On the Construction of Lightweight Circulant Involutory MDS Matrices

Yongqiang Li[a,b], Mingsheng Wang[a]

a. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
b. Science and Technology on Communication Security Laboratory, Chengdu, China
yongq.lee@gmail.com
wangmingsheng@iie.ac.cn

Abstract. In the present paper, we investigate the problem of constructing MDS matrices with as few bit XOR operations as possible. The key contribution of the present paper is constructing MDS matrices with entries in the set of $m \times m$ non-singular matrices over $\mathbb{F}_2$ directly, and the linear transformations we used to construct MDS matrices are not assumed pairwise commutative. With this method, it is shown that circulant involutory MDS matrices, which have been proved do not exist over the finite field $\mathbb{F}_{2^m}$, can be constructed by using non-commutative entries. Some constructions of 4×4 and 5×5 circulant involutory MDS matrices are given when $m = 4, 8$. To the best of our knowledge, it is the first time that circulant involutory MDS matrices have been constructed. Furthermore, some lower bounds on XORs that required to evaluate one row of circulant and Hadamard MDS matrices of order 4 are given when $m = 4, 8$. Some constructions achieving the bound are also given, which have fewer XORs than previous constructions.

Keywords: MDS matrix, circulant involutory matrix, Hadamard matrix, lightweight

1 Introduction

Linear diffusion layer is an important component of symmetric cryptography which provides internal dependency for symmetric cryptography algorithms. The performance of a diffusion layer is measured by branch number. Using a diffusion layer with bigger branch number in cryptography provides better resistance to differential and linear attack. As for lightweight cryptography, which is aiming to provide security in a limited resource environment, the cost of implementing an linear diffusion layer is also of importance. With the rapid development of lightweight cryptography, it is of particular interest to investigate the problem of constructing lightweight linear diffusion with bigger branch number.

A linear diffusion layer is a linear transformation over $(\mathbb{F}_2^m)^n$, where m is the bit length of an S-box and n is the number of S-boxes that the linear diffusion layer acts on. Note that every linear transformation can be represented by a matrix, then a linear diffusion layer is often represented by a $n \times n$ matrix and the entries can be viewed as linear transformations over $\mathbb{F}_2^m$. The maximum branch number of a $n \times n$ matrix over $(\mathbb{F}_2^m)^n$ is $n + 1$. A linear diffusion layer with maximum branch number is called a perfect diffusion layers or a Maximal Distance Separable (MDS) matrix. An MDS matrix is a linear multipermutation [22].

A common way to construct MDS matrices is using MDS codes over finite fields. Multiplication with elements in finite fields is a basic operation in the evaluation of a matrix over finite fields. Usually, this operation is heavy in implementation. To improve its implementation efficiency, it is often constructing a matrix with fewer different elements of finite fields and choosing elements of finite fields with lower Hamming weight. Therefore, some matrices can be defined by fewer elements are preferred, such as circulant matrix and Hadamard matrix. The diffusion layer of AES is an typical example of this construction method. It is a 4×4 circulant MDS matrix over $\mathbb{F}_{2^8}$.

Another main method to construct lightweight MDS matrices is recursive construction. The main idea is that firstly constructing a linear transformation which is sparse and compact in implementation, and then composing it several times to get an MDS matrix. This method is first used in the design of Photon lightweight hash family [10] and LED lightweight block cipher [9], and then attracted lots of attentions. The method is extended by using linear transformations instead of multiplications of elements in finite fields in [20]. Then the work is improved by using linear transformations with fewer XORs in [23], where some extreme lightweight MDS matrices are given. A method is given to get rid of expensive symbolic computations of the above method for constructing larger recursive MDS matrices in [1]. The method is also further investigated in [12]. The construction of recursive MDS matrices also has a relation with coding theory. It is shown that recursive MDS matrices can be constructed from Gabidulin codes [4], and also can be obtained directly from shortened MDS cyclic codes [2].

However, a recursive MDS matrix may leads to high latency since it has to run several rounds to get outputs. Then how to construct lightweight MDS matrices without using recursive construction is an interesting problem needs further study. Some works revisit the method of constructing MDS matrices over finite fields by choosing elements whose multiplication's implementation efficiency can be further improved. Recently, it is shown that the choice of the irreducible polynomial used to compute multiplication with elements over finite fields has a great influence of the efficiency [19]. This property is further investigated in [21], where algorithms are designed to search lightweight MDS matrices with few XORs that required to evaluate one row of the corresponding matrix. Several constructions and their comparisons with previous constructions are also given in [21].

Our Contributions. In the present paper, we investigate the problem of constructing MDS matrices with as few bit XOR operations as possible. Note that multiplication with elements of the finite field $\mathbb{F}_{2^m}$ is only a special type of linear transformations over $\mathbb{F}_2^m$. Moreover, there exist many other linear transformations over $\mathbb{F}_2^m$ which can not be represented by multiplication with elements over $\mathbb{F}_{2^m}$. Therefore, constructing matrices over the space of linear transformations over $\mathbb{F}_2^m$ may leads to new constructions of lightweight MDS matrices.

In previous constructions, the entries used to construct MDS matrices are pairwise commutative, such as MDS matrices over finite fields, or assumed pairwise commutative, such as recursive MDS matrices with elements being linear transformations [20,23]. Note that a matrix over a commutative ring is nonsingular if and only if its determinant is a unity in the ring, then the assumption is convenient for charactering MDS matrices since the determinants of square sub-matrices can be computed.

However, the restriction of choosing commutative linear transformations may lose MDS matrices with fewer XORs. Then we do not assume the linear transformations over $\mathbb{F}_2^m$ that used to construct MDS matrices are pairwise commutative in the present paper.

The strategy we used to determine whether a construction is MDS is computing all its square sub-matrices' rank. Then it is too complex to construct MDS matrices with larger order. In symmetric cryptography algorithms, the most often used S-boxes are 4-bit and 8-bit S-boxes, and it is often use diffusion layers of order 4. Therefore, we focus on constructing 4×4 MDS matrices with entries in the space of linear transformations over $\mathbb{F}_2^4$ and $\mathbb{F}_2^8$ in the present paper.

The first result is that circulant involutory MDS matrices can be constructed with our method. Circulant involutory MDS matrices can be implemented efficiently and the same circuit can be used both in encryption and decryption. However, it has been proved in [16,13] that there do not exist circulant involutory MDS matrices over the finite field $\mathbb{F}_{2^m}$. In fact, the proof is only valid when the entries of the matrix are pairwise commute. This property is satisfied by previous construction methods but not our method.

