World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:6, 2017

On the Construction of Lightweight Circulant Maximum Distance Separable Matrices

Qinyi Mei, Li-Ping Wang

Abstract—MDS matrices are of great significance in the design of block ciphers and hash functions. In the present paper, we investigate the problem of constructing MDS matrices which are both lightweight and low-latency. We propose a new method of constructing lightweight MDS matrices using circulant matrices which can be implemented efficiently in hardware. Furthermore, we provide circulant MDS matrices with as few bit XOR operations as possible for the classical dimensions 4×4, 8×8 over the space of linear transformations over finite field $\mathbb{F}_2^4$. In contrast to previous constructions of MDS matrices, our constructions have achieved fewer XORs.

Keywords—Linear diffusion layer, circulant matrix, lightweight, MDS matrix.

I. Introduction

LINEAR diffusion layer is widely used in many symmetric key primitives such as block ciphers and hash functions [10], [12]. Branch number is a measure of its performance. A block cipher using a diffusion layer with bigger branch number provides better resistance to differential and linear attack, which are two well-known attacks on block ciphers. On the other hand, the cost of implementing a diffusion layer is also of importance in lightweight cryptography. Consequently, it is a challenge for designers to construct lightweight linear diffusions layer with bigger branch numbers in lightweight cryptography.

A linear diffusion layer is a linear transformation over $(\mathbb{F}_2^m)^n$ with positive integers m and n, which can be represented by an $n \times n$ matrix and the entries can be regarded as linear transformation over $\mathbb{F}_2^m$. A linear diffusion layer with maximum branch number $n+1$ is called a perfect diffusion layer or a Maximal Distance Separable (MDS) matrix.

A common approach to construct MDS matrices is extracting them from MDS codes [15]. Many block ciphers [3], [7], [6], [17], especially AES, use this method to construct the diffusion layers. A disadvantage of using MDS matrices as that in AES is the operation is heavy in hardware implementation [19]. Therefore, these MDS matrices are not well suited for resource constrained environments, such as RFID systems and sensor networks.

Another method to construct lightweight MDS matrices is recursive construction, respectively [8], [9], [16], [19], [2], [11], [4], [1]. This method maybe lead to high latency. Recently, researchers began to construct lightweight MDS matrices over finite fields by choosing elements whose multiplication's implementation efficiency can be further improved [13], [18], [14]. In particular, a new way of constructing MDS matrices was proposed in [14]. The authors constructed MDS matrices with entries in the set of $m \times m$ non-singular matrices over $\mathbb{F}_2$ directly, and assume the linear transformations over $\mathbb{F}_2^m$ are not pairwise commutative. The authors used the following notation to represent 4×4 circulant matrix,

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

where $A, B, C, D \in GL(m, \mathbb{F}_2)$ with $m = 4, 8$. To construct lightweight circulant involutory MDS matrices, they started with a circulant matrix $L = \mathrm{Circ}(I, A, B, C)$ where I is the identity matrix with order m. Then they search all pairs (A, C) such that $A^2 = C^2 = I$ and the multiplication order of $A + C$ equals $4k - 2$ for some integer k with $k > 1$, which are properties of involutory matrices. Finally they test whether L is MDS when $B = (A + C)^{2k}$ is completely determined by A and C. Other MDS matrices such as Hadamard involutory MDS matrices are constructed in the similar way.

Our Contributions. In the present paper we propose a new approach to construct lightweight MDS matrices. As mentioned above, the direct construction using MDS codes is heavy in implementation and the recursive construction is high-latency. Therefore, we concentrate on the problem of constructing MDS matrices balancing implementation with latency. Different from the construction strategy in [14], we construct MDS matrix using multiplication of two matrices which are block matrices and the entries are linear transformations over finite field. We show that the circulant MDS matrix can be constructed with our method efficiently. For circulant MDS matrices constructed in this paper, the fewest sum of XOR operations of one row's entries is 1. We show that for circulant MDS matrix $\mathrm{Circ}(A + I, A, I, A + I)$, we have found 48 different 4×4 matrices A with 1 XOR operation in the first row, and 80640 different 8×8 matrices A with 1 XOR operation in the first row. Compare with previous direct constructions of MDS matrices, our constructions have achieved fewer XORs.

Outline of This Paper. The organization of the paper is as follows. In Section II, we provide some preliminaries. In Section III, we investigate the construction of MDS matrices using circulant matrices. Finally, we give our conclusion in Section IV.

