Para:
Mis Papas y Lety

Luchaba, pues, contra una dificultad insuperable;
mi cerebro echaba fuego, mi vista se obscurecía
de tanto mirar el papel; las ciento treinta y dos letras
parecían revolotear en torno mío...

cuando, en una de estas rápidas vueltas,
en el momento de quedar el reverso ante mis ojos,
creí ver aparecer palabras perfectamente latinas...

Súbitamente se presentó la claridad en mi espíritu:
acababa de descubrir la clave del enigma.

Julio Verne.

UNIVERSIDAD AUTÓNOMA METROPOLITANA-Iztapalapa

Departamento de Matemáticas

Criptografía de Curvas Hiperelípticas bajo el esquema IBE

Presenta
L.M.A. Oziel Martínez Delgado

Asesor de tesis
Dr. Horacio Tapia Recillas

Agradecimientos

A Dios, por haberme permitido alcanzar una meta más.

A mi familia, a mi papá, por su apoyo y consejos en cada momento, a mi mamá, por su cariño y sus palabras de aliento que me permitieron seguir adelante, a mi abuelita, por sus oraciones, a Ana Lilia por su plática y compañía, a Víctor por impulsarme con su ejemplo a conseguir las metas, a Gerardo, por los retos que me marca y sus observaciones, a Lety, por su amor, su comprensión, el tiempo compartido en este trabajo, y por ser Lety.

A mi familia adoptiva, a la Sra. Olivia y el Sr. Raúl, por convertirse en mi familia, por estar al pendiente de mí, por compartir sus alegrías y alejar de mí la soledad. A la Sra. Leticia, el Sr. Roberto y a Pily, por haberme aceptado en su familia, por sus deseos y darme un motivo más para terminar de este trabajo.

A mis Amigos, Rocío, Víctor, Alejandro, Ismael, Polo y Reynaldo, por hacer más fáciles los momentos de trabajo y tensión, por compartir los ideales, y por multiplicar los momentos de esparcimiento. A Sol, Rosa, Janeth, Perla, Tere, Hugo, Juan Carlos, Héctor y Cosme, por su amistad. A Georgina, Orizel, Juan Eduardo y Edgar, por impulsarme para lograr este objetivo y estar siempre presentes.

A mis Sinodales, por todo el tiempo dedicado a este trabajo, por sus observaciones y preguntas que lo enriquecieron.

A mis Maestros, al Dr. Horacio, por la exigencia impuesta, por las palabras de aliento, por compartir su conocimiento, por guiarme, por sus enseñanzas, por el tiempo dedicado. A todos y cada uno de los maestros que de alguna forma han colaborado en mi formación.

Al posgrado de la UAM, por la oportunidad brindada, a todos quienes hicieron posible este sueño, en especial a la Dra. Shirley, a la universidad y al CONACYT por el apoyo económico para realizar el posgrado.

Agradecimientos

A Dios, por haberme permitido alcanzar una meta más.

A mi familia, a mi papá, por su apoyo y consejos en cada momento, a mi mamá, por su cariño y sus palabras de aliento que me permitieron seguir adelante, a mi abuelita, por sus oraciones, a Ana Lilia por su plática y compañía, a Víctor por impulsarme con su ejemplo a conseguir las metas, a Gerardo, por los retos que me marca y sus observaciones, a Lety, por su amor, su comprensión, el tiempo compartido en este trabajo, y por ser Lety.

A mi familia adoptiva, a la Sra. Olivia y el Sr. Raúl, por convertirse en mi familia, por estar al pendiente de mí, por compartir sus alegrías y alejar de mí la soledad. A la Sra. Leticia, el Sr. Roberto y a Pily, por haberme aceptado en su familia, por sus deseos y darme un motivo más para terminar de este trabajo.

A mis Amigos, Rocío, Víctor, Alejandro, Ismael, Polo y Reynaldo, por hacer más fáciles los momentos de trabajo y tensión, por compartir los ideales, y por multiplicar los momentos de esparcimiento. A Sol, Rosa, Janeth, Perla, Tere, Hugo, Juan Carlos, Héctor y Cosme, por su amistad. A Georgina, Orizel, Juan Eduardo y Edgar, por impulsarme para lograr este objetivo y estar siempre presentes.

A mis Sinodales, por todo el tiempo dedicado a este trabajo, por sus observaciones y preguntas que lo enriquecieron.

A mis Maestros, al Dr. Horacio, por la exigencia impuesta, por las palabras de aliento, por compartir su conocimiento, por guiarme, por sus enseñanzas, por el tiempo dedicado. A todos y cada uno de los maestros que de alguna forma han colaborado en mi formación.

Al posgrado de la UAM, por la oportunidad brindada, a todos quienes hicieron posible este sueño, en especial a la Dra. Shirley, a la universidad y al CONACYT por el apoyo económico para realizar el posgrado.

Notación

$\overline{\mathbb{K}}$	Cerradura del campo $\mathbb{K}$.
$\mathbb{F}_q$	Campo con q elementos.
$\mathbf{A}_2(\mathbb{K})$	Plano afín sobre $\mathbb{K}$.
$\mathbf{P}_2(\mathbb{K})$	Plano proyectivo sobre $\mathbb{K}$.
$\mathbb{K}[x_1, x_2, ..., x_n]$	Polinomios de n variables sobre $\mathbb{K}$.
$sing(C)$	Conjunto de puntos singulares en C.
P_∞	Punto al infinito de una curva.
$\mathbb{K}[C]$	Anillo de polinomios $\frac{\mathbb{K}[x,y]}{\langle R \rangle}$.
$E(\mathbb{K})$	Conjunto (grupo) de los puntos racionales de la curva E sobre el campo $\mathbb{K}$.
$\widetilde{P}$	El punto opuesto a P.
$\overline{G}$	El conjugado de la función racional G.
$N(G)$	Norma de la función racional G.
$gr(G)$	Grado de G.
$ord_P(G)$	Orden de la función G en el punto P.
$Div(C)$	Conjunto (grupo) de divisores de C.
$supp(D)$	Soporte del D.
$deg(D)$	Grado del divisor D.
$Div^0(C)$	Conjunto (grupo) de divisores de grado 0 en C.
$div(F)$	Divisor asociado a la función F.
$\mathcal{J}(C)$	El jacobiano de C.
$gr_u(F)$	Grado de u en F.
$\mathbb{P}$	Conjunto (grupo) de divisores principales.
$\bigoplus$	Suma binaria entrada a entrada.
$\bigoplus$	Suma directa.
$\widetilde{\mathcal{M}}$	Matrices de 8×8 sobre $\mathbb{F}_{2^8}$
$O(\mathbb{G})$	Orden del grupo $\mathbb{G}$.
$o(P)$	Orden del punto P.
μ_m	Grupo de las raíces m-ésimas de la unidad.
$E[m]$	El m-ésimo grupo de torsión sobre E.
τ	Automorfismo de Frobenius sobre $\mathbb{F}_p$ $(\tau(x,y) = x^p, y^p)$.
$\|p\|_2$	longitud de la representación binaria de p.
$C : v^2 + h(u)v = f(u)$	Forma general de una curva hiperelíptica.

Índice general

Introducción

El manejo de la información de forma segura siempre ha sido indispensable y más cuando esta es confidencial, con la modernización y el uso masivo de las comunicaciones es importante tener medios para garantizar el buen uso de la información. La palabra *criptografía*, proviene del griego "*kryptos*" **esconder** y "*graphein*" **escritura**, es decir, la criptografía establece mecanismos para transformar los datos de tal manera que no se logre recuperar la información original, salvo que se cuente con los datos para recuperar la información.

La criptografía tomó un gran impulso con el creciente uso de las computadoras a principios de los años 70's, ya que estas permitieron realizar cálculos rápidamente. La búsqueda de esquemas de cifrados prácticos para poder comunicarse de forma segura se hizo patente y en el año 1973 el NIST (National Institute of Standards and Technology) de EUA, lanzó una convocatoria a nivel mundial para crear un estándar, al esquema ganador se le llamó "DES"(Data Encryption Standard)[**1**],[**10**],[**11**].

Si una entidad envía un mensaje transformado o cifrado, es necesario que la otra entidad sea capaz de descifrarlo, es decir, recuperar el mensaje original, de forma sencilla conociendo la llave secreta y no se debe de poder recuperar el mensaje sin esta, pues de lo contrario perdería sentido. El proceso de cifrar la información y de crear las llaves, se le conoce como esquema de cifrado ó criptosistema ó esquema criptográfico.

La idea general de los esquemas criptográficos se presenta en la fig. (1) en donde la entidad A usa algún algoritmo, junto con una llave para cifrar el mensaje el cual se envía a través de un canal convencional, probablemente inseguro, y llega a la entidad B que le aplica un algoritmo y su llave para recuperar el mensaje original; cuando las dos llaves K_a y K_b son iguales se dice que el cifrado es *simétrico* o de

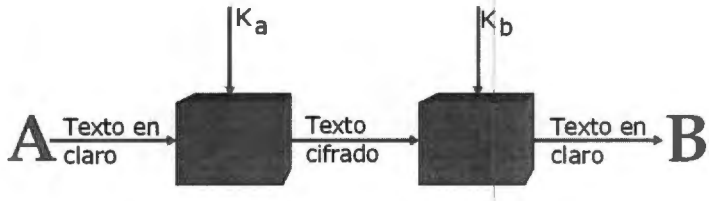

FIGURA 1. Esquema básico de los esquemas de Cifrado

llave privada, y cuando son diferentes se le llama *asimétrico* o de llave pública.

Existen diversos esquemas de cifrado asimétrico entre los que destacan el creado por Ronald Rivest, Adi Shamir y Leonard Adleman [**10**], llamado RSA que fue el primero en su género y ha permanecido como uno de mayor uso, este se basa en el problema de la factorización entera. En tanto el esquema ElGamal propuesto en 1984 por Taher ElGamal [**14**], se basa en el problema del logaritmo discreto (PLD).

El uso de curvas algebraicas en criptografía se da de forma importante en 1986 cuando de manera independiente Victor Miller y Neal Koblitz presentaron sus trabajos [**32**], [**21**], sobre el uso de curvas elípticas en criptografía, con lo cual se despertó un gran interés. La principal motivación fue el hecho de que el orden del campo, requerido para trabajar usando el grupo de puntos racionales de una curva elíptica, es considerablemente menor al del campo utilizado en los grupos tradicionales.

Al mismo tiempo en 1984 Adi Shamir propone el concepto IBE ("Identity Based Encryption") [**37**], que es un tipo de crifrado de llave pública, pero es hasta el año 2001 que se le da un fuerte impulso debido a las propuestas de Dan Boneh y Matt Franklin [**3**], [**9**]. Estos autores además de rescatar el concepto IBE, utilizan los problemas Diffie-Hellman y los mapeos bilineales no degenerados.

Un tipo importante de funciones en criptografía, son las llamadas funciones *hash*. Estas tienen la propiedad de que sin importar la longitud del dato a evaluar, esta siempre da como resultado una cadena de longitud fija. Uno de los usos de estas funciones se encuentra en los esquemas de firma digital y en algunos esquemas de cifrado, aunque también estas son usadas en bases de datos y en búsquedas [**10**], [**6**], [**7**].

Cuando comenzaron los ataques a la criptografía de curvas elípticas se estudió ¿cómo resolver el PLD en el grupo de puntos racionales de una curva elíptica?, esto se logró parcialmente en 1991 cuando Menezes, Okamoto y Vanstone [**27**], presentaron el algoritmo conocido como MOV, en el que se reduce el PLD sobre curvas elípticas supersingulares al PLD sobre campos finitos, en los cuales es más fácil resolver el problema, por lo que este tipo de curvas fueron alejadas del ámbito criptográfico [**16**], [**23**], [**28**].

Al año siguiente, Neal Koblitz [**23**], describe las curvas no-supersingulares apropiadas para el uso del esquema ElGamal, sobre campos de característica 2. A estas curvas las llamó curvas anómalas, las cuales ahora son conocidas como *curvas de Koblitz*, y actualmente son utilizadas para aplicaciones criptográficas.

Una década después de la aparición del MOV, el cual utiliza como principal herramienta el mapeo de Weil, las curvas supersingulares regresan al escenario criptográfico, ya que en los puntos racionales de estas curvas se puede evaluar fácilmente el mapeo de Weil y a que Dan Boneh y Matt Franklin recuperaron el esquema propuesto originalmente por Adi Shamir en 1984, usando como fortaleza del algoritmo presentado la intratabilidad computacional del problema bilineal Diffie-Hellman [**6**], [**9**], [**34**].

De esta forma, en los esquemas criptográficos que se adaptan para curvas hiperelípticas, en este trabajo, se deben tener en cuenta tres aspectos importantes, el esquema IBE, los problemas Diffie-Hellman, y los mapeos bilineales no degenerados, [**3**],[**34**]. Las curvas elípticas son un caso particular de las curvas hiperelípticas: curvas hiperelípticas de género 1. Mientras aumenta el género de la curva, el orden del campo sobre el cual se requiere trabajar es menor; sin embargo al aumentar el género de la curva hiperelíptica, la aritmética en la jacobiana de esta puede complicarse.

El esquema IBE se considera una variante de los esquemas de llave pública, cuya diferencia es que en este existe una autoridad la cual se encarga de asignar las llaves y proteger la llave maestra del sistema, es decir, el funcionamiento general de estos esquemas es igual al de llave pública sólo que existe otro par de "llaves"generales. [**3**], [**9**].

Los problemas Diffie-Hellman, los cuales se definen sobre dos grupos finitos conmutativos, son quienes dan la fortaleza a estos esquemas;

y son de cierta forma equivalentes al PLD. Estos problemas son: el computacional, el de decisión, el gap y el bilineal. En este último se requiere de un mapeo bilineal no degenerado, adicionalmente existe un co-problema por cada uno de estos, para los cuales se necesita un grupo más [3], [8], [34].

Los mapeos bilineales no degenerados, más conocidos en la teoría de curvas algebraicas, son el de Weil y el de Tate, y recientemente se han creado el mapeo Eta y el Ate, los cuales provienen del mapeo de Tate. Todos estos mapeos esencialmente se definen sobre subgrupos del *m-ésimo* grupo de torsión de los puntos racionales de una curva elíptica al grupo de las raíces *m-ésimas* de la unidad. Estos mapeos son definidos tradicionalmente sobre curvas elípticas, veremos como usarlo en curvas de género mayor para aplicar los esquema IBE, y se darán algunos ejemplos con grupos de orden pequeño.

El objetivo principal de este trabajo es extender, al caso de las curvas hiperelípticas, las ideas de la criptografía basada en el IBE ya que hasta el momento el esquema IBE se ha trabajado principalmente utilizando curvas elípticas. Así mismo, se pretende dar un panorama general de los elementos que la rodean y que históricamente condujeron a este tipo de esquemas.

El uso de curvas elípticas en criptografía, se debe principalmente al hecho de que se puede trabajar en un campo de cardinalidad "pequeña", pero con un grupo de orden mayor. Las curvas hiperelípticas generalizan a las curvas elípticas, pero además es posible definir grupos de orden mayor, conforme se aumenta el género de la curva. El problema a abordar será el uso de curvas hiperelípticas en los esquemas IBE, justificado en el uso de campos "pequeños."

El presente trabajo está estructurado de la siguiente manera. En el primer capítulo, se presentan conceptos básicos sobre las curvas elípticas y las curvas hiperelípticas como una generalización de las primeras. Así mismo se muestra la necesidad de definir la jacobiana para obtener la estructura de grupo deseada, la cual se utiliza en los siguientes capítulos [15], [24], [40].

En el capítulo 2, se presentan algunas funciones hash utilizadas en criptografía, después se describen los sistemas de llave pública de mayor uso, el RSA y el ElGamal, así como la firma digital propuesta

por Taher ElGamal. Finalmente se descirba el cifrado ElGamal para curvas elípticas y los problemas que surgen al implementar este [**10**], [**21**], [**14**].

