

Institute of Cryptography, Cuba

Generation of recursive MDS matrices with irreducible characteristic polynomial from known ones: a practical approach

Autors: Pablo Freyre Arrozarena
Alejandro Freyre Echevarría
Ramses Rodríguez Aulet
Oristela Cuellar Justiz

Introduction

- In cryptography, matrices having maximum diffusion coefficient are highly important in the design of symmetric cryptographic algorithms.
- One of more important class of matrix is the MDS (**M**aximum **D**istance **S**eparable (MDS))

- In cryptography, matrices having maximum diffusion coefficient are highly important in the design of symmetric cryptographic algorithms.
- One of more important class of matrix is the MDS (**M**aximum **D**istance **S**eparable (MDS))
- We can to construct MDS using Vandermonde matrices Cauchy construction and some recursive code how Reed-Solomon or variant Georgiade code.
- But in general the search for new methods to synthesize linear transformations which grant the desired cryptographic quality of the cipher as a whole and allow an efficient implementation in software/hardware is not a trivial problem.

- In *Dynamic cryptographic algorithms* Kuznyechik and Magma the authors introduce a dynamic variant of Kuznyechik where several transformations are derived from the key.
- Recently, the authors in *Efficient multiplication of a vector by an MDS matrix with irreducible characteristic polynomial* analyzed the effect the multiplication of permutation matrices and diagonal matrices by one MDS matrix has towards the characteristic polynomial of the latter.

- In *Dynamic cryptographic algorithms* Kuznyechik and Magma the authors introduce a dynamic variant of Kuznyechik where several transformations are derived from the key.
- Recently, the authors in *Efficient multiplication of a vector by an MDS matrix with irreducible characteristic polynomial* analyzed the effect the multiplication of permutation matrices and diagonal matrices by one MDS matrix has towards the characteristic polynomial of the latter.

We discuss some of the design strategies to obtain linear transformations with maximum diffusion coefficient defined over any finite field $\mathbb{F}_{2^n}$, $n \geq 4$ with irreducible polynomial

Efficient multiplication of a vector by an MDS matrix with irreducible characteristic polynomial

Algorithm 1: Generation of the MDS matrix $A_{r \times r}$

Input: $g(x) = g_0 + g_1x + \dots + g_{r-1}x^{r-1} + x^r$, polynomial generator of a nontrivial linear MDS code $[n,k,d]$ over $\mathbb{F}_2^s$

Input: $r \leq l_1 \leq k - r$

Output: The MDS matrix $A_{r \times r}$

// Calculation of the j -th row of the matrix ($1 \leq j \leq r$)

for j from 1 to r do

- $(a_0, a_1, \dots, a_{r-1})$ is the canonical vector with value 1 in the $(j-1)$ -th coordinate.
 - $(\hat{a}_0 + \hat{a}_1x + \dots + \hat{a}_{r-1}x^{r-1}) = (a_0 + a_1x + \dots + a_{r-1}x^{r-1})(x^{l_1}) \bmod g(x)$
 - $\text{Row}_j = (\hat{a}_0, \hat{a}_1, \dots, \hat{a}_{r-1})$
-

The whole procedure works as follows.

- Step 1:** Obtain the MDS matrix $A_{r \times r}$ over the field $\mathbb{F}_{2^s}$ using Algorithm 1.
- Step 2:** Determine the characteristic polynomial of the matrix obtained in **Step 1**. If such polynomial is irreducible then $l_i = 1, \forall i = \overline{0, r-1}$, the diagonal and the permutation matrix are equal to the identity and proceed to **Step 6**.
- Step 3:** In the matrix $A_{r \times r}$ columns permutations are performed which is equivalent to operate the multiplication $A_{r \times r}H$ assuming that H is distinct from the identity. Then the obtained matrix is multiplied by a diagonal matrix on the left and a new matrix $D(A_{r \times r}H)$ is obtained where $l_i \in \mathbb{F}_{2^s}$ are unknown values.
- Step 4:** Select an irreducible polynomial $\text{Irr}(x) = \gamma_0 + \gamma_1x + \dots + \gamma_{r-1}x^{r-1} + x^r \in \mathbb{F}_{2^s}[x]$ of degree r and suppose that the endomorphism $f : \text{end } \mathbb{F}_{2^s}^r$ is determined by the matrix $B_{r \times r}$ accompanying the polynomial $\text{Irr}(x)$ such that $B_{r \times r} = M(f, (e_i))$ where (e_i) is the canonical basis of $\mathbb{F}_{2^s}^r$ and $D(A_{r \times r}H) = M(f, (\delta_i))$ where (δ_i) is another basis of $\mathbb{F}_{2^s}^r$.

