IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Matemática computacional

Aritmética sobre Torres de Campos Finitos de característica dos, aplicada a la generación de polinomios primitivos

Aritmetic on Tower over Finite Field of characteristic two, applied to primitive polynomials generation

Alberto Pérez Roble [1*], Beatriz Pérez López [2], Oristela Cuellar Justiz [3], Evaristo J. Madarro Capó [4]

[1]Empresa Eléctrica Sancti Spíritus. Calle 1ra del Oeste final. Reparto Colón. Sancti Spíritus. Cuba. aproble91@gmail.com
[2]Universidad de Sancti Spíritus José Martí Pérez. Ave. Comandante Fajardo s/n. Olivos 1. Sancti Spíritus. Cuba. beatrizpl@uniss.edu.cu
[3]Universidad de las Ciencias Informáticas. Torrens. La Habana. Cuba. Carretera San Antonio km 2 1/2. Código Postal 17100. oristelacj@uci.cu
[4]Universidad de La Habana. Instituto de Criptografía. San lázaro y L. Plaza de la Revolución. La Habana. Cuba. jcapovc@gmail.com

*Autor para correspondencia: aproble91@gmail.com

Resumen
Con el avance de la Criptografía y las nuevas herramientas puestas a su disposición, la seguridad de los algoritmos criptográficos se basa principalmente en el empleo de campos finitos de grandes dimensiones lo que dificulta la aritmética sobre ellos, además los sistemas simétricos que emplean polinomios primitivos sobre estos campos, también presentan grandes dificultades para la determinación de los mismos. En este trabajo se analizan las torres de campos finitos como herramienta para lograr una aritmética eficiente, también se exponen ejemplos de estas, a través de la representación de los elementos, pertenecientes a campos de característica dos en bases normales, haciendo énfasis en la operación de exponenciación. Por último, se propone el empleo de torres de campos sobre bases normales en el cálculo del polinomio mínimo, operación fundamental y de mayor complejidad en el algoritmo de generación de polinomios primitivos de E. Madarro en 2017.

Palabras claves: Torres de campos finitos, bases normales, polinomios primitivos.

Abstract
With the advancement of cryptography and the new tools made available, the security of cryptographic algorithms is based mainly on the use of finite fields of big dimensions what makes difficult the arithmetic on them, besides the symmetrical systems that use primitive polynomials on these fields, also present great difficulties for the determination of the same. In this work we analyze the towers of finite fields as a tool for efficient arithmetic, examples of these are also given, through the representation of the elements, belonging to fields of characteristic two on normal bases, emphasizing in exponentiation operation. Finally, is analyzed a proposal that employs towers with representation on normal bases in the algorithm of generation of primitive polynomials exposed by E. Madarro in 2017.

Keywords: *Tower finite field, normal bases, primitive polynomials, arithmetic*

Introducción

Muchos de los algoritmos criptográficos, fundamentan su seguridad a partir de la dimensión del campo donde se trabaja. De esta manera, existe una tendencia a utilizar campos de gran cardinalidad para diseñar algoritmos criptográficos. Así mismo, mientras que se busca poseer una seguridad considerable frente a los ataques que existen y los medios de cómputos actuales, los diseños tienden a utilizar operaciones más costosas desde un punto de vista computacional. Así, se hace necesario, determinar una vía que permita reducir de alguna manera el costo de las operaciones sobre campos grandes empleando una aritmética rápida. La aritmética en torres de campos finitos es muy usada para este fin, ya que poseen características esenciales para una aritmética más eficiente. Entre los primeros trabajos vinculados a la criptografía, donde se emplean las torres de campos finitos se encuentran: *"Efficient Algorithms for Finite Fields, with Applications in Elliptic Curve Cryptography"* Baktir (2003), realizado por Baktir y Sunar en el 2003, y un año más tarde *"Optimal Tower Fields"* Baktir and Sunar (2004) y *"Optimal Tower Fields for Hyperelliptic Curve Cryptosystems"* Baktir et˜al. (2004), donde introducen las torres de campos óptimas las cuales constituyen una clase especial de extensiones de campos óptimas introducidas por Bailey y Paar en *"Optimal Extension Fields for fast arithmetics in public-key algorithms"* Bailey and Paar (1998). Con el transcurso de los años se han empleado en las operaciones de los emparejamientos bilineales para curva elípticas tal como lo abordan los trabajos de Kerins et˜al. (2005), Cortez (2009) y González (2010). Otros autores las han empleando en la implementación de dispositivos FPGA como Velásquez and Castaño (2013). También, se han implementado de forma eficiente, operaciones sobre torres de campos en las S-cajas del AES como se muestra en los trabajos Bonnecaze et˜al. (2013), Ueno et˜al. (2015), Reyhani-Masoleh et˜al. (2018b), Reyhani-Masoleh et˜al. (2018a) . Además, las torres se han empleado como herramientas en el diseño de cifradores de flujo, así lo muestran los trabajos de Fan et˜al. (2013), Zidaric (2014) y Zidaric et˜al. (2019). Los detalles sobre estos y otros trabajos en donde se emplean las torres de campos dentro de la Criptografía se pueden encontrar en Pérez˜Roble (2017).