El capítulo 3 aborda algunas consecuencias del desarrollo de la criptografía de curvas elípticas. Se presentan diversos métodos para resolver el PLD, los tradicionales y las ideas utilizadas por Menezes, Okamoto y Vanstone en la reducción del PLDCE al PLDCF, lo cual propició el uso de curvas no-supersingulares [**27**]. Se habla de las curvas de Koblitz que surgen en la búsqueda de curvas elípticas con buenas propiedades criptograficas [**23**]. Finalmente, se presenta el enfoque de la criptografía basada en el IBE, [**34**] presentando el primer trabajo en esta dirección el esquema de cifrado Boneh-Franklin, así como el cifrado Boneh-Boyen y de firma digital Boneh-Boyen que son más sencillos en su implementación [**6**], [**8**], [**7**], por el tipo de operaciones que se requieren.

En el capítulo final se presentan los principales elementos del IBE, como lo son los problemas Diffie-Hellman, los mapeos bilineales de Weil y Tate, que se definen sobre la jacobiana de una curva hiperelíptica. Posteriormente, se dan algunos resultados que relacionan los mapeos bilineales y las curvas hiperelípticas. Finalmente, se presenta un ejemplo donde se aplica la generalización de los mapeos a la jacobiana de un curva hiperelíptica.

Capítulo 1

Curvas hiperelípticas

Las curvas elípticas son curvas algebraicas con ciertas características que permiten darles estructuras de grupo. Su uso en criptografía se debe a que la longitud del campo con el que se trabaja se reduce. Estos grupos son utilizados en esquemas criptográficos basados en la estructura de grupo como lo son el ElGamal ó el Boneh-Franklin, entre otros. La generalización de las curvas elípticas son las curvas hiperelípticas. La jacobiana de estas ha sido utilizada en criptografía en esquemas como el ElGamal; sin embargo, el desarrollo para su uso en esquemas IBE no ha sido explotado. Para el desarrollo de esto se parte del conocimiento de conceptos básicos de campos finitos.

1.1. Curvas algebraicas

En esta sección se abordan conceptos generales sobre curvas algebraicas. Para mayores detalles se puede consultar [**15**], [**29**]. Los campos que se utilizarán son campos finitos. $\mathbb{F}_q$ es un campo con q elementos donde $q = p^r$, p es un número primo y r un entero.

Definición 1.1. *Sea* $\mathbb{K}$ *un campo y* $\boldsymbol{A}_2(\mathbb{K})$ *el plano afín sobre* $\mathbb{K}$. *Una curva algebraica plana afín definida por* $F(x,y) \in \mathbb{K}[x,y]$ *es:*

$$C_F = \{(x,y) \in \boldsymbol{A}_2(\mathbb{K}) : F(x,y) = 0\}. \tag{1}$$

De igual forma, una *curva algebraica proyectiva* C_{F^H}, se define como el conjunto solución de $F^H(x : y : z) = 0$ sobre el plano proyectivo $\mathbf{P}_2(\mathbb{K})$, donde F^H es la función homogeneizada de F.

Definición 1.2. *Punto Singular.*

Un punto $P = (a : b : c)$ $((a,b))$ *de la curva algebraica proyectiva (afín) definida por* $F \in \mathbb{K}[x,y,z](\mathbb{K}[x,y])$ *se llama singular si todas las derivadas parciales de* F *se anulan simultáneamente.*

Al conjunto de los puntos singulares de una curva algebraica C se le denota como $sing(C)$. Una curva algebraica se dice singular si $sing(C) \neq \emptyset$ y se denomina no-singular si $sing(C) = \emptyset$. Las curvas

utilizadas en este trabajo son las no singulares, ya que satisfacen las propiedades adecuadas como se muestra más adelante. Además, las curvas que se utilizan tienen un sólo punto al infinito, es decir, un punto proyectivo de la forma $(a : b : 0)$ el cual se denotará como P_∞.

1.1.1. Funciones racionales

Un aspecto esencial, en el estudio de curvas algebraicas es el siguiente anillo. Sea $\mathbb{K}$ un campo y sea $R(x, y)$ en $\mathbb{K}[x, y]$ tal que $C : R(x, y) = 0$ es una curva no singular. El anillo de polinomios de C es:

$$\mathbb{K}[C] = \mathbb{K}[x, y]/\langle R \rangle \tag{2}$$

El campo de cocientes existe ya que la curva es no singular. Similarmente se define $\overline{\mathbb{K}}[C]$ y $\overline{\mathbb{K}}(C)$, donde $\overline{\mathbb{K}}$ es la cerradura algebraica de $\mathbb{K}$. Los elementos de $\overline{\mathbb{K}}(C)$ son denominados *funciones racionales.*

Sea f una función racional no cero en $\overline{\mathbb{K}}(C)$ y $P \in C \setminus \{P_\infty\}$. Si f se puede representar de la forma $f = \frac{g}{h}$ donde $g, h \in \overline{\mathbb{K}}[C]$ y $h(P) \neq 0$ se dice que f está bien definida en el punto P.

Si f no está bien definida en P se dice que f tiene un polo en P, en tal caso se denotará como $f(P) = \infty$. Si $f(P) = 0$ se dice que f tiene un cero en P. Otra forma de expresar este concepto es la siguiente: dado $P \in \mathbb{K}(C)$ y $f \in \mathbb{K}[C]$ se puede determinar una representación para f de la forma $f = \frac{g}{h}$ tal que $g(P) \neq 0$ ó $h(P) \neq 0$, si $g(P) = 0$ entonces P es un cero de f y si $h(P) = 0$, P es un polo de f. El caso en que $P = P_\infty$ depende del grado de los polinomios que definen la función racional, esto se exponen más adelante.

1.2. Curvas Elípticas

Definición 1.3. *Curva Elíptica.*

Sea $\mathbb{K}$ un campo y $\overline{\mathbb{K}}$ su cerradura algebraica. Una curva elíptica E sobre $\mathbb{K}$ es una curva algebraica no singular definida por $F[x, y] = y^2 + h(x)y - f(x) \in \mathbb{K}[x, y]$ y se denota como:

$$E : F[x, y] = 0 \tag{3}$$

donde $h(x) \in \mathbb{K}[x]$ y su grado es a lo más 1, en tanto $f(x) \in \mathbb{K}[x]$ es de grado 3.

De esta manera se tiene que una curva elíptica es de la forma:

$$E : a_1 + a_2x + a_3y + a_4x^2 + a_5xy + a_6y^2 + a_7x^3 = 0 \tag{4}$$

tal que $a_1, a_2, \ldots, a_7 \in \mathbb{K}$ y $a_6, a_7 \neq 0$. Debido a esto se puede hacer el cambio de variable $x = -a_6a_7x', y = a_6a_7^2y'$ quedando la ecuación 4 como:

$$E : a_1 - a_2a_6a_7x + a_3a_6a_7^2y + a_4a_6^2a_7^2x^2 - a_5a_6^2a_7^3xy + a_6^3a_7^4y^2 - a_6^3a_7^4x^3 = 0 \tag{5}$$

al dividir por $a_6^3a_7^2$ y renombrar los coeficientes se llega a la forma normal de Weierstrass dada por:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6}$$

o bien en su forma homogeneizada:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{7}$$

con $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.

Al conjunto de todos los pares $(x, y) \in \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ junto con el punto al infinito P_∞, denotado por $E(\overline{\mathbb{K}})$, se le llama *puntos racionales.* Al conjunto de todos los pares $(x, y) \in \mathbb{K} \times \mathbb{K}$ junto con el punto al infinito P_∞, denotado por $E(\mathbb{K})$ se le llama $\mathbb{K}$-puntos racionales. Si no se considera al punto al infinito se llaman puntos finitos.

Teorema 1.4. *Hasse*
Sea $\#E(\mathbb{F}_q) = q + 1 - t$. *Entonces* $|t| \leq 2\sqrt{q}$.

Ejemplo 1.5.

- $C_1 : v^2 + v = u^3 + 1$ *sobre* $\mathbb{F}_2$
- $C_2 : v^2 + uv = u^3 + u + 1$ *sobre* $\mathbb{F}_7$

El conjunto de puntos racionales de C_1 *es:*

$$C_1(\mathbb{F}_2) = \{P_1 = (1, 0), P_2 = (1, 1), P_\infty\}$$

además tiene sentido obtener los puntos racionales sobre cualquier extensión de $\mathbb{F}_2$, por ejemplo

$$C_1(\mathbb{F}_{2^4}) = \{(1, 1), (1, 0), (\alpha^5, 0), (\alpha^5, 1), (\alpha^{10}, 0), (\alpha^{10}, 1), P_\infty\}$$

donde $\alpha^4 + \alpha + 1 = 0$.

En tanto que el conjunto de puntos racionales de C_2 es:

$$C_2(\mathbb{F}_7) = \{(0,1),(0,6),(2,1),(2,4),(3,2),(6,3),(6,5),P_\infty\}$$

Definición 1.6. *Se dice que dos curvas elípticas E y E' sobre $\mathbb{K}$, dadas en su forma normal de Weierstrass son equivalentes si existe una transformación de la forma $\phi(x,y) = (u^2x+r, u^3y+su^2x+t)$ con $u,r,s,t \in \mathbb{K}$ y $u \neq 0$ tal que manda a los puntos de E a puntos E', es decir, transforma a E en E'* [1], [40].

De la definición anterior se puede observar que la transformación inversa es de la misma forma, por lo que se tiene una relación de equivalencia.

A cada curva elíptica se le puede asociar un discriminante Δ y un $j-invariante$. Estos parámetros se dan en función de los coeficientes, y permiten clasificar las curvas elípticas y las fórmulas explícitas se pueden encontrar en [1], [40].

Con estas observaciones la ecuación de una curva elíptica se puede reducir a las siguientes expresiones

- Si la característica del campo es diferente a 2 y 3 entonces la curva es de la forma:

$$E : y^2 = x^3 + a_4x + a_6 \tag{8}$$

- Si la característica del campo es 3 se tendrán dos casos:

$$E : y^2 = x^3 + a_2x^2 + a_6 \tag{9}$$

$$E : y^2 = x^3 + a_4x + a_6 \tag{10}$$

- Si la característica del campo es 2 también se tendrán dos casos:

$$E : y^2 + a_3y = x^3 + a_4x + a_6 \tag{11}$$

$$E : y^2 + xy = x^3 + a_2x^2 + a_6 \tag{12}$$

En criptografía son de especial interés las curvas definidas sobre campos de característica 2. Para utilizar estas es necesario tener la estructura de grupo, la cual se define mediante la siguiente operación, para cualquier característica.

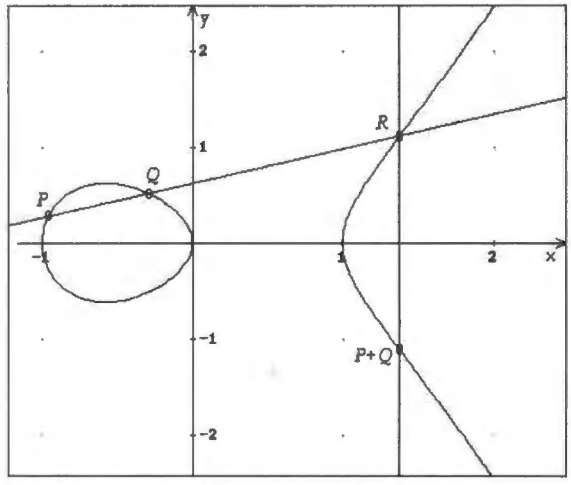

FIGURA 1. adición de puntos de la curva $y^2 = x^3 - x$ sobre $\mathbb{R}$

1.2.1. La operación

Al conjunto de puntos racionales de una curva elíptica E sobre $\mathbb{K}$ se le puede dotar de una estructura de grupo. Como una curva elíptica está definida por una ecuación cúbica en x, cualquier línea cortará sobre el plano $Z = 1$ a la curva de la ecuación homogeneizada en a lo más 3 puntos; sin embargo, se puede considerar que una línea recta siempre corta en 3 puntos a la curva, tomando en cuenta lo siguiente:

- Si una línea corta a la curva en sólo dos puntos se tienen dos subcasos
  - Si la línea es tangente a uno de los puntos, este se considera el tercer punto.
  - Si la línea no es tangente a ninguno de los puntos se considerará que el tercer punto es P_∞.
- Si la línea corta a un sólo punto entonces será una recta tangente, por lo cual se considerará como un segundo punto al mismo punto y como tercero a P_∞.
- Para la recta tangente a P_∞ el segundo y tercer punto en esta será también P_∞.

Con esta consideración se define la suma entre dos puntos racionales de la curva elíptica, P, Q de la siguiente manera: considere la recta L que pasa por los puntos P y Q y denotando con R al tercer punto en $L \cap E(\mathbb{K})$ y sea L' la línea que pasa por los puntos R y P_∞ y sea R' el

tercer punto en $L' \cap E(K)$, entonces $P + Q = R'$. La idea geométrica se muestra en figura 1. La representación sobre un campo finito no es tan clara como en $\mathbb{R}$.

Teorema 1.7. *El conjunto $E(\mathbb{K})$ con la operación $+$ es un grupo abeliano.*

DEMOSTRACIÓN. Sea E una curva elíptica y $P, Q \in E(\mathbb{K})$ entonces $P + Q \in E$ por definición, así la operación es cerrada.

Ahora bien si R es el tercer punto en $\overline{PP_\infty} \cap E(\mathbb{K})$ entonces el tercer punto en $\overline{RP_\infty} \cap E(\mathbb{K})$ es P por lo que $P + P_\infty = P$ teniendo así que P_∞ es el neutro aditivo.

Por otro lado, si R es el tercer punto en $\overline{PQ} \cap E(\mathbb{K})$ y se define $X_P = Q + R$ entonces se tiene que P, X_P, P_∞ están sobre una recta, luego se tiene que $P + X_P = P_\infty$ teniendo así que cualquier punto tiene su inverso.

Además, como las rectas $\overline{PQ}$ y $\overline{QP}$ son la misma se tiene que la operación es conmutativa.

Para ver que la operación es asociativa sean $P, Q, R \in E(\mathbb{K})$ y se considera que $S = P + Q$, $U = Q + R$, $W = S + R$, $W = P + U$, y se definen las siguientes rectas $L_1 = \overline{PQ}$, $M_1 = \overline{SP_\infty}$, $L_2 = \overline{SR}$, $M_2 = \overline{QR}$, $L_3 = \overline{UP_\infty}$, $M_3 = \overline{PU}$, y por último $L = (L_1 \cup L_2 \cup L_3)$ y $M = (M_1 \cup M_2 \cup M_3)$ obteniendo así:

$$\begin{aligned} L_1 \cap E &= \{P, Q, X_S\} & M_1 \cap E &= \{P_\infty, S, X_S\} \\ L_2 \cap E &= \{R, S, X_T\} & M_2 \cap E &= \{Q, R, X_U\} \\ L_3 \cap E &= \{P_\infty, U, X_U\} & M_3 \cap E &= \{P, U, X_W\} \\ L \cap E &= \{P_\infty, P, Q, R, S, U, X_S, X_U, X_T\} \\ M \cap E &= \{P_\infty, P, Q, R, S, U, X_S, X_U, X_W\} \end{aligned}$$

Así pues, se obtiene que $X_T = X_W$, por la proposición 5.2.3 en [**15**], lo cual implica que $T = W$ y como $(P + Q) + R = S + R = T$ y $P + (Q + R) = P + U = W$ se tiene que la operación es asociativa.

Por lo tanto $(E(\mathbb{K}), +)$ es un grupo abeliano finito.

