Construction of orthomorphic MDS matrices with primitive characteristic polynomial

Oliver Coy Puente and Reynier A. de la Cruz Jiménez

Institute of Criptography, Havana University, Cuba

September 15, 2020

Contents

Contents

Motivation

1. In recent years, there has been a lot of work on the construction and characterization of MDS matrices with a low implementation cost, in the context of the so-called lightweight schemes.
2. But, many authors does not pay attention to the influence of reducibility of the proposed linear MDS mappings and as a consequence an adversary can exploit the nontrivial invariant subspaces associated to these matrices.
3. We consider the problem of building an special kind of linear mappings (here called orthomorphic MDS mappings) with primitive characteristic polynomial and acceptable implementation cost having the following advantages, such as no non-zero fixed points and better resistance again the so-called invariant subspace attacks.

Contents

Let be $k \geqslant 2, Q = \text{GF}(q) = \text{GF}(p)[x]/q(x)$ the finite field of $q = p^n$ elements, where $q(x)$ is a es irreducible polynomial of degree n over $\text{GF}(p)$ and p is a prime number.
For the proposed matrices we have obtained some results relate with its characteristic polynomial.

Proposition

Let be $Q = GF(q)$ and $f(x) \in Q[x]$ an irreducible polynomial of degree k over Q. Then for any integer $i \in \{1, \ldots, k-1\}$ the following equality holds

$$\chi_{S_f^{q^i}}(x) = f(x).$$

Proposition

Let be $Q = GF(q)$ and $f(x) \in Q[x]$ a primitive polynomial of degree k over Q. Then for any integer $t \in \{1, \ldots, q^k - 1\}$ such that $(t, q^k - 1) = 1$, the polynomial $\chi_{S_f^t}(x)$ is primitive over Q.

Proposition

Let be $f(x) \in Q[x]$ a primitive polynomial over Q, then for any integer $t < q^{\frac{k}{2}}$:

1. *$m_{S_f^t}(x)$ is an irreducible polynomial over Q;*
2. *$deg(m_{S_f^t}(x)) = k$.*

Notice that the results of propositions 1, 2 and 3 allow us to describe some integers t, for which the linear mapping $\mathcal{L} : Q^k \to Q^k$, defined as $\mathcal{L}(\vec{a}) = \vec{a} \cdot S_f^t$, where $\vec{a} \in Q^k$, does not have invariant subspaces when $f(x) \in Q[x]$ is a primitive polynomial.

In what follows, we shall consider the field Q of even characteristic, i.e., $p = 2$.

Definition

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

Proposition

For all $\vec{a} \in Q^k$ and any invertible matrix $A \in Q_{k,k}$ the linear transformation $\mathcal{L} : Q^k \to Q^k$, defined as $\mathcal{L}(\vec{a}) = \vec{a} \cdot A$ is a linear orthomorphism if and only if $\mathcal{L}$ has no non-zero fixed points.

Proposition

Let be A an invertible matrix of size $k \times k$ over Q. Then for any $\alpha \in Q^*$ the matrix $\alpha \cdot I_{k \times k} \oplus A$ is invertible over Q if and only if $(x \oplus \alpha) \nmid \chi_A(x)$.

Corollary

If the polynomial $\chi_{S_f}(x) \in Q[x]$ is primitive over Q, then for any $\alpha \in Q^*$ the matrix $\alpha \cdot I_{k\times k} \oplus S_f^t \in Q_{k,k}$ is invertible for any integer t such that the following conditions holds:

1. $t < 2^{\frac{k}{2}}$;
2. $t \in \{1, \ldots, 2^k - 1\}$ *with* $(t, 2^k - 1) = 1$.

Definition

A matrix $A \in Q_{k,k}$ is said to be an orthomorphic MDS matrix if both matrices A and $A \oplus I_{k\times k}$ have the MDS property over Q.

Contents

In this section we study the possibility of constructing orthomorphic MDS matrices from companion matrices.
We propose a method for constructing 4×4 orthomorphic MDS matrices with primitive characteristic polynomial from the companion matrix of the polynomial

$$f(x) = x^4 \oplus \gamma^{-1}x^3 \oplus \gamma^t x^2 \oplus \gamma^{-1}x \oplus \gamma \in Q[x]. \quad (1)$$

Proposition

Let be $Q = GF(2^8)$, $\gamma \in Q$ a primitive element, $f(x) \in Q[x]$ a polynomial of the form (1). If $t \in \{2, \ldots, 254\}$ is a prime number and $f(x)$ is an irreducible polynomial over Q, then the matrix S_f^4 is an orthomorphic MDS matrix.