Por otra parte, los polinomios primitivos son de vital importancia por su utilización en los diseños de algunos componentes de los criptosistemas simétricos existentes como los LFSRs (*Registros de Desplazamiento con Realimentación Lineal*) Golomb (1982); Mullen and Panario (2013); Delgado (2010); Peralta (2005); Fan et˜al. (2013); Zidaric (2014); Zidaric et˜al. (2019); El-Razouk et˜al. (2015), en cifradores en flujo, en generación de matrices MDS (*Maximum Distance Separable*) Junod and Vaudenay (2004); Pérez (2014); Freyre et˜al. (2014); Dehnavi et˜al. (2014); Gupta and Ray (2015); Cuellar (2017); Gupta and Pandey (2017); Mahmoodi et˜al. (2019) y en cifradores en bloque (*AES*). En el 2017, E. Madarro Madarro (2017), Madarro and Cuellar

(2021) presentó un algoritmo de generación de polinomios primitivos sobre $\mathbb{F}_{2^m}$, el cual se descompone en tres partes fundamentales: la búsqueda de los cosetos q-ciclotómicos, el cálculo del polinomio mínimo y el cálculo del polinomio reverso; siendo la segunda la de mayor complejidad ya que es en donde intervienen operaciones de multiplicación y exponenciación; debido a esto surge la necesidad de encontrar herramientas que permitan reducir la cantidad de operaciones a realizar en dicho algoritmo. Para esto se llevó a cabo un estudio de diferentes métodos escogiendo el empleo de las torres de campos finitos en bases normales por las ventajas que proporcionan para el cálculo. El objetivo de este trabajo es aplicar bases normales sobre torres de campos finitos en las operaciones de multiplicación y exponenciación que intervienen en el cálculo del polinomio mínimo del algoritmo propuesto por E. Madarro. Este artículo forma parte de los resultados obtenidos en la tesis de maestría Pérez˜Roble (2019) (*Aritmética sobre Torres de Campos Finitos de característica dos, aplicada a la generación de polinomios primitivos*) presentada en la Universidad de La Habana en el 2019.

Materiales y métodos o Metodología computacional

En la literatura se presentan varios algoritmos para la generación de polinomios primitivos, entre los que se encuentran: *"Porto, Guida y Montolivo"* di˜Porto et˜al. (1992), propuesto por A. Di Porto, F. Guida y E. Montolivo en 1993; *"G. Filho y D. Filho"* da˜Silva and Lima (1993), presentado en 1993 por Joel Guilherme da Silva Filho y Dimas de Queiroz Lima Filho; *"Rifa y Borrell"* Rifa and Borrell (1995) de 1995 construido por J. Rifa, y J. Borrell; *"FactorPower"*, propuesto por Saxena y McCluskey en 2004 Saxena and MacCuskey (2004); y los algoritmos de *"Shoup"* Shoup (1999, 2008) presentados en 1999 y 2008, respectivamente.

En el 2017, E. Madarro Madarro (2017) presenta un algoritmo de generación de polinomios primitivos sobre $\mathbb{F}_{2^m}$; empleando como entradas: dos polinomios primitivos f y g de grados m y n respectivamente, los cuales definen las extensiones $\mathbb{F}_{2^m}$ y $\mathbb{F}_{(2^m)^n}$; un elemento primitivo a del campo $\mathbb{F}_{q^n}$, donde $q = 2^m$. El primer paso del algoritmo propuesto por Madarro, busca los cosetos líderes q-ciclotómicos módulo $q^n - 1$ asociados a los elementos del campo, que a su vez constituyen elementos primitivos descritos en Cuellar et˜al. (2016); Madarro and Cuellar (2016). Luego de obtenido los cosetos, se realiza el cálculo del polinomio mínimo para cada conjunto formado por los elementos $\alpha^h, \alpha^{hq}, \alpha^{hq^2}, ..., \alpha^{hq^{n-1}}$, siendo está la operación más costosa debido a la cantidad de operaciones (multiplicaciones y exponenciaciones) a realizar. Por último, se calcula su polinomio reverso, ya que este también es primitivo.

Con el fin de encontrar formas más eficientes para el cómputo de las operaciones en campos finitos, varios autores han expuestos disimiles enfoques; siendo el trabajo sobre torres de campos uno de los más llamativos. Las torres de campos finitos permiten reducir la cantidad de operaciones aritméticas a realizar en los subcampos contenidos en él.

Una torre sobre un campo finito F es estrictamente un conjunto de extensiones finitas de F las cuales están totalmente ordenadas por inclusión, Mullen and Panario (2013).

Definición 1 (Torres de campos) Sean $F_1, F_2, ..., F_k$ campos finitos tal que $F_1 \subset F_2 \subset F_3 \subset ... \subset F_{k-1} \subset F_k$. Entonces se llama a $F_k/.../F_2/F_1$ una torre de campos.

Otro de los aspectos considerados para reducir la cantidad de operaciones fue el tipo de base empleada en la descripción de los campos finitos y las ventajas operacionales de las mismas. El algoritmo propuesto por Madarro, trabaja los elementos descritos a través de una base polinomial sobre el campo primo, una de las más conocidas y estudiadas; no obstante se decidió analizar el mismo si se considera la representación de los elementos a través de una base normal por las ventajas de la operación de exponenciación en las mismas. Las definiciones, proposiciones y teoremas, sobre las torres de campo, las bases normales y sus operaciones se encuentran en Mullen and Panario (2013); Lidl and Niederreiter (1986); Fraleigh (2003).

