Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional

Unidad Zacatenco

Departamento de Computación

Construcción de polinomios básicos primitivos y la expresión p-ádica aditiva de un anillo de Galois para un esquema de autenticación

Tesis que presenta

Miguel Angel Márquez Hidalgo

para obtener el grado de

Maestría en Ciencias

en Computación

Director de Tesis

Juan Carlos Ku Cauich

Ciudad de México **Noviembre de 2020**

Índice general

Índice de tablas

Índice de algoritmos

Resumen

Cuando dos entidades desean establecer comunicación a través de un canal público, el cual puede ser inseguro, existe la posibilidad de que un intruso inserte un mensaje en dicho canal para cualquiera de las entidades, esperando que lo acepten como auténtico o alterar la integridad de un mensaje enviado. Para proveer de autenticidad a los mensajes enviados entre sí, hacen uso de un esquema de autenticación. Es importante tomar en cuenta que en estos esquemas están dadas las probabilidades de ataques de sustitución y personificación por parte del intruso.

Existen dos tipos de esquemas de autenticación: con secreto y sin secreto. Este trabajo se enfoca en los que esquemas de autenticación sin secreto. Presentamos dos esquemas de autenticación sin secreto empleando anillos de Galois, funciones resilientes y la función de Gray, así como las probabilidades de sustitución y personificación para el primero y únicamente la probabilidad de personificación para el segundo.

Por otra parte, los anillos de Galois pueden ser generados por polinomios primitivos y polinomios básicos primitivos, estos últimos son de mayor interés ya que un anillo de Galois generado por estos permiten obtener al conjunto de Teichmüller, el cual permite expresar a sus elementos en forma p-ádica. Además, dado un polinomio primitivo sobre un campo finito $\mathbb{F}_q$, es posible obtener su levantamiento de Hensel, esto es, cada polinomio básico primitivo correspondiente a su polinomio primitivo inicial sobre cada anillo $\mathbb{Z}_{s_1}$, $s_1 \leq s$, $s \in \mathbb{Z}^+$.

En este trabajo se presenta un listado de polinomios básicos primitivos de diversos grados para ciertos números primos, además de otra lista en la que se incluye el levantamiento de Hensel de algunos básicos primitivos obtenidos en el listado anterior, así como la implementación de los algoritmos en la aplicación matemática SageMath.

Abstract

When two entities want to communicate through a public communication channel which could be insecure, there exist the possibility that an intruder inserts a message in the communication channel to any of the entities and waiting to be accepted as authentic or change its integrity. To provide authenticity to messages sent to each other, the entities use an authentication scheme. It is essential to notice that when using these schemes, the probabilities of success of impersonation attack and substitution attack are given.

There are two types of authentication schemes: with secrecy and without secrecy. This thesis focus on authentication schemes without secrecy. We propose two authentication schemes without secrecy making use of Galois rings, resilient, and Gray functions, as well as the calculation of substitution and impersonation probabilities for the first scheme and only the calculation of the impersonation probability for the second.

On the other hand, Galois rings can be generated by primitive polynomials and basic primitive polynomials; the latter are of great interest since a Galois ring generated by them allow to obtain the Teichmüller set, which let express its elements in their p-adic form. Besides, given a basic primitive polynomial, it is possible to find its Hensel's lift, *i.e.*, every basic primitive polynomial corresponding to its primitive polynomial over each ring $\mathbb{Z}_{s_1}$, $s_1 \leq s$, $s \in \mathbb{Z}^+$.

We present a list of primitive basic polynomials of different degrees and prime numbers, as well as another list which includes Hensel's lift for some primitive basic polynomials obtained in the previous list, along with the implementation of the algorithms in SageMath.

ABSTRACT

Capítulo 1

Introducción

La criptografía es el arte y la técnica de crear mensajes codificados con procedimientos o claves secretas, con el objetivo de que no pueda ser descifrado salvo por la persona a quien está dirigido o quien poseea la clave ([25]). Ha sido históricamente usada para ocultar la comunicación entre entidades. Para ésta es importante garantizar los servicios de seguridad como los siguientes:

1. Confidencialidad: sólo el receptor destinado a recibir el mensaje puede leerlo.
2. Autenticación: estar convencido de que se establece comunicación con la persona correcta.
3. Integridad: ningún mensaje recibido o enviado ha sido modificado.
4. No repudio: cuando se reciba un mensaje, el remitente no pueda negar haber enviado ese mensaje ([2]).

La primitiva o servicio de autenticación es de interés para este trabajo, en particular los esquemas sistemáticos de autenticación. Estos se dividen en dos: con secreto y sin secreto. Los esquemas de autenticación sin secreto son tuplas de la forma

$$\mathcal{A} = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}),$$

donde $\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}$ son llamados los espacios fuente, de etiquetas, de llaves y de reglas de cifrado respectivamente ([12]). La diferencia entre los esquemas sin secreto y los esquemas con secreto radica en que en el esquema con secreto es necesario agregar a la tupla del esquema una función f llamada función de cifrado ([7]).

El presente trabajo consiste de la siguiente estructura:

En el capítulo 2 se muestran gran parte de los conceptos y resultados básicos, importantes para un mejor entendimiento del tema principal de esta tesis. En la sección 2.1 y

sección 2.2 se revisa de modo general la teoría de grupos y de anillos: subanillos, ideales, anillos de polinomios, con énfasis en el anillo finito $\mathbb{Z}_{p^s}$ y el anillo de polinomios $\mathbb{Z}_{p^s}[x]$, los cuales cumplen un importante papel para este trabajo; también se introducen los campos. En la sección 2.3, referente a los anillos de Galois, se introduce la función traza, las expresiones aditiva y p-ádica de los elementos de estos anillos, así como un ejemplo sencillo de esta estructura algebraica para la fácil comprensión del lector.

La sección 2.4 trata acerca de la función de Gray, cuyo dominio consta de un anillo de Galois y codominio el espacio vectorial $\mathbb{F}_q^{q^{s-1}}$. Adicionalmente se considera la transformada de Fourier sobre los anillos de Galois, ya que bajo esta transformada es definido el peso homogéneo. La distancia homogénea y la distancia de Hamming mantienen una isometría bajo el mapeo de Gray. La expresión de las imágenes de esta función son sumas de vectores de longitud q^{s-1}. Se aprovecha esta característica para darle estructura a los esquemas de autenticación propuestos en el capítulo 4. Por otro lado, para evaluar un elemento del anillo de Galois bajo la función de Gray es necesario que este tenga su forma p-ádica. De esta manera se tiene una relación estrecha entre la función de Gray y la expresión p-ádica.

La sección 2.5 define las funciones t-resilientes: funciones balanceadas cuando las preimágenes se restringen a t entradas. Estas funciones, en este trabajo, son consideradas sobre los anillos de Galois.

Finalmente en este capítulo, la sección 2.6 describe que es posible obtener fácilmente la expresión p-ádica de un anillo de Galois dada la forma aditiva; sin embargo, obtener la transformación inversa parece ser un problema difícil de resolver, dado que es necesario encontrar $s-1$ potencias de un elemento primitivo del anillo de Galois.

El capítulo 3, acerca de los polinomios primitivos y levantamiento de Hensel, introduce algunas definiciones y propiedades respecto a los polinomios sobre un anillo arbitrario. Posteriormente, se tienen tres algoritmos, implementados en SageMath:

En primer lugar, se encuentran todos los polinomios mónicos básicos primitivos sobre un anillo de Galois utilizando la definición de éstos. Un segundo algoritmo se basa, en parte, en el proceso de demostración del levantamiento de Hensel 3.0.1 de un polinomio primitivo sobre un campo finito a los polinomios básicos primitivos sobre los anillos de Galois correspondientes $\mathbb{Z}_{p^s}$. Esta implementación es dada sólo para polinomios básicos primitivos de grado dos. Una vez obtenido un polinomio básico primitivo de grado m sobre $\mathbb{Z}_{p^s}$ se construye el anillo de Galois $GR(p^s, m)$, escribiendo sus elementos en su forma aditiva.

El siguiente apartado del capítulo expone dos tablas:

1. La primera corresponde a los polinomios básicos primitivos obtenido con la primera implementación. Este encuentra todos los polinomios mónicos básicos primitivos sobre $\mathbb{Z}_{p^s}$ de grado m, m fijo.

2. La segunda es con respecto al levantamiento de Hensel de un polinomio primitivo de grado dos, con coeficientes en $\mathbb{F}_p$. Este encuentra cada polinomio mónico básico primitivo correspondiente al polinomio primitivo dado inicialmente, sobre cada anillo $\mathbb{Z}_{p^{s'}}$, $s' \leq s$.

En capítulo 4, en primer lugar, se define un esquema sistemático de autenticación. Posteriormente se presentan dos esquemas de autenticación, los cuáles utilizan las distintas funciones ya definidas: función de Gray, funciones resilientes y función traza. Todas estas funciones sobre los anillos de Galois, considerando los campos correspondientes.

1. Esquema 1: Usando anillos de Galois con característica p^2, como un caso particular.

2. Esquema 1, caso general: Usando anillos de Galois con característica p^s, $s > 1$, como caso general del anterior.

3. Esquema 2: Usando anillos de Galois con característica p^2, suprimiendo al ideal pR del esquema 1. El conjunto anterior surge como caso particular cuando $s = 2$.

4. Esquema 2, caso general: Usando anillos de Galois con característica p^s, $s > 1$ y suprimiendo al ideal $p^{s-1}R$, del esquema 1 (caso general).

Respecto al esquema 1. El espacio fuente, dada la forma que ésta tiene, resulta tener mayor cardinalidad que el espacio dado en [21]. Manteniendo los valores mínimos de las probabilidades P_I y P_S (personificación y sustitución respectivamente). Propiedades adicionales de la función traza permiten una prueba más sencilla y corta de la biyección entre llaves y reglas de codificación.

Respecto al esquema 2. Se obtiene una menor magnitud del espacio de llaves, manteniendo la misma cardinalidad del espacio fuente del esquema anterior. La prueba de inyectividad se reduce a dos casos, y el valor mínimo de la probabilidad de personificación se mantiene.

Capítulo 2

Preliminares

2.1. Grupos

Definición 2.1.1. [13] Sea G un conjunto distinto del vacío.

1. Un *grupo* es un par ordenado $(G, *)$ donde $*$ es una operación binaria sobre G que satisface los siguientes axiomas:

   - $*$ es asociativa.
   - Existe un elemento e_G en G llamado identidad de G, tal que para toda $a \in G$ se tiene que

     $$a * e_G = e_G * a = a.$$

   - Para toda $a \in G$ existe un elemento $a^{-1} \in G$, llamado *inverso* de a, tal que

     $$a * a^{-1} = a^{-1} * a = e_G.$$

2. El grupo $(G, *)$ se dice que es *abeliano* (o *conmutativo*) si

   $$a * b = b * a, \quad \forall a, b \in G.$$

Ejemplos:

1. Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos bajo la operación $+$ con $e = 0$ y $a^{-1} = -a$, para toda a.

2. $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ son grupos bajo la operación $\times$ con $e = 1$ y $a^{-1} = 1/a$, para toda a en los conjuntos anteriores.
   Sin embargo, $\mathbb{Z} - \{0\}$ no es un grupo bajo $\times$, ya que el elemento 2 no posee un inverso en $\mathbb{Z} - \{0\}$.

Definición 2.1.2. [13] Para G un grupo y $x \in G$, se define el *orden* de x como el menor entero positivo n tal que $x^n = e_G$ y se denota a este entero por $o(x)$. En este caso se dice que x es de orden n. Si no existe una potencia positiva de x que sea igual a la identidad, se define el orden de x como infinito y se dice que x es de orden infinito.

Ejemplos:

1. En los grupos aditivos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ todo elemento distinto de la identidad tiene orden infinito.

2. En los grupos $\mathbb{Q} - \{0\}$ y $\mathbb{R} - \{0\}$, el elemento -1 tiene orden 2 y el resto de los elementos distintos de la identidad poseen orden infinito.

Definición 2.1.3. [13] Un grupo G es *cíclico* si G puede ser generado por un sólo elemento, *i.e.*, existe algún $x \in G$ tal que

$$G := \{ x^n \mid n \in \mathbb{Z} \}.$$

En notación aditiva, G es *cíclico* si $G := \{ nx \mid n \in \mathbb{Z} \}$. En ambos casos se escribe $G = \langle x \rangle$ y se dice que G es generado por x (y x es un *generador* de G).

Ejemplo: Sea $G = \mathbb{Z}$ con la operación $+$. Entonces $G = \langle 1 \rangle$ (aquí 1 es el entero y la identidad de G es 0) y cada elemento de G se puede escribir de manera única en la forma $n \cdot 1$, para algún $n \in \mathbb{Z}$.

Definición 2.1.4. [13] Sean $(G, *)$ y $(H, \cdot)$ grupos. Una función $\varphi : G \to H$ tal que

$$\varphi(x * y) = \varphi(x) \cdot \varphi(y), \ \forall x, y \in G$$

es llamada un *homomorfismo*.

Si φ es inyectiva, entonces es llamada un *monomorfismo*. Si φ es suprayectiva, se dice que φ es un *epimorfismo*. Un homomorfismo $\varphi : G \to G$ se llama *endomorfismo*.

Observación. Cuando las operaciones de grupo para G y H no están explícitamente escritas, la condición de homomorfismo simplemente se convierte en

$$\varphi(xy) = \varphi(x)\varphi(y),$$

pero es importante tener en cuenta que el producto xy del lado izquierdo está calculado en G, y el producto $\varphi(x)\varphi(y)$ del lado derecho en H.

2.2. Anillos

Definición 2.2.1. [13] Sea R un conjunto no vacío

1. Un *anillo* $(R, +, \times)$ es una terna junto con dos operaciones binarias $+$ y $\times$ (llamadas suma y multiplicación) que satisfacen los siguientes axiomas:

   - $(R, +)$ es un grupo abeliano,
   - $\times$ es asociativa: $(a \times b) \times c = a \times (b \times c), \forall\, a, b, c \in R$,
   - Las leyes distributivas son validas en $R : \forall\, a, b, c \in R$

   $$(a + b) \times c = (a \times c) + (b \times c) \quad y \quad a \times (b + c) = (a \times b) + (a \times c).$$

2. El anillo R es *conmutativo* si la multiplicación es conmutativa.

3. R es un *anillo con identidad* si existe un elemento $1 \in R$ de modo que

   $$1 \times a = a \times 1 = a, \forall\, a \in R.$$

Ejemplos:

1. El anillo de los enteros (bajo las operaciones usuales de suma y multiplicación) es un anillo conmutativo con identidad (el entero 1). Los axiomas de un anillo se siguen de los axiomas básicos para el sistema de los números naturales.

2. De modo similar, los números racionales $\mathbb{Q}$, los números reales $\mathbb{R}$ y los números complejos $\mathbb{C}$ son anillos conmutativos con identidad. Los axiomas de anillos para cada uno de ellos se siguen de los axiomas de anillo para $\mathbb{Z}$.

Definición 2.2.2. [13] Un *subanillo* S del anillo R es un subconjunto de R de manera que las operaciones de suma y multiplicación en R cuando se restringen a S dan a S la estructura de un anillo.

Ejemplo: $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ y $\mathbb{Q}$ es un subanillo de $\mathbb{R}$.

Definición 2.2.3. [13] Sea R un anillo.

1. Un elemento $a \in R$, $a \neq 0$, es un *divisor de cero* si existe un elemento $b \in R$, con $b \neq 0$ tal que $ab = 0$ o $ba = 0$.

2. Suponga que R tiene un elemento identidad $1 \neq 0$. Entonces un elemento $u \in R$ es una *unidad* si existe algún $v \in R$ tal que

   $$uv = vu = 1.$$

   El conjunto de unidades en R se denota por $R^{\times}$.

3. Un *campo* F es un anillo conmutativo con identidad $1 \neq 0$ en el cual todo elemento distinto de cero es una unidad, esto es,

$$F^{\times} = F - \{0\}.$$

Observación. Un elemento divisor de cero no puede ser una unidad: suponga que a es una unidad en el anillo R y que $ab = 0$ para algún elemento $b \in R$, con $b \neq 0$. Entonces $va = 1$ para algún $v \in R$, por lo que se tiene

$$b = 1 \cdot b = (va)b = v(ab) = v \cdot 0 = 0,$$

lo cual es una contradicción. Análogamente, si $ba = 0$ para algún elemento b, con $b \neq 0$, entonces a no pueder ser unidad. Esto muestra en particular que los campos no contienen divisores de cero.

Ejemplos:

1. $\mathbb{Z}$ no posee divisores de cero y sus únicas unidades son ± 1, *i.e.*, $\mathbb{Z}^{\times} = \{\pm 1\}$.

2. $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son ejemplos triviales de campos.

Definición 2.2.4. [13] Un anillo conmutativo con identidad $1 \neq 0$ recibe el nombre de *dominio entero* si no contiene divisores de cero.

Definición 2.2.5. [24] Sea R un anillo. Si existe el menor entero positivo n tal que $na = 0, \forall a \in R$, entonces se dice que R tiene *característica* n. Si el entero antes mencionado no existe, entonces R tiene característica cero (notación: car $(R) = n$).

La definición anterior es importante para este trabajo ya que es una propiedad que poseen las estructuras tratadas aquí.

Proposición 2.2.1. [24] *La característica de un campo F es 0 o un primo p.*

Definición 2.2.6. [39] Sea g un generador de $\mathbb{Z}_p^*$, p un número primo, y sea h un elemento de $\mathbb{Z}_p$ arbitrario diferente de cero. El *problema de logaritmo discreto* consiste en hallar al exponente $x \in \mathbb{Z}_{p-1}$ de modo que

$$g^x \equiv h \pmod{p}.$$

Definición 2.2.7. [13] Sean R y S anillos. Una función $\psi : R \to S$ es un *homomorfismo de anillos* si para toda $a, b \in R$ se cumple que:

$$\psi(a + b) = \psi(a) + \psi(b) \quad y \quad \psi(ab) = \psi(a)\psi(b).$$

De manera análoga al caso de homomorfismos de grupos, se definen los monomorfismos, epimorfismos, automorfismos, endomorfismos e isomorfismos de anillos.

Definición 2.2.8. [24] Sea R un anillo. Un subanillo I de un anillo R es un *ideal izquierdo* si satisface que:

$$r \in R \quad y \quad x \in I \Rightarrow rx \in I.$$

I es un *ideal derecho* si cumple que:

$$r \in R \quad y \quad x \in I \Rightarrow xr \in I.$$

I es un *ideal* si es tanto un ideal derecho como un ideal izquierdo.

Para el caso de anillos conmutativos los conceptos de ideal derecho, ideal izquierdo e ideal, coinciden.

Ejemplo: El conjunto $2\mathbb{Z} = \{2 \cdot n \mid n \in \mathbb{Z}\}$ es un ideal de los números enteros debido a que la suma de dos números pares es un número par y el producto de un entero arbitrario y un número par también lo es.

Proposición 2.2.2. [13] *Sea R un anillo e I un ideal de R. Entonces R/I es un anillo bajo las operaciones binarias:*

$$(r + I) + (s + I) = (r + s) + I \quad y \quad (r + I) \times (s + I) = (rs) + I,$$

para todo $r, s \in R$. Recíprocamente, si I es cualquier subgrupo tal que las operaciones anteriores están bien definidas, entonces I es un ideal de R.

Definición 2.2.9. [13] Cuando I es un ideal de R, el anillo R/I con las operaciones de la proposición anterior es llamado el *anillo cociente* de R sobre I.

Definición 2.2.10. [13] Sea R un anillo conmutativo,

1. Un ideal P es llamado *ideal primo* si $P \neq R$, y si $a, b \in R$ son tales que $ab \in P$, entonces $a \in P$ o $b \in P$.

2. Un ideal M de R es llamado *ideal maximal* si $M \neq R$ y los únicos ideales que contienen a M son M y R.

3. Un anillo R es *local* si posee un único ideal maximal.

La siguiente proposición caracteriza a los ideales primos y maximales con respecto a sus anillos cociente.

Proposición 2.2.3. [13] *Suponga que R es un anillo conmutativo. Entonces*

1. *El ideal M es maximal si y sólo si el anillo cociente R/M es un campo.*

2. *El ideal P es primo si y sólo si el anillo cociente R/P es un dominio entero.*

Definición 2.2.11. [13] Sean $a, b, n \in \mathbb{Z}^+$. Si $n|(a-b)$, entonces a es *congruente con b módulo n* y se denota $a \equiv b \pmod{n}$.