Analogously, to the previous case we propose a construction of orthomorphic MDS matrices of size 6×6 with primitive characteristic polynomial from the companion matrix of the polynomial

$$g(x) = x^6 \oplus \gamma_1 x^5 \oplus \gamma_2 x^4 \oplus \gamma_3 x^3 \oplus \gamma_2 x^2 \oplus \gamma_1 x \oplus \gamma \in Q[x]. \qquad (2)$$

Proposition

Let be $\gamma \in Q = GF(2^8)$ a primitive element and $g(x) \in Q[x]$ a polynomial of the form (2). If $(\gamma_1, \gamma_2, \gamma_3) \in \{(\gamma^{-3}, \gamma^{-4}, \gamma^4), ((\gamma \oplus 1)^{-1}, \gamma^3, \gamma^2), ((\gamma \oplus 1)^{-1}, \gamma^{-1} \oplus 1, \gamma), (\gamma^{-2} \oplus 1, \gamma^{-1}, \gamma^{-1} \oplus 1)\}$, then the matrix S_g^6 is an orthomorphic MDS matrix.

Contents

As we can see in the next definition, the companion matrix is a particular case of the $\mathcal{P}$ - companion matrix – a new concept which is defined as follows.

Definition

Let be $f(x) = f_0 - f_1x - f_2x^2 - \ldots - f_{k-2}x^{k-2} - f_{k-1}x^{k-1} - x^k \in Q[x]$, the matrix $S_f(\mathcal{P}_{(k-1)\times(k-1)}) \in Q_{k,k}$, defined as

$$S_f(\mathcal{P}) = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & f_0 \\ & & & f_1 \\ & & & \vdots \\ & \mathcal{P}_{(k-1)\times(k-1)} & & \vdots \\ & & & f_{k-2} \\ & & & f_{k-1} \end{array}\right)_{k\times k}$$

is called $\mathcal{P}$ - companion matrix of the polynomial $f(x)$, where $\mathcal{P}_{(k-1)\times(k-1)}$ is a permutation matrix.

Let be $h(x) = x^k \oplus \bigoplus_{i=0}^{k-1} h_i x^i$, $h^{\downarrow} = (h_1, \ldots, h_{k-1})^{\top}$, $f^{\downarrow} = (f_1, \ldots, f_{k-1})^{\top} = \mathcal{P}_{(k-1)\times(k-1)} \cdot h^{\downarrow}$, where $\mathcal{P}_{(k-1)\times(k-1)} = (p_{ij})_{(k-1)\times(k-1)}$ is a permutation matrix.

In this section we study the possibility of constructing orthomorphic MDS matrices from $\mathcal{P}$ - companion matrices of the polynomial $h(x)$. Permutations matrices for which $\chi_{S_h(\mathcal{P}_{(k-1)\times(k-1)})}(x) = f(x)$ are of particular interest, where $f(x) = x^k \oplus \bigoplus_{i=0}^{k-1} f_i x^i$, and $f_0 = h_0$.

If $f(x)$ is an irreducible polynomial over Q, then from proposition 3 follows that for any integer $t < q^{\frac{k}{2}}$ the matrix $(S_h(\mathcal{P}_{(k-1)\times(k-1)}))^t$ has an irreducible characteristic polynomial. In this case the coefficients of the polynomial $h(x)$ can be defined according to the following rule

$$h_i = \begin{cases} 1, & i = k \\ \bigoplus_{j=1}^{k-1} \hat{p}_{ij} f_j, & i \in \overline{1, k-1} \\ f_0, & i = 0 \end{cases},$$

where $\mathcal{P}^{-1} = (\hat{p}_{ij})_{(k-1)\times(k-1)}$.

For $k = 4$ we propose a method for constructing 4×4 orthomorphic MDS matrices with primitive characteristic polynomial of the form (1) using the so-called $\mathcal{P}$ - companion matrices of the polynomial h, which is defined as

$$h(x) = x^4 \oplus \gamma^{-1}x^3 \oplus \gamma^{-1}x^2 \oplus \gamma^t x \oplus \gamma. \tag{3}$$

Proposition

Let be $Q = GF(2^8)$, $\gamma \in Q$ a primitive element, $f(x) \in Q[x]$ a polynomial of the form (1) and

$$\mathcal{P}_{3\times 3} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

If $t \in \{2, \ldots, 254\}$ is a prime number and $f(x)$ is an irreducible polynomial over Q, then the matrix $(S_h(\mathcal{P}_{3\times 3}))^4$ is an orthomorphic MDS matrix, where $h(x) = x^4 \oplus \gamma^{-1}x^3 \oplus \gamma^{-1}x^2 \oplus \gamma^t x \oplus \gamma$.

