CONSTRUCTION OF NEW FAMILIES OF MDS DIFFUSION LAYERS

S. M. Dehnavi
Department of Mathematical and Computer Sciences
University of Kharazmi
Tehran, Iran
std_dehnavsim@khu.ac.ir

A. Mahmoodi Rishakani
Department of Sciences
Shahid Rajaee Teacher Training University
Tehran, Iran
am.rishakani@srttu.edu

M. R. Mirzaee Shamsabad
Department of Mathematics and Computer Science
University of Shahid Bahonar
Kerman, Iran
mohammadmirzaeesh@yahoo.com

Hamidreza Maimani
Department of Sciences
Shahid Rajaee Teacher Training University
Tehran, Iran
maimani@ipm.ir

Einollah Pasha
Department of Mathematical and Computer Sciences
University of Kharazmi
Tehran, Iran
pasha@khu.ac.ir

Abstract. **Diffusion layers are crucial components of symmetric ciphers. These components, along with suitable Sboxes, can make symmetric ciphers resistant against statistical attacks like linear and differential cryptanalysis. Conventional MDS diffusion layers, which are defined as matrices over finite fields, have been used in symmetric ciphers such as AES, Twofish and SNOW. In this paper, we study linear, linearized and nonlinear MDS diffusion layers. We investigate linearized diffusion layers, which are a generalization of conventional diffusion layers; these diffusion layers are used in symmetric ciphers like SMS4, Loiss and ZUC. We introduce some new families of linearized MDS diffusion layers and as a consequence, we present a method for construction of randomized linear diffusion layers over a finite field. Nonlinear MDS diffusion layers are introduced in Klimov's thesis; we investigate nonlinear MDS diffusion layers theoretically, and we present a new family of nonlinear MDS diffusion layers. We show that these nonlinear diffusion layers can be made randomized with a low implementation cost. An important fact about linearized and nonlinear diffusion layers is that they are more resistant against algebraic attacks in comparison to conventional diffusion layers. A special case of diffusion layers are (0,1)-diffusion layers. This type of diffusion layers are used in symmetric ciphers like ARIA. We examine (0,1)-diffusion layers and prove a theorem about them. At last, we study linearized MDS diffusion layers of symmetric ciphers Loiss, SMS4 and ZUC, from the mathematical viewpoint.**

Keywords. **MDS, Linearized, Nonlinear, Diffusion Layer, Linear Branch Number, Differential Branch Number**

1. Introduction

Diffusion layers are important components of symmetric ciphers. It is well-known that these components, along with suitable Sboxes, can make symmetric ciphers resistant against statistical attacks like linear and differential cryptanalysis. Conventional MDS diffusion layers, which are defined as matrices on finite fields, have been used in symmetric ciphers such as AES[1], Twofish[2] and SNOW[3]. In this paper, we study linear, linearized and nonlinear MDS diffusion layers; in fact, we

examine block-wise MDS matrices over a finite commutative ring with identity.

Linearized MDS diffusion layers are used in symmetric ciphers like SMS4[4], Loiss[5] and ZUC[6]. We present some families of linearized diffusion layers, wich can be seen as a generalization of conventional diffusion layers. We prove that some types of conventional cyclic diffusion layers, including the MDS matrix used in AES, are MDS for almost all elements of the base finite field on which these diffusion layers are defined, and based on this fact, we present a method for randomizing these types of diffusion layers.

We also investigate nonlinear MDS diffusion layers. These types of MDS diffusion layers are introduced in [7]. We construct a new family of nonlinear MDS diffusion layers, based on a mathematical study; we show that these nonlinear diffusion layers can be made randomized with a low implementation cost. An important fact about linearized and nonlinear diffusion layers is that they are more resistant against algebraic attacks compared to conventional diffusion layers.

We study (0,1)-diffusion layers and prove that, in a (0,1)-diffusion layer, if we replace 1 entries by a bit-wise nonsingular matrix, then the resulting linearized matrix has the same differential and linear branch numbers. These types of matrices, are used in symmetric ciphers like ARIA[8]. At last, we study linearized MDS diffusion layers of symmetric ciphers Loiss, SMS4 and ZUC, from the mathematical viewpoint.

In Section 2, we present preliminary notations and definitions. Section 3 is devoted to the proof of our main theorem about MDS diffusion layers. In Section 4, we construct new linearized MDS diffusion layers. Section 5 examines nonlinear MDS diffusion layers. Section 6 studies (0,1)-diffusion layers. Section 7 is devoted to linearized MDS diffusion layers of symmetric ciphers Loiss, SMS4 and ZUC and Section 8 is the conclusion.

2. **Notations and Definitions**

We use these notations in this paper:
$|A|$: number of elements or cardinality of a finite set A,
$\mathcal{B}_n$: set of all $n \times n$ binary matrices,
$\mathcal{M}_n(R)$: set of all $n \times n$ matrices with entries in a ring R,
A^{-1}: the inverse of a matrix A,
A^T: entry-wise transpose of a matrix A,
$d(A)$: determinant of a matrix A in $\mathcal{B}_n$,

$d_R(A)$: determinant of a matrix A in $\mathcal{M}_n(R)$,
$\equiv$: natural isomorphism between algebraic structures and also equivalence of vectors,
$\gg$: right shift operator,
$\ll$: left shift operator,
$\ggg$: right cyclic shift or rotation operation,
$\lll$: left cyclic shift or rotation operation,
$\wedge$: bitwise AND operator,
$\oplus$: XOR of two binary vectors or matrices,
$\mathbf{0}$: any vector or matrix zero,
I: every identity matrix,
F_{2^n}: finite field with 2^n elements,
Z_{2^n}: ring of integers modulo 2^n,
F_2^n: Cartesian product of n copies of F_2,
R^n: Cartesian product of n copies of R.

