Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

Tipo de artículo: Artículo original
Temática: Matemática computacional, Seguridad informática

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

Multiplicación eficiente de un vector por una matriz MDS con polinomio característico irreducible

Pablo Freyre Arrozarena[1] https://orcid.org/0000-0001-7149-232X
Oristela Cuellar Justiz [2*] https://orcid.org/0000-0002-6685-8013
Ramsés Rodríguez Aulet [1] https://orcid.org/0000-0001-7653-324X
Alejandro Freyre Echevarría[1] https://orcid.org/0000-0002-0537-9430

[1]Institute of Cryptography. University of Havana. San Lázaro y L. Plaza de la Revolución, Havana, Cuba.
[2]University of Informatics Sciences. Faculty of Computer Sciences and Technologies. Carretera a San Antonio Km 21/2.Torrens.La Lisa, Havana.

*Autor para la correspondencia: oristelacj@uci.cu

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

ABSTRACT

Multiplication of a vector by an MDS matrix is a key process in many fields, such as cryptography. Algorithms for efficient multiplication of a vector by an MDS matrix have been designed to optimize the multiplication process, reducing the computational complexity, which allows for more efficient resource utilization. In this paper, based on previous work by the lead author, a new algorithm for the efficient multiplication of a vector by an MDS matrix with irreducible characteristic polynomial was designed and substantiated. The presented algorithm is based on the multiplication of two polynomials modulo a generator polynomial of a nontrivial linear MDS code [n, k, d] over $\mathbb{F}_{2^s}$ and in the worst case it is only necessary to store $3(n - k)$ values of the $\mathbb{F}_{2^s}$ for the multiplication of a vector by an MDS $(n-k) \times (n-k)$ matrix over $\mathbb{F}_{2^s}$ and $4(n-k)$ values for the multiplication of the vector by the inverse matrix. Multiplying two polynomials of degree m over $\mathbb{F}_{2^s}$ has a complexity of $O(m \log_2 m)$, whereas if the Karatsuba approach and its improvements are used, the complexity is $O(m^\alpha)$, $1 \leq \alpha \leq 2$, where $\alpha = 1.46$ for the best known algorithm . So, the complexity of the algorithm is $O(m \log_2 m)$, plus a multiplication in $\mathbb{F}_{2^s}$ and it is not necessary to explicitly write the matrix or the inverse.

Keywords: non-singular matrices; multiplication of polynomials; inverse matrix; characteristic polynomial.

RESUMEN

La multiplicación de un vector por una matriz MDS es un proceso clave en muchos campos, como la criptografía. Los algoritmos para la multiplicación eficiente de un vector por una matriz MDS se han diseñado para optimizar el proceso de multiplicación, reduciendo la complejidad computacional, lo que permite la utilización de los recursos de manera más eficiente. En este artículo, sobre la base de trabajos anteriores del autor principal se diseñó y fundamentó un nuevo algoritmo para la multiplicación eficiente de un vector por una matriz MDS con polinomio característico irreducible. El algoritmo que se presenta se basa en la multiplicación de dos polinomios módulo un polinomio generador de un código MDS lineal no trivial [n, k, d] sobre $\mathbb{F}_{2^s}$ y en el peor caso sólo es necesario almacenar $3(n - k)$ valores de la $\mathbb{F}_{2^s}$ para la multiplicación de un vector por una matriz MDS $(n-k) \times (n-k)$ sobre $\mathbb{F}_{2^s}$ y $4(n-k)$ valores para la multiplicación

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

del vector por la matriz inversa. Multiplicar dos polinomios módulo un polinomio sobre $\mathbb{F}_{2^s}$ de grado m tiene una complejidad de $O(m \log_2 m)$, mientras que, si se utiliza el enfoque de Karatsuba y sus mejoras, la complejidad es $O(m^{\alpha})$, $1 \leq \alpha \leq 2$, donde $\alpha = 1{,}46$ para el mejor algoritmo conocido. Así que la complejidad del algoritmo es $O(m \log_2 m)$, más una multiplicación en $\mathbb{F}_{2^s}$ y no es necesario escribir explícitamente la matriz o la inversa.

Palabras clave: matrices no singulares; multiplicación de polinomios; matriz inversa; polinomio característico.