Definición 2 Sea $\mathbb{F}_{q^n}$ una extensión del campo $\mathbb{F}_q$, un elemento $\gamma \in \mathbb{F}_{q^n}$ se denomina elemento normal sobre $\mathbb{F}_q$ si el sistema $\left\{\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^i}, \ldots, \gamma^{q^{n-1}}\right\}$ formado por γ y sus conjugados es un sistema linealmente independiente.

Definición 3 Sea $\gamma \in \mathbb{F}_{q^n}$. Donde $\mathbb{F}_{q^n}$ es una extensión de $\mathbb{F}_q$ donde q es la potencia de un primo. El sistema

$$B_N = \{\gamma, \gamma^q, ..., \gamma^{q^{n-1}}\}$$

es una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ si γ constituye un elemento normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Teorema 1 (Existencia) Para cualquier campo finito K y cualquier extensión finita F de K, existe una base normal de F sobre K.

Toda base normal posee una tabla de multiplicar, la cual constituye una matriz $n \times n$, cuyas entradas son las coordenadas c_{ij} del producto $\gamma \cdot \gamma^{q^k}$ en la base normal.

La operación de multiplicación entre elementos representados a través de bases normales tiende a facilitarse pues los productos entre los elementos de la base ya están definidos en la tabla de multiplicar de la base, o sea:

Sean los elementos $\beta_1, \beta_2 \in \mathbb{F}_{q^n}$ representados de la forma:

$$\beta_1 = \sum_{i=0}^{n-1} a_i \gamma^{q^i} \quad \text{y} \quad \beta_2 = \sum_{j=0}^{n-1} b_j \gamma^{q^j} \quad \text{donde} \quad a_i, b_j \in \mathbb{F}_q.$$

Entonces,

$$\beta_1 \cdot \beta_2 = (\sum_{i=0}^{n-1} a_i \gamma^{q^i})(\sum_{j=0}^{n-1} b_j \gamma^{q^j}) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(a_i b_j)\gamma^{q^i} \cdot \gamma^{q^j},$$

calculando los productos $\gamma^{q^i} \cdot \gamma^{q^j}$ siendo $i \leq j$ se obtiene:

$$\begin{aligned} \gamma^{q^i} \cdot \gamma^{q^j} &= \gamma^{q^i + q^j} \\ &= \gamma^{q^i(1+q^{j-i})} \\ &= (\gamma^{1+q^{j-i}})^{q^i} \\ &= (\gamma \cdot \gamma^{q^{j-i}})^{q^i} \end{aligned} \tag{1}$$

Las coordenadas del producto $\gamma \cdot \gamma^{q^{j-i}}$ en la base normal están en la tabla de multiplicar de la base.

En el campo $\mathbb{F}_{q^n}$, tomando como base normal $\{\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}}\}$ el cálculo de potencias del tipo q^i, se realiza a través de la siguiente proposición:

Proposición 1 Sea $\beta = b_0\gamma + b_1\gamma^q + +... + b_{n-1}\gamma^{q^{n-1}}$ y sea $\bar{\beta} = (b_0, ..., b_{n-1})$ un vector formado por los coeficientes de β. Entonces, a β^{q^i} le corresponde el vector $\bar{\beta}_i$ con $0 \leq i \leq n-1$, donde $\bar{\beta}_i$ es un corrimiento de i lugares hacia la derecha de $\bar{\beta}$, es decir

$$\bar{\beta}_i = (b_{n-i}, b_{n-i+1}, ..., b_{n-1}, b_0, ..., b_{n-i-2}, b_{n-i-1}).$$

Cosetos ciclotómicos y bases normales

Uno de los principales pasos del algoritmo de generación de polinomios primitivos es el cálculo de los cosetos líderes (h) q-ciclotómicos módulo $q^n - 1$, por lo que se tiene el conjunto $\{h, hq, hq^2, ..., hq^{n-1}\}$ a partir del cual se construyen los conjugados del elemento β^h que se emplean en el cálculo del polinomio mínimo.

La forma que tienen dichos cosetos es análoga a la forma de los exponentes de los elementos de una base normal. Por lo que, si se emplea una base normal $\{\gamma, \gamma^q, \gamma^{q^2}, ..., \gamma^{q^{n-1}}\}$ sobre $\mathbb{F}_{q^n}$ y siendo β un elemento primitivo de $\mathbb{F}_{q^n}$, para calcular los elementos $\beta^h, \beta^{hq}, \beta^{hq^2}, ..., \beta^{hq^{n-1}}$, solo es necesario calcular las coordenadas de β^h en la

base normal, ya que las demás potencias van a ser corrimientos de estas, por la proposición 1.

Torres de campos con bases normales

El análisis de la aritmética en las torres se realiza a través del comportamiento de esta en cada una de las extensiones que la integran, debido a que las torres varían en cuanto cantidad de extensiones y la cardinalidad de cada extensión se vuelve muy complejo la generalización de las operaciones Bonnecaze et˜al. (2013).

Teniendo en cuenta que todos los campos finitos, que poseen la misma cardinalidad, son isomorfos; muchos trabajos en donde se emplean estos, se apoyan en torres y se construye el campo sobre el que se desea trabajar como una extensión de algún subcampo contenido estrictamente en él y no necesariamente sobre el campo primo o sobre algún campo base como se explicó con anterioridad. A pesar de que estos campos son isomorfos, la complejidad de sus operaciones es diferente.