Qinyi Mei is also at University of Chinese Academy of Sciences, Beijing, China (e-mail: meiqinyi@iie.ac.cn).

II. Preliminaries

In this section, we introduce some concepts and results we need later.

We call a map M from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ linear if $M(x+y) = M(x) + M(y)$ holds for any $x, y \in \mathbb{F}_2^n$. Given a vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$, we can represent a linear map over $\mathbb{F}_2^n$ by an $n \times n$ matrix over $\mathbb{F}_2$, which is also denoted by M. Notice that $M(x) = M \cdot x$, where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ is regarded as a column vector in the subsequent discussions. We denote the set of all $m \times m$ matrices with entries in S by $Mat(m \times m, S)$.

For $M \in Mat(m \times m, \mathbb{F}_2)$, here we give a simplified representation of M by extracting the nonzero positions in each row of M. For instance, $[1, [2,3], [4], [1,2,3]$ is the simplified representation of the matrix as follows,

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

Every linear diffusion can be represented by a matrix as follows,

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

where $L_{i,j}$ is an $m \times m$ matrix over $\mathbb{F}_2$ for $1 \leq i, j \leq n$. For $X = (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_2^m)^n$,

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

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

To improve the efficiency of implementation, we often use circulant matrices in the construction of MDS matrices.

For $X = (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_2^m)^n$, the bundle weight of X is defined as the number of nonzero entries of X, which is marked as $w_b(X)$. The branch number of L is defined as

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

The branch number of L is upper bounded by $n+1$, and a matrix with maximal branch number is called a MDS matrix.

There are several ways to prove that a matrix is MDS [5]. In the present paper we restate one of the most commonly used statements that can be used to identify MDS matrix in [15].

Proposition 1: Given an $n \times n$ matrix M over $\mathbb{F}_2^m$, it is an MDS matrix if and only if every square sub-matrix (formed from any i rows and any i columns, for any $i = 1, 2, \cdots, n$) of M is nonsingular.

According to Proposition 1, the computation would be complicated when n is large. Based on this result, we concentrate on 4×4 matrices, which are widely used in cryptography. To be more exactly, our major target is constructing MDS matrix with good hardware implementation.

III. Construction of Lightweight Circulant MDS Matrices

In this section, we investigate the problem of constructing lightweight circulant MDS matrices.

First of all, for a 4×4 circulant matrix, we note that

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

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

Remember that our target is constructing MDS matrices which are not only lightweight but also low-latency. Therefore, we specially choose to construct MDS matrices by multiplying two matrices to reduce latency. Meanwhile, we tend to use linear transformations with low XOR operations for the efficiency of implementation.

For convenience of expression, we use O denote null matrix over $Mat(m \times m, \mathbb{F}_2)$, I denote identity matrix over $Mat(m \times m, \mathbb{F}_2)$. Then we have the following result.

Proposition 2: Let $L = Circ(A, B, C, D)$ be a circulant matrix, where $A, B, C, D \in Mat(m \times m, \mathbb{F}_2)$. If there is one null matrix and one identity matrix or at least two null matrix among A, B, C, D, then L^2 is not an MDS matrix.

Proof: Let $L = Circ(A, B, C, D)$ be a circulant matrix. The square of a circulant matrix is still a circulant matrix. Thus, L^2 is a circulant matrix.

Next we prove that L^2 is not an MDS matrix when there is one null matrix and one identity matrix among A, B, C, D. There are 12 cases needed to be considered. Without loss of generality, we suppose

$$A = O, B = I.$$

Assume $L = Circ(O, I, C, D)$. Then

$$L^2 = Circ(C^2, CD + DC, C^2 + I, O)$$

is a matrix formed with one null matrix. According to Proposition 1, L^2 is not an MDS matrix. The other 11 cases with different orders of entries can be proved in the similar way.

Secondly, we prove that if there are two null matrices among A, B, C, D, then L^2 is not an MDS matrix. There are 6 cases Without loss of generality, we suppose

$$A = O, B = O.$$

We assume that $L = Circ(O, O, C, D)$. Then

$$L^2 = Circ(C^2, CD + DC, D^2, O)$$

is a matrix formed with one null matrix. According to Proposition 1, L^2 is not an MDS matrix. The other 5 cases with different orders of entries can be proved in the similar way.