We show that there exist circulant involutory MDS matrices over the space of linear transformations over $\mathbb{F}_2^m$. Some constructions are also given. To the best of our knowledge, it is the first time that circulant involutory MDS matrices have been constructed. For 4×4 circulant involutory MDS matrices constructed in the present paper, the fewest sum of XORs of one row's entries is $m+1, m = 4, 8$. Moreover, we also construct 4×4 orthogonal circulant MDS matrix, which is also proved do not exist over finite fields [13].

Lower bounds on XORs that required to evaluate one row of circulant (noninvolution) MDS matrices, involutory Hadamard MDS matrices and Hadamard (noninvolution) MDS matrices are also investigated. We show that for circulant MDS matrices with the first row's entries are $[I, I, A, B]$, the fewest sum of XORs of A and B is 3. For involutory Hadamard MDS matrices, the fewest sum (the fewest sum we get) of the XORs of entries in the first row is $m + 2$ for $m = 4$ ($m = 8$). For Hadamard MDS matrices, the fewest sum of XORs of one row's entries is 4 for $m = 4$ and the fewest sum we get of XORs of one row's entries is 5 for $m = 8$. Lower bounds on the entries of "optimal" 4×4 MDS matrices is also characterized.

Outline of This Paper. The present paper is organized as follows. In Sect. 2, we give some preliminaries. A general bound on XORs that required to evaluate one row of circulant and Hadamard MDS matrices is also given. In Sect. 3, we investigate the construction of lightweight involutory, non-involutory and orthogonal circulant MDS matrices. In Sect. 4, we investigate the construction of lightweight involutory and non-involutory Hadamard MDS matrices. Comparisons with previous constructions are given at the end of the section. In Sect. 5, we investigate the construction of lightweight "optimal" 4 × 4 MDS matrices. A short conclusion is given in Sect. 6.

2 Preliminaries and a general bound

A map $A : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ is called linear if $A(x + y) = A(x) + A(y)$ for $x, y \in \mathbb{F}_2^m$. Fixed a basis of $\mathbb{F}_2^m$ over $\mathbb{F}_2$, a linear map over $\mathbb{F}_2^m$ can be represented by an $m \times m$ matrix over $\mathbb{F}_2$, which is also denoted by A. Then $A(x) = A \cdot x$, where $x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$ is viewed as a column vector throughout this paper. A linear map is a permutation over $\mathbb{F}_2^m$ if and only if its matrix representation is non-singular. The notation $GL(m, S)$ denotes the set of all $m \times m$ non-singular matrices with entries in S.

For $a, b \in \mathbb{F}_2$, $a + b$ is called the bit XOR operation. For $A \in GL(m, \mathbb{F}_2)$, $\#A$ denotes the number of XOR operations that required to evaluate $A \cdot x$ directly, where $x \in \mathbb{F}_2^m$, and we call A has $\#A$ XOR operations. It is easy to see that $\#A$ equals the number of XORs in $A(x)$ and hence

$$\#A = \sum_{i=1}^{m} (\omega(A[i]) - 1),$$

where $\omega(A[i])$ means the number of nonzero entries in the i-th row of A. For $A \in GL(m, \mathbb{F}_2)$, a simplified representation of A is given by extracting the nonzero positions in each row of A. For example, [2, 3, 4, [1,4]] is the representation of the following matrix

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

and it is a matrix with 1 XOR operation.

Every linear diffusion can be represented by a matrix as follows

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

where $L_{i,j}$ is an $m \times m$ matrix over $\mathbb{F}_2$ for $1 \leq i, j \leq n$. For $X = (x_1, \ldots, x_n) \in (\mathbb{F}_2^m)^n$,

$$L(X) = (\sum_{i=1}^{n} L_{1,i}(x_i), \ldots, \sum_{i=1}^{n} L_{n,i}(x_i)),$$

where $L_{i,j}(x_k) = L_{i,j} \cdot x_k$, for $1 \leq i, j \leq n, 1 \leq k \leq m$. A linear diffusion L defined as above is called involutory if $L \circ L(X) = X$ for all $X \in (\mathbb{F}_2^m)^n$, which is equivalent to that L^2 is the identity matrix of order mn.

For $X = (x_1, \ldots, x_n) \in (\mathbb{F}_2^m)^n$, the bundle weight of X, which is denoted by $\omega_b(X)$, is defined as the number of nonzero entries of X. This means

$$\omega_b(X) = |\{x_i : x_i \neq 0, 1 \leq i \leq n\}|.$$

The branch number of L is defined as

$$\min\{\omega_b(X) + \omega_b(L(X)) \mid X \in (\mathbb{F}_2^m)^n, X \neq 0\}.$$

The upper bound on the branch number of L is $n + 1$, and a matrix achieved the bound is called an MDS matrix.

Square sub-matrices of L of order t means the following matrices

$$L(J, K) = (L_{j_l, k_p}, 1 \leq l, p \leq t)$$

where $J = [j_1, \ldots, j_t]$ and $K = [k_1, \ldots, k_t]$ are two sequence of length t, and $1 \leq j_1 < \ldots < j_t \leq n$, $1 \leq k_1, \ldots, k_t \leq n$. Note that $L(J, K) \cdot (x_1, \ldots, x_t) = 0$ does not have nonzero solutions if and only if $L(J, K)$ is of full rank. Then the following result holds, which is proved in [5].

Theorem 1. *Let $L = (L_{i,j}), 1 \leq i, j \leq n$, and the entries of L are $m \times m$ matrices over $\mathbb{F}_2$. Then L is an MDS matrix if and only if all square sub-matrices of L of order t are of full rank for $1 \leq t \leq n$.*

According to Theorem 1, the computation would be complicated when n is large. Then in the present paper we focus on 4×4 matrices, which are widely used in cryptography. More precisely, we construct lightweight MDS matrices using circulant matrix and Hadamard matrix. Both of them can be defined by the first row's entries and hence can be implemented efficiently.

2.1 A general bound

In this subsection, we give a general bound of XORs on circulant and Hadamard MDS matrices.

A matrix is called circulant if each row is rotated to the right of the preceding row by one entry. Then for a 4×4 circulant matrix, we means

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

where $A, B, C, D \in GL(m, \mathbb{F}_2)$.

A $2^k \times 2^k$ matrix H is called a Hadamard matrix if it can be represented as

$$\begin{pmatrix} H_1, & H_2 \\ H_2, & H_1 \end{pmatrix},$$

where H_1, H_2 are two $2^{k-1} \times 2^{k-1}$ Hadamard matrices. Then for a 4×4 Hadamard matrix, we means

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

where $A, B, C, D \in GL(m, \mathbb{F}_2)$.