Las torres T_1 y T_2 son dos variantes que se pueden obtener del campo $\mathbb{F}_{q^n}/\mathbb{F}_q$ donde n se descompone en $n_1 \cdot n_2$, aunque no son las únicas ya que se pueden construir otras torres combinando las cantidad de divisores n.

$$\begin{array}{ccccc} T_0 & & T_1 & & T_2 \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{F}_{q^n} & \cong & \mathbb{F}_{(q^{n_1})^{n_2}} & \cong & \mathbb{F}_{(q^{n_2})^{n_1}} \\ | & & | & & | \\ \mathbb{F}_q & & \mathbb{F}_{q^{n_1}} & & \mathbb{F}_{q^{n_2}} \\ & & | & & | \\ & & \mathbb{F}_q & & \mathbb{F}_q \end{array}$$

El empleo de las bases normales dentro del trabajo con las torres de campos conlleva a identificar elementos normales de la torre. Además se hace necesario, para poder implementar las operaciones, la tabla de multiplicar de la base normal escogida. Como en este trabajo solo se emplearán las torres conformadas por 2 extensiones (T_1, T_2) solo es necesario dos tablas de multiplicar de tamaño $n_1 \times n_1$ y $n_2 \times n_2$ para describir los elementos en cada una de ellas, que brindan ventaja en espacio si se considera que la tabla de multiplicar del campo $\mathbb{F}_{q^n}$ tiene tamaño $n \times n$.

Resultados y discusión

Exponenciación

Antes de introducir la exponenciación, se analiza la multiplicación usual, la cual opera elemento a elemento. La cantidad de operaciones que realiza está relacionada directamente con la dimensión del campo donde se trabaja, en el caso de $\mathbb{F}_{q^n}$ se realizan n^2 operaciones. Para representar de forma más cómoda las operaciones, se denota a las multiplicaciones y exponenciaciones triviales con las letras M y E respectivamente.

La multiplicación entre elementos de las torres T_1 o T_2 se realiza de la misma manera que se indicó anteriormente, apoyándose en sus correspondientes tablas de multiplicar, por lo que en T_1 se realizan $(n_2)^2$ operaciones en $\mathbb{F}_{(q^{n_1})^{n_2}}$ y de forma análoga en T_2, $(n_1)^2$ operaciones en $\mathbb{F}_{(q^{n_2})^{n_1}}$ como se muestra en la Tabla 1. Ya que esta operación se comporta de la misma manera en dichas torres, de ahora en lo adelante se hace referencia solo a T_1 y se denota como $\hat{M}$ a las multiplicaciones que se realizan en esta y $\bar{M}$ a las multiplicaciones en T_0.

Tabla 1: Comportamiento de la multiplicación en T_0, T_1 y T_2

	T_0	T_1	T_2
Multiplicación	n^2M	$(n_2)^2M$	$(n_1)^2M$

La exponenciación es una de las operaciones más costosas, por lo que se hace necesario emplear mejores métodos de exponenciación. Uno de estos es el clásico método de exponenciación binaria del exponente Knuth (1997), el cual emplea la expansión binaria de este utilizando $\log_2(t)$ multiplicaciones y $\log_2(t)$ exponenciaciones.

En este caso, se emplean las características del método anterior con algunas modificaciones a la hora de representar el exponente para realizar la operación β^t, con $\beta \in \mathbb{F}_{q^n}$. Para esto, t se descompone de la siguiente forma,

$$t = a_0q^0 + a_1q^1 + ... + a_iq^i + ... + a_{z-1}q^{z-1},$$

donde a_i son todas las potencias de 2 menores que q, siendo q potencia de 2. Esta forma de representación está dada para aprovechar la proposición 1, en la exponenciación con bases normales.

Con este tipo de representación, una elevación a cualquier potencia t se reduce a k exponenciaciones, siendo k las potencias de 2 menores que q de la representación de t y $w(t) - 1$ multiplicaciones, donde $w(t)$ es el peso de Hamming del vector que representa t en base 2. Además, $w(t)$ puede ser acotado superiormente con $\lceil \log_2 t \rceil + 1$ ya que este representa la cantidad de lugares que se necesitan para representar a t en base 2 y k a su vez puede ser también acotado con $\log_2 q$.

Tabla 2: Cantidad de operaciones para calcular $\beta^t \in \mathbb{F}_{q^n}$

Exponenciación	**Operaciones en $\mathbb{F}_{q^n}$**
Método propuesto ($\hat{E}$)	$(\log_2 t)M + (\log_2 q)E$
Método binario ($\bar{E}$)	$(\log_2 t)M + (\log_2 t)E$

La Tabla 2 muestra la cantidad de operaciones como máximo que se necesitan para calcular $\beta^t \in \mathbb{F}_{q^n}$ con el método de exponenciación propuesto en bases normales ($\hat{E}$) y el método binario en base polinomial ($\bar{E}$), donde se puede apreciar la disminución de operaciones del primero frente al último.

Aplicando los métodos de exponenciación descritos anteriormente $\hat{E}$ en T_1 y $\bar{E}$ en T_0 nos queda lo siguiente.

- El método $\hat{E}$ en T_1 realiza $(\log_2 t)\hat{M}+(\log_2 q^{n_1})E$, donde se tiene que $\hat{M}$ representa $(n_2)^2$ multiplicaciones en T_1.
- El método $\bar{E}$ en T_0 realiza $(\log_2 t)\bar{M} + (\log_2 t)E$, donde $\bar{M}$ representa $(n)^2$ multiplicaciones en T_0.