Thirdly, we prove that if there are three null matrices among A, B, C, D, then L^2 is not an MDS matrix. There are 4 cases needed to be considered. Without loss of generality, we suppose

$$A = O, B = O, C = O.$$

We assume that $L = Circ(O, O, O, D)$. Then

$$L^2 = Circ(O, O, D^2, O)$$

is a matrix formed with three null matrices. According to Proposition 1, L^2 is not an MDS matrix. The other 3 cases with different orders of entries can be proved in the similar way.

If A, B, C, D are all null matrices, then $L^2 = (O, O, O, O)$ is definitely not an MDS matrix. ■

Based on the above limitation on the square of circulant matrices, we turn to construct MDS matrix with multiplication of two different circulant matrices M and N, which both are block matrices.

Remark 1 We assume that the entries of M (N) are among O, I, A, B, where A and B represent unknown matrices over $Mat(m \times m, \mathbb{F}_2)$. M (N) with same entries and different orders of entries are regarded as one type. For example, circulant block matrices, which are formed with A, B, O, I, all can be represented by $CIRC(O, I, A, B)$.

Furthermore we investigate the property of the multiplication of M and N. We calculate all factors $f(A, B)$ of determinants of all square sub-matrices of MN, denote the set of all factors $f(A, B)$ as $C1$.

Theorem 1: MN is an MDS matrix if and only if every matrix in the condition set $C1$ is nonsingular.

Proof: According to Proposition 1, MN is an MDS matrix if and only if every square sub-matrix of MN is nonsingular, if and only if the determinant of every square sub-matrix of MN is nonzero, if and only if all factors of the determinant of every square sub-matrix of MN is nonsingular, if and only if every matrix in the condition set $C1$ is nonsingular. ■

In the present paper, we discuss M, N with at least one null matrix in regard of hardware implementation. Our constructing method is as follows.

- 1)Construct two different 4×4 circulant matrices M and N, such that MN is an MDS matrix. M and N are block matrices with entries over $Mat(m \times m, \mathbb{F}_2)$.
- 2)According to Theorem 1, search A, B over $Mat(m \times m, \mathbb{F}_2)$, where $m = 4, 8$. Notice that if no A or B satisfy the condition that MN is MDS, in this case, we will change the choice of M or N.

According to the above procedures, we can calculate matrix A and B which make MN MDS. In particular, we search A and B with 1 XOR operation to achieve good efficiency of constructing MDS matrix.

In order to be specific, we give a construction of MDS matrix MN in the following.

First of all, the types of M and N which make MN MDS are listed in Table I. Amount represent the number of MDS matrices produced by each type of M and N.

To construct MDS matrix with XOR operations as few as possible, we choose a special type of M and N which may have fewest XORs. The type of M is $CIRC(O, O, I, A)$. The type of N is $CIRC(O, I, I, I)$. According to Table I, there are 32 pairs of M and N satisfying the condition that MN is MDS matrix. These 32 pairs of M, N and corresponding MDS matrices are listed in Table II.

TABLE I
AMOUNT OF MDS MATRICES

Type of M	Type of N	Amount
CIRC(O, I, A, A)	CIRC(O, I, A, B)	96
CIRC(O, I, A, A)	CIRC(O, I, I, A)	32
CIRC(O, I, A, A)	CIRC(O, I, I, B)	96
CIRC(O, I, A, B)	CIRC(O, I, A, B)	96
CIRC(O, I, A, B)	CIRC(O, I, I, A)	96
CIRC(O, I, A, B)	CIRC(O, I, I, I)	48
CIRC(O, I, I, A)	CIRC(O, I, I, B)	96
CIRC(O, O, A, B)	CIRC(O, I, A, A)	64
CIRC(O, O, A, B)	CIRC(O, I, A, B)	44
CIRC(O, O, A, B)	CIRC(O, I, I, A)	64
CIRC(O, O, A, B)	CIRC(O, I, I, I)	16
CIRC(O, O, I, A)	CIRC(O, I, A, A)	32
CIRC(O, O, I, A)	CIRC(O, I, A, B)	96
CIRC(O, O, I, A)	CIRC(O, I, B, B)	128
CIRC(O, O, I, A)	CIRC(O, I, I, A)	32
CIRC(O, O, I, A)	CIRC(O, I, I, B)	128
CIRC(O, O, I, A)	CIRC(O, I, I, I)	32

Furthermore, we implement M and N respectively. We emphasize that we first implement N and then implement M instead of implenenting MN directly. For example,

$$M = Circ(O, I, I, I), N = Circ(O, I, A, O).$$

Then we have MDS matrix

$$MN = Circ(A + I, A, I, A + I).$$

In order to determine A, we calculate the condition set $C1$ as follows.

$$C1 = \{A, A + I, A^2 + A + I, A^3 + A + I, A^3 + A^2 + I\}.$$

When $m = 4$, we search A over $Mat(4 \times 4, \mathbb{F}_2)$. There exist A such that $Circ(A+I, A, I, A+I)$ is MDS. The fewest sum of XORs of one rows' entries of an MDS $Circ(A+I, A, I, A+I)$ constructed as above is 1.There are 48 A with this property.