Recibido: 21/06/2024
Aceptado: 18/12/2024

Introduction

Algorithms for efficient multiplication of a vector by an MDS matrix are designed to optimize the multiplication process, reducing the number of operations required and improving overall performance (Arrozarena and Fiallo 2022). In addition, by reducing computational complexity, resources can be used more efficiently, which is especially beneficial in environments with memory and computational power constraints. Its proper implementation can make a difference in terms of speed and efficiency in data processing. Multiplying a vector by an MDS matrix is a key process in many fields, such as cryptology, signal processing and information theory. The efficiency of this computation is crucial to improve the performance of systems and applications that depend on it. In a general way these algorithms are based on techniques such as block matrix multiplication, application of fast Fourier transforms (FFT) (Ashdhir, Arya and Rani 2021) and exploitation of special properties of MDS matrices (Gupta, Pandey and Venkateswarlu 2019) (Luong, Cuong and Tho 2019) (Kesarwani, Sarkar and Venkateswarlu 2019) (Gupta, Pandey and Samanta 2023). In cryptanalysis by invariant subgroups the multiplication of a vector by an MDS matrix is of particular

importance (Guo et al. 2016) (Todo, Leander, and Sasaki 2019) (Mennink and Neves 2021) (Grassi, Rechberger, and Schofnegger 2020).

The search for efficient algorithms for the multiplication of a vector by a matrix is an open area of research in Cryptography, coding theory, information theory among others.

In (Arrozarena and Fiallo 2022) the authors present algorithms for the generation of $m \times m$ MDS matrices over the finite field $\mathbb{F}_q$ to compute their inverses and for the multiplication of a vector by a matrix or by its inverse, they are based on the multiplication of two polynomials modulo a nontrivial linear MDS code generator polynomial of degree m.

The objective of this work is to build on the algorithm presented in (Arrozarena and Fiallo 2022) to obtain an efficient algorithm for the multiplication of a vector by an MDS matrix over $\mathbb{F}_{\mathbf{2}^s}$ with irreducible characteristic polynomial.

The algorithm presented is based on the multiplication of two polynomials modulo a generator polynomial of a nontrivial linear MDS code $[n, k, d]$ over $\mathbb{F}_{\mathbf{2}^s}$ (MacWilliams and Sloane 1977) (Gupta, Pandey and Venkateswarlu 2017) (Baylis 2018) (De Piccoli, Visconti and Rizzo 2020) (Gupta, Pandey and Samanta 2023) and in the worst case it is only necessary to store $3(n - k)$ values of the finite field $\mathbb{F}_{\mathbf{2}^s}$ for the multiplication of a vector by an MDS $(n-k) \times (n-k)$ matrix over $\mathbb{F}_{\mathbf{2}^s}$ and $4(n-k)$ values for the multiplication of the vector by the inverse matrix. Multiplying two polynomials of degree m over $\mathbb{F}_{\mathbf{2}^s}$ has a complexity of $O(m \log_2 m)$, whereas if the Karatsuba approach and its improvements are used, the complexity is $O(m^{\alpha})$, $1 \leq \alpha \leq 2$, where $\alpha = 1{,}46$ for the best known algorithm (Peterson and Weldon 1972). So, the complexity of the algorithm is $O(m \log_2 m)$, plus a multiplication in $\mathbb{F}_{\mathbf{2}^s}$ and it is not necessary to explicitly write the matrix or the inverse.

Methods or Computational Methodology

As mentioned in the introduction, the new algorithm presented here takes as a starting point the algorithms presented in (Arrozarena and Fiallo 2022). Before explaining its theoretical basis and to facilitate the reader's

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

understanding, the algorithm for generating MDS matrices and the algorithm for multiplying a vector by an MDS matrix are presented below.

Algorithm 1: Generation of the MDS matrix A_{rxr}

Input:

- $g(x) = (g_0 + g_1x + \cdots + g_{r-1}x^{r-1} + x^r)$ it is the polynomial generator of a nontrivial linear MDS code [n, k, d] over $\mathbb{F}_{2^s}$ [2].
- $r \leq l_1 \leq k - r$.

Output: An MDS matrix A_{rxr}

//Calculation of the row j of matrix A_{rxr}, $1 \leq j \leq r$

Receive: $(a_0, a_1, \ldots, a_{r-1}) = (0, \ldots, 0, \underbrace{1}_{j}, 0 \ldots 0)$ (the canonical vector has a 1 in the *j* position)

$$(a_0 + a_1x + \cdots + a_{r-1}x^{r-1})(x^{l_1})\ mod g(x) = (\hat{a}_0 + \hat{a}_1x + \ldots + \hat{a}_{r-1}x^{r-1})$$

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

Return: $\text{Row}_j = (a_0, a_1, \ldots, a_{r-1})$

Algorithm 2: To multiply a vector by the MDS matrix A_{rxr}

Input:

- Same as algorithm 1
- $(a_0, a_1, \ldots, a_{r-1})$; $a_i \in \mathbb{F}_{2^s}$

Output: A vector $(a_0, a_1, \ldots, a_{r-1})\ A_{rxr}$

Receive: $(a_0, a_1, \ldots, a_{r-1})$

$$(a_0 + a_1x + \cdots + a_{r-1}x^{r-1})(x^{l_1}))\ mod g(x) = \quad = (\hat{a}_0 + \hat{a}_1x + \ldots + \hat{a}_{r-1}x^{r-1})$$

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

Return: $(a_0, a_1, \ldots, a_{r-1})$

Theoretical foundations of the new algorithm

Before presenting the algorithm for the efficient multiplication of a vector by an MDS matrix, it is necessary to analyze its theoretical foundations. From Linear Algebra the following results are known and can be found in (Kostrikin 1983) (Noriega Sanchez and Arazoza Rodriguez 2003) (Varela 2008) or among other classic books on the subject and others such as (Dickinson 2019) (Liu et al. 2022).