It is noteworthy that the use of $\mathcal{P}$ - companion matrices have some effect over simple companion matrices when looking for MDS matrices. For example, the matrix $(S_h(\mathcal{P}_{3\times 3}))^4$ have the MDS property over $Q = GF(2^8) = GF(2)[x]/x^8 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$ for $t = 29$, while the matrix S_h^4 does not exhibits this useful property.

The high level of view of a round of transformations $\vec{a} \cdot S_h^4$ and $\vec{a} \cdot (S_h(\mathcal{P}_{3\times 3}))^4$ is given in Figures 1 and 2 respectively, where $\vec{a} \in Q^4$ and $h(x) \in Q[x]$, $\mathcal{P}_{3\times 3}$ are defined in proposition 8.

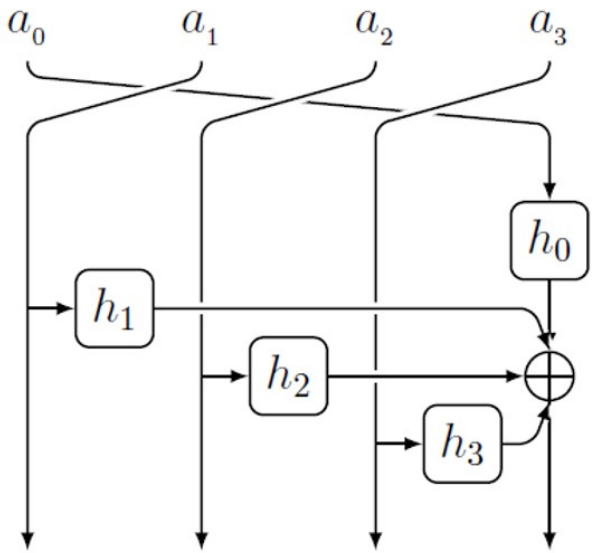

Fig. 1: High level of view of a round of transformation $\vec{a} \cdot S_h^4$

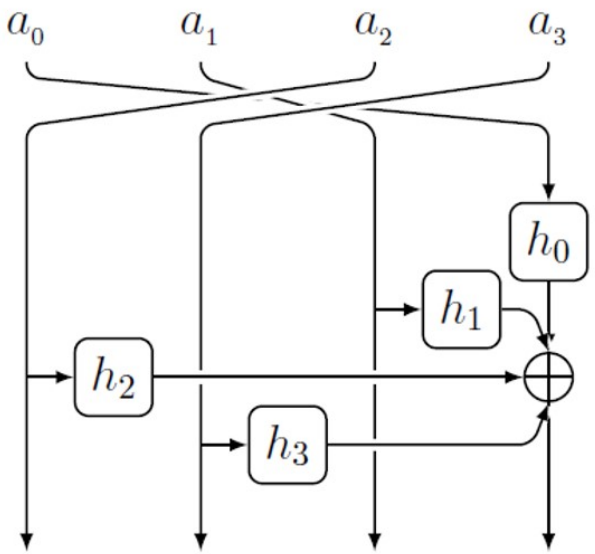

Fig. 2: High level of view of a round of transformation $\vec{a} \cdot (S_h(\mathcal{P}_{3\times 3}))^4$

For $k = 6$ we have constructed orthomorphic MDS over $Q = GF(2^8)$ matrices with primitive characteristic polynomial using the $\mathcal{P}$ - companion matrix of the polynomial $h(x) = x^6 \oplus \bigoplus_{i=0}^{5} h_i x^i$, where for the primitive element γ the coefficients $h_i \in \{1, \gamma, \gamma^{-1}, \gamma^2, \gamma^{-2}, \gamma^3\}$, $i \in \overline{0,5}$ due to the low XOR-count metric of these elements. In table 1 we compile some instances of the $\mathcal{P}$ - companion matrix defined by the polynomial $h(x)$.

Table : Some matrices of the form $(S_h(\mathcal{P}_{5\times 5}))^6$ and it's building blocks.