□

Ahora bien, con base en esta definición se pueden encontrar expresiones para la adición de puntos, basados en las coordenadas de los puntos, si se considera a $P = (x_1, y_1)$, y $Q = (x_2, y_2)$ se obtienen los siguientes resultados:

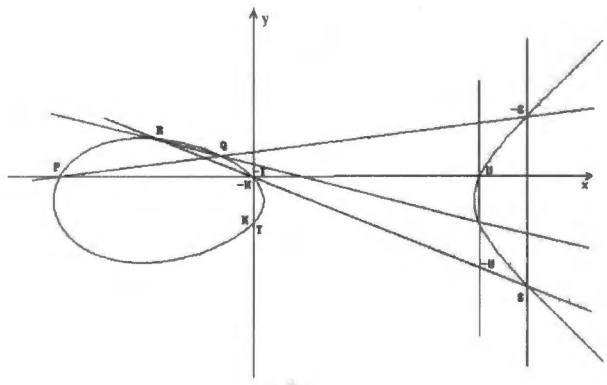

FIGURA 2. Representación de la asociatividad

- El inverso aditivo de P es

$$-P = (x_1, -y_1 - a_1x_1 - a_3). \tag{13}$$

- Si $Q = -P$ entonces $R = P + Q = P_\infty$
- Si $Q = P$ entonces el doble de un punto, $R = 2P = (x_3, y_3)$, está dado por las siguientes expresiones:

$$\begin{aligned} x_3 &= m^2 + a_1m - a_2 - x_1 - x_2 \\ y_3 &= -mx_3 - b - a_1x_3 - a_3 \end{aligned} \tag{14}$$

donde $m = \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}$ y $b = y_1 - mx_1$

- En cualquier otro caso $R = P + Q = (x_3, y_3)$ está dado por:

$$\begin{aligned} x_3 &= m^2 + a_1m - a_2 - x_1 - x_2 \\ y_3 &= -mx_3 - b - a_1x_3 - a_3 \end{aligned} \tag{15}$$

donde $m = \frac{y_1-y_2}{x_1-x_2}$ y $b = y_1 - mx_1$

Ejemplo 1.8. *La curva* $E : Y^2Z + YZ^2 = X^3 + XZ^2 + Z^3$, *sobre* $\mathbb{F}_{2^3}$ *considerando que* α *es raíz de* x^3+x+1, *tiene como conjunto de puntos racionales:*

$E(\mathbb{F}_{2^3}) = \{P_\infty, (\alpha : 0 : 1), (\alpha^2 : 0 : 1), (\alpha^4 : 0 : 1), (\alpha : 1 : 1), (\alpha^2 : 1 : 1), (\alpha^4 : 1 : 1), (\alpha^3 : \alpha : 1), (\alpha^6 : \alpha^2 : 1), (\alpha^5 : \alpha^4 : 1), (\alpha^3 : \alpha^3 : 1), (\alpha^6 : \alpha^6 : 1), (\alpha^5 : \alpha^5 : 1)\}$

Se observa que el orden de este grupo es 13 por lo cual es un grupo cíclico y cualquier elemento diferente al neutro es un generador. Considere que $P = (\alpha : 0 : 1)$ entonces se tiene que:

$* \ 1P = (\alpha : 0 : 1)$

* $2P = (\alpha : 0 : 1) + (\alpha : 0 : 1)$
  $m = \alpha^2 + 1 = \alpha^6 \qquad b = 0 + \alpha^6\alpha = \alpha^7 = 1$
  $x_2 = \alpha^{12} = \alpha^5 \qquad y_2 = \alpha^{18} + 1 + 1 = \alpha^4$
  por lo que $2P = (\alpha^5 : \alpha^4 : 1)$

* $3P = (\alpha : 0 : 1) + (\alpha^5 : \alpha^4 : 1)$
  $m = \frac{0+\alpha^4}{\alpha+\alpha^5} = \frac{\alpha^4}{\alpha^6} = \alpha^5$
  $b = 0 + \alpha^5\alpha = \alpha^6$
  $x_2 = \alpha^{10} + \alpha + \alpha^5 = \alpha^3 + \alpha + \alpha^5 = \alpha^4$
  $y_2 = \alpha^5\alpha^4 + \alpha^6 + 1 = \alpha^2 + \alpha^6 + 1 = 0$
  por lo que $3P = (\alpha^4 : 0 : 1)$

* $4P = (\alpha^5 : \alpha^4 : 1) + (\alpha^5 : \alpha^4 : 1)$
  $m = \alpha^{10} + 1 = \alpha^3 + 1 = \alpha$
  $b = \alpha^4 + \alpha\alpha^5 = \alpha^4 + \alpha^6 = \alpha^3$
  $x_2 = \alpha^2$
  $y_2 = \alpha^3 + \alpha^3 + 1 = 1$
  por lo que $4P = (\alpha^2 : 1 : 1)$

* $5P = (\alpha : 0 : 1) + (\alpha^2 : 1 : 1) = (\alpha^3 : \alpha : 1)$

* $6P = (\alpha^4 : 0 : 1) + (\alpha^4 : 0 : 1)(\alpha^6 : \alpha^2 : 1)$

* $7P = (\alpha : 0 : 1) + (\alpha^6 : \alpha^2 : 1) = (\alpha^6 : \alpha^6 : 1)$

* $8P = (\alpha^2 : 1 : 1) + (\alpha^2 : 1 : 1) = (\alpha^3 : \alpha^3 : 1)$

* $9P = (\alpha : 0 : 1) + (\alpha^3 : \alpha^3 : 1) = (\alpha^2 : 0 : 1)$

* $10P = (\alpha^3 : \alpha : 1) + (\alpha^3 : \alpha : 1) = (\alpha^4 : 1 : 1)$

* $11P = (\alpha : 0 : 1) + (\alpha^4 : 1 : 1) = (\alpha^5 : \alpha^5 : 1)$

* $12P = (\alpha^6 : \alpha^2 : 1) + (\alpha^6 : \alpha^2 : 1) = (\alpha : 1 : 1)$

* $13P = (\alpha : 0 : 1) + (\alpha : 1 : 1)$
  como $x_0 = x_1$ y $y_0 + y_1 + 1 = 0 + 1 + 1 = 0$
  entonces $13P = (0 : 1 : 0)$

Un resultado importante en cuanto a la estructura de grupo en las curvas elípticas sobre un campo finito es el siguiente:

Teorema 1.9. *(2.12 en* [**28**]*)*
El grupo de puntos racionales de una curva elíptica E sobre el campo $\mathbb{F}_q$ es un grupo abeliano de rango 1 ó 2, es decir, $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, donde $n_2|n_1$ aún más $n_2|q-1$.

1.3. Definición de curvas hiperelípticas

Las curvas elípticas, son un caso particular de las curvas hiperelípticas. A continuación se dan algunos resultados básicos e importantes en las curvas hiperelípticas.

Definición 1.10. *Curvas Hiperelípticas*
Sea $\mathbb{K}$ un campo y $\overline{\mathbb{K}}$ su cerradura algebraica; una curva hiperelíptica C sobre $\mathbb{K}$ de género g es una curva algebraica no singular de la forma:

$$C : v^2 + h(u)v = f(u) \text{ en } \mathbb{K}[u,v] \tag{16}$$

donde $h(u) \in \mathbb{K}[u]$ y su grado es a lo más g, en tanto $f(u) \in \mathbb{K}[u]$ es de grado $2g+1$.

En el caso de curvas hiperelípticas suelen utilizarse las variables u, v en lugar de x, y. De igual forma, que para curvas elípticas, se define el conjunto de todos los pares $(u,v) \in \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ junto con el punto al infinito P_∞, denotado por $C(\overline{\mathbb{K}})$ al que se llama conjunto de puntos racionales, al conjunto de todos los pares $(u,v) \in \mathbb{K} \times \mathbb{K}$ junto con el punto al infinito P_∞, denotado por $C(\mathbb{K})$ se le llama $\mathbb{K}$-puntos racionales. Cuando no se considera al punto al infinito se llaman puntos finitos.

En lo sucesivo, salvo que se indique lo contrario, u, v se utilizarán como variables de funciones racionales. Además h, f representarán los polinomios que definen a una curva curva hiperelíptica y g será el género de la curva de que se haga referencia.

Ejemplo 1.11.

- $C_1 : v^2 + v = u^5 + 1$ *sobre* $\mathbb{F}_2$
- $C_2 : v^2 + uv = u^3 + u + 1$ *sobre* $\mathbb{F}_7$
- $C_3 : v^2 + uv = u^5 + u + 1$ *sobre* $\mathbb{F}_{23}$

El conjunto de puntos racionales de C_1, que es una curva de género 2, es:

$$C_1(\mathbb{F}_2) = \{P_1 = (1,0), P_2 = (1,1), P_\infty\}$$

además tiene sentido obtener los puntos racionales sobre cualquier extensión de $\mathbb{F}_2$, por ejemplo

$C_1(\mathbb{F}_{2^4}) = \{(0,\alpha^5),(0,\alpha^{10}),(1,0),(1,1),(\alpha,\alpha^2),(\alpha,\alpha^8),(\alpha^2,\alpha),(\alpha^2,\alpha^4),$
$(\alpha^3,0),(\alpha^3,1),(\alpha^4,\alpha^2),(\alpha^4,\alpha^4),(\alpha^5,\alpha),(\alpha^5,\alpha^8),(\alpha^6,0),(\alpha^6,1),(\alpha^7,\alpha^2),$
$(\alpha^7,\alpha^8),(\alpha^8,\alpha),(\alpha^8,\alpha^4),(\alpha^9,0),(\alpha^9,1),(\alpha^{10},\alpha^2),(\alpha^{10},\alpha^8),(\alpha^{11},\alpha),$
$(\alpha^{11},\alpha^4),(\alpha^{12},0),(\alpha^{12},1),(\alpha^{13},\alpha^2),(\alpha^{13},\alpha^8),(\alpha^{14},\alpha),(\alpha^{14},\alpha^4),P_\infty\}$

donde $\alpha^4+\alpha+1=0$.

En tanto que el conjunto de puntos racionales de C_2, que es una curva de género 1, es:

$$C_2(\mathbb{F}_7) = \{(0,1),(0,6),(2,1),(2,4),(3,2),(6,3),(6,5),P_\infty\}$$

De la misma manera se observa que el conjunto de puntos racionales de C_3, cuyo género es 2, es:

$C_3([F_{23}]) = \{(0,1),(0,22),(1,8),(1,14),(2,5),(2,16),(3,5),(3,15),(6,5),$
$(6,12),(8,4),(8,11),(10,15),(10,21),(15,0),(15,8),(16,0),(16,7),(17,8),$
$(17,21),(19,11),(19,16),(20,9),(20,17),P_\infty\}$

Definición 1.12. *Sea $\sigma : C \to C$ definida por*

$$\sigma(x,y) = (x,-y-h(x)) \tag{17}$$

Es fácil ver que si $P=(x,y)$ es un punto finito sobre la curva C, entonces $\sigma^2(P)=P$

Definición 1.13. *El opuesto de $P \in C$ está definido por: $\widetilde{P} = \sigma(P)$. En el caso del punto al infinito se define su opuesto como él mismo, es decir, $\widetilde{P}_\infty = P_\infty$.*

Se dice que el punto P es ordinario si $\sigma(P) \neq P$, en caso contrario se dice que es un punto especial.

Es evidente que $\widetilde{\widetilde{P}} = P$. En la curva C_2 sobre $\mathbb{F}_7$ hay dos puntos especiales que son $(3,2)$ y P_∞.

En el caso de una curva hiperelíptica, debido a la forma del polinomio que la define, de grado 2 sobre v, se tiene que el anillo de cocientes se puede expresar como:

$$\mathbb{K}[C] = \mathbb{K}[u] + \mathbb{K}[u]v \tag{18}$$

es decir, es un $\mathbb{K}[u]$-módulo finitamente generado, que tiene como generador al conjunto $\{v, 1\}$.

Con base en esta observación se puede definir el conjugado de una función racional de la forma $G = a(u) - b(u)v$ como $\overline{G} = a(u) + b(u)(h(u) + v)$, con lo cual se induce la norma sobre $\mathbb{K}[C]$ de G definiéndola como $N(G) = G\overline{G}$, de esta forma se tiene que $N(G) = N(\overline{G})$.

Definición 1.14. *Grado de un polinomio.*
El grado del polinomio $G = a(u) - b(u)v \in \mathbb{K}[C]$ se define como:

$$gr(G) = max[2gr_u(a), 2g + 1 + 2gr_u(b)] \tag{19}$$

Lema 1.15. *(propiedades del grado)*
Si $G, H \in \mathbb{K}[C]$ entonces se cumple:

- $gr(G) = gr_u(N(G))$.
- $gr(\overline{G}) = gr(G)$.
- $gr(GH) = gr(G) + gr(H)$.

DEMOSTRACIÓN. Se define las funciones $G(u, v) = a(u) - b(u)v$, $H(u, v) = c(u) - d(u)v \in \mathbb{K}[C]$, entonces

- Se tiene que

$$N(G) = [a(u) - b(u)v][a(u) + b(u)(h(u) + v)] = a^2(u) + a(u)b(u) + b^2(u)f(u)$$

de donde se sigue que

$$gr_u(N(G)) = max[2gr_u(a), 2g + 1 + 2gr_u(b)] = gr(G)$$

- Del punto anterior y de la última observación:

$$gr(G) = gr_u(N(G)) = gr_u(N(\overline{G})) = gr(\overline{G})$$

- Por último se observa que

$$gr(GH) = gr_u(N(GH)) = gr_u(N(G)N(H)) = gr(G) + gr(H).$$

□

Con la definición de grado de un polinomio es posible definir la evaluación de una función racional en el punto al infinito P_∞.

Definición 1.16. *Evaluación en el punto al infinito.*
Sea $F \in \mathbb{K}(C)^*$ de la forma $F = G/H$ con $G, H \in \mathbb{K}[C]$ entonces $F(P_\infty)$ se define como:

- *Si $gr(G) < gr(H)$ entonces $F(P_\infty) = 0$*
- *Si $gr(G) > gr(H)$ se tiene que $F(P_\infty)$ no está bien definida, o bien, $F(P_\infty) = \infty$*

- *Si $gr(G) = gr(H)$ entonces $F(P_\infty)$ es la razón entre los coeficientes líderes.*

Lema 1.17. *Sea $G \in \mathbb{K}[C]$ y $P \in C$ entonces $G(P) = \overline{G}(\widetilde{P})$*

DEMOSTRACIÓN. Sean $G = a(u) - b(u)$ y $P = (x, y)$, entonces $\overline{G} = a(u) + b(u)(v + h(u))$ y $\widetilde{P} = (x, -y - h(x))$, por lo cual $\overline{G}(\widetilde{P}) = a(x) + b(x)((-y - h(x)) + h(x)) = a(x) - b(x)y = G(P)$ □

Si $G \in \mathbb{K}(C)$ y $P \in C(\mathbb{K})$, entonces G se puede factorizar como $G = U^i S$, con $i \in \mathbb{Z}$, donde $U, S \in \mathbb{K}(C)$ tienen la propiedad de que $U(P) = 0$, y P no es ni cero ni polo de S. Esta factorización es importante y en los siguientes resultados se muestra cómo se logra esto.

Lema 1.18. *Sea $P = (x, y) \in C$ y $G = a(u) - b(u)v \in \mathbb{K}[C]$ tal que P es un cero de G, y que x no es una raíz de $a(u)$ y $b(u)$, luego $\overline{G}(P) = 0$ si y solo si P es un punto especial.*

DEMOSTRACIÓN. Sea $P = (x, y) \in C$ y $G(u, v) = a(u) + b(u)v$ tales que $G(P) = 0$, $\overline{G}(P) = 0$, $a(x) \neq 0$ y $b(x) \neq 0$. Entonces

$$a(x) - b(x)y = 0 \text{ y } a(x) + b(x)(y + h(x)) = 0$$

$$a(x) - b(x)y = a(x) + b(x)(y + h(x))$$

$$2b(x)y = -b(x)h(x)$$

y como $b(x) \neq 0$ se tiene que $2y = -h(x)$, es decir, P es un punto especial.

Si $P = (x, y)$ es un punto especial se cumple que $-y = y + h(x)$. Si $G(P) = 0$ se obtiene

$$0 = G(x, y) = a(x) - b(x)y = a(x) + b(x)(y + h(x)) = \overline{G}(P)$$

□

Lema 1.19. *Sea $P = (x, y)$ un punto ordinario de C además sea $G = a(u) - b(u)v \in \mathbb{K}[C]^*$, supóngase que $G(P) = 0$ y x no es una raíz de $a(u)$ y $b(u)$, entonces G se puede escribir de la forma $(u - x)^s S$ donde s es la máxima potencia de $(u - x)$ que divide a $N(G)$ y P no es cero ni polo de $S \in \mathbb{K}(C)$.*

DEMOSTRACIÓN. Sea $G(u, v) = a(u) - b(u)v \in \mathbb{K}[C]^*$ luego

$$G(u, v) = \frac{G\overline{G}}{\overline{G}} = \frac{N(G)}{\overline{G}} = \frac{a^2(u) + a(u)b(u)h(u) - b^2(u)f(u)}{a(u) + b(u)(h(u) + v)}$$

sea $P = (x, y)$ un punto ordinario tal que $G(P) = 0$, por el lema 1.18 se tiene que $\overline{G}(P) \neq 0$.