Si se desea darle un significado a una expresión,

$$a_0 + a_1X + \cdots + a_nX,$$

donde $a_i \in R$, con R anillo conmutativo, y X es una "variable", considérese un grupo cíclico infinito generado por un elemento X. Sea S el subconjunto que consiste de potencias X^r, con $r \geq 0$. Se define el *conjunto de polinomios* $R[X]$ como el conjunto de funciones $S \to R$ las cuales son iguales a cero, excepto para un número finito de elementos de S. Para cada elemento $a \in A$ se denota por aX^n la función que tiene el valor a sobre X^n y el valor 0 para todos los demás elementos de S. Entonces es inmediato que un polinomio puede ser escrito de manera única como un suma finita

$$a_0X^0 + \cdots + a_nX^n$$

para algún número natural $n \in \mathbb{N}$ y $a_i \in R$; tal polinomio se denota por $f(X)$.
Los elementos a_i son llamados *coeficientes de f*. Dados los polinomios

$$f(X) = \sum_{i=0}^{n} a_iX^i \quad \text{y} \quad g(X) = \sum_{j=0}^{m} b_jX^j$$

se define el *producto* como [27]:

$$f(X)g(X) = \sum_{k=0}^{m+n}\Big(\sum_{i+j=k} a_ib_j\Big)X^k.$$

Nótese que existe un elemento unidad, denotado por $1X^0$. Además, para $c \in R$ se tiene que $cf(X) = \sum ca_iX^i$. Observe que dada la definición se tiene la igualdad de los polinomios

$$\sum a_iX^i = \sum b_iX^i$$

si y sólo si $a_i = b_i$ para toda i.

Definición 2.2.12. [27] Considérese al polinomio $f(x) \in R[x]$, con R un anillo arbitrario. El elemento $a \in R$ recibe el nombre de *raíz* de $f(x)$ si $f(a) = 0$.

Definición 2.2.13. [40] Sea $f(x)$ un polinomio mónico de grado m sobre $\mathbb{F}_p[x]$. Si $f(x)$ tiene un elemento de orden $p^m - 1$ de $\mathbb{F}_{p^m}$ como una de sus raíces, entonces $f(x)$ es llamado un *polinomio primitivo* de grado m sobre $\mathbb{F}_p$.

Definición 2.2.14. [40] Sea $f(x)$ un polinomio de grado $m \geq 1$ en $\mathbb{Z}_{p^s}[x]$. Si $\overline{f}(x)$ es irreducible (o primitivo) en $\mathbb{F}_p[x]$, $f(x)$ es llamado un polinomio mónico *básico irreducible* (o mónico *básico primitivo*) en $\mathbb{Z}_{p^s}[x]$, donde los coeficientes de $\overline{f}(x)$ son las imágenes reducción módulo p de los coeficientes de $f(x)$.

Note que los polinomios mónicos básicos primitivos en $\mathbb{Z}_{p^s}[x]$ son mónicos básicos irreducibles.

Teorema 2.2.1. [40] *Para cualquier entero $m \geq 1$, existen polinomios mónicos básicos irreducibles (y mónicos básicos primitivos) de grado m sobre $\mathbb{Z}_{p^s}$ que dividen al polinomio $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$.*

Se presenta ahora el lema de Hensel. Su importancia radica no únicamente en la proposición, sino también en los razonamientos empleados para demostrarlo, los cuales son de utilidad para una implementación.

Teorema 2.2.2. *Versión íntegra del lema de Hensel.* [1] *Sea p un número primo y $k \geq 1$ un entero positivo. Suponga que $u(x), f(x), g(x) \in \mathbb{Z}[x]$ son polinomios mónicos de manera que $f(x)$ y $g(x)$ son primos relativos módulo p y*

$$u(x) \equiv f(x)g(x) \pmod{p^{k+1}}.$$

Entonces es posible determinar de manera única dos polinomios $f_1(x), g_1(x) \in \mathbb{Z}_{p^{k+1}}$, primos relativos módulo p, los cuales satisfacen las siguientes congruencias:

1. $f(x) \equiv f_1(x) \pmod{p^k}$,
2. $g(x) \equiv g_1(x) \pmod{p^k}$,
3. $u(x) \equiv f_1(x)g_1(x) \pmod{p^{k+1}}$.

2.3. Anillos de Galois

Los *anillos de Galois* fueron desarrollados por Wolfgang Krull en 1924. Posteriormente, Gerald Janusz y Raghavendran estudiaron sus propiedades de manera independiente en 1966 y 1969 respectivamente.

Sean $s, m, n \in \mathbb{Z}^+$, $q = p^m$, p un número primo.

Definición 2.3.1. [40] Un **anillo de Galois** sobre $\mathbb{Z}_{p^s}$ con grado de extensión m sobre $\mathbb{Z}_{p^s}$ está definido como el cociente $\mathbb{Z}_{p^s}[x]/\langle f(x)\rangle$, en donde $f(x)$ es un polinomio mónico básico irreducible (o básico primitivo) de grado m sobre $\mathbb{Z}_{p^s}$. Un anillo de Galois con las características anteriores es denotado por $GR(p^s, m)$.

Se denota a los anillos de Galois $GR(p^s, mn)$, $GR(p^s, m)$ como S y R respectivamente, donde S es una extensión de R.

Ejemplos: El anillo $GR(2^2, 2)$ es un anillo de Galois de característica 4 y de cardinalidad 16. El ejemplo trivial de un anillo de Galois es $\mathbb{Z}_{p^s}$ ya que $\mathbb{Z}_{p^s} = GR(p^s, 1)$.

Definición 2.3.2. [14] Sea R un anillo. Entonces:

1. R es un *anillo de cadena* si todos sus ideales forman una cadena bajo la inclusión.
2. Los anillos finitos de cadena son anillos finitos locales cuyos ideales maximales son principales.

Una peculiaridad de los elementos de un anillo de Galois es que poseen una *expresión aditiva* y una *p-ádica*:

Teorema 2.3.1. [40] *Existe una raíz $\xi \in R$ de orden $p^m - 1$, distinta de cero, del polinomio básico primitivo $f(x)$ que divide al polinomio $x^{p^m-1} - 1$ sobre el anillo $\mathbb{Z}_{p^s}$. Más aún, se presentan expresiones aditivas y p-ádicas de los elementos de R respectivamente:*

$$\{a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} : a_i \in \mathbb{Z}_{p^s},\ i = 0, 1, \ldots, m-1\}$$

y

$$\{b_0 + b_1 p + \cdots + b_{s-1}p^{s-1} : b_i \in T_R,\ i = 0, 1, \ldots, s-1\},$$

donde $T_R := \{0, \xi, \xi^2, \ldots, \xi^{q-1}\}$.

Nota: El conjunto T_R del teorema anterior es llamado el *conjunto de Teichmüller* de R.

El teorema 2.3.1 requiere que el polinomio $f(x)$ sea básico primitivo, ya que tener al elemento ξ como raíz y de orden $q-1$ permite generar al conjunto de Teichmüller de un anillo de Galois. Esto no sucede si $f(x)$ sólo es un polinomio básico irreducible.

Ejemplo: Sea $f(x) = x^2 + 4x + 8$ un polinomio básico primitivo en $\mathbb{Z}_{3^2}$ el cual divide al polinomio $x^8 - 1$. Si ξ es raíz de $f(x)$, entonces $\xi^2 + 4\xi + 8 = 0$, por lo que $\xi^2 = 1 + 5\xi$ y $\xi^3 = 5 + 8\xi$. Prosiguiendo de esta manera es posible verificar que el orden de ξ es 8.

Debido a lo anterior, el conjunto de Teichmüller del anillo de Galois $GR(3^2, 2)$ es

$$T_{GR(3^2,2)} = \{0,\ 1,\ \xi,\ \xi^2,\ \xi^3,\ \xi^4,\ \xi^5,\ \xi^6,\ \xi^7\}$$

y

$$GR(3^2, 2) = \{b_0 + b_1 p \mid b_i \in T_{GR(3^2,2)}\},$$

esto es,

$$GR(3^2,2)=\{0,1,\xi,\xi^2,...,\xi^7,3,3\xi,3\xi^2,...,1+3\xi^7,...,\xi^7+3,\xi^7+3\xi,...,\xi^7+3\xi^7\},$$

que resulta ser la expresión p-ádica de los elementos de $GR(3^2,2)$, de característica 9, y con 81 elementos.

Ya que $f(x)$ es un básico primitivo, es posible generar al conjunto de Teichmüller, pero tomar a un polinomio básico irreducible no permite expresar a $GR(3^2,2)$ en forma p-ádica. Considere como ejemplo al polinomio x^3+x+1, el cual es un polinomio básico irreducible, pero no un básico primitivo.

Dados el anillo de Galois R y el campo finito $\mathbb{F}_{p^m}$, es posible establecer una relación entre ellos haciendo uso de la función reducción módulo p. Más aún, esta relación prevalece si se consideran extensiones de estas, cuya definición se explica a continuación.

Definición 2.3.3. [13] Si K es un campo que contiene al subcampo F, entonces K es una *extensión de campos* (o simplemente una *extensión*) de F. El campo F es llamado el *campo base* de la extensión.

Observación. También se tienen extensiones de anillos de Galois; más aún, los anillos están en una correspondencia módulo p con los campos finitos correspondientes:

$$\begin{array}{ccc} S=GR(p^s,mn) & \overset{\bar{*}}{\to} & \mathbb{F}_{q^n} \\ | & & | \\ R=GR(p^s,m) & \overset{\bar{*}}{\to} & \mathbb{F}_q \\ | & & | \\ \mathbb{Z}_{p^s} & \overset{\bar{*}}{\to} & \mathbb{F}_p \end{array}$$

Lema 2.3.2. [22] *Sea $R=GR(p^s,m)$ un anillo de Galois. Entonces R tiene un único subanillo de la forma $GR(p^s,r)$ si y sólo si $r|m$.*

Definición 2.3.4. [32] Sea $GR(p^l,t)$ un anillo de Galois. Se define a la *función traza* como,

$$\begin{array}{rccc} Tr_t: & GR(p^l,t) & \to & \mathbb{Z}_{p^l} \\ & \sum_{i=0}^{l-1}p^ir_i & \mapsto & \sum_{i=0}^{l-1}(r_i+r_i^p+\cdots+r_i^{p^{t-1}})p^i. \end{array}$$

El subíndice t de la función traza se refiere al grado de la extensión (de anillos de Galois) generada por el dominio y codominio de la misma. Por ejemplo, en el siguiente diagrama

$$\begin{array}{c} GR(p^l,mn) \\ | \, n \\ GR(p^l,m) \\ | \, m \\ \mathbb{Z}_{p^l} \end{array}$$

Observe que el grado de la extensión de $GR(p^l, m)$ sobre $\mathbb{Z}_{p^l}$ es m, el grado de $GR(p^l, mn)$ sobre $GR(p^l, m)$ es n y el grado de $GR(p^l, mn)$ sobre $\mathbb{Z}_{p^l}$ es $m \cdot n$.

Teorema 2.3.3. [40] *Sean S y R anillos de Galois, con S extensión de R de grado n, $a, b \in S$ y $c \in R$. Entonces*

1. $Tr_n(a) \in R$.
2. $Tr_n(a + b) = Tr_n(a) + Tr_n(b)$.
3. $Tr_n(c \cdot a) = c \cdot Tr_n(a)$.

2.4. Función de Gray

Nachaev (1991) y Hammons *et al.* (1994) mostraron que gran cantidad de códigos binarios no lineales pueden ser identificados como imágenes de códigos lineales en $\mathbb{Z}_4$ bajo la *función de Gray* entre $\mathbb{Z}_4$ y $\mathbb{Z}_2^2$ ([16], [15]). Desde entonces, se han publicado artículos acerca de códigos sobre $\mathbb{Z}_4$ y en algunos de ellos se desarrollan generalizaciones de la función de Gray ([9], [10], [16]), pero no fue hasta 1998 que Carlet introdujo lo que él llamó una generalización de la función de Gray e identificó al anillo de Galois $\mathbb{Z}_{2^{m+1}}$ bajo isomorfismo con el espacio vectorial $\mathbb{Z}_2^{2^m}$ ([3]).

Para un entero positivo k y un elemento $y \in \mathbb{F}_q$, la siguiente notación será utilizada:

$$[y]_k := (y, y, ..., y),\ k - \text{veces},$$

es decir, $[y]_k$ es la k-tupla cuyas entradas son todas iguales a y.

Considérese ahora a los vectores $v = [1]_q, u \in \mathbb{F}_q^q$, con $u = (0, 1, 2, ..., q-1)$ y

$$c_i := (v + \delta_{i,0}(u - v)) \otimes \cdots \otimes (v + \delta_{i,s-2}(u - v)), i \in \{0, ..., s-1\},$$

donde δ es la delta de Kronecker. Se puede observar que $c_i \in \mathbb{F}_q^{q^{s-1}}$, $\forall i \in \{0, ..., s-1\}$.

Definición 2.4.1. [14] La *función de Gray* está definida como,

$$\begin{array}{rccc} \Phi: & R & \to & \mathbb{F}_q^{q^{s-1}} \\ & \sum_{i=0}^{s-1} a_i p^i & \mapsto & \sum_{i=0}^{s-1} \overline{a}_i c_i \end{array},$$

donde $R = GR(p^s, m)$ y $\overline{*}$ es la función reducción módulo p.

Para emplear la función de Gray es necesario conocer la expresión p-ádica de los elementos de un anillo de Galois y por ende, determinar al conjunto de Teichmüller del mismo.

Los vectores c_i pueden ser expresados de la siguiente manera:

$$\begin{aligned}
c_0 &= ([0]_{q^{s-2}}, [\xi]_{q^{s-2}}, ..., [\xi^{q-1}]_{q^{s-2}}),\\
c_1 &= ([[0]_{q^{s-3}}, [\xi]_{q^{s-3}}, ..., [\xi^{q-1}]_{q^{s-3}}]_q),\\
c_2 &= ([[0]_{q^{s-4}}, [\xi]_{q^{s-4}}, ..., [\xi^{q-1}]_{q^{s-4}}]_{q^2}),\\
&\vdots\\
c_{s-4} &= ([[0]_{q^2}, [\xi]_{q^2}, ..., [\xi^{q-1}]_{q^2}]_{q^{s-4}}),\\
c_{s-3} &= ([[0]_q, [\xi]_q, ..., [\xi^{q-1}]_q]_{q^{s-3}}),\\
c_{s-2} &= ([[0]_{q^0}, [\xi]_{q^0}, ..., [\xi^{q-1}]_{q^0}]_{q^{s-2}}),\\
c_{s-1} &= ([1, ..., 1]_{q^{s-1}}).
\end{aligned}$$

Recordemos que $s, m, n \in \mathbb{Z}^+$, $q = p^m$, p un número primo, y que $S = GR(p^s, mn)$, $R = GR(p^s, m)$, donde S es una extensión de R.

Definición 2.4.2. [30] Sea $n \in \mathbb{Z}^+$. Se define *distancia de Hamming* entre dos elementos $x, y \in \mathbb{F}_q^n$ como el número de entradas donde estos difieren y se denota por $dis_H(x, y)$.

Definición 2.4.3. [30] El *peso de Hamming* de un vector $x \in \mathbb{F}_q^n$ es el número de entradas diferentes de cero y es denotado por $w_H(x)$.

Lema 2.4.1. [19] *Sea Φ la función de Gray sobre R. Entonces,*

$$\Phi(a + b) = \Phi(a) + \Phi(b),$$

para toda $a \in R$ y $b \in p^{s-1}R$.

Empleando la transformada de Fourier sobre anillos de Galois, se presentan los siguientes resultados que serán de importancia para simplificar las propuestas de este trabajo presentadas en el capítulo 4.

Lema 2.4.2. [32] *Sea $u \in R$. Entonces,*

$$\sum_{x \in R} e^{2\pi i \frac{Tr_m(ux)}{p^s}} = \begin{cases} q^s, & \text{si } u = 0,\\ 0, & \text{si } u \neq 0. \end{cases}$$

Demostración. El caso $u = 0$ es trivial. Para el caso $u \neq 0$, ya que la función traza es suprayectiva existe $y \in R$ de modo que $Tr_m(uy) \neq 0$. Entonces

$$\sum_{x \in R} e^{2\pi i \frac{Tr_m(ux)}{p^s}} = \sum_{x+y \in R} e^{2\pi i \frac{Tr_m(u(x+y))}{p^s}} = e^{2\pi i \frac{Tr_m(uy)m}{p^s}} \sum_{x \in R} e^{2\pi i \frac{Tr_m(ux)}{p^s}}.$$

Como

$$1 - e^{2\pi i \frac{Tr_m(uy)}{p^s}} \neq 0,$$

se obtiene el resultado deseado. □

Lema 2.4.3. [32] *Si $u \in R$, entonces se obtiene que,*

$$\sum_{x \in pR} e^{2\pi i \frac{Tr_m(ux)}{p^s}} = \begin{cases} q^{s-1}, & \text{si } u \in p^{s-1}R, \\ 0, & \text{si } u \in R - p^{s-1}R. \end{cases}$$

Demostración. El caso $u \in p^{s-1}R$ es trivial. Si $u \in R - p^{s-1}R$, la suprayectividad de Tr_m implica la existencia de un elemento $y \in p^{s-1}R$ tal que $Tr_m(uy) \neq 0$. El resto de la demostración es similar al lema anterior. □

Lema 2.4.4. [32] *Para cualquier $u \in R$ se cumple que*

$$\sum_{x \in R - pR} e^{2\pi i \frac{Tr_m(ux)}{p^s}} = \begin{cases} q^s - q^{s-1}, & \text{si } u = 0, \\ -q^{s-1}, & \text{si } u \in p^{s-1}R - \{0\}, \\ 0, & \text{si } u \in R - p^{s-1}R. \end{cases}$$

Demostración. Combinando los lemas 2.4.2 y 2.4.3 se concluye la prueba. □

Se introduce ahora la definición de peso homogéneo.

Definición 2.4.4. [32] El *peso homogéneo* sobre el anillo R se define como la función $w_h : R \to \mathbb{N}, u \mapsto w_h(u)$, donde

$$w_h(u) = (q^{s-1} - q^{s-2}) - \frac{1}{q} \sum_{x \in R - pR} e^{2\pi i \frac{Tr_m(ux)}{p^s}}.$$

Observación. Dada la definición anterior y los lemas previos se tienen valores concretos para el peso homogéneo. Sea $u \in R$, entonces,

$$w_h(u) = \begin{cases} 0, & \text{si } u = 0, \\ q^{s-1}, & \text{si } u \in p^{s-1}R - \{0\}, \\ q^{s-1} - q^{s-2}, & \text{si } u \in R - p^{s-1}R. \end{cases}$$

La función de Gray mantiene una igualdad entre la distancia homogénea y la de Hamming sobre el campo finito correspondiente. Sea

$$d_h(u, v) = w_h(u - v)$$

la distancia homogénea inducida por el peso homogéneo, u, $v \in R$.

Teorema 2.4.5. [14] *Sean* $u, v \in R$. *Entonces*

$$d_h(u, v) = dis_H(\Phi(u), \Phi(v)),$$

donde dis_H *es la distancia de Hamming.*

Note que los resultados anteriores, se puede deducir que sobre los anillos de Galois se tiene definido el peso homogéneo en términos de la transformada de Fourier sobre tales anillos. Por otro lado, la función de Gray relaciona la distancia homogénea y la distancia de Hamming sobre un anillo de Galois y su campo finito correspondiente.

2.5. Funciones Resilientes

Chot *et al.* introdujeron por primera vez el concepto de *función resiliente* en 1985, y de manera independiente por Bennet, Brassard y Robert en 1988. Algunas áreas donde las funciones resilientes tienen aplicación son cómputo distribuido tolerante a fallos, distribución de llave en criptografía cuántica y generación de sucesiones aleatorias en cifradores de flujo ([26], [8], [35]).

Definición 2.5.1. [20] Sean $n \in \mathbb{Z}^+$, $J := \{j_0, ..., j_{t-1}\} \subset \{0, ..., n-1\}$. La *J-variedad afín* determinada por $a = (a_0, ..., a_{t-1}) \in \mathbb{F}_2^t$ es el conjunto dado por

$$V_{J,a,n} := \{x \in \mathbb{F}_2^n \mid \forall k \in \{0, ..., t-1\} \ : \ x_{j_k} = a_{j_k} \}.$$

Definición 2.5.2. [20] Sea $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ una función, con $m \leq n$.

1. La función f es *J-resiliente* si $\forall a \in \mathbb{F}_2^t$, la función $f|_{V_{J,a,n}}$ es balanceada.
2. La función f es *t-resiliente* si es J-resiliente para cualquier conjunto J tal que $|J| = t$.

Ejemplos:

1. La función $f : \mathbb{F}_2^n \to \mathbb{F}_2$ dada por

   $$f(x_1, ..., x_n) = x_1 + \cdots + x_n$$

   es $(n-1)$-resiliente [26].
2. La función $f : \mathbb{F}_2^n \to \mathbb{F}_2^2$ dada por

   $$f(x_1, ..., x_{3h}) = (x_1 + \cdots + x_{2h}, x_{2h+1} + \cdots + x_{3h})$$

   es $(2h-1)$-resiliente, para cualquier $h \in \mathbb{Z}^+$ [26].