Step 5: Next select one of two ways to obtain the values of the l_i .

Option 1: Solve the system of linear equations

$$f(\delta_i) = a_{0i}l_0\delta_0 + a_{1i}l_1\delta_1 + \cdots + a_{(r-1)i}l_{r-1}\delta_{r-1}$$

for $i = \overline{0, r-1}$ and determine the values of $l_i \in \mathbb{F}_{2^s}$ that nullifies the determinant of the matrix associated to the system of equations.

Option 2: Calculate the characteristic polynomial of the matrix obtained in **Step 3** which have the following form

$$\chi(x) = x^r + i_{r-1}(l_0, \dots, l_{r-1})x^{r-1} + \cdots + i_1(l_0, \dots, l_{r-1})x + i_0(l_0, \dots, l_{r-1})$$

Using the irreducible polynomial selected in **Step 4** solve the following system of equations

$$\begin{cases} i_0(l_0, \dots, l_{r-1}) &= \gamma_0, \\ &\vdots \\ i_{r-1}(l_0, \dots, l_{r-1}) &= \gamma_{r-1}. \end{cases}$$

to obtain the values for $l_0, l_1, \dots, l_{r-1}$ to conform the MDS matrix whose characteristic polynomial is $Irr(x)$.

Step 6: Multiply a vector by the obtained MDS matrix using the following Algorithm 2.

Algorithm 2: Multiply a vector by the MDS matrix $D(A_{r \times r}H)$ with irreducible characteristic polynomial

Input: $g(x) = g_0 + g_1x + \dots + g_{r-1}x^{r-1} + x^r$, polynomial generator of a nontrivial linear MDS code $[n,k,d]$ over $\mathbb{F}_{2^s}$

Input: $r \leq \mu_1 \leq k - r$

Input: Permutation π associated to the permutation matrix H

Input: The values $l_i \in \mathbb{F}_{2^s}$ obtained in **Step 5**

Input: The vector $(a_0, a_1, \dots, a_{r-1})$ such that $a_i \in \mathbb{F}_{2^s}$

Output: A vector $(a_0, a_1, \dots, a_{r-1})D(A_{r \times r}H)$

$$(a_0, a_1, \dots, a_{r-1}) = (l_0 a_0, l_1 a_1, \dots, l_{r-1} a_{r-1})$$

$$(\hat{a}_0 + \hat{a}_1 x + \dots + \hat{a}_{r-1} x^{r-1}) = (a_0 + a_1 x + \dots + a_{r-1} x^{r-1})(x^{\mu_1}) \bmod g(x)$$

$$(a_0, a_1, \dots, a_{r-1}) = (\hat{a}_0, \hat{a}_1, \dots, \hat{a}_{r-1})$$

$$(a_0, a_1, \dots, a_{r-1}) = (a_{\pi(0)}, a_{\pi(1)}, \dots, a_{\pi(r-1)})$$

return $(a_0, a_1, \dots, a_{r-1})$

Generating recursive MDS matrices with irreducible characteristic polynomial from the one of Kuznyechik