For example, in (Noriega Sánchez and Arazoza Rodríguez 2003) the definitions of matrix associated to a linear application and of similar matrices are given as follows.

Definition 1: Let $\boldsymbol{f}$ be a linear application between the vector spaces $\boldsymbol{E}$ and $\boldsymbol{F}$ over the field $\boldsymbol{K}$, let $(\boldsymbol{a_1}, \boldsymbol{a_2}, \ldots., \boldsymbol{a_n})$be a basis of $\boldsymbol{E}$ and $(\boldsymbol{b_1}, \boldsymbol{b_2}, \ldots., \boldsymbol{b_m})$ a basis of $\boldsymbol{F}$, the matrix whose coefficient $(\boldsymbol{i}, \boldsymbol{j})$ is given by the i-th coordinate in the basis $(\boldsymbol{b_i})$ of the vector $\boldsymbol{f}(\boldsymbol{a_j})$ is called the matrix associated to f in the bases $(\boldsymbol{a_j})$ and $(\boldsymbol{b_i})$ and is denoted by $\boldsymbol{M}(\boldsymbol{f}, (\boldsymbol{a_i}), (\boldsymbol{a_i}))$. If f is an n-dimensional endomorphism ($f: end\ E$) and $(\boldsymbol{a_i})$ is a basis of $\boldsymbol{E}$ then $\boldsymbol{M}(\boldsymbol{f}, (\boldsymbol{a_i}), (\boldsymbol{a_i}))$will be denoted as $\boldsymbol{M}(\boldsymbol{f}, (\boldsymbol{a_i}))$.

Definition 2: Two invertible matrices A and B over a field K are called similar if and only if there exists an invertible matrix P over K such that: $\boldsymbol{B = P^{-1}AP}$

Theorem 1: Two invertible matrices A and B over a field K are similar if and only if they are associated to the same endomorphism $f: end\ E$ in two distinct bases of E.

According to corollary1 of Lemma 2.5 of (Gupta et al. 2019) If $\mathbf{A_{rxr}}$ is an MDS matrix over the field $\mathbb{F}_{\boldsymbol{2^s}}$ and one has two nonsingular diagonal matrices $\mathrm{D}_1 = diag(l_0, l_1, \ldots., l_{r-1})$ y $\mathrm{D}_2 = diag(d_0, d_1, \ldots., d_{r-1}), l_i\ y\ d_i \in \mathbb{F}_{2^s}, l_i$ y $d_i \neq 0$ con $0 \leq i \leq r - 11$, then the matrix $\mathrm{D}_1\mathrm{A}_{rxr}\mathrm{D}_2$ is also MDS.

Let $Irr(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{r-1}x^{r-1} + x^r \in \mathbb{F}_{\boldsymbol{2^s}}[x]$ be a polynomial, then its accompanying matrix is

$$\mathrm{B}_{rxr} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ \gamma_0 & \gamma_1 & \gamma_2 & \cdots & \gamma_{r-1} \end{pmatrix},$$

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

Considering B_{rxr} as the matrix associated to the endomorphism f: $end\ \mathbb{F}_{2^s}^r$ with respect to the canonical basis (e_i) of $\mathbb{F}_{2^s}^r$ then $B_{rxr} = M(f,(e_i))$.

Theorem 2: Let the matrix A_{rxr} MDS, the diagonal matrix $D = diag(l_0, l_1, \ldots., l_{r-1})$, of size r both with coefficients $\mathbb{F}_{2^s}$, f : end $\mathbb{F}_{2^s}^r$, (e_i) be the canonical basis of $\mathbb{F}_{2^s}^r$. If the characteristic polynomial of $B_{rxr} = M(f,(e_i))$ is irreducible and having that (δ_i) is another basis of $\mathbb{F}_{2^s}^r$, which satisfies that $DA_{rxr} = M(f,(\delta_i))$ then if there exist values l_i, $i = 0..r-1$ such that the determinant of the matrix associated to the system of equations $f(\delta_i) = a_{0i}l_0\delta_0 + a_{1i}l_1\delta_1 + \cdots + a_{r-1i}l_{r-1}\delta_{r-1,}i = 0 \ldots r-1$, is equal to zero the matrix DA_{rxr} is MDS and its characteristic polynomial is irreducible.