3. Sea $f : S^r \to S$ una función t-resiliente. Entonces

   - Si $a \in S - pS$, la función $S^r \to S, x \mapsto af(x)$, es t- resiliente.
   - Si $a \in S - pS$, la función $S^r \to \mathbb{Z}_{p^s}, x \mapsto Tr_{mn}(af(x))$, donde Tr_{mn} es la función traza, es una función balanceada.
   - La función
     $$\gamma_{abf} : S^r \to R,\ \gamma_{abf} : x \mapsto Tr_n(af(x) + b \cdot x)$$
     es balanceada siempre que $w_H(b) \leq t$, $(a, b) \in (S^\times \cup \{0\}) \times (S^\times \cup \{0\})^r$, con $(a, b) \neq (0, \mathbf{0})$ (o $(a, b) \in (S - pS) \times S^r$).
   - La transformada de Fourier de la función af está dada por
     $$S^r \to \mathbb{C},\ b \mapsto \zeta_{af}(b),\ \zeta_{af}(b) = \sum_{x \in S^r} e^{\frac{2\pi}{p^s} iTr_{mn}(af(x) - b \cdot x)}.$$
     la cual cumple que $\zeta_{af}(b) = 0$ bajo las condiciones del punto anterior, debido a que la función $x \mapsto Tr_{mn}(af(x) + b \cdot x)$ es balanceada.

2.6. Equivalencia entre la forma p-ádica y aditiva

Recordemos que el teorema 2.3.1 nos garantiza que los elementos de un anillo de Galois se pueden expresar en forma p-ádica y aditiva.

Dado el elemento $a \in R$ expresado en forma p-ádica $a = \sum_{i=0}^{s-1} a_i p^i$, entonces

$$a = \sum_{i=0}^{s-1} \left(\sum_{j=0}^{m-1} x_{ij} \xi^j \right) p^i = \sum_{j=0}^{m-1} \left(\sum_{i=0}^{s-1} x_{ij} p^i \right) \xi^j = \sum_{j=0}^{m-1} b_j \xi^j, \tag{2.1}$$

donde para toda $j = 0, ..., m-1$,

$$b_j = \sum_{i=0}^{s-1} x_{ij} p^i \in \mathbb{Z}_{p^s}. \tag{2.2}$$

Esta relación determina la conversión de la representación p-ádica a su correspondiente forma aditiva.

Recíprocamente, sea $a \in R$ un elemento expresado en forma aditiva

$$a = \sum_{j=0}^{m-1} b_j \xi^j. \tag{2.3}$$

Si expresamos cada coeficiente $b_j \in \mathbb{Z}_{p^s}$ en la forma $\sum_{i=0}^{s-1} x_{ij} p^i$, $x_{ij} \in \mathbb{Z}_p$, se tiene

$$a = \sum_{j=0}^{m-1} b_j \xi^j = \sum_{j=0}^{m-1} \sum_{i=0}^{s-1} x_{ij} p^i \xi^j = \sum_{i=0}^{s-1} \left(\sum_{j=0}^{m-1} x_{ij} \xi^j \right) p^i = \sum_{i=0}^{s-1} a_i p^i, \tag{2.4}$$

donde cada $a_i = \sum_{j=0}^{m-1} x_{ij} \xi^j$.

Observación. $\overline{a_i'} \neq 0 \Rightarrow \exists k_i \in \mathbb{Z}_{p^m-2} \ : \ (\overline{a_i'})^{k_i} = \sum_{j=0}^{m-1} \overline{x_{ij}} \overline{\xi^j}$.

Derivado de la observación, es importante resaltar que en campos finitos la suma de potencias de ξ es una potencia de ξ. A diferencia, en los anillos de Galois, el razonamiento de la ecuación (2.4) para encontrar la forma p-ádica no es de ayuda, ya que la expresión $\sum_{j=0}^{m-1} x_{ij} \xi^j$ de esta ecuación no siempre resulta ser una potencia de ξ, esto es, no siempre es un miembro del conjunto de Teichmüller.

Considérese al polinomio básico primitivo $x^2 + x + 1 \in \mathbb{Z}_4[x]$, el cual divide al polinomio $x^3 - 1$, y que debido a él es posible generar al anillo de Galois $GR(4,2) \cong \mathbb{Z}_4[x]/\langle x^2+x+1 \rangle$.

Sea ξ raíz de $x^2 + x + 1$. Entonces $\xi^2 + \xi + 1 = 0$, luego $\xi^2 = 3\xi + 3$. Por lo que se tiene que

$$GR(4,2) = \{a_0 + a_1 \xi \mid a_i \in \mathbb{Z}_4, \ \ i = 0, 1\}$$

y

$$GR(4,2) = \{b_0 + b_1 \cdot p \mid b_i \in T_{GR(4,2)}, \ \ i = 0, 1\},$$

donde $T_{GR(4,2)} = \{0, 1, \xi, \xi^2\}$.

De manera equivalente se obtiene

$$GR(4,2) = \{0, 1, 2, 3, \xi, 2\xi, 3\xi, 1+\xi, 3+\xi, 1+2\xi, 1+3\xi, 2+\xi, 2+2\xi, 2+3\xi, 3+2\xi, 3+3\xi\}$$

y

$$\begin{aligned} GR(4,2) &= \{0, 1, \xi, \xi^2, 2, 2\xi, 2\xi^2, 3, 1+2\xi, 1+2\xi^2, 2+\xi, 3\xi, \xi+2\xi^2, 2+\xi^2, 2\xi+\xi^2, 3\xi^2\} \\ &= \{0, 1, \xi, 3+3\xi, 2, 2\xi, 2+2\xi, 3, 1+2\xi, 3+2\xi, 2+\xi, 3\xi, 2+3\xi, 1+3\xi, 3+\xi, 1+\xi\}. \end{aligned}$$

Note que si se realiza la sustitución de ξ^2 en la forma p-ádica de los elementos de $GR(4,2)$, se llega a la expresión aditiva de los mismos.

Ejemplo: Tomemos al elemento $1+2\xi^2$ en forma p-ádica y expresémoslo en forma aditiva

$$\begin{aligned} 1+2\xi^2 = 1\cdot 2^0 + \xi^2\cdot 2 &= (1+0\cdot\xi)2^0 + (3+3\xi)2 \\ &= 1+0+6+6\xi = (1+6)+(0+3\xi)2 \\ &= 7+6\xi = 3+2\xi. \end{aligned}$$

Realizar la igualdad anterior es posible debido a la relación (2.1).

Ahora, si elegimos al elemento $1+3\xi$ de la forma aditiva, se tiene que

$$\begin{aligned} 1+3\xi = 1+(1+2)\cdot\xi &= (1+0\cdot 2)+(1+1\cdot 2)\cdot\xi \\ &= (1+0)+(\xi+\xi\cdot 2) = (1+1\cdot\xi)+(0+\xi)\cdot 2 \\ &= (1+1\cdot\xi)+\xi\cdot 2, \end{aligned}$$

pero $1+1\xi$ no es un elemento de $T_{GR(4,2)}$, así que no es posible expresar al elemento $1+3\xi$ en forma p-ádica. Esto muestra que dado un elemento en forma aditiva no siempre se puede obtener su expresión p-ádica.

El ejemplo anterior muestra que la ecuación (2.1) obtiene fácilmente la forma aditiva de un elemento de un anillo de Galois a partir de su expresión p-ádica. Sin embargo, la relación (2.4) no siempre proporciona una manera de obtener la forma p-ádica a partir de la aditiva, por lo que es natural pensar que solucionar dicho problema podría ser más complejo que proponer una igualdad como (2.4).

Derivado de la observación, es importante resaltar que en campos finitos siempre es posible expresar a un elemento como potencia de ξ , sin embargo, en anillos de Galois parece ser un problema más complicado; por un lado se tiene el problema de hallar una potencia de ξ en campos finitos y por otro el problema de obtener obtener la forma p-ádica en el anillo.

1. Problema sobre campos finitos,

$$\begin{aligned} \overline{a} = \overline{a_o} + \overline{a_1}\xi + \cdots + \overline{a_{l-1}}\xi^{m-1} \\ \Big| \\ \overline{\xi}^r \end{aligned}$$

2. Problema sobre el anillo de Galois,

$$\begin{array}{c} a = a_o + a_1\xi + \cdots + a_{l-1}\xi^{m-1} \\ \Big| \\ \xi^{r_0} + \xi^{r_1}p + \cdots + \xi^{r_{s-1}}p^{s-1} \end{array}$$

El problema sobre campos finitos consiste en que dado el elemento $\overline{a}$ es necesario hallar al entero r tal que $\xi^r = \overline{a}$.

Por otra parte, el problema sobre anillos de Galois radica en encontrar el valor de cada exponente r_i de cada ξ correspondiente a los coeficientes en la suma de potencias de p tal que la suma sea igual a a y además determinar qué exponente r_i de ξ le corresponde a su respectiva potencia de p. En 2019, Ku y Morales le dan el nombre de el problema de logaritmo discreto sobre anillos de Galois ([18]), el cual permanece como un problema abierto dentro del área del álgebra moderna.

Capítulo 3

Levantamiento de Hensel y polinomios primitivos

Utilizando la definición de un polinomio mónico básico primitivo se ha elaborado un algoritmo que permite construir estos con los parámetros deseados. Por otro lado, los razonamientos utilizados para la demostración del lema de Hensel, el cual "levanta" un polinomio primitivo, han permitido desarrollar un algoritmo más para la obtención de los básicos primitivos, restringiendo en este caso, de grado a lo más dos. Finalmente, un último algoritmo encuentra los elementos de un anillo de Galois, pues ya construido un polinomio mónico básico primitivo es posible la construcción del anillo de Galois correspondiente.

Antes de revisar su prueba se introducen las siguientes definiciones que son importantes para una mejor comprensión.

Definición 3.0.1. [33] Sean A un anillo y $f(x), g(x) \in A[x]$. Entonces $f(x)$ *divide a* $g(x)$ (denotado como $f(x)|g(x)$) si existe $h(x) \in A[x]$ tal que

$$g(x) = f(x)h(x).$$

Definición 3.0.2. [33] El polinomio $h(x) \in A[x]$ es el *máximo común divisor* de $f(x)$ y $g(x)$:

1. Si $h(x)|f(x)$ y $h(x)|g(x)$ (es decir, $h(x)$ es un divisor común).
2. Si $k(x)|f(x)$ y $k(x)|g(x)$, entonces $k(x)|h(x)$.

El máximo común divisor de $f(x)$ y $g(x)$ se denota por $\text{mcd}(f(x), g(x))$.

Proposición 3.0.1. [33] *Si $h(x)$ es el máximo común divisor de $f(x)$ y $g(x)$, entonces existen $a(x), b(x) \in A[x]$ de manera que*

$$a(x)f(x) + b(x)g(x) = h(x).$$

Observación. Los polinomios $a(x), b(x)$ de la proposición anterior son llamados coeficientes de *Bezout*.

Se enuncia nuevamente el lema de Hensel como recordatorio para el lector junto con su demostración.

Teorema 3.0.1. *(Versión íntegra del lema de Hensel.)* [1] *Sea p un número primo y $k \geq 1$ un entero positivo. Suponga que $u(x), f(x), g(x) \in \mathbb{Z}[x]$ son polinomios mónicos de manera que $f(x)$ y $g(x)$ son primos relativos módulo p y*

$$u(x) \equiv f(x)g(x) \pmod{p^{k+1}}.$$

Entonces, es posible determinar de manera única dos polinomios $f_1(x), g_1(x) \in \mathbb{Z}_{p^{k+1}}$, primos relativos módulo p, los cuales satisfacen las siguientes congruencias:

1. $f(x) \equiv f_1(x) \pmod{p^k}$,
2. $g(x) \equiv g_1(x) \pmod{p^k}$,
3. $u(x) \equiv f_1(x)g_1(x) \pmod{p^{k+1}}$.

Demostración. [1] Se desea hallar de manera explícita dos polinomios mónicos

$$\tilde{f}_1(x), \tilde{g}_1(x) \in \mathbb{Z}[x]$$

de la forma

$$\tilde{f}_1(x) = f(x) + p^k v(x),$$

$$\tilde{g}_1(x) = g(x) + p^k w(x),$$

de modo que, si $f_1(x)$ y $g_1(x)$ son los polinomios $\tilde{f}_1(x)$ y $\tilde{g}_1(x)$ reducidos módulo p^{k+1}, satisfacen 1 y 2.

Si $s, n \in \mathbb{Z}^+$, entonces

$$sp^k \pmod{p^{k+1}} = sp^k + np^{k+1} = (s + np)p^k = (s \pmod{p^k})p^k;$$

por lo que $v(x), w(x) \in \mathbb{Z}_p[x]$.

Por otra parte, al aplicar la condición 3 se obtiene

$$u(x) \equiv f_1(x)g_1(x) \equiv \tilde{f}_1(x)\tilde{g}_1(x) \pmod{p^{k+1}},$$

donde $\tilde{f}_1(x)\tilde{g}_1(x) = f(x)g(x) + (w(x)f(x) + v(x)g(x))p^k + v(x)w(x)p^{2k}$, y como $2k \geq 1$, la congruencia anterior se convierte en

$$u(x) \equiv f_1(x)g_1(x) = f(x)g(x) + (w(x)f(x) + v(x)g(x))p^k \pmod{p^{k+1}}.$$

Obteniendo así,

$$u(x) - f(x)g(x) \equiv (w(x)f(x) + v(x)g(x))p^k \pmod{p^{k+1}},$$

y por hipótesis, $u(x) - f(x)g(x) \equiv 0 \pmod{p^k}$. Luego, si

$$c(x) = \frac{u(x) - f(x)g(x)}{p^k} \in \mathbb{Z}[x]$$

se tiene que

$$c(x) \equiv w(x)f(x) + v(x)g(x) \pmod{p}.$$

Como $f(x)$ y $g(x)$ son primos relativos módulo p, existen dos polinomios $a(x), b(x) \in \mathbb{Z}[x]$ tales que

$$a(x)f(x) + b(x)g(x) \equiv 1 \pmod{p}.$$

Al multiplicar la congruencia anterior por $c(x)$, se sigue que

$$c(x) \equiv c(x)a(x)f(x) + c(x)b(x)g(x) \pmod{p}.$$

Si se expresa $w(x) \equiv c(x)a(x) \pmod{p}$ y $v(x) \equiv c(x)b(x) \pmod{p}$, se tiene la congruencia

$$w(x)f(x) + v(x)g(x) \equiv c(x) \pmod{p}.$$

Debido a la elección de $c(x) \in \mathbb{Z}[x]$, se tiene que $\text{grad}(c(x)) < \text{grad}(f(x)) + \text{grad}(g(x))$, por lo que sin pérdida de generalidad, se puede suponer que $w(x)$ y $v(x)$ satisfacen que $\text{grad}(v(x)) < \text{grad}(f(x))$ y $\text{grad}(w(x)) < \text{grad}(g(x))$.

Los polinomios $v(x), w(x) \in \mathbb{Z}[x]$ están determinados de manera única, pues si existiesen $v_1(x), w_1(x) \in \mathbb{Z}_p[x]$ que cumplieran con 1 y tales que $\text{grad}(w_1(x)) < \text{grad}(g(x))$, $\text{grad}(v_1(x)) < \text{grad}(f(x))$ y con coeficientes en $\mathbb{Z}_p$, entonces

$$(w(x) - w_1(x))f(x) \equiv -(v(x) - v_1(x))g(x) \pmod{p}.$$

Como $\text{grad}(w(x) - w_1(x)) < \text{grad}(g(x))$ y $(f(x), g(x)) = 1 \pmod{p}$, se deduce que

$$w(x) = w_1(x),$$

y de modo similar,

$$v(x) = v_1(x).$$

Por lo tanto, $f_1(x)$ y $g_1(x)$ están determinados de manera única como polinomios en $\mathbb{Z}_{p^{k+1}}$, más aún, son de la forma

$$\tilde{f}_1(x) = f(x) + p^k v(x)$$

y

$$\tilde{g}_1(x) = g(x) + p^k w(x),$$

con $\text{grad}(v(x)) < \text{grad}(f(x))$ y $\text{grad}(w(x)) < \text{grad}(g(x))$.

Finalmente, si se considera $a(x)f_1(x) + b(x)g_1(x) = t(x) \in \mathbb{Z}[x]$, entonces

$$t(x) \equiv a(x)f(x) + b(x)g(x) \equiv 1 \pmod{p},$$

lo cual muestra que $f_1(x)$ y $g_1(x)$ son primos relativos módulo p.

□

Una vez revisada la demostración del lema de Hensel, a continuación se presentan los siguientes algoritmos:

1. El primero, determina todos los polinomios mónicos básicos primitivos, del grado deseado, en $\mathbb{Z}_{p^s}[x]$. Este los encuentra de modo directo utilizando la definición, es decir, evaluando todos los polinomios sobre $\mathbb{Z}_{p^s}$ al considerar los cocientes de $\mathbb{Z}_{p^s}[x]$ y el polinomio. Previamente se consideran los parámetros: un primo p, un entero positivo s y el grado del polinomio. Debido a la cantidad de operaciones a realizar, no es recomendable para parámetros de gran magnitud.

2. El segundo algoritmo utiliza los razonamientos empleados en la demostración anterior, el levantamiento de Hensel de un polinomio básico primitivo de grado 2 en particular, dados un polinomio mónico primitivo, un primo p y un entero positivo s. La implementación encuentra todos los polinomios mónicos básicos primitivos, correspondientes al polinomio mónico primitivo, sobre cada anillo de Galois de característica p^{s_1}, $s_1 < s$.

A continuación se presenta el primer algoritmo.

Algoritmo 1 Polinomios primitivos.

Entrada: primo p, $m, s \in \mathbb{Z}^+$.
Salida: Polinomio mónico básico primitivo en $\mathbb{Z}_{p^s}[x]$.

1: $P \leftarrow \mathbb{Z}_{p^s}[x]$; // Anillo de polinomios con coeficientes en $\mathbb{Z}_{p^s}$.
2: $I \leftarrow \langle g(x) \rangle$; // Ideal generado por g.
3: $R \leftarrow P/I$; // Anillo de Galois S.
4: $T \leftarrow \langle \xi \rangle \cup \{0\}$; // Conjunto de Teichmüller.
5: **if** $\xi^{p^m-1} = 1$ y $\xi^i \neq 1$, con $1 \leq i \leq p^m - 2$. **then**
6: imprimir: Polinomio mínimo g;
7: imprimir: Conjunto de Teichmüller;
8: **else** Descartar polinomio g;
9: **end if**

Algoritmo utilizando el levantamiento de Hensel.

Algoritmo 2 Levantamiento de Hensel.

Entrada: primo p, elementos $m = 2, l, s \in \mathbb{Z}^+$ y polinomio mónico primitivo $f \in \mathbb{Z}_{p^s}[x]$.
Salida: polinomio $fu2$, el levantamiento de Hensel de f, para $s \leftarrow 2$ a l.

1: $P \leftarrow \mathbb{Z}[x]$; // Anillo de polinomios con coeficientes en $\mathbb{Z}$.
2: $h \leftarrow x^{p^m-1} - 1$;
3: $g \leftarrow coc(h, f)$; // Cociente de h dividido entre f.
4: $c_0 \leftarrow res(h, f)$; // Residuo resultante de la división de h entre f.
5: $v \leftarrow res(g, f)$;
6: $o \leftarrow mcd(f, g)$;
7: $o_2 \leftarrow a(x)$; // Coeficiente de Bezout.
8: $f2 \leftarrow \overline{f}$; // Reducción módulo p de los coeficientes de f.
9: **for** $s \leftarrow 2$ **to** l **do**
10: $fu2 \leftarrow \tilde{f2}$; // Reducción módulo p^{s-1} de los coef. de $f2$.
11: $gu_2 \leftarrow coc(h, fu2)$;
12: $cm_1 \leftarrow res(h, fu2)$;
13: $c_1 \leftarrow coc(h - fu2 \cdot gu_2, p^{s-1})$;
14: $c \leftarrow \overline{c_1}$;
15: $v_5 \leftarrow c \cdot o_2$;
16: $v \leftarrow \overline{v_5}$;
17: $fu2 \leftarrow (fu_2 + ((p^{s-1} \cdot v \pmod{p^s}))) \pmod{p^s}$;
18: $a \leftarrow (fu_0, fu_1, fu_2)$. // fu_i coeficientes de $fu2$;
19: **if** $a_m \neq 1$ **then**
20: $h1 \leftarrow a_m^{-1} \pmod{p^s}$;
21: $fu2 \leftarrow (h1 \cdot fu2) \pmod{p^s}$;
22: **end if**
23: **end for**

Ahora, en la siguiente tabla se muestran algunos polinomios básicos primitivos obtenidos con el primer programa, estos son de grado a lo más 4 y con $s = 1$ y 2 para los primos $2, 3, 5, 7, 11$ y 13.

Tabla 3.1: Listado de polinomios básicos primitivos.