Suppose that R is a finite commutative ring with identity and $x \in R^n$ is a column-wise vector with $n = km$; the weight of x with respect to m-tuples is defined as the number of nonzero m-tuples of x. More precisely, if

$$x = (x_{k-1}, \ldots, x_1, x_0)^T$$

$$\equiv (x_{k-1,m-1}, \ldots, x_{k-1,0}; \ldots; x_{1,m-1}, \ldots, x_{1,0}; x_{0,m-1}, \ldots, x_{0,0})^T,$$

then we have,

$$w_m(x) = |\{0 \leq i < k | x_i \neq \mathbf{0}\}|.$$

Let R be a finite commutative ring with identity, n be a natural number, $n = mk$ and $A \in \mathcal{M}_n(R)$. The matrix A can be represented as a block-wise matrix

$$A = [A_{i,j}]_{k \times k}, \quad A_{i,j} \in \mathcal{M}_m(R), \quad 1 \leq i, j \leq k. \tag{2.1}$$

Let $M \in \mathcal{M}_n(R)$ with $n = mk$. We define the branch number of M with respect to m-tuples as

$$\min_{x \in R^n - \{\mathbf{0}\}} \{w_m(x) + w_m(Mx)\}.$$

Regarding (2.1), the matrix A is called MDS with respect to m-tuples iff its branch number with respect to m-tuples equals $k+1$. It's not hard to see that we can construct a $(2k, |R|^{mk}, k+1)$-code over R^m which is MDS.

Suppose that $M \in \mathcal{B}_n$ with $n = mk$. The linear branch number of M with respect to m-bit words is defined as

$$\min_{x \in F_2^n - \{\mathbf{0}\}} \{w_m(x) + w_m(M^T x)\},$$

and the differential branch number of M with respect to m-bit words is defined as

$$\min_{x \in F_2^n - \{\mathbf{0}\}} \{w_m(x) + w_m(Mx)\}.$$

Let $f : F_2^n \to F_2^n$ with $n = mk$ be a function. The linear branch number of f with respect to m-bit words is defined as

$$\min_{\alpha,\beta \in F_2^n, (\alpha,\beta) \neq (0,0), P(\alpha.x \oplus \beta.f(x)=0) \neq \frac{1}{2}} \{w_m(\alpha) + w_m(\beta)\},$$

and the differential branch number of f with respect to m-bit words is defined as

$$\min_{x,y \in F_2^n, x \neq y} \{w_m(x \oplus y) + w_m(f(x) \oplus f(y))\}.$$

A function $f : F_2^n \to F_2^n$ is called a linearized function iff for all $x, y \in F_2^n$, we have,

$$f(x \oplus y) = f(x) \oplus f(y).$$

Regarding the notation (2.1), we note that the definition of linear and differential branch numbers with respect to m-bit words, for a function f from F_2^n to itself, with $n = mk$, is a generalization of the corresponding definitions in the case that f is a linearized function: in this case, f has a corresponding matrix F in $\mathcal{B}_n$ and the linear and differential branch numbers of f and F, with respect to m-bit words, are equal. Likewise, the definition of branch number for a commutative ring R with identity, in the case that R is the field F_{2^t}, and $m = 1$ or $n = k$, matches with the defintion of differential branch number for a $k \times k$ matrix over F_{2^t} or a matrix in $\mathcal{B}_{kt}$. Moreover, the definition of branch number for a commutative ring R with identity, in the case that R is the ring Z_{2^t}, $n = mk$ and $t > 1$, equals to differential branch number of a nonlinear (nonlinearized) function with respect to mt-bit words.

As stated before, regarding (2.1), we denote the entry-wise transpose of the matrix $A \in \mathcal{M}_n(R)$ with $n = mk$ by A^T which can also be represented as

$$A^T = [B_{i,j}]_{k \times k}, \quad B_{i,j} = A^T_{j,i}, \quad 1 \leq i, j \leq k,$$

and the block-wise transpose of A by

$$A^t = [C_{i,j}]_{k\times k}, \quad C_{i,j} = A_{j,i}, \quad 1 \leq i,j \leq k,$$

and the transpose of A which we call in-block, by

$$A^\tau = [D_{i,j}]_{k\times k}, \quad D_{i,j} = A_{i,j}^T, \quad 1 \leq i,j \leq k.$$

For any finite commutative ring R with identity, the block-wise determinant of an $n \times n$ matrix A with $n = mk$ in the ring $\mathcal{M}_k(\mathcal{M}_m(R))$, regarding representation (2.1), is denoted by $d_m(A)$: in this definition, we suppose that all k^2 blocks of A are pairwise commutable.

For an $n \times n$ sparse (0,1)-matrix $M = [m_{i,j}]$, we represent it by an n-tuple of sets representing the index of 1 entries of M, begining from the first row and from the index zero, from the right. For example, for the matrix

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

with the corresponding linearized function

$$f(x_3, x_2, x_1, x_0) = (x_1, x_3 \oplus x_2, x_0, x_3),$$

we have,

$$f(f(x_3, x_2, x_1, x_0)) = (x_0, x_1 \oplus x_2 \oplus x_3, x_3, x_1).$$

So,

$$M = (\{1\}, \{2,3\}, \{0\}, \{3\}),$$

and consequently,

$$M^2 = (\{0\}, \{1,2,3\}, \{3\}, \{1\}).$$

We use this notation and correspondence, in Section 4.