Demonstration

By the corollary of Lemma 2.1 of (Gupta et al. 2019) it is proved that DA_{rxr} is an MDS matrix if A_{rxr} is MDS.

Let $Irr(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{r-1}x^{r-1} + x^r \in \mathbb{F}_{2^s}[x]$ be an irreducible polynomial, and let B_{rxr} be its companion matrix then the minimum polynomial of B_{rxr} and its characteristic polynomial coincide and is $Irr(x)$ (Peterson and Weldon 1972). Considering B_{rxr} as the matrix associated to the endomorphism f : end $\mathbb{F}_{2^s}^r$ with respect to the canonical basis (e_i) of $\mathbb{F}_{2^s}^r$ we have that $B_{rxr} = M(f,(e_i))$, and assuming that (δ_i) is another basis of $\mathbb{F}_{2^s}^r$ that satisfies that $DA_{rxr} = M(f,(\delta_i))$, then by Theorem 1 it is satisfied that B_{rxr} and DA_{rxr} are similar, for this to be satisfied it suffices to solve the system of equations $f(\delta_i) = a_{0i}l_0\delta_0 + a_{1i}l_1\delta_1 + \cdots + a_{r-1i}l_{r-1}\delta_{r-1,}i = 0..r-1,$. .r-1, and determine the values l_i, $i = 0..r-1$, that satisfy the above system of equations and this is satisfied when the determinant of the matrix associated to the above system of equations is equal to zero proving the theorem.

In general, we obtain a homogeneous system of linear equations of r^2 equations with r^2 unknowns. Since in addition the values of l_i are unknown we would have in total $r^2 + r$ unknowns.

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

The variables can be ordered as follows: $\delta_{00} \cdots \delta_{(r-1)0}\ \delta_{01} \cdots \delta_{(r-1)1} \delta_{02} \cdots \delta_{(r-1)2} \cdots$

The equations can be ordered in such a way that a matrix containing r blocks of size r is obtained. We obtain blocks such as: the null matrix of order r, the identical matrix of order r, scalar matrices of order r whose diagonal elements are the coefficients of the irreducible polynomial $Irr(x)$, among others.

To calculate the determinant of this matrix of order in r^2 blocks of size r, methods such as those proposed in (Gao et al. 2020) (Ali and Khan 2020) (Saadetoğlu and Dinsev 2023) (Kaddoura and Mourad 2022) can be used.

Corollary 1: Let the matrix A_{rxr} MDS, the diagonal matrix D, the matrix A_{rxr} D is MDS with irreducible characteristic polynomial if $B_{rxr} = M(f, (e_i))$ and there exists a basis (δ_i) such that $A_{rxr}D = M(f, (\delta_i))$.
The demonstration is similar to that of Theorem 2

Lemma 2: Let A_{rxr} be an MDS matrix over the field $\mathbb{F}_q$ and let H be the permutational matrix H, the matrix HA_{rxr} is MDS with irreducible characteristic polynomial if $B_{rxr} = M(f, (e_i))$ and there exists a basis (δ_i) such that $HA_{rxr} = M(f, (\delta_i))$.
The demonstration is similar to that of Theorem 2 by changing the permutational matrix H by the diagonal matrix D.

Corollary 2: Given the MDS matrix $\mathbf{A_{rxr}}$ and the permutational matrix H_2, the matrix $\mathbf{A_{rxr}}H$ is MDS with irreducible characteristic polynomial if $B_{rxr} = M(f, (e_i))$ and there exists a basis (δ_i) such that $A_{rxr}H = M(f, (\delta_i))$.

The demonstration is similar to that of Lemma 2.

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

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

The steps of the algorithm for efficient multiplication of a vector by an MDS matrix with irreducible characteristic polynomial are:

Step #1: Obtain the MDS matrix A_{rxr} over the field $\mathbb{F}_{2^s}$ by applying Algorithm 1.

Step # 2: Determine the characteristic polynomial of the matrix obtained in Step # 1. If the characteristic polynomial is irreducible then $l_i = 1 \ \forall i\ , i = \overline{0, r-1},$, the diagonal matrix D and the permutation matrix coincide with the identity matrix and go to Step # 6.

Step #3: To the MDS matrix A_{rxr} , column permutations are performed, which is equivalent to multiplying by a permutational matrix H on the right, that is different from the identity permutation, the obtained matrix is multiplied by a diagonal matrix on the left and a new matrix $A_{rxr}H$ is obtained where the $l_i \in \mathbb{F}_{2^s}, l_i$ and $i = \overline{0, r-1}$ are unknowns.