Tabla 3: Cantidad de operaciones en los métodos de exponenciación $\hat{E}$ en T_1 y $\bar{E}$ en T_0.

Exponenciación	**Operaciones en T_1 y T_0**
Método propuesto ($\hat{E}$)	$(\log_2 t)(n_2)^2M + (\log_2 q^{n_1})E$ en T_1
Método binario ($\bar{E}$)	$(\log_2 t)n^2M + (\log_2 t)E$ en T_0

En la Tabla 3 se puede apreciar la disminución de operaciones a realizar del método $\hat{E}$ en T_1 frente a $\bar{E}$ en T_0, ya que n_2 es un divisor de n y q^{n_1} forma parte de la descomposición del exponente t.

Torres de Campos en el cálculo de polinomio mínimo

El objetivo del algoritmo de Madarro es calcular los polinomios primitivos de grado n sobre un campo $\mathbb{F}_q$ y como bien se observó las operaciones entre binomios y las potencias para hallar los conjugados se realiza con elementos de $\mathbb{F}_{q^n}$. Para emplear las torres se asume que n se puede expresar como el producto de n_1 y n_2 lo que permite construir una torre formada por las siguientes campos extendidos: $\mathbb{F}_q$, $\mathbb{F}_{q^{n_1}}$, $\mathbb{F}_{(q^{n_1})^{n_2}}$. Dado que $\mathbb{F}_{q^n}$ y $\mathbb{F}_{(q^{n_1})^{n_2}}$ poseen la misma cardinalidad, entonces se puede establecer una relación de isomorfismo entre

un elemento $\gamma \in \mathbb{F}_{(q^{n_1})^{n_2}}$ y un elemento $\alpha \in \mathbb{F}_{q^n}$ los cuales van a tener el mismo orden. Por tanto, el cálculo de un polinomio mínimo de grado n sobre $\mathbb{F}_q$ viene dado por fórmula

$$f_h(x) = \prod_{j=0}^{n-1}(x - \gamma^{hq^j}) \tag{2}$$

con h coseto líder, donde $\gamma^{hq^j} \in \mathbb{F}_{(q^{n_1})^{n_2}}$ son las raíces de $f_h(x)$. En esta operación se tienen que multiplicar n binomios de ese tipo pero se observa que aparecen n_1 raíces de la forma γ^{hq^r} con r entre 0 y $n_1 - 1$, cada uno con $n_2 - 1$ conjugados que corresponden con las n raíces del polinomio, o sea:

$$\underbrace{\{\overbrace{\gamma^h, \ldots, \gamma^{hq^{n_1-1}}}^{n_1\ elementos}, \overbrace{\gamma^{hq^{n_1}}, \ldots, \gamma^{hq^{n_1-1}q^{n_1}}}^{n_1\ elementos}, \cdots, \overbrace{\gamma^{h(q^{n_1})^{(n_2-1)}}, \ldots, \gamma^{hq^{n_1-1}(q^{n_1})^{(n_2-1)}}}^{n_1\ elementos}\}}_{n_2\ grupos\ de\ n_1\ elementos} \tag{3}$$

Con las coordenadas del elemento γ sobre la base normal, para el cálculo de γ^h, se emplea el método de exponenciación propuesto, en este caso buscando la representación de h en potencias de q^{n_1} para lo cual solo hay que calcular los elementos γ^k, siendo k las potencias de 2 menores que q^{n_1}.

De manera general, para la construcción de un polinomio mínimo de grado n sobre $\mathbb{F}_q$ empleando la torre T_1 con bases normales, es necesario realizar $\frac{n^2-n}{2}$ multiplicaciones y n_1 exponenciaciones con el método propuesto $\hat{E}$, donde cada multiplicación equivale a $(n_2)^2$ operaciones en $\mathbb{F}_{(q^{n_1})^{n_2}}$. Las n_1 exponenciaciones representan los elementos del primer grupo de 3 y las demás van a ser corrimientos de estas. En el siguiente ejemplo se muestra cómo se realizan las operaciones en torres de campos con bases normales a través del algoritmo de Madarro.

Ejemplo 1 . Se desea calcular los polinomios primitivos de grado 4 sobre el campo $\mathbb{F}_4$. El campo de búsqueda natural para los elementos primitivos es la extensión $\mathbb{F}_{4^4}/\mathbb{F}_4$. Dicho campo es isomorfo al descrito a través de la torre $\mathbb{F}_{(4^2)^2}/\mathbb{F}_{4^2}/\mathbb{F}_4$ ($\mathbb{F}_{(q^{n_1})^{n_2}}/\mathbb{F}_{q^{n_1}}/\mathbb{F}_q$), un elemento primitivo de $\mathbb{F}_{(4^2)^2}/\mathbb{F}_{4^2}$ es $W = \gamma$, siendo γ raíz del polinomio irreducible $f(x) = x^2 + x + \alpha\beta + 1$, tal que $\beta \in \mathbb{F}_{4^2}$ es raíz del polinomio irreducible $x^2 + x + \alpha$ sobre $\mathbb{F}_4$ y $\alpha \in \mathbb{F}_4$.

