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

Ramses R. Aulet
Reinier A. de la Cruz Jiménez

Institute of Cryptography, Havana University, Cuba

September 15, 2020

Introducction

Properties

- Diffusion
- Confusion

Lineal Transformation: MDS matrices

Practical point of view

Matrix should be implemented efficiently both in software/hardware

Methods

- Cauchy and Hadamard
- Coding Theory

Introducction

Properties

- Diffusion
- Confusion

Lineal Transformation: MDS matrices

Practical point of view

Matrix should be implemented efficiently both in software/hardware

Methods

- Cauchy and Hadamard
- Coding Theory

- Adnan B. Mustafa C. and Mehmet O.
  Feistel Like Construction of Involutory BinaryMatrices With High Branch Number
- Mahdi S. and Mohsen M.

  Construction of Lightweight MDS Matrices from Generalized Feistel Structures

The aim of this work is to build involutory or almost involutory MDS matrices combining the Feistel, Misty and Lai-Massey schemes.

- Adnan B. Mustafa C. and Mehmet O.
  Feistel Like Construction of Involutory BinaryMatrices With High Branch Number
- Mahdi S. and Mohsen M.

  Construction of Lightweight MDS Matrices from Generalized Feistel Structures

The aim of this work is to build involutory or almost involutory MDS matrices combining the Feistel, Misty and Lai-Massey schemes.

Definition and Notation

- $P = GF(2^t) = GF(2)[x]/g(x)$—finite field with 2^t elements, for some irreducible polynomial $g(x)$ of degree t;
- P^n—vector space of dimension n over P;
- $P_{n,n}$—the ring of $n \times n$ matrices over finite field P;
- 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 $\vec{a} \in P^n$, i.e. the number of its nonzero coordinates;
- $\omega(\mathcal{M})$—the number of 1's in the matrix $\mathcal{M}$;
- Ψ^{-1}—the inverse transformation to some invertible mapping Ψ;
- $I_{n,n}$—the identity matrix of $P_{n,n}$.
- $O_{n,n}$—the zero matrix of $P_{n,n}$.

Involutive Transform

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.

Lineal Transform

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

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

Involutive Transform

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.

Lineal Transform

An transformation φ :$P^n \to P^n$ is called linear transformation, if the following relation holds

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

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 $\vec{\alpha}$.

Branch Number

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

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

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

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

Almost Involutori Matrix

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 $\mathcal{M}_{2\times 2} = \begin{pmatrix} 1 & C \\ C & E \end{pmatrix} \in P_{2,2}$. It can be easy checked that $\mathcal{M}^{-1}_{2\times 2} = \begin{pmatrix} E & C \\ C & 1 \end{pmatrix} \in P_{2,2}$
- Matrix of cipher Kuznyechik

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

Almost Involutori Matrix

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 $\mathcal{M}_{2\times 2} = \begin{pmatrix} 1 & C \\ C & E \end{pmatrix} \in P_{2,2}$. It can be easy checked that $\mathcal{M}^{-1}_{2\times 2} = \begin{pmatrix} E & C \\ C & 1 \end{pmatrix} \in P_{2,2}$
- Matrix of cipher Kuznyechik

Preprosition

If $A \in P_{n,n}$ is an involutory MDS matrix and $\Pi \in P_{n,n}$ is permutation matrix then the matrix $A\Pi$ and ΠA are almost involutory MDS.

Characteristic Polynomial

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

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

DXC and GO

1. **Direct XOR Count**. Given a matrix $\mathcal{M} \in GF(2)_{t\times n,t\times n}$, the direct XOR count DXC($\mathcal{M}$) of $\mathcal{M}$ is $\omega(\mathcal{M}) - nt$. This metric corresponds to counting the number of gates used in a naive implementation of the linear mapping $\mathcal{M}$.
2. **Global Optimization**. For a matrix $\mathcal{M} \in GF(2)_{t\times n,t\times n}$, it is posible to obtain an estimation of its cost in hardware by finding a good linear straight-line program corresponding to $\mathcal{M}$.

Preprosition

If $A \in P_{n,n}$ is an involutory MDS matrix and $\Pi \in P_{n,n}$ is permutation matrix then the matrix $A\Pi$ and ΠA are almost involutory MDS.