3. **Main Theorem**

In this section, we prove the main theorem of this paper. This theorem is proved in special cases, in several books and papers; e. g. [9, Chap. 11] and [10,11]. For the proof of next theorem, we note that for any (nonsingular) square matrix B over a finite commutative ring R with identity, there exists a matrix B' (called the adjoint of B) such that,

$$B'B = BB' = d_R(B)I.$$

Also we note that [16] if R is a finite commutative ring with identity, then $A \in \mathcal{M}_n(R)$ is nonsingular iff the R-linear mapping

$$f : R^n \to R^n,$$
$$f(r_1, \ldots, r_n) = (r_1, \ldots, r_n)A,$$

is a bijection, or equivalently, iff f has zero kernel.

Theorem 3.1. *Let R be a finite commutative ring with identity, n be a natural number, $n = mk$ and $A \in \mathcal{M}_n(R)$. Then, according to representation (2.1), A is MDS with respect to m-tuples iff each block-wise square submatrix of A is nonsingular as a matrix over R.*

Proof. At first, we suppose that every square block-wise submatrix of A is nonsingular. Now, suppose that A is not an MDS matrix; then, the branch number of A is less than $k + 1$. So, there exist vectors $Y = (Y_1, \ldots, Y_k)$ and $X = (X_1, \ldots, X_k)$ with $AX = Y$, $w_m(X) = t$ and $w_m(Y) < k + 1 - t$. Here, X_i's and Y_i's, $1 \leq i \leq k$, are m-tuples with entries in R. Let nonzero indices of X be j_r's, $1 \leq r \leq t$. Since Y has at least t zeros, supposing that the indices of these zeros are i_r's, $1 \leq r \leq t$, the square block-wise submatrix indexed by j_r block-rows and i_r block-columns, $1 \leq r \leq t$, is singular, which is a contradiction.

Now suppose that A is MDS; then for any natural number t and any vector X with $w_m(X) = t$, such that its nonzero indices are $I = \{i_1, \ldots, i_t\}$, we have $w_m(AX) \geq k + 1 - t$. If $Y = AX$, then for any $J = \{j_1, \ldots, j_t\}$, the vector Y' derived from Y with nonzero m-tuples with indices in J, is nonzero. Considering A' as the block-wise square submatrix with block-column indices in J and block-row indices in I, the linear mapping (over R)

$$X \to A'X,$$

has zero kernel. Thus, A' is nonsingular or $d_R(A')$ is invertible in R. □

Corollary 3.2. *Let R be a finite commutative ring with identity, n be a natural number, $n = mk$ and $A \in \mathcal{M}_n(R)$. Then, A is MDS with respect to m-tuples iff A^T is MDS with respect to m-tuples.*

Corollary 3.3. *Let n be a natural number, $n = mk$ and $A \in \mathcal{B}_n$. Regarding (2.1), A is MDS with respect to m-bit words iff each block-wise square submatrix of A is nonsingular as a matrix over F_2.*

Corollary 3.4. *Let n be a natural number, $n = mk$ and $A \in \mathcal{B}_n$. Then A is MDS with respect to m-bit words iff A^T is MDS with respect to m-bit words.*

4. Construction of New Families of Linearized MDS Diffusion Layers

In this section, we investigate linearized MDS diffusion layers and construct some new families of block-wise 4×4 linearized MDS diffusion layers.

Theorem 4.1. *Let $A, B \in \mathcal{B}_m$ and*

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

Then, invertibility of the following matrices in $\mathcal{B}_m$ is a necessary condition for M to be MDS:

$$A \oplus B,\ AB \oplus I,\ A^2 \oplus B,\ A \oplus B^2.$$

Proof. Using Corollary 3.3, all 36 two-by-two submatrices of M are nonsingular. We have verified all these submatrices for invertibility. We used Schur's lemma for computing the determinant of matrices. For example, the submatrix

$$\begin{pmatrix} A & B \\ I & A \end{pmatrix}$$

is nonsingular iff $A^2 \oplus B$ is nonsingular. □

The proof of the following lemma can be found in [12].

Lemma 4.2. *Let n be a natural number, R be a finite commutative ring with identity, $n = km$ and $A \in \mathcal{M}_n(R)$. Consider the block-wise representation (2.1) of A. If the k^2 blocks of A are pairwise commutable, then we have,*

$$d_R(A) = d_R(d_m(A)).$$

Lemma 4.2 offers another systematic and efficient method to check (by programming) whether a matrix is MDS or not, using Theorem 3.1. For instance, by Lemma 4.2, we can easily verify that some of the matrices wich are given in [13] are MDS.

Theorem 4.3. *Let $m \geq 2$ and A, B, $\mathcal{A} = A \oplus I$ and $\mathcal{B} = B \oplus I$ are nonsingular matrices in $\mathcal{B}_m$ such that $AB = BA$. Define $M \in \mathcal{B}_{4m}$ as*

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

Then, M is MDS iff all of the following matrices in $\mathcal{B}_m$ are nonsingular:

$$A\mathcal{A}^2 \oplus \mathcal{B}^2,$$
$$B\mathcal{B}^2 \oplus \mathcal{A}^2,$$
$$B\mathcal{A}^2 \oplus \mathcal{B}^2,$$
$$A\mathcal{B}^2 \oplus \mathcal{A}^2,$$
$$AB \oplus I,$$
$$A^2 \oplus B = \mathcal{A}^2 \oplus \mathcal{B},$$
$$A \oplus B^2 = \mathcal{A} \oplus \mathcal{B}^2,$$
$$A \oplus B = \mathcal{A} \oplus \mathcal{B}.$$

