

# Construction of linear involutory transformations over finite fields through the multiplication of polynomials modulus a polynomial

Authors: **Ramsés Rodríguez Aulet, Alejandro Freyre, Pablo Freyre**

# Introduction

Let  $\mathcal{P} = \mathbb{F}_q$  be a finite field of  $q = p^t$  elements being  $p$  a prime number and  $t \in \mathbb{N}$ . We have that  $\mathcal{P}[x]$  is the ring of polynomials having coefficients in  $\mathcal{P}$  and using the polynomial  $F(x) \in \mathcal{P}[x]$  let us build the ring  $\mathcal{R} = \mathcal{P}[x]/_{F(x)}$ . Let  $g(x), \mu(x)$  be elements of  $\mathcal{R}$  we define the transformation  $\Psi : \mathcal{R} \rightarrow \mathcal{R}$  as

$$\Psi(g(x)) = g(x)\mu(x) \bmod F(x). \quad (1)$$

## Our Interest

- Conditions Conditions for the  $\Psi$  transformation to be involutory?
- Construction MDS involutory matrices from  $\Psi$

# Introduction

Let  $\mathcal{P} = \mathbb{F}_q$  be a finite field of  $q = p^t$  elements being  $p$  a prime number and  $t \in \mathbb{N}$ . We have that  $\mathcal{P}[x]$  is the ring of polynomials having coefficients in  $\mathcal{P}$  and using the polynomial  $F(x) \in \mathcal{P}[x]$  let us build the ring  $\mathcal{R} = \mathcal{P}[x]/_{F(x)}$ . Let  $g(x), \mu(x)$  be elements of  $\mathcal{R}$  we define the transformation  $\Psi : \mathcal{R} \rightarrow \mathcal{R}$  as

$$\Psi(g(x)) = g(x)\mu(x) \bmod F(x). \quad (1)$$

## Our Interest

- Conditions for the  $\Psi$  transformation to be involutory?
- Construction MDS involutory matrices from  $\Psi$

# Relation between nilpotent and involutory elements

## Definition

- 1 The element  $r \in \mathcal{R}$ ,  $r \neq 0$  is called a zero divisor if exists  $r' \in \mathcal{R}$ ,  $r' \neq 0$  such that

$$r * r' = 0.$$

- 2 A zero divisor  $r \in \mathcal{R}$  is called nilpotent if exists  $n \in \mathbb{N}$  such that

$$r^n = 0.$$

The lowest  $n = n(r)$  which satisfies the previous property is called nilpotency index.

## Proposition

1. If  $\mathcal{R}$  contains at least one involutory element  $r \in \mathcal{R}$  then  $\mathcal{R}$  contains at least one nilpotent element with nilpotency index 2.
2. Let  $r'$  be one involutory element of  $\mathcal{R}$  then the remaining involutory elements  $r$  are uniquely defined by

$$r = r' + w$$

where  $w$  is a nilpotent element with nilpotency index 2, i.e., any two involutory elements are related by a nilpotent element.

Let denote  $D(2)$  the union of all the ideal  $\mathcal{R}a$  where  $a$  is a nilpotent element with nilpotency index 2 and let  $b \in D(2)$  be a fixed element, then for any  $r \in \mathcal{R}$  such that  $rb \neq 0$  the element

$$a = e + rb \tag{2}$$

is an involutory element. Hence, any transformation  $\Psi : \mathcal{R} \rightarrow \mathcal{R}$  constructed as

$$\Psi(x) = x(e + rb) \tag{3}$$

is a linear involutory transformation.

# Existence criteria

Let be  $\mathcal{P}$  finite field and  $\mathcal{R} = P[x]/_{F(x)}$  where  $F(x) \in P[x]$ , the transformation  $\Psi : \mathcal{R} \rightarrow \mathcal{R}$  is defined as

$$\Psi(g(x)) = g(x)\mu(x) \bmod F(x).$$

considering that  $F(x)$  has canonical factorization

$$F(x) = f_1(x)^{k_1} \cdots f_s(x)^{k_s}$$

with  $\deg(F(x)) = m$  and  $\deg(f_i(x)) = m_i$ , such that  $m = k_1 m_1 + \cdots + k_s m_s$ .

## Proposition

The amount of polynomials  $h(x) \in \mathcal{P}[x]$  such that  $\deg(h(x)) < \deg(F(x))$  and  $\gcd(h(x), F(x)) = 1$  is

$$q^m \left(1 - \frac{1}{q^{m_1}}\right) \cdots \left(1 - \frac{1}{q^{m_t}}\right) \quad (4)$$



## Theorem

The ring  $\mathcal{R}$  contains involutory elements iff one of the following conditions holds

1.  $p$  is an odd value
2. If  $p = 2$  in the canonical factorization of  $F(x)$  exists  $i \in \{1, \dots, t\}$  such that  $k_i \geq 2$ .

## Corollary 1

For any  $n \in \mathbb{N}$ ,  $n > 1$  it is possible to build a ring  $\mathcal{R}$  of  $p^{tn}$  elements which contain involutory elements.