Step #4: Select an irreducible polynomial $Irr(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{r-1}x^{r-1} + x^r \in \mathbb{F}_{2^s}[x]$ of degree r and suppose that the endomorphism $f: end\mathbb{F}_{2^s}^r$ is determined by the matrix B_{rxr} accompanying the polynomial $Irr(x)$ such that $B_{rxr} = M(f, (e_i))$ where (e_i) is the canonical basis of $\mathbb{F}_{2^s}^r$ and $D\ (A_{rxr}H) = M(f, (\delta_i))$ where (δ_i) is another basis of $\mathbb{F}_{2^s}^r$.

Step #5:

Variant # 1: Solve the system of linear equation

$f(\delta_i) = l_0 a_{0i}\delta_0 + l_1 a_{1i}\delta_1 + \cdots + l_{r-1}a_{r-1i}\delta_{r-1,} i = \overline{0, r-1}$ and determine the values $l_i \in \mathbb{F}_{2^s}, i = \overline{0, r-1}$ that satisfy that the determinant of the matrix associated to the system of equations is zero.

Variant # 2: Obtain the characteristic polynomial of the MDS matrix AD_{rxr} obtained in step 3 which has the following form.

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

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

Using the irreducible polynomial selected a priori. Solve the following system of equations.

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

After determined the solutions for $l_0, \dots, l_{r-1}$ form the MDS matrix with irreducible characteristic polynomial.

Step # 6:

Algorithm 3: To multiply a vector by the MDS matrix $\boldsymbol{D}(A_{rxr}H)$ with irreducible characteristic polynomial.

Input:

- Same as algorithm 1
- the values $l_i \in \mathbb{F}_{\mathbf{2}^s}$, $i = \overline{0, r-1}$ determined in the previous step.
- Permutational matrix that determines the permutation π.
- $(a_0, a_1, \dots., a_{r-1})$; $a_i \in \mathbb{F}_{\mathbf{2}^s}$

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

Receive: $(a_0, a_1, \dots., a_{r-1})$

$(a_0, a_1, \dots., a_{r-1}) = (l_0a_0, l_1a_1, \dots., l_{r-1}a_{r-1})$

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

$(a_0 + a_1x + \cdots + a_{r-1}x^{r-1})(x^{\mu_1}))\ mod g(x) = (\hat{a}_0 + \hat{a}_1x + \ldots + \hat{a}_{r-1}x^{r-1})$

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

$(a_0, a_1, \ldots., a_{r-1}) = \left(a_{\pi(0)}, a_{\pi(1)}, \ldots, a_{\pi(r-1)}\right)$

Return: $(a_0, a_1, \ldots., a_{r-1})$

Observations:

1. Calculating the inverse matrix $(A_{rxr})^{-1}$ with irreducible characteristic polynomial and multiplying a vector by it is done with the use of algorithms presented in (Arrozarena and Fiallo 2022).
2. If $e(\text{odd})$ is the order of the polynomial $g(x) = (g_0 + g_1x + \cdots + g_{r-1}x^{r-1} + x^r)$ which is the generating polynomial of a nontrivial linear MDS code [n, k, d] over $\mathbb{F}_{2^s}$ then if $l_i = (e-1)/2$ is used to multiply a vector by the MDS matrix A_{rxr}, the multiplication of a vector by its inverse matrix is carried out with $l_i = 1 + (e-1)/2$ and having as MDS matrix inverse $B_{rxr}A_{rxr}$ where B_{rxr} is the companion matrix of the polynomial $g(\text{x})$.
3. If $l_i = r$ only $2r$ values of $\mathbb{F}_{2^s}$ are required at most to multiply a vector by the MDS matrix with irreducible characteristic polynomial and $3r$ values to multiply a vector by its inverse.
4. The above algorithm was performed for when the matrix is $D(A_{rxr}H)$ where H is a permutational matrix and D is a non-singular diagonal matrix, but can be performed in addition for the following cases:$(\text{A}_{rxr}H)D$, $D(H\text{A}_{rxr})$, $(\text{A}_{rxr}H)D$, $H(DA_{rxr})$, $H(A_{rxr}\ D)$, $(DA_{rxr})\ H$, $(A_{rxr}\ D)H$ .The use of these variants leads to adjustments in Algorithm 3.

Results and discussion

This article aims only to present the new algorithm, to expose its implementation, its applications in different contexts, as well as the validation of its results another article is prepared by the authors.

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

We now present two examples of application of the proposed algorithm.

Example 1:

Let be the field $\mathbb{F}_{2^4}$

$\mathbb{F}_{2^4} \sim \mathbb{F}_{2^4}[\alpha]/\langle \alpha^4 + \alpha + 1 \rangle$

Step 1: A 3x3 MDS square matrix is generated according to Algorithm 1 using as the generating polynomial of a nontrivial MDS code [15, k, d] over the field $\mathbb{F}_{2^4}$ a.