Como P es un cero de G entonces $N(G)(x) = 0$. De esta forma, un factor de $N(G)$ es $(u-x)$. Sea s el mayor entero tal que $(u-x)^s | N(G)$, luego $N(G) = (u-x)^s S'$ donde $S'(x) \neq 0$.

Si $S(u,v) = \frac{S'(u)}{a(u)+b(u)(h(u)+v)}$ entonces P no es cero de S y tampoco es polo. Así $G(u,v) = (u-x)^s S$ como se quería. □

Lema 1.20. *Sea $P = (x,y)$ un punto especial de C, entonces $(u-x)$ se puede escribir como $(v-y)^2 S(u,v)$, donde P no es ni cero ni polo de $S \in \mathbb{K}(C)$.*

DEMOSTRACIÓN. Sea $H = (v-y)^2$ y $S = (u-x)/H$, de aquí $HS = (u-x)$. Sea $P = (x,y)$ un punto especial, luego $2y + h(x) = 0$ y además como P es no singular se tiene que $h'(x)y - f'(x) \neq 0$ también $f(x) = y^2 + h(x)y = y^2 + (-2y)y = -y^2$. De aquí se sigue que:

$$H(u,v) = (v-y)^2 = v^2 - 2yv + y^2 = f(u) - h(u)v - 2yv + y^2$$

y así

$$\frac{1}{S(u,v)} = \frac{f(u)+y^2}{u-x} - v\left(\frac{h(u)+2y}{u-x}\right) \tag{20}$$

La parte derecha de la ecuación 20 es un polinomio, ya que $u-x$ es factor tanto $f(u)-y^2$ como de $h(u)+2y$. Sea $s(u) = H(u,y)$ luego $s(x) = 0$ aún más $s'(x) \neq 0$ lo cual indica que $(u-x)$ divide a $s(u)$ pero $(u-x)^2$ no lo divide. De esta forma, $S(P) \neq 0, \infty$. □

Lema 1.21. *Sea $P \in C$, entonces existe al menos una función $U_P \in \mathbb{K}(C)$, llamada parámetro uniformizante, con las siguientes propiedades: (i) $U_P(P) = 0$, (ii) para cada polinomio $G \in \mathbb{K}[C]^*$, existe $S \in \mathbb{K}(C)$ tal que $G = U_P^d S$ y d no depende de la elección de U_P, además se tiene que:*

- *Si $P = P_\infty$ entonces $U_P = \frac{u^g}{v}$*
- *Si $P = (x,y)$ es un punto ordinario entonces $U_P = (u-x)$*
- *Si $P = (x,y)$ es un punto especial entonces $U_P = (v-y)$*

DEMOSTRACIÓN. Sea $G(u,v) \in \mathbb{K}[C]^*$ y sea $P \in C$. Si $G(P) \neq 0, \infty$ entonces sea U cualquier función que satisfaga $U(P) = 0$ y se tiene que $G = U^0 G$, en particular las funciones dadas lo cumplen. En caso contrario se consideran tres casos,

1. Si $P = P_\infty$ entonces se considera a $U = \frac{u^g}{v}$, como $gr(u^g)$ es menor que $gr(v)$ se tiene que $U(P_\infty) = 0$, y de esta forma

$$G = \left(\frac{u^g}{v}\right)^d \left(\frac{v}{u^g}\right)^d G$$

donde $d = -gr(G)$, y así tomando $S = (v/u^g)^d G$, se obtiene el resultado en este caso.

2. Sean $P = (x, y)$ un punto ordinario y $U = (u - x)$. Es claro que $U(P) = 0$, defina $G = a - bv$, y a r como el mayor entero tal que $(u - x)^r | a(u), b(u)$ y de esta forma $G = (u - x)^r G_0 = (u - x)^r (a_0(u) - b_0(u)v)$, si $G_0(P) \neq 0$ entonces $S = G_0$ y $r = d$, si no por el lema 1.19, se tiene que $G_0 = (u - x)^s S$ y por tanto $G = (u-x)^{r+s} S$, y considerando $d = s+r$ se obtiene el resultado.
3. Sea $P = (x, y)$ un punto especial y $U = (v - y)$. Es claro que $U(P) = 0$, en este caso como G es un polinomio de grado $2g$ en u se considera que:

$$G(u, v) = u^{2g} b_{2g}(v) + u^{2g-1} b_{2g-1}(v) + \cdots + u b_1(v) + b_0(v)$$

donde $b_i(v) \in K[v]$. Sustituyendo u por $(u - x) + x$ y simplificando se obtiene

$$G(u, v) = (u-x)^{2g} \bar{b}_{2g}(v) + (u-x)^{2g-1} \bar{b}_{2g-1}(v) + \cdots + (u-x)\bar{b}_1(v) + \bar{b}_0(v)$$

$$G(u, v) = (u - x)B(u, v) + \bar{b}_0(v)$$

y como $G(P) = 0$ entonces $\bar{b}_0(y) = 0$ y así $\bar{b}_0(v) = (v - y)c(v)$ y por el lema 1.20 se tiene que $(u-x) = (v-y)^2/A(u, v)$ donde $A \in K[C]$ y P no es ni polo ni cero, por lo cual:

$$G = \frac{v - y}{A(u, v)} [(v - y)B(u, v) + A(u, v)c(v)] = \frac{v - y}{A(u, v)} G_1(u, v)$$

Si $G_1(P) \neq 0$ entonces se toma $S = G_1/A$, en caso contrario se tiene que $c(y) = 0$, por lo tanto $c(y) = (v - y)c_1(v)$ y se considera

$$G = \frac{(v - y)^2}{A(u, v)} [B(u, v) + A(u, v)c_1(v)] = \frac{(v - y)^2}{A(u, v)} G_2(u, v)$$

Si $G_2(P) \neq 0$ entonces se toma a $S = G_2/A$ y termina, si no se repite el proceso.

Para verificar que el valor de d es independiente al parámetro uniformizante que se tome, considere que dado U se selecciona otro parámetro U_1, entonces se satisface que $U(P) = U_1(P) = 0$ y también $U = U_1^a A$ y $U_1 = U^b B$ donde $a, b \geq 1$ y además $A(P) \neq 0, \infty$, $B(P) \neq 0, \infty$.

Sustituyendo el valor de U_1 en la expresión para U se obtiene, $U = (U^b B)^a A = U^{ab}(B^a A)$ lo cual implica que $U^{ab-1}(B^a A) = 1$ es decir $ab - 1 = 0$ entonces $a = b = 1$ y finalmente $G = U^d S = U_1^d (A^d S)$, y P no es ni cero ni polo de $A^d S$. □

Con base en el parámetro uniformizante se establece la siguiente definición.

Definición 1.22. *Sean $G \in \mathbb{K}(C)^*$, $P \in C$ y $U \in \mathbb{K}(C)$ un parámetro uniformizante de P, luego $G = U^d S$ donde $S \in \mathbb{K}(C)$ no tiene polos ni ceros en P. Entonces el orden de G en P es d y se denota como*

$$ord_P(G) = d \tag{21}$$

Lema 1.23. *Sean $G_1, G_2 \in K[C]^*$ y $P \in C$, supóngase que $ord_P(G_1) = r_1$ y $ord_P(G_2) = r_2$. Se cumplen las siguientes afirmaciones:*

- $ord_P(G_1 G_2) = r_1 + r_2$.
- *Si $G_1 \neq -G_2$ y $r_1 \neq r_2$ entonces $ord_P(G_1 + G_2) = min(r_1, r_2)$.*
- *Si $G_1 \neq -G_2$ y $r_1 = r_2$ entonces $ord_P(G_1 + G_2) \geq r_1$.*

DEMOSTRACIÓN. Como $ord_P(G_1) = r_1$ y $ord_P(G_2) = r_2$ entonces existen funciones racionales S_1, S_2 tales que $G_1 = U^{r_1} S_1$ y $G_2 = U^{r_2} S_2$, donde U es un parámetro uniformizante de P.

De esta manera, $G_1 G_2 = U^{r_1} S_1 U^{r_2} S_2 = U^{r_1 + r_2} S_1 S_2$ con lo cual se tiene que $ord_P(G_1 G_2) = r_1 + r_2$.

Sea $r = min(r_1, r_2)$ luego

$$G_1 + G_2 = U^{r_1} S_1 + U^{r_2} S_2 = U^r (U^{r_1 - r} S_1 + U^{r_2 - r} S_2)$$

Si $r_1 \neq r_2$ entonces $r_1 \neq r$ o bien $r_2 \neq r$ sin pérdida de generalidad supongamos que $r_2 \neq r$, es decir, $r_2 - r > 0$. Esto implica que

$$G_1 + G_2 = U^r (S_1 + U^{r_2 - r} S_2)$$

y como $S_1(P) + U^{r_2 - r}(P) S_2(P) = S_1(P)$ por lo cual se cumple que $ord_P(G_1 + G_2) = min(r_1, r_2)$

Si $r_1 = r_2$ entonces $r_1 = r = r_2$ y se tiene que

$$G_1 + G_2 = U^r (S_1 + S_2)$$

como puede suceder que $S_1(P) + S_2(P) = 0$, luego $ord_P(G_1 + G_2) \geq r_1$. □

Con está definición de orden de un polinomio en un punto, no es fácil de calcularlo, por lo cual se utiliza una definición alterna. Para el caso

de las funciones racionales, se puede extender la definición considerando

$$ord_P\left(\frac{G}{H}\right) = ord_P(G) - ord_P(H). \tag{22}$$

Definición 1.24. *Orden de un polinomio en un punto(Alterna)*

Sean $G = a(u) - b(u)v \in \mathbb{K}[C]^*$ y $P \in C$. El orden de G en P se define como:

- *Si $P = P_\infty$ entonces*

$$ord_P(G) = -max\{2gr_u(a), 2g+1+2gr_u(b)\} \tag{23}$$

- *Si $P = (x, y)$ entonces sea r la máxima potencia de $(u - x)$ que divide tanto a $a(u)$ como a $b(u)$ y escribir a G de la forma $G = (u-x)^r(a_0(u) - b_0(u)v)$, si $(a_0(x) - b_0(x)y) \neq 0$ entonces $s = 0$, en caso contrario sea s la máxima potencia de $(u - x)$ que divide a $N((a_0(u) - b_0(u)v))$. Si P es un punto ordinario entonces*

$$ord_P(G) = r + s \tag{24}$$

si P es un punto especial entonces

$$ord_P(G) = 2r + s. \tag{25}$$

Teorema 1.25. *Sea $G \in \overline{\mathbb{K}}(C)^*$ entonces G tiene un número finito de ceros y polos, más aún $\sum_{P \in C} ord_P(G) = 0$.*

DEMOSTRACIÓN. Sólo se considera el caso en que $G \in \overline{\mathbb{K}}[C]^*$, esto se debe a la ecuación 22. De esta forma se tiene que el único polo de G es P_∞ y además como un cero de G es también un cero de $N(G)$ entonces

$$\sum_{P \in C \setminus \{P_\infty\}} ord_P(G) \leq max\{2gr_u(a), 2g+1+2gr_u(b)\} = -ord_{P_\infty}(G).$$

Como el orden de un punto es positivo y si este es un cero, entonces se tiene que el número de ceros y polos de G es finito, sólo basta ver que en la desigualdad anterior se da la igualdad.

Para esto se considera a $G = a(u) + b(u)v$ y es suficiente verificar que todo cero de $N(G)$ implica un cero de G. Si x_i es una raíz de $N(G)$ entonces existe $y_i \in \overline{\mathbb{K}}$ tal que $P_i = (x_i, y_i)$, $\widetilde{P}_i = (x_i, -y_i - h(x_i)) \in C$, ahora bien

$$0 = N(G)(P_i) = [a(x_i) - b(x_i)y_i][a(x_i) + b(x_i)(h(x_i) + y_i)]$$

Lo cual implica que:

$$[a(x_i) - b(x_i)y_i] = 0$$

ó

$$[a(x_i) + b(x_i)(h(x_i) + y_i)] = 0,$$

si $[a(x_i) - b(x_i)y_i] = 0$ entonces P_i es cero de G y si:

$$[a(x_i) + b(x_i)(h(x_i) + y_i)] = 0$$

entonces $\widetilde{P}_i$ es cero de G.

□

Ejemplo 1.26. *Considere la curva hiperelíptica* $C : y^2 = x^3 + 3x$ *sobre* $\mathbb{F}_{11}$ *y considere* $f = \frac{y+x+1}{x+8}$. *Entonces, esta función tiene polos en* P_∞, $(3,5)$, $(3,6)$, *además tiene un cero en* $(1,9)$. *Esta función tiene otros dos ceros los cuales no se encuentran sobre* $\mathbb{F}_{11}$, *pero si en* $\mathbb{F}_{11^2}$, *luego los parámetros uniformizantes son:*

P	u	s	d
P_∞	$\frac{x}{y}$	$\frac{y^d(y+x+1)}{x^d(x+8)}$	-1
$(3,5)$	$(x-3) = (x+8)$	$\frac{(x+8)^{-d}(y+x+1)}{x+8}$	-1
$(3,6)$	$(x-3) = (x+8)$	$\frac{(x+8)^{-d}(y+x+1)}{x+8}$	-1
$(1,9)$	$(x-1) = (x+10)$	$\frac{(x+10)^{-d}(y+x+1)}{x+8}$	1

1.4. Divisores

La generalización de la estructura de grupo de las curvas elípticas a las curvas hiperelípticas no se da, puesto que una linea recta corta a la curva en más de tres puntos. Para tener un grupo usando curvas hiperelípticas de género mayor a 1, el grupo se define sobre la Jacobiana de la curva, por lo que es necesario analizar otros aspectos basados en los divisores.

Definición 1.27. *Un divisor* D *sobre una curva hiperelíptica* C *es una suma formal sobre los puntos en* C, *es decir,*

$$D = \sum_{P \in C} n_P P \tag{26}$$

donde $n_P = 0$ *para todos excepto un número finito de* $P \in C$.

Al conjunto de los divisores sobre una curva hiperelíptica se le denota como $Div(C)$. $Div(C)$ es el $\mathbb{Z}-$*módulo* libre generado por los puntos de la curva. De esta forma se tiene:

$$\sum_{P\in C} n_P(P) + \sum_{P\in C} m_P(P) = \sum_{P\in C}(n_P + m_P)(P) \tag{27}$$

El soporte de un divisor $D = \sum_{P\in C} n_p(P)$ es el conjunto

$$supp(D) = \{P \in C | n_p \neq 0\}. \tag{28}$$

El grado de un divisor $D = \sum_{P\in C} n_p(P)$ es:

$$deg(D) = \sum_{P\in C} n_p \tag{29}$$

y *el orden de* D *sobre* P está definido por $ord_P(D) = n_P$.

El conjunto de los divisores de grado 0 forma un subgrupo de $Div(C)$ y se denota por $Div^0(C)$.

Definición 1.28. *El divisor de* $F \in \overline{\mathbb{K}}(C)^*$ *está definido como:*

$$div(F) = \sum_{P\in C} ord_p(F)(P) \tag{30}$$

Dos observaciones importantes son que $div(F) = 0$ solamente si F es constante y además se tiene que $div(FG) = div(F) + div(G)$.

Definición 1.29. *Un divisor* $D \in Div(C)$ *es llamado principal si existe una función racional* F*, tal que* $D = div(F)$.

Con estas definiciones es posible establecer una relación de equivalencia entre los divisores de grado cero dada por $D_1 \sim D_2$ si $D_1 - D_2$ es principal, es decir, si $D_1 = D_2 + div(F)$ para alguna función racional F y por tanto, se dirá que D_1 y D_2 son equivalentes.

Al conjunto de divisores principales se le denotará como $\mathbb{P}$, el cual es un subconjunto de $Div^0(C)$ por el teorema 1.25, aún más es un subgrupo debido a las observaciones anteriores.