- Let be $Q = \mathbb{F}_2[x]/p(x)$ where $p(x) = x^8 + x^7 + x^6 + x + 1$ is a irreducible polynomial over field $\mathbb{F}_2[x]$; the elements of Q are represented in such way that the element $z_0 + z_1\beta + \dots + z_7\beta^7$ of Q corresponds to integer $z_0 + 2z_1 + \dots + 2^7z_7$ where $z_i \in \{0, 1\}$, $i = 0, 1, \dots, 7$ y β denotes a residue class modulo $p(x)$ containing x .
- For a vector $a = (a_0, a_1, \dots, a_{15})$ belonging to the binary vector space V_{128} whose components a_i are elements of the vector space V_8 the linear transformation is the mapping $I : V_{128} \rightarrow V_8$ such that:

$$\begin{aligned} I(a) = & \eta(148 \cdot \rho(a_0) + 32 \cdot \rho(a_1) + 133 \cdot \rho(a_2) + 16 \cdot \rho(a_3) + 194 \cdot \rho(a_4) + \\ & 192 \cdot \rho(a_5) + \delta(a_6) + 251 \cdot \rho(a_7) + \delta(a_8) + 192 \cdot \rho(a_9) + 194 \cdot \rho(a_{10}) \\ & + 16 \cdot \rho(a_{11}) + 133 \cdot \rho(a_{12}) + 32 \cdot \rho(a_{13}) + 148 \cdot \rho(a_{14}) + \rho(a_{15})) \end{aligned}$$

From the mapping I the transformation $R : V_{128} \rightarrow V_{128}$ is defined as:

$$R(a_0, a_1, \dots, a_{15}) = (I(a_0, a_1, \dots, a_{15}), a_0, a_1, \dots, a_{14})$$

The associate matrix to transformation R is:

$$A_R = \begin{pmatrix} 148 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 32 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 133 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 194 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 192 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 251 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 192 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 194 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 133 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 32 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 148 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

It is straightforward to notice that A_R^{16} result in the matrix representing the linear layer of Kuznyechik.

- In order to represent such transformation through the multiplication of polynomials modulus a polynomial we construct the polynomial:

$$p(x) = x^{16} + l^*(x)$$

where $l^*(x) = x^{15} \cdot l(x^{-1})$

- We apply Algorithm 1 with input parameters $p(x)$, $r = 16$, $l_1 = 1$ the resulting matrix is

$$A_p = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 148 & 32 & 133 & 16 & 194 & 192 & 1 & 251 & 1 & 192 & 194 & 16 & 133 & 32 & 148 \end{pmatrix}$$

- Notice that

$$A_p = P \cdot A_R^T \cdot P$$

where A_R^T denotes the transpose of A_R and P is the matrix described by the involutory permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{pmatrix}$$

- The matrix A_p is also MDS.

- The resulting matrix will be

$$A_p^{16} = P \cdot M_K^T \cdot P$$

where M_K^T is the transpose of the matrix representing the linear layer of Kuznyechik and it is easy to check that A_p^{16} is MDS. The matrix representation of A_p^{16} is shown below