Proof. Since $AB = BA$, we can use Lemma 4.2. We should verify the invertibility of all

$$\sum_{i=1}^{4} \binom{4}{i}^2 = \binom{8}{4} - 1 = 69$$

block-wise submatrices of M. There are 16 one-by-one submatrices which are invertible by the assumptions of the theorem. By Theorem 4.1, the 36 two-by-two submatrices are invertible. We have verified all 16 three-by-three submatrices and the whole matrix, i.e. M. For instance, using Lemma 4.1 and the indentity

$$(X \oplus I)^2 = X^2 \oplus I,$$

we have,

$$d\begin{pmatrix} B & I & I \\ A & B & I \\ I & A & B \end{pmatrix} = d\left(B(d_m\begin{pmatrix} B & I \\ A & B \end{pmatrix}) \oplus I(d_m\begin{pmatrix} A & I \\ I & B \end{pmatrix}) \oplus I(d_m\begin{pmatrix} A & B \\ I & A \end{pmatrix})\right)$$

$$= d(B(B^2 \oplus A) \oplus I(AB \oplus I) \oplus I(A^2 \oplus B)) = d(B^3 \oplus A^2 \oplus B \oplus I) = d(B\mathcal{B}^2 \oplus \mathcal{A}^2).$$

□

Corollary 4.4. *Let $m \geq 2$ and A and $A \oplus I$ are nonsingular matrices in $\mathcal{B}_m$. Define $M \in \mathcal{B}_{4m}$ as*

$$M = \begin{pmatrix} A & A \oplus I & I & I \\ I & A & A \oplus I & I \\ I & I & A & A \oplus I \\ A \oplus I & I & I & A \end{pmatrix}. \tag{4.1}$$

Then, M is MDS iff $A^3 \oplus I$ and $A^7 \oplus I$ are nonsingular matrices in $\mathcal{B}_m$.

Proof. Using Theorem 4.3 and doing some matrix computations, the theorem is proved. □

We have searched matrices of the form (4.1) by programming. The followiong matrix in $\mathcal{B}_8$ satisfies the conditions of Corollary 4.4:

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

Now, we show that some of the MDS matrices which are given in [13], including the linear MDS diffusion layer of AES, are MDS for almost all elements of the base finite field on which these diffusion layers are defined.

Corollary 4.5. *Let $m \geq 2$ and α and $\beta = \alpha + 1$ are nonzero elements of F_{2^m}. Define M as*

$$M = \begin{pmatrix} \alpha & \beta & 1 & 1 \\ 1 & \alpha & \beta & 1 \\ 1 & 1 & \alpha & \beta \\ \beta & 1 & 1 & \alpha \end{pmatrix}.$$

Then, M is MDS iff α^3 and α^7 are not equal to 1.

Corollary 4.5 states that for almost all elements of F_{2^m}, the matrix M is MDS. More precisely, the number of elements α in F_{2^m} which do not make M MDS, is equal to

$$gcd(3, 2^m - 1) + gcd(7, 2^m - 1).$$

For instance, in F_{2^8}, only 4 elements do not make M MDS. Using Corollary 4.5, we can construct a randomized family of MDS diffusion layers: we can save a table of the elements of F_{2^m} which do not make M MDS, and based on a value depending on key, data, IV or state in symmetric ciphers, we randomly choose an α which makes a random MDS matrix.

Theorem 4.6. *Let R be a finite commutative ring with identity and $A \in \mathcal{M}_n(R)$ with $n = km$. Regarding block-wise representation (2.1) of A, suppose that all the k^2 blocks of A are pairwise commutable. If A is MDS, then the entry-wise transpose, the block-wise transpose and the in-block transpose of A are also MDS.*

Proof. For the entry-wise transpose A^T, we can use Corollary 3.2. For the block-wise transpose A^t we can use Lemma 4.2, and at last for the in-block transpose A^τ, we note that,

$$A^\tau = (A^T)^t = (A^t)^T.$$

□

Using the methods and concepts given in this section, the matter of verification that a linear matrix is MDS or not, is simply done by programming. For instance, all of the matrices in [14] can be easily verified by our method. Of course, these matrices are for instance, of the form

$$M_{_A} = \begin{pmatrix} p_{1,1}(A) & p_{1,2}(A) & p_{1,3}(A) & p_{1,4}(A) \\ p_{2,1}(A) & p_{2,2}(A) & p_{2,3}(A) & p_{2,4}(A) \\ p_{3,1}(A) & p_{3,2}(A) & p_{3,3}(A) & p_{3,4}(A) \\ p_{4,1}(A) & p_{4,2}(A) & p_{4,3}(A) & p_{4,4}(A) \end{pmatrix};$$

here, $p_{i,j}$'s , $1 \leq i, j \leq 4$, are polynomials in A, and we know that each two polynomial entries of the matrix $M_{_A}$ are commutable. The case of matrices with polynomial entries is also studied in [11].

Lemma 4.7. *Suppose that $A \in \mathcal{B}_n$ and $A^5 = I$. In this case, invertibility of $A \oplus I$ is a sufficient condition for satisfaction of the conditions of Corollary 4.4.*

Proof. Since $A^5 = I$, A is invertible. Now,

$$A^3 \oplus I = A^{-2} \oplus I = (A^{-1} \oplus I)^2,$$

and since $A(A^{-1} \oplus I) = A \oplus I$, so $A^3 \oplus I$ is nonsingular. Also, we have,

$$A^7 \oplus I = A^2 \oplus I = (A \oplus I)^2;$$

thus, $A^7 \oplus I$ is also nonsingular. □

Example. The function $f : F_2^{16} \to F_2^{16}$ with

$$f(x) = (x \ggg 4) \oplus ((x \lll 4) \gg 4) = (x \ggg 4) \oplus (x \wedge 4095)$$

satisfies the conditions of Lemma 4.7.