Definición 1.30. *Al grupo cociente* $\frac{Div^0(C)}{\mathbb{P}}$*, se le llama la Jacobiana de* C*, y se denota por* $\mathbb{J}(C)$.

Como se ha mencionado, el grupo utilizado en criptografía de curvas hiperelípticas es la jacobiana y consiste en clases laterales de divisores. Al realizar operaciones es necesario tener "buenos" representantes. Para esto, se definen algunos tipos de divisores, sus distintas representaciones, cómo se pueden relacionar y la forma de operarlos.

Definición 1.31. *Un divisor semirreducido es un divisor de la forma* $D = \sum m_i P_i - (\sum m_i) P_\infty$, *donde* $m_i \geq 0$ *y los* P_i*'s son puntos finitos tales que si* $P_i \in supp(D)$ *entonces* $\widetilde{P_i} \notin supp(D)$, *salvo que* P_i *sea un punto especial, en cuyo caso* $m_i = 1$.

Definición 1.32. *Un divisor es reducido si* D *es semirreducido, es decir,* $D = \sum m_i P_i - (\sum m_i) P_\infty$ *y además* $\sum m_i \leq g$.

Definición 1.33. *La norma de un divisor* $D = \sum_{P \in C} m_P P$ *está dada por:*

$$|D| = \sum_{P \in C \setminus \{P_\infty\}} |m_p|. \tag{31}$$

Teorema 1.34. *Para cada divisor* $D \in Div^0(C)$ *existe un divisor* D_1 *semirreducido tal que* $D \sim D_1$.

DEMOSTRACIÓN. Sea $D = \sum_{P_i \in C} m_i P_i \in Div^0$, sea C_1 el conjunto de los puntos ordinarios tales que si $P \in C_1$ entonces $\widetilde{P} \notin C_1$ y $m_p < m_{\widetilde{P}}$, C_2 el conjunto de los puntos ordinarios P tal que $P \notin C_1$, y C_0 el conjunto de los puntos especiales. Entonces se tiene que:

$$D = \sum_{P \in C_0} m_P P + \sum_{P \in C_1} m_P P + \sum_{P \in C_2} m_P P - m P_\infty$$

Si se considera el divisor:

$$D_1 = D - \sum_{P=(x,y) \in C_1} m_P div(u-x) - \sum_{P=(x,y) \in C_0} \lfloor \frac{m_P}{2} \rfloor div(u-x)$$

entonces $D \sim D_1$ y además:

$$D_1 = \sum_{P \in C_2} (m_P - m_{\widetilde{P}}) P + \sum_{P \in C_0} \left(m_P - 2 \lfloor \frac{m_P}{2} \rfloor \right) P - m_1 P_\infty$$

aún más de esto se tiene que $|D_1| < |D|$. □

Lema 1.35. *Sea* $P = (x, y)$ *un punto ordinario en* C *y sea* $R \in \overline{\mathbb{K}}(C)$ *tal que* P *no es polo de esta. Entonces para cada entero no negativo* k, *existen elementos únicos* $c_0, c_1, \ldots, c_k \in \overline{\mathbb{K}}$ *y* $R_k \in \overline{\mathbb{K}}(C)$, *tal que* $R = \sum_{i=0}^{k} c_i (x-u)^i + (u-x)^{k+1} R_k$ *y* P *no es polo de* R_k.

DEMOSTRACIÓN. Sea $c_0 = R(x, y)$, entonces P es un cero de $R - c_0$ y como $(u - x)$ es un parámetro uniformizante de P, se tiene que $R - c_0 = (u - x) R_1$ para algún $R_1 \in \overline{\mathbb{K}}(C)$, luego $R = c_0 + (u - x) R_1$ y siguiendo el proceso por inducción se tiene el resultado. □

Lema 1.36. *Sea $P = (x, y)$ un punto ordinario en C, entonces para cada $k \geq 1$ existe un único polinomio $b_k(u) \in \overline{\mathbb{K}}[C]$ tal que:*

1. $gr_u(b_k) < k$.
2. $b_k(x) = y$.
3. $b_k^2(u) + b_k(u)h(u) \equiv f(u) \pmod{(u-x)^k}$.

DEMOSTRACIÓN. Considérese que $v = \sum_{i=0}^{k-1} c_i(u-x)^i + (u-x)^k R_{k-1}$ donde $c_i \in \overline{\mathbb{K}}$ y $R_{k-1} \in \overline{\mathbb{K}}(C)$, lo cual es posible por el lema anterior, y se define $b_k(u) = \sum_{i=0}^{k-1} c_i(u-x)^i$, con lo cual se tiene que $c_0 = y$ y de esta forma $b_k(x) = y$, además es claro que $gr_u(b_k) < k$, como $v^2 + h(u)v = f(u)$ al sustituir v por b_k se obtiene:

$$(b_k + (u-x)^k R_k)^2 + (b_k + (u-x)^k R_k)h(u) = f(u)$$

por lo tanto

$$b_k^2(u) + b_k(u)h(u) \equiv f(u) \pmod{(u-x)^k}$$

□

Definición 1.37.

El máximo común divisor de dos divisores

$$D_1 = \sum_{P \in C} m_P P \qquad D_2 = \sum_{P \in C} n_P P$$

es:

$$gcd(D_1, D_2) = \sum_{P \in C} min(m_P, n_P)P - \left(\sum_{P \in C} min(m_P, n_P) \right) P_\infty. \tag{32}$$

Notación 1.38. *Las siguientes expresiones serán equivalentes:*

$$gcd(div(a(u), div(b(u) - v)) = div(a, b) = (a, b) \tag{33}$$

Teorema 1.39. *Sea $D = \sum m_i P_i - (\sum m_i) P_\infty$ un divisor semirreducido, donde $P_i = (x_i, y_i)$, sea $a(u) = \prod (u - x_i)^{m_i}$ y $b(u)$ el único polinomio que satisface*

i) $gr_u(b) < gr_u(a)$;
ii) $b(x_i) = y_i$ *para todo* i *tal que* $m_i \neq 0$,
iii) $a(u)$ *divide a* $b^2 + bh - f$,

entonces $D = gcd(div(a(u)), div(b(u) - v))$.

DEMOSTRACIÓN. Sea C_1 el conjunto de todos los puntos ordinarios en el soporte de D, $C_2 = \{\widetilde{P} \in C | P \in C_1\}$ y C_0 el conjunto de los puntos especiales en $supp(D)$ entonces se tiene que

$$D = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - mP_\infty$$

donde $m_i, m\ \mathbb{Z}_{\geq 1}$.

Para cada $P_i \in C_1$ por el lema 1.36 existe un único polinomio $b_i(u)$ tal que

i) $gr_u(b_i) < m_i$,
ii) $b_i(x_i) = y_i$ y
iii) $b_i^2(u) + b_i(u)h(u) - f(u) \equiv 0(\mod (u-x)^k)$

además que para cada $P_i \in C_0$, $b_i(u) = y_i$ es el único que satisface que

i) $gr_u(b_i) < 1$,
ii) $b_i(x_i) = y_i$ y
iii) $b_i^2(u) + b_i(u)h(u) - f(u) \equiv 0(\mod (u-x)^k)$,

luego sea $b(u)$ tal que:

$$b(u) \equiv b_i(u) (\mod (u-x_i)^{m_i})\ \forall i$$

Como $gr_u(b_i) < m_i$, entonces se tiene que $gr_u(b) < \sum m_i = gr_u(a)$. Además como $b(u) = b_i(u) + (x_i - u)r_i(u)$, entonces $b(x_i) = b_i(x_i) = y_i$.

Ahora bien tenemos que:

$$div(a(u)) = div\left(\prod (x_i - u)^{m_i}\right) = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \widetilde{P}_i + (n)P_\infty$$

y

$$div(b(u) - v) = \sum_{P_i \in C_0} t_i P_i + \sum_{P_i \in C_1} s_i P_i + \sum_{P_i \in C \setminus (C_0 \cup C_1 \cup C_2 \cup \{P_\infty\})} m_i P_i$$

como $s_i \geq m_i$ puesto que $(u - x_i)^{m_i}$ divide a $N(b - v)$, además si consideramos que $P = (x, y) \in C_0$ entonces $(u - x)$ divide a $b^2 + bh - f$, cuya derivada evaluada en $u = x$ es

$$2b(x)b'(x) + b'(x)h(x) + b(x)h'(x) - f'(x) = b'(x)\,(2y + h(x)) + (h'(x)y - f'(x))$$

como P es un punto especial entonces se cumple que $2y + h(x) = 0$ y $h'(x)y - f'(x) \neq 0$, por lo tanto $t_i = 1$, y de esta forma se tiene que:

$$div(a, b) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - mP_\infty$$

donde $m = \sum_{P_i \in C_0} 1 + \sum_{P_i \in C_1} m_i$ □

Lema 1.40. *Sean $a(u), b(u) \in \overline{\mathbb{K}}[U]$ tal que $gr_u(b) < gr_u(a)$. Entonces $div(a, b)$ es semirreducido.*

Lema 1.41. *Sea R una función racional en $\overline{\mathbb{K}}(C)$, si R no tiene polos excepto P_∞ entonces R es una función polinomial.*

DEMOSTRACIÓN. Sea $R = G/H$ donde $G, H \in \overline{\mathbb{K}}[C]^*$. Entonces se tiene que $R = \frac{G\overline{H}}{H\overline{H}} = \frac{G\overline{H}}{N(H)} = \frac{a-bv}{c}$ donde $a, b, c \in \overline{\mathbb{K}}[u]$ y $c \neq 0$. Sea $x \in \overline{\mathbb{K}}$ una raíz de c, $P = (x, y)$ un punto en C y sea d la máxima potencia de $(u - x)$ que divide a c.

Si P es un punto ordinario entonces $ord_P(c) = ord_{\tilde{P}}(c) = d$, y como R no tiene polos finitos entonces $ord_P(a - bv) \geq d$ y $ord_{\tilde{P}}(a - bv) \geq d$, así $(u - x)^d$ es un divisor común de c y $(a - bv)$.

Si P es un punto especial entonces $ord_P(c) = 2d$ por lo cual $ord_P \geq 2d$ con lo que $(a - bv) = \frac{(v-y)^{2d}D}{A^d}$, donde $A, D \in \overline{\mathbb{K}}[C]^*$ y A satisface que $(v - y)^2 = (u - x)A$ y así se tiene que $a - bv = (u - x)D$ y de esta forma $(u - x)^d$ es factor común de $a - bv$ y c.

Finalmente se repite este procedimiento para todas las raíces de c por lo cual R es una función polinomial.

□

Teorema 1.42. *Sea $D \in Div^0(C)$. Entonces existe un único D_1 divisor reducido tal que $D \sim D_1$.*

DEMOSTRACIÓN. (Existencia) Sea D' un divisor semirreducido obtenido como en el teorema 1.34. Luego $|D'| \leq |D|$ si $|D'| \leq g$, entonces D' es reducido, de otra manera sean $P_1, P_2, \ldots, P_{g+1}$ puntos finitos en $supp(D')$ no necesariamente distintos y sean a, b tal que $div(a, b)$ es la representación de

$$P_1 + P_2 + \ldots + P_{g+1} - (g + 1)P_\infty$$

dados como en el teorema 1.39, y como $gr_u(b) \leq g$ se sigue que $gr_u(b(u) - v) = 2g + 1$, luego

$$div(b - v) = P_1 + P_2 + \cdots + P_{g+1} + Q_1 + \cdots + Q_g - (2g + 1)P_\infty$$

para algunos Q_i's. Substrayendo estos de D' se define D'' donde $D'' \sim D' \sim D$ y $|D''| < |D'|$ así si $|D''| < g$, se tiene el resultado. En caso contrario se repite el procedimiento hasta obtener el divisor reducido.

(Unicidad) Suponga que D_1, D_2 son dos divisores reducidos tales que $D_1 \sim D_2$ y además $D_1 \neq D_2$. Ahora bien, sea D_3 un divisor semirreducido y principal tal que $D_3 \sim D_1 - D_2$. Como $D_1 \neq D_2$ existe P tal que $ord_P(D_1) \neq ord_P(D_2)$ sin pérdida de generalidad suponga que $ord_P(D_1) = m_1 \geq 1$ y además se cumple una de las siguientes condiciones, ya que D_2 es un divisor reducido:

- $ord_P(D_2) = ord_{\widetilde{P}}(D_2) = 0$, entonces $ord_P(D_3) = m_1 \geq 1$
- $m_1 > ord_P(D_2) = m_2 \geq 1$ lo que implica $ord_P(D_3) = m_1 - m_2$
- $m_1 > ord_{\widetilde{P}}(D_2) = m_2 \geq 1$, con lo cual $ord_P(D_3) = m_1 + m_2$

En todos los casos se tiene que $ord_P(D_3) \geq 1$ y así $D_3 \neq 0$ y también $|D_3| \leq |D_1 - D_2| \leq |D_1| + |D_2| \leq 2g$. Sea G una función racional tal que $div(G) = D_3$ la cual existe pues D_3 es principal, además como G no tiene polos finitos entonces G es una función polinomial y de esta forma $G = a - bv$ pero como $gr(G) \leq 2g$, entonces $b = 0$ y así $G \in \overline{K}[u]$. Si se supone que $gr_u(a) \geq 1$, entonces existe $x \in \overline{K}$ que es raíz de $a(u)$, por lo cual $P = (x, y) \in C$, si P es ordinario entonces P y $\widetilde{P}$ son ceros de G lo cual contradice que D_3 es semirreducido. Si P es un punto especial se tiene $ord_P(G) = 2$ que también contradice que D_3 es semirreducido; con lo cual se concluye que $gr_u(a) = 0$ y así $D_3 = 0$. □

1.4.1. La aritmética

Como se ha visto cada elemento de la Jacobiana tiene sólo un divisor reducido, por lo cual se tomarán estos como representantes, y se verá como sumar dos divisores reducidos de tal forma que el resultado sea otro divisor reducido.

Definición 1.43. *Un divisor $D = \sum m_P P$ se dice que está definido sobre $\mathbb{K}$ si $D^\sigma = \sum m_P P^\sigma = D$ para todo automorfismo σ de $\overline{\mathbb{K}}$ sobre $\mathbb{K}$.*

Algoritmo 1.44.
Entrada: Divisores reducidos $D_1 = div(a_1, b_2)$ y $D_2 = div(a_2, b_2)$ definidos sobre $\mathbb{K}$

1. *Mediante el algoritmo extendido de Euclides se obtienen d_1,e_1, $e_2 \in K[u]$ donde $d_1 = mcd(a_1, a_2)$ y $d_1 = e_1 a_1 + e_2 a_2$*
2. *Mediante el algoritmo extendido de Euclides se obtienen d, c_1, $c_2 \in K[u]$ donde $d = mcd(d_1, b_1 + b_2 + h)$ y $d = c_1 d_1 + c_2(b_1 + b_2 + h)$*
3. *Sea $s_1 = c_1 e_1$, $s_2 = c_1 e_2$ y $s_3 = c_2$*
4. *Sean*
$$a' = \frac{a_1 a_2}{d^2}$$
$$b' = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \mod a'$$
5. *Mientras $gr_u(a') > g$ hacer*
   - $a = a'$ y $b = b'$

- *Defina*

$$a' = \frac{f - bh - b^2}{a}$$

$$b' = (-h - b) \mod a'$$

6. *Sea c el coeficiente líder de a'. Tomar $a' = c^{-1}a'$*
7. *Obtener $D = div(a', b')$*

Salida: D es un divisor reducido tal que $D \sim D_1 + D_2$

Este algoritmo se debe en diferentes etapas a Neal Koblitz en [**22**], David G. Cantor en [**12**] y Menezes, Wu y Zuccherato en [**29**], presentado por claridad en dos partes, en la primera suman dos divisores reducidos y da como resultado un divisor semirreducido, en tanto la segunda parte transforma un divisor semirreducido a uno reducido.