Remember that our aim is constructing MDS matrices with as few XOR operations as possible. Then we prefer linear transformations with no XORs. However, the following results limits the amounts of such linear transformations used in our constructions.

Lemma 1. *Let* $L = \begin{pmatrix} L_1, & L_2 \\ L_3, & L_4 \end{pmatrix}$, $L_i \in GL(m, \mathbb{F}_2), 1 \leq i \leq 4$. *If* $\mathrm{rank}(L) = 2m$, *then* $\sum_{i=1}^{4} \#L_i \geq 1$.

Proof. Assume $\#L_i = 0$, $1 \leq i \leq 4$. Then for $1 \leq i \leq 4$, each row and each column of L_i has exactly one entry equals 1 since L_i are non-singular. This means every entry of $\sum_{j=1}^{m} L_i[j]$ equals to 1. Therefore, every entry of $\sum_{i=1}^{2m} L[i]$ equals to 0, which means $\mathrm{rank}(L) < 2m$ and we complete the proof. □

Then we have the following result.

Theorem 2. *1. Let* $L = Circ(A, B, C, D)$ *be a circulant MDS matrix, where* $A, B, C, D \in GL(m, \mathbb{F}_2)$. *Then* $\#A + \#B + \#C + \#D \geq 2$.

2. Let $L = Had(A, B, C, D)$ *be a Hadamard MDS matrix, where* $A, B, C, D \in GL(m, \mathbb{F}_2)$. *Then* $\#A + \#B + \#C + \#D \geq 3$.

Proof. Let $L = Circ(A, B, C, D)$ be a circulant MDS matrix. Assume

$$\#A + \#B + \#C + \#D \leq 1.$$

Then there are at least 3 entries with 0 XORs in the first row. Without loss of generality, we suppose $\#A = \#B = \#C = 0$. Then according to Lemma 1, it holds

$$\mathrm{rank}(L([1, 2], [2, 3])) = \mathrm{rank}(\begin{pmatrix} B & , C \\ A & , B \end{pmatrix}) < 2m.$$

This is a contradiction since L is an MDS matrix. The other cases can be proved similarly.

Let $L = Had(A, B, C, D)$ be a Hadamard MDS matrix. Assume

$$\#A + \#B + \#C + \#D \leq 2.$$

Then there are at least 2 entries with 0 XORs in the first row. Without loss of generality, we suppose $\#A = \#C = 0$. Then according to Lemma 1, it holds

$$\mathrm{rank}(L([1, 3], [1, 3])) = \mathrm{rank}(\begin{pmatrix} A\ , C \\ C\ , A \end{pmatrix}) < 2m.$$

This is a contradiction since L is an MDS matrix. The other cases can be proved similarly. □

The above result means that there are at most two entries with no XORs in one row of a circulant MDS matrix, and there are at most one entry with no XORs in one row of a Hadamard MDS matrix. We suppose $L[1, 1] = I$ in our constructions, where I denotes the identity matrix throughout this paper.

3 Lightweight circulant MDS matrices

In this section, we investigate the construction of lightweight circulant involutory, non-involutory and orthogonal MDS matrices respectively.

3.1 Constructing circulant involutory MDS matrices

First, we have the following result.

Lemma 2. *Let $L = Circ(I, A, B, C)$ be a circulant matrix, where $A, B, C \in GL(m, \mathbb{F}_2)$. Then L is an involution if and only if the following equalities hold:*

$$AB = BA, BC = CB, A^2 = C^2, AC + CA = B^2.$$

Proof. By matrix multiplication, it can be checked that

$$\begin{aligned} L^2 &= Circ(I, A, B, C) \cdot Circ(I, A, B, C) \\ &= Circ(I + AC + CA + B^2, BC + CB, A^2 + C^2, AB + BA). \end{aligned}$$

On the other hand, L is an involution if and only if $L^2 = Circ(I, 0, 0, 0)$. Therefore, L is an involution if and only if

$$AB = BA, BC = CB, A^2 = C^2, AC + CA = B^2$$

hold simultaneously. □

We give a general construction of circulant involutory matrix in the following result. For $A \in GL(m, \mathbb{F}_2)$, the multiplication order of A is defined as the minimum positive integer d such that $A^d = I$.

Lemma 3. *Suppose $A, C \in GL(m, \mathbb{F}_2)$ with $A^2 = C^2 = I$, and the multiplication order of $A+C$ equals $4k-2$ for some integer k with $k > 1$. Let $B = (A+C)^{2k}$. Then the matrix $Circ(I, A, B, C)$ is an involution.*

Proof. Let $B = (A+C)^{2k}$. Note that

$$A^2 = C^2 = I,$$

then according to Lemma 2, we only need to prove that A, B, C satisfy the following equalities

$$AB = BA, BC = CB, AC + CA = B^2.$$

First, it is easy to see that

$$(A+C)^2 = A^2 + AC + CA + C^2 = AC + CA.$$

Then we have

$$B = (A+C)^{2k} = (AC + CA)^k.$$

Therefore,

$$\begin{aligned} AB &= A(AC+CA)^k \\ &= A(AC+CA)(AC+CA)^{k-1} \\ &= (A^2C + ACA)(AC+CA)^{k-1} \\ &= (CA^2 + ACA)(AC+CA)^{k-1} \\ &= (CA + AC)A(AC+CA)^{k-1} \\ &= \cdots \\ &= (AC+CA)^k A \\ &= BA. \end{aligned}$$

Similarly, it can be checked that

$$BC = CB.$$

Note that $(A+C)^{4k-2} = I$, then we have

$$B^2 = (A+C)^{4k} = (A+C)^2 = AC + CA.$$

According to Lemma 2, we have $Circ(I, A, (A+C)^{2k}, C)$ is an involution. □

Remark 1. If $k = 1$, then the multiplication order of $A+C$ equals 2 and $B = (A+C)^2 = I$. In this case, $L = Circ(I, A, I, C)$ constructed as above is also a circulant involution. However, it is not an MDS matrix since $\text{rank}(L([1,3],[1,3])) < 2m$. Then we always suppose $k > 1$ since we want to construct circulant involutory MDS matrices.

Using above results, our searching strategy is as follows. Firstly, we get the set S which contains all involutory matrix from the set which we want to search. Then for each pair of $(A, C) \in S \times S$, we compute the multiplication order

d of $A+C$. If $d \bmod 4 = 2$, then let $B = (A+C)^{\frac{d}{2}+1}$, and test whether $Circ(I,A,B,C)$ is MDS by Theorem 1.

