Ciencias Matemáticas, Vol. 33, No. 1, Pag. 87-92, 2019

Construction of MDS matrices combining the Feistel and Lai-Massey schemes

Ramses Rodríguez Aulet[1], Reynier A. de la Cruz Jiménez[1]*

Abstract In Cryptography maximum distance separable (MDS) matrices are an important structural element to provide the diffusion property in the block ciphers, stream ciphers and hash functions. To discover new kind of transformations that can generate a series of new MDS matrices which could be used in practice is not a trivial task. In this article we propose new methods for constructing such matrices combining the well-known Feistel and Lai-Massey structures.

Keywords
Diffusion — Involutory matrix — Almost involutory matrix — MDS matrix

[1] *Instituto de Criptografía, Universidad de La Habana, La Habana, Cuba, djr.antonio537@gmail.com*
***Autor para Correspondencia**

Introduction

In the work [4] Claude Shannon defines confusion and diffusion as two properties necessary for the construction of block ciphers; these properties are also required for construction of hash functions. One strategy to obtain maximum diffusion and avoid linear and differential attacks is to use global linear mappings with optimal diffusion, combined with the local nonlinear mappings (S-Boxes) (see [9, 10, 11]). The linear transformations choose by designers should be able to spread the internal dependencies as much as possible. Hence, designers commonly used optimal diffusion matrices called Maximum Distance Separable (because they are related to a Maximum Distance Separable code) matrices to maximise the diffusion ability of the diffusion layer. Example of their use can be found no only in the design of block ciphers like AES, TwoFish, KHAZAD, Picaro, etc, but also in the Hash function PHOTON [15], Whirlpool, Grostl, and even in stream ciphers (MUGI).

From practical point of view, is not only desirable that an MDS matrix can be implemented efficiently both in software/hardware but also when encryption and decryption implementations are required and the inverse of the MDS matrix will have to be implemented as well (except for Feistel and Lai-Massey structures, where the inverse of the internal function is not required for decryption [2]). For this reason it is of a great significance that one can use exactly (or almost exactly) the same linear transformarion for encryption and decryption. One strategy to achieve this goal is employing involutory MDS matrices and we can found several ciphers like Anubis, Khazad , Iceberg or Prince that using this approach have the same implementation for encryption and decryption.

The construction of MDS matrices, is not an easy problem to solve. There are several ways for constructing such matrices, for instances: using the Cauchy and Hadamard matrices [20]. In [1] it is shown that it is possible to build involutive binary matrices with a high degree of diffusion by exploiting the properties of the Feistel network and in [19] it is shown that using the general Feistel networks it is possible to build MDS matrices on finite fields, in this case the authors do not build involutory MDS matrices. The aim of this article is to build involutory or almost involutory MDS matrices combining Lai-Massey and Feistel schemes.

This article is structured as follows: In Section 2 we give the basic definitions and some results about MDS matrices. Some construcions which can generate MDS matrices are presented in Section 3. We provide an implementation of a concrete matrix in Section 4. A comparison with the state-oh-the-art is performed in Section 5. Our work is concluded in Section 6.

1. Preliminaries and Basic Definitions

Let be $P = GF(2^t) = GF(2)[x]/g(x)$ finite field with 2^t elements, for some irreducible polynomial $g(x)$ of degree t. The vector space of dimension n over P is denoted by P^n. We use the notation $P_{n,n}$ for the ring of $n \times n$ matrices over finite field P. Throughout the article, we shall use the following operations and notations:

1	- the neutral element of the multiplicative group P^*;
$\oplus$	- addition in GF(2^t);
$w_H(\vec{a})$	- the Hamming weight of a vector $\vec{a} \in P^n$;
$\omega(\mathscr{M})$	- the number of 1's in the matrix $\mathscr{M}$;
Ψ^{-1}	- the inverse transformation to some invertible mapping Ψ;
$I_{n,n}$	- the identical matrix of $P_{n,n}$.
$O_{n,n}$	- the zero matrix of $P_{n,n}$.
$\lvert A\rvert$	- the determinant of the matrix of $A \in P_{n,n}$.

In what follows, for the sake of simplicity we shall write a polynomial as its coefficient vector interpreted as a hexadecimal number, for example, $x^8 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$ corresponds to 0x11D. We extend the same philosophy to matrices over finite field P, i.e., each coefficient of such matrix will be writen in hexadecimal notation.

Definition 1 *An transformation $\varphi : P^n \to P^n$ is called involutive, if $\forall \alpha \in P^n$ the following equality hold $\varphi(\varphi(\alpha)) = \alpha$.*

Clearly, if φ is an involutive transformation then for any $\phi : P^n \to P^n$ the transformation $\hat{\varphi} = \phi \circ \varphi \circ \phi^{-1}$ will be an ivolution too.

Definition 2 *An transformation $\varphi : P^n \to P^n$ is called linear transformation , if the following relation holds*

$$\forall, \vec{\alpha}, \vec{\beta} \in P^n, a_1, a_2 \in P : \varphi(a_1\vec{\alpha} + a_2\vec{\beta}) = a_1\varphi(\vec{\alpha}) + a_2\varphi(\vec{\beta}), \tag{1}$$

It is shown in [7] that the composition of linear transformations is again a linear transformation.

Definition 3 *Let be $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ a basis of the vector space P^n. The matrix $A_{\vec{\alpha}}(\varphi) \in P_{n,n}$ defined as follows*

$$A_{\vec{\alpha}}(\varphi) = (\varphi(\alpha_1)^{\downarrow}_{\vec{\alpha}}, \ldots, \varphi(\alpha_1)^{\downarrow}_{\vec{\alpha}}) \tag{2}$$

is called the matrix associated with the linear transformation φ in the basis $\vec{\alpha}$.