$h(x) = x^6 \oplus \bigoplus_{i=0}^{5} h_i x^i$	$\mathcal{P}_{5\times 5}$	$S_h(\mathcal{P}_{5\times 5})$	$(S_h(\mathcal{P}_{5\times 5}))^6$
$x^6 \oplus 04x^5 \oplus 04x^4 \oplus 91x^3 \oplus E1x^2 \oplus 91x \oplus 04$	$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 00 & 00 & 00 & 00 & 00 & 04 \\ 00 & 00 & 00 & 01 & 00 & 91 \\ 01 & 00 & 00 & 00 & 00 & E1 \\ 00 & 00 & 00 & 00 & 01 & 91 \\ 00 & 00 & 01 & 00 & 00 & 04 \\ 00 & 01 & 00 & 00 & 00 & 04 \end{pmatrix}$	$\begin{pmatrix} 04 & 1B & 10 & C2 & 41 & 7E \\ 91 & 1E & 90 & E5 & B4 & 51 \\ E1 & F9 & 06 & C8 & B1 & 64 \\ 91 & 8F & 05 & E2 & 40 & 0D \\ 04 & D3 & F1 & 73 & 47 & 87 \\ 04 & FE & 81 & 76 & D1 & 60 \end{pmatrix}$
$x^6 \oplus 04x^5 \oplus 01x^4 \oplus 08x^3 \oplus 04x^2 \oplus 91x \oplus 04$	$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 00 & 00 & 00 & 00 & 00 & 04 \\ 00 & 00 & 01 & 00 & 00 & 91 \\ 00 & 00 & 00 & 00 & 01 & 04 \\ 01 & 00 & 00 & 00 & 00 & 08 \\ 00 & 00 & 00 & 01 & 00 & 01 \\ 00 & 01 & 00 & 00 & 00 & 04 \end{pmatrix}$	$\begin{pmatrix} 04 & 0F & D3 & 10 & 41 & 8F \\ 91 & 1A & 5C & 05 & A0 & BD \\ 04 & D9 & 76 & 11 & 4D & D8 \\ 08 & CD & 24 & 24 & 92 & D2 \\ 01 & 57 & D6 & 0C & A5 & 9E \\ 04 & 53 & 73 & 81 & 44 & 95 \end{pmatrix}$
$x^6 \oplus E1x^5 \oplus E1x^4 \oplus 08x^3 \oplus 91x^2 \oplus 08x \oplus 04$	$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 00 & 00 & 00 & 00 & 00 & 04 \\ 00 & 00 & 01 & 00 & 00 & 08 \\ 00 & 00 & 00 & 01 & 00 & 91 \\ 00 & 00 & 00 & 00 & 01 & 08 \\ 01 & 00 & 00 & 00 & 00 & E1 \\ 00 & 01 & 00 & 00 & 00 & E1 \end{pmatrix}$	$\begin{pmatrix} 04 & 7A & E0 & 21 & 02 & BA \\ 08 & 2D & 51 & E3 & 95 & 54 \\ 91 & E3 & D9 & 52 & A1 & 8A \\ 08 & C9 & AC & D7 & E5 & C9 \\ E1 & 7E & 3D & AF & 95 & FC \\ E1 & CF & FF & 38 & 99 & AB \end{pmatrix}$

Proposition

Let be $Q = GF(2^8)$. The matrices of the form $(S_h(\mathcal{P}_{5\times 5}))^6$ from table 1 are orthomorphic MDS matrices.

Contents

In this section we study how to construct orthomorphic MDS matrices of the form

$$\left(\mathcal{M}\begin{pmatrix} \gamma_1 & \cdots & \gamma_{\lceil \frac{k}{2} \rceil} \\ \mathcal{R}_{k,k}^{(1)} & \cdots & \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil)} & \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil+1)} \end{pmatrix}\right)^k, \tag{4}$$

with primitive characteristic polynomial, where

$$\mathcal{M}\begin{pmatrix} \gamma_1 & \cdots & \gamma_{\lceil \frac{k}{2} \rceil} \\ \mathcal{R}_{k,k}^{(1)} & \cdots & \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil)} & \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil+1)} \end{pmatrix} = \left(\gamma_1 \cdot \mathcal{R}_{k,k}^{(1)} \oplus \cdots \oplus \gamma_{\lceil \frac{k}{2} \rceil} \cdot \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil)} \oplus \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil+1)}\right),$$

all binay non-zero matrices $\mathcal{R}_{k,k}^{(1)}, \ldots \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil)}, \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil+1)} \in GF(2)_{k,k}$, and in order to achieve an efficiently implementation the finite fields elements $\gamma_1, \ldots, \gamma_{\lceil \frac{k}{2} \rceil}$ belong to the set $\{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}, \alpha^3, \alpha^{-3}\}$ where α is a primitive element.