When $m=4$, we search A,C over $GL(4,\mathbb{F}_2)$. There exist A,C such that $Circ(I,A,B,C)$ is MDS. The fewest sum of XORs of one rows' entries of an MDS involutory $Circ(I,A,B,C)$ constructed as above is 5. There are 48 pairs of A,C with this property. These 48 matrices are of the type $Circ(I,A,B,C)$ and $Circ(I,C,B,A)$ for 24 different pairs of A,C.

When $m=8$, we search A,C over all 8×8 non-singular matrices over $\mathbb{F}_2$ with less than or equal to 3 bit XOR operations. The fewest sum of XORs of one rows' entries of an MDS $Circ(I,A,B,C)$ constructed as above is 9. There are 40320 pairs of A,C satisfy this property. For all these pairs of A,C, $Circ(I,C,B,A)$ are also circulant involutory MDS matrices.

Theorem 3. *Their exist $A,B,C \in GL(m,\mathbb{F}_2)$, $m=4,8$, such that $Circ(I,A,B,C)$ is an involutory MDS matrix. Furthermore, the following statements hold.*

1. *When $m=4$, circulant involutory MDS matrices constructed with the above method satisfy $\#A+\#B+\#C \geq 5$.*
2. *When $m=8$, if $\#A \leq 3$ and $\#C \leq 3$, then circulant involutory MDS matrices constructed with the above method satisfy $\#A+\#B+\#C \geq 9$.*

Example 1. Examples of A,B,C such that $Circ(I,A,B,C)$ are circulant involutory MDS matrices with $\#A+\#B+\#C = m+1$.[1]

(1) $m=4$, $A=[1,2,[1,3],[1,2,4]]$, $C=[4,3,2,1]$, $B=(A+C)^4=[2,[1,2],[3,4],3]$.
(2) $m=8$, $A=[1,2,[1,3],[1,2,4],6,5,8,7]$, $C=[5,8,[2,6],7,1,[3,8],4,2]$, and $B=(A+C)^{16}=[[7,8],1,7,[3,8],[2,4],[1,4],6,5]$.

We further investigate the construction of 5×5 circulant involutory MDS matrices. In order to simplify our characterization, we investigate 5×5 circulant matrices of the type $Circ(I,A,B,B,A)$, where $A,B \in GL(m,\mathbb{F}_2)$. Concerning the property of involutory of $Circ(I,A,B,B,C)$, it is easy to prove the following result.

Lemma 4. *Let $L = Circ(I,A,B,B,A)$ be a circulant matrix, where $A,B \in GL(m,\mathbb{F}_2)$. Then L is an involution if and only if $A^2 = AB+BA = B^2$.*

We give constructions by exhaustive searching for A,B with the following method. The method is often used hereafter in the paper, and we give a detailed general description here.

The following result is helpful. It can be proved via elementary linear algebra and we omit the proof here.

Lemma 5. *Suppose $A,B,C \in GL(m,\mathbb{F}_2)$ are $m\times m$ non-singular matrices over $\mathbb{F}_2$. Then the following statements hold.*

[1] More examples of circulant involutory MDS matrices with $\#A+\#B+\#C=m+1$ are given in the appendix of the extended version of the paper [14].

(1) $\begin{pmatrix} I, & A \\ B, & C \end{pmatrix}$ *is of full rank if and only if* $\mathrm{rank}(BA + C) = m$*.*

(2) $\begin{pmatrix} A, & I \\ B, & C \end{pmatrix}$ *is of full rank if and only if* $\mathrm{rank}(CA + B) = m$*.*

(3) $\begin{pmatrix} A, & B \\ I, & C \end{pmatrix}$ *is of full rank if and only if* $\mathrm{rank}(AC + B) = m$*.*

(4) $\begin{pmatrix} A, & B \\ C, & I \end{pmatrix}$ *is of full rank if and only if* $\mathrm{rank}(BC + A) = m$*.*

Let $L = Circ(I, A, B, B, A)$. According to Theorem 1, if L is MDS, then all its square sub-matrices are of full rank. According to Lemma 5, we have the following fact by investigating all square sub-matrices of order 2. If L is MDS, then the following matrices are non-singular:

$$A + I, A^2 + I, B + I, B^2 + I, A^2 + B, A + B^2, A + B.$$

Note that $A^2 + I$ is non-singular if and only if $A + I$ is non-singular. Then the conditions can be simplified as the following matrices are non-singular:

$$A + I, B + I, A + B^2, A^2 + B, A + B.$$

Based on the above observations, we have the following searching strategy. First, note that both A and B should satisfy $\mathrm{rank}(X + I) = m, X = A, B$. The equalities that both A and B satisfied are called general rules. Then we can select the candidate set of A and B from the set we want to search over by using general rules, which means

$$S_{A,B} := \{X : X \in S_{search} \mid \mathrm{rank}(X + I) = m\}.$$

The for $A \in S_{A,B}$, we can get the candidate set of B by using the other conditions that should be satisfied, which means

$$\begin{aligned} S_B := \{B : B \in S_{A,B} \mid & \mathrm{rank}(A + B) = m \wedge \mathrm{rank}(A^2 + B) = m \wedge \mathrm{rank}(A + B^2) = m \\ & \wedge A^2 = AB + BA \wedge A^2 = B^2\}. \end{aligned}$$

At last, for $B \in S_B$, we test whether L is MDS by Theorem 1.

When $m = 4$, we search A, B over $GL(4, \mathbb{F}_2)$. The fewest XORs of one row's entries of an involutory MDS $Circ(I, A, B, B, A)$ is 4. There are 24 pairs of A, B such that $Circ(I, A, B, B, A)$ are involutory circulant MDS matrices with $\#A + \#B = 2$. These 24 MDS matrices are of the type $Circ(I, A, A^T, A^T, A)$ and $Circ(I, A^T, A, A, A^T)$ for 12 different A.

When $m = 8$, we search A, B over $GL(8, \mathbb{F}_2)$ with $\#A + \#B \leq 3$. No involutory MDS matrix returns. Therefore, if $Circ(I, A, B, B, A)$ is an involutory MDS matrix, then $\#A + \#B \geq 4$.

Then we have the following result.