Definition 4 *The branch number ρ of matrix $A \in P_{n,n}$ is defined as*

$$\rho(A) = \min_{\vec{a} \neq \vec{0}} \{ w_H(\vec{a}) + w_H(\vec{a}A) \}. \tag{3}$$

Definition 5 *A matrix $A \in P_{n,n}$ is called maximal distance separable (MDS) matrix if $\rho(A) = n+1$.*

Theorem 1 *Matrix A is an MDS matrix if and only if every sub-matrix is non-singular.*

Proposition 1 *[12] Any 4×4 matrix over P with all entries non zero is an MDS matrix if and only if it is a full rank matrix with the inverse matrix having all entries non zero and all of its 4×4 submatrices are full rank.*

For efficient implementation of an MDS matrix in software, it is desirable to have maximum number of 1's in the matrix. In [13], authors studied this property and constructed some matrices achieving the maximum number of 1's. Here we restate the definition of the number of occurrences of one, which we will use in our constructions.

Definition 6 *Let be $A = (a_{ij})_{n \times n}$ an arbitrary matrix over P. The number of occurrences of one in A denoted by $\mathscr{N}_1(A)$ is the the number of (i, j) pairs such that a_{ij} is equal to one.*

It is well known from [13] that for any MDS matrix $A \in P_{4,4}$ we have $\mathscr{N}_1(A) = 9$ and $\mathscr{N}_1(A) = 16$ when A is an MDS matrix of $P_{6,6}$.

Definition 7 *Let be $A = (a_{ij})_{n \times n}$ an arbitrary matrix over P. We say that A has the almost involutory property if*

1. *$A^{-1} \neq A$;*
2. *All coefficients of A can be found in A^{-1} too.*

For example, let be $P = GF(2^4)/0x13$ and

$$\mathscr{M}_{2\times2} = \begin{pmatrix} 1 & C \\ C & E \end{pmatrix} \in P_{2,2}.$$

It can be easy checked that $\mathscr{M}_{2\times2}^{-1} = \begin{pmatrix} E & C \\ C & 1 \end{pmatrix} \in P_{2,2}$ and the coefficients of $\mathscr{M}_{2\times2}$ are present in $\mathscr{M}_{2\times2}^{-1}$ too, so this matrix has the almost involutory property. Other example of a matrix having the almost involutory property can be found in the linear layer of the block cipher Kuznyechik which can be expresed as a power of the companion matrix of the follwowing polynomial $h(y) = y^{16} \oplus 94y^{15} \oplus 20y^{14} \oplus 85y^{13} \oplus 10y^{12} \oplus C2y^{11} \oplus C0y^{10} \oplus 01y^9 \oplus FBy^8 \oplus 01y^7 \oplus C0y^6 \oplus C2y^5 \oplus 10y^4 \oplus 85y^3 \oplus 20y^2 \oplus 94y \oplus 01$ over $P = GF(2^8)/0x1C3$.

We can see that involutory and almost involutory MDS matrices can be useful when implementing the inverse of an SPN cipher, because the inverse of these kind of matrices can also be implemented efficiently.

Proposition 2 *If $A \in P_{n,n}$ is an involutory MDS matrix and $S \in P_{n,n}$ is permutation matrix then the matrix AS and SA are almost involutory MDS.*

Proof: Let be A involutive MDS matrix and S permutation matrix then S^{-1} is permutation matrix. Then we have that $(AS)(S^{-1}A) = A(SS^{-1})A = AA = I_{n,n}$ and taking into account that S permutation matrix we obtain that AS is an MDS matrix which has the almost involutory property.

Definition 8 *The characteristic polynomial of a linear transformation of a matrix $A \in P_{n,n}$, denoted by $\chi_A(x)$, is defined as follow*

$$\chi_A(x) = |I_{n,n}x \oplus A|. \tag{4}$$

In work [5] the authors showed the possibility of invariant attacks on the cipher type XSL-network (Khazad, Kuznyechik) where for any $a \in P$ and $k \in \mathbb{N}$ $(x+a)^k$ divide the characteristic polynomial of the lineal transformation. For this reason we will study the characteristic polynomial of those matrices generate by our constructions.

Definition 9 *The polynomial $m_A(x)$ is called the minimal polynomial of matrix A if and only if $m_A(A) = O_{n,n}$, and for any $h \in P[x]$ such that $h(A) = O_{n,n}$, $deg(m_A(x)) \leq deg(h(x))$.*

A direct consequence of the above definition is that always $m_A(x) \big| \chi_A(x)$.

Proposition 3 *For any involutive matrix A the following relations holds:*

1. *$\chi_A(x) = (x \oplus 1)^n$;*

2. $m_A(x) = (x \oplus 1)^2$.