Proof. Suppose that A is the corresponding matrix of f. Using the notations of Section 2, we have,

$$A = \big(\{3\},\{2\},\{1\},\{0\},\{11,15\},\{10,14\},\{9,13\},\{8,12\},\{7,11\},$$
$$\{6,10\},\{5,9\},\{4,8\},\{3,7\},\{2,6\},\{1,5\},\{0,4\}\big).$$

So,

$$A^2 = \big(\{3,7\},\{2,6\},\{1,5\},\{0,4\},\{3,11,15\},\{2,10,14\},\{1,9,13\},$$
$$\{0,8,12\},\{7,15\},\{6,14\},\{5,13\},\{4,12\},\{3,11\},\{2,10\},\{1,9\},\{0,8\}\big).$$

Now, we have,

$$A^4 = \big(\{3,7,11,15\},\{2,6,10,14\},\{1,5,9,13\},\{0,4,8,12\},\{3,7,15\},$$
$$\{2,6,14\},\{1,5,13\},\{0,4,12\},\{3,15\},\{2,14\},\{1,13\},\{0,12\},\{15\},$$
$$\{14\},\{13\},\{12\}\big).$$

It's not hard to see that $A^5 = I$. Now,

$$A \oplus I = \big(\{3,15\},\{2,14\},\{1,13\},\{0,12\},\{15\},\{14\},\{13\},\{12\},\{11\},$$
$$\{10\},\{9\},\{8\},\{7\},\{6\},\{5\},\{4\}\big).$$

It can be easily verified that $A \oplus I$ is nonsingular; therefore the conditions of Lemma 4.7 are satisfied. □

Lemma 4.8. *Let $A \in \mathcal{B}_n$ and $A^{10} = I$. In this case, invertibility of $A^3 \oplus I$ is a sufficient condition for satisfaction of the conditions of Corollary 4.4.*

Proof. Since $A^{10} = I$, so A is invertible. Now we have,

$$A^3 = (A \oplus I)(A^2 \oplus A \oplus I);$$

thus, $A \oplus I$ is nonsingular. Also we have,

$$A^7 \oplus I = A^{-3} \oplus I,$$

and since $A^3(A^{-3} \oplus I) = A^3 \oplus I$, then $A^7 \oplus I$ is nonsingular. □

Example. The function $f : F_2^{16} \to F_2^{16}$ with

$$f(x) = (x \ggg 2) \oplus ((x \lll 4) \gg 4) = (x \ggg 2) \oplus (x \wedge 4095)$$

satisfies the conditions of Lemma 4.8.

Proof. Suppose that A is the corresponding matrix of f. Using the notations of Section 2, we have,

$$A = \big(\{1\}, \{0\}, \{15\}, \{14\}, \{11, 13\}, \{10, 12\}, \{9, 11\}, \{8, 10\}, \{7, 9\}, \{6, 8\},$$
$$\{5, 7\}, \{4, 6\}, \{3, 5\}, \{2, 4\}, \{1, 3\}, \{0, 2\}\big),$$

and

$$A^2 = \big(\{1, 3\}, \{0, 2\}, \{1\}, \{0\}, \{11, 13, 15\}, \{10, 12, 14\}, \{9, 13\}, \{8, 12\},$$
$$\{7, 11\}, \{6, 10\}, \{5, 9\}, \{4, 8\}, \{3, 7\}, \{2, 6\}, \{1, 5\}, \{0, 4\}\big).$$

It follows that,

$$A^4 = \big(\{1, 3, 5, 7\}, \{0, 2, 4, 6\}, \{1, 5\}, \{0, 4\}, \{3, 11, 13, 15\}, \{2, 10, 12, 14\},$$
$$\{1, 9, 13\}, \{0, 8, 12\}, \{7, 13, 15\}, \{6, 12, 14\}, \{5, 13\}, \{4, 12\}, \{3, 11\}, \{2, 10\},$$
$$\{1, 9\}, \{0, 8\}\big),$$

and,

$$A^8 = \big(\{1, 3, 5, 7, 9, 11, 15\}, \{0, 2, 4, 6, 8, 10, 14\}, \{1, 5, 9, 13\}, \{0, 4, 8, 12\},$$
$$\{3, 7, 13, 15\}, \{2, 6, 12, 14\}, \{1, 5, 13\}, \{0, 4, 12\}, \{3, 13, 15\}, \{2, 12, 14\}, \{1, 13\},$$
$$\{0, 12\}, \{13, 15\}, \{12, 14\}, \{13\}, \{12\}\big).$$

Thus $A^{10} = I$. On the other hand, it's not hard to verify that

$$A^3 \oplus I = \big(\{1, 5, 15\}, \{0, 4, 14\}, \{1, 3, 13\}, \{0, 2, 12\}, \{1, 13, 15\}, \{0, 12, 14\},$$
$$\{11, 15\}, \{10, 14\}, \{9, 11, 13\}, \{8, 10, 12\}, \{7, 9, 11\}, \{6, 8, 10\}, \{5, 7, 9\},$$
$$\{4, 6, 8\}, \{3, 5, 7\}, \{2, 4, 6\}\big)$$

is an invertible matrix. So the conditions of Lemma 4.8 are satisfied. □

We emphasize that linearized maps are linear as bit-wise maps; but these maps are not necessarily linear as functions over finite fields with dimensions greater than 1.