Characteristic Polynomial

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

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

DXC and GO

1. **Direct XOR Count**. Given a matrix $\mathcal{M} \in GF(2)_{t\times n, t\times n}$, the direct XOR count DXC($\mathcal{M}$) of $\mathcal{M}$ is $\omega(\mathcal{M}) - nt$. This metric corresponds to counting the number of gates used in a naive implementation of the linear mapping $\mathcal{M}$.
2. **Global Optimization**. For a matrix $\mathcal{M} \in GF(2)_{t\times n, t\times n}$, it is posible to obtain an estimation of its cost in hardware by finding a good linear straight-line program corresponding to $\mathcal{M}$.

Transformations Lai-Massey, Feistel and Misty

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 $\mathcal{L} \in P_{n,n}$

Lai-Massey-like transformation:

$$\varphi_1(\vec{x}) = \left(\vec{x_1} \oplus \mathcal{L}(\vec{x_1} \oplus \vec{x_2})\right) \Big|\Big| \left(\vec{x_2} \oplus \mathcal{L}(\vec{x_1} \oplus \vec{x_2})\right).$$

Feistel-like transformation:

$$\varphi_2(\vec{x}) = \left(\vec{x_1} \oplus \mathcal{L}(\vec{x_2})\right) \Big|\Big| \vec{x_2}.$$

Misty-like transformation:

$$\varphi_3(\vec{x}) = \mathcal{L}(\vec{x_1} \oplus \vec{x_2}) \Big|\Big| \vec{x_2}.$$

Let be $n = 4$ and $f_1(x) = x^2 \oplus x \oplus 1$, $f_2(x) = x^4 \oplus x^3 \oplus 1$, $f_3(x) = x^4 \oplus x^3 \oplus x^2 \oplus x \oplus 1$—some polynomials over field P. In the following we work in the field $P = GF(2^8)$.

Transformations Lai-Massey, Feistel and Misty

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 $\mathcal{L} \in P_{n,n}$

Lai-Massey-like transformation:

$$\varphi_1(\vec{x}) = \left(\vec{x_1} \oplus \mathcal{L}(\vec{x_1} \oplus \vec{x_2})\right) \Big|\Big| \left(\vec{x_2} \oplus \mathcal{L}(\vec{x_1} \oplus \vec{x_2})\right).$$

Feistel-like transformation:

$$\varphi_2(\vec{x}) = \left(\vec{x_1} \oplus \mathcal{L}(\vec{x_2})\right) \Big|\Big| \vec{x_2}.$$

Misty-like transformation:

$$\varphi_3(\vec{x}) = \mathcal{L}(\vec{x_1} \oplus \vec{x_2}) \Big|\Big| \vec{x_2}.$$

Let be $n = 4$ and $f_1(x) = x^2 \oplus x \oplus 1$, $f_2(x) = x^4 \oplus x^3 \oplus 1$, $f_3(x) = x^4 \oplus x^3 \oplus x^2 \oplus x \oplus 1$—some polynomials over field P. In the following we work in the field $P = GF(2^8)$.

Construction 1

Construction of $\mathcal{M}_{n\times n}^{\Phi_A}$

Let be $\Phi_A = \varphi_2 \circ \varphi_1 \circ \varphi_2$. Then $\mathcal{M}_{4\times 4}^{\Phi_A} = A_{\vec{\alpha_4}}(\Phi_A)$;

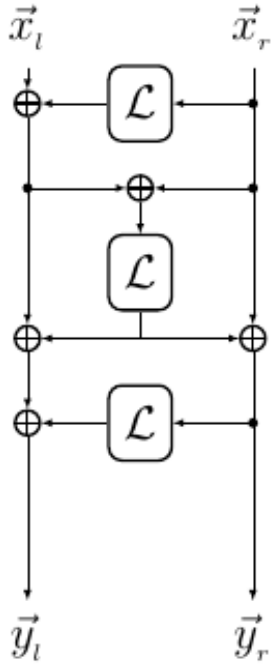

Fig. 1: Structure of Φ_A.

Proposition

Let be an element $a \in P^*$, $a \neq 1$ for which $f_1(a) \neq 0$. The matrix $\mathcal{M}_{4\times 4}^{\Phi_A}$ of transformation Φ_A with $\mathcal{L} = \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix}$ is an involutory MDS matrix.

$$\mathcal{M}_{4\times 4}^{\Phi_A} = \begin{pmatrix} a^2 \oplus a & 1 & a & 1 \\ 1 & a^2 \oplus a & 1 & a \\ a^3 & a^2 & a^2 \oplus a & 1 \\ a^2 & a^3 & 1 & a^2 \oplus a \end{pmatrix}$$