Proof: Firstly we will determine the minimal polynomial lineal of the involutive transformation φ. Let be

$$\vec{\alpha}_1 = (1, 0, \ldots, 0), \ldots, \vec{\alpha}_n = (0, 0, \ldots, 0, 1),$$

the canonical basis of dimension n. It's well known [7, proposition 31, p. 321] that

$$m_\varphi(x) = lcm(m_{\alpha_1,\varphi}(x), m_{\alpha_2,\varphi}(x), \ldots, m_{\alpha_n,\varphi}(x)), \quad (5)$$

where $lcm(\cdot)$ denote the least common multiple. Now taking into account that the linear transformation φ is an involution we can use the following auxiliary proposition

Proposition 4 *[7, p. 321] Let be φ —an aribitrary linear transformation of dimension n. Then for any nonzero vector γ there exist a natural number $k = 1, \ldots, n$ such that the following vectors*

$$\gamma, \varphi(\gamma), \ldots, \varphi^{k-1}(\gamma) \quad (6)$$

are linearly independent and $\varphi^k(\gamma)$ is a linear combination of the previous system. In this case if

$$\varphi^k(\gamma) = \gamma c_0 \oplus \varphi(\gamma)c_1 \oplus \ldots \oplus \varphi^{k-1}(\gamma)c_{k-1}, \quad (7)$$

then

$$m_{\gamma,\varphi}(x) = x^k \oplus c_{k-1}x^{k-1} \oplus c_1 x \oplus c_0, \quad (8)$$

from which it follows that $m_{\alpha_i,\varphi}(x) = (x \oplus 1)^2 \ \forall i = 1, \ldots, n$ and hence $m_\varphi(x) = (x \oplus 1)^2$.

Now we shall determine the characteristic polynomial. We know that

$$\deg(\chi_A(x)) = n. \quad (9)$$

For any matrix A we have that $(Ix \oplus A)$ is similar to $\mathscr{K}(Ix \oplus A)$, where $\mathscr{K}(Ix \oplus A)$,is the canonical form $(Ix \oplus A)$. It's well known [7, theorems 10 and 12, p. 342-343] that

$$\mathscr{K}(Ix \oplus A) = diag(1, \ldots, 1, u_1(x), \ldots, u_s(x), (x \oplus 1)^2),$$

where $s \in \mathbb{N}$, $u_s(x) \big| (x \oplus 1)^2$. So, using this fact and relation (10) we obtain that $u_1(x) = \ldots = u_s(x) = x \oplus 1$, hence $\chi_A(x) = (x \oplus 1)^n$. $\square$

Every $n \times n$ matrix over P can be written as an $(tn) \times (tn)$ matrix over $GF(2)$. When considering a hardware implementation, it is natural to consider only matrices over $GF(2)$. Measurements of implementation costs will then only involve the number of bit-operations (XORs) needed. It is an interesting question to evaluate the efficiency of a given matrix. The following metrics are useful for estimating the hardware cost of a linear operation.

1. **Direct XOR Count**. Given a matrix $\mathscr{M} \in GF(2)_{t\times n, t\times n}$, the direct XOR count $\mathsf{DXC}(\mathscr{M})$ of $\mathscr{M}$ is $\omega(\mathscr{M}) - nt$. This metric corresponds to counting the number of gates used in a naive implementation of the linear mapping $\mathscr{M}$.
2. **Global Optimization**. For a matrix $\mathscr{M} \in GF(2)_{t\times n, t\times n}$, it is posible to obtain an estimation of its cost in hardware by finding a good linear straight-line program corresponding to $\mathscr{M}$ with state-of-the-art automatic tools based on certain SLP[1] heuristic [3], and this metric is denoted as $\mathsf{SLP}(\mathscr{M})$.

2. Constructing MDS matrices combining the Lai-Massey and Feistel transformations

Let be $n = 2t$ an even number, in what follows $\vec{x} = (\vec{x_1} || \vec{x_2})$ where $\vec{x_1} = (x_1, \ldots, x_t)$ and $\vec{x_2} = (x_{t+1}, \ldots, x_{2t})$. For any $\mathscr{L} \in P_{n,n}$ using the well-known Lai-Massey and Feistel schemes we define the following transformation as follows ;

Lai-Massey-like transformation:

$$\varphi_1(\vec{x}) = \big(\vec{x_1} \oplus \mathscr{L}(\vec{x_1} \oplus \vec{x_2})\big) \big\| \big(\vec{x_2} \oplus \mathscr{L}(\vec{x_1} \oplus \vec{x_2})\big). \quad (10)$$

Feistel-like transformation:

$$\varphi_2(\vec{x}) = \big(\vec{x_1} \oplus \mathscr{L}(\vec{x_2})\big) \big\| \vec{x_2}. \quad (11)$$

it is not difficult to see that the transformations given by relations (6) and (7) are involutions

Using the matrix given by relation (2), canonical basis of P^4

$$\vec{\alpha}_4 = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\},$$

and the previuos transformations, we construct the following matrices of dimension $n \times n$, $n = 4$, as follows

Construction of $\mathscr{M}^{\Phi_A}_{n\times n}$
Let be $\Phi_A = \varphi_2 \circ \varphi_1 \circ \varphi_2$. Then $\mathscr{M}^{\Phi_A}_{4\times 4} = A_{\vec{\alpha}_4}(\Phi_A)$;

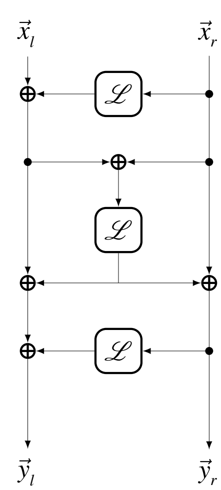

Fig. 1: Structure of Φ_A.

[1]Note that this is so far the most accurate estimation that is practical for 32×32 binary matrices.