Primo p	m	s	Polinomio básico primitivo
2	2	1 2	$x^2 + x + 1$
	3	1	$x^3 + x^2 + 1$ $x^3 + x + 1$
		2	$x^3 + 2x^2 + 3$ $x^3 + 3x^2 + 2x + 3$
	4	1	$x^4 + x^3 + 1$ $x^4 + x + 1$
		2	$x^4 + 3x^3 + 2x^2 + 1$ $x^3 + 2x^2 + 3x + 1$
	5	1	$x^5 + x^3 + 1$ $x^5 + x^2 + 1$ $x^5 + x^4 + x^3 + x^2 + 1$ $x^5 + x^4 + x^3 + x + 1$ $x^5 + x^4 + x^2 + x + 1$ $x^5 + x^3 + x^2 + x + 1$
		2	$x^5 + 2x^4 + x^3 + 3$ $x^5 + x^4 + 3x^3 + x + 3$ $x^5 + x^4 + 3x^3 + x^2 + 2x + 3$ $x^5 + 3x^2 + 2x + 3$ $x^5 + 3x^4 + x^2 + 3x + 3$ $x^5 + 2x^4 + 3x^3 + x^2 + 3x + 3$
	6	1	$x^6 + x^5 + 1$ $x^6 + x^5 + x^3 + x^2 + 1$ $x^6 + x + 1$ $x^6 + x^5 + x^4 + x + 1$ $x^6 + x^4 + x^3 + x + 1$ $x^6 + x^5 + x^2 + x + 1$
		2	$x^6 + 3x^5 + 2x^3 + 1$ $x^6 + 3x^5 + 2x^4 + x^2 + x + 1$ $x^6 + 3x^5 + x^3 + x^2 + 2x + 1$ $x^6 + 2x^5 + x^4 + x^3 + 3x + 1$ $x^6 + 2x^3 + 3x + 1$ $x^6 + x^5 + x^4 + 2x^2 + 3x + 1$

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
2	7	1	x^7+x^6+1
			x^7+x^4+1
			$x^7+x^6+x^5+x^4+1$
			x^7+x^3+1
			$x^7+x^5+x^4+x^3+1$
			$x^7+x^6+x^5+x^2+1$
			$x^7+x^6+x^4+x^2+1$
			$x^7+x^4+x^3+x^2+1$
			$x^7+x^6+x^5+x^4+x^3+x^2+1$
			x^7+x+1
		2	$x^7+2x^5+x^3+3$
			$x^7+3x^6+2x^3+3$
			$x^7+3x^4+2x^2+3$
			$x^7+2x^6+3x^5+x^4+x^3+2x^2+3$
			$x^7+x^6+3x^5+3x^4+2x^3+2x^2+3$
			x^7+2x^4+x+3
			$x^7+3x^6+2x^5+x^4+2x^3+2x^2+x+3$
			$x^7+2x^6+3x^5+3x^3+2x^2+x+3$
			$x^7+3x^6+2x^5+2x^4+3x^3+2x^2+x+3$
			$x^7+3x^6+2x^5+x^4+x^2+2x+3$
	8	2	$x^8+2x^7+x^6+3x^5+x^3+1$
			$x^8+3x^7+2x^6+x^5+3x^3+1$
			$x^8+2x^7+3x^6+x^5+3x^4+2x^3+2x^2+1$
			$x^8+3x^7+2x^5+x^2+x+1$
			$x^8+x^7+3x^6+x^5+2x^4+x^2+x+1$
			$x^8+2x^7+3x^6+x^4+3x^3+x^2+x+1$
			$x^8+x^7+x^6+2x^4+x^3+3x^2+x+1$
			$x^8+2x^7+x^6+2x^5+x^3+x^2+2x+1$
			$x^8+2x^7+x^6+x^5+2x^3+x^2+2x+1$
			$x^8+x^5+3x^3+x^2+2x+1$
			$x^8+3x^7+2x^4+3x^3+x^2+2x+1$
			$x^8+x^7+x^6+3x^5+x^4+3x^2+2x+1$
			$x^8+2x^6+2x^5+3x^4+x^3+3x^2+2x+1$
			$x^8+2x^7+x^6+3x^5+2x^4+3x+1$
			$x^8+x^7+x^6+2x^3+3x+1$
			$x^8+3x^5+x^3+2x^2+3x+1$
	9	2	$x^9+2x^7+x^5+3$
			$x^9+3x^8+3x^6+x^5+2x^4+2x^3+3$

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
2	9	2	$x^9+x^8+x^7+3x^6+3x^5+3x^3+3$ $x^9+2x^7+x^6+x^5+2x^4+3x^3+3$ $x^9+3x^8+2x^7+2x^6+x^5+x^4+2x^2+3$ $x^9+3x^4+2x^2+3$ $x^9+x^8+3x^7+2x^6+3x^5+3x^4+x^3+2x^2+3$ $x^9+2x^8+x^7+3x^6+2x^5+3x^4+2x^3+2x^2+3$ $x^9+x^8+3x^7+3x^6+x^4+3x^3+2x^2+3$ $x^9+2x^8+3x^7+3x^6+x^5+x^4+3x^3+2x^2+3$ $x^9+x^6+2x^5+3x^4+3x^3+2x^2+3$ $x^9+x^8+x^7+x^6+3x^5+x+3$ $x^9+x^8+x^7+x^6+3x^5+x^4+x^3+x+3$ $x^9+2x^6+2x^5+3x^4+x^3+x+3$ $x^9+3x^8+2x^7+3x^5+2x^4+2x^3+x+3$ $x^9+2x^8+3x^7+2x^6+3x^5+2x^4+2x^3+x+3$
3	2	1	x^2+x+2 x^2+2x+2
		2	x^2+4x+8 x^2+5x+2
	3	1	x^3+2x^2+1 x^3+2x^2+x+1 x^3+2x+1 x^3+x^2+2x+1
		2	x^3+3x^2+2x+1 x^3+2x^2+3x+1 x^3+7x^2+5x+3 x^3+5x^2+7x+3
		3	$x^3+20x^2+12x+1$ $x^3+12x^2+20x+1$ $x^3+25x^2+23x+1$ $x^3+23x^2+25x+1$
		4	$x^3+74x^2+39x+1$ $x^3+77x^2+52x+1$ $x^3+39x^2+74x+1$ $x^3+52x^2+77x+1$

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
3	4	1	x^4+x^3+2 x^4+2x^3+2 x^4+x+2 $x^4+2x^3+x^2+x+2$ $x^4+2x^3+2x^2+x+2$ x^4+2x+2 $x^4+x^3+x^2+2x+2$ $x^4+x^3+2x^2+2x+2$
		2	$x^4+3x^3+3x^2+x+8$ $x^4+5x^3+7x^2+x+8$ $x^4+x^3+6x^2+3x+8$ $x^4+8x^3+2x^2+4x+8$ $x^4+x^3+2x^2+5x+8$ $x^4+8x^3+6x^2+6x+8$ $x^4+6x^3+3x^2+8x+8$ $x^4+4x^3+7x^2+8x+8$
5	2	1	x^2+x+2 x^2+4x+2 x^2+2x+3 x^2+3x+3
		2	$x^2+11x+7$ $x^2+14x+7$ $x^2+2x+18$ $x^2+23x+18$
	3	1	x^3+x^2+x+2 x^3+3x^2+2 x^3+3x^2+x+2 x^3+4x^2+x+2 x^3+2x^2+2x+2 x^3+3x^2+2x+2 x^3+3x+2 x^3+4x+2 x^3+2x^2+4x+2 x^3+4x^2+4x+2
		2	x^3+3x^2+x+7 x^3+7x^2+4x+7 x^3+9x^2+4x+7 x^3+8x^2+5x+7

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
5	3	2	$x^3 + 12x^2 + 7x + 7$ $x^3 + 11x^2 + 10x + 7$ $x^3 + 3x^2 + 12x + 7$ $x^3 + 24x^2 + 16x + 7$ $x^3 + 10x^2 + 19x + 7$ $x^3 + 20x^2 + 23x + 7$
	4	1	$x^4 + x^3 + 2x^2 + 2$ $x^4 + 4x^3 + 2x^2 + 2$ $x^4 + 2x^3 + 3x^2 + 2$ $x^4 + 3x^3 + 3x^2 + 2$ $x^4 + 3x^3 + x + 2$ $x^4 + 4x^3 + x + 2$ $x^4 + x^3 + 2x^2 + x + 2$ $x^4 + 4x^3 + 3x^2 + x + 2$ $x^4 + 4x^2 + x + 2$ $x^4 + 2x^3 + 2x + 2$
		2	$x^4 + x^3 + x^2 + 3$ $x^4 + 3x^3 + x^2 + 3$ $x^4 + 4x^3 + x^2 + 3$ $x^4 + 6x^3 + x^2 + 3$ $x^4 + 2x^3 + 2x^2 + 3$ $x^4 + 5x^3 + 2x^2 + 3$ $x^4 + 2x^3 + 3x^2 + 3$ $x^4 + 5x^3 + 3x^2 + 3$ $x^4 + 2x^3 + 4x^2 + 3$ $x^4 + 5x^3 + 4x^2 + 3$
7	2	1	$x^2 + x + 3$ $x^2 + 2x + 3$ $x^2 + 5x + 3$ $x^2 + 6x + 3$ $x^2 + 2x + 5$ $x^2 + 3x + 5$ $x^2 + 4x + 5$ $x^2 + 5x + 5$
		2	$x^2 + 9x + 19$ $x^2 + 17x + 19$ $x^2 + 32x + 19$ $x^2 + 40x + 19$

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
7	2	2	$x^2+12x+31$ $x^2+15x+31$ $x^2+34x+31$ $x^2+37x+31$
	3	1	x^3+x^2+x+2 x^3+6x^2+x+2 x^3+3x^2+2x+2 x^3+4x^2+2x+2 x^3+3x+2 x^3+4x^2+3x+2 x^3+5x^2+3x+2 x^3+6x^2+3x+2 x^3+2x^2+4x+2 x^3+5x^2+4x+2
		2	$x^3+44x^2+6x+18$ $x^3+38x^2+7x+18$ $x^3+22x^2+9x+18$ $x^3+40x^2+9x+18$ $x^3+46x^2+10x+18$ $x^3+31x^2+12x+18$ $x^3+12x^2+13x+18$ $x^3+47x^2+14x+18$ $x^3+23x^2+15x+18$ $x^3+24x^2+15x+18$
	4	1	$x^4+x^3+x^2+3$ $x^4+3x^3+x^2+3$ $x^4+4x^3+x^2+3$ $x^4+6x^3+x^2+3$ $x^4+2x^3+2x^2+3$ $x^4+5x^3+2x^2+3$ $x^4+6x^3+4x^2+x+3$ $x^4+3x^3+5x^2+x+3$ $x^4+5x^3+5x^2+x+3$ x^4+4x^3+2x+3
11	2	1	x^2+4x+2 x^2+5x+2 x^2+6x+2 x^2+7x+2

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
11	2	1	x^2+2x+6
			x^2+3x+6
			x^2+8x+6
			x^2+9x+6
			x^2+x+7
			x^2+4x+7
			x^2+7x+7
			$x^2+10x+7$
			x^2+x+8
			x^2+3x+8
			x^2+8x+8
			$x^2+10x+8$
		2	$x^2+26x+40$
			$x^2+45x+40$
			$x^2+76x+40$
			$x^2+95x+40$
			$x^2+8x+94$
			$x^2+42x+94$
			$x^2+79x+94$
			$x^2+113x+94$
			$x^2+15x+112$
			$x^2+49x+112$
			$x^2+72x+112$
			$x^2+106x+112$
			$x^2+14x+118$
			$x^2+43x+118$
			$x^2+78x+118$
			$x^2+107x+118$
	3	1	x^3+x^2+3
			x^3+3x^2+3
			x^3+6x^2+3
			x^3+8x^2+3
			x^3+x^2+x+3
			x^3+4x^2+x+3
			x^3+8x^2+x+3
			x^3+9x^2+x+3
			x^3+x^2+2x+3
			x^3+2x^2+2x+3

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
11	3	2	x^3+57x^2+3x+3 x^3+20x^2+6x+3 x^3+103x^2+8x+3 $x^3+90x^2+21x+3$ $x^3+107x^2+23x+3$ $x^3+57x^2+24x+3$ $x^3+93x^2+25x+3$ $x^3+22x^2+27x+3$ $x^3+51x^2+27x+3$ $x^3+43x^2+29x+3$
13	2	1	x^2+x+2 x^2+4x+2 x^2+6x+2 x^2+7x+2 x^2+9x+2 $x^2+12x+2$ x^2+2x+6 x^2+3x+6 x^2+4x+6 x^2+9x+6 $x^2+10x+6$ $x^2+11x+6$ x^2+2x+7 x^2+3x+7 x^2+6x+7 x^2+7x+7 $x^2+10x+7$ $x^2+11x+7$ $x^2+4x+11$ $x^2+5x+11$ $x^2+6x+11$ $x^2+7x+11$ $x^2+8x+11$ $x^2+9x+11$
	2	2	$x^2+55x+19$ $x^2+63x+19$ $x^2+74x+19$ $x^2+95x+19$

Continua en la siguiente página

Tabla 3.1 – Continuación de la página anterior

Primo p	m	s	Polinomio básico primitivo
13	2	2	$x^2 + 106x + 19$ $x^2 + 114x + 19$ $x^2 + 12x + 80$ $x^2 + 72x + 80$ $x^2 + 82x + 80$ $x^2 + 87x + 80$ $x^2 + 97x + 80$ $x^2 + 157x + 80$ $x^2 + 5x + 89$ $x^2 + 6x + 89$ $x^2 + 30x + 89$ $x^2 + 139x + 89$ $x^2 + 163x + 89$ $x^2 + 164x + 89$ $x^2 + 16x + 150$ $x^2 + 37x + 150$ $x^2 + 59x + 150$ $x^2 + 110x + 150$ $x^2 + 132x + 150$ $x^2 + 153x + 150$
	3	1	$x^3 + x^2 + 2$ $x^3 + 2x^2 + 2$ $x^3 + 3x^2 + 2$ $x^3 + 5x^2 + 2$ $x^3 + 6x^2 + 2$ $x^3 + 11x^2 + x + 2$ $x^3 + 12x^2 + x + 2$ $x^3 + 10x^2 + 3x + 2$ $x^3 + 9x^2 + 4x + 2$ $x^3 + 12x^2 + 5x + 2$

La siguiente tabla muestra el levantamiento de Hensel de polinomios primitivos de grado 2, para los primos 2, 3, 5, 7, 11 y 13, con $s \in \{2, ..., 8\}$.

Tabla 3.2: Levantamiento de Hensel de polinomios primitivos de grado 2.

Primo p	s	Polinomio primitivo	Levantamiento de Hensel
2	2 3 4 5 6 7 8	$x^2 + x + 1$	$x^2 + x + 1$
3	2	$x^2 + x + 2$	$x^2 + 4x + 8$
	3		$x^2 + 22x + 26$
	4		$x^2 + 22x + 80$
	5		$x^2 + 22x + 242$
	6		$x^2 + 508x + 728$
	7		$x^2 + 508x + 2186$
	8		$x^2 + 2695x + 6560$
3	2	$x^2 + 2x + 2$	$x^2 + 5x + 8$
	3		$x^2 + 5x + 26$
	4		$x^2 + 59x + 80$
	5		$x^2 + 221x + 242$
	6		$x^2 + 221x + 728$
	7		$x^2 + 1679x + 2186$
	8		$x^2 + 3866x + 6560$
5	2	$x^2+11x+7$	$x^2 + 11x + 7$
	3		$x^2 + 36x + 57$
	4		$x^2 + 286x + 182$
	5		$x^2 + 1536x + 2057$
	6		$x^2 + 7786x + 14557$
	7		$x^2 + 39036x + 45807$
	8		$x^2 + 273411x + 280182$
5	2	$x^2+14x+7$	$x^2 + 14x + 7$
	3		$x^2 + 89x + 57$
	4		$x^2 + 339x + 182$
	5		$x^2 + 1589x + 2057$
	6		$x^2 + 7839x + 14557$
	7		$x^2 + 39089x + 45807$

Continua en la siguiente página

Tabla 3.2 – Continuación de la página anterior

Primo p.	s.	Polinomio primitivo.	Levantamiento de Hensel.
5	8	$x^2+14x+7$	$x^2+117214x+280182$
5	2	$x^2+2x+18$	$x^2+2x+18$
	3		$x^2+52x+68$
	4		$x^2+177x+443$
	5		$x^2+177x+1068$
	6		$x^2+12677x+1068$
	7		$x^2+75177x+32318$
	8		$x^2+153302x+110443$
5	2	$x^2+23x+18$	$x^2+23x+18$
	3		$x^2+73x+68$
	4		$x^2+448x+443$
	5		$x^2+2948x+1068$
	6		$x^2+2948x+1068$
	7		$x^2+2948x+32318$
	8		$x^2+237323x+110443$
7	2	x^2+x+3	$x^2+15x+31$
	3		$x^2+113x+325$
	4		$x^2+456x+1354$
	5		$x^2+14862x+1354$
	6		$x^2+98897x+34968$
	7		$x^2+804791x+740862$
	8		$x^2+5746049x+2387948$
7	2	x^2+2x+3	$x^2+37x+31$
	3		$x^2+86x+325$
	4		$x^2+429x+1354$
	5		$x^2+10033x+1354$
	6		$x^2+60454x+34968$
	7		$x^2+648699x+740862$
	8		$x^2+2295785x+2387948$
7	2	x^2+5x+3	$x^2+12x+31$
	3		$x^2+257x+325$
	4		$x^2+1972x+1354$
	5		$x^2+6774x+1354$
	6		$x^2+57195x+34968$
	7		$x^2+174844x+740862$
	8		$x^2+3469016x+2387948$
7	2	x^2+6x+3	$x^2+34x+31$

Continua en la siguiente página

Tabla 3.2 – Continuación de la página anterior

Primo p.	s.	Polinomio primitivo.	Levantamiento de Hensel.
7	3	x^2+6x+3	$x^2+230x+325$
	4		$x^2+1945x+1354$
	5		$x^2+1945x+1354$
	6		$x^2+57195x+34968$
	7		$x^2+18752x+740862$
	8		$x^2+18752x+2387948$
7	2	x^2+2x+5	$x^2+9x+19$
	3		$x^2+254x+19$
	4		$x^2+2312x+1048$
	5		$x^2+7114x+15454$
	6		$x^2+74342x+82682$
	7		$x^2+544938x+82682$
	8		$x^2+2192024x+3376854$
7	2	x^2+3x+5	$x^2+17x+19$
	3		$x^2+262x+19$
	4		$x^2+605x+1048$
	5		$x^2+5407x+15454$
	6		$x^2+22214x+82682$
	7		$x^2+22214x+82682$
	8		$x^2+3316386x+3376854$
7	2	x^2+4x+5	$x^2+32x+19$
	3		$x^2+81x+19$
	4		$x^2+1796x+1048$
	5		$x^2+11400x+15454$
	6		$x^2+95435x+82682$
	7		$x^2+801329x+82682$
	8		$x^2+2448415x+3376854$
7	2	x^2+5x+5	$x^2+40x+19$
	3		$x^2+89x+19$
	4		$x^2+89x+1048$
	5		$x^2+9693x+15454$
	6		$x^2+43307x+82682$
	7		$x^2+278605x+82682$
	8		$x^2+3572777x+3376854$
11	2	x^2+4x+2	$x^2+15x+112$
	3		$x^2+1104x+596$
	4		$x^2+14414x+12575$

Continua en la siguiente página

Tabla 3.2 – Continuación de la página anterior

Primo p.	s.	Polinomio primitivo.	Levantamiento de Hensel.
11	5	x^2+4x+2	$x^2+43696x+27216$
	6		$x^2+43696x+349318$
	7		$x^2+3586818x+5664001$
	8		$x^2+3586818x+181048540$
11	2	x^2+5x+2	$x^2+49x+112$
	3		$x^2+1017x+596$
	4		$x^2+11665x+12575$
	5		$x^2+128793x+27216$
	6		$x^2+611946x+349318$
	7		$x^2+18327556x+5664001$
	8		$x^2+37814727x+181048540$
11	2	x^2+6x+2	$x^2+72x+112$
	3		$x^2+314x+596$
	4		$x^2+2976x+12575$
	5		$x^2+32258x+27216$
	6		$x^2+1159615x+349318$
	7		$x^2+1159615x+5664001$
	8		$x^2+176544154x+181048540$
11	2	x^2+7x+2	$x^2+106x+112$
	3		$x^2+227x+596$
	4		$x^2+227x+12575$
	5		$x^2+117355x+27216$
	6		$x^2+1727865x+349318$
	7		$x^2+15900353x+5664001$
	8		$x^2+210772063x+181048540$
11	2	x^2+2x+6	$x^2+79x+94$
	3		$x^2+1047x+699$
	4		$x^2+6371x+12678$
	5		$x^2+138140x+56601$
	6		$x^2+1426548x+378703$
	7		$x^2+1426548x+9236508$
	8		$x^2+79375232x+9236508$
11	2	x^2+3x+6	$x^2+113x+94$
	3		$x^2+1202x+699$
	4		$x^2+14512x+12678$
	5		$x^2+160922x+56601$
	6		$x^2+966177x+378703$