$$A_p^{16} = \begin{pmatrix} 1 & 148 & 32 & 133 & 16 & 194 & 192 & 1 & 251 & 1 & 192 & 194 & 16 & 133 & 32 & 148 \\ 148 & 165 & 60 & 68 & 209 & 141 & 180 & 84 & 222 & 111 & 119 & 93 & 150 & 116 & 45 & 132 \\ 132 & 100 & 72 & 223 & 211 & 49 & 166 & 48 & 224 & 90 & 68 & 151 & 202 & 117 & 153 & 221 \\ 221 & 13 & 248 & 82 & 145 & 100 & 255 & 123 & 175 & 61 & 148 & 243 & 217 & 208 & 233 & 16 \\ 16 & 137 & 72 & 127 & 145 & 236 & 57 & 239 & 16 & 191 & 96 & 233 & 48 & 94 & 149 & 189 \\ 189 & 162 & 72 & 198 & 254 & 235 & 47 & 132 & 201 & 173 & 124 & 26 & 104 & 190 & 159 & 39 \\ 39 & 127 & 200 & 152 & 243 & 15 & 84 & 8 & 246 & 238 & 18 & 141 & 47 & 184 & 212 & 93 \\ 93 & 75 & 142 & 96 & 1 & 42 & 108 & 9 & 73 & 171 & 141 & 203 & 20 & 135 & 73 & 184 \\ 184 & 110 & 42 & 212 & 177 & 55 & 175 & 212 & 190 & 241 & 46 & 187 & 26 & 78 & 230 & 122 \\ 122 & 22 & 245 & 82 & 120 & 153 & 235 & 213 & 231 & 196 & 45 & 6 & 23 & 98 & 213 & 72 \\ 72 & 195 & 2 & 14 & 88 & 144 & 225 & 163 & 110 & 175 & 188 & 197 & 12 & 236 & 118 & 108 \\ 108 & 76 & 221 & 101 & 1 & 196 & 212 & 141 & 164 & 2 & 235 & 32 & 202 & 107 & 242 & 114 \\ 114 & 232 & 20 & 7 & 73 & 246 & 215 & 166 & 106 & 214 & 17 & 28 & 12 & 16 & 51 & 118 \\ 118 & 227 & 48 & 159 & 107 & 48 & 99 & 161 & 43 & 28 & 67 & 104 & 112 & 135 & 200 & 162 \\ 162 & 208 & 68 & 134 & 45 & 184 & 100 & 193 & 156 & 137 & 72 & 144 & 218 & 198 & 32 & 110 \\ 110 & 77 & 142 & 234 & 169 & 246 & 191 & 10 & 243 & 242 & 142 & 147 & 191 & 116 & 152 & 207 \end{pmatrix}$$

Proposition

Let $g(x)$ be the r -degree polynomial generator of a nontrivial linear MDS code $[n,k,d]$ over $\mathbb{F}_{2^s}$, $\mathcal{C}_{\mathbb{F}_{2^s}}$ denote the complexity of multiplying two elements in $\mathbb{F}_{2^s}$ and $\mathcal{C}_P(k)$ denotes the complexity of multiplying two polynomials modulus a k – degree polynomial. Then, the complexity of Algorithm 3 satisfies the following inequality

$$T(r) \leq r \cdot (\mathcal{C}_{\mathbb{F}_{2^s}} + 1) + \mathcal{C}_P(r)$$

Linear MDS transformation with irreducible polynomial

Algorithm 3: Multiply a vector by the MDS matrix $D(HA_{r \times r})$ with irreducible characteristic polynomial

Input: $g(x) = g_0 + g_1x + \dots + g_{r-1}x^{r-1} + x^r$, polynomial generator of a nontrivial linear MDS code $[n,k,d]$ over $\mathbb{F}_{2^s}$

Input: $r \leq \mu_1 \leq k - r$

Input: Permutation π associated to the permutation matrix H

Input: The values $l_i \in \mathbb{F}_{2^s}$ obtained in **Step 5** of Section 3

Input: The vector $(a_0, a_1, \dots, a_{r-1})$ such that $a_i \in \mathbb{F}_{2^s}$

Output: The vector $(a_0, a_1, \dots, a_{r-1}) \cdot D(HA_{r \times r})$

$$(a_0, a_1, \dots, a_{r-1}) = (l_0 a_0, l_1 a_1, \dots, l_{r-1} a_{r-1})$$

$$(a_0, a_1, \dots, a_{r-1}) = (a_{\pi(0)}, a_{\pi(1)}, \dots, a_{\pi(r-1)})$$

$$(\hat{a}_0 + \hat{a}_1 x + \dots + \hat{a}_{r-1} x^{r-1}) = (a_0 + a_1 x + \dots + a_{r-1} x^{r-1})(x^{\mu_1}) \bmod g(x)$$

$$(a_0, a_1, \dots, a_{r-1}) = (\hat{a}_0, \hat{a}_1, \dots, \hat{a}_{r-1})$$

return $(a_0, a_1, \dots, a_{r-1})$

Example

We take the following parametr

- Let $M = A_p^{16}$. Taking the matrix H represented by the permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 3 & 0 & 15 & 14 & 10 & 7 & 11 & 8 & 12 & 6 & 2 & 13 & 9 & 5 & 1 \end{pmatrix}$$