Construction of $\mathscr{M}_{n\times n}^{\Phi_B}$
Let be $\Phi_B = \varphi_1 \circ \varphi_2 \circ \varphi_1$. Then $\mathscr{M}_{4\times 4}^{\Phi_B} = A_{\vec{\alpha}_4}(\Phi_B)$;

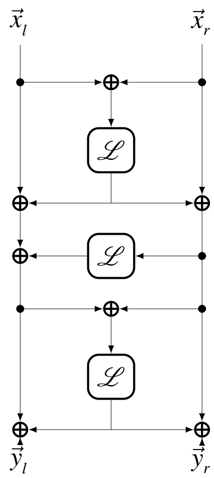

Fig. 2: Structure of Φ_B.

Let be $n = 4$ and $f_1(x) = x^2 \oplus x \oplus 1, f_2(x) = x^3 \oplus x \oplus 1, f_3(x) = x^3 \oplus x^2 \oplus 1, f_4(x) = x^4 \oplus x^3 \oplus 1$ —some polynomials over field P.

Proposition 5 *If there exist an element $a \in P^*$, $a \neq 1$, for which $f_i(a) \neq 0$ where $i = 1,2,4$ then the matrix $\mathscr{M}_{4\times 4}^{\Phi_B}$ of transformation Φ_B with $\mathscr{L} = \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix}$ is an involutory MDS. For the element $a \in P^*$ for which $f_i(a) \neq 0$, where $i = 1,2,3$, the matrix $\mathscr{M}_{4\times 4}^{\Phi_B}$ with $\mathscr{L} = \begin{pmatrix} 1 & 1 \\ a & 1 \end{pmatrix}$ is also an involutory MDS matrix.*

Proof: The matrix $\mathscr{M}_{n\times n}^{\Phi_B} \in P_{4,4}$, for $\mathscr{L} = \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix} \in P_{2,2}$, has the following form

$$\mathscr{M}_{4\times 4}^{\Phi_B} = \begin{pmatrix} a^3 \oplus a^2 \oplus a & a^2 \oplus 1 & a^3 \oplus a & a^2 \oplus 1 \\ a^2 \oplus 1 & a^3 \oplus a^2 \oplus a & a^2 \oplus 1 & a^3 \oplus a \\ a^3 & a^2 & a^3 \oplus a^2 \oplus a & a^2 \oplus 1 \\ a^2 & a^3 & a^2 \oplus 1 & a^3 \oplus a^2 \oplus a \end{pmatrix} \quad (12)$$

Taking into account that $\mathscr{M}_{4\times 4}^{\Phi_B} = (\mathscr{M}_{4\times 4}^{\Phi_B})^{-1}$ we only need to check in correspondence with proposition 1 that all minors of order 2 of $\mathscr{M}_{4\times 4}^{\Phi_B}$ are nonzero over P. These minors are on the following set

$\{a^2 \oplus 1, a^6 \oplus a^4 \oplus a^2 \oplus 1, a^4 \oplus a^3 \oplus a^2 \oplus a, a^2, a^3, a^4, a^6, a^6 \oplus 1, a^3 \oplus a, a^4 \oplus a^2, a^6 \oplus a^2 \oplus 1, a^6 \oplus a^4, a^6 \oplus a^5 \oplus a^4 \oplus a^3 \oplus a^2 \oplus 1, a^3 \oplus a^2 \oplus a, a^6 \oplus a^5 \oplus a^2\}$

whose factors are

$\{(a\oplus 1)^2, (a\oplus 1)^6, a\cdot(a\oplus 1)^3, a^2, a^3, a^4, a^6, (a\oplus 1)^2\cdot(a^2\oplus a\oplus 1)^2, a\cdot(a\oplus 1)^2, a^2\cdot(a\oplus 1)^2, (a^3\oplus a\oplus 1)^2, (a\oplus 1)^2\cdot a^4, (a\oplus 1)^2\cdot(a^4\oplus a^3\oplus 1), a\cdot(a^2\oplus a\oplus 1), a^2\cdot(a^4\oplus a^3\oplus 1)\}$

Therefore for any nonzero $a \in P$ such that

$$\begin{aligned} \alpha &\neq 0, \\ \alpha \oplus 1 &\neq 0, \\ \alpha^2 \oplus \alpha \oplus 1 &\neq 0, \\ \alpha^3 \oplus \alpha \oplus 1 &\neq 0, \\ \alpha^4 \oplus \alpha^3 \oplus 1 &\neq 0, \end{aligned}$$

the matrix $\mathscr{M}_{4\times 4}^{\Phi_B}$ is an involutory MDS matrix over P.

For $\mathscr{L} = \begin{pmatrix} 1 & 1 \\ a & 1 \end{pmatrix} \in P_{2,2}$, we have that

$$\mathscr{M}_{4\times 4}^{\Phi_B} = \begin{pmatrix} 1 & a\oplus 1 & a\oplus 1 & a\oplus 1 \\ a^2\oplus a & 1 & a^2\oplus a & a\oplus 1 \\ a & a & 1 & a\oplus 1 \\ a^2 & a & a^2\oplus a & 1 \end{pmatrix} \quad (13)$$

Here again, by using the fact that $\mathscr{M}_{4\times 4}^{\Phi_B} = (\mathscr{M}_{4\times 4}^{\Phi_B})^{-1}$ we only need to check in correspondence with proposition 1 that all minors of order 2 of $\mathscr{M}_{4\times 4}^{\Phi_B}$ are nonzero over P. These minors are on the following set