Continua en la siguiente página

Tabla 3.2 – Continuación de la página anterior

Primo p.	s.	Polinomio primitivo.	Levantamiento de Hensel.
11	7	x^2+3x+6	$x^2+966177x+9236508$
	8		$x^2+117889203x+9236508$
11	2	x^2+8x+6	$x^2+8x+94$
	3		$x^2+129x+699$
	4		$x^2+129x+12678$
	5		$x^2+129x+56601$
	6		$x^2+805384x+378703$
	7		$x^2+18520994x+9236508$
	8		$x^2+96469678x+9236508$
11	2	x^2+9x+6	$x^2+42x+94$
	3		$x^2+284x+699$
	4		$x^2+8270x+12678$
	5		$x^2+22911x+56601$
	6		$x^2+345013x+378703$
	7		$x^2+18060623x+9236508$
	8		$x^2+134983649x+9236508$
13	2	x^2+x+2	$x^2+157x+80$
	3		$x^2+495x+418$
	4		$x^2+2692x+4812$
	5		$x^2+116936x+119056$
	6		$x^2+4201159x+861642$
	7		$x^2+28335204x+24995687$
	8		$x^2+593071857x+526983823$
13	2	x^2+4x+2	$x^2+82x+80$
	3		$x^2+927x+418$
	4		$x^2+927x+4812$
	5		$x^2+86610x+119056$
	6		$x^2+457903x+861642$
	7		$x^2+29418757x+24995687$
	8		$x^2+719652444x+526983823$
13	2	x^2+6x+2	$x^2+97x+80$
	3		$x^2+1449x+418$
	4		$x^2+5843x+4812$
	5		$x^2+5843x+119056$
	6		$x^2+748429x+861642$
	7		$x^2+24882474x+24995687$
	8		$x^2+777864678x+526983823$

Continua en la siguiente página

Tabla 3.2 – Continuación de la página anterior

Primo p.	s.	Polinomio primitivo.	Levantamiento de Hensel.
13	2	x^2+7x+2	$x^2+72x+80$
	3		$x^2+748x+418$
	4		$x^2+22718x+4812$
	5		$x^2+365450x+119056$
	6		$x^2+4078380x+861642$
	7		$x^2+37866043x+24995687$
	8		$x^2+37866043x+526983823$
13	2	x^2+2x+6	$x^2+106x+19$
	3		$x^2+613x+1540$
	4		$x^2+9401x+23510$
	5		$x^2+123645x+109193$
	6		$x^2+494938x+1965658$
	7		$x^2+10148556x+30926512$
	8		$x^2+700382243x+281920580$
13	2	x^2+3x+6	$x^2+55x+19$
	3		$x^2+1914x+1540$
	4		$x^2+12899x+23510$
	5		$x^2+127143x+109193$
	6		$x^2+4582659x+1965658$
	7		$x^2+48023940x+30926512$
	8		$x^2+487263559x+281920580$
13	2	x^2+2x+7	$x^2+132x+150$
	3		$x^2+470x+657$
	4		$x^2+26834x+5051$
	5		$x^2+369566x+262100$
	6		$x^2+3339910x+2861151$
	7		$x^2+8166719x+31822005$
	8		$x^2+572903372x+533810141$
13	2	x^2+6x+7	$x^2+110x+150$
	3		$x^2+2138x+657$
	4		$x^2+26305x+5051$
	5		$x^2+197671x+262100$
	6		$x^2+3910601x+2861151$
	7		$x^2+8737410x+31822005$
	8		$x^2+71485927x+533810141$

Una vez encontrado un polinomio mónico básico primitivo es posible la construcción de su anillo de Galois correspondiente. De este modo podemos encontrar todos los elementos del anillo, expresados en su forma aditiva. Aquí se presenta el algoritmo.

Algoritmo 3 Forma aditiva de un anillo de Galois.

Entrada: primo p, $m, s, \in \mathbb{Z}^+$, polinomio g arbitrario.
Salida: Elementos en forma p-ádica del anillo de Galois R.

1: $P \leftarrow \mathbb{Z}_{p^s}[x]$; // Polinomios con coeficientes en $\mathbb{Z}_{p^s}$.
2: $I \leftarrow \langle g(x) \rangle$; // Ideal generado por g.
3: $R \leftarrow P/I$; // Anillo de Galois R.
4: $T_1 \leftarrow \langle \xi \rangle$.
5: **for** $a_0, a_1, ..., a_{m-1} \in \mathbb{Z}_{p^s}$. **do**
6: imprimir $a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{m-1}\xi^{m-1}$;
7: **end for**

Capítulo 4

Esquemas de autenticación y función de Gray

La primera sección de este capítulo define en general un esquema de autenticación sin secreto, posteriormente se dan las herramientas necesarias para la construcción de los dos esquemas dados más adelante.

Se presentan dos esquemas de autenticación, el primero de ellos obtiene mejoras respecto a la construcción realizada en 2018 ([20]). Estas mejoras son la forma y tamaño de los espacios, pues el tamaño del espacio fuente en este trabajo tiene tamaño mayor y el espacio de llaves mantiene su magnitud; además, se simplifican las operaciones necesarias para la demostración de sus propiedades. El segundo esquema reduce el tamaño del espacio de llaves del primer esquema, ya que elimina los elementos del ideal más pequeño de anillo de Galois intermedio, permitiendo de este modo una mejor relación entre el espacio de llaves y el espacio fuente.

En la construcción de estos esquemas se utilizan la función de Gray, funciones resilientes y la función traza sobre anillos de Galois. La función de Gray es de suma importancia, ya que es la que permite esa relación entre los anillos de Galois y los campos finitos correspondientes; las funciones resilientes permiten el balanceo en la estructura de las reglas de codificación; finalmente, la función traza relaciona las extensiones de anillos de Galois y mantiene el balanceo, inicialmente dado por las funciones resilientes, en la estructura de las reglas de codificación.

4.1. Esquema general de autenticación sin secreto

Suponga que un transmisor y un receptor, Alicia y Beto, desean comunicarse a través de un canal público. Ya que se comunican a través de un canal inseguro existe la posibilidad

de que un intruso, en este caso Eva, pueda simplemente insertar un mensaje en el canal de comunicación, esperando que Beto lo acepte como auténtico, o alterar la integridad de un mensaje que ya ha sido enviado. Para darle autenticidad a los mensajes que Alicia envía ellos utilizan un *esquema de auntenticación* sin secreto; de este modo, comparten entre sí una llave secreta, previamente establecida. Se supone también que no es de interés mantener en secreto la información enviada. Con la ayuda del esquema, Beto es capaz de saber si un mensaje que ha recibido fue modificado, y rechazarlo si es el caso.

En un esquema de autenticación sin secreto se tienen dos problemas principales: obtener la mínima probabilidad de que un mensaje insertado por un intruso sea aceptado como auténtico y mantener la mayor diferencia de cardinalidad entre el espacio de llaves y los mensajes (el producto de los elementos del espacio fuente y el espacio de etiquetado), considerano el espacio de llaves con menor tamaño.

Definición 4.1.1. [20] Un *esquema de autenticación* sin secreto es una tupla

$$\mathcal{A} = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}),$$

donde $\mathcal{S}$ es el espacio fuente, $\mathcal{T}$ es el espacio de etiquetas, $\mathcal{K}$ es el espacio de llaves y $\mathcal{E} = (e_k)_{k\in\mathcal{K}}$ es el espacio de reglas de cifrado o codificación $\mathcal{S} \to \mathcal{T}$.

Un transmisor y un receptor acuerdan una llave secreta $k \in \mathcal{K}$. Siempre que un elemento $s \in \mathcal{S}$ deba ser enviado, los participantes proceden de acuerdo al siguiente protocolo:

Alicia		Beto
evalua $t = e_k(s) \in \mathcal{T}$ y envía el par $m = (s,t)$	$\underrightarrow{m}$	recibe $m' = (s',t')$, evalua $t'' = e_k(s') \in \mathcal{T}$. Si $t' = t''$, entonces acepta a s', de lo contrario, rechaza a m'.
Nota: m es la dupla que se envía y s es el mensaje en claro		

Tabla 4.1: Protocolo para enviar un elemento $s \in \mathcal{S}$.

El canal de comunicación es público y un intruso puede realizar ataques de *personificación* y *sustitución*. Las probabilidades de éxito del intruso para estos ataques son respectivamente,

$$P_I = \max_{(s,t)\in\mathcal{S}\times\mathcal{T}} \frac{|\{k \in \mathcal{K}|\, e_k(s) = t\}|}{|\mathcal{K}|},$$

$$P_S = \max_{(s,t)\in\mathcal{S}\times\mathcal{T}} \max_{(s',t')\in(\mathcal{S}-\{s\})\times\mathcal{T}} \frac{|\{k\in\mathcal{K}|\ e_k(s)=t\ \&\ e_k(s')=t'\}}{|\{k\in\mathcal{K}|\ e_k(s)=t\}|}.$$

Se tienen las siguientes cotas generales para P_I y P_S [11]:

$$P_I \geq \frac{1}{|\mathcal{T}|} \text{ y } P_S \geq \frac{1}{|\mathcal{T}|},$$

ya que $|\mathcal{T}|P_I \geq \sum_{t\in\mathcal{T}} \frac{|\{k\in\mathcal{K}:E_k(s)=t\}|}{|\mathcal{K}|} = 1$. En forma análoga para P_S. Por lo tanto el objetivo es tener P_I y P_S lo más cercano posible a

$$\frac{1}{|\mathcal{T}|}.$$

4.2. Antecedentes a los esquemas propuestos

Antes de introducir los esquemas de autenticación se definen algunos conjuntos en los anillos de Galois, los cuales forman parte de los espacios de los esquemas de autenticación dados más adelante. Utilizando la función traza, funciones resilientes y la función de Gray se define una función sobre estos conjuntos, la que será una regla codificación. En particular, se encuentra la distancia de Hamming entre dos vectores sobre un un campo finito; para esto, se utiliza la isometría dada en el teorema 2.4.5, pues los elementos son dados inicialmente en el anillo de Galois correspondiente. Finalmente, se prueban algunas propiedades de la función traza, necesarias en las pruebas implicadas en la construcción de nuestros esquemas.

Recordemos que $s, m, n \in \mathbb{Z}^+$, $q = p^m$, con p un número primo, y que $S = GR(p^s, mn)$, $R = GR(p^s, m)$, donde S es extensión de R.

Sea $f : S^r \to S$ una función t-resiliente. Para $r \in \mathbb{Z}^+$, $r > 1$ arbitrario, se definen los siguientes conjuntos:

$$L := \{\sum_{i=0}^{s-2} r_i p^i \mid (r_0, ..., r_{s-2}) \in T_R^{r-1}\}$$

y

$$S_0 := S^\times \cup \{0\},\ S_1 := (S^\times \cup \{0\})^r,\ S_2 := L.$$

Note que

$$|S_0| = (q^n - 1)q^{(s-1)n} + 1, |S_1| = [(q^n - 1)q^{(s-1)n} + 1]^r, |S_2| = q^{r-1}.$$

Denotemos $\mathcal{S} = \{(s_0, s_1, s_2) \in S_0 \times S_1 \times S_2 \mid (s_0, s_1) \neq (0, \mathbf{0}), w_H(b) \leq \frac{t}{2}\}$.

Tambien para cada $s = (s_0, s_1, s_2) \in \mathcal{S}$ y cada $w \in p^{s-1}R$, considere la función

$$v_{s,w} : S^r \to R, x \mapsto v_{s,w}(x),$$

donde

$$v_{s,w}(x) = Tr_n(s_0 f(x) + s_1 x) + s_2 + w.$$

Por último,

$$u_{s,w} = (\Phi(v_{s,w}(x)))_{x \in S^r} \in (\mathbb{F}_q^{q^{s-1}})^{q^{nsr}}$$

y

$$u_s = (u_{s,w})_{w \in p^{s-1}R} \in (\mathbb{F}_q^{q^{s-1}})^{q^{nsr+1}} \cong \mathbb{F}_q^{q^{s(nr+1)}}.$$

A continuación se demuestra el siguiente resultado, en donde se considera la extensión S sobre R y la extensión R sobre $\mathbb{Z}_{p^s}$. Nótese la importancia de la función de Gray y cómo se relaciona la distancia de Hamming y la distancia homogénea.

Proposición 4.2.1. [20] *Sea d_H la distancia de Hamming sobre el espacio vectorial $\mathbb{F}_q^{q^{s(nr+1)}}$ y $f : S^r \to S$ una función t-resiliente. Dados dos puntos*

$$s_0 = (s_{00}, s_{10}, s_{20}), s_1 = (s_{01}, s_{11}, s_{21}) \in \mathcal{S}$$

arbitrarios con $s_0 \neq s_1$ y $w_0, w_1 \in p^{s-1}R$ arbitrarios, se cumple la siguiente igualdad:

$$d_H(u_{s_0,w_0}, u_{s_1,w_1}) = q^{snr}(q^{s-1} - q^{s-2}).$$

Demostración. Sea $s_2 = s_0 - s_1$ y $w_2 = w_0 - w_1$. Entonces, aplicando la definición de distancia de Hamming y el hecho de que la función de Gray es una isometría se tiene

$$\begin{aligned}
d_H(u_{s_0,w_0}, u_{s_1,w_1}) &= \sum_{x\in R^r} d_H(\Phi(v_{s_0,w_0}(x)), \Phi(v_{s_1,w_1}(x))) \\
&= \sum_{x\in R^r} d_H(v_{s_0,w_0}(x), v_{s_1,w_1}(x)) \\
&= \sum_{x\in R^r} w_h(v_{s_0,w_0}(x) - v_{s_1,w_1}(x)) \\
&= \sum_{x\in R^r} w_h(v_{s_2,w_2}(x)) \\
&= \sum_{x\in R^r} ((q^{s-1} - q^{s-2}) - \frac{1}{q} \sum_{r_0\in R-pR} e^{2\pi i \frac{Tr_m(r_0 v_{s_2,w_2}(x))}{p^s}} \\
&= q^{snr}(q^{s-1} - q^{s-2}) - \frac{1}{q} \sum_{x\in S^r} \sum_{r_0\in R-pR} e^{2\pi i \frac{Tr_m(r_0 v_{s_2,w_2}(x))}{p^s}} \\
&= q^{snr}(q^{s-1} - q^{s-2}) \\
&\quad -\frac{1}{q} \sum_{r_0\in R-pR} e^{2\pi i \frac{Tr_m(r_0 w_2)}{p^s}} e^{2\pi i \frac{Tr_m(r_0 s_{22})}{p^s}} \sum_{x\in S^r} e^{2\pi i \frac{Tr_{mn}(r_0 s_{02} f(x) + r_0 s_{12} x)}{p^s}}
\end{aligned}$$

de la cadena de igualdades se obtienen dos casos:

1. Si $(s_0, s_1) \neq (0,0)$, como f es t-resiliente y $x \mapsto Tr_{mn}(r s_{12} x)$ es una función balanceada, se sigue que
$$d_H(u_{s_0,w_0}, u_{s_1,w_1}) = q^{snr}(q^{s-1} - q^{s-2}).$$
2. Si $(s_0, s_1) = (0,0)$, entonces
$$d_H(u_{s_0,w_0}, u_{s_1,w_1}) = \sum_{x\in S^r} w_h(v_{s_2,w_2}(x)) = \sum_{x\in S^r} w_h(s_{22} + w_2) = q^{snr}(q^{s-1} - q^{s-2})$$
ya que $s_{22} + w_2 \in R - p^{s-1}R$.

□

Nótese que en la proposición anterior se aprecia la importacia de que los pesos de Hamming de s_{10} y s_{11} sean menores o iguales a $t/2$.

Sean $S = GR(p^s, mn)$ y $R = GR(p^s, m)$ como antes. Los siguientes resultados respecto a la traza serán de utilidad.

Lema 4.2.1. *Sean S, R y $Tr_n : S \to R$ la función traza, $n > s$. Si $r \in R$ y $x \in S$, $x \neq 0$. Entonces existe $s \in S^\times$ tal que $Tr_n(xs) = r$.*

Demostración. Expresemos $q = p^m$. Se divide la demostración en los siguientes casos:

1. Suponga que x es unidad.
Recordemos que

$$|S| = q^{sn}, y \ \ |R| = q^s,$$

luego

$$\frac{|S|}{|R|} = \frac{q^{sn}}{q^s} = q^{s(n-1)},$$

es el número de elementos en S que son preimágenes de r. Por otro lado, $|p^{s-1}S| = q^{(s-1)n}$ es el número divisores de cero de S. Por lo tanto, ya que $q^{s(n-1)} > q^{(s-1)n}$ si $n > s$, entonces existe un elemento $s' \in S^\times$ tal que $Tr_n(s') = r$, por lo que existe un elemento $s \in S^\times$ tal que $Tr_n(xs) = r$.

2. Suponga ahora que x es un divisor de cero.
Sea $r = r'p^{s-1}$. Nótese que $x = p^i x'$, $1 \leq i \leq s-1$, donde x' es unidad. Luego se tiene que $Tr_n(x) = p^i \cdot Tr_n(x')$. Por el caso anterior sabemos que existe $s \in S^\times$ tal que $Tr_n(sx') = r'p^{s-i-1}$. Entonces, $Tr_n(xs) = p^i Tr_n(sx') = r'p^{s-1} = r$.

Por los casos anteriores se concluye la prueba.

□

Corolario 4.2.1.1. *Sea $x \in S$, $x \neq 0$. Entonces existe $s \in S^\times$ tal que $Tr_n(xs) = 0$.*

Demostración. La afirmación es un caso particular de la proposición 4.2.1. □

Corolario 4.2.1.2. *Sea $x \in S$, $x \neq 0$. Entonces existe $s \in S^\times$ tal que*

$$Tr_n(xs) \in p^{s-1}R - \{0\}.$$

Demostración. La afirmación es un caso particular de la proposición 4.2.1. □

Ahora se presenta el algoritmo de un esquema general de autenticación:

Algoritmo 4 Esquema general de autenticación.

Entrada: primo p, enteros $m, n, s \in \mathbb{Z}^+$, $q = p^m$.
Salida: Mensaje del autenticador: Aceptar el mensaje o Rechazar el mensaje.

Alicia y Beto comparten la llave $k \in \mathcal{K}$;
Alicia envía el mensaje $m = (s, t)$ a Beto, con s texto en claro;
Beto recibe el mensaje $m' = (s', t')$ e inicia el proceso de autenticación;
$aut \leftarrow Autenticador(m)$; // Aplicación de la función autenticador al mensaje m
if $aut = m'$ **then**
    imprimir: Aceptar el mensaje;
else
    imprimir: Rechazar el mensaje;
end if
Eva elige una llave $k' \in \mathcal{K}$;
Eva envía el mensaje $m' = (s', t')$ a Beto e inicia el proceso de autenticación;
if $aut' = m'$ **then**
    imprimir: Aceptar el mensaje;
else
    imprimir: Rechazar el mensaje;
end if

Note que un inconviente que presenta este esquema es el hecho de que existe la posibilidad de que la llave que elija Eva (de manera aleatoria) coincida con la llave secreta de Alicia, por lo que Beto aceptará cualquier mensaje que le envíe Eva o cualquiera que mande Alicia y que altere Eva.

4.3. Esquemas propuestos

Se presentan dos esquemas, el primero de ellos es derivado del esquema elaborado en 2018, Ku, Morales y Tapia ([20]). En ese trabajo se construye un esquema de autenticación con probabilidades P_S y P_I óptimas. Sin embargo, un inconveniente es el tamaño y forma de los espacios, principalmente el espacio fuente el cual es complejo y poco práctico. Derivado de estos espacios, la prueba de biyectividad entre el espacio de llaves y las reglas de codificación, posteriormente definidas, es larga y tediosa, aproximadamente ocho hojas. Además de que el espacio fuente en este trabajo es de mayor tamaño, lo que hace una mayor diferencia respecto al espacio de llaves; por otro lado, también se simplifica su estructura lo que genera un esquema accesible y una prueba de biyectividad entre llaves y reglas de codificación relativamente sencilla. Finalmente en nuestro primer esquema también se alcanzan los valores mínimos para P_I y P_S.

El segundo esquema simplifica aún más el primero, pues se prescinde de un parámetro, el cual reduce el tamaño del espacio de llaves y mantiene el tamaño del espacio fuente, por lo que se obtiene una mejor comparación entre estos. La prueba de inyectivad es reducida a dos casos, de tres que tiene el primer esquema. Además, que la probabilidad de personificación para este esquema también alcanza su valor mínimo.

En cada uno de los esquemas, primero se analiza el caso particular con característica p^2 y posteriormente el caso general. El modo natural como se fueron obteniendo los resultados, y que además permite una mejor comprensión de estos.

4.3.1. Esquema 1: característica p^2

Derivado de los resultados hasta ahora obtenidos de la sección, se muestra un caso particular del esquema de autenticación, es decir, se considera como p^2 a la característica en los anillos de Galois S y R antes definidos.