Construction 2

Construction of $\mathcal{M}_{n\times n}^{\Phi_B}$

Let be $\Phi_B = \varphi_1 \circ \varphi_2 \circ \varphi_1$. Then $\mathcal{M}_{4\times 4}^{\Phi_B} = A_{\vec{\alpha_4}}(\Phi_B)$;

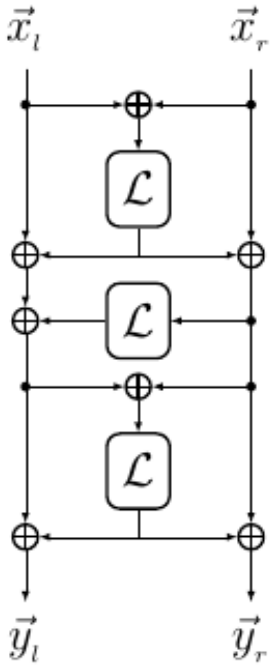

Fig. 2: Structure of Φ_B.

Proposition

Let be an element $a \in P^*$, $a \neq 1$, for which $f_1(a) \neq 0$ then the matrix $\mathcal{M}_{4\times 4}^{\Phi_B}$ of transformation Φ_B with $\mathcal{L} = \begin{pmatrix} 1 & 1 \\ a & 1 \end{pmatrix}$ is an involutory MDS.

$$\mathcal{M}_{4\times 4}^{\Phi_B} = \begin{pmatrix} 1 & a\oplus 1 & a\oplus 1 & a\oplus 1 \\ a^2\oplus a & 1 & a^2\oplus a & a\oplus 1 \\ a & a & 1 & a\oplus 1 \\ a^2 & a & a^2\oplus a & 1 \end{pmatrix}$$

Construction 3

Construction of $\mathcal{M}_{n\times n}^{\Phi_C}$

Let be $\Phi_C = \varphi_3 \circ \varphi_2 \circ \varphi_3^{-1}$. Then $\mathcal{M}_{4\times 4}^{\Phi_C} = A_{\vec{\alpha_4}}(\Phi_C)$;

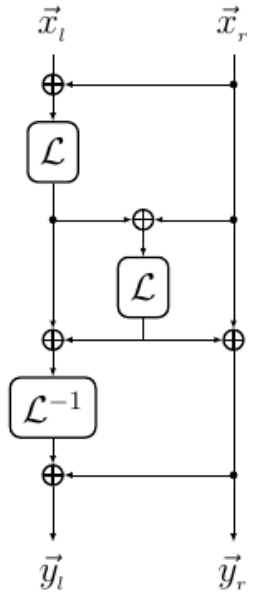

Fig. 3: Structure of Φ_C.

Proposition

Let be an element $a \in P^*$, $a \neq 1$ for which $f_i(a) \neq 0$ where $i = 1, 2, 3$ then the matrix $\mathcal{M}_{4\times 4}^{\Phi_C}$ of transformation Φ_C with $\mathcal{L} = \begin{pmatrix} a & 1 \\ a & a^2 \end{pmatrix}$ is an involutory MDS matrix.

Ortomotphism

Ortomorphism

The linear mapping $\mathcal{L} : P^k \to P^k$, defined as $\mathcal{L}(\vec{a}) = \vec{a} \cdot A$, where $\vec{a} \in P^k, A \in P^*_{k,k}$ is called a linear orthomorphism if the matrix $A \oplus I_{k \times k}$ is invertible over P.

$$\Pi_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \Pi_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$\mathcal{M}^{\Phi_A}_{4\times 4} \circ \Pi_1 \qquad \mathcal{M}^{\Phi_B}_{4\times 4} \circ \Pi_2 \qquad \mathcal{M}^{\Phi_C}_{4\times 4} \circ \Pi_3$$

Ortomotphism

Ortomorphism

The linear mapping $\mathcal{L} : P^k \to P^k$, defined as $\mathcal{L}(\vec{a}) = \vec{a} \cdot A$, where $\vec{a} \in P^k, A \in P^*_{k,k}$ is called a linear orthomorphism if the matrix $A \oplus I_{k \times k}$ is invertible over P.

$$\Pi_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \Pi_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$\mathcal{M}^{\Phi_A}_{4\times 4} \circ \Pi_1$ $\mathcal{M}^{\Phi_B}_{4\times 4} \circ \Pi_2$ $\mathcal{M}^{\Phi_C}_{4\times 4} \circ \Pi_3$

Ortomotphism

Ortomorphism

The linear mapping $\mathcal{L} : P^k \to P^k$, defined as $\mathcal{L}(\vec{a}) = \vec{a} \cdot A$, where $\vec{a} \in P^k, A \in P^*_{k,k}$ is called a linear orthomorphism if the matrix $A \oplus I_{k \times k}$ is invertible over P.