$\{1, a^3, a, a\oplus 1, a^2\oplus 1, a^3\oplus 1, a^3\oplus a^2, a^2\oplus a, a^2\oplus a\oplus 1, a^3\oplus a\oplus 1, a^3\oplus a^2\oplus 1, a^3\oplus a, a^2, a^3\oplus a^2\oplus a, a^3\oplus a^2\oplus a\oplus 1\}$

whose factors are

$\{1, a^3, a, (a\oplus 1), (a\oplus 1)^2, (a\oplus 1)\cdot(a^2\oplus a\oplus 1), (a\oplus 1)\cdot a^2, a\cdot(a\oplus 1), (a^2\oplus a\oplus 1), (a^3\oplus a\oplus 1), (a^3\oplus a^2\oplus 1), a\cdot(a\oplus 1)^2, a^2, a\cdot(a^2\oplus a\oplus 1), (a\oplus 1)^3\}$

Therefore for any nonzero $a \in P$ such that

$$\begin{aligned} \alpha &\neq 0, \\ \alpha \oplus 1 &\neq 0, \\ \alpha^2 \oplus \alpha \oplus 1 &\neq 0, \\ \alpha^3 \oplus \alpha \oplus 1 &\neq 0, \\ \alpha^3 \oplus \alpha^2 \oplus 1 &\neq 0, \end{aligned}$$

the matrix $\mathscr{M}_{4\times 4}^{\Phi_B}$ is an involutory MDS matrix over P.

Proposition 6 *If there exist an element $a \in P^*$, $a \neq 1$ for which $f_i(a) \neq 0$ where $i = 1,3$ then the matrix $\mathscr{M}_{4\times 4}^{\Phi_A}$ of transformation Φ_A with $\mathscr{L} = \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix}$ is an involutory MDS matrix.*

Proof: The matrix $\mathscr{M}_{n\times n}^{\Phi_A} \in P_{4,4}$, for $\mathscr{L} = \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix} \in P_{2,2}$, has the following form

$$\mathscr{M}_{4\times 4}^{\Phi_A} = \begin{pmatrix} a^2\oplus a & 1 & a & 1 \\ 1 & a^2\oplus a & 1 & a \\ a^3 & a^2 & a^2\oplus a & 1 \\ a^2 & a^3 & 1 & a^2\oplus a \end{pmatrix} \quad (14)$$

Taking into account that $\mathscr{M}_{4\times 4}^{\Phi_A} = (\mathscr{M}_{4\times 4}^{\Phi_A})^{-1}$ we only need to check according with proposition 1 that all minors of order 2 of $\mathscr{M}_{4\times 4}^{\Phi_A}$ are nonzero over P. These minors are on the following set

$\{1, a^5\oplus a^4\oplus a^2, a, a^2, a^3, a^4, a^4\oplus 1, a^2\oplus a, a^3\oplus a^2\oplus 1, a^4\oplus a^2\oplus 1, a^6\oplus a^4, a^2\oplus 1, a^3\oplus a^2\oplus a\}$

whose factors are
$\{1, a^2\cdot(a^3\oplus a^2\oplus 1), a, a^2, a^3, a^4, (a\oplus 1)^4, a\cdot(a\oplus 1), (a^3\oplus a^2\oplus 1), (a^2\oplus a\oplus 1)^2, (a\oplus 1)^2\cdot a^4, (a\oplus 1)^2, a\cdot(a^2\oplus a\oplus 1)\}$

Therefore for any nonzero $a\in P$ such that

$$\begin{array}{rcl}\alpha & \neq & 0,\\ \alpha\oplus 1 & \neq & 0,\\ \alpha^2\oplus\alpha\oplus 1 & \neq & 0,\\ \alpha^3\oplus\alpha^2\oplus 1 & \neq & 0,\end{array}$$

the matrix $\mathscr{M}_{4\times 4}^{\Phi_A}$ is an involutory MDS matrix over P.

In Table 1 we list certain properties of some matrices generated by ours constructions.