$g(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3) = x^3 + x^2(\alpha + \alpha^2 + \alpha^3) + x(1 + \alpha^2 + \alpha^3) + \alpha^2 + \alpha^3$

$$A = \begin{pmatrix} \alpha^2 + \alpha^3 & 1 + \alpha^2 + \alpha^3 & \alpha + \alpha^2 + \alpha^3 \\ \alpha^2 & \alpha + \alpha^2 & \alpha + \alpha^2 \\ \alpha + \alpha^2 + \alpha^3 & \alpha^2 + \alpha^3 & \alpha^2 \end{pmatrix}$$

Step 2: Its characteristic polynomial is $P(x) = x^3 + x^2(\alpha + \alpha^2 + \alpha^3) + x\alpha^2 + \alpha^3$ has no roots in the field $\mathbb{F}_{2^4}$ therefore it is irreducible.

In this case the l_i are equal to one i.e. the diagonal matrix and the permutation matrix coincide with the identity matrix.

As the matrix is MDS and its characteristic polynomial is irreducible, we go to step 6 of the proposed algorithm, that is, we apply algorithm 6 to multiply a vector by a MDS matrix with irreducible characteristic polynomial.

Step 6: The input of the algorithm would be the vector $(a_0, a_1, a_2) = (1 + \alpha + \alpha^3, 1 + \alpha^2, 1 + \alpha)$

$(1 + \alpha + \alpha^3 + (1 + \alpha^2)x + (1 + \alpha)x^2)(x^5))\ mod g(x) = (1 + \alpha^2 + \alpha^3, 0, \alpha^2 + \alpha^3)$

Return: $(1 + \alpha^2 + \alpha^3, 0, \alpha^2 + \alpha^3)$

Example 2:

Let be the field $\mathbb{F}_{2^8}$

$\mathbb{F}_{2^8} \sim \mathbb{F}_{2^8}[\alpha]/\langle \alpha^8 + +\alpha^5 + \alpha^3 + \alpha + 1 \rangle$

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

Step 1: A 4x4 MDS square matrix is generated according to Algorithm 1 with parameter $\mu_1 = 4$ using as a non-trivial code generator polynomial MDS [255, k, d] over the field $\mathbb{F}_{2^8}$.

g(x)= $(x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4)$

$$M = \begin{pmatrix} \alpha^7+\alpha^5+\alpha^3+\alpha^2 & \alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1 & \alpha^7+\alpha^6+\alpha^4+\alpha^3 & \alpha^4+\alpha^3+\alpha^2+a \\ \alpha^7+\alpha^4+a^2+\alpha+1 & \alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha & \alpha^6+\alpha^5+\alpha^4+\alpha^2+1 & \alpha^7+\alpha^5+\alpha^2+\alpha+1 \\ \alpha^5+1 & \alpha^6+\alpha^2 & \alpha^7+a^2+1 & \alpha^5+\alpha^4 \\ \alpha^2 & \alpha^6+\alpha^5+\alpha^3 & \alpha^7+\alpha^6+\alpha^4+\alpha^3 & \alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha+1 \end{pmatrix}$$

Step 2: The characteristic polynomial of this matrix $PC(x) = x^4 + (\alpha^2 + \alpha^4 + \alpha^5)x^3 + (\alpha + \alpha^3)x^2 + (\alpha + \alpha^7)x + (\alpha + \alpha^3 + \alpha^5 + \alpha^6)$is reducible, it has four roots in the field $\mathbb{F}_{2^8}$ which are $\mathbb{F}_{2^8}$: $\{\alpha^4 + 1, \alpha^5 + \alpha^3 + \alpha + 1, \alpha^7 + \alpha^6 + \alpha^5 + \alpha^2 + \alpha, \alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + 1\}$.

Step 3: The matrix M is given permutations of the rows determined by the permutation matrix $H = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$. Then the matrix $A = HM_{4\times4}$ has characteristic polynomial $PC_A(x) = x^4 + (\alpha + \alpha^2 + \alpha^3 + \alpha^7)x^3 + (\alpha + \alpha^2 + \alpha^4 + \alpha^5)x^2 + (1 + \alpha + \alpha^4 + \alpha^7)x + (\alpha + \alpha^3 + \alpha^5 + \alpha^6)$ irreducible in the field $\mathbb{F}_{2^8}$. Then taking the diagonal matrix $D = I_{4\times4}$ we have that the matrix resulting from operating $D(HM_{4\times4})$, denoted as M', is an MDS matrix with irreducible characteristic polynomial.

$$M' = \begin{pmatrix} \alpha^5+1 & \alpha^6+\alpha^2 & \alpha^7+a^2+1 & \alpha^5+\alpha^4 \\ \alpha^7+\alpha^5+\alpha^3+\alpha^2 & \alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1 & \alpha^7+\alpha^6+\alpha^4+\alpha^3 & \alpha^4+\alpha^3+\alpha^2+a \\ \alpha^2 & \alpha^6+\alpha^5+\alpha^3 & \alpha^7+\alpha^6+\alpha^4+\alpha^3 & \alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha+1 \\ \alpha^7+\alpha^4+a^2+\alpha+1 & \alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha & \alpha^6+\alpha^5+\alpha^4+\alpha^2+1 & \alpha^7+\alpha^5+\alpha^2+\alpha+1 \end{pmatrix}$$