## Corollary 2

For any  $n \in \mathbb{N}$  such that  $n > 1$  exist one linear involutory transformation

$$\Psi : \mathcal{R} \rightarrow \mathcal{R}$$

build by the rule in (1).

## Theorem

The ring  $\mathcal{R}$  contains involutory elements iff one of the following conditions holds

1.  $p$  is an odd value
2. If  $p = 2$  in the canonical factorization of  $F(x)$  exists  $i \in \{1, \dots, t\}$  such that  $k_i \geq 2$ .

## Corollary 1

For any  $n \in \mathbb{N}$ ,  $n > 1$  it is possible to build a ring  $\mathcal{R}$  of  $p^{tn}$  elements which contain involutory elements.

## Corollary 2

For any  $n \in \mathbb{N}$  such that  $n > 1$  exist one linear involutory transformation

$$\Psi : \mathcal{R} \rightarrow \mathcal{R}$$

build by the rule in (1).

If the order of  $F(x)$ , denoted by  $e$ , is even, then the application  $\Psi : \mathcal{R} \rightarrow \mathcal{R}$  of the form

$$\Psi(g(x)) = g(x)x^{\frac{e}{2}} \bmod F(x) \quad (5)$$

is involutory.

# Branch Number

Let be function  $\tau : \mathcal{R} \rightarrow \mathbb{N}_0$  defined as:

$$\tau(g(x)) = \sum_{i=0}^{m-1} \delta_{0,f_i}$$

where

$$\delta_{0,f_i} = \begin{cases} 1, & \text{if } f_i \neq 0 \\ 0, & \text{if } f_i = 0, \end{cases}$$

## Definition

The branch number  $\rho$  of a linear transformation  $\Psi : \mathcal{R} \rightarrow \mathcal{R}$  is defined as

$$\rho(\Psi) = \min_{g(x) \neq 0} \{\tau(g(x)) + \tau(\Psi(g(x)))\}.$$

The linear transformation  $\Psi$  is called MDS if  $\rho(\Psi) = m + 1$ .

# Branch Number

Let be function  $\tau : \mathcal{R} \rightarrow \mathbb{N}_0$  defined as:

$$\tau(g(x)) = \sum_{i=0}^{m-1} \delta_{0,f_i}$$

where

$$\delta_{0,f_i} = \begin{cases} 1, & \text{if } f_i \neq 0 \\ 0, & \text{if } f_i = 0, \end{cases}$$

## Definition

The branch number  $\rho$  of a linear transformation  $\Psi : \mathcal{R} \rightarrow \mathcal{R}$  is defined as

$$\rho(\Psi) = \min_{g(x) \neq 0} \{\tau(g(x)) + \tau(\Psi(g(x)))\}.$$

The linear transformation  $\Psi$  is called MDS if  $\rho(\Psi) = m + 1$ .

## Proposition

Let  $(\alpha_0, \dots, \alpha_s)$  be elements of the set  $\mathcal{P}^*$ , such that  $\forall i, j \in \{0, \dots, s\} \alpha_i \neq \alpha_j$  and let be the polynomials such that

$$f(x) = (x + \alpha_0)^{n-1} (x + \alpha_1) \cdots (x + \alpha_s) \text{ and } F(x) = (x + \alpha_0)f(x).$$

For all element  $h(x) \in \mathcal{R}$  the transformation  $\Psi$  defined by the rule (1) is a linear involutory transformation whose branch number satisfies that

$$\rho(\Psi) \leq 4.$$

If the matrix associated to  $\Psi$  does not contain any zero coefficient then

$$\rho(\Psi) = 4.$$

## Proposition

Let  $a$  be element of field  $\mathcal{P}$  such that  $a \neq 1$ , and let be the polynomials such that

$$f(x) = (x^n + a) \text{ and } F(x) = f(x)^2.$$

For all element  $h(x) \in \mathcal{R}$  the transformation  $\Psi$  form by the rule (1) is a linear involutory transformation whose branch number satisfies that

$$\rho(\Psi) \leq 4.$$

If the matrix associated to  $\Psi$  does not contain any zero coefficient then

$$\rho(\Psi) = 4.$$

# Example MDS involutory transformation

Take  $\mathcal{P} = \mathbb{F}_2[x]/_{x^8+x^4+x^3+x^2+1}$  having  $\beta$  a primitive element on  $\mathcal{P}$  and selecting the following parameters

$n$	$f(x)$	$F(x)$	$h(x)$
4	$(x + \beta)(x + \beta^2)$	$f(x)^2$	$x$
6	$(x + \beta)(x + \beta^2)(x + \beta^3)$	$f(x)^2$	$x^2 + x$

the transformation

$$\Psi(g(x)) = g(x)(1 + f(x)h(x)) \bmod F(x)$$

is an involutory MDS transformation.



For the class of application  $\Psi$  such that

$$\Psi(g(x)) = g(x)(1 + (x^n + a)h(x)) \bmod x^{2n} + a^2,$$

$\forall a \in \mathcal{P}^*$  y  $\forall h(x) \in \mathcal{R}$  does not exist MDS matrices.