Example. In Theorem 3.1, put $n = 1$ and suppose that R is the ring $\frac{F_2[z]}{<z^2>}$. Since $r = z + 1$ is an invertible element in R, so the function

$$f : R \to R,$$
$$f(x) = rx,$$

is MDS. Now, if we represent this map on the field F_{2^2}, defined by the unique irreducible polynomial $z^2 + z + 1$, we have,

$$f : F_{2^2} \to F_{2^2},$$
$$f(x) = \alpha^2 x^2,$$

where $\alpha = z$. Obviously, f is a quadratic function over F_{2^2}, but f is a linearized function:

$$f(x \oplus y) = \alpha^2(x \oplus y) = \alpha^2 x^2 \oplus \alpha^2 y^2 = f(x) \oplus f(y).$$

5. Construction of Nonlinear MDS Diffusion Layers

In this section, we investigate nonlinear MDS diffusion layers. This type of MDS diffusion layers are discussed in [7]. We present a new family of nonlinear MDS diffusion layers. The proof of the following Lemma is not hard.

Lemma 5.1. *Let n and t be natural numbers and $\mathcal{A} = [\alpha_{i,j}] \in \mathcal{M}_n(Z_{2^t})$. Define $A = [a_{i,j}] \in \mathcal{B}_n$ as*

$$a_{i,j} = \begin{cases} 0 & \alpha_{i,j} \text{ is even,} \\ 1 & \alpha_{i,j} \text{ is odd.} \end{cases}$$

Then we have,

$$d(A) = d_{Z_{2^t}}(\mathcal{A}) \bmod 2.$$

Theorem 5.2. *Let n and t be natural numbers, $n = mk$ and $A = [a_{i,j}] \in \mathcal{B}_n$. Suppose that A is MDS with respect to m-bit words, regarding representation (2.1). Let $\alpha_{i,j} \in Z_{2^t}$, $1 \leq i, j \leq n$, be such that $\alpha_{i,j}$ is odd if $a_{i,j} = 1$ and $\alpha_{i,j}$ is even if $a_{i,j} = 0$. Then the matrix $\mathcal{A} = [\alpha_{i,j}]$, defined on $\mathcal{M}_n(Z_{2^t})$, is a (nonlinear) MDS diffusion layer with respect to tm-bit words.*

Proof. According to Theorem 3.1, it suffices to prove that every square block-wise submatrix of $\mathcal{A}$ is nonsingular, or equivalently, the determinant of every block-wise square submatrix of $\mathcal{A}$ is an odd number. Since A is MDS, so every square block-wise submarix of A is nonsingular in F_2; so by Lemma 5.1, every square block-wise submatrix of $\mathcal{A}$ is nonsingular in Z_{2^t}, and this ends the proof. □

As mentioned in Section2, we note that Theorem 5.2 states that $\mathcal{A}$ has maximum differential branch number. Using [15, Theo. B.1.2], it is proved that $\mathcal{A}$ has also maximum linear branch number.

We note that, based on Theorem 5.2, we can construct a family of randomized nonlinear diffusion layers. In fact, in this theorem, some of $\alpha_{i,j}$'s can be selected randomly based on key, IV, data or state in symmetric ciphers; the only restriction is that the least significant bit of $\alpha_{i,j}$'s must be 0 or 1 according to $a_{i,j}$'s.

It is also worth noting that nonlinear (and nonlinearized) diffusion layers are more resistant against algebraic attacks in comparison to conventional diffusion layers, as we stated in Section 4: in fact, linearized maps can be nonlinear over finite fields with dimensions greater that 1 and nonlinear maps, in general, can be nonlinear even on F_2.

Example. In Theorem 3.1, put $n = 1$ and suppose that R is the ring Z_{2^3}. Since 3 is an invertible element in R, so the function

$$f : R \to R,$$
$$f(x) = 3x \ \ mod \ \ 2^3,$$

is MDS. Now, if we represent this map on F_2, we have,

$$f : F_2^3 \to F_2^3,$$
$$f(x_2, x_1, x_0) = (x_2 \oplus x_1 \oplus x_1x_0, x_1 \oplus x_0, x_0).$$

Obviously, f is a quadratic function over F_2; or equivalently, the (maximum) degree of f is 2.

Example. Consider $A \in \mathcal{B}_4$ as,

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

It is not hard to see that A is MDS with respect to 2-bit words: i.e. A has linear and differential branch numbers equal to 3 with respect to 2-bit words. By Theorem 5.2, the map

$$F : \left(F_2^{16}\right)^2 \equiv (Z_{2^8})^4 \to \left(F_2^{16}\right)^2 \equiv (Z_{2^8})^4,$$
$$F(X_1, X_0) = (Y_1, Y_0),$$

with

$$X_1 = (X_1^H, X_1^L), \ X_0 = (X_0^H, X_0^L), \ Y_1 = (Y_1^H, Y_1^L), \ Y_0 = (Y_0^H, Y_0^L),$$

and,

$$Y_1^H = (151X_1^H + X_0^H + X_0^L) \ \ mod \ \ 2^8,$$
$$Y_1^L = (X_1^L + 218X_0^H + X_0^L) \ \ mod \ \ 2^8,$$
$$Y_0^H = (X_1^H + X_0^H + 102X_0^L) \ \ mod \ \ 2^8,$$

$$Y_0^L = (X_1^H + 73X_1^L + X_0^L,) \ mod \ 2^8,$$

is a nonlinear MDS diffusion layer with respect to 16-bit words; of course, F corresponds to the matrix

$$\mathcal{F} = \begin{pmatrix} 151 & 0 & 1 & 1 \\ 0 & 1 & 218 & 1 \\ 1 & 0 & 1 & 102 \\ 1 & 73 & 0 & 1 \end{pmatrix},$$

which is defined over Z_{2^8}. Thus, F or $\mathcal{F}$ is a nonlinear (nonlinearized) diffusion layer over 32-bit words or F_2^{32}, which has linear and differential branch numbers equal to 3, with respect to 16-bit words.