Matrix M	$\mathscr{L}$	Finite field P	Involutory	Almost involotory	$\mathscr{N}_1(M)$	$\chi_M(x)$	$\chi_M(x)$ is irreducible over P	Factorization of $\chi_M(x)$
$\mathscr{M}_{4\times4}^{\Phi_A} = \begin{pmatrix} 1 & 4 & 9 & 4\\ 1 & 1 & 1 & 9\\ 4 & 6 & 1 & 4\\ 8 & 4 & 1 & 1\end{pmatrix}$	$\begin{pmatrix} 9 & 4\\ 1 & 9\end{pmatrix}$	$GF(2^4)/0x13$	Yes	No	7	$x^4\oplus 1$	No	$\chi_M(x)=(x\oplus 1)^4$
$\mathscr{M}_{4\times4}^{\Phi_B} = \begin{pmatrix} 6 & 8 & 2 & 1\\ 8 & 3 & 1 & 1\\ 2 & 1 & 2 & 9\\ 1 & 1 & 9 & 1\end{pmatrix}$	$\begin{pmatrix} 1 & 2\\ 4 & 1\end{pmatrix}$	$GF(2^4)/0x13$	No	Yes	7	$x^4\oplus 6x^3\oplus 3x^2\oplus 6x\oplus 1$	No	$\chi_M(x)=(x^2\oplus 2x\oplus 9)(x^2\oplus 4x\oplus 2)$
$\mathscr{M}_{4\times4}^{\Phi_A} = \begin{pmatrix} 9B & 01 & 56 & 43\\ 01 & 47 & 43 & 01\\ 56 & 43 & 56 & 04\\ 43 & 01 & 04 & 01\end{pmatrix}$	$\begin{pmatrix} 04 & 01\\ 56 & 04\end{pmatrix}$	$GF(2^8)/0x11C$	No	Yes	5	$x^4\oplus 8Bx^3\oplus 1Bx^2\oplus 8Bx\oplus 01$	Yes	–
$\mathscr{M}_{4\times4}^{\Phi_A} = \begin{pmatrix} 04 & 08 & 01 & 06\\ 08 & 04 & 06 & 01\\ 01 & 06 & 01 & 02\\ 06 & 01 & 02 & 01\end{pmatrix}$	$\begin{pmatrix} 02 & 01\\ 01 & 02\end{pmatrix}$	$GF(2^8)/0x11C$	No	Yes	6	$x^4\oplus 55x^2\oplus 01$	No	$\chi_M(x)=(x\oplus 94)^2(x\oplus 9B)^2$
$\mathscr{M}_{4\times4}^{\Phi_A} = \begin{pmatrix} 0A & 06 & 06 & 01\\ 06 & 03 & 01 & 01\\ 06 & 01 & 06 & 02\\ 01 & 01 & 02 & 01\end{pmatrix}$	$\begin{pmatrix} 02 & 01\\ 06 & 02\end{pmatrix}$	$GF(2^8)/0x11C$	No	Yes	7	$x^4\oplus 0Ex^3\oplus 22x^2\oplus 0Ex\oplus 01$	No	$\chi_M(x)=(x^2\oplus 87x\oplus 32)(x^2\oplus 89x\oplus 6F)$
$\mathscr{M}_{4\times4}^{\Phi_B} = \begin{pmatrix} 02 & 02 & 03 & 01\\ 02 & 04 & 01 & 06\\ 03 & 01 & 03 & 03\\ 01 & 06 & 03 & 06\end{pmatrix}$	$\begin{pmatrix} 01 & 02\\ 01 & 01\end{pmatrix}$	$GF(2^8)/0x11C$	No	Yes	4	$x^4\oplus 03x^3\oplus 0Cx^2\oplus 03x\oplus 01$	No	$\chi_M(x)=(x^2\oplus 31x\oplus B0)(x^2\oplus 32x\oplus 87)$
$\mathscr{M}_{4\times4}^{\Phi_B} = \begin{pmatrix} 01 & 02 & 8F & 01\\ 02 & 08 & 01 & 0C\\ 8F & 01 & 8F & 03\\ 01 & 0C & 03 & 0C\end{pmatrix}$	$\begin{pmatrix} 01 & 04\\ 8E & 01\end{pmatrix}$	$GF(2^8)/0x11C$	No	Yes	5	$x^4\oplus 8Ax^3\oplus FAx^2\oplus 8Ax\oplus 01$	Yes	–

Table 1: Properties of some matrices generated by ours constructions.

3. Implementation of concrete $\mathscr{M}_{4\times 4}^{\Phi_A}$

In this section we provide both software/hardware implementations for the following candidate matrix

$$\mathscr{M}_{4\times 4}^{\Phi_A} = \begin{pmatrix} 06 & 01 & 02 & 01\\ 01 & 06 & 01 & 02\\ 08 & 04 & 06 & 01\\ 04 & 08 & 01 & 06\end{pmatrix} \in P_{4,4}, \qquad (15)$$

where $\mathscr{M}_{4\times 4}^{\Phi_A}\in P_{4,4}$, $P = GF(2^8)/0\text{x}11\text{C}$.

3.1 Software implementation

The following code describe a way for implementing the multiplication by the matrix $\mathscr{M}_{4\times 4}^{\Phi_A}$ in C programm language.

```
#define Mult_2(x) ((x<<1)^(x & 0x80 ? 0x1C : 0x00)
    )

uint32_t M(uint32_t x){
  uint8_t a = x, b = x>>8, c = x>>16, d = x>>24,
       e1, e2;
  d ^= Mult_2(b)^a;
  c ^= Mult_2(a)^b;
  e1 = Mult_2((d^b))^(a^c);
  e2 = Mult_2((a^c))^(b^d);
  d ^= e1;
  c ^= e2;
  b ^= e1;
  a ^= e2;
  d ^= Mult_2(b)^a;
  c ^= Mult_2(a)^b;
  return ((((((uint32_t)d<<8)|c)<<8)|b)<<8)|a;
}
```

As it can be seen from the code, the number of field multiplications is decreased up to 6 in comparison with the direct multiplication of $\vec{x}\in P^4$ by $\mathscr{M}_{4\times 4}^{\Phi_A}$. Other matrices generated by our methods can be implemented in a similar way.

3.2 Hardware implementation

The multiplication operation by the MDS matrix given in (15) has the following binary representation over $GF(2)_{32,32}$.

$$\mathscr{M}_{32\times 32}^{\Phi_A} = \left(\begin{array}{cccccccc|cccccccc|cccccccc|cccccccc}
0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0\\
1&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&1&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1\\
\hline
1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1\\
\hline
0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&1&0&1&1&0&0&0&0&0&1&0&1&1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1\\
\hline
0&0&0&0&0&0&1&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&1\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&1&0&1&1&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&1&0\\
0&0&0&0&0&1&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1
\end{array}\right) \qquad (16)$$

From this representation we obtaint that $\mathsf{DXC}(\mathscr{M}_{32\times 32}^{\Phi_A}) = 166$ and using a linear straight-line program corresponding to $\mathscr{M}_{32\times 32}^{\Phi_A}$ with automatic tools proposed in [3] we have found an implementation of $\mathscr{M}_{32\times 32}^{\Phi_A}$ (given in Table 2) which require 99 bitwise XORs.