- A diagonal matrix D whose vector representation is $\vec{d} = (1, 1, 1, \dots, 1, 1, 2)$

Then the matrix $M' = D(HM)$ with representation

$$M' = \begin{pmatrix} 132 & 100 & 72 & 223 & 211 & 49 & 166 & 48 & 224 & 90 & 68 & 151 & 202 & 117 & 153 & 221 \\ 110 & 77 & 142 & 234 & 169 & 246 & 191 & 10 & 243 & 242 & 142 & 147 & 191 & 116 & 152 & 207 \\ 108 & 76 & 221 & 101 & 1 & 196 & 212 & 141 & 164 & 2 & 235 & 32 & 202 & 107 & 242 & 114 \\ 148 & 165 & 60 & 68 & 209 & 141 & 180 & 84 & 222 & 111 & 119 & 93 & 150 & 116 & 45 & 132 \\ 1 & 148 & 32 & 133 & 16 & 194 & 192 & 1 & 251 & 1 & 192 & 194 & 16 & 133 & 32 & 148 \\ 162 & 208 & 68 & 134 & 45 & 184 & 100 & 193 & 156 & 137 & 72 & 144 & 218 & 198 & 32 & 110 \\ 72 & 195 & 2 & 14 & 88 & 144 & 225 & 163 & 110 & 175 & 188 & 197 & 12 & 236 & 118 & 108 \\ 39 & 127 & 200 & 152 & 243 & 15 & 84 & 8 & 246 & 238 & 18 & 141 & 47 & 184 & 212 & 93 \\ 184 & 110 & 42 & 212 & 177 & 55 & 175 & 212 & 190 & 241 & 46 & 187 & 26 & 78 & 230 & 122 \\ 118 & 227 & 48 & 159 & 107 & 48 & 99 & 161 & 43 & 28 & 67 & 104 & 112 & 135 & 200 & 162 \\ 189 & 162 & 72 & 198 & 254 & 235 & 47 & 132 & 201 & 173 & 124 & 26 & 104 & 190 & 159 & 39 \\ 93 & 75 & 142 & 96 & 1 & 42 & 108 & 9 & 73 & 171 & 141 & 203 & 20 & 135 & 73 & 184 \\ 122 & 22 & 245 & 82 & 120 & 153 & 235 & 213 & 231 & 196 & 45 & 6 & 23 & 98 & 213 & 72 \\ 114 & 232 & 20 & 7 & 73 & 246 & 215 & 166 & 106 & 214 & 17 & 28 & 12 & 16 & 51 & 118 \\ 16 & 137 & 72 & 127 & 145 & 236 & 57 & 239 & 16 & 191 & 96 & 233 & 48 & 94 & 149 & 189 \\ 121 & 26 & 51 & 164 & 225 & 200 & 61 & 246 & 157 & 122 & 235 & 37 & 113 & 99 & 17 & 32 \end{pmatrix}$$

have a primitive polynomial.

Quasi-involutory matrices from the multiplication of polynomials modulus a polynomial

Quasi-involutory matrices

Let $n \in \mathbb{N}$. The bijective linear transformation

$$\Psi : P[x]/_{g(x)} \rightarrow P[x]/_{g(x)}$$

defined by the rule

$$\forall p(x) \in P[x]/_{g(x)} : \Psi(p(x)) = p(x) \cdot x^n \mod g(x)$$

is quasi-involutory if its inverse Ψ^{-1} is the transformation

$$\Psi^{-1}(p(x)) = \Psi(p(x)) \cdot x \mod g(x)$$

Quasi-involutory matrices from the multiplication of polynomials modulus a polynomial

Quasi-involutory matrices

Let $n \in \mathbb{N}$. The bijective linear transformation

$$\Psi : P[x]/_{g(x)} \rightarrow P[x]/_{g(x)}$$

defined by the rule

$$\forall p(x) \in P[x]/_{g(x)} : \Psi(p(x)) = p(x) \cdot x^n \mod g(x)$$

is quasi-involutory if its inverse Ψ^{-1} is the transformation

$$\Psi^{-1}(p(x)) = \Psi(p(x)) \cdot x \mod g(x)$$

- With the input parameter l_1 of Algorithm 1 to be $l_1 = 127$ and using polynomial $p(x) = x^{16} + l^*(x)$ one can obtain a quasi-involutory MDS matrix.