When $m = 8$, we search A over $Mat(8 \times 8, \mathbb{F}_2)$. There exist A such that $Circ(A + I, A, I, A + I)$ is MDS. The fewest sum of XORs of one rows' entries of an MDS $Circ(A + I, A, I, A + I)$ constructed as above is 1. There are 80640 A with this property.

As follows, we give examples of A such that $Circ(A + I, A, I, A + I)$ are circulant MDS matrices when $m = 4, 8$.

Example 1: When $m = 4$,

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

TABLE II
32 PAIRS OF M, N

M	N	MN
Circ(O, I, I, I)	Circ(0, I, A, O)	Circ(A+I, A, I, A+I)
Circ(O, I, I, I)	Circ(C, I, O, O)	Circ(I, A, A+I, A+I)
Circ(O, I, I, I)	Circ(O, O, A, I)	Circ(A+I, A+I, I, X)
Circ(O, I, I, I)	Circ(I, A, O, O)	Circ(A, I, A+I, A+I)
Circ(O, I, I, I)	Circ(O, A, I, O)	Circ(A+I, I, A, A+I)
Circ(O, I, I, I)	Circ(I, O, O, A)	Circ(A, A+I, A+I, I)
Circ(O, I, I, I)	Circ(O, O, I, A)	Circ(A+I, A+I, A, I)
Circ(O, I, I, I)	Circ(A, O, O, I)	Circ(I, A+I, A+I, A)
Circ(I, O, I, I)	Circ(0, I, A, O)	Circ(A+I, A+I, A, I)
Circ(I, O, I, I)	Circ(A, I, O, O)	Circ(A+I, I, A, A+I)
Circ(I, O, I, I)	Circ(O, O, A, I)	Circ(A, A+I, A+I, I)
Circ(I, O, I, I)	Circ(I, A, O, O)	Circ(A+I, A, I, A+I)
Circ(I, O, I, I)	Circ(O, A, I, O)	Circ(A+I, A+I, I, A)
Circ(I, O, I, I)	Circ(I, O, O, A)	Circ(I, A, A+I, A+I)
Circ(I, O, I, I)	Circ(O, O, I, A)	Circ(I, A+I, A+I, A)
Circ(I, O, I, I)	Circ(A, O, O, I)	Circ(A, I, A+I, A+I)
Circ(I, I, I, O)	Circ(O, I, A, O)	Circ(A, I, A+I, A+I)
Circ(I, I, I, O)	Circ(A, I, O, O)	Circ(A, A+I, A+I, I)
Circ(I, I, I, O)	Circ(O, O, A, I)	Circ(A+I, I, A, A+I)
Circ(I, I, I, O)	Circ(I, A, O, O)	Circ(I, A+I, A+I, A)
Circ(I, I, I, O)	Circ(O, A, I, O)	Circ(I, A, A+I, A+I)
Circ(I, I, I, O)	Circ(I, O, O, A)	Circ(A+I, A+I, I, A)
Circ(I, I, I, O)	Circ(O, O, I, A)	Circ(A+I, A, I, A+I)
Circ(I, I, I, O)	Circ(A, O, O, I)	Circ(A+I, A+I, A, I)
Circ(I, I, O, I)	Circ(O, I, A, O)	Circ(I, A+I, A+I, A)
Circ(I, I, O, I)	Circ(A, I, O, O)	Circ(A+I, A+I, I, A)
Circ(I, I, O, I)	Circ(O, O, A, I)	Circ(I, A, A+I, A+I)
Circ(I, I, O, I)	Circ(I, A, O, O)	Circ(A+I, A+I, A, I)
Circ(I, I, O, I)	Circ(O, A, I, O)	Circ(A, A+I, A+I, I)
Circ(I, I, O, I)	Circ(I, O, O, A)	Circ(A+I, I, A, A+I)
Circ(I, I, O, I)	Circ(O, O, I, A)	Circ(A, I, A+I, A+I)
Circ(I, I, O, I)	Circ(A, O, O, I)	Circ(A+I, A, I, A+I)

TABLE III
COMPARISON WITH PREVIOUS CONSTRUCTIONS OF CIRCULANT MDS MATRICES

elements	the first row	XOR count	Reference
$GL(4, \mathbb{F}_2)$	[A+I, A, I, A+I]	$1 + 3 \times 4 = 13$	Example 1
$GL(4, \mathbb{F}_2)$	[I, I, A, B]	$3 + 3 \times 4 = 15$	[14]

Example 2: When $m = 8$,

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

We give comparisons of our constructions with previous constructions in Tables III and IV.