Dos bases normales correspondientes con las extensiones descritas son: $B_{N_1} = \{\beta, \beta + 1\} = \{w, w^4\}$ de $\mathbb{F}_{4^2}/\mathbb{F}_4$ y $B_{N_2} = \{\gamma, \gamma + 1\} = \{v, v^{16}\}$ de $\mathbb{F}_{(4^2)^2}/\mathbb{F}_{4^2}$ cuyas tablas de multiplicar son:

$T(B_{N_1})$	w	w^4
ww	$\alpha+1$	α
ww^4	α	α

$T(B_{N_2})$	v	v^{16}
vv	αw	$(\alpha+1)w+w^4$
vv^{16}	$(\alpha+1)w+w^4$	$(\alpha+1)w+w^4$

De esta forma se tiene que W tiene coordenadas $(1,0)$ en la base B_{N_2}.

Como se explicó anteriormente, se hace necesario calcular las coordenadas de W elevado a las potencias 2 menores que 16, las cuales se van a emplear en todos los cálculos para la generación de los polinomios primitivos. En este caso:

$$W^2 = [\alpha w]v + \left[(\alpha+1)w + w^4\right]v^{16}$$
$$W^4 = wv + w^4v^{16}$$
$$W^8 = [(\alpha+1)w^4]v + [w + \alpha w^4]v^{16}$$

Los cosetos 4-ciclotómicos líderes primos relativos con 255 son {1, 2, 7, 11, 13, 14, 19, 22, 23, 26, 29, 31, 37, 38, 41, 43, 46, 47, 53, 58, 59, 61, 62, 86, 91, 94, 103, 106, 107, 122, 127, 191}, por lo tanto h toma valores en dicha lista.

Se calcula el polinomio primitivo a partir de la sustitución en la ecuación 2 de los valores de h

$$(x+W^h)(x+W^{h4})(x+W^{h16})(x+W^{h4*16})$$

Para $h=19$ se tiene:

$$\left(x+W^{19}\right)\left(x+(W^{19})^4\right)\left(x+(W^{19})^{16}\right)\left(x+(W^{19})^{4*16}\right)$$

Se debe calcular las coordenadas de W^{19} y $(W^{19})^4$, ya que por la proposición 1 $(W^{19})^{16}$ y $(W^{19})^{4*16}$ son un

corrimiento respectivamente de las anteriores. Al emplear el método de exponenciación propuesto:

$$W^{19} = W^{16} \cdot W^2 \cdot W$$
$$(W^{19})^4 = (W^4)^{16} \cdot W^8 \cdot W^4$$

Luego

$$W^{19} = wv + [(\alpha+1)w + (\alpha+1)w^4]v^{16}$$

y su corrimiento

$$(W^{19})^{16} = [(\alpha+1)w + (\alpha+1)w^4]v + wv^{16}$$

$$(W^{19})^4 = [\alpha w + \alpha w^4]v + [\alpha w]v^{16}$$

y su corrimiento

$$(W^{19})^{4*16} = [\alpha w]v + [\alpha w + \alpha w^4]v^{16}$$

Con estos valores, el polinomio resultante es:

$$x^4 + \alpha x^3 + (\alpha+1)x + \alpha$$

Entonces, para todos los cosetos líderes restantes se obtienen los polinomios primitivos que aparecen en la tabla 4.

Para obtener cada polinomio se realizan $6\hat{M} + 2\hat{E}$ en $\mathbb{F}_{(4^2)^2}$. ■

El método original, usando la torre T_0 con bases polinomiales realiza $\frac{n^2-n}{2}$ multiplicaciones y n exponenciaciones, donde cada multiplicación equivale a n^2 operaciones en $\mathbb{F}_{q^n}$ y las n exponenciaciones representan todas las raíces del polinomio resultante. Por tanto se puede apreciar las diferencias que existe en cuanto a la cantidad de operaciones que se necesitan para resolver el problema planteado del cálculo del polinomio mínimo expuestos en la tabla 5.

Tabla 4: Polinomios primitivos de grado 4 sobre $\mathbb{F}_4$.

h	$f(x)$	h	$f(x)$
1	$x^4+(\alpha+1)x^2+\alpha x+\alpha$	46	$x^4+x^2+(\alpha+1)x+\alpha$
2	$x^4+\alpha x^2+(\alpha+1)x+\alpha+1$	47	$x^4+x^3+x+\alpha+1$
7	$x^4+\alpha x^2+\alpha x+\alpha$	53	$x^4+\alpha x^3+\alpha x^2+\alpha+1$
11	$x^4+\alpha x^3+(\alpha+1)x^2+\alpha x+\alpha+1$	58	$x^4+(\alpha+1)x^3+\alpha x^2+\alpha$
13	$x^4+\alpha x^3+\alpha x+\alpha$	59	$x^4+\alpha x^3+x+\alpha+1$
14	$x^2+(\alpha+1)x^2+(\alpha+1)x+\alpha+1$	61	$x^4+(\alpha+1)x^3+x^2+(\alpha+1)x+\alpha$
19	$x^4+\alpha x^3+(\alpha+1)x+\alpha$	62	$x^4+x^3+x^2+\alpha+1$
22	$x^4+(\alpha+1)x^3+\alpha x^2+(\alpha+1)x+\alpha$	86	$x^4+\alpha x^2+\alpha x+\alpha+1$
23	$x^4+x^2+\alpha x+\alpha+1$	91	$x^4+x^3+x^2+\alpha x+\alpha$
26	$x^4+(\alpha+1)x^3+(\alpha+1)x+\alpha+1$	94	$x^4+x^3+x+\alpha$
29	$x^4+\alpha x^3+(\alpha+1)x^2+\alpha+1$	103	$x^4+(\alpha+1)x^3+x+\alpha$
31	$x^4+x^3+x^2+\alpha$	106	$x^4+(\alpha+1)x^3+(\alpha+1)x^2+\alpha$
37	$x^4+x^3+\alpha x^2+\alpha x+\alpha$	107	$x^4+x^3+x^2+(\alpha+1)x+\alpha+1$
38	$x^4+(\alpha+1)x^3+\alpha x+\alpha+1$	122	$x^4+\alpha x^3+x^2+\alpha x+\alpha+1$
41	$x^4+x^3+(\alpha+1)x^2+(\alpha+1)x+\alpha+1$	127	$x^4+x^3+(\alpha+1)x^2+\alpha$
43	$x^4+(\alpha+1)x^2+(\alpha+1)x+\alpha$	191	$x^4+x^3+\alpha x^2+\alpha+1$