With the aid of Theorem 5.2, it's possible to construct nonliear MDS diffusion layers of large sizes. These diffusion layers are efficiently implemented in modern processors, i.e. 32-bit or 64-bit processors; because, in the implementation of this type of diffusion layers, we only need the operations of addition and multiplication modulo a power of two, which are amongst the basic instructions of modern processors.

6. (0,1)-Diffusion Layers

In some applications in symmetric cryptography, (0,1)-matrices are used; for instanse, in [8], this type of diffusion layers is used. Another example of these matrices are 4×4 almost MDS diffusion layers with linear and differential branch numbers 4. For example, the matrix

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

is an almost MDS diffusion layer with linear and differential branch numbers 4; in fact, the matrix M is equivalent to the matrix

$$M = \begin{pmatrix} \mathbf{0} & I & I & I \\ I & \mathbf{0} & I & I \\ I & I & \mathbf{0} & I \\ I & I & I & \mathbf{0} \end{pmatrix}.$$

Next theorem is somehow obvious.

Theorem 6.1. *Suppose that $M = [m_{i,j}]$, $1 \leq i, j \leq m$, is a (0,1)-matrix with (bit-wise) linear branch number l and differential branch number d*

and $A \in \mathcal{B}_n$ is a nonsingular matrix. Then $\mathcal{M} = [M_{i,j}]$, $1 \leq i, j \leq m$, with

$$M_{i,j} = \begin{cases} A & m_{i,j} = 1, \\ \mathbf{0} & m_{i,j} = 0, \end{cases}$$

is a linearized diffusion layer with linear branch number l and differential branch number d, with respect to n-bit words.

We know that the function

$$f : F_2^n \to F_2^n,$$
$$f(x) = x^2,$$

defined on the field F_{2^n}, is a one-to-one linearized function. So for each m, $1 \leq m \leq n$, the function

$$f_m : F_2^n \to F_2^n,$$
$$f_m(x) = x^{2^m},$$

is also a one-to-one linearized function. Now, as an example, using Theorem 6.1, we can prove that the linearized diffusion layer defined on $\mathcal{B}_{4n}$ with the defining equations

$$\begin{aligned} Y_1 &= X_2^{2^m} \oplus X_3^{2^m} \oplus X_4^{2^m}, \\ Y_2 &= X_1^{2^m} \oplus X_3^{2^m} \oplus X_4^{2^m}, \\ Y_3 &= X_1^{2^m} \oplus X_2^{2^m} \oplus X_4^{2^m}, \\ Y_4 &= X_1^{2^m} \oplus X_2^{2^m} \oplus X_3^{2^m}, \end{aligned}$$

which also can be seen as a function over n-bit words, has linear and differential branch numbers equal to 4. Since for each $x \in F_{2^n}$ we have $x^{2^n} = x$, then the inverse of this diffusion layer can be represented as

$$\begin{aligned} Y_1 &= X_2^{2^{n-m}} \oplus X_3^{2^{n-m}} \oplus X_4^{2^{n-m}}, \\ Y_2 &= X_1^{2^{n-m}} \oplus X_3^{2^{n-m}} \oplus X_4^{2^{n-m}}, \\ Y_3 &= X_1^{2^{n-m}} \oplus X_2^{2^{n-m}} \oplus X_4^{2^{n-m}}, \\ Y_4 &= X_1^{2^{n-m}} \oplus X_2^{2^{n-m}} \oplus X_3^{2^{n-m}}. \end{aligned}$$

Let the corresponding matrix of the function $f_m(x) = x^{2^m}$ be A_m. Then, the corresponding matrix of the aforementioned diffusion layer is

$$M = \begin{pmatrix} \mathbf{0} & A_m & A_m & A_m \\ A_m & \mathbf{0} & A_m & A_m \\ A_m & A_m & \mathbf{0} & A_m \\ A_m & A_m & A_m & \mathbf{0} \end{pmatrix},$$

or equivalently,

$$Y_1 = A_m(X_2 \oplus X_3 \oplus X_4),$$
$$Y_2 = A_m(X_1 \oplus X_3 \oplus X_4),$$
$$Y_3 = A_m(X_1 \oplus X_2 \oplus X_4),$$
$$Y_4 = A_m(X_1 \oplus X_2 \oplus X_3).$$

In fact, we can implement this diffusion layer with four additional lookup tables: on the other hand, the new linearized diffusion layer has better bitwise diffusion and is stronger from algebraic viewpoint. Moreover, the new linearized diffusion layer has less fixed points, in general. We also notice that, we can use the corresponding matrix of the linearized function

$$f : F_2^n \to F_2^n,$$
$$f(x) = x \ggg t,$$

for an arbitrary t, $1 \leq t < n$, instead of A_m, which has a fast implementation in modern processors.

7. **Diffusion Layers of SMS4, Loiss and ZUC**

In this section, we study MDS diffusion layers of symmetric ciphers SMS4, Loiss and ZUC. For example, the following MDS diffusion layer is used in [5,6].

$$f(x) = x \oplus (x \ggg 2) \oplus (x \ggg 10) \oplus (x \ggg 18) \oplus (x \ggg 24). \tag{7.1}$$

It is worth to note that in (7.1), we have $x \in F_2^{32}$. Define

$$g : F_2^{32} \to F_2^8,$$
$$g(x_0, x_1, x_2, x_3) =$$
$$(x_0 \oplus (x_0 \gg 2)) \oplus (x_1 \oplus (x_1 \ll 6)) \oplus ((x_2 \gg 2) \oplus (x_2 \ll 6)) \oplus ((x_3 \gg 2) \oplus (x_3 \ll 6)).$$