$$\Pi_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \Pi_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$\mathcal{M}^{\Phi_A}_{4\times 4} \circ \Pi_1 \qquad \mathcal{M}^{\Phi_B}_{4\times 4} \circ \Pi_2 \qquad \mathcal{M}^{\Phi_C}_{4\times 4} \circ \Pi_3$$

Some exampel

Matrix M	$\mathcal{L}$	Finite field P	Involutory	Almost involotory	$\mathcal{N}_1(M)$	$\chi_M(x)$	$\chi_M(x)$ is irreducible over P	Factorization of $\chi_M(x)$
$\mathcal{M}^{\Phi_A}_{4\times4} = \begin{pmatrix} 08 & 04 & 06 & 01 \\ 04 & 08 & 01 & 06 \\ 06 & 01 & 02 & 01 \\ 01 & 06 & 01 & 02 \end{pmatrix}$	$\begin{pmatrix} 02 & 01 \\ 01 & 02 \end{pmatrix}$	$GF(2^8)/0x1C3$	No	Yes	6	$x^4 \oplus 0Fx^2 \oplus 01$	No	$(x^2 \oplus 0Fx \oplus 01)^2$
$\mathcal{M}^{\Phi_A}_{4\times4} = \begin{pmatrix} 06 & 01 & 08 & 04 \\ 01 & 06 & 04 & 08 \\ 02 & 01 & 06 & 01 \\ 01 & 02 & 01 & 06 \end{pmatrix}$	$\begin{pmatrix} 02 & 01 \\ 01 & 02 \end{pmatrix}$	$GF(2^8)/0x1C3$	yes	no	6	$(x \oplus 1)^4$	No	$(x \oplus 1)^4$
$\mathcal{M}^{\Phi_A}_{4\times4} = \begin{pmatrix} 9B & 01 & 56 & 43 \\ 01 & 47 & 43 & 01 \\ 56 & 43 & 56 & 04 \\ 43 & 01 & 04 & 01 \end{pmatrix}$	$\begin{pmatrix} 04 & 01 \\ 56 & 04 \end{pmatrix}$	$GF(2^8)/0x11C$	No	Yes	5	$x^4 \oplus 8Bx^3 \oplus 1Bx^2 \oplus 8Bx \oplus 01$	Yes	–
$\mathcal{M}^{\Phi_B}_{4\times4} = \begin{pmatrix} 01 & 06 & 02 & 04 \\ 03 & 01 & 02 & 02 \\ 03 & 06 & 01 & 06 \\ 03 & 03 & 03 & 01 \end{pmatrix}$	$\begin{pmatrix} 01 & 01 \\ 02 & 01 \end{pmatrix}$	$GF(2^8)/0x1C3$	Yes	No	4	$(x \oplus 1)^4$	No	$(x \oplus 1)^4$
$\mathcal{M}^{\Phi_B}_{4\times4} = \begin{pmatrix} 06 & 02 & 04 & 01 \\ 01 & 02 & 02 & 03 \\ 06 & 01 & 06 & 03 \\ 03 & 03 & 01 & 03 \end{pmatrix}$	$\begin{pmatrix} 01 & 01 \\ 02 & 01 \end{pmatrix}$	$GF(2^8)/0x1C3$	No	Yes	4	$x^4 \oplus x^3 \oplus 0Fx^2 \oplus 02x \oplus 1$	No	$(x \oplus 6f)(x^3 \oplus 6Ex^2 \oplus D2x \oplus 24)$
$\mathcal{M}^{\Phi_B}_{4\times4} = \begin{pmatrix} 01 & 02 & 8F & 01 \\ 02 & 08 & 01 & 0C \\ 8F & 01 & 8F & 03 \\ 01 & 0C & 03 & 0C \end{pmatrix}$	$\begin{pmatrix} 01 & 04 \\ 8E & 01 \end{pmatrix}$	$GF(2^8)/0x1C3$	No	Yes	5	$x^4 \oplus 8Ax^3 \oplus FAx^2 \oplus 8Ax \oplus 01$	Yes	–
$\mathcal{M}^{\Phi_C}_{4\times4} = \begin{pmatrix} 05 & 0e & 07 & 0c \\ 07 & 017 & 06 & 13 \\ 06 & 0c & 05 & 0e \\ 06 & 12 & 07 & 17 \end{pmatrix}$	$\begin{pmatrix} 02 & 01 \\ 02 & 04 \end{pmatrix}$	$GF(2^8)/0x1C3$	Yes	No	0	$(x \oplus 1)^4$	No	$(x \oplus 1)^4$
$\mathcal{M}^{\Phi_C}_{4\times4} = \begin{pmatrix} 07 & 0e & 0c & 05 \\ 06 & 17 & 13 & 07 \\ 05 & 0c & 0e & 06 \\ 07 & 12 & 17 & 06 \end{pmatrix}$	$\begin{pmatrix} 02 & 01 \\ 02 & 04 \end{pmatrix}$	$GF(2^8)/0x1C3$	No	Yes	0	$x^4 \oplus 18x^3 \oplus 1Ax^2 \oplus 1Ax \oplus 1$	No	$(x \oplus 37)(x \oplus CC)(x^2 \oplus E3x \oplus F)$
$\mathcal{M}^{\Phi_C}_{4\times4} = \begin{pmatrix} 87 & CB & 93 & 17 \\ 28 & 1D & 7B & 36 \\ CB & 87 & 16 & 93 \\ 1D & 29 & 36 & 7B \end{pmatrix}$	$\begin{pmatrix} 84 & 4C \\ 4D & 35 \end{pmatrix}$	$GF(2^8)/0x1C3$	No	Yes	0	$x^4 \oplus F7x^3 \oplus 65x^2 \oplus F7x \oplus 1$	Yes	–