Tabla 5: Comparación entre la cantidad de operaciones

Polinomio Mínimo	**Cant. Operaciones**
T_1 con B. Normales	$\frac{n^2-n}{2}\hat{M}+n_1\hat{E}$ en $\mathbb{F}_{(q^{n_1})^{n_2}}$
T_0 con B. Polinomiales	$\frac{n^2-n}{2}\bar{M}+n\bar{E}$ en $\mathbb{F}_{q^n}$

$\hat{E}$: Método de exponenciación propuesto en bases normales, $\hat{M}$: Multiplicaciones en la torre,
$\bar{E}$: Método de exponenciación binario en base polinomial, $\bar{M}$: Multiplicaciones en el campo base.

Conclusiones

En este trabajo se analizaron los principales conceptos relacionadas con el uso de las torres de campos utilizando bases normales para el algoritmo de generación de polinomios primitivos y se arribó a las siguientes conclusiones:

- Las Torres de Campos Finitos construidas con varias extensiones son una herramienta poderosa para lograr una aritmética más eficiente.
- Se emplearon las bases normales por las buenas propiedades que poseen respecto al cálculo de las potencias, lo que trajo consigo la propuesta de un método de exponenciación que aprovecha estas ventajas.
- La forma de los cosetos q-ciclotómicos módulo $q^n - 1$ es análoga a la forma de los exponentes de las bases normales, lo que contribuyó a disminuir la cantidad de potencias a realizar en el cálculo de las raíces del polinomio mínimo.

Para trabajos futuros, se recomienda:

- Implementar el algoritmo empleando las torres de campos con bases normales y realizar un estudio más profundo de la incidencia de estos en la complejidad general del algoritmo.
- Analizar el comportamiento de las operaciones empleando otros tipos de torres.

Referencias

Bailey, D. and Paar, C. (1998). Optimal ExtensionFields for Fast Arithmetic in Public-Key Algorithms. *CRYPTO'98*, pages 472–485.

Baktir, S. (2003). Efficient algorithms for finite fields, with applications in elliptic curve cryptography. Master's Thesis, ECE Department, Worcester Polytechnic Institute, Worcester, Massachusetts, USA.

Baktir, S., Pelzl, J., Wollinger, T., Sunar, B., and Paar, C. (2004). Optimal tower fields for hyperelliptic curve cryptosystems. In *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, volume 1, pages 522–526. IEEE.

Baktir, S. and Sunar, B. (2004). Optimal Tower Fields. *IEEE Transactions on Computers*, 53(10):1231–1243.

Bonnecaze, A., Liardet, P., and Venelli, A. (2013). AES Side-Channel Countermeasure using Random Tower Field Constructions. *Codes and Cryptography*.

Cortez, N. (2009). Multiplicadores de arquitectura segmentada y su aplicación al cómputo de emparejamientos bilineales. Tesis de Maestría, Director: Dr. Francisco Rodríguez Henríquez, Instituto Politécnico Nacional, México D.F.

Cuellar, O. (2017). *Homomorfismos de inmersión y matrices MDS en la Criptografía.* Tesis Doctoral, Universidad Central "Marta Abreu" de Las Villas, Cuba.

Cuellar, O., Madarro, E., Freyre, P., and Sosa, G. (2016). The Zech's Logarithm and cyclotomic coset. *Journal of Advances in Mathematic.*

da Silva, J. and Lima, D. (1993). Construção de Polinômios Primitivos sobre Corpos Finitos GF(q).

Dehnavi, S., Rishakani, A., Shamsabad, M., and Pasha, E. (2014). Construction of New Families of MDS Diffusion Layers. *IACR.*

Delgado, O. (2010). *Nuevos Protocolos y Esquemas de Seguridad para Redes Ad-hoc Móviles Inalámbricas.* Tesis doctoral, Universidad Carlos III de Madrid.

di Porto, A., Guida, F., and Montolivo, E. (1992). Fast algorithm for finding primitive polynomials over GF(q). *Electronics Letters*, 28(2):118–120.

El-Razouk, H., Reyhani-Masoleh, A., and Gong, G. (2015). New Hardware Implementations of $WG(29, 11)$ and $WG-16$ StreamCiphers Using Polynomial Basis. *IEEE Transactions on Computers*, 64(7):2020–2035.