For $k = 4, 6$ we have performed a search based on random generation of matrices $\mathcal{R}_{k,k}^{(1)}, \ldots \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil)}, \mathcal{R}_{k,k}^{(\lceil \frac{k}{2} \rceil + 1)}$ with few number of 1's and as a result have obtained the following matrices given in tables 2 and 3 having an efficient implementation.

Table : Some matrices of the form (4) and it's building blocks for $k = 4$.

(γ_1, γ_2)	$\left(\mathcal{M}\left(\begin{smallmatrix}\gamma_1 & \gamma_2\\ \mathcal{R}^{(1)}_{4,4} & \mathcal{R}^{(2)}_{4,4} & \mathcal{R}^{(3)}_{4,4}\end{smallmatrix}\right)\right)^4$	$\mathcal{R}^{(1)}_{4,4}$	$\mathcal{R}^{(2)}_{4,4}$	$\mathcal{R}^{(3)}_{4,4}$	$\mathcal{M}\left(\begin{smallmatrix}\gamma_1 & \gamma_2\\ \mathcal{R}^{(1)}_{4,4} & \mathcal{R}^{(2)}_{4,4} & \mathcal{R}^{(3)}_{4,4}\end{smallmatrix}\right)$
(01, E1)	70 90 E1 01 A9 E1 91 48 90 E1 E1 E1 A9 91 90 70	0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0	0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0	00 01 00 01 00 00 00 E1 01 00 00 00 E1 00 01 00
(01, 91)	24 B4 91 01 BC 91 B5 2D B4 91 91 91 BC B5 B4 24	0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0	0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0	00 01 00 01 00 00 00 91 01 00 00 00 91 00 01 00
(A9, E1)	5D B4 A9 01 5E E1 B5 5A B4 A9 E1 A9 5E BC B4 5D	0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0	0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0	0 1 0 1 0 0 0 0 1 0 0 0 0 0 1 0	00 01 00 01 00 00 00 E1 01 00 00 00 A9 00 01 00

Proposition

Let be $Q = GF(2^8)$. *The matrices of the form* $\left(\mathcal{M}\left(\begin{smallmatrix}\gamma_1 & \gamma_2\\ \mathcal{R}^{(1)}_{4,4} & \mathcal{R}^{(2)}_{4,4} & \mathcal{R}^{(3)}_{4,4}\end{smallmatrix}\right)\right)^4$ *from table 2 are orthomorphic MDS matrices.*

Table : Some matrices of the form (4) and it's building blocks for $k = 6$.

$(\gamma_1, \gamma_2, \gamma_3)$	$\left(\mathcal{M}\left(\begin{smallmatrix}\gamma_1 & \gamma_2 & \gamma_3\\ \mathcal{R}^{(1)}_{6,6} & \mathcal{R}^{(2)}_{6,6} & \mathcal{R}^{(3)}_{6,6} & \mathcal{R}^{(4)}_{6,6}\end{smallmatrix}\right)\right)^6$	$\mathcal{R}^{(1)}_{6,6}$	$\mathcal{R}^{(2)}_{6,6}$	$\mathcal{R}^{(3)}_{6,6}$	$\mathcal{R}^{(4)}_{6,6}$	$\mathcal{M}\left(\begin{smallmatrix}\gamma_1 & \gamma_2 & \gamma_3\\ \mathcal{R}^{(1)}_{6,6} & \mathcal{R}^{(2)}_{6,6} & \mathcal{R}^{(3)}_{6,6} & \mathcal{R}^{(4)}_{6,6}\end{smallmatrix}\right)$
$(02, 08, 02)$	$\begin{pmatrix} AF & 01 & 10 & 05 & 48 & 05\\ 88 & 86 & 8A & 90 & 80 & 20\\ F5 & 4D & EB & 15 & 55 & 82\\ 9A & 18 & C8 & 87 & 41 & 95\\ 20 & 10 & 90 & 02 & 86 & 0A\\ 48 & 48 & 44 & 10 & 45 & AF \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 1&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&1&0&0&1\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0\\ 1&1&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&1&0&0 \end{pmatrix}$	$\begin{pmatrix} 00&00&01&00&00&01\\ 00&00&00&00&00&02\\ 00&00&00&00&01&08\\ 01&01&00&00&00&00\\ 02&00&00&00&00&00\\ 08&00&00&01&00&00 \end{pmatrix}$
$(08, 02, 08)$	$\begin{pmatrix} AF & 02 & 10 & 05 & 90 & 05\\ 44 & 86 & 45 & 48 & 80 & 10\\ F5 & 9A & EB & 15 & AA & 82\\ 9A & 30 & C8 & 87 & 82 & 95\\ 10 & 10 & 48 & 01 & 86 & 05\\ 48 & 90 & 44 & 10 & 8A & AF \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 1&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0\\ 0&1&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&1&0&0&1\\ 0&0&0&0&0&1\\ 0&0&0&0&0&0\\ 1&0&0&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&1&0&0 \end{pmatrix}$	$\begin{pmatrix} 00&00&01&00&00&01\\ 00&00&00&00&00&01\\ 00&00&00&00&02&08\\ 01&02&00&00&00&00\\ 01&00&00&00&00&00\\ 08&00&00&01&00&00 \end{pmatrix}$
$(A9, E1, 91)$	$\begin{pmatrix} F8 & 49 & 91 & 86 & 09 & A8\\ 1C & 13 & 66 & 09 & B5 & A9\\ 07 & 8F & E4 & 01 & F7 & 79\\ DD & 2A & 1D & B3 & 8F & 69\\ A9 & A9 & E5 & C5 & 98 & 43\\ A8 & 09 & 1C & A9 & 66 & 73 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 1&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&1&0&0&1\\ 0&0&0&0&0&1\\ 0&0&0&0&1&0\\ 0&1&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&1&0&0 \end{pmatrix}$	$\begin{pmatrix} 00&00&01&00&00&01\\ 00&00&00&00&00&01\\ 00&00&00&00&01&A9\\ A9&01&00&00&00&00\\ E1&00&00&00&00&00\\ 91&00&00&01&00&00 \end{pmatrix}$