Theorem 4. *Their exist* $A, B \in GL(m, \mathbb{F}_2)$*,* $m = 4, 8$*, such that* $Circ(I, A, B, B, A)$ *is an* 5×5 *involutory MDS matrix. Furthermore, if* $Circ(I, A, B, B, A)$ *is an involutory MDS matrix, then* $\#A + \#B \geq \frac{m}{2}$*.*

Similar as the method "Subfield construction" that used in [6,19,21], it is easy to construct involutory MDS $Circ(I, A, B, B, A)$ over $\mathbb{F}_2^8$ with $\#A + \#B = 4$, since we have constructed involutory MDS $Circ(I, A, B, B, A)$ over $\mathbb{F}_2^4$ with $\#A + \#B = 2$. Let $X \in GL(4, \mathbb{F}_2)$, $\#X = 1$ and $Circ(I, X, X^T, X^T, X)$ is an involutory MDS matrix. Then $Circ(I, A, A^T, A^T, A)$ is also an involutory MDS matrix, where $A \in GL(8, \mathbb{F}_2)$ of the following form

$$A = \begin{bmatrix} X, & 0 \\ 0, & X \end{bmatrix}.$$

Then we can construct 24 circulant involutory MDS by using the above method and the searching result when $m = 4$.

In order to get more circulant involutory MDS matrices, we searching A over $GL(8, \mathbb{F}_2)$ with $\#A = 2$. We get 20160 A such that $Circ(I, A, A^T, A^T, A)$ are involutory MDS matrices and $\#A + \#A^T = 4$.

Example 2. Examples of A, B such that $Circ(I, A, B, B, A)$ are circulant involutory MDS matrices with $\#A + \#B = \frac{m}{2}$.

(1) $m = 4$, $A = [2, 3, 4, [1, 3]]$, $B = A^T = [4, 1, [2, 4], 3]$.

(2) $m = 8$, $X = [2, 3, 4, [1, 3]]$, $A = \begin{bmatrix} X, & 0 \\ 0, & X \end{bmatrix} = [2, 3, 4, [1, 3], 6, 7, 8, [5, 7]]$, $B = A^T = [4, 1, [2, 4], 3, 8, 5, [6, 8], 7]$.

(3) $m = 8$, $A = [[3, 5], 8, 1, 3, 4, 2, 6, [2, 7]]$, $B = A^T = [3, [6, 8], [1, 4], 5, 1, 7, 8, 2]$.

It is interesting that 5 × 5 circulant involutory MDS matrices can be constructed with only 3 different entries. We have tried some other methods to construct circulant involutory MDS matrices with higher order. However, we do not get an circulant involutory MDS matrix with order large than or equal to 6 until present. We leave it as an open problem.

Problem 1. Construct $n \times n$ circulant involutory MDS matrices over $GL(m, \mathbb{F}_2)$ or prove that they do not exist, where $n \geq 6$, $m = 4, 8$.

3.2 Constructing circulant non-involutory MDS matrices

In this subsection, we want to construct non-involutory MDS matrices with as few XORs as possible. We consider circulant matrices of the type

$$Circ(I, I, A, B),$$

since it has the most many entries with no XORs in one row.

The searching strategy is similar as previous subsection. If $Circ(I, I, A, B)$ is MDS, then the following matrices are non-singular:

$$A + I, B + I, A + B, AB + I, A^2 + B, A + B^2.$$

When $m = 4$, we search A, B over $GL(4, \mathbb{F}_2)$. The fewest XORs of one row's entries of an MDS $Circ(I, I, A, B)$ is 3. Their are 48 pair of (A, B) such that

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

When $m = 8$, we search A, B over all 8×8 non-singular matrices over $\mathbb{F}_2$ with 1 bit XOR. No MDS matrix returns. This means if $Circ(I, I, A, B)$ is an MDS matrix over $GL(8, \mathbb{F}_2)$, then either A or B has at least 2 XORs, and hence $\#A + \#B \geq 3$. Therefore, the following result hold.

Theorem 5. *Let $L = Circ(I, I, A, B)$, where $A, B \in GL(m, \mathbb{F}_2)$, $m = 4, 8$. If L is an MDS matrix, then $\#A + \#B \geq 3$.*

In order to get circulant MDS matrix with the above equality holds when $m = 8$, we let $B = A^{-2}$ and search A over all 8×8 non-singular matrices over $\mathbb{F}_2$ with 1 bit XOR. At last, we get 80640 A such that $Circ(I, I, A, A^{-2})$ are MDS matrices with $\#A + \#A^{-2} = 3$. Furthermore, $Circ(I, I, A^{-2}, A)$ are also MDS matrices for all these A.

Example 3. Examples of A, B such that $Circ(I, I, A, B)$ and $Circ(I, I, B, A)$ are MDS matrices with $\#A + \#B = 3$.

(1) $m = 4$, $A = [2, 3, 4, [1, 4]]$, $B = A^{-2} = [[2, 3], [3, 4], 1, 2]$.
(2) $m = 8$, $A = [2, 3, 4, 5, 6, 7, 8, [1, 3]]$, $B = A^{-2} = [[1, 7], [2, 8], 1, 2, 3, 4, 5, 6]$.

3.3 Constructing circulant orthogonal MDS matrices

A square matrix L is called orthogonal if $L^{-1} = L^T$, where L^T is the transpose of L. It is proven in [13] there do not exist $2^d \times 2^d$ circulant orthogonal MDS matrix over finite fields. In this subsection, we show that 4×4 circulant orthogonal MDS matrices can also be constructed with non-commutative entries.

Firstly, note that for $L = Circ(I, A, B, C)$, where $A, B, C \in \mathbb{F}_{2^m}$, it holds $L^T = Circ(I, C^T, B^T, A^T)$. This means one have to implement new entries A^T, B^T, C^T in decryption circuit when L is orthogonal. In order to simplify implementation, we let $A, B, C \in GL(m, \mathbb{F}_2)$ are symmetric matrices, which means $A = A^T, B = B^T, C = C^T$. Then it holds

$$L^T = Circ(I, C^T, B^T, A^T) = Circ(I, C, B, A),$$

and it is easy to prove the following result.

Lemma 6. *Let $L = Circ(I, A, B, C)$ be a circulant matrix, where $A, B, C \in GL(m, \mathbb{F}_2)$ are symmetric matrices. Then L is orthogonal if and only if the following equalities hold:*

$$A^2 + B^2 = C^2, AC = CA, A + C = BA + CB, A + C = AB + BC.$$

If $L = Circ(I, A, B, C)$ is MDS, then the following matrices are non-singular:

$$B + I, B + A^2, B + C^2, AC + I, AB + C.$$

When $m = 4$, we search symmetric A, B, C over $GL(4, \mathbb{F}_2)$. The fewest XORs of one row's entries of an orthogonal MDS $Circ(I, A, B, C)$ is 8. Their are 24 triples of A, B, C such that $Circ(I, A, B, C)$ are orthogonal MDS matrices with $\#A + \#B + \#C = 8$. Then we have the following result.