Implementation of concrete $\mathcal{M}_{4\times4}^{\Phi_A}$

Software and Hardware implementation of matrix

$$\mathcal{M}_{4\times4}^{\Phi_A} = \begin{pmatrix} 01 & 07 & E1 & 03 \\ E1 & 04 & E1 & 02 \\ 01 & 03 & E0 & 01 \\ 01 & E8 & 90 & E5 \end{pmatrix} \in P_{4,4},$$

where $\mathcal{M}_{4\times4}^{\Phi_A} \in P_{4,4}$, $P = GF(2^8)/0x1C3$.

Software

```
uint32_t M (uint32_t x){
  uint8_t a = x, b = x>>8, c = x>>16, d = x>>24, e1, e2;
  d ^= Mult(0xE1,a)      ^ Mult(0x2,b);
  c ^= Mult(0x2   ,(a^b)) ^ a;
  e1 = Mult(0xE1,(a^b^c^d));
  e2 = Mult(0x2   ,(a^b^c^d)) ^ (b^d);
  d ^= e1;
  c ^= e2;
  b ^= e1;
  a ^= e2;
  d ^= Mult(0xE1, a)      ^ Mult(0x2,b);
  c ^= Mult(0x2   ,(a^b)) ^ a;
  return ((((((uint32_t)d<<8)|c)<<8)|b)<<8)|a;
}
```

Where *Mult(x,y)* is the multiplication x and y over field.

Hardware

$$\mathcal{M}_{4\times4}^{\Phi_A} = \mathcal{M}_{32\times32}^{\Phi_A} =$$

$$\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&0&1&0&1&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&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)$$

#	Operación	#	Operación	#	Operación	#	Operación	#	Operación
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	$y_{28} = t_{36} \oplus t_{78}$		

$$\mathrm{DXC}(\mathcal{M}^{\Phi_A}_{32\times 32}) = 199 \text{ and } \mathrm{GO}(\mathcal{M}^{\Phi_A}_{32\times 32}) = 80$$

Comparing our Matrices with State of the Art

Matrix	Involutory	Almost involutory	SLP
$\mathcal{M}_{\text{AES}}$	✗	✗	97
$\mathcal{M}_{\text{KLSW}}$	✓	✗	84
$\mathcal{M}_{\text{SSCZL}}$	✓	✓	80
$\mathcal{M}_{\text{SG}}$	✗	✗	78
$\mathcal{M}_{\text{MM}}$	✗	✓	83
$\mathcal{M}_{A}$ [this work]	✓	✓	80

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

Conclusion

- In this work we have presented some new schemes based on the well-known Feistel, Misty and Lai-Massey structures for constructing MDS matrices of size $n = 2k, k = 2$ over field $GF(2^8)$.
- Combining these structures we provide involutory and almost involutory MDS matrices which can be implemented efficiently.
- Our results can be generalized for the case of any field although it is necessary to say that with our constructions main MDS is not obtained over field $GF(2^2)$.

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

Ramses R. Aulet
Reinier A. de la Cruz Jiménez

Institute of Cryptography, Havana University, Cuba

September 15, 2020