#	Operation	#	Operation	#	Operation	#	Operation	#	Operation
1	$t_0=x_6\oplus x_{14}$	21	$t_{20}=x_7\oplus t_{18}$	41	$t_{40}=x_3\oplus t_{21}$	61	$t_{60}=x_{15}\oplus y_{15}$	81	$t_{80}=t_{30}\oplus t_{38}$
2	$t_1=x_7\oplus x_{23}$	22	$t_{21}=x_4\oplus x_{20}$	42	$y_5=t_{10}\oplus t_{40}$	62	$y_{23}=t_{47}\oplus t_{60}$	82	$y_2=t_{29}\oplus t_{80}$
3	$t_2=x_{15}\oplus x_{31}$	23	$t_{22}=x_{10}\oplus x_{27}$	43	$t_{42}=t_{11}\oplus t_{25}$	63	$t_{62}=x_{15}\oplus t_{46}$	83	$t_{82}=x_{19}\oplus t_{78}$
4	$t_3=x_5\oplus x_{22}$	24	$t_{23}=x_3\oplus x_{28}$	44	$y_{14}=x_{31}\oplus t_{42}$	64	$y_{22}=t_{59}\oplus t_{62}$	84	$y_{19}=t_{80}\oplus t_{82}$
5	$t_4=x_{13}\oplus x_{30}$	25	$t_{24}=x_2\oplus x_{19}$	45	$t_{44}=t_6\oplus y_7$	65	$y_{22}=t_{59}\oplus t_{62}$	85	$t_{84}=t_6\oplus t_{31}$
6	$t_5=x_5\oplus x_{21}$	26	$t_{25}=x_{12}\oplus t_{10}$	46	$y_{16}=t_{20}\oplus t_{44}$	66	$y_{25}=t_{20}\oplus t_{64}$	86	$y_{24}=t_{60}\oplus t_{84}$
7	$t_6=x_{14}\oplus x_{31}$	27	$t_{26}=x_1\oplus x_{10}$	47	$t_{46}=x_{30}\oplus t_{39}$	67	$t_{66}=x_{17}\oplus t_{33}$	87	$t_{86}=t_7\oplus t_{30}$
8	$t_7=x_8\oplus x_{15}$	28	$t_{27}=x_{11}\oplus t_{22}$	48	$t_{47}=x_{14}\oplus t_{46}$	68	$y_9=t_{37}\oplus t_{66}$	88	$y_{18}=t_{31}\oplus t_{86}$
9	$t_8=x_6\oplus x_{23}$	29	$y_{12}=t_{21}\oplus t_{27}$	49	$y_6=t_8\oplus t_{47}$	69	$t_{68}=x_{19}\oplus x_{28}$	89	$t_{88}=t_9\oplus t_{31}$
10	$t_9=x_0\oplus x_7$	30	$t_{29}=x_{18}\oplus t_{26}$	50	$t_{49}=x_{11}\oplus x_{29}$	70	$y_{20}=t_{29}\oplus t_{68}$	90	$y_1=t_{32}\oplus t_{88}$
11	$t_{10}=x_{13}\oplus x_{29}$	31	$t_{30}=x_{17}\oplus x_{26}$	51	$y_{21}=t_{36}\oplus t_{49}$	71	$t_{70}=x_{21}\oplus t_{22}$	91	$t_{90}=x_2\oplus x_{18}$
12	$t_{11}=x_{22}\oplus t_0$	32	$t_{31}=x_{16}\oplus t_8$	52	$t_{51}=x_2\oplus t_{27}$	72	$y_{29}=t_{23}\oplus t_{70}$	92	$t_{91}=t_7\oplus t_{32}$
13	$t_{12}=t_1\oplus t_2$	33	$t_{32}=x_9\oplus x_{25}$	53	$y_3=t_{29}\oplus t_{51}$	73	$t_{72}=x_{25}\oplus y_7$	93	$y_{10}=t_{90}\oplus t_{91}$
14	$y_7=t_3\oplus t_{12}$	34	$t_{33}=x_1\oplus t_7$	54	$t_{53}=x_3\oplus x_{10}$	74	$y_{17}=t_{17}\oplus t_{72}$	94	$t_{93}=x_3\oplus x_{11}$
15	$y_{15}=t_4\oplus t_{12}$	35	$t_{34}=x_{19}\oplus x_{26}$	55	$y_{11}=t_{35}\oplus t_{53}$	75	$t_{74}=x_{25}\oplus t_{33}$	95	$t_{94}=t_5\oplus t_{57}$
16	$t_{15}=x_{16}\oplus t_6$	36	$t_{35}=x_9\oplus t_{34}$	56	$t_{55}=x_7\oplus y_{14}$	76	$y_{27}=t_{34}\oplus t_{74}$	96	$y_{13}=t_{93}\oplus t_{94}$
17	$y_8=x_0\oplus t_{15}$	37	$t_{36}=x_{20}\oplus t_{24}$	57	$y_{31}=t_{44}\oplus t_{55}$	77	$t_{76}=x_{25}\oplus t_{37}$	97	$t_{96}=x_7\oplus t_{42}$
18	$t_{17}=x_{15}\oplus t_{15}$	38	$t_{37}=x_{24}\oplus t_6$	58	$t_{57}=x_{12}\oplus t_{23}$	78	$y_{26}=t_{38}\oplus t_{76}$	98	$t_{97}=t_{46}\oplus y_{13}$
19	$t_{18}=x_{24}\oplus t_8$	39	$t_{38}=x_{18}\oplus t_9$	59	$y_4=t_{24}\oplus t_{57}$	79	$t_{78}=x_{27}\oplus t_{35}$	99	$y_{30}=t_{96}\oplus t_{97}$
20	$y_0=x_8\oplus t_{18}$	40	$t_{39}=x_4\oplus t_5$	60	$t_{59}=y_5\oplus t_{42}$	80	$y_{28}=t_{36}\oplus t_{78}$		

Table 2: An implementation of $\mathscr{M}_{4\times 4}^{\Phi_A}$ with 99 XORs.