Ejemplo 1.45. *Considere la curva hiperelípticas C_3 del ejemplo 1.11 y considérense los divisores $D_1 = (0, 22) - P_\infty$ y $D_2 = (1, 8) - P_\infty$. Entonces según el teorema 1.39 se tiene que para D_1 se define $a_1(u) = (u-0) = u$ y $b_1(u) = 22$, ($a_1(u) = u$ divide a $b_1^2 + b_1 h - f = 22^2 + 22u - u^5 - u - 1 = 21u - u^5$) y para D_2 se tiene que $a_2(u) = (u-1)$ y $b_2(u) = 8$, ($a_2(u) = (u-1)$ divide a $b_2^2 + b_2 h - f = 8^2 + 8u - u^5 - u - 1 = 17 + 7u - u^5$). Así pues se se procede como sigue:*

1. *Se tiene que $gcd(u, u-1) = 1$ y además $1 = u - (u-1)$ es decir $d_1 = 1$, $e_1 = 1$, $e_2 = -1$.*
2. *Además $gcd(1, 22 + 8 + u) = 1$ y $1 = (u+8)(1) + (-1)(u+7)$ con lo que $d = 1$, $c_1 = (u+8)$, $c_2 = (-1)$.*
3. *Se define $s_1 = (u+8)(1) = u + 8$, $s_2 = (u+8)(-1) = -u - 8$, $s_3 = -1$*
4. *Así*

$$a = \frac{u(u-1)}{1} = u^2 - u$$

$$b = \frac{(u+8)(u)8 + (-u-8)(u-1)22 - 1(22(8) + u^5 + u + 1)}{1} \mod (u^2 - u)$$

es decir

$$b = 8u^2 + 18u + u^2 + 7u - 8 + 8 - u^5 - u - 1 \mod u^2 - u$$

por lo que $b = 9u - 1$

5. *Como $2 = gr_u(a') \not> g = 2$ entonces se tiene que*
6. *$div(a'(u)) = div(u(u-1)) = (0, 1) + (0, 22) + (1, 8) + (1, 14) - 4P_\infty$*
7. *Para algunos $x_1, x_2, x_3, y_1, y_2, y_3 \in \overline{\mathbb{F}}_{23}$*

$$div(b'(u) - v) = div(9u - 1 - v)$$
$$= (0, 22) + (1, 8) + (x_1, y_1) + (x_2, y_2) + (x_3, y_3) - 5P_\infty$$

8. $D = div(a', b') = (0, 22) + (1, 8) - 2P_\infty$

el cual era el resultado esperado.

Estos son los resultados básicos que se ocupan en este trabajo, sin embargo en los capítulos siguientes se darán otros resultados necesarios en el desarrollo.

Capítulo 2

Sistemas Criptográficos

El desarrollo de las computadoras aceleró la investigación de nuevos sistemas criptográficos seguros y prácticos para la comunicación digital. Como consecuencia a petición del National Institute of Standards and Technology (NIST) de los Estados Unidos de América, en 1975 surgió un estándar el cual se conoce como "DES"(Data Encryption Standard) [**10**], [**11**], [**33**]. Otros esquemas de gran importancia por su uso son, el creado por Ronald Rivest, Adi Shamir y Leonard Adleman [**10**], [**36**] conocido como RSA, y el esquema ElGamal propuesto en 1984 por Taher ElGamal [**14**].

En este capítulo, en primera instancia se presentan algunas funciones hash utilizadas en criptografía, las cuales son de especial importancia pues permiten un adecuado manejo de los datos. Después se describen algunos de los sistemas de llave pública, primero el RSA y después el sistema ElGamal, y se exponen los problemas que surgen al implementar este último, considerando principalmente el grupo de puntos racionales de una curva elíptica. Finalmente, se presenta la firma digital propuesta por ElGamal.

2.1. Funciones Hash

Las funciones hash son de gran importancia en muchos de los sistemas criptográficos, cuya función principal es como códigos de detección de modificación, ya que permiten estandarizar el tamaño de los datos que se manejan, otras aplicaciones de este tipo de funciones se da en bases de datos para realizar búsquedas de manera eficiente. En criptografía estas funciones son usadas principalmente en la firma digital y en algunos esquemas como el Boneh-Franklin. Una función hash ó función resumen, esencialmente se puede ver como una proyección de un conjunto con una cantidad arbitraria de elementos sobre otro de tamaño fijo. Para propósitos criptográficos es importante que tenga las siguientes propiedades que se detallan mas adelante [**10**]:

- Eficiente cálculo computacional
- Ser de un sólo sentido.
- Determinar una colisión es difícil.

En la presente sección se considerara que Σ es un alfabeto. Una función hash es un mapeo de la forma:

$$h : \Sigma^? \to \Sigma^n, \qquad n \in \mathbb{N} \tag{34}$$

donde $\Sigma^?$ indica que la longitud del vector no esta determinada, es decir, que a la función no le importa si la entrada es un vector de un espacio de dimensión 10 o de un espacio de dimensión 1000000, lo cual se puede ver como:

$$\Sigma^? = \cup_{n=0}^{\infty} \Sigma^n$$

Por una *función de un sólo sentido*, se entenderá que no es factible determinar la inversa de h, es decir, que dado $s \in \Sigma^n$ no es computacionalmente factible encontrar $x \in \Sigma^?$ tal que $s = h(x)$.

Una *colisión* de h es un par $(x, x') \in \Sigma^? \times \Sigma^?$ para el cual $x \neq x'$ y además $h(x) = h(x')$. Todas las funciones hash presentan colisiones ya que claramente $\Sigma^n \subsetneq \Sigma^?$ y por ende no son inyectivas.

Definición 2.1. *Una función h es débilmente resistente a colisiones si dado $x \in \Sigma^?$ la probabilidad de obtener x' tal que (x, x') es una colisión, es pequeña.*

Definición 2.2. *Una función h es fuertemente resistente a colisiones si la probabilidad de encontrar cualquier colisión (x, x'), es pequeña.*

Nótese que en el caso de que h sea una función débilmente resistente a colisiones dado un valor x únicamente se busca otro valor y con $x \neq y$ tal que $h(x) = h(y)$, en tanto que la función sea fuertemente resistente a colisiones sólo bastara buscar un par de valores $x \neq y$ tales que $h(x) = h(y)$.

Esto indica que si una función es fuertemente resistente a colisiones, entonces también será débilmente resistente a colisiones, pero si una función es débilmente resistente a colisiones no necesariamente será fuertemente resistente. Suponga que se desea encontrar una colisión de x, $h(x) = y$, y en la búsqueda se encuentran los valores de h para $x_1, x_2, \cdots, x_n$ se tiene que $h(x_i) \neq y \quad \forall i$ pero $h(x_l) = h(x_k)$ para algunos valores de l y k, entonces la función sera débilmente resistente a colisiones pero no fuertemente.

Ejemplo 2.3. *Un ejemplo sencillo de función hash más no útil criptográficamente es el siguiente.*

$$h : \mathbb{F}_2^? \to \mathbb{F}_2^n, \qquad (b_1, b_2, \cdots, b_k) \mapsto b_1 \oplus b_2 \oplus \cdots \oplus b_k \tag{35}$$

de donde:

$$(10101110) \mapsto 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 1$$
$$(101010) \mapsto 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 1$$
$$(10101110001) \mapsto 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 = 0$$
$$(01110) \mapsto 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 1$$

El principal inconveniente de esta función es que es muy fácil encontrar colisiones.

Para determinar la probabilidad de encontrar una colisión en una función hash se utiliza el ataque del cumpleaños, basado en la paradoja del cumpleaños, esto es, que en un grupo de 23 personas la probabilidad de encontrar dos personas que cumplan años el mismo día es mayor a 0.5. Para conseguir esto, en una función hash es necesario tener un conjunto de k elementos tal que

$$k \geq \frac{1 + \sqrt{1 + (8 \ln 2)|\Sigma|^n}}{2} \tag{36}$$

Para ver esto se considera lo siguiente. Sea $\mathcal{A} \subset \Sigma^?$ de cardinalidad k. Sea h una función hash como en (34). Luego la probabilidad de que $|h(\mathcal{A})| = k$ es

$$\prod_{i=0}^{k-1} \frac{\eta - i}{\eta} \text{ donde } \eta = |\Sigma|^n \tag{37}$$

de donde se observa que:

$$\prod_{i=0}^{k-1} \frac{\eta - i}{\eta} = \prod_{i=0}^{k-1} (1 - \frac{i}{\eta}) \leq \prod_{i=0}^{k-1} e^{-i/\eta} = e^{\frac{-k(k-1)}{2\eta}}$$

y como se quiere que la probabilidad sea menor a 0.5 entonces basta con que se cumpla que $\frac{-k(k-1)}{2\eta} \leq -ln(2)$ y de aquí se obtiene (36).

De esta manera, para prevenir este tipo de ataques, cuando $\Sigma = \{0, 1\}$ se requiere que el cálculo de $2^{n/2}$ valores no sea factible computacionalmente [**10**], la factibilidad computacional se puede ver en el Apéndice B.

2.1.1. Funciones hash a partir de funciones de compresión

Las funciones de compresión difieren un poco a las funciones hash, y esta diferencia se presenta únicamente en el dominio, en este caso la "longitud" del dominio es fija, es decir, es una función de la forma:

$$g : \Sigma^m \to \Sigma^n \qquad m > n \tag{38}$$

de igual manera en estas funciones se tendrán colisiones, y se define de forma similar que una función sea fuerte ó débilmente resistente a colisiones.

La importancia de las funciones de compresión es que a partir de estas se pueden construir funciones hash. Para ilustrar esto se considera $\Sigma = \mathbb{F}_2$ y la idea de cómo hacerlo se da a continuación.

Notación 2.4.
Sea x un número entero y sea $x_1x_2\cdots x_l$ la representación binaria de x entonces $|x|_2 = l$. Además, si x es la cadena de bits $x_1x_2\cdots x_l$, su longitud se denotará de igual forma, es decir, $|x|_2 = l$.

Sean g una función de compresión como en (38) y $r = m - n$, dado que se desea construir h_g de la forma (35), se considera $x \in \mathbb{F}_2^?$, y se define $l = |x|_2$, luego existen $s, t \in \mathbb{N} \cup \{0\}$ únicos tales que $l = sr + t$ y $0 \leq t < r$. Si $t \neq 0$ se le agregan $r - t$ ceros al principio de x, en caso contrario se queda igual. Por otro lado, se considera la expansión binaria de l y se agregan ceros de tal forma que la longitud sea divisible por $r-1$ y a cada bloque de longitud $r-1$ se le agrega un 1. Se concatenan ambos arreglos, teniendo como resultado un arreglo $\widehat{x}$ de longitud divisible por r. Considerando que $|\widehat{x}|_2 = kr$, este arreglo se puede ver como:

$$\widehat{x} = x_1|x_2|\cdots|x_k, \qquad x_i \in \mathbb{F}_2^r \tag{39}$$

Con esto se define la sucesión en $\mathbb{F}_2^n$ dada por $h_0 = \overline{0}$, $h_i = g(h_{i-1}|x_i)$ y finalmente

$$h_g(x) = h_k \tag{40}$$

Ejemplo 2.5. *Defina la función de compresión como:*

$$g : \mathbb{F}_2^6 \to \mathbb{F}_2^3, \qquad (x_1, x_2, x_3, x_4, x_5, x_6) \mapsto (x_3 + x_4, x_1 + x_5, x_2 + x_6)$$

y evalué $h_g(0101010101011)$.

Solución.

En este caso se tiene que $m = 6, n = 3, r = 3$ y $x = 0101010101011$ luego $|x|_2 = 13$ por lo que se agregan dos ceros obteniendo la cadena

$$000\ 101\ 010\ 101\ 011$$

Por otro lado, se tiene que $13_2 = 1101$, lo cual indica que $|13|_2 = 4$, por lo que se agregan unos resultando

$$111\ 101$$

haciendo la concatenación se obtiene

$$000\ 101\ 010\ 101\ 011\ 111\ 101$$

y se calcula la sucesión h_i

$$\begin{array}{ll} h_0 = 000 & h_4 = g(100\ 101) = (111) \\ h_1 = g(000\ 000) = (000) & h_5 = g(111\ 011) = (100) \\ h_2 = g(000\ 101) = (101) & h_6 = g(100\ 111) = (101) \\ h_3 = g(101\ 010) = (100) & h_7 = g(101\ 101) = (011) \end{array}$$

así pues, $h_g(0101010101011) = (011)$ ■

De forma similar se puede definir la siguiente función hash.

Definición 2.6. *Defina la función de compresión como:*

$$g : \mathbb{Z}_p^2 \to \mathbb{Z}_p, \qquad (x_1, x_2) \mapsto (x_1 * x_2 + x_1 + x_2) \mod p \tag{41}$$

defina la sucesión como $h_0 = q$ para algún $q \in \mathbb{Z}_p$ y $h_i = g(h_{i-1}, x_i)$ y sea

$$h_g : \mathbb{Z}_p^? \to \mathbb{Z}_p, \qquad (x_1, ..., x_k) \mapsto h_k$$

Ejemplo 2.7. *Defina la función de compresión como:*

$$g : \mathbb{Z}_{757}^2 \to \mathbb{Z}_{757}, \qquad (x_1, x_2) \mapsto (x_1 * x_2 + x_1 + x_2) \mod 757$$

y defina la sucesión como $h_0 = 355$ y $h_i = g(h_{i-1}, x_i)$. Evaluar $h_g(181, 273, 281, 704)$.

Solución.

Para determinar la compresión se calcula la sucesión h_i como sigue:

- $h_0 = 355$
- $h_1 = g(355, 181) = 355 * 181 + 355 + 181 = 446$
- $h_2 = g(446, 273) = 446 * 273 + 446 + 273 = 600$
- $h_3 = g(600, 281) = 600 * 281 + 600 + 281 = 137$
- $h_4 = g(137, 704) = 137 * 704 + 137 + 704 = 393$

así pues $h_g(181, 273, 281, 704) = 393$ ■

Existen varias funciones hash que son usadas para fines criptográficos entre las cuales destacan MD-4, MD-5, SHA-0, SHA-1, Tiger-128, Tiger-160 y Whirlpool [4], [11], [38]. Para tener en cuenta lo que hay detrás de estas funciones se explicará la metodología de dos de ellas. MD-5, por su gran popularidad que tiene y ser similares a las demás, y Whirlpool, por ser de reciente creación.