Quasi-involutory matrices from the multiplication of polynomials modulus a polynomial

Quasi-involutory matrices

Let $n \in \mathbb{N}$. The bijective linear transformation

$$\Psi : P[x]/_{g(x)} \rightarrow P[x]/_{g(x)}$$

defined by the rule

$$\forall p(x) \in P[x]/_{g(x)} : \Psi(p(x)) = p(x) \cdot x^n \mod g(x)$$

is quasi-involutory if its inverse Ψ^{-1} is the transformation

$$\Psi^{-1}(p(x)) = \Psi(p(x)) \cdot x \mod g(x)$$

- With the input parameter l_1 of Algorithm 1 to be $l_1 = 127$ and using polynomial $p(x) = x^{16} + l^*(x)$ one can obtain a quasi-involutory MDS matrix.
- we obtain that

- Assuming that there exist a permutation matrix H and a diagonal matrix D such that the matrix $D(HA_p^{127})$ have irreducible characteristic polynomial then the multiplication of a vector by such matrix is conducted through Algorithm 3 using $\mu_1 = 127$.

- Assuming that there exist a permutation matrix H and a diagonal matrix D such that the matrix $D(HA_p^{127})$ have irreducible characteristic polynomial then the multiplication of a vector by such matrix is conducted through Algorithm 3 using $\mu_1 = 127$. Then if one need to multiply a vector by the inverse matrix, in this particular case we have to take into account the following:
 - 1 The inverse of the permutation matrix H is equal to its transpose.
 - 2 The inverse of the matrix D is the matrix D^{-1} described by the vector $\vec{d'} = (d_0^{-1}, d_1^{-1}, \dots, d_{15}^{-1})$ where d_i^{-1} is the multiplicative inverse of element d_i of the diagonal of matrix D .
 - 3 The polynomial representation of the vector is multiplied by x^{μ_1+1} having $\mu_1 + 1 = 128$.

Proposition

Let $g(x)$ be the r -degree polynomial generator of a nontrivial linear MDS code $[n,k,d]$ over $\mathbb{F}_{2^s}$, $\mathcal{C}_{\mathbb{F}_{2^s}}$ denote the complexity of multiplying two elements in $\mathbb{F}_{2^s}$, $\mathcal{I}_{\mathbb{F}_{2^s}}$ denote the complexity of finding the multiplicative inverse in $\mathbb{F}_{2^s}$ and $\mathcal{C}_P(k)$ denotes the complexity of multiplying two polynomials modulus a k – degree polynomial. Then, the complexity of Algorithm 3 satisfies the following inequality

$$T(r) \leq r \cdot (\mathcal{C}_{\mathbb{F}_{2^s}} + \mathcal{I}_{\mathbb{F}_{2^s}} + 1) + \mathcal{C}_P(r)$$

Conclusions

- We show an alternative method to represent the linear layer of Kuznyechik through the multiplication of polynomials modulus a polynomial using the reciprocal of the polynomial described in transformation $I(x)$ to obtain a similar matrix to the one of Kuznyechik and present the algorithm to efficiently multiply a vector by one MDS matrix with irreducible characteristic polynomial constructed from it.
- We also extend our results to the case of quasi involutory matrices where we also present the algorithm to multiply by the inverse of a quasi-involutory matrix of the form $D(HA_{r \times r})$.
- Other types of matrix constructions based on the method described can be explored and the algorithms to conduct the multiplication of a vector by the resulting matrix will be similar to these shown our paper.

Institute of Cryptography, Cuba

Generation of recursive MDS matrices with irreducible characteristic polynomial from known ones: a practical approach

Autors: Pablo Freyre Arrozarena
Alejandro Freyre Echevarría
Ramses Rodríguez Aulet
Oristela Cuellar Justiz