\cdot 1=1\\
&h_2(x)=x^4+x^2+x+1=(x+1)(x^3+x^2+1)\\
&\Rightarrow (x+1)\cdot x^2+(x^3+x^2+1)\cdot 1=1\\
&h_3(x)=x^4+x^3+x+1=(x+1)(x^2+x+1)\\
&\Rightarrow (x+1)(x^2+x)+(x^3+x+1)\cdot 1=1\\
&h_4(x)=x^4+x^3+x^2+1=(x^1+1)(x^3+x+1)\\
&\Rightarrow (x^2+1)(x+1)+(x^2+x+1)\cdot x=1\\
\\
&q_{11}(x)=(x+1)\cdot x=x^2+x,\\
&q_{12}(x)=x^2+x+1,\\
&q_{21}(x)=(x+1)\cdot x^2=x^3+x^2,\\
&q_{22}(x)=x^3+x^2+1,\\
&q_{31}(x)=(x+1)(x^2+x)=x^3+x,\\
&q_{32}(x)=x^3+x+1,\\
&q_{41}(x)=(x^2+1)(x+1)=x^3+x^2+x+1,\\
&q_{42}(x)=(x^2+x+1)\cdot x=x^3+x^2+x.
\end{aligned}
\tag{4}
$$

Over 4×4 matrix polynomial residue rings, by using Algorithm 2, constructing 80 4×4 circulant orthogonal MDS matrices with 24 XORs takes less than 1 second. Let $T=[[1,2],3,4,1]$. Details will be shown at Table 2. The following matrix is a circulant orthogonal MDS matrix with 24 XORs.

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

Table 2 Number of Lightweight 4×4 Circulant Orthogonal MDS Matrices

Matrix type	Entries	Sum of XORs	Number	Running time
$Orthogonal\ Circ(a,b,c,d)$	$\mathbb{F}_2[T_{4\times 4}]$	24	80	<1seconds
$Orthogonal\ Circ(a,b,c,d)$	$\mathbb{F}_2[T_{8\times 8}]$	40	80640	39minute19second

Table 3 Comparisons with previous constructions of orthogonal circulant MDS matrices

Matrix type	Elements	Sum of XORs	Ref.
$OrthogonalCirc(I,A,B,C)$	$GL(4,\mathbb{F}_2)$	$\geqslant 24$	[9]
$OrthogonalCirc(A,B,C,D)$	$GL(4,\mathbb{F}_2)$	$\geqslant 24$	Ours
$OrthogonalCirc(A,B,C,D)$	$GL(8,\mathbb{F}_2)$	$\geqslant 40$	Ours

6 Conclutions

In present paper, we mainly investigate constructions of 4×4 lightweight orthogonal MDS matrices over the matrix polynomial residue ring. We propose a necessary-and-sufficient condition, which is more efficient than the traditional method, for judging whether an orthogonal matrix is MDS. We discuss the existence of the circulant orthogonal MDS matrix over the matrix polynomial residue ring. Although the circulant orthogonal MDS matrix has been proven not to exist, we get an efficient method to judge which polynomial residue ring can be used to construct circulant orthogonal MDS matrices. With this method, a lot of new lightweight circulant orthogonal MDS matrices are constructed for the first time.

Acknowledgements This work was supported by the National Natural Science Foundation of China (NSFC) (Nos. 61370194, 61502048).

Conflict of interest The authors declare that they have no conflict of interest.

Supporting information Appendix A. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In Annual Cryptology Conferencepp. 222-239. Springer Berlin Heidelberg (2011)
2 Daemen, J., Knudsen, L., Rijmen, V.: The block cipher Square. In International Workshop on Fast Software Encryption, pp. 149-165. Springer Berlin 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. 326-341. Springer, Heidelberg (2011)
4 Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)
5 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. http://competitions.cr.yp.to/round1/primatesv1.pdf(2014)
6 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. 355-371. Springer, Heidelberg (2013)
7 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. 564-576. Springer, Heidelberg (2014)
8 Sim, S. M., Khoo, K., Oggier, F., Peyrin, T.: Lightweight MDS involution matrices. In International Workshop on Fast Software Encryption, pp. 471-493. Springer Berlin Heidelberg(2015)
9 Li, Y., Wang, M.: On the construction of lightweight circulant involutory MDS matrices. In International Conference on Fast Software Encryption, pp. 121-139. Springer Berlin Heidelberg(2016)
10 Berger, T. P., El Amrani, N.: Codes over $L(GF(2)^m, GF(2)^m)$, MDS Diffusion Matrices and Cryptographic Applications. In International Conference on Codes, Cryptology, and Information Security, pp. 197-214. Springer International Publishing(2015)
11 Gupta, K. C., Ray, I. G.: On constructions of MDS matrices from companion matrices for lightweight cryptography. In International Conference on Availability, Reliability, and Security, pp. 29-43. Springer Berlin Heidelberg(2013)
12 Liu, M., Sim, S. M.: Lightweight MDS generalized circulant matrices. In International Conference on Fast Software Encryption, pp. 101-120. Springer Berlin Heidelberg(2016)
13 Beierle, C., Kranz, T., Leander, G.: Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices. In Annual Cryptology Conference, pp. 625-653. Springer Berlin Heidelberg(2016)
14 Li T., Bai J., Sun Y., Wang D., Lin D.: The Lightest 4x4 MDS Matrices over GL (4, F2) http://eprint.iacr.org/2016/686.pdf(2016)
15 Barreto, P., Rijimen, V.: The anubis block cipher. Submission to the NESSIE Project(2000)
16 Junod, P., Vaudenay, S.: Perfect diffusion primitives for block ciphers. In International Workshop on Selected Areas in Cryptography, pp. 84-99. Springer Berlin Heidelberg(2004)