Considérese la siguiente extensión:

$$\begin{array}{c} S = GR(p^2, mn) \\ | \\ R = GR(p^2, m) \\ | \\ \mathbb{Z}_{p^2} \end{array}$$

Sea $f : S^r \to S$ una función t-resiliente, $q-1$ un número par, $n > 2$ y

$$S_0 := S^\times \cup \{0\},\ S_1 := (S^\times \cup \{0\})^r,\ S_2 := T_R.$$

Definimos el primer esquema:

$$\mathcal{A}_2 := (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}).$$

- $\mathcal{S} := \{(s_0, s_1, s_2) \in S_0 \times S_1 \times S_2 \mid (s_0, s_1) \neq (0, \mathbf{0}), w_H(b) \leq \frac{t}{2}\}$, el espacio fuente,
- $\mathcal{T} := \mathbb{F}_q$, el espacio de etiquetas,
- $\mathcal{K} := \mathbb{Z}_{q^{2(nr+1)}}$, el espacio de llaves,
- $\mathcal{E} := (e_k)_{k\in\mathcal{K}}$, $e_k : \mathcal{S} \to \mathcal{T}$, $s \mapsto e_k(s), e_k = \pi_k(u_s)$, las reglas de codificación, π la función proyección, esto es, $\pi_k(u_s)$ es la k-ésima entrada de u_s,

donde para cada $s = (s_0, s_1, s_2) \in \mathcal{S}$ y cada $w \in pR$, se define la función

$$v_{s,w} : S^r \to R, x \mapsto v_{s,w}(x),$$

$$\begin{aligned} v_{s,w}(x) &= Tr_n(s_0 f(x) + s_1 x) + s_2 + w, \\ u_{s,w} &= (\Phi(v_{s,w}(x)))_{x \in S^r} \in (\mathbb{F}_q^q)^{q^{2nr}}, \\ u_s &= (u_{s,w})_{w \in pR} \in (\mathbb{F}_q^q)^{q^{2nr+1}} \cong \mathbb{F}_q^{q^{2(nr+1)}}. \end{aligned}$$

Note que

$$|S_0| = (q^n - 1)q^n + 1, |S_1| = [(q^n - 1)q^n + 1]^r, |S_2| = q.$$

En este esquema se desean encontrar las cotas P_I y P_S. Para esto es necesario probar algunos resultados, entre éstos, la prueba de inyectividad, la cual será dada por casos.

La función de Gray Φ para este caso adopta la forma:

$$\begin{array}{rccc} \Phi : & R & \to & \mathbb{F}_q^q \\ & a_0 + a_1 p & \mapsto & \overline{a}_0 c_0 + \overline{a}_1 c_1 \end{array},$$

donde

$$\begin{aligned} c_0 &= (0, \xi, ..., \xi^{q-1}), \\ c_1 &= (1, ..., 1). \end{aligned}$$

Teorema 4.3.1. *La función $H : \mathcal{K} \to \mathcal{E}$, dada por $H(k) = e_k$ es inyectiva.*

Demostración. La demostración del teorema será dada considerando tres casos.
Se compararán todas las coordenadas de u_s considerando la longitud de u_s por partes, para esto dividimos en los siguientes casos:

Caso 1: Considere dos coordenadas de $\Phi(v_{s,w}(x))$, con $x \in S^r$.

Si elegimos un elemento fijo $(s_0, s_1) \in S_0 \times S_1$ y aplicando el lema 2.4.1 se tiene

$$\Phi(v_{s,w}(x)) = \Phi(Tr_n(s_0 f(x) + s_1 x) + s_2 + w) = \Phi(Tr_n(s_0 f(x) + s_1 x) + s_2) + \Phi(w).$$

Note que $\overline{a}_0 c_0$ tiene todas sus entradas distintas si $\overline{a}_0 \neq 0$, $\overline{a}_1 c_1$ tiene sus entradas iguales, luego $\overline{a}_0 c_0 + \overline{a}_1 c_1$ posee todas sus entradas distintas si $\overline{a}_0 \neq 0$.

Por lo anterior, si $Tr_n(s_0 f(x) + s_1 x) = a_0 + a_1 p$, entonces existe $d_0 \in S_2$, de modo que $Tr_n(s_0 f(x) + s_1 x) + d_0 = a_0 + b_0 + a_1 p$, en donde $b_0 \neq 0$ si $a_0 = 0$ y $b_0 = 0$ si $a_0 \neq 0$.

Tomando ahora el elemento $(s_0, s_1, d_0) \in \mathcal{S}$ y aplicando la función de Gray se tiene $\Phi(Tr_n(s_0 f(x) + s_1 x) + s_2 + d_0) + \Phi(w)$ tiene todas sus coordenadas distintas. Resultado que concluye la prueba del caso 1.

Caso 2: Se elige una coordenada de $\Phi(v_{s,w}(x))$ y una de $\Phi(v_{s,w}(y))$, donde $x, y \in S$, $x \neq y$.

Denotemos como $\Phi_l(\cdot)$ la l-ésima proyección de $\Phi(\cdot)$. Consideremos como un primer subcaso la misma coordenada l en $\Phi(v_{s,w}(x))$ y en $\Phi(v_{s,w}(y))$. Supongamos también que $x_i - y_i \neq 0$, la i-ésima entrada de $x - y$.

Por el corolario 4.2.1.2, existe $s' \in S^\times$ tal que $Tr_n((x_i - y_i)s') \in pR - \{0\}$. Denotemos

$$Tr_n(x_i s') = a_0 + a_1 p \text{ y } Tr_n(y_i s') = b_0 + b_1 p,$$

entonces

$$(a_0 - b_0) + (a_1 - b_1)p \in pR - \{0\},$$

por lo que $a_0 - b_0 = 0$, $a_1 - b_1 \neq 0$. Por lo tanto $Tr_n(x_i s') \neq Tr_n(y_i s')$. Ahora, si tomamos al elemento

$$(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), 0) \in \mathcal{S},$$

con s' en la i-ésima entrada. Entonces

$$\Phi_l(v_{s,w}(x)) = \Phi_l(Tr_n(x_j s')) + \Phi_l(w) \neq \Phi_l(Tr_n(y_j s')) + \Phi_l(w) = \Phi_l(v_{s,w}(y)).$$

Como el segundo subcaso, consideremos ahora a la k-ésima entrada de $\Phi(v_{s,w}(x))$ y la t-ésima entrada de $\Phi(v_{s,w}(y))$. Por el corolario 4.2.1.2 existe $s' \in S^\times$ de modo que

$$Tr_n((x_i - y_i)s) \in pR - \{0\}.$$

Si

$$Tr_n(x_i s') = a_0 + a_1 p \text{ y } Tr_n(y_i s') = b_0 + b_1 p,$$

entonces, de forma similar al caso anterior,

$$Tr_n(x_i s') = a_0 + a_1 p \text{ y } Tr_n(y_i s') = a_0 + b_1 p,\ a_1 \neq b_1.$$

Tomando al elemento $(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), -a_0) \in \mathcal{S}$, se tiene

$$\Phi_k(v_{s,w}(x)) = \Phi_k(Tr_n(a_1 p)) + \Phi_k(w) \neq \Phi_t(Tr_n(b_1)) + \Phi_t(w) = \Phi_t(v_{s,w}(y)).$$

Nótese que si $u \in pS$, entonces $\Phi(u) = \overline{u}_1 c_1$ posee todas sus entradas iguales. Por lo tanto, se concluye la prueba de este caso.

Caso 3: Sean $w_0, w_1 \in pR$, con $w_0 \neq w_1$. Este caso se divide en: $x = y$ y $x \neq y$.

Suponga que $x = y$. Si se elige una misma coordenada para $\Phi(v_{s,w_0}(x))$ y para $\Phi(v_{s,w_1}(y))$, y como $\Phi(w_1) \neq \Phi(w_2)$, luego se tiene el resultado deseado.

Por otra parte, si se toman coordenadas distintas k y t de $\Phi_k(Tr_n(s_0 f(x) + s_1 x) + w_0)$ y $\Phi_t(Tr_n(s_0 f(y) + s_1 y) + w_1)$ respectivamente. entonces por el corolario 4.2.1.1 existe $s' \in S^\times$ tal que $Tr_n(x_i s') = 0$ (si $x_i = 0$ se tiene el mismo resultado). Si

$$Tr_n(x_i s') = Tr_n(y_i s') = a_0 + a_1 p,$$

luego, se elige al elemento $(s_0, s_1, s_2) = (0, (0, ..., s', ..,0), -a_0) \in \mathcal{S}$. Por lo que

$$\Phi_k(v_{s,w_0}(x)) = \Phi_k(a_1 p) + \Phi_k(w_0) \neq \Phi_t(a_1 p) + \Phi_t(w_1) = \Phi_t(v_{s,w_1}(y)).$$

Nótese que $-a_0 \in T_S$ ya que $q - 1$ es un número par.

Supongamos ahora que $x \neq y$ y considere coordenadas iguales, $\Phi_k(v_{s,w_0}(x))$ y $\Phi_k(v_{s,w_1}(y))$. Por el corolario 4.2.1.1 se puede elegir $s' \in S^\times$ de manera que $Tr_n((x_i - y_i)s') = 0$, es decir, $Tr_n(x_i s') = Tr_n(y_i s')$. Si elegimos al elemento

$$(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), 0) \in \mathcal{S}$$

se obtiene

$$\Phi_k(v_{s,w_0}(y)) = \Phi_k(Tr_n(sx)) + \Phi_k(w_0) \neq \Phi_k(Tr_n(sy)) + \Phi_k(w_1) = \Phi_k(v_{s,w_1}(y)).$$

Consideremos finalmente coordenadas distintas k y t en $\Phi_k(v_{s,w_0})$ y $\Phi_t(v_{s,w_1})$. Usando el corolario 4.2.1.1, se puede elegir $s' \in S^\times$ tal que $Tr_n((x_i - y_i)s') = 0$. Podemos escribir

$$Tr_n(x_i s') = Tr_n(y_i s') = a_0 + a_1 p.$$

Por lo que si tomamos el elemento $(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), -a_0) \in \mathcal{S}$ se obtiene la desigualdad,

$$\Phi(v_{s,w_0}(x)) \neq \Phi(v_{s,w_1}(y)).$$

Los casos tratados anteriormente demuestran el teorema.

□

La prueba para hallar las probabilidades P_I y P_S son similares a la tratada en [19], por lo que damos por hecho este resultado.

Teorema 4.3.2. *Sea $\mathcal{A}_2$ el esquema de autenticación propuesto. Entonces*

$$P_I = \frac{1}{q} \quad y \quad P_S = \frac{1}{q}.$$

4.3.2. Esquema 1: caso general, p^s

Aquí se considera el caso general del esquema 1 :

Sea $f : S^r \to S$ una función t-resiliente, $q-1$ un número par, $n > s$ y

$$S_0 := S^\times \cup \{0\},\ S_1 := (S^\times \cup \{0\})^r,\ S_2 := \{r_0 + r_1 + \cdots + r_{s-2}p^{s-2} \mid r_0, \ldots, r_{s-2} \in T_R\}.$$

Definimos el esquema 1, caso general:

$$\mathcal{A}_s := (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}).$$

- $\mathcal{S} := \{(s_0, s_1, s_2) \in S_0 \times S_1 \times S_2 \mid (s_0, s_1) \neq (0, \mathbf{0}), w_H(b) \leq \frac{t}{2}\}$, el espacio fuente,
- $\mathcal{T} := \mathbb{F}_q$, el espacio de etiquetas,
- $\mathcal{K} := \mathbb{Z}_{q^{s(nr+1)}}$, el espacio de llaves,
- $\mathcal{E} := (e_k)_{k\in\mathcal{K}}$, $e_k : \mathcal{S} \to \mathcal{T}$, $s \mapsto e_k(s), e_k = \pi_k(u_s)$, las reglas de codificación, π la función proyección, esto es, $\pi_k(u_s)$ es la k-ésima entrada de u_s,

donde para cada $s = (s_0, s_1, s_2) \in \mathcal{S}$ y cada $w \in p^{s-1}R$, se define la función

$$v_{s,w} : S^r \to R, x \mapsto v_{s,w}(x),$$

$$\begin{aligned} v_{s,w}(x) &= Tr_n(s_0 f(x) + s_1 x) + s_2 + w, \\ u_{s,w} &= (\Phi(v_{s,w}(x)))_{x\in S^r} \in (\mathbb{F}_q^{q^{s-1}})^{q^{snr}}, \\ u_s &= (u_{s,w})_{w\in pR} \in (\mathbb{F}_q^{q^{s-1}})^{q^{snr+1}} \cong \mathbb{F}_q^{q^{s(nr+1)}}. \end{aligned}$$

Note que

$$|S_0| = (q^n - 1)q^{(s-1)n} + 1, |S_1| = [(q^n - 1)q^{(s-1)n} + 1]^r, |S_2| = q^{s-1}.$$

En este esquema buscamos demostrar la inyectividad de la función $H : \mathcal{K} \to \mathcal{E}$ que toma más importancia que el esquema anterior ya que este es un caso general, para luego determinar cotas óptimas para las probabilidades de personificación y sustitución.

Además, como generalización del esquema anterior, si p es un número primo, $s, m, n \in \mathbb{Z}^+$, $s, m, n > 1$ y $q = p^m$. Si $n > s$, entonces

$$q^n > q^s,$$

luego tomando recíprocos y multiplicando la desigualdad por q^{sn} se tiene

$$\frac{q^{sn}}{q^s} > \frac{q^{sn}}{q^n}.$$

Ahora presentamos la demostración del teorema anterior para el caso p^s, con $s > 1$.

Teorema 4.3.3. *La función $H : \mathcal{K} \to \mathcal{E}$, dada por $H(k) = e_k$ es inyectiva.*

Demostración. Comparamos las coordenadas de u_s considerando la longitud de u_s por partes, para esto dividimos en los siguientes casos:
Caso 1: Consideramos dos coordenadas distintas de $\Phi(v_{s,w}(x))$, con $x \in S^r$.

Se toma un elemento $(s_0, s_1) \in S_0 \times S_1$ fijo. Si $a \in S_2$, entonces

$$a = a_0 + a_1 p + \cdots + a_{s-3}p^{s-3} + a_{s-2}p^{s-2},$$

y al aplicar la función de Gray se obtiene la suma de vectores

$$\Phi(a) = \overline{a}_0 c_0 + \overline{a}_1 c_1 + \cdots + \overline{a}_{s-3}c_{s-3} + \overline{a}_{s-2}c_{s-2}.$$

Sean $k, j \in \mathbb{Z}^+$, $k > j$ los enteros asociados a las entradas a comparar, por lo que tenemos los siguientes casos:

- Si $k - j$ no es un múltiplo de q, elegimos $a \in S_2$ tal que $a_{s-2} \neq 0$, por lo que las dos coordenadas de $\Phi(a)$ son diferentes.
- Si $k - j$ es un múltiplo de q de manera que $q^i \leq k - j < q^{i+1}$, $i \in \{0, 1, ..., s-2\}$, basta tomar $a \in S_2$ de modo que $a_l \neq 0$, donde $l = s - 2 - i$ y así $\Phi(a)$ tiene coordenadas diferentes.
- Si $k - j = q^{s-1}$, tomando $a \in S_2$ con $a_0 \neq 0$ se tiene que $\Phi(a)$ posee coordenadas diferentes.

Ahora, si $Tr_n(s_0 f(x) + s_1 x) = a_0 + \cdots + a_k p^k + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1}$, con $a_i \in T_R$, entonces existe $s_2 = -a_0 - a_1 p + \cdots + s'_k p^k - \cdots - a_{s-2}p^{s-2} \in S_2$ (ya que $q - 1$ es par) de modo que

$$Tr_n(s_0 f(x) + s_1 x) + s_2 = a_k pk + a_{s-1}p^{s-1} \text{ si } a_k \neq 0$$

o

$$Tr_n(s_0 f(x) + s_1 x) + s_2 = s'_k pk + a_{s-1}p^{s-1} \text{ si } a_k = 0.$$

Por lo que si $w \in p^{s-1}R$ y empleando el lema 2.4.1 se tiene

$$\Phi(Tr_n(s_0 f(x) + s_1 x) + s_2 + w) = \Phi(a_k p^k) + \Phi(a_{s-1}p^{s-1}) + \Phi(w)$$

o

$$\Phi(Tr_n(s_0 f(x) + s_1 x) + s_2 + w) = \Phi(s'_k p^k) + \Phi(a_{s-1}p^{s-1}) + \Phi(w).$$

Y debido a que $k \in \{0, ..., s-2\}$, por las observaciones al inicio del caso se obtiene el resultado deseado.

Caso 2: Considere una coordenada de $\Phi(v_{s,w}(x))$ y una de $\Phi(v_{s,w}(y))$, donde $x, y \in S$ con $x \neq y$.

Tomemos la misma coordenada k en $\Phi(v_{s,w}(x))$ y en $\Phi(v_{s,w}(y))$. Como $x-y \neq 0$, luego $x_i - y_i \neq 0$, entonces existe $s' \in S^\times$ tal que $Tr_n(s'(x_i - y_i)) \in p^{s-1}R$, y si

$$Tr_n(s'x_i) = a_0 + a_1 p + \cdots + a_{s-1}p^{s-1} \text{ y } Tr_n(s'y_i) = b_0 + b_1 p + \cdots + b_{s-1}p^{s-1},$$

entonces

$$(a_0 - b_0) + (a_1 - b_1)p + \cdots + (a_{s-1} - b_{s-1})p^{s-1} \in p^{s-1}R - \{0\},$$

por lo que $a_0 = b_0$, luego $p((a_1 - b_1) + (a_2 - b_2)p + \cdots + (a_{s-1} - b_{s-1})p^{s-2}) \in p^{s-1}R - \{0\}$, es decir, $(a_1 - b_1) + (a_2 - b_2)p + \cdots + (a_{s-1} - b_{s-1})p^{s-2} \in p^{s-2}R - \{0\}$ y en consecuencia $a_1 - b_1 = 0$. Repitiendo el proceso se tiene que $(a_{s-2} - b_{s-2}) + (a_{s-1} - b_{s-1})p \in pR - \{0\}$, por lo que $a_{s-2} - b_{s-2} = 0$, esto implica $a_{s-1} - b_{s-1} \neq 0$. De lo anterior se sigue que

$$Tr_n(s'x_i) = a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1}$$

y

$$Tr_n(s'y_i) = a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + b_{s-1}p^{s-1}.$$

Por lo tanto $\Phi(Tr_n(s'x_i)) \neq \Phi(Tr_n(s'y_i))$. Si se toma al elemento

$$(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), 0) \in \mathcal{S},$$

se tiene

$$\Phi(v_{s,w}(x)) = \Phi_k(Tr_n(xs)) + \Phi_k(w) \neq \Phi_k(Tr_n(sy)) + \Phi_k(w) = \Phi(v_{s,w}(y)).$$

Consideremos ahora a la k-ésima entrada de $\Phi(v_{s,w}(x))$ y la t-ésima entrada de $\Phi(v_{s,w}(y))$. La prueba es similar al subcaso anterior con la excepción de tomar al elemento

$$(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), s_2) \in \mathcal{S},$$

donde $s_2 = -a_0 - a_1 p - \cdots - a_{s-2}p^{s-2}$. De esta manera se tiene que

$$\Phi_k(v_{s,w}(x)) = \Phi_k(Tr_n(a_{s-1}p^{s-1})) + \Phi_k(w) \neq \Phi_t(Tr_n(b_{s-1}p^{s-1})) + \Phi_t(w) = \Phi_t(v_{s,w}(x)).$$

Caso 3: Sean $w_0, w_1 \in p^{s-1}R$, con $w_0 \neq w_1$. Este caso se divide en dos subcasos: $x = y$ y $x \neq y$.

Suponga que $x = y$. Primero se elige una coordenada de $\Phi(v_{s,w_0}(x))$ y una de $\Phi(v_{s,w_1}(y))$. Por el corolario 4.2.1.1 existe $s' \in S^\times$ tal que $Tr_n((x_i - y_i)s') = 0$, es decir,

$$Tr_n(x_i s') = Tr_n(y_i s').$$

Sea el elemento $(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), 0) \in \mathcal{S}$, luego $\Phi_k(w_0) \neq \Phi_k(w_1)$, obteniendo así el resultado deseado.