Theorem 6. *There exist symmetric $A, B, C \in GL(4, \mathbb{F}_2)$ such that $Circ(I, A, B, C)$ is an orthogonal MDS matrix. Furthermore, if $Circ(I, A, B, C)$ is an orthogonal MDS matrix, then $\#A + \#B + \#C \geq 8$.*

Example 4. Example of A, B, C such that $Circ(I, A, B, C)$ is an orthogonal circulant MDS matrix $\#A + \#B + \#C = 2m$.

(1) $m = 4$, $A = [1, 2, 4, [3, 4]]$, $B = [[1, 4], [2, 3, 4], [2, 3], [1, 2, 4]]$, $C = [2, [1, 2], 3, 4]$.

(2) $m = 8$, $A = \begin{bmatrix} A_1, & 0 \\ 0, & A_1 \end{bmatrix}$, $B = \begin{bmatrix} B_1, & 0 \\ 0, & B_1 \end{bmatrix}$, $C = \begin{bmatrix} C_1, & 0 \\ 0, & C_1 \end{bmatrix}$, where A_1, B_1, C_1 are the A, B, C in the above item.

4 Lightweight Hadamard MDS matrices

In this section, we investigate the construction of lightweight Hadamard involutory and non-involutory MDS matrices respectively.

4.1 Constructing Hadamard involutory MDS matrices

In the case of a, b, c are elements of finite fields, $Had(1, a, b, c)$ is an involution if and only if $a^2 + b^2 = c^2$. In the case of $A, B, C \in GL(m, \mathbb{F}_2)$, we have the following result.

Lemma 7. *Let $A, B, C \in GL(m, \mathbb{F}_2)$. Then $L = Had(I, A, B, C)$ is an involution if and only if A, B, C are pairwise commutative and $A^2 + B^2 = C^2$.*

Proof. By matrix multiplication, it can be checked that

$$\begin{aligned} L^2 &= Had(I, A, B, C) \cdot Had(I, A, B, C) \\ &= Had(I + A^2 + B^2 + C^2, BC + CB, AC + CA, AB + BA). \end{aligned}$$

Therefore, L is an involution if and only if $L^2 = Had(I, 0, 0, 0)$, which is equivalent to

$$AB = BA, BC = CB, AC = CA, A^2 + B^2 = C^2$$

hold simultaneously. □

When $m = 4$, we search A, B, C over $GL(4, \mathbb{F}_2)$ as previous. The fewest XORs of one row's entries of an involutory MDS $Had(I, A, B, C)$ is 6. There are 144 triples of A, B, C such that $Had(I, A, B, C)$ are involutory MDS matrices with $\#A + \#B + \#C = 6$. These 144 matrices are of the type $Had(I, A_1, A_2, A_3)$, where (A_1, A_2, A_3) is a permutation of $(A, A^{-1}, A + A^{-1})$ for 24 different A.

When $m = 8$, we also consider Hadamard matrix of the type

$$L = Had(I, A, A^{-1}, A + A^{-1}),$$

where $A \in GL(m, \mathbb{F}_2)$. According to the above lemma, L is an involution. We use the method in [20,23] to characterize whether L is MDS. By computing the determinants of all the square sub-matrices of L and factorizing these polynomials, we get that L is an MDS matrix if and only if all the following matrices are non-singular:

$$A, A+I, A^2+A+I, A^3+A+I, A^3+A^2+I.$$

Then we search A over $GL(8, \mathbb{F}_2)$ with $\#A \leq 3$. The fewest XORs of one row's entries of an involutory MDS $Had(I, A, A^{-1}, A+A^{-1})$ is 10. We get 80640 A such that $Had(I, A, A^{-1}, A+A^{-1})$ are involutory MDS matrices with $\#A + \#A^{-1} + \#(A+A^{-1}) = 10$.

We also have searched some other types of Hadamard matrices. However, we do not get a Hadamard involutory matrix with one row's XORs less then 10 until present.

Theorem 7. *1. Let $A, B, C \in GL(4, \mathbb{F}_2)$. If $L = Had(I, A, B, C)$ is an MDS involution matrix, then $\#A + \#B + \#C \geq 6$.*

2. Let $A \in GL(8, \mathbb{F}_2)$ with $\#A \leq 3$. If $L = Had(I, A, A^{-1}, A+A^{-1})$ is an MDS involution matrix, then $\#A + \#A^{-1} + \#(A+A^{-1}) \geq 10$.

Example 5. Examples of A, B, C such that $Had(I, A, B, C)$ are involutory MDS matrices with $\#A + \#B + \#C = m + 2$.

(1) $m = 4$, $A = [2, [1, 3], 4, [2, 3]]$, $B = A^{-1} = [[1, 2, 4], 1, [1, 4], 3]$, $C = A+A^{-1} = [[1, 4], 3, 1, 2]$.

(2) $m = 8$, $A = [2, 3, 4, 5, 6, 7, 8, [1, 3]]$, $B = A^{-1} = [[2, 8], 1, 2, 3, 4, 5, 6, 7]$, $C = A + A^{-1} = [8, [1, 3], [2, 4], [3, 5], [4, 6], [5, 7], [6, 8], [1, 3, 7]]$.

4.2 Constructing non-involutory Hadamard MDS matrices

In this subsection, we want to construct non-involutory Hadamard MDS matrix with as few XORs as possible. The searching strategy is similar as previous. If $Had(I, A, B, C)$ is MDS, then the following matrices are non-singular:

$$A+I, B+I, C+I, AB+C, AC+B, BA+C, BC+A, CB+A, CA+B.$$

When $m = 4$, we search A, B, C over $GL(4, \mathbb{F}_2)$. The fewest XORs of one rows' entries of an MDS $Had(I, A, B, C)$ is 4. There are 72 triples of A, B, C such that $Had(I, A, B, C)$ are MDS matrices with $\#A + \#B + \#C = 4$. These 72 matrices are of the type $Had(I, A_1, A_2, A_3)$, where (A_1, A_2, A_3) is a permutation of $(A, A^T, A+A^T)$ for 12 different A.

When $m = 8$, we search A over $GL(8, \mathbb{F}_2)$ with $\#A \leq 2$. The fewest XORs of one rows' entries of an MDS $Had(I, A, A^T, A+A^T)$ is 8.

In order to get Hadamard MDS matrices with fewer XORs in one row, we investigate Hadamard matrices of the type $Had(I, A, A^T, B)$. According to our searching, if $\#A \leq 1$ and $\#B \leq 2$, then there are no MDS $Had(I, A, A^T, B)$. Then we have the following result.