# Generation of $4 \times 4$ involutory MDS

Let  $\mathcal{P} = \mathbb{F}_{2^t}$ , given  $a \in \mathcal{P}^*$ ,  $f_1(x) = x^n + a$ ,  $F_1(x) = x^{2n} + a^2$ ,  
 $f_2(x) = x^n + 1$ ,  $F_2(x) = x^{2n} + 1$ , we construct the transformations  $\Psi_1$   
and  $\Psi_2$  from  $\mathcal{P}_i$  to  $\mathcal{P}_i$  where  $\mathcal{P}_i = \mathcal{P}[x]/_{F_i(x)}$ ,  $i = 1, 2$

$$\Psi_1(g(x)) = g(x)(1 + f_1(x)h(x)) \bmod F_1(x)$$

and

$$\Psi_2(g(x)) = g(x)(1 + f_2(x)x) \bmod F_2(x).$$

Let us denote by “ $\circ$ ” the composition of two applications and by  $\mathcal{R}(2n)$  the set of all polynomials with coefficients in  $\mathcal{P}$  whose degree is lower than  $2n$ . We define the transformation

$$\Psi : \mathcal{R}(2n) \rightarrow \mathcal{R}(2n)$$

of the following form

$$\forall g(x) \in \mathcal{R}(2n), \Psi(g(x)) = \Psi_1 \circ \Psi_2 \circ \Psi_1(g(x)). \quad (6)$$

## Proposition

Let be  $n = 4$ . For a given polynomial  $h(x) = h_3x^3 + \dots + h_0$  such that  $h_1 \neq ah_3$  and for any value of  $h_2$  there exist a value of  $h_0$  such that the matrix associated to transformation  $\Psi$  is MDS. Particularly one can take  $h_1 = ah_3 + 1$ .

## Algorithm

INPUT:  $a \in \mathcal{P} \setminus \{0\}$  and  $h_2, h_3 \in \mathcal{P}$

STEP 1: Make  $h_1 = ah_3 + 1, i = 1$ .

STEP 2: Make the  $i$ -th row of the matrix  $\mathcal{A}_{h_0}, \delta_i(x) = \Psi(x^{i-1})$ .

## Proposition

Let be  $n = 4$ . For a given polynomial  $h(x) = h_3x^3 + \dots + h_0$  such that  $h_1 \neq ah_3$  and for any value of  $h_2$  there exist a value of  $h_0$  such that the matrix associated to transformation  $\Psi$  is MDS. Particularly one can take  $h_1 = ah_3 + 1$ .

## Algorithm

**INPUT:**  $a \in \mathcal{P} \setminus \{0\}$  and  $h_2, h_3 \in \mathcal{P}$

**STEP 1:** Make  $h_1 = ah_3 + 1, i = 1$ .

**STEP 2:** Make the  $i$ -th row of the matrix  $\mathcal{A}_{h_0}, \delta_i(x) = \Psi(x^{i-1})$ .

**STEP 3.1:** Discard all roots of the polynomials  $\delta_{i,1}(h_0), \dots, \delta_{i,4}(h_0)$ .

**STEP 3.2:** Make  $i = i + 1$

**STEP 3.3:** If  $i = 5$  go to **STEP 4**, otherwise go to **STEP 2**.

**STEP 4:** Discard from  $\mathcal{A}_{h_0}$  all the roots of the polynomials result from calculating its order 2 minors.



**RETURN:** The set of values for  $h_0$  such that the polynomials  $h(x) = h_3x^3 + h_2x^2 + h_1x + h_0$  generate an involutory MDS matrix.

Make  $\mathcal{P} = \mathbb{F}_2[x]/_{x^8+x^4+x^3+x^2+1}$  having  $\beta$  a primitive element on  $\mathcal{P}$  and selecting the following parameters:

- $f(x) = x^2 + \beta$
- $F(x) = f(x)^2$
- $h_3 = 1$
- $h_2 = 0$

Applying the above procedure we obtain 230 distinct values of  $h_0$  such that the polynomial  $h(x) = h_3x^3 + h_2x^2 + h_1x + h_0$  generate an involutory MDS matrix.

The method presented in this section to generate involutory MDS matrices can be also used to generate key-dependent MDS matrices for dynamic encryption algorithms, for example in following work authors using this point of view

- 1  Pablo Freyre, Oristela Cuellar, Nelson Dáz, Adrián Alfonso. *From AES to Dynamic AES*. Journal of Science and Technology on Information Security, 2020.
- 2  Pablo Freyre, Oristela Cuellar, Nelson Díaz, Ramses Rodríguez, Adrián Alfonso. *Dynamic Cryptographic Algorithms Kuznyechik and Magma*. Journal of Science and Technology on Information Security, 2020.

## Conclusion

We board the construction of involutory elements using the nilpotent elements of a ring with nilpotency index 2. From such construction we study the involutory linear applications generated by multiplication of polynomials with coefficients in a finite field, characterizing the branch number of such applications. Finally, we introduce a new proposal which allow to generate MDS matrices using the results of the paper towards involutory elements and alternating between two different rings. However, how to reduce from quadratic to linear equations, which allow to increase the dimension of the matrix, remains as open question and future line of work in our research.