Ahora tomemos coordenadas distintas k y t de $\Phi_k(v_{s,w_0}(x))$ y $\Phi_t(v_{s,w_1}(y))$ respectivamente y denotemos

$$Tr_n(x_i s') = Tr_n(y_i s') = a_0 + a_1 p + \cdots + a_{s-2} p^{s-2} + a_{s-1} p^{s-1}.$$

Sea el elemento $(0, (0, ..., s', .., 0), -a_0 - a_1 p - \cdots - a_{s-2} p^{s-2}) \in \mathcal{S}$, entonces

$$\Phi_k(v_{s,w_0}(x)) = \Phi_k(a_{s-1} p^{s-1}) + \Phi_k(w_0) \neq \Phi_t(a_{s-1} p^{s-1}) + \Phi_t(w_1) = \Phi_t(v_{s,w_1}(x)).$$

Por otra parte, suponga que $x \neq y$ y considere coordenadas iguales de $\Phi(v_{s,w_0}(x))$ y $\Phi(v_{s,w_1}(y))$. Luego podemos tomar $s' \in S^\times$ de manera que

$$Tr_n((x_i - y_i)s') = 0,$$

esto es, $Tr_n(x_i s') = Tr_n(y_i s')$. Si se toma al elemento

$$(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), 0) \in \mathcal{S}$$

se tiene que

$$\Phi_k(v_{s,w_0}(x)) = \Phi_k(Tr_n(sx)) + \Phi_k(w_0) \neq \Phi_t(Tr_n(sy)) + \Phi_t(w_1) = \Phi_t(v_{s,w_1}(y)).$$

Finalmente considere coordenadas distintas k y t en $\Phi_k(v_{s,w_0})$ y $\Phi_t(v_{s,w_1})$. Sea $s' \in S^\times$ tal que $Tr_n(x_i s') = Tr_n(y_i s') = a_0 + a_1 p + \cdots + a_{s-1} p^{s-1}$. Si se elige al elemento

$$(s_0, s_1, s_2) = (0, (0, ..., s, ..., 0), -a_0 - a_1 p - \cdots - a_{s-2} p^{s-2}) \in \mathcal{S}$$

se obtiene $\Phi(v_{s,w_0}(x)) \neq \Phi(v_{s,w_1}(y))$.

Los casos tratados anteriormente demuestran el teorema.

□

Note que en el presente esquema el espacio $\mathcal{S}$ se encuentra formado por tres conjuntos de sencilla estructura, los cuales poseen cardinalidad ya conocidas. De esta manera obtenemos espacios simples y como consecuencia también se tiene una demostración relativamente sencilla de la inyectividad.

La prueba para hallar las probabilidades P_I y P_S son similares a la tratada en [19], por lo que damos por hecho este resultado.

Teorema 4.3.4. *Sea $\mathcal{A}_s$ el esquema de autenticación propuesto. Entonces*

$$P_I = \frac{1}{q} \quad y \quad P_S = \frac{1}{q}.$$

4.3.3. Esquema 2: característica p^2

Este esquema de autenticación, a comparación del esquema 1, prescinde del elemento w en el ideal pR. Simplificando de este modo aún más los espacios de este y la prueba de inyectividad a dos casos. Al igual que en el esquema anterior, consideramos inicialmente la característica p^2 de los anillos de Galois R y S.

Sea $f : S^r \to S$ una función t-resiliente, $q-1$ un número par, $n > 2$ y

$$S_0 := S^\times \cup \{0\},\ S_1 := (S^\times \cup \{0\})^r,\ S_2 := T_R.$$

Definimos el esquema 2, caso p^2 :

$$\mathcal{B}_2 := (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}).$$

- $\mathcal{S} := \{(s_0, s_1, s_2) \in S_0 \times S_1 \times S_2 \mid (s_0, s_1) \neq (0, \mathbf{0}), w_H(b) \leq \frac{t}{2}\}$, el espacio fuente,
- $\mathcal{T} := \mathbb{F}_q$, el espacio de etiquetas,
- $\mathcal{K} := \mathbb{Z}_{q^{2(nr+1)-1}}$, el espacio de llaves,
- $\mathcal{E} := (e_k)_{k\in\mathcal{K}}$, $e_k : \mathcal{S} \to \mathcal{T}$, $s \mapsto e_k(s), e_k = \pi_k(u_s)$, las reglas de codificación, π la función proyección, esto es, $\pi_k(u_s)$ es la k-ésima entrada de u_s,

donde para cada $s = (s_0, s_1, s_2) \in \mathcal{S}$ y cada $w \in pR$, se define la función

$$v_s : S^r \to R, x \mapsto v_s(x),$$

$$v_s(x) = Tr_n(s_0 f(x) + s_1 x) + s_2,$$

$$u_s = (\Phi(v_s(x)))_{x\in S^r} \in (\mathbb{F}_q^q)^{q^{2nr}} \cong \mathbb{F}_q^{q^{2(nr+1)-1}}.$$

Note que

$$|S_0| = (q^n - 1)q^n + 1, |S_1| = [(q^n - 1)q^n + 1]^r, |S_2| = q.$$

Además considere al elemento $u_s = (\Phi(v_s(x)))_{x\in S^r}$, donde $u_s \in \mathbb{F}_q^{q^{2(rn+1)-1}}$. Ya que este esquema suprime el ideal pR en la función v_s y como $|pR| = q$, entonces se tiene que $u_s \in \mathbb{F}_q^{q^{2(rn+1)-1}}$, es decir, se reduce el número de entradas de u_s.

La siguiente prueba de correspondencia uno a uno entre el espacio de llaves y las reglas de codificación se reduce a sólo dos casos en este esquema.

Teorema 4.3.5. *La función $H : \mathcal{K} \to \mathcal{E}$, dada por $H(k) = e_k$ es inyectiva.*

Demostración. La demostración será dada en dos casos:

Caso 1: La prueba es similar a la del teorema 4.3.1 del esquema 1, caso p^2. Considere dos coordenadas de $\Phi(v_s(x))$, con $x \in S^r$.

Si elegimos un elemento fijo $(s_0, s_1) \in S_0 \times S_1$

$$\Phi(v_s(x)) = \Phi(Tr_n(s_0 f(x) + s_1 x) + s_2) = \Phi(Tr_n(s_0 f(x) + s_1 x) + s_2).$$

Note que $\overline{a}_0 c_0$ tiene todas sus entradas distintas si $\overline{a}_0 \neq 0$, $\overline{a}_1 c_1$ tiene sus entradas iguales, luego $\overline{a}_0 c_0 + \overline{a}_1 c_1$ posee todas sus entradas distintas si $\overline{a}_0 \neq 0$.

Por lo anterior, si $Tr_n(s_0 f(x) + s_1 x) = a_0 + a_1 p$, entonces existe $d_0 \in S_2$, de modo que $Tr_n(s_0 f(x) + s_1 x) + d_0 = a_0 + b_0 + a_1 p$, en donde $b_0 \neq 0$ si $a_0 = 0$ y $b_0 = 0$ si $a_0 \neq 0$.

Tomando ahora el elemento $(s_0, s_1, d_0) \in \mathcal{S}$ y aplicando la función de Gray se sigue que $\Phi(Tr_n(s_0 f(x) + s_1 x) + s_2 + d_0)$ tiene todas sus coordenadas distintas. Resultado que concluye la prueba del caso 1.

Caso 2: Se elige una coordenada de $\Phi(v_s(x))$ y una de $\Phi(v_s(y))$, con $x, y \in S$ y $x \neq y$.

Sea $\Phi_k(\cdot)$ la k-ésima entrada de $\Phi(\cdot)$. Considere primero la misma coordenada k en $\Phi(v_s(x))$ y en $\Phi(v_s(y))$.

Por el corolario 4.2.1.2 existe $s' \in S^\times$ de modo que $Tr_n((x_i - y_i)s') \in pR - \{0\}$, donde $x_i - y_i \neq 0$. Si $Tr_n(x_i s') = a_0 + a_1 p$ y $Tr_n(y_i s') = b_0 + b_1 p$, entonces

$$(a_0 - b_0) + (a_1 - b_1)p \in pR - \{0\}.$$

Luego $a_0 - b_0 = 0$ y $a_1 - b_1 \neq 0$, así que $Tr_n(xs) \neq Tr_n(ys)$.

Si se elige $(s_0, s_1, s_2) = (0, (0, ..., s, ..., 0), 0) \in \mathcal{S}$ se tiene

$$\Phi_k(v_s(x)) = \Phi_k(Tr_n(x_j s)) \neq \Phi_k(Tr_n(y_j s)) = \Phi_k(v_s(y)).$$

Por otra parte, considérese a la k-ésima entrada de $\Phi(v_s(x))$ y la t-ésima entrada de $\Phi(v_s(y))$. El lema 4.2.1.2 garantiza la existencia de $s \in S^\times$ tal que

$$Tr_n((x_i - y_i)s') \in pR - \{0\}.$$

Si $Tr_n(x_i s') = a_0 + a_1 p$ y $Tr_n(y_i s') = b_0 + b_1 p$, entonces $a_0 - b_0 = 0$ y $a_1 - b_1 \neq 0$, esto es

$$Tr_n(x_i s') = a_0 + a_1 p \text{ y } Tr_n(x_i s') = a_0 + b_1 p,$$

y al tomar $(s_0, s_1, s_2) = (0, (0, ..., s, ..., 0), -a_0) \in \mathcal{S}$ se obtiene

$$\Phi_k(v_s(x)) = \Phi_k(a_1 p)) \neq \Phi_t(b_1 p) = \Phi_t(v_s(y)).$$

Los casos tratados demuestran el teorema.

□

Uno de los puntos más importantes en un esquema de autenticación es encontrar las cotas para las probabilidades P_I y P_S, más aún, que estas cotas sean mínimas. En el siguiente teorema P_I alcanza su valor mínimo.

Teorema 4.3.6. *Sea $\mathcal{B}_2$ el esquema de autenticación propuesto. Entonces*

$$P_I = \frac{1}{q}.$$

Demostración. Ya que la característica del anillo de Galois $R = GR(p^2, m), q = p^m$ es p^2, entonces $\Phi(a) = \overline{a}_0 c_0 + \overline{a}_1 c_1$, con $a \in R$, $a = a_0 + a_1 p$. Por ser Tr_n balanceada , conocemos el número de elementos de S^r que proyectan a cierta imagen.

Sea $t \in \mathbb{F}_q$, un elemento constante, y la expresión p-ádica $a = a_0 + a_1 p \in R$ de todos los elementos del anillo de Galois R.

1. Sea $a_0 \neq 0$ fijo. Si se consideran todos los elementos $a_1 \in T_R$, entonces se tienen q elementos del anillo de Galois R que satisfacen $\pi_k(\overline{a}_0 c_0 + \overline{a}_1 c_1) = t$, para cualquier $k \in \{1, \ldots, q\}$. Ya que $|T_R| = q$ y $|T_R - \{0\}| = q - 1$, luego se tienen $(q-1)q$ imágenes igual a t. El resultado anterior se obtiene al considerar todas las posibles combinaciones de los dos sumandos cuando a_0 es distinto de cero.

2. Si $a_0 = 0$, entonces de los q posibles elementos a_1 en T_R, sólo uno de ellos satisface $\pi_k(\overline{a}_0 c_0 + \overline{a}_1 c_1) = t$ para toda $k \in \{1, \ldots, q\}$. Nótese que los demás elementos a_1 no obtienen ninguna imagen igual a t, por tanto se tienen q imágenes adicionales igual a t. Estas imágenes se consideran como un caso independiente, por lo que se suma a la cantidad anterior. Así, se tienen q^2 imágenes igual a t al considerar todos los elementos del anillo de Galois.

Las observaciones anteriores son válidas para todos los elementos en R repetidos una sóla vez. Ya que se tienen l elementos tal que

$$|\{x \in S^r \mid Tr_n(s_0 f(x) + s_1 x) + s_2 = a_0 + a_1 p\}| = l = \frac{|S^r|}{|R|} = \frac{q^{2nr}}{q^2} = q^{2nr-2}.$$

Entonces $q^2 \cdot l = q^{2nr}$, es el número de elementos de $\mathcal{K}$ que mandan la proyección de u_s a t.

Dado que

$$P_I = \max_{(s,t)\in\mathcal{S}\times\mathcal{T}} \frac{|\{k \in \mathcal{K} |\, e_k(s) = t\}|}{|\mathcal{K}|},$$

entonces

$$P_I = \frac{q^{2nr}}{q^{2nr+1}} = \frac{1}{q}.$$

Por lo que el teorema queda demostrado.

□

4.3.4. Esquema 2: caso general, p^s

Presentamos ahora el caso general del esquema 2. Lo denotamos $\mathcal{B}_s$. El suprimir un parámetro respecto al esquema $\mathcal{A}_s$ genera un análisis más profundo del comportamiento de la función de Gray al probar el valor mínimo de la probabilidad P_I.

Sea $f : S^r \to S$ una función t-resiliente, $q-1$ un número par, $n > s$ y

$$S_0 := S^\times \cup \{0\},\ S_1 := (S^\times \cup \{0\})^r,\ S_2 := \{r_0 + r_1 + \cdots + r_{s-2}p^{s-2} \mid r_0, r_1 \ldots, r_{s-2} \in T_R\}.$$

Definimos el esquema 2, caso p^s :

$$\mathcal{B}_s := (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}).$$

- $\mathcal{S} := \{(s_0, s_1, s_2) \in S_0 \times S_1 \times S_2 \mid (s_0, s_1) \neq (0, \mathbf{0}), w_H(b) \leq \frac{t}{2}\}$, el espacio fuente,
- $\mathcal{T} := \mathbb{F}_q$, el espacio de etiquetas,
- $\mathcal{K} := \mathbb{Z}_{q^{s(nr+1)-1}}$, el espacio de llaves,
- $\mathcal{E} := (e_k)_{k\in\mathcal{K}}$, $e_k : \mathcal{S} \to \mathcal{T}$, $s \mapsto e_k(s), e_k = \pi_k(u_s)$, las reglas de codificación, π la función proyección, esto es, $\pi_k(u_s)$ es la k-ésima entrada de u_s,

donde para cada $s = (s_0, s_1, s_2) \in \mathcal{S}$ se define la función

$$v_s : S^r \to R, x \mapsto v_s(x),$$

$$v_s(x) = Tr_n(s_0 f(x) + s_1 x) + s_2,$$
$$u_s = (\Phi(v_s(x)))_{x\in S^r} \in (\mathbb{F}_q^{q^{s-1}})^{q^{snr}} \cong \mathbb{F}_q^{q^{s(nr+1)-1}}.$$

Note que

$$|S_0| = (q^n - 1)q^n + 1, |S_1| = [(q^n - 1)q^n + 1]^r, |S_2| = q^{s-1}.$$

El siguiente resultado es la generalización del teorema 4.3.5 para una característica arbitraria para lo anillos de Galois S y R definidos anteriormente.

Teorema 4.3.7. *La función $H : \mathcal{K} \to \mathcal{E}$, dada por $H(k) = e_k$ es inyectiva.*

Demostración. La demostración se divide en dos casos:

Caso 1: Comparamos dos coordenadas distintas de $\Phi(v_s(x))$, con $x \in S^r$.

Sea $(s_0, s_1) \in S_0 \times S_1$ y recordemos que si $a \in S_2$,

$$a = a_0 + a_1 p + \cdots + a_{s-3}p^{s-3} + a_{s-2}p^{s-2}$$

y

$$\Phi(a) = \overline{a}_0 c_0 + \overline{a}_1 c_1 + \cdots + \overline{a}_{s-3} c_{s-3} + \overline{a}_{s-2} c_{s-2}.$$

Sean $k, j \in \mathbb{Z}^+$ con $k > j$ las entradas a comparar,

- Si $k - j$ no es un múltiplo de q, basta elegir $a \in S_2$ con $a_{s-2} \neq 0$; así las dos coordenadas de $\Phi(a)$ son distintas.
- Si $k - j$ es un múltiplo de q con $q^i \leq k - j < q^{i+1}$, $i \in \{0, 1, ..., s-2\}$, entonces se toma $a \in S_2$ con $a_l \neq 0$, donde $l = s-2-i$. Luego $\Phi(a)$ tiene coordenadas distintas.
- Si $k-j = q^{s-1}$, entonces se elige $a \in S_2$, $a_0 \neq 0$. En este caso $\Phi(a)$ posee coordenadas diferentes.

Si $Tr_n(s_0 f(x) + s_1 x) = a_0 + \cdots + a_k p^k + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1}$, con $a_i \in T_R$, entonces existe un elemento $s_2 = -a_0 - a_1 p + \cdots + s'_k p^k - \cdots - a_{s-2}p^{s-2} \in S_2$, (ya que $p-1$ es par) tal que, si $a_k \neq 0$

$$Tr_n(s_0 f(x) + s_1 x) + s_2 = a_k pk + a_{s-1}p^{s-1},$$

y si $a_k = 0$, luego

$$Tr_n(s_0 f(x) + s_1 x) + s_2 = s'_k pk + a_{s-1}p^{s-1}.$$

De esta manera

$$\Phi(Tr_n(s_0 f(x) + s_1 x) + s_2) = \Phi(a_k p^k) + \Phi(a_{s-1}p^{s-1})$$

o

$$\Phi(Tr_n(s_0 f(x) + s_1 x) + s_2) = \Phi(s'_k p^k) + \Phi(a_{s-1}p^{s-1}).$$

Como $k \in \{0, ..., s-2\}$ y por lo discutido al inicio del caso se obtiene el resultado.

Caso 2: Consideramos una coordenada de $\Phi(v_s(x))$ y una de $\Phi(v_s(y))$, donde $x, y \in S$ con $x \neq y$.

Primero considere la misma coordenada k en $\Phi(v_s(x))$ y en $\Phi(v_s(y))$. Como $x - y \neq 0$,

por el corolario 4.2.1.2 existe $s' \in S^{\times}$ tal que $Tr_n(s'(x_i - y_i)) \in p^{s-1}R - \{0\}$, $x_i - y_i \neq 0$, y si se denota $Tr_n(s'x_i) = a_0 + a_1 p + \cdots + a_{s-1}p^{s-1}$ y $Tr_n(s'y_i) = b_0 + b_1 p + \cdots + b_{s-1}p^{s-1}$. De manera similar a las pruebas anteriores se tiene que $a_j = b_j$, $j \in \{0, ..., s-2\}$, y $a_{s-1} \neq b_{s-1}$. De este modo $\Phi(Tr_n(s'x_i)) \neq \Phi(Tr_n(s'y_i))$, luego, si se elige

$$(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), 0) \in \mathcal{S},$$

entonces se sigue que $\Phi_k(v_s(x)) \neq \Phi_k(v_s(y))$.

Considere la k-ésima entrada de $\Phi(v_s(x))$ y la t-ésima entrada de $\Phi(v_s(y))$. Del párrafo anterior se deduce que

$$Tr_n(s'x_i) = a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1}$$

y

$$Tr_n(s'y_i) = a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + b_{s-1}p^{s-1}.$$

Por lo tanto, si se elige al elemento

$$(s_0, s_1, s_2) = (0, (0, ..., s', ..., 0), -a_0 - a_1 p - \cdots - a_{s-2}p^{s-2}) \in \mathcal{S}$$

se obtiene el resultado deseado.

Los casos tratados prueban el teorema. □

Antes de calcular la probabilidad P_I, hacemos un análisis del número de entradas de la imagen de la función de Gray igual a un valor $t \in \mathbb{F}_q$ (campo correspondiente al anillo de Galois $R = GR(p^s, m)$). Este análisis se realiza considerando la forma p-ádica de los elementos del anillo de Galois R, es decir, la imagen de Gray de los elementos de la forma $a = a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1}$, donde $a \in R$. En particular se analizan los sumandos de $\Phi(a)$, donde $\Phi(a) = \overline{a}_0 c_0 + \overline{a}_1 c_1 + \cdot + \overline{a}_{s-2}c_{s-2} + \overline{a}_{s-1}c_{s-1}$.

Teorema 4.3.8. *La suma de cualquier subconjunto del conjunto de vectores* $\{c_0, c_1, \ldots, c_{s-2}\}$ *de la función de Gray es de la forma* $\left[[P\zeta_0(c'_l)]_{q^{l-r-1}}, [P\zeta_1(c'_l)]_{q^{l-r-1}}, \ldots, [P\zeta_{q-1}(c'_l)]_{q^{l-r-1}}\right]_{q^r}$, $\zeta_i \in \mathcal{T}_R$, $i = 0, \ldots, q-1$, $\zeta_0 = 0$, *en donde* c_l *y* c_r *son el último y penúltimo sumando, en orden creciente de los índices, respectivamente, y* $c'_l = \left[[0]_{q^{s-l-2}}, [\xi]_{q^{s-l-2}}, \ldots, [\xi^{q-1}]_{q^{s-l-2}}\right]$ *tal que* $P\zeta_i(c'_l) = [\zeta_i]_{q^{s-r-2}} + [c'_l]_{q^{l-r-1}}$, $i = 0, \ldots, q-1$.

Demostración. Procedamos por inducción.