Therefore, it is not necessary to perform Steps 4 and 5 of the procedure and one can proceed directly to perform **Step 6** by executing Algorithm 3. It should be noted that, when performing permutations of the rows of the matrix M, the permutation performed at the end of Algorithm 3 on the output vector is carried over to the initial stage before performing the multiplication of the polynomials as presented below:

Input:

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 4, Octubre-Diciembre, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-17

- g(x)= $(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$ generator polynomial of a non-trivial MDS code [255, k, d] over the field $\mathbb{F}_{2^8}$.
- $\mu_1 = 4$
- the values of $l_i = 1$, $i = 0,1,2,3$.
- Permutational matrix that determines the permutation π
- $(a_0, a_1, a_2, a_3) = (1, \alpha, \alpha^2, \alpha^3) \in \mathbb{F}_{2^8}^4$

Receive: (a_0, a_1, a_2, a_3)

$(a_0, a_1, a_2, a_3) = (1, \alpha, \alpha^2, \alpha^3)$ since all $l_i = 1$

Taking as permutational matrix the matrix H obtained in Step 3 we then have that:

$(a_0, a_1, a_2, a_3) = (1, \alpha, \alpha^2, \alpha^3) * H = (\alpha, \alpha^3, 1, \alpha^2)$

$(\alpha + (\alpha^3)x + (1)x^2 + (\alpha^2)x^3)(x^4))\ mod\ g(x)$

$= (\alpha + \alpha^2 + \alpha^4 + \alpha^6 + (1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5)x + (\alpha + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^7)x^2 + (\alpha)x^3)$

Return $(\alpha + \alpha^2 + \alpha^4 + \alpha^6, 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5, \alpha + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^7, \alpha)$

Conclusions

In this work, an algorithm for multiplying a vector by an MDS matrix or its inverse is presented. The characteristic polynomial of the matrix is irreducible and the algorithm has as input parameters:

1. The polynomial generator of a nontrivial linear MDS code [n, k, d] over $\mathbb{F}_{2^s}$.
2. $3(n-k)$ values of the $\mathbb{F}_{2^s}$ for the multiplication of a vector by a $(n-k)$ x $(n-k)$ MDS matrix over $\mathbb{F}_{2^s}$ and $4(n-k)$ values for the multiplication of the vector by the inverse matrix. The paper presents the particular case in which $(n-k)+\mathbf{1}$ values of the $\mathbb{F}_{2^s}$ are needed for the multiplication of a vector by a $(n-k)$ x $(n-k)$ MDS matrix over $\mathbb{F}_{2^s}$ and $2(n-k)+1$ values for the multiplication of the vector by the inverse matrix.

It is noted that a random selection of the matrix is carried out by randomly selecting irreducible polynomial.

References

Ali, M.Y. Y Khan, I.A., 2020. Computing Determinants Of Block Matrices. ,

Arrozarena, P.F. Y Fiallo, E.D., 2022. Efficient Multiplication Of A Vector By A Matrix Mds. *Journal Of Science And Technology On Information Security*, Vol. 3, No. 17, Issn 2615-9570.

Ashdhir, P., Arya, J. Y Rani, C.E., 2021. Exploring The Fundamentals Of Fast Fourier Transform Technique And Its Elementary Applications In Physics. *European Journal Of Physics*, Vol. 42, No. 6, Issn 0143-0807.

Baylis, D.J., 2018. *Error Correcting Codes: A Mathematical Introduction*. S.L.: Routledge. Isbn 0-203-75667-3.

De Piccoli, A., Visconti, A. Y Rizzo, O.G., 2020. Polynomial Multiplication Over Binary Finite Fields: New Upper Bounds. *Journal Of Cryptographic Engineering*, Vol. 10, No. 3, Issn 2190-8508.

Dickinson, B.W., 2019. Matrices And Linear Algebra. *Control System Fundamentals*. S.L.: Crc Press, Pp. 33-50.

Gao, H., Han, G., Sun, Y., Sun, F. Y Ren, Y., 2020. Block H-Matrices And Spectrum Of Block Matrices. *Journal Of Physics: Conference Series*. S.L.: Iop Publishing, Pp. 012114. Vol. 1575. Isbn 1742-6596.