Proposition

Let be $Q = GF(2^8)$. *The matrices of the form* $\left(\mathcal{M}\left(\begin{smallmatrix}\gamma_1 & \gamma_2 & \gamma_3\\ \mathcal{R}^{(1)}_{6,6} & \mathcal{R}^{(2)}_{6,6} & \mathcal{R}^{(3)}_{6,6} & \mathcal{R}^{(4)}_{6,6}\end{smallmatrix}\right)\right)^6$ *from table 3 are orthomorphic MDS matrices.*

The high level of view of a round of transformations $\vec{a} \cdot \left(\mathcal{M}\left(\begin{smallmatrix} 01 & E1 \\ \mathcal{R}^{(1)}_{4,4} & \mathcal{R}^{(2)}_{4,4} \; \mathcal{R}^{(3)}_{4,4} \end{smallmatrix}\right)\right)^4$ and $\vec{b} \cdot \left(\mathcal{M}\left(\begin{smallmatrix} 02 & 08 & 02 \\ \mathcal{R}^{(1)}_{6,6} & \mathcal{R}^{(2)}_{6,6} & \mathcal{R}^{(3)}_{6,6} \; \mathcal{R}^{(4)}_{6,6} \end{smallmatrix}\right)\right)^6$ are given in figures 3 and 4, respectively. As we can see these output are the result of a recursive transformations, which can be implemented efficiently. The high level of view of the others matrices displayed in tables 2 and 3 can be represented in a similar fashion to the previous ones.

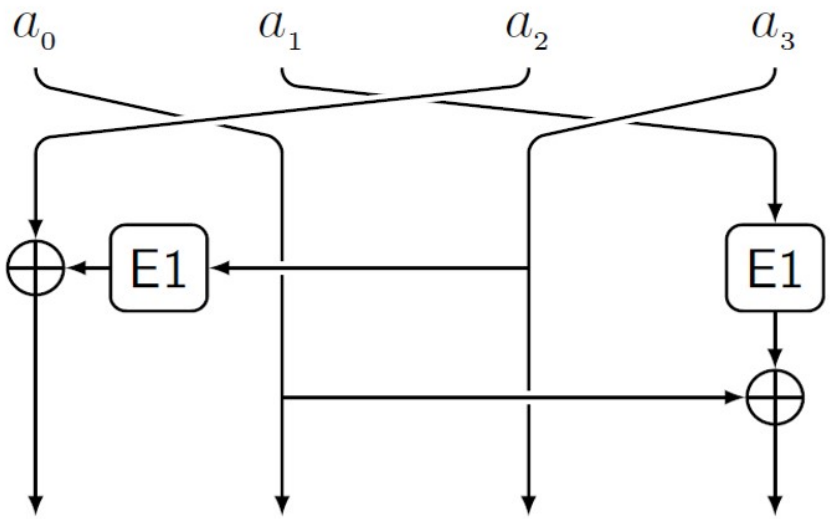

Fig. 3: High level of view of a round of transformation $\vec{a} \cdot \left(\mathcal{M}\begin{pmatrix} 01 & E1 \\ \mathcal{R}^{(1)}_{4,4} & \mathcal{R}^{(2)}_{4,4} \; \mathcal{R}^{(3)}_{4,4} \end{pmatrix}\right)^4$.