Si se tienen dos sumandos:

Considere la suma de dos vectores arbitrarios: c_j y c_i, $j < i$, $j \in \{0, \ldots, s-3\}$ y $i \in \{1, \ldots, s-2\}$. Sabemos que

$$c_j = \left[[0]_{q^{s-j-2}}, [\xi]_{q^{s-j-2}}, \ldots, [\xi^{q-1}]_{q^{s-j-2}}\right]_{q^j}$$

y

$$c_i = \left[[0]_{q^{s-i-2}}, [\xi]_{q^{s-i-2}}, \ldots, [\xi^{q-1}]_{q^{s-i-2}}\right]_{q^i}.$$

Nótese que

$$c_i = \left[\left[\left[[0]_{q^{s-i-2}}, [\xi]_{q^{s-i-2}}, \ldots, [\xi^{q-1}]_{q^{s-i-2}}\right]_{q^{i-j-1}}\right]_q\right]_{q^j}.$$

Lo que nos indica que cada vector $[\zeta]_{q^{s-j-2}}$ de c_j tiene exactamente q^{i-j-1} veces la longitud del vector c_i'. De este modo si $\zeta \in \mathcal{T}_R$, luego cada suma,

$$[\zeta]_{q^{s-j-2}} + [c_i']_{q^{i-j-1}} = \left[[\zeta+0]_{q^{s-i-2}}, [\zeta+\xi]_{q^{s-i-2}}, \ldots, [\zeta+\xi^{q-1}]_{q^{s-i-2}}\right]_{q^{i-j-1}}$$

permuta los vectores de longitud q^{s-i-2} de c_i', repitiendo esta permutación de los elementos de c_i', q^{i-j-1} veces.

De todo lo anterior,

$$c_j + c_i = \left[[P0(c_i')]_{q^{i-j-1}}, [P\xi(c_i')]_{q^{i-j-1}}, \ldots, [P\xi^{q-1}(c_i')]_{q^{i-j-1}}\right]_{q^j},$$

$$P\zeta(c_i') = [\zeta]_{q^{s-j-2}} + [c_i']_{q^{i-j-1}} = \left[[\zeta+0]_{q^{s-i-2}}, [\zeta+\xi]_{q^{s-i-2}}, \ldots, [\zeta+\xi^{q-1}]_{q^{s-i-2}}\right],$$

$\zeta \in \{0, \xi, \ldots, \xi^{q-1}\}$.

Supongamos ahora que se tiene la suma de $k-1$ vectores (sumando en orden creciente respecto a los índices) del conjunto $\{c_0, c_1, \ldots, c_{s-2}\}$ de vectores de la función de Gray, en donde el penúltimo vector es r y el último es l:

Se sabe que

$$c_l = \left[\left[\left[[0]_{q^{s-l-2}}, [\xi]_{q^{s-l-2}}, \ldots, [\xi^{q-1}]_{q^{s-l-2}}\right]_{q^{l-r-1}}\right]_q\right]_{q^r}.$$

Por otro lado supongamos que

$$\cdots + c_r + c_l = \left[[P0(c_l')]_{q^{l-r-1}}, [P\zeta_1(c_l')]_{q^{l-r-1}}, \ldots, [P\zeta_{q-1}(c_l')]_{q^{l-r-1}}\right]_{q^r},$$

donde $\{0, \zeta_1, \ldots \zeta_{q-1}\} = \mathcal{T}_R$. Observe que la expresión de la suma es el resultado de aplicar las permutaciones cada vez que se realiza la suma de un vector.

Veamos que al sumar un k-ésimo vector (un vector c_v) a toda la suma anterior se tiene la misma expresión de permutación, en este caso de los vectores c'_v:

$$c_v = \left[\left[\left[[0]_{q^{s-v-2}}, [\xi]_{q^{s-v-2}}, \ldots, [\xi^{q-1}]_{q^{s-v-2}}\right]_{q^{v-r-1}}\right]_q\right]_{q^r},$$

luego

$$c_v = \left[\left[[c'_v]_{q^{v-l-1}}\right]_{q^{l-r-1}qq}\right]_{q^r}.$$

Por lo tanto al efectuar la suma $\cdots + c_r + c_l + c_v$:

$$\left[[P0(c'_l)]_{q^{l-r-1}}, [P\zeta_1(c'_l)]_{q^{l-r-1}}, \ldots, [P\zeta_{q-1}(c'_l)]_{q^{l-r-1}}\right]_{q^r} + \left[\left[[c'_v]_{q^{v-l-1}qq}\right]_{q^{l-r-1}}\right]_{q^r}.$$

De q vectores $[c'_v]$, cada uno de ellos permuta sus elementos de longitud q^{s-v-2}, q^{v-l-1} veces para cada uno de los q vectores de la forma $[\psi]_{q^{s-l-2}}$, $\psi \in \mathcal{T}_R$, de cada uno de los vectores

$$[P0(c'_l)], [P\zeta_1(c'_l)], \ldots [P\zeta_{q-1}(c'_l)].$$

Todo esto se repite $q^{l-r-1}q^r = q^{l-1}$ veces. Por lo tanto,

$$\cdots + c_r + c_l = \left[[P0(P0(c'_l))]_{q^{v-l-1}}, [P\xi(P\zeta_1(c'_l))]_{q^{v-l-1}}, \ldots, [P\xi^{q-1}(P\zeta_{q-1}(c'_l))]_{q^{v-l-1}}\right]_{q^r}.$$

De donde se tiene la prueba del teorema, por el método de inducción.

□

Corolario 4.3.8.1. *Sea $R = GR(p^s, m)$ y $c = c_0, c_1, \ldots, c_{s-2}$ los primeros $s-2$ vectores de la función de Gray. Entonces en la suma de a lo más $s-2$ de ellos se tiene que todo elemento $t \in \mathbb{F}_q$ se encuentra en q^{s-2} entradas.*

Demostración. Consideremos una suma finita tal que los vectores c_v y c_l corresponden al último y penúltimo índice en orden creciente de los sumandos respectivamente.

Por el teorema anterior, ya que el vector resultante está conformado por la permutación de los vectores $[\zeta]_{q^{s-l-2}}$ de c'_v, y c_v es igual a

$$c_v = \left[\left[[c'_v]_{q^{v-l-1}}\right]_{q^{l-r-1}qq}\right]_{q^r},$$

en donde

$$c'_v = \left[[0]_{q^{s-v-2}}, [\xi]_{q^{s-v-2}}, \ldots, [\xi^{q-1}]_{q^{s-v-2}}\right].$$

Entonces el número de entradas igual a un valor $t \in \mathbb{F}_q$ es igual a q^{s-2}, ya que cada elemento $[\zeta]_{q^{s-v-2}}$ de c'_v se repite $q^{v-l-1}q^{l-r-1}qqq^r = q^v$ veces. □

Ahora se demuestra que $\mathcal{B}_s$ tiene la probabilidad P_I mínima para el caso general que considera cualquier característica para los anillos de Galois S y R definidos anteriormente.

Teorema 4.3.9. *Sea $\mathcal{B}_s$ el esquema de autenticación propuesto. Entonces*

$$P_I = \frac{1}{q}.$$

Demostración. Por el corolario 4.3.8.1 se tiene que en la suma de a lo más $s-2$ vectores de $c = c_0, c_1, \ldots, c_{s-2}$ de la función de Gray, todo elemento $t \in \mathbb{F}_q$ se encuentra en q^{s-2} entradas. Por otro lado, si un elemento $a = a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1} \in R$, entonces $\Phi(a) = \overline{a}_0 c_0 + \overline{a}_1 c_1 + \cdots + \overline{a}_{s-2}c_{s-2} + \overline{a}_{s-1}c_{s-1} \in \mathbb{F}_q^{q^{s-1}}$. Por lo que para tener el número de imágenes $\Phi(a)$ igual a un valor $t \in \mathbb{F}_q$ para todo elemento a en R es necesario considerar los posibles valores que pueden tener los coeficientes $a_0, a_1, \ldots, a_{s-2}, a_{s-1}$:

Consideremos inicialmente las combinaciones posibles que se pueden tener para $s-1$ sumandos, sin tomar en cuenta el caso cuando $a_0 = a_1 = \cdots = a_{s-2} = 0$, y sin considerar el último sumando $\overline{a}_{s-1}$,

Nótese que se tienen $qq^{s-2} \cdot qq^{s-2} \cdot qq^{s-2} \cdot \cdots \cdot qq^{s-2} - 1 = (q^{s-1}-1) \cdot q^{s-2}$ entradas que coinciden. Se puede observar que se resta el caso cuando $\overline{a}_i = 0$, para toda $i \in \{0, \ldots, s-2\}$.

Ahora, si se considera el término $\overline{a}_{s-1}c_{s-1}$, se tienen las siguientes observaciones:

1. Si la suma de los primeros $s-1$ sumandos es distinta de cero, entonces el número de combinaciones aumenta a $(q^{s-1}-1) \cdot q^{s-2} \cdot q = (q^{s-1}-1) \cdot q^{s-1}$, ya que se tienen q elementos $\overline{a}_{s-1}$ distintos.

2. Si la suma de los primeros $s-1$ sumandos es igual a cero, entonces se tendrá únicamente el término $\overline{a}_{s-1}c_{s-1}$. Como existe $\overline{a}_{s-1} \in \mathbb{F}_q$ único tal que $\overline{a}_{s-1} = t$, entonces se tiene un vector con q^{s-1} entradas igual a t. Note que el resultado obtenido se debe sumar al del punto anterior, ya que este caso no depende de los demás sumandos, sólo de $\overline{a}_{s-1}c_{s-1}$, por lo que las combinaciones posibles son

$$(q^{s-1}-1) \cdot q^{s-1} + q^{s-1} = q^{2s-2}.$$

Lo anterior es válido para todos los elementos en R repetidos una sóla vez, y como en u_s cada elemento de R se repite $l = q^{snr-s}$ veces, luego existen $q^{snr+s-2}$ elementos en $\mathcal{K}$ que mandan la proyección de $\Phi(v_s)$ al elemento t.

De esta manera tenemos que la probabilidad de personificación es

$$P_I = \frac{|\{k \in \mathcal{K}|\ e_k(s) = t\}|}{|\mathcal{K}|} = \frac{q^{snr+s-2}}{q^{srn+s-1}} = \frac{1}{q}.$$

□

Resultados

1. Se obtuvieron un par de algoritmos para encontrar polinomios mónicos básicos primitivos.

   El primero encuentra todos los polinomios mónicos básicos primitivos de grado m en $\mathbb{Z}_{p^s}$, para un valor s dado. Para ésto, utiliza su defínción, es decir, analiza si cada polinomio dado tiene un elemento primitivo en el anillo de Galois $GR(p^s, m)$ sobre $\mathbb{Z}_{p^s}$. El segundo algoritmo, dado un polinomio mónico primitivo sobre $\mathbb{F}_{p^m}$, y dado un entero positivo s, encuentran todos los levantamientos de Hensel, los cuales son polinomios mónicos básicos primitivos sobre $\mathbb{Z}_{p^{s'}}$ para cada $s' \leq s$.

2. Ya obtenido un polinomio mónico básico primitivo, un tercer algoritmo encuentra los elementos del anillo de Galois correspondiente.

3. Tablas de los polinomios obtenidos.

4. Se tiene la implementación de un esquema general de autenticación sin secreto sobre campos finitos: se simula a Alicia mandando un mensaje (el cual consta de un texto en claro y una etiqueta de autenticación) a Beto, En este caso, Beto al corroborar el mensaje lo acepta como auténtico. Por otro lado, un adversario, Eva, inserta un mensaje en el canal de comunicación, texto en claro distinto al de Alicia. Al pasar por el proceso de autenticación, Beto rechaza el mensaje. Se considera un campo base $\mathbb{F}_q$, $q = p^m$, y una extensión de grado n, teniendo así el campo $\mathbb{F}_{q^n}$ en la punta de la torre.

5. Se obtuvieron dos esquemas de autenticación.

   El primero de ellos, simplifica el espacio fuente del esquema propuesto por Ku, Morales y Tapia ([21]). Obteniendo de este modo más elementos en el espacio fuente en nuestro esquema. La forma del espacio y propiedades de la traza permitieron una prueba relativamente sencilla y más corta de la correspondencia uno a uno entre el espacio de llaves y las reglas de codificación del esquema. En este esquema se obtuvieron los valores mínimos para P_I y P_S.

   El segundo esquema reduce q veces el tamaño del espacio de llaves respecto al primer esquema y mantiene el tamaño del espacio fuente, obteniendo de esta manera una

mayor diferencia entre estos espacios. En este esquema es de recalcar la importancia del análisis del comportamiento de las imágenes de la función de Gray, desde el punto de vista de los sumandos que componen la forma de sus imágenes. Este análisis fue finalmente importante para la obtención del valor mínimo en la cota P_I de este esquema.

Todos los algoritmos fueron implementados en la plataforma SageMath. El lector que lo desee consultar los archivos de los algoritmos empleados en este trabajo puede hacerlo consultando la página:

https://drive.google.com/drive/folders/1XvUcdfTjS9Kfd02z$_V bkT1-RICz5iYoL?usp = sharing$

Conclusiones

En este trabajo se estudiaron los anillos de Galois, estructuras algebraicas que pueden ser generadas por polinomios mónicos básicos irreducibles y polinomios básicos primitivos. Nosotros nos enfocamos en estudiar estos últimos, ya que generan al conjunto de Teichmüller, el cual a su vez permite dotar a los elementos de un anillo de su expresión p-ádica, lo que hace posible emplear la función de Gray. Al estudiar estos polinomios básicos primitivos, estudiamos la estructura de los anillos de Galois.

Por otro lado, la función de Gray nos genera un puente entre los anillos de Galois y los campos finitos correspondientes. Siendo una relación, la isometría entre la distancia homogénea sobre los anillos y la distancia de Hamming sobre los campos correspondientes. En nuestro caso, respecto a los esquemas, nos permitió tener elementos del espacio fuente sobre un anillo de Galois, y las etiquetas de los esquemas sobre un campo finito.

Los esquemas aquí tratados simplificaron operaciones respecto al esquema tratado por Ku, Morales y Tapia, manteniendo las probabilidades de P_I y P_S mínimas, para el caso del primer esquema, y para el segundo únicamente se determinó el valor mínimo de la cota de la probabilidad de personificación. Además de que se hizo un análisis más profundo de la función de Gray.

En conclusión, a pesar de que los anillos de Galois han sido estudiados desde el siglo pasado, desde hace algunas décadas han resultado ser de gran utilidad en el área de la criptografía, en este caso, en esquemas de autenticación, por lo que se considera necesario continuar con el estudio de éstos.

Trabajo a futuro

1. Generalizar el algoritmo de Hensel para polinomios básicos primitivos de cualquier grado.

2. Algoritmo que permita encontrar polinomios mónicos básicos primitivos sobre anillos de Galois $GR(p^s, m)$, $m > 1$, es decir sobre extensiones de $\mathbb{Z}_{p^s}$, utilizando el lema de Hensel.

3. Obtener una fórmula para determinar la forma p-ádica de un elemento de un anillo de Galois, dada la expresión aditiva de ésta.

4. Determinar el valor mínimo de la cota de la probabilidad de personificación para el esquema 2.

5. Construir un esquema, utilizando las funciones aquí tratadas, para la elaboración de esquemas de autenticación *con secreto*.

Bibliografía

[1] Bini, G. and Flamini, F. *Finite Commutative Rings and Their Applications.* Editorial Springer, 2002.

[2] Canard, S., *et al. Guide to pairing-based cryptography.* CRC Press. Boca Raton, FL. 2017.

[3] Carlet, C., $\mathbb{Z}_{2^k}$*-linear codes*, IEEE Transactions on Information Theory, vol. 44, pp. 1543-1547, July 1999.

[4] Carlet, C., *More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings.* EUROCRYPT; Fumy, W., Ed. Springer, Berlin/Heidelberg, Germany. 1997. Volume 1233, pp. 422-433.

[5] Carlet, C., Ding, C., Niederreiter, H., *Authentication Schemes from Highly Nonlinear Functions.* Des. Codes Cryptogr., 2006, 40, 71-79.

[6] Carlet, C., Ku-Cauich, J. C., Tapia-Recillas, H., *Bent functions on a Galois ring and systematic authentication codes.* Adv. Math. Commun. 2012, 6, 249-258.

[7] Chaipunya, P., *et al. New methods of construction of cartesian authentication codes from geometries over finite commutative rings.* J. Math. Cryptol. 2018, 12, pp. 119-136.

[8] Chor, B., Goldreich, O. Hastad, J., Friedman, J., Rudich, S., Smolensky, R., *The Bit Extraction Problem of t-Resilient Functions (Preliminary version).* In Proceedings of the 26th Annual Symposium on Foundations of Computer Science, Portland, OR, USA, 21-23 October 1985; pp. 396-407.

[9] Constantinescu, I., *Lineare Codes über Restklassenringen ganzar Zahlen und ihre Automorphismen bezüglich einer verallgemeinerten Hamming-Metrik*, Ph.D. dissertation, Tech. Univ. münchen, München, Germany, 1995.

[10] Constantinescu, I. and Heise, W., *A metric for codes over residue class rings of integers*, Probl. Pered. Inform, vol. 33, n. 3, pp. 22-28, 1997.

[11] Ding, C., Niederreiter, H., *Systematic authentication codes from highly non-linear functions.* IEEE Trans. Inf. Theory, 2004, 50 , 2421-2428.

[12] Ding, C., Wang, X., *A coding theory construction of new systematic authentication codes.* Theoretical Computer Science 330, 2005. pp. 81-99.

[13] Dummit, D., Foote, R., *Abstract Algebra*. Editorial John Wiley and Sons, 2008.

[14] Greferath, M. and Schmidt, S. E., *Gray isometries for finite chain rings and non-linear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Transactions on Information Theory, vol. 45, n. 7, 1999, pp. 2522-2524.

[15] Hammons, A. R., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The 4 -linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, vol. 40, pp. 301–319, 1994.

[16] Heise, W. and Nechaev, A., *Weighted modules and representations of codes*,in Proc. ACCT 6 Inform, pp. 123-129, 1998.

[17] Ku-Cauich, J. C. and Morales-Luna G., *Authentication codes based on resilient Boolean maps.* Des. Codes Cryptogr. 2015, 1-15, doi: 10.1007/s10623-015-0121-3.

[18] Ku-Cauich, J. C. and Morales-Luna G., *Conversion of element representations in Galois rings* Aceptado a ser publicado en el Mathematics in Computer Science, Springer.

[19] Ku-Cauich, J. C. and Tapia-Recillas, H., *Systematic Authentication Codes Based on a Class of Bent Functions and the Gray Map on a Galois Ring*, SIAM, J. Discrete Math, vol 27, No. 2, 2013, pp. 1159-1170.

[20] Ku-Cauich, J. C., Morales-Luna, G. and Tapia-Recillas, H., *An Authentication Code over Galois Rings with Optimal Impersonation and Substitution Probabilities*. Mathematical and Computational Applications, vol. 23, n. 46, 2018.

[21] Ku-Cauich, J. C., Morales-Luna, G. and Tapia-Recillas, H., *Proof of Correspondence between Keys and Encoding Maps in an Authentication Code.* Technical Report. arxiv 2017, arXiv: 1703.08147.

[22] Hanan, A. *The Structure of Chain Rings* . King Saud University. Recuperado en
http://citeseerx.ist.psu.edu/viewdoc/download?
doi=10.1.1.624.1297& rep=rep1& type=pdf

[23] Hoffstein, J., Pipher, J., Silverman, J., *An Introduction to Mathematical Cryptography.* Editorial Springer, 2008, pp. 81-90.

[24] Hungerford, T., *Algebra.* Editorial Springer, 1974.

[25] Katz, J., Lindell Y., *Introduction to Modern Cryptography.* Taylor and Francis Group, 2006.

[26] Editado por Lamb, J. D. and Preece, D. A. *Surveys in Combinatorics.*, Cambridge University Press, 1999.

[27] Lang, S., *Algebra.* Editorial Springer, 2002,

[28] Lidl, R., Niederreiter, H. *Encyclopedia of Mathematics and its Applications.* Cambrigde University Prees, 1996.

[29] Lipschutz, S., *Álgebra Lineal.* Editorial John Wiley, 1991, pp. 105-108, 331-333.

[30] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes.* North-Holland Publishing Company, 1977.

[31] McDonald, B., *Finite Rings with Identity.* Pure and Applied Mathematics Series, Marcel Dekker Incorporated. New York, USA, 1974.

[32] Özbudak, F. and Saygi, Z., *Some constructions of systematic authentication codes using Galois rings*, Designs, Codes and Cryptography, vol. 41, no. 3, 2006, pp. 343-357.

[33] Rincón, H. A, *Álgebra lineal.* Editorial UNAM, 2001.

[34] Roman, S., *Coding and information theory.* Graduate texts in mathematics. Ed. Springer. California, USA. 1992.

[35] Rueppel, R., *Analysis and Design of Stream Ciphers.* Springer, Berlin, Germany, 1986.

[36] Stinson, D.R., *Combinatorial characterizations of authentication codes.* Des. Codes Cryptogr. 1992, 2, pp. 175-187.

[37] Stinson, D.R., *Cryptography: theory and practice.* CRC Press, Boca Raton, FL.

[38] V. Uspensky, *Theory of Equations.* New York, Mc Graw Hill, 1948.

[39] Von zur Gathen, J. and Gerhard, J., *Modern Computer Algebra.* Cambridge University Press, 2013.

[40] Wan, Zhe-Xian, *Lectures on Finite Fields and Galois Rings.* World Scientific Publishing Co. Pte. Ltd., 2003.