TABLE IV
COMPARISON WITH PREVIOUS CONSTRUCTIONS OF CIRCULANT MDS MATRICES

elements	the first row	XOR count	Reference
$GL(8, \mathbb{F}_2)$	[A+I, A, I, A+I]	$1 + 3 \times 8 = 25$	Example 2
$GL(8, \mathbb{F}_2)$	[I, I, A, B]	$3 + 3 \times 8 = 27$	[14]

IV. CONCLUSION

In the present paper, We show that the circulant MDS matrices can be constructed with our method efficiently. To reduce the latency of constructing, we construct MDS matrix with multiplication of two matrices. We search MDS matrices with XOR operations as few as possible to make sure eff implementation on hardware. Compare to previous constructions of circulant MDS matrices, our constructions have achieved fewer XORs. The problem of constructing lightweight MDS matrices of large order with the method in this paper need further study.

APPENDIX

In Tables V and VI, we respectively give all the 4×4 and partial 8×8 matrices A with one XOR operation, which make $MN = Circ(A + I, A, I, A + I)$ MDS matrices.

TABLE V
4×4

A=(2, 4, 1, [3, 4])	A=(4, [1, 4], 2, 3)
A=(3, [1, 2], 4, 2)	A=(2, 4, [1, 2], 3)
A=([1, 4], 1, 2, 3)	A=(2, 3, [3, 4], 1)
A=(3, 4, [2, 3], 1)	A=(3, 4, 2, [1, 3])
A=(3, [1, 3], 4, 2)	A=(4, 3, [1, 3], 2)
A=(3, [2, 4], 2, 1)	A=(2, [2, 3], 4, 1)
A=([2, 4], 3, 1, 2)	A=([1, 4], 3, 1, 2)
A=(4, [2, 3], 1, 2)	A=(3, 4, 2, [1, 4])
A=([2, 3], 3, 4, 1)	A=([2, 3], 4, 2, 1)
A=(4, 3, [1, 4], 2)	A=(2, [3, 4], 1, 3)
A=(4, 1, 2, [2, 3])	A=([2, 3], 3, 1, 4)
A=(4, 3, 1, [2, 3])	A=(3, 1, [3, 4], 2)
A=(3, [1, 4], 2, 1)	A=(2, [3, 4], 4, 1)
A=(4, [1, 2], 2, 3)	A=(4, [1, 3], 1, 2)
A=([3, 4], 1, 4, 2)	A=(2, [2, 4], 1, 3)
A=(2, 3, 4, [1, 2])	A=(2, 3, [1, 4], 1)
A=([1, 2], 3, 4, 1)	A=(3, 4, [2, 4], 1)
A=(4, 1, 2, [3, 4])	A=(4, 3, 1, [2, 4])
A=(4, 1, [1, 2], 3)	A=([3, 4], 1, 2, 3)
A=([1, 3], 4, 2, 1)	A=(4, 1, [2, 3], 3)
A=(3, 1, 4, [2, 4])	A=(2, 3, 4, [1, 4])
A=(2, 4, [1, 3], 3)	A=([2, 4], 4, 1, 3)
A=([1, 3], 1, 4, 2)	A=(3, 1, [2, 4], 2)
A=(2, 4, 1, [1, 3])	A=([1, 2], 4, 1, 3)