Fan, X., Zidaric, N., Aagaard, M., and Gong, G. (2013). Efficient hardware implementation of the stream cipher WG-16 with composite field arithmetic. In *Proceedings of the 3rd international workshop on Trustworthy embedded devices*, pages 21–34. ACM.

Fraleigh, J. (2003). *A First Course in Abstract Algebra.* 7ed edition.

Freyre, P., Díaz, N., and Pérez, C. (2014). Random Generation of MDS matrices. *CTCrypt.*

Golomb, S. (1982). *Shift register sequences.* Aegean Park Press.

González, J. (2010). Diseño e Implementación Eficiente del Emparejamiento Óptimo ATE. Tesis de Maestría, Director: Dr. Francisco Rodríguez Henríquez, Instituto Politécnico Nacional, México D.F.

Gupta, K. and Pandey, S. (2017). Applications of design theory for the constructions of MDS matrices for lightweight cryptography. *Journal of Mathematical Cryptology*, 11(2):85–116.

Gupta, K. and Ray, I. (2015). Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. *Cryptography and Communications*, 7:257–287.

Junod, P. and Vaudenay, S. (2004). Building Efficient MDS Matrices. In *Perfect Diffusion Primitives for Block Ciphers.*

Kerins, T., Marnane, W., Popovici, E., and Barreto, P. (2005). Efficient Hardware for the Tate Pairing Calculation in Characteristic Three. *Cryptographic Hardware and Embedded Systems*, pages 412–426.

Knuth, D. (1997). *The Art of Computer Programming: Seminumerical Algorithms.*, volume 2. Addison-Wesley Professional, 3 edition.

Lidl, R. and Niederreiter, H. (1986). *Introduction to finite fields and their applications*. Cambridge university press.

Madarro, E. (2017). Generación de polinomios primitivos sobre extensiones de campos finitos $\mathbb{F}_{2^n}$. Tesis de Maestría, Director: M.Sc. Oristela Cuellar Justiz, Universidad Central "Marta Abreu" de Las Villas, Cuba.

Madarro, E. and Cuellar, O. (2016). Algoritmo para la generación de polinomios primitivos sobre extensiones de campos finitos de característica 2. In *III Seminario Naicional de Criptografía*, La Habana, Cuba. Instituto Nacional de Criptografía.

Madarro, E. J. and Cuellar, O. (2021). Algoritmo para la generación de polinomios primitivos sobre extensiones de campos finitos de característica dos. *Revista Cubana de Ciencias Informáticas*, 15(1):114–128.

Mahmoodi, A., Mirzaee, M., Dehnavi, S., Amiri, M., Maimani, H., and Bagheri, N. (2019). Lightweight 4x4 MDS Matrices for Hardware-Oriented Cryptographic Primitives. *The ISC International Journal of Information Security*, 11(1):35–46.

Mullen, G. and Panario, D. (2013). *Handbook of finite fields*. CRC Press.

Peralta, F. (2005). Diseño de Arquitecturas Digitales para Criptografía. Tesis de maestría, Escuela Superior de Ingeniería Mecánica y Eléctrica de Culhuacan.

Pérez, C. (2014). Matrices MDS y Funciones Booleanas Vectoriales. Diseño de un Algoritmo Criptográfico. Tesis de maestría, Universidad de la Habana.

Pérez Roble, A. (2017). Principales aplicaciones de las torres de campos en la criptografía moderna. In *XV Congreso Internacional de Computación y Matemática (COMPUMAT)*.

Pérez Roble, A. (2019). Aritmética sobre Torres de Campos Finitos de característica 2, aplicados a la generación de polinomios primitivos. Master's thesis, Universidad de La Habana, Cuba.

Reyhani-Masoleh, A., Taha, M., and Ashmawy, D. (2018a). New area record for the AES combined S-box/inverse S-box. In *2018 IEEE 25th Symposium on Computer Arithmetic (ARITH)*, pages 145–152. IEEE.

Reyhani-Masoleh, A., Taha, M., and Ashmawy, D. (2018b). Smashing the implementation records of AES S-box. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 298–336.

Rifa, J. and Borrell, J. (1995). A Fast Algorithm To Compute Irreducible and Primitive Polynomials in Finite Fields. *Math. Systems Theory*, pages 13–20.

Saxena, E. and MacCuskey, N. (2004). Primitive Polynomial Generation Algorithms Implementation and Performance Analysis.

Shoup, V. (1999). Efficient computation of minimal polynomials in algebraic extensions of finite fields. In *In Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation*, pages 53–58, New York.

Shoup, V. (2008). *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press.

Ueno, R., Homma, N., Sugawara, Y., Nogami, Y., and Aoki, T. (2015). Highly Efficient $GF(2^8)$ Inversion Circuit Based on Redundant GF Arithmetic and Its Application to AES Design. *Cryptographic Hardware and Embedded Systems*.

Velásquez, F. and Castaño, J. F. (2013). Implementación de aritmética de torres de campos finitos binarios de extensión 2 en fpga. *INGE CUC*.

Zidaric, N. (2014). Hardware implementations of the WG-16 stream cipher with composite field arithmetic. Tesis de Maestría, University of Waterloo.

Zidaric, N., Aagaard, M., and Gong, G. (2019). Hardware Optimizations and Analysis for the WG-16 Cipher with Tower Field Arithmetic. *IEEE Transactions on Computers*, 68(1):67–82.