Grassi, L., Rechberger, C. Y Schofnegger, M., 2020. Proving Resistance Against Infinitely Long Subspace Trails: How To Choose The Linear Layer. *Cryptology Eprint Archive*,

Guo, J., Jean, J., Nikolić, I., Qiao, K., Sasaki, Y. Y Sim, S.M., 2016. Invariant Subspace Attack Against Midori64 And The Resistance Criteria For S-Box Designs. *Cryptology Eprint Archive*,

Gupta, K.C., Pandey, S.K., Ray, I.G. Y Samanta, S., 2019. Cryptographically Significant Mds Matrices Over Finite Fields: A Brief Survey And Some Generalized Results. *Advances In Mathematics Of Communications*, Vol. 13, No. 4, Issn 1930-5346.

Gupta, K.C., Pandey, S.K. Y Samanta, S., 2023. On The Direct Construction Of Mds And Near-Mds Matrices. *Arxiv Preprint Arxiv:2306.12848*,

Gupta, K.C., Pandey, S.K. Y Venkateswarlu, A., 2017. On The Direct Construction Of Recursive Mds Matrices. *Designs, Codes And Cryptography*, Vol. 82, Issn 0925-1022.

Gupta, K.C., Pandey, S.K. Y Venkateswarlu, A., 2019. Almost Involutory Recursive Mds Diffusion Layers. *Designs, Codes And Cryptography*, Vol. 87, Issn 0925-1022.

Kaddoura, I. Y Mourad, B., 2022. On A Special Class Of Block Matrices And Some Applications. *Arxiv Preprint Arxiv:2212.13291*,

Kesarwani, A., Sarkar, S. Y Venkateswarlu, A., 2019. Exhaustive Search For Various Types Of Mds Matrices. *Iacr Transactions On Symmetric Cryptology*, Issn 2519-173x.

Kostrikin, A.I., 1983. *Introducción Al Álgebra*. Segunda. Moscú: Mir.

Liu, X., Zhao, Z., Liu, W.-H. Y Jin, X.-Q., 2022. *An Introduction To Linear Algebra*. S.L.: Edp Sciences. Isbn 2-7598-3045-4.

Luong, T.T., Cuong, N.N. Y Tho, H.D., 2019. Constructing Recursive Mds Matrices Effective For Implementation From Reed-Solomon Codes And Preserving The Recursive Property Of Mds Matrix Of Scalar Multiplication. *Journal Of Informatics & Mathematical Sciences*, Vol. 11, No. 2, Issn 0974-875x.

Macwilliams, F.J. Y Sloane, N.J.A., 1977. *The Theory Of Error-Correcting Codes*. S.L.: Elsevier. Vol. 16. Isbn 0-444-85010-4.

Mennink, B. Y Neves, S., 2021. On The Resilience Of Even-Mansour To Invariant Permutations. *Designs, Codes And Cryptography*, Vol. 89, No. 5, Issn 0925-1022.

Noriega Sánchez, T. Y Arazoza Rodríguez, H., 2003. *Algebra Tomo I*. Primera Reimpresión. S.L.: Félix Varela. Isbn 959-258-490-7.

Peterson, W.W. Y Weldon, E.J., 1972. *Error-Correcting Codes*. S.L.: Mit Press. Isbn 0-262-16039-0.

Saadetoğlu, M. Y Dinsev, Ş.M., 2023. Inverses And Determinants Of N× N Block Matrices. *Mathematics*, Vol. 11, No. 17, Issn 2227-7390.

Todo, Y., Leander, G. Y Sasaki, Y., 2019. Nonlinear Invariant Attack: Practical Attack On Full Scream, I Scream, And Midori 64. *Journal Of Cryptology*, Vol. 32, No. 4, Issn 0933-2790.

Varela, M.V., 2008. *Álgebra Lineal*. La Habana,Cuba: Félix Varela. Isbn 959-528-533-4.

Conflict of Interest

The authors authorize the distribution and use of their article.

Authors' contributions

Conceptualization: Pablo Freyre Arrozarena, Oristela Cuellar Justiz.

Data curation: Pablo Freyre Arrozarena, Oristela Cuellar Justiz, Ramses Rodríguez Aulet.

Formal analysis: Pablo Freyre Arrozarena, Oristela Cuellar Justiz.

Research: Pablo Freyre Arrozarena, Oristela Cuellar Justiz, Ramsés Rodríguez Aulet.

Methodology: Pablo Freyre Arrozarena.

Project Administration: Pablo Freyre Arrozarena.

Resources: Ramsés Rodríguez Aulet, Alejandro Freyre Echevarría.

Software: Oristela Cuellar Justiz; Alejandro Freyre Echevarría.

Supervision: Pablo Freyre Arrozarena.

Validation: Oristela Cuellar Justiz; Alejandro Freyre Echevarría.

Visualization: Pablo Freyre Arrozarena, Oristela Cuellar Justiz.

Writing - original draft: Pablo Freyre Arrozarena.

Writing - proofreading and editing: Oristela Cuellar Justiz.