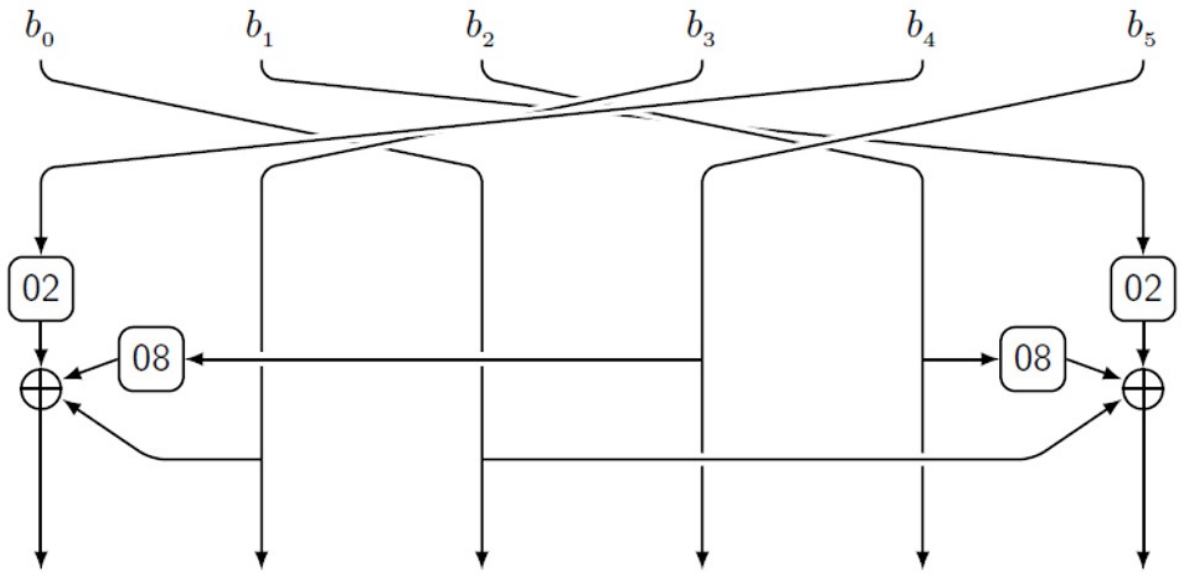

Fig. 4: High level of view of a round of transformation $\vec{b} \cdot \left(\mathcal{M}\left(\begin{smallmatrix} 02 & 08 & 02 \\ \mathcal{R}^{(1)}_{6,6} & \mathcal{R}^{(2)}_{6,6} & \mathcal{R}^{(3)}_{6,6} & \mathcal{R}^{(4)}_{6,6} \end{smallmatrix}\right)\right)^6$.

Contents

XOR-count as a complexity metric

Some authors proposed quantify the complexity of implementing the linear layer of a block cipher by counting the number of bitwise XOR operations, necessary to implement the multiplication of any vector by the linear mappings used as building block to achieve the diffusion property. In this articles we shall use this metric to assess the cost of the proposed constructions.

Let be $f(x),\ g(x) \in Q[x]$ two polynomials of the form (1) and (2), respectively. We have obtained that for $(\gamma, t) = (02, 7)$ and $(\gamma, \gamma_1, \gamma_2, \gamma_3) = (02, 90, \mathrm{E1}, \mathrm{E0})$, $\mathrm{XOR}(S_f^4) = 220$ and $\mathrm{XOR}(S_g^6) = 396$, respectively.
It is not difficult to see that $\mathrm{XOR}(S_f^4) = \mathrm{XOR}((S_h(\mathcal{P}_{3\times 3}))^4) = 220$, where $t = 2,\ h(x) \in Q[x]$ is a polynomial of the form (3) for $\gamma = 02$ and $\mathcal{P}_{3\times 3}$ the permutation matrix of the proposition 8. From table 1 we have that $\mathrm{XOR}((S_h(\mathcal{P}_{5\times 5}))^6) \in \{318, 342, 360\}$ for any permutation matrix $\mathcal{P}_{5\times 5}$, where
$h(x) \in \{x^6 \oplus \mathrm{B4}x^5 \oplus 08x^4 \oplus 01x^3 \oplus \mathrm{B4}x^2 \oplus 08x \oplus \mathrm{B4},\ x^6 \oplus 01x^5 \oplus 04x^4 \oplus 02x^3 \oplus 04x^2 \oplus \mathrm{5A}x \oplus 04,\ x^6 \oplus \mathrm{5A}x^5 \oplus \mathrm{5A}x^4 \oplus 02x^3 \oplus 04x^2 \oplus \mathrm{5A}x \oplus 02\}$, respectively.