TABLE VI
8×8

A=(2, 7, 4, 8, 6, 1, [2, 3], 5)	A=(4, 5, 8, [2, 3], 6, 7, 1, 2)
A=(8, 6, 1, 7, 2, [2, 3], 5, 4)	A=(7, 6, 4, 1, 2, [2, 3], 8, 5)
A=([2, 3], 1, 6, 5, 8, 7, 4, 2)	A=(7, 5, 8, 1, 6, 4, [2, 3], 2)
A=(5, 4, 1, [2, 3], 8, 7, 2, 6)	A=(5, 6, 7, 1, 8, [2, 3], 4, 2)
A=(4, 8, 6, [2, 3], 1, 2, 5, 7)	A=(7, 1, 6, 8, 4, 2, 5, [2, 3])
A=(5, 8, 6, [2, 3], 7, 2, 4, 1)	A=(6, 1, 5, 7, 2, 8, [2, 3], 4)
A=([2, 3], 5, 8, 6, 4, 7, 1, 2)	A=(5, 7, 8, [2, 3], 4, 1, 6, 2)
A=([2, 3], 1, 8, 5, 2, 4, 6, 7)	A=(8, 4, 6, 1, 7, 2, [2, 3], 5)
A=(7, 6, 8, 1, 4, [2, 3], 2, 5)	A=(4, 6, 7, 2, 8, [2, 3], 5, 1)
A=(4, 8, 6, 5, 7, 1, 2, [2, 3])	A=(4, 1, 5, 6, 2, 8, [2, 3], 7)
A=(5, 7, 4, 2, 6, 8, 1, [2, 3])	A=(6, 7, 5, [2, 3], 2, 8, 1, 4)
A=(5, 4, 6, 1, 8, 2, [2, 3], 7)	A=(2, 6, 5, 7, 4, [2, 3], 8, 1)
A=(5, 4, 7, 6, [2, 3], 8, 2, 1)	A=(8, 6, 5, 1, 2, 4, [2, 3], 7)
A=([2, 3], 1, 6, 8, 2, 7, 4, 5)	A=(7, 5, 4, 6, [2, 3], 1, 8, 2)
A=(4, 1, 7, 5, 6, 8, 2, [2, 3])	A=(7, 6, 4, 5, 8, [2, 3], 2, 1)
A=(7, 4, 8, 5, 6, 1, [2, 3], 2)	A=(4, 5, 7, 6, [2, 3], 2, 8, 1)
A=(2, 7, 1, 5, 8, [2, 3], 4, 6)	A=(6, 5, 4, 8, [2, 3], 7, 2, 1)
A=(5, 4, 8, [2, 3], 6, 2, 1, 7)	A=(2, 5, 1, 6, 8, 7, [2, 3], 4)
A=(6, 7, 8, 1, [2, 3], 5, 4, 2)	A=(2, 4, 1, 7, 6, [2, 3], 8, 5)
A=(5, 8, 6, 1, 7, 2, [2, 3], 4)	A=(6, 4, 8, [2, 3], 7, 2, 1, 5)
A=(4, 8, 1, 7, 6, 2, 5, [2, 3])	A=(4, 6, 8, [2, 3], 7, 5, 1, 2)
A=(4, 8, 6, 5, 7, 2, [2, 3], 1)	A=(8, 7, 5, [2, 3], 2, 1, 6, 4)
A=(6, 8, 5, 1, 4, 7, 2, [2, 3])	A=(7, 6, 4, 2, 8, 5, [2, 3], 1)

Acknowledgment

The authors would like to thank the anonymous referees for their helpful comments. We also wish to thank Yongqiang Li for providing useful and valuable suggestions.

References

[1] 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.

[2] 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.

[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] Daemen, J., Knudsen, L. R., Rijmen, V.: The Block Cipher SQUARE. In Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149-165. Springer, Heidelberg (1997).

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

[8] 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).

[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] Gupta, K. C., Ray, I. G.: On Constructions of Involutory MDS Matrices. In AFRICACRYPT, pages 43-60, 2013.

[11] 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).

[12] Junod, P., Vaudenay, S.: Perfect Diffusion Primitives for Block Ciphers Building Effcient MDS Matrices. In: Handschuh, H., Hasan, M. A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 84-99. Springer, Heidelberg (2004).

[13] 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.

[14] Li, Y., Wang, M.: On the construction of lightweight circulant involutory MDS matrices. In: Thomas, P. (ed.): FSE 2016, LNCS 9783, pp. 121-139. Springer, Heidelberg (2016).

[15] MacWilliams, F. J., Sloane, N. J. A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, 2nd edition (1986).

[16] 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).

[17] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-Bit Blockcipher CLEFIA (Extended Abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181195. Springer, Heidelberg (2007).

[18] Sim, S.M., Khoo, K., Oggier, F., Peyrin, T.: Lightweight MDS Involution Matrices. In: Leander, G., Demirci, H. (eds.) FSE 2015. LNCS, Springer (2015).

[19] 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.