Theorem 8. *1. Let $A, B, C \in GL(4, \mathbb{F}_2)$. If $L = Had(I, A, B, C)$ is an MDS matrix, then $\#A + \#B + \#C \geq 4$.*

matrix type	elements	the first row	XOR count	Ref.
Circulant	$GL(8, \mathbb{F}_2)$	$[I, I, A, B]$	$3 + 3 \times 8 = 27$	Subsection 3.2
Circulant	$\mathbb{F}_{2^8}$/0x11b	(0x02, 0x03, 0x01, 0x01)	$14 + 3 \times 8 = 38$	AES [8]
Hadamard	$GL(8, \mathbb{F}_2)$	$[I, A, A^T, B]$	$5 + 3 \times 8 = 29$	Subsection 4.2
Hadamard	$\mathbb{F}_{2^8}$/0x1c3	(0x01, 0x02, 0x04, 0x91)	$13 + 3 \times 8 = 37$	[21]
Subfield-Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x2, 0x8, 0x9)	$2 \times (5 + 3 \times 4) = 34$	[21]

Table 1. Comparisons with previous constructions of non-involutory MDS matrices

matrix type	elements	the first row	XOR count	Ref.
Circulant	$GL(8, \mathbb{F}2)$	$[I, A, B, C]$	$9 + 3 \times 8 = 33$	Subsection 3.1
Hadamard	$GL(8, \mathbb{F}2)$	$[I, A, A^{-1}, A + A^{-1}]$	$10 + 3 \times 8 = 34$	Subsection 4.1
Subfield-Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x4, 0x9, 0xd)	$2 \times (6 + 3 \times 4) = 36$	[21]
Hadamard	$\mathbb{F}_{2^8}$/0x165	(0x01, 0x02, 0xb0, 0xb2)	$16 + 3 \times 8 = 40$	[21]
Hadamard	$\mathbb{F}_{2^8}$/0x11d	(0x01, 0x02, 0x04, 0x06)	$22 + 3 \times 8 = 46$	[3]
Compact Cauchy	$\mathbb{F}_{2^8}$/0x11b	(0x01, 0x12, 0x04, 0x16)	$54 + 3 \times 8 = 78$	[7]
Hadamard-Cauchy	$\mathbb{F}_{2^8}$/0x11b	(0x01, 0x02, 0xfc, 0xfe)	$74 + 3 \times 8 = 98$	[11]

Table 2. Comparisons with previous constructions of involutory MDS matrices

2. *Let $A, B \in GL(8, \mathbb{F}_2)$. If $L = Had(I, A, A^T, B)$ is an MDS matrix, then $\#A + \#A^T + \#B \geq 5$.*

In order to get MDS $Had(I, A, A^T, B)$ with $\#A + \#A^T + \#B = 5$, we choose A with $\#A = 2$ and $\text{rank}(A + I) = 8$ randomly, and then test whether there exist B with $\#B = 1$ such that $Had(I, A, A^T, B)$ is MDS. We repeat the process several times and get 622 pairs of $A, B \in GL(8, \mathbb{F}_2)$, such that $Had(I, A, A^T, B)$ is MDS and $\#A + \#A^T + \#B = 5$.

Example 6. Examples of A, B, C such that $Had(I, A, B, C)$ are MDS matrices with the bounds in the above theorem hold.

(1) $m = 4$, $A = [2, 3, 4, [1, 3]]$, $B = A^T = [4, 1, [2, 4], 3]$, $C = A + A^T = [[2, 4], [1, 3], 2, 1]$.
(2) $m = 8$, $A = [2, 3, 4, [1, 5], 8, 7, 5, [3, 6]]$, $B = A^T = [4, 1, [2, 8], 3, [4, 7], 8, 6, 5]$, $C = [[4, 7], 6, 5, 8, 7, 1, 2, 3]$.

We give comparisons of our constructions with previous constructions in Table 1, Table 2 and Table 3 respectively.

The lower bounds on XORs of circulant and Hadamard MDS matrices given in Section 3 and Section 4 are under the supposition $L[1, 1] = I$. Therefore, it is possible to improve the previous lower bounds when $L[1, 1] \neq I$. However, we have the following result with searching, which shows that the lower bounds can not be improved when $m = 4$.

matrix type	elements	the first row	XOR count	Ref.
Circulant	$GL(4,\mathbb{F}2)$	$[I, I, A, B]$	$3+3\times 4=15$	Subsection 3.2
Involutory circulant	$GL(4,\mathbb{F}2)$	$[I, A, B, C]$	$5+3\times 4=17$	Subsection 3.1
Hadamard	$GL(4,\mathbb{F}2)$	$[I, A, B, C]$	$4+3\times 4=16$	Subsection 4.2
Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x2, 0x8, 0x9)	$5+3\times 4=17$	[21]
Involutory Hadamard	$GL(4,\mathbb{F}2)$	$[I, A, A^{-1}, A+A^{-1}]$	$6+3\times 4=18$	Subsection 4.1
Involutory Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x4, 0x9, 0xd)	$6+3\times 4=18$	[21,15]
Involutory Hadamard	$\mathbb{F}_{2^4}$/0x19	(0x1, 0x2, 0x6, 0x4)	$6+3\times 4=18$	[18]

Table 3. Comparisons of MDS matrices over $\mathbb{F}_2^4$ and $\mathbb{F}_{2^4}$

Theorem 9. *Let $A_i \in GL(4, \mathbb{F}_2)$, and $\mathcal{A} = \sum_{i=1}^{4} \# A_i$. Then the following statements hold.*

1. *If $Circ(A_1, A_2, A_3, A_4)$ is a circulant MDS matrix, then $\mathcal{A} \geq 3$.*
2. *If $Circ(A_1, A_2, A_3, A_4)$ is a circulant involutory MDS matrix, then $\mathcal{A} \geq 5$.*
3. *If $Had(A_1, A_2, A_3, A_4)$ is a Hadamard MDS matrix, then $\mathcal{A} \geq 4$.*
4. *If $Had(A_1, A_2, A_3, A_4)$ is a Hadamard involutory MDS matrix, then $\mathcal{A} \geq 6$.*

5 Lightweight “Optimal” 4×4 MDS matrices

It is proven in [17] that the highest possible number of 1 and the lowest possible number of different entries for a 4×4 MDS matrix over finite fields are 9 and 3 respectively. The matrix with the two properties hold simultaneously are called “optimal” in their presentation slides. The following matrix

$$\begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 1 & b & a \\ 1 & a & 1 & b \\ 1 & b & a & 1 \end{pmatrix}$$

is an example of “optimal” matrix which is given in [17]. Similarly as above, we investigate the following special matrix,

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

where $A, B \in GL(m, \mathbb{F}_2)$ are $m \times m$ non-singular matrices over $\mathbb{F}_2$.