From tables 2 and 3 we have that

$$\text{XOR}\left(\left(\mathcal{M}\left(\begin{smallmatrix}01\\ \mathcal{R}^{(1)}_{4,4}\end{smallmatrix}\ \begin{smallmatrix}E1\\ \mathcal{R}^{(2)}_{4,4}\end{smallmatrix}\ \begin{smallmatrix}\\ \mathcal{R}^{(3)}_{4,4}\end{smallmatrix}\right)\right)^4\right) = 88, \quad \text{XOR}\left(\left(\mathcal{M}\left(\begin{smallmatrix}02\\ \mathcal{R}^{(1)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}08\\ \mathcal{R}^{(2)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}02\\ \mathcal{R}^{(3)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}\\ \mathcal{R}^{(4)}_{6,6}\end{smallmatrix}\right)\right)^6\right) = 312,$$

$$\text{XOR}\left(\left(\mathcal{M}\left(\begin{smallmatrix}01\\ \mathcal{R}^{(1)}_{4,4}\end{smallmatrix}\ \begin{smallmatrix}91\\ \mathcal{R}^{(2)}_{4,4}\end{smallmatrix}\ \begin{smallmatrix}\\ \mathcal{R}^{(3)}_{4,4}\end{smallmatrix}\right)\right)^4\right) = 104, \quad \text{XOR}\left(\left(\mathcal{M}\left(\begin{smallmatrix}08\\ \mathcal{R}^{(1)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}02\\ \mathcal{R}^{(2)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}08\\ \mathcal{R}^{(3)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}\\ \mathcal{R}^{(4)}_{6,6}\end{smallmatrix}\right)\right)^6\right) = 312,$$

$$\text{XOR}\left(\left(\mathcal{M}\left(\begin{smallmatrix}A9\\ \mathcal{R}^{(1)}_{4,4}\end{smallmatrix}\ \begin{smallmatrix}E1\\ \mathcal{R}^{(2)}_{4,4}\end{smallmatrix}\ \begin{smallmatrix}\\ \mathcal{R}^{(3)}_{4,4}\end{smallmatrix}\right)\right)^4\right) = 104, \quad \text{XOR}\left(\left(\mathcal{M}\left(\begin{smallmatrix}A9\\ \mathcal{R}^{(1)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}E1\\ \mathcal{R}^{(2)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}91\\ \mathcal{R}^{(3)}_{6,6}\end{smallmatrix}\ \begin{smallmatrix}\\ \mathcal{R}^{(4)}_{6,6}\end{smallmatrix}\right)\right)^6\right) = 324.$$

where the matrices $\mathcal{R}^{(1)}_{4,4}, \mathcal{R}^{(2)}_{4,4}, \mathcal{R}^{(3)}_{4,4}$ and $\mathcal{R}^{(1)}_{6,6}, \mathcal{R}^{(2)}_{6,6}, \mathcal{R}^{(3)}_{6,6}, \mathcal{R}^{(4)}_{6,6}$ are given in table 2 and 3, respectively.

Contents

Conclusion

- We have introduced a new concept of the $\mathcal{P}$ - companion matrix wich not only generalize the notion of companion matrix but also can be used to extend the class of MDS mappings that can be obtained using this kind of matrices.
- We have presented some new constructions based on the use of recursive schemes for generating a special kind of MDS matrices (here called orthomorphic MDS matrices) of dimension 4×4 and 6×6, respectively.

Conclusion

- The main advantage of ours MDS orthomorphic matrices is the absence of invariant subspaces, due to the irreducibility of their characteristic polynomials.
- For the proposed matrices we have analyzed the XOR-count metric and the obtained results shows that these matrices could be attractive for the so-called lightweight schemes offering a good trade offs between security and implementation.

The End

Thanks for your attention!

Questions?