2.1.2. MD-5

La función MD-5 (Message-Digest Algorithm 5), devuelve una cadena de 128 bits. Fue desarrollada por Rivest en 1991, debido a que en el MD-4 se observaron deficiencias importantes. Con el avance de la computación se ha encontrado que MD-5 también presenta algunas deficiencias. El esquema del MD-5 es el siguiente:

Esquema 2.8. [38]*MD-5*

1: *Entrada. El mensaje m de longitud arbitraria n.*

2: *Parámetros iniciales,* $A, B, C, D \in \mathbb{F}_2^{32}$ $F, G, H, I : \mathbb{F}_2^{32} \times \mathbb{F}_2^{32} \times \mathbb{F}_2^{32} \to \mathbb{F}_2$

- $A = 00000001\ 00100011\ 01000101\ 01100111$
- $B = 10001001\ 10101011\ 11001101\ 11101111$
- $C = 11111110\ 11011100\ 10111010\ 10011000$
- $D = 01110110\ 01010100\ 00110010\ 00010000$
- $F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$ $\quad H(X,Y,Z) = X \oplus Y \oplus Z$
- $G(X,Y,Z) = (X \wedge Z) \vee (\neg Z \wedge Y)$ $\quad I(X,Y,Z) = Y \oplus (X \vee \neg Z)$
- $T(i) = [2^{32}|sen(i)|]$ *donde i se considera en radianes.*

3: *Procedimiento*

- $r \equiv n(\mod 512)$
- $m' = 100\cdots0$, *si* $r < 448$ *entonces* $m' \in \mathbb{F}_2^{448-r}$ *de otra forma* $m' \in \mathbb{F}_2^{960-r}$
- $b' = [n]_2$ *(representación binaria de n de longitud 64)*
- $m' = m|m'|b'$ *(m' tiene longitud un múltiplo de 512)*
- $k = \frac{|m'|_2}{512}$ *(ver notación 2.4)*
- $m' = m'_0|m'_1|\cdots|m'_{k-1}$ *con* $m'_i \in \mathbb{F}_2^{512}$
- *Para* $j = 0$ *hasta* $k-1$ *hacer*
  - $m'_j = X_0|X_1|\cdots|X_{15}$ *con* $X_i \in \mathbb{F}_2^{32}$
  - *Para* $i = 0$ *hasta* 15*:*
    - *Hacer* $A' = A$, $B' = B$, $C' = C$, $D' = D$.
    - *Para* $j = 0$ *hasta* 3 *hacer:*
      - $A = B + ROT((A + F(B,C,D) + X[j*4] + T[j*4+1]), 7)$
      - $D = A + ROT((D + F(A,B,C) + X[j*4+1] + T[j*4+2]), 12)$
      - $C = D + ROT((C + F(D,A,B) + X[j*4+2] + T[j*4+3]), 17)$
      - $B = C + ROT((B + F(C,D,A) + X[j*4+3] + T[j*4+4]), 22)$
    - *Para* $j = 0$ *hasta* 3 *hacer:*

- $A = B + ROT((A + G(B,C,D) + X[j*4+1] + T[j*4+17]), 5)$
- $D = A + ROT((D + G(A,B,C) + X[j*4+6 \mod 16] + T[j*4+18]), 9)$
- $C = D + ROT((C + G(D,A,B) + X[j*4-5 \mod 16] + T[j*4+19]), 14)$
- $B = C + ROT((B + G(C,D,A) + X[j*4] + T[j*4+20]), 20)$

- *Para* $j = 0$ *hasta* 3 *hacer:*
  - $A = B + ROT((A + H(B,C,D) + X[j*12+5 \mod 16] + T[j*4+33]), 4)$
  - $D = A + ROT((D + H(A,B,C) + X[j*12+8 \mod 16] + T[j*4+34]), 11)$
  - $C = D + ROT((C + H(D,A,B) + X[j*12-5 \mod 16] + T[j*4+35]), 16)$
  - $B = C + ROT((B + H(C,D,A) + X[j*12-2 \mod 16] + T[j*4+36]), 23)$
- *Para* $j = 0$ *hasta* 3 *hacer:*
  - $A = B + ROT((A + I(B,C,D) + X[j*12 \mod 16] + T[j*4+49]), 6)$
  - $D = A + ROT((D + I(A,B,C) + X[j*12+7 \mod 16] + T[j*4+50]), 10)$
  - $C = D + ROT((C + I(D,A,B) + X[j*12-2 \mod 16] + T[j*4+51]), 15)$
  - $B = C + ROT((B + I(C,D,A) + X[j*12+5 \mod 16] + T[j*4+52]), 21)$
- $A = A + A'$
- $B = B + B'$
- $C = C + C'$
- $D = D + D'$

4: *Salida*

- $H = A|B|C|D$

Observaciones:

La función $ROT(\overline{a}, k)$ indica un corrimiento circular del vector $\overline{a}$ en k posiciones a la izquierda.

La inicialización de las variables A, B, C, D, corresponde a las expresiones binarias de:

$$A = 0|\ 1|\ 2|\ 3|\ 4|\ 5|\ 6|\ 7$$
$$B = 8|\ 9|10|11|12|13|14|15$$
$$C = 15|14|13|12|11|10|\ 9|\ 8$$
$$D = 7|\ 6|\ 5|\ 4|\ 3|\ 2|\ 1|\ 0$$

Las funciones F y G son equivalentes en el sentido de que

$$G(X,Y,Z) = F(Z,X,Y) \tag{42}$$

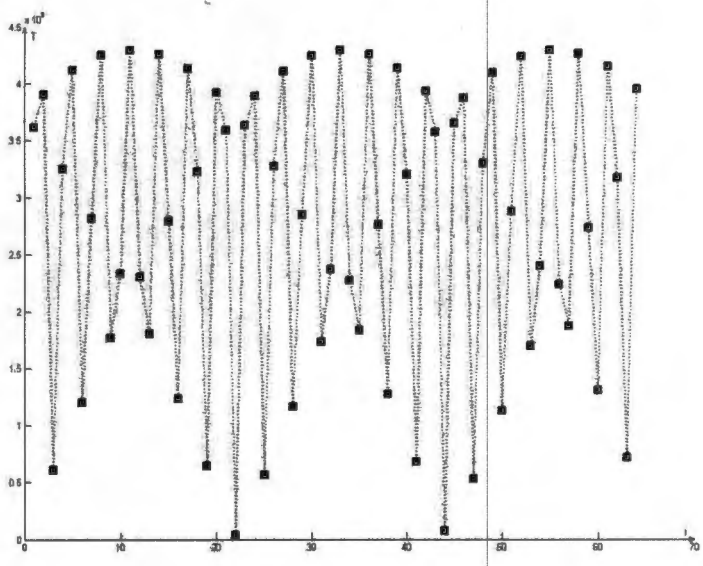

FIGURA 1. Distribución de la sucesión T[i] de MD-5

además es fácil ver, observando las tablas de verdad, que las cuatro funciones, F, G, H, I son balanceadas, es decir, todas las salidas tienen la misma probabilidad de salir.

La sucesión $T[i]$ tiene como objetivo alterar un poco los valores que se van obteniendo, la distribución de esta sucesión se muestra en la figura 1.

Ejemplo 2.9. *MD5*

Si se desea encontrar el valor del vacío en el MD-5 se obtiene:

$$d41d8cd98f00b204e9800998ecf8427e$$

Si se desea obtener el hash de 1011101010011 *usando MD-5 se tiene el valor:*

$$2d56d4c5a992c05e0a16fff997596750$$

Estos valores están dados en representación hexadecimal y los resultados fueron calculados en [17].

2.1.3. Whirlpool

La función hash Whirlpool fue diseñada por Vincent Rijmen y Paulo S. L. M. Barreto [4]. El uso de esta función se recomienda para arreglos

de bits de longitud menor a 2^{256} y produce una salida de 512 bits. Esta función se define mediante un algoritmo de dominio público [4]. Su nombre se debe a la galaxia del mismo nombre en la constelación Canes Venatici la cual fue descubierta por Charles Messier el 13 de octubre de 1773.

Al igual que el MD-5 este se basa en la construcción de una función de compresión. El funcionamiento es el siguiente: a la cadena original se le agrega al final un 1 y una cadena de ceros hasta que la longitud de la cadena sea congruente con 256 módulo 512. Posteriormente se le agrega la expresión binaria en $\mathbb{F}_2^{256}$ de la longitud original del mensaje, consiguiendo de esta forma una sucesión $\{m_i\}$ en $\mathbb{F}_2^{512}$ tal que:

$$m = m_1|m_2|m_3|\cdots|m_t \tag{43}$$

y en base a esto se crea otra sucesión $\{H_i\}$ definida como:

$$H_i = W[H_{i-1}](m_i) \oplus H_{i-1} \oplus m_i \tag{44}$$

Donde $H_0 = \overline{0} \in \mathbb{F}_2^{512}$.

La salida de la función hash Wirhpool es H_t.

Para describir la función $W[K]$, que aparece en la ecuación (44), se hacen algunas consideraciones y se definen primero unas funciones y constantes.

Para esto es conveniente fijar la siguiente notación.

Notación 2.10.

Para polinomios binarios. Sea $u(x) = \sum_{i=0}^{m-1} u_i x^i \in \mathbb{N}[x]$ *donde* $u_i \in \{0,1\}$ *y sea* $z = u(2)_{16}$*, es decir, el valor de* u *en* 2 *en notación hexadecimal, este polinomio se representará de la forma* $u(x) := z_x$*, el cual se puede considerar como un polinomio en* $\mathbb{F}_2[x]$.

Por ejemplo, el polinomio $p_4(x) = x^4 + x + 1$ tiene la representación 13_x, el polinomio $p_8(x) := x^8 + x^4 + x^3 + x^2 + 1$ está dado por $11D_x$ y el polinomio $q_8(x) := x^8 + x^4 + x^3 + x + 1$ mediante $11B_x$.

Los elementos en $\mathbb{F}_{2^8}$ se podrán representar como rs_β, donde $\beta \in \mathbb{F}_{2^8}$ es una raíz del polinomio $p_8(x)$, el cual es irreducible primitivo. Además, se denotará con $\zeta \in \mathbb{F}_{2^8}$ a una raíz del polinomio $q_8(x)$, que es irreducible pero no primitivo. De igual manera, los elementos en $\mathbb{F}_{2^4}$ se podrán representar como r_α, donde $\alpha \in \mathbb{F}_{2^4}$ es una raíz del polinomio $p_4(x)$, el cual también es irreducible primitivo.

Para un mejor manejo de los m_i's se observa que, $\mathbb{F}_2^{512} \cong (\mathbb{F}_2^8)^{64} \cong (\mathbb{F}_{2^8})^{64}$ y se define el mapeo $\mu : (\mathbb{F}_{2^8})^{64} \to \widetilde{\mathcal{M}} = M_{8\times 8}(\mathbb{F}_{2^8})$ definido como $\mu(\overline{a}) = B$ tal que $b_{i,j} = a_{8i+j}$ con $0 \leq i, j \leq 7$. De esta forma los m_i's se pueden considerar como matrices.

Por una *matriz circulante*, denotada por $cir(\overline{a})$, se entenderá la matriz cuyas entradas se definen como $c_{i,j} = a_{j-i \bmod n}$, donde $\overline{a} = (a_1, a_2, \ldots, a_{n-1})$.

La función Whirpool usa una caja de sustitución, S-Box, definida sobre $\mathbb{F}_2^8$, la cual se denotará con S. Para definir esta S-box, se utilizan dos S-box, E y R, definidas sobre $\mathbb{F}_2^4$ las cuales interactúan como se muestra en la figura 2 para definir a S. Las permutaciones se pueden representar de diversas maneras, una de ellas es el polinomio de permutación que se presentan a continuación:

- E se obtiene mediante los polinomios:
  $1 + Ex + 5x^2 + Cx^3 + 6x^4 + Bx^5 + x^6 + 2x^7 + 5x^9 + 2x^{10} + Bx^{11} + Ex^{12} + 2x^{13} + 3x^{14}$
  ó
  $1 + \alpha^{11}x + \alpha^8x^2 + \alpha^6x^3 + \alpha^5x^4 + \alpha^7x^5 + x^6 + \alpha x^7 + \alpha^8x^9 + \alpha x^{10} + \alpha^7x^{11} + \alpha^{11}x^{12} + \alpha x^{13} + \alpha^4x^{14}$
- E^{-1} se obtiene mediante los polinomios:
  $F + 3x + Ax^2 + x^3 + Ex^4 + Bx^5 + 7x^6 + 4x^7 + 2x^8 + Bx^9 + 4x^{10} + 2x^{11} + 7x^{12} + Cx^{13} + Fx^{14} + Ax^{15}$
  ó
  $\alpha^{12} + \alpha^4x + \alpha^9x^2 + x^3 + \alpha^{11}x^4 + \alpha^7x^5 + \alpha^{10}x^6 + \alpha^2x^7 + \alpha x^8 + \alpha^7x^9 + \alpha^2x^{10} + \alpha x^{11} + \alpha^{10}x^{12} + \alpha^6x^{13} + \alpha^{12}x^{14} + \alpha^9$
- R se obtiene mediante los polinomios:
  $7 + Ax + 7x^2 + 2x^3 + 6x^4 + 7x^5 + 6x^6 + 4x^7 + Ax^8 + Dx^9 + 8x^{11} + 4x^{12} + Bx^{13} + 6x^{14}$
  ó
  $\alpha^{10} + \alpha^9x + \alpha^{10}x^2 + \alpha x^3 + \alpha^5x^4 + \alpha^{10}x^5 + \alpha^5x^6 + \alpha^2x^7 + \alpha^9x^8 + \alpha^{13}x^9 + \alpha^3x^{11} + \alpha^2x^{12} + \alpha^7x^{13} + \alpha^5x^{14}$
- S se puede obtener mediante diversos polinomios, los cuales se presentan en el Apéndice A.

Las S-boxes sobre $\mathbb{F}_2^4$ expresadas como tablas son:

u	0_β	1_β	2_β	3_β	4_β	5_β	6_β	7_β	8_β	9_β	A_β	B_β	C_β	D_β	E_β	F_β
$E(u)$	1_β	B_β	9_β	C_β	D_β	6_β	F_β	3_β	E_β	8_β	7_β	4_β	A_β	2_β	5_β	0_β

u	0_β	1_β	2_β	3_β	4_β	5_β	6_β	7_β	8_β	9_β	A_β	B_β	C_β	D_β	E_β	F_β
$R(u)$	7_β	C_β	B_β	D_β	E_β	4_β	9_β	F_β	6_β	3_β	8_β	A_β	2_β	5_β	1_β	0_β

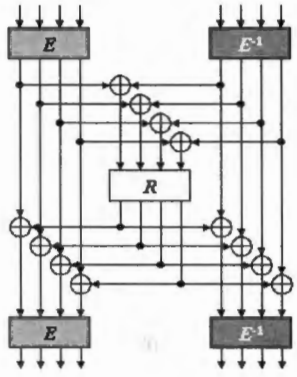

FIGURA 2. Esquema de la simplificación de la S-Box usada

La permutación E, se puede obtener mediante una relación simple a partir de la representación de los elementos en el campo $\mathbb{F}_{2^4}$ dada por:

$$E(u) = \begin{cases} 0, & \text{si } u = F_\alpha; \\ \alpha^{7*\phi(u)}, & \text{en otro caso} \end{cases} \tag{45}$$

donde

$$\phi\left(\sum_{i=0}^{3} a_i \alpha^i\right) = \sum_{i=0}^{3} a_i 2^i \tag{46}$$

Las otras funciones utilizadas en la definición de la función $W[K]$, son:

Una *función no lineal* γ definida como:

$$\gamma : \widetilde{\mathcal{M}} \to \widetilde{\mathcal{M}} \qquad A \mapsto B = [b_{i,j} = S(a_{i,j})] \tag{47}$$

Una *permutación cíclica* π, de orden 8, definida como:

$$\pi : \widetilde{\mathcal{M}} \to \widetilde{\mathcal{M}} \qquad A \mapsto B = [b_{i,j} = a_{(i-j \mod 8),j}] \tag{48}$$

Una *función de difusión* θ dada por:

$$\theta : \widetilde{\mathcal{M}} \to \widetilde{\mathcal{M}} \qquad A \mapsto A \cdot C \tag{49}$$

donde $C = cir(01_x, 01_x, 04_x, 01_x, 08_x, 05_x, 02_x, 09_x)$.

Una *función de adición*, la cual depende de una matriz $K \in \widetilde{\mathcal{M}}$, denotada como $\sigma[K]$ definida por:

$$\sigma[K] : \widetilde{\mathcal{M}} \to \widetilde{\mathcal{M}} \qquad A \mapsto A \oplus K \tag{50}$$

Una *función ronda* ρ, la cual consiste en la composición de las anteriores funciones:

$$\rho[K] = \sigma[K] \circ \theta \circ \pi \circ \gamma \tag{51}$$

Las constantes que son necesarias son las siguientes:

$$C^r \in \widetilde{\mathcal{M}} \qquad r > 0 \tag{52}$$

$$c^r_{0,j} \equiv S[((8(r-1)+j)_{16})_\alpha] \qquad 0 \leq j \leq 7 \tag{53}$$

$$c^r_{i,j} \equiv 0 \qquad 1 \leq i \leq 7 \quad 0 \leq j \leq 7 \tag{54}$$

Finalmente se define la *sucesión de expansión* denotada por $\{K^i\}$, dada $K \in \widetilde{\mathcal{M}}$ se considera la relación $K^r = \rho[c^r(K^{r-1})]$ donde $K^0 = K$.

La función $W[K]$, llamada *función de cifrado*, está dada por:

$$\begin{gathered} W[K] : \widetilde{\mathcal{M}} \to \widetilde{\mathcal{M}} \\ W[K] \mapsto \rho[K^R] \circ \rho[K^{R-1}] \circ \cdots \rho[K^1] \circ \sigma[K^0] \end{gathered} \tag{55}$$

En la definición de la función de cifrado, Barreto y Rijmen recomiendan que $R = 10$, sin embargo mencionan que en general se puede tomar cualquier valor [4].