In (7.1), we have $x = (x_0, x_1, x_2, x_3)$ with $x_i \in F_2^8$, $0 \leq i \leq 3$, and $f(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$, where,

$$y_0 = g(x_0, x_1, x_2, x_3),$$
$$y_1 = g(x_1, x_2, x_3, x_0),$$
$$y_2 = g(x_2, x_3, x_0, x_1),$$
$$y_3 = g(x_3, x_0, x_2, x_2).$$

So, the corresponding matrix of this diffusion layer is

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

with

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

and,

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

and $C = A \oplus B$.
We investigated all the diffusion layers of the form

$$f(x) = x \oplus (x \ggg a) \oplus (x \ggg b) \oplus (x \ggg c) \oplus (x \ggg d),$$

with $0 \leq a, b, c, d \leq 31$, by programming. The only linearized MDS diffusion layers of this form are,

$$f_1(x) = x \oplus (x \ggg 2) \oplus (x \ggg 10) \oplus (x \ggg 18) \oplus (x \ggg 24),$$

$$f_2(x) = x \oplus (x \ggg 6) \oplus (x \ggg 14) \oplus (x \ggg 22) \oplus (x \ggg 24),$$

$$f_3(x) = x \oplus (x \ggg 8) \oplus (x \ggg 10) \oplus (x \ggg 18) \oplus (x \ggg 26),$$

$$f_4(x) = x \oplus (x \ggg 8) \oplus (x \ggg 14) \oplus (x \ggg 22) \oplus (x \ggg 30).$$

8. **Conclusion**

Diffusion layers are crucial components of symmetric ciphers. These components, along with suitable Sboxes, can make symmetric ciphers resistant against statistical attacks like linear and differential cryptanalysis. Conventional MDS diffusion layers, which are defined as matrices over finite fields, have been used in symmetric ciphers such as AES, Twofish and SNOW.

In this paper, we studied MDS diffusion layers over a finite commutative ring with identity. We investigated linearized diffusion layers, which are a generalization of conventional diffusion layers. These diffusion layers are used in symmetric ciphers like SMS4, Loiss and ZUC. We introduced some new families of linearized MDS diffusion layers and we presented a method for construction of randomized diffusion layers over a finite field.

Nonlinear MDS diffusion layers are introduced in Klimov's thesis. After some theoretical discussions, we presented a new family of nonlinear MDS diffusion layers and we showed that this family of nonlinear MDS diffusion layers can be made randomized with a low implementation cost. An important fact about linearized and nonlinear diffusion layers is that they are more resistant against algebraic attacks than conventional diffusion layers.

A special case of diffusion layers are (0,1)-diffusion layers; this type of diffusion layers are used in symmetric ciphers like ARIA. We examined (0,1)-diffusion layers and proved a theorem about them. At last, we studied linearized MDS diffusion layers of symmetric ciphers SMS4, Loiss and ZUC.

References

[1] J. Daemen, V. Rijmen, AES proposal: Rijndael. Selected as the Advanced Encryption Standard. Available from http://nist.gov/aes

[2] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish: A 128-bit Block Cipher; 15 June, 1998

[3] P. Ekdahl, T. Johansson, SNOW a new stream cipher, Proceedings of first NESSIE Workshop, Heverlee, Belgium, 2000

[4] Chinese State Bureau of Cryptography Administration, Cryptographic algorithms SMS4 used in wireless LAN products, available at: http://www.oscca.gov.cn/Doc/6/News-1106.htm

[5] Dengguo Feng, Xiutao Feng, Wentao Zhang, Xiubin Fan and Chuankun Wu, Loiss: A Byte-Oriented Stream Cipher, Available at http://www.eprint.iacr.org/2010/489.pdf

[6] ETSI/SAGE: Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 128-EIA3 Document 2: ZUC Specification. Version 1.5, 4th January 2011. Tech. rep., ETSI (2011), http://www.gsmworld.com/documents/EEA3-EIA3-ZUC-v1-5.pdf
[7] A. Klimov, Applications of T-functions in Cryptography, Thesis for the degree of Ph.D., Weizmann Institute of Science, 2005.
[8] Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung, Yaekwon Sohn, Jung Hwan Song, Yongjin Yeom, E-Joong Yoon, Sangjin Lee, Jaewon Lee, Seongtaek Chee, Daewan Han, and Jin Hong, "New Block Cipher: ARIA", In Jong In Lim and Dong Hoon Lee editors, Information Security and Cryptology - ICISC 2003: 6th International Conference, volume 2791 of Lecture Notes in Computer Science, pages 432-445. Springer-Verlag, 2004.
[9] F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1998.
[10] Blaum, M., Roth, R. M.: On Lowest Density MDS Codes. IEEE TRANSACTIONS ON INFORMATION THEORY, vol. 45(1), pp. 46-59 (January 1999)
[11] Daniel Augot, Matthieu Finiasz, "Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions", ISIT 2013: 1551-1555.
[12] Ivan Kovacs, Daniel S. Silver, and Susan G. Williams, "Determinants of Commuting-Block Matrices", The American Mathematical Monthly, Vol. 106, No. 10, Dec. 1999, 950-952.
[13] Pascal Junod, Statistical Cryptanalysis of Block Ciphers, Phd Thesis, Lausanne, EPFL, 2005
[14] Mahdi Sadjadieh, Mohammad Dakhilalian, Hamid Mala, Pouyan Sepehrdad, Recursive Diffusion Layers for Block Ciphers and Hash Functions, fse2012, USA, 2012
[15] Joan Daemen and Vincent Rijmen, The design of rijndael: AES - the advanced encryption standard, Springer, 2002.
[16] Victor Shoup, A Computational Introduction to Number Theory and Algebra (Version 2), Cambridge University Press, 2008.