If L is MDS, then the following matrices are non-singular:

$$A + I, B + I, A + B, A + B^2, A^2 + B, AB + I.$$

When $m = 4$, we search A, B over $GL(4, \mathbb{F}_2)$, which is the set of all 4×4 non-singular matrices over $\mathbb{F}_2$. The fewest XORs of "optimal" MDS matrices is 13. There are 24 pairs of $A, B \in GL(m, \mathbb{F}_2)$ such that the corresponding constructions are MDS matrices with $4\#A + 3\#B = 13$. All these pairs satisfy $B = A^{-2}$.

When $m = 8$, we search A, B over the set of all 8×8 non-singular matrices over $\mathbb{F}_2$ with 1 bit XOR operation. No MDS matrix returns. This means if L is a "optimal" MDS matrix over $GL(8, \mathbb{F}_2)$, then either A or B has at least 2 XORs, and hence $\#L \geq 10$.

Then we have the following result.

Theorem 10. *Let L be a matrix constructed as above, where $A, B \in GL(m, \mathbb{F}_2)$, $m = 4, 8$. If L is an MDS matrix, then*

$$4\#A + 3\#B \geq \begin{cases} 13, & m = 4; \\ 10, & m = 8. \end{cases}$$

In order to get "optimal" matrices over $GL(8, \mathbb{F}_2)$ with 10 XORs, we let $B = A^{-2}$ and search A over all 8×8 non-singular matrices over $\mathbb{F}_2$ with 1 bit XOR operation. We get 40320 $A \in GL(8, \mathbb{F}_2)$ such that the corresponding constructions are "optimal" MDS matrices with 10 XORs.

It is interesting that "optimal" 4×4 MDS matrices over $GL(8, \mathbb{F}_2)$ has fewer XORs than "optimal" 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$.

Example 7. Examples of A, B such that L are "optimal" MDS matrices with the bounds in the above result hold.

(1) Let $A = [[2, 3], 4, 2, 1]$, $B = A^{-2} = [2, [1, 3], [1, 3, 4], 3]$. Then L constructed as above is an MDS matrix with $4\#A + 3\#B = 13$.
(2) Let $A = [4, 5, 6, 8, 3, [4, 7], 1, 2]$, $B = A^{-2} = [[1, 6], 4, 2, 7, 8, 5, [3, 7], 1]$. Then L constructed as above is an MDS matrix with $4\#A + 3\#B = 10$.

6 Conclusion

In the present paper, we mainly investigate the construction of 4×4 lightweight MDS matrices with entries in the set of $m \times m$ non-singular matrices over $\mathbb{F}_2$. With this method, circulant, Hadamard and involutory Hadamard MDS matrices with fewer XORs than previous constructions are given. Moreover, circulant involutory MDS matrices are also constructed with our method. Constructing lightweight MDS matrices of large order with the method of the present paper is an interesting problem need further study.

Acknowledgements

The authors are very grateful to the anonymous reviewers for their valuable comments. This work was supported by the 973 project under Grant (2013CB834203), by the National Science Foundation of China (No.61303255, No.61379142).

References

1. Augot, D., Finiasz, M.: Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, pages 1551-1555. IEEE, 2013.
2. Augot, D., Finiasz, M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS 8540, pp. 3-17, 2015.
3. Barreto, P., Rijmen, V.: The Anubis Block Cipher. Submission to the NESSIE Project, 2000.
4. Berger, T.P.: Construction of Recursive MDS Diffusion Layers from Gabidulin Codes. In INDOCRYPT, LNCS 8250, pages 274-285. 2013.
5. Blaum, M., Roth, R.M.: On Lowest Density MDS Codes. IEEE Transactions on Information Theory 45(1), 46-59 (1999)
6. Choy, J., Yap, H., Khoo, K., Guo, J., Peyrin, T., Poschmann, A., Tan, C.H.: SPN-Hash: Improving the Provable Resistance against Differential Collision Attacks. In: AFRICACRYPT. (2012) 270-286
7. Cui, T., Jin, C.i, Kong, Z.: On compact cauchy matrices for substitution permutation networks. IEEE Transactions on Computers, 99(PrePrints):1, 2014.
8. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, 2002.
9. 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)
10. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222-239. Springer,Heidelberg (2011)
11. Gupta, K. C., Ray, I. G.: On Constructions of Involutory MDS Matrices. In AFRICACRYPT, pages 43-60, 2013.
12. Gupta, K. C., Ray, I. G.: On constructions of MDS matrices from companion matrices for lightweight cryptography. In: Cuzzocrea, A., Kittl, C., Simos, D.E., Weippl, E., Xu, L. (eds.) CD-ARES Workshops 2013. LNCS, vol. 8128, pp. 29-43. Springer, Heidelberg (2013)
13. Gupta, K. C., Ray, I. G.: Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. Cryptogr. Commun. (2015) 7:257-287
14. Li, Y., Wang, M.: On the construction of lightweight circulant involutory MDS matrices (Extend version). FSE 2016. http://eprint.iacr.org/2016/406.
15. Jean J., Nikolić I., Peyrin T.: Joltik v1.1, 2014. Submission to the CAESAR competition, http://www1.spms.ntu.edu.sg/ syllab/Joltik.
16. Jorge Nakahara Jr. and lcio Abraho. A new involutory mds matrix for the AES. I. J. Network Security, 9(2):109-116, 2009.
17. Junod, P., Vaudenay, S.: Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 84-99. Springer, Heidelberg (2004)
18. Kavun E. B., Lauridsen M. M., Leander G., Rechberger C., Schwabe P., Yalcn T.: Prøst v1.1, 2014. Submission to the CAESAR competition, http://competitions.cr.yp.to/round1/proestv11.pdf.

19. Khoo, K., Peyrin, T., Poschmann, A., Yap, H.: FOAM: Searching for Hardware Optimal SPN Structures and Components with a Fair Comparison. In Cryptographic Hardware and Embedded Systems CHES 2014, volume 8731 of Lecture Notes in Computer Science, pages 433-450. Springer Berlin Heidelberg, 2014.
20. 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. 385-401. Springer, Heidelberg (2012)
21. Sim, S.M., Khoo, K., Oggier, F., Peyrin, T.: Lightweight MDS Involution Matrices. In: Leander, G., Demirci, H. (eds.) FSE 2015. LNCS, Springer (2015)
22. Vaudenay, S.: On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER. In: 2nd International Workshop on Fast Software Encryption. Springer-Verlag, pp.286–297 (1994)
23. Wu, S., Wang, M., Wu, W.: Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions. In: L.R. Knudsen and H. Wu (Eds.): SAC 2012, LNCS 7707, pp. 355-371, 2013.