4. Comparing our MDS matrices with the state-of-the-art

In Table 3 we compare our matrices with others by different methods in the public literature. We can see that the the implementations cost in hardware of the linear transformations obtained by our approach is comparable with state-of-the-art. Moreover, we can obtain a trade offs between software and hardware implementations for some matrices produced by using using our techniques.

5. Conclusion and Future Work

In this work we have presented some new schemes based on the well-known Lai-Massey and Feistel structures for constructing MDS matrices of size $n = 2k, k = 2$. Combining

Matrix	Involutory	Almost involutory	SLP
$\mathscr{M}_{\mathsf{AES}}$ [21]	✗	✗	97
$\mathscr{M}_{\mathsf{KLSW}}$ [17]	✓	✗	84
$\mathscr{M}_{\mathsf{SSCZL}}$ [23]	✓	✓	80
$\mathscr{M}_{\mathsf{SG}}$ [6]	✗	✗	78
$\mathscr{M}_{\mathsf{MM}}$ [22]	✗	✓	83
$\mathscr{M}_{\mathsf{A}}$ [this work]	✓	✓	99

Table 3:A comparison with the sate-of-the-art.

these structures we provide involutory and almost involutory MDS matrices which can be implemented efficiently. We have found some matrices having the MDS property which are very actractive for the so-called lightweight schemes. In the future, we aim to further optimise the search for constructing MDS matrices of size $2k, k \geq 3$ using our aproach.

References

[1] Adnan B. Mustafa C. and Mehmet O. Feistel Like Construction of Involutory Binary Matrices With High Branch Number. Cryptology ePrint Archive, Report 2016/751.

[2] Alferyorov A. P. Zubov A. Y. Kuzmin A. S. Cheryomushkin A. V. Basics of the cryptography. Gelios ARV. 2001. (In Russian)

[3] Boyar J., Matthews P., Peralta R.: Logic minimization techniques with applications to cryptology. J. Cryptology, 26(2):280–312, 2013.

[4] C. Shannon. Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 1949

[5] Dmitry Burov, Boris, Pogorelov. The influence of linear mapping reducibility on choice of round constants. CTCcrypt 216

[6] Duval S. and Leurent G.: MDS Matrices with Lightweight Circuits. In FSE, volume 2018, pages 48-78. Springer, 2018.

[7] Glukhov M. M., Elizarov V. P., Nechaev A. A. Algebra. LAN. 2015. 595 p. (In Russian)

[8] Hong X., Lin T. Xuejia L. On the recursive construction of MDS matrices for ligtweight Cryptography

[9] H. M. Heys, and S. E. Tavares,The Design of Substitution-Permutation Networks Resistatnt to Diferential and Linear Cryptanalysis, Proceedings of 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, pp. 148-155, 1994.

[10] H. M. Heys, and S. E. Tavares,The Design of Product Ciphers Resistatnt to Diferential and Linear Crypt-analysis, Journal Of Cryptography, Vol. 9, No. 1, pp. 1-19, 1996

[11] H. M. Heys, and S. E. Tavares,Avalanche Characteristics of Substitution-Permutation Encryption Networks.

[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] Junod P. and Vaudenay S.: Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices, Selected Areas in Cryptography 2004: Waterloo, Canada, August 9-10,2004. Revisited papers,LNCS. Springer-Verlag. Journal Information Security Practice and Experience, Springer pp 552-563. 2014.

[14] Jorge N. and Elcio A. A New Involutory MDS Matrix for the AES. International Journal of Network Security, Vol.9, No.2, PP.109–116, 2009

[15] Jian G., Thomas P. and Axel P. The PHOTON Family of Lightweight Hash Functions. Cryptology ePrint Archive, Report 2011/609.

[16] Kishan C. G., Sumit K. P. and Ayineedi Venkateswarlu. On the direct construction of recursive MDS matrices. Springer 2016.

[17] Kranz H., Leander G., Stoffelen K., and Wiemer F. Shorter Linear Straight-Line Programs for MDS Matrices. In FSE, volume 2017, pages 188-211. Springer, 2017.

[18] Lidl, R., and Niederreiter, H. Finite Fields, vol. 20 of Encyclopedia of Mathematics

[19] Mahdi S. and Mohsen M. Construction of Lightweight MDS Matrices from Generalized Feistel Structures. Cryptology ePrint Archive, Report 2018/1072.

[20] Mahdi S., Mohammad D., Hamid M. and Behnaz O. On construction of involutory MDS matrices from Vandermonde Matrices in $GF(2^q)$. Springer. Published November 2011.

[21] NIST. Advanced Encryption Standard. Federal Information Processing Standard (FIPS) 197,November 2001.

[22] Sajadieh M., and Mousavi M.: Construction of Lightweight MDS Matrices from Generalized Feistel Structures. Cryptology ePrint Archive, Report 2018/1072.

[23] Shun Li1, Siwei Sun1, Chaoyun Li Zihao Wei1 and Lei Hu1: Constructing Low-latency Involutory MDS Matrices with Lightweight Circuits. In FSE. Springer, 2019.