2.2. Criptosistemas de llave pública

La mayoría de los criptosistemas de llave pública están basados en la intratabilidad computacional de problemas de Teoría de Números, es decir no es posible resolver el problema mediante el uso de computadoras actuales en un tiempo razonable. En ocasiones estos problemas se combinan con otras áreas como es el caso de la criptografía de curvas

elípticas. Los principales problemas utilizados son: el problema de la factorización entera y el problema del logaritmo discreto.

Los esquemas de llave pública se basan en la idea de que cada usuario tendrá asignadas dos llaves. Una será de uso exclusivo del usuario y solo él la conocerá; como el nip de una tarjeta de crédito; por lo que se le denomina *llave privada.* La segunda se denomina *pública* ya que estará disponible para cualquier entidad; como el número de cuenta asociado a la tarjeta; al igual que el esquema usado para el cifrado. Además, no deberá ser factible determinar la llave privada a partir de los datos públicos, lo cual se logra en base a la intratabilidad de los problemas mencionados.

El Problema de la factorización entera consiste en dado $n \in \mathbb{N}$ encontrar todos los factores primos de n.

Ejemplo 2.11. *Encontrar la factorización de los siguientes números:*

- $36 = (2)^2(3)^2$
- $11,857 = (71)(167)$
- $5964848081 = 5964848081$
- $9999000099990001 = (1676321)(5964848081)$
- $1094173864157052742180970732204035761200373294544920599091384213147634998428893478471799725789126733249762575289978173379707653724402714674353159335433389 7 =?$

El problema del Logaritmo Discreto en un grupo finito consiste en determinar, si existe, solución sobre este grupo de la ecuación $a^x = b$, para a y b conocidos.

Estos problemas son la base de los esquemas que se presentan a continuación. El problema del logaritmo discreto se analiza con mayor detenimiento en la sección 3.1.

2.2.1. RSA

El sistema de cifrado RSA, desarrollado en 1978, toma el nombre de las iniciales de las personas que lo diseñaron: Ronald Rivest, Adi Shamir y Leonard Adleman [**36**]. El RSA es un sistema de llave pública y uno de los más populares y robustos el cual sirve para mantener la confidencialidad y autenticidad de la información, ha sido usado durante mucho tiempo en los sistemas bancarios entre otros. En la

actualidad es usado en protocolos de seguridad en internet y en varios software como el Adobe.

Se considerá que ϕ es la función de Euler y $\mathbb{Z}_n^*$ es el grupo de unidades en $\mathbb{Z}_n$.

Este esquema basa su seguridad en el problema de la factorización entera. Considerando el caso particular cuando el número a factorizar es del orden de 150-200 dígitos. El esquema general es el siguiente:

Esquema 2.12. *RSA*

1. *Generación de Llaves*
   a) *Obtener de forma aleatoria p y q dos primos distintos.*
   b) *Calcular $n = pq$ y $\phi(n) = (p-1)(q-1)$*
   c) *Seleccionar $e \in \mathbb{Z}_{\phi(n)}^*$*
   d) *Calcular $d = e^{-1}$ en $\mathbb{Z}_{\phi(n)}^*$*
   e) *La llave pública es (n, e) y la privada es (d)*
2. *Cifrado*
   a) *Expresar el mensaje a cifrar como $m \in \mathbb{Z}_n$*
   b) *Calcular $c = m^e \mod n$, que será el mensaje cifrado.*
3. *Descifrado*
   a) *Calcular $m' \equiv c^d \mod n$, el cual es el mensaje original.*

En el descifrado se recuperá realmente el mensaje ya que:

$$m' \equiv c^d \mod n \equiv m^{ed} \mod n \equiv$$
$$m^{k\phi(n)+1} \mod n \equiv (m^{\phi(n)})^k m \mod n \equiv m$$

El problema de encontrar la llave privada (d) a partir de la pública (n, e) radica esencialmente en encontrar el valor de $\phi(n)$. En general, esto es sencillo sólo si se conoce la factorización de n, es decir, la seguridad del sistema se basa en la intratabilidad de la factorización de números enteros.

De esta forma, si una entidad B desea enviar información cifrada a la entidad A por medio del sistema RSA, B cifra el texto original con la llave pública, (n, e), de A y debido a que la pareja (e, d) es única, sólo la entidad A puede recuperar el texto original usando su llave privada (d).

Ejemplo 2.13. *Sean $p = 71$, $q = 167$, por lo tanto $n = pq = 11,857$ y $\phi(n) = (70)(166) = 11620$. Sea $e = 117 \in \mathbb{Z}_{11620}^*$ y se obtiene su inverso multiplicativo el cual es $d = 9733 \in \mathbb{Z}_{11620}^*$. Así pues se tendrá que la*

llave pública es (11857, 117), *y la llave para descifrar, es decir, la llave privada es* $d = 9733$. *Se desea enviar el mensaje FIN.*

Solución.

Como se desea cifrar el mensaje *FIN*, el cual usando la identificación natural del alfabeto con los enteros módulo 26, la letra F se identifica con el 6, la letra I con 9 y la letra N con el 14, es decir, el mensaje se expresa como:

$$6(26^2) + 9(26) + 14 = 4304.$$

La entidad emisora envía: $(FIN)^e = (4304)^{117} \mod n = 3689$, es decir, $3689 = 5(26^2) + 11(26) + 23$ y como el 5 corresponde a la letra E, el 11 a la letra K y el 23 a la W, el mensaje cifrado es EKW.

La entidad receptora, para recuperar el mensaje original calcula:

$$(EKW)^d = (3689)^{9733} \mod n = 4304 = FIN$$

■

2.2.2. ElGamal

Este esquema de cifrado, propuesto por Taher ElGamal en 1984 [14], está basado en el problema del logaritmo discreto, lo cual marca la importancia de este esquema. El esquema fue creado para cualquier grupo cíclico y al igual que el esquema RSA sirve para mantener la confidencialidad de la información. A continuación se presenta el esquema original:

Esquema 2.14. ElGamal

- *Generación de llaves*
  - *Obtener de forma aleatoria un primo* p *y un generador* α *de* $\mathbb{Z}_p^*$
  - *Seleccionar un entero* $a \in [1, p-1]$
  - *La llave pública es:* (p, α, α^a),
  - *La llave privada:* a
- *Pasos para el cifrado.*
  - *Representar el mensaje como un entero* $m \in \mathbb{Z}_p^*$
  - *Seleccionar un entero* $k \in [1, p-1]$
  - *Calcular* $\gamma = \alpha^k \mod p$ *y* $\delta = m(\alpha^a)^k \mod p$
  - *El mensaje cifrado será:* $C = (\gamma, \delta)$
- *Pasos para el descifrado*
  - *Calcular* $\beta = \gamma^{p-1-a}$
  - *Recuperar el mensaje* $m = \beta\delta \mod p$.

El cifrado funciona ya que:

$$\beta\delta = \gamma^{p-1-a} m(\alpha^a)^k = (\alpha^k)^{p-1-a} m\alpha^{ak} = m \tag{56}$$

y como se observa, la recuperación del mensaje depende del conocimiento de a. Para obtener el valor de a, apartir de los datos públicos $(p, \alpha, \alpha^a = \beta)$ es necesario determinar un entero n tal que $\alpha^n = \beta \mod p$, es decir obtener $log_\alpha(\beta)$, por lo cual toda la seguridad del sistema se basa en que no se pueda obtener dicho logaritmo.

Ejemplo 2.15.

Sea $p = 757$ seleccionado aleatoriamente, de igual manera se obtiene el valor de $\alpha = 17$ y el entero $a = 20$. De esta forma se tiene que $\alpha^a \equiv 17^{20} \mod 757 = 326$, así la llave pública resulta ser $(p,\ \alpha,\ \alpha^a) = (757,\ 17,\ 326)$ y la respectiva llave privada es $a = 17$. Se desea cifrar "HOLA".

Solución. Para cifrar el mensaje "HOLA" procedemos como en el ejemplo (2.13), sobre un alfabeto de 27 caracteres considerando a la $\tilde{n}$ y con la asignación habitual. De esta manera "HO LA"se tomará como $HO = H(27)+O = 8(27)+16 = 232$ y $LA = L(27)+A = 12(27)+1 = 325$. Después de esto se selecciona de forma aleatoria $k_1 = 33$ y $k_2 = 64$ y se obtiene:

$$\gamma_1 = \alpha^{k_1} = 17^{33} = 181 = FR$$

$$\gamma_2 = \alpha^{k_2} = 17^{64} = 281 = JK$$

luego se calcula:

$$\delta_1 = m_1(\alpha^a)^{k_1} = 232(326^{33}) = 273 = JC$$

$$\delta_2 = m_2(\alpha^a)^{k_2} = 325(326^{64}) = 704 = ZB$$

y de esta forma se tiene que el mensaje cifrado es: "FRJC JKZB".

Para recuperar el mensaje se calcula

$$\beta_1 = \gamma_1^{756-20} = 181^{736} = 231$$

$$\beta_2 = \gamma_2^{756-20} = 281^{736} = 51$$

finalmente se calcula

$$m_1 = \beta_1\delta_1 = 231(273) = 232 = ho$$

$$m_2 = \beta_2\delta_2 = 51(704) = 325 = la$$

■

2.3. Firma digital

En cuestiones de seguridad es importante tener la confianza de que los mensajes que uno envía o recibe solamente pueden ser entendidos por los interesados, es decir se mantiene la confidencialidad. Además es importante, cuando uno recibe el mensaje, tener una forma de verificar quién envía el mensaje es quien dice ser, se debe poder autentificar.

La autenticidad de un mensaje, así como de las entidades que participan, se da meadiante un sello ó firma. *La firma digital* realiza esta función y al igual que los esquemas de cifrado, la firma digital está basada en problemas computacionalmente intratables.

2.3.1. Firma digital de ElGamal

Al igual que el esquema de cifrado ElGamal, la firma digital de ElGamal se basa en el problema del logaritmo discreto, aún más, la generación de llaves es igual. La descripción del algoritmo es la siguiente:

Esquema 2.16. Firma digital de ElGamal

- *Generación de llaves*
  - *Obtener aleatoriamente un primo p y un generador α de $\mathbb{Z}_p^*$*
  - *Seleccionar un entero $a \in [1, p-1]$*
  - *Calcular $y = \alpha^a$*
  - *La llave pública es: (p, α, y),*
  - *La llave privada: a*

- *Firma*
  - *Sea $M \in \mathbb{Z}_p$ el mensaje a firmar*
  - *Seleccionar aleatoriamente $k \in \mathbb{Z}_p^*$ tal que $(k, p-1) = 1$*
  - *Calcular $x = \alpha^k \mod p$*
  - *Obtener b resolviendo $M \equiv (xa + kb) \mod (p-1)$*
  - *La firma es el par ordenado: (x, b)*

- *Verificación*
  - *Obtener $f_1 = y^x x^b \mod p$ y $f_2 = \alpha^M \mod p$*
  - *Si $f_1 = f_2$ entonces la firma es válida.*

La verificación se cumple ya que

$$
\begin{aligned}
f_1 - f_2 = y^x x^b - \alpha^M &\equiv \\
&\equiv (\alpha^a)^x(\alpha^k)^b - \alpha^{xa+kb} \mod p \\
&\equiv 0
\end{aligned} \tag{57}
$$

Si una entidad quiere firmar un mensaje como otra, para obtener el valor de b nuevamente es necesario el valor de a que se puede obtener siempre y cuando sea posible obtener $log_\alpha(y)$.

Ejemplo 2.17.

Considere que en el ejemplo (2.15) la persona B que cifra el mensaje "HOLA" para la persona A, tiene como llave pública $(p, \alpha, y_B) = (757, 17, 601)$ *(las dos primeras son generales para quienes usan el mismo sistema) y la llave privada es* $a_B = 527$. *Las llaves de A son* $(p, \alpha, y_A) = (757, 17, 326)$ *y* $a_A = 20$.

Solución.

Como se vió antes el mensaje cifrado es

$$\text{"}FR\ JC\ JK\ ZB\text{"} \equiv 181, 273, 281, 704$$

y para expresarlo como un elemento de $\mathbb{Z}_{757}$ se usa la función hash, definida en el ejemplo 2.7, se tiene que $h_g(181, 273, 281, 704) = 393 = 24 * 27 + 15 = \text{WÑ}$.

Ahora se selecciona aleatoriamente $k = 97$ y se obtiene $x = 17^{97} = 142$, y se resuelve $393 \equiv (142)(527) + (97)(b) \mod 756$ es decir $97b \equiv 403 \mod 756$ usando el algoritmo de Euclides se tiene que $97(265) \equiv 1 \mod 757$ con lo que $b \equiv 199 \mod 756$; teniendo así que la firma será $(x, b) = (142, 199) = EGGJ$, así pues el mensaje enviado y firmado por B a A es

$$FRJC\ JKZB\ EGGJ$$

Para verificar la firma se observa que $f_1 = 601^{142}142^{199} = 186$ y además que: $f_2 = 17^{393} = 186$, teniendo así que la firma es válida.

■

2.4. ElGamal para curva elípticas

El esquema propuesto originalmente por Thaer ElGamal, está basado en el problema del logaritmo discreto [14]. Esto propició, en un principio, que este fuera el utilizado para cifrar usando el grupo de puntos

racionales de una curva elíptica sobre un campo finito [**32**], [**21**]. A continuación se presenta la adaptación para curvas elípticas:

Esquema 2.18. ElGamal para Curvas Elípticas

1. *Generación de llaves*
   a) *Seleccionar una curva elíptica* $E(\mathbb{K})$ *sobre el campo finito* $\mathbb{K}$
   b) *Elegir un punto* $P \in E(\mathbb{K})$ *y* $s = o(P)$ *(el orden del punto)*
   c) *Seleccionar un entero* $a \in [2, s-1]$ *y obtener* $Q = aP$
   d) *La llave pública es:* $(E(\mathbb{K}), P, Q)$*, y la llave privada:* (a)

2. *Pasos para el cifrado.*
   a) *Representar el mensaje como un punto* $m \in E(\mathbb{K})$
   b) *Seleccionar un entero* $k \in [2, s-1]$
   c) *Calcular* $\gamma = kP$ *y* $\delta = m + kQ$
   d) *El mensaje cifrado es:* $C = (\gamma, \delta)$

3. *Pasos para el descifrado*
   a) *Calcular* $\beta = (s-a)\gamma$
   b) *Recuperar el mensaje como* $m = \beta + \delta$

Tradicionalmente se hace la selección de a y k en $\mathbb{Z}_s^*$; sin embargo, como requisito deseable se pide que el orden de a sea $\phi(s)$. En el caso de k se debe evitar el valor de 1 pues el mensaje sería recuperable con los valores públicos. Además de que el mensaje se puede recuperar si es factible la solución del PLD en el grupo de puntos racionales de la curva elíptica.

El siguiente ejemplo, a pesar de que representa grandes deficiencias en cuanto a la seguridad, es un ejemplo sencillo para ilustrar el esquema. Además de que la relación entre los valores alfabéticos y los puntos sobre la curva es original.

Ejemplo 2.19.

Considérese la curva del ejemplo 1.8, pero como sólo se tienen 13 puntos para representar 26 caracteres, se determinará que cada punto represente dos caracteres, por lo que se deberá tener cuidado al cifrar y descifrar considerando la asignación mostrada en el cuadro 1.

Para tener una asignación sistemática y cuidadosa la parte γ *del mensaje cifrado se tomará del mismo renglón que el texto en claro y la parte* δ *se tomará del renglón contrario. Por ejemplo si se tiene que el*

A	B	C	D	E	F	G	H	I	J	K	L	M
$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$

CUADRO 1. Correspondencia entre caracteres y puntos racionales.

cifrado de Z es $(7P, 5P)$ entonces el mensaje que se deberá de enviar es: UF.

*Ahora bien, supónganse que se desea enviar el mensaje "**vamos a ver libros**" a una entidad cuya llave pública está dada por $(C(\mathbb{K}), (\alpha : 0 : 1), (\alpha^4 : 0 : 1))$, $s = 13$.*

Solución.

Para cifrar el mensaje se tiene:

t.c	m	k	γ	δ	γ	δ
v	$8P$	7	$7P$	$8P + 7(3P) = 3P$	U	D
a	$0P$	6	$6P$	$0P + 6(3P) = 5P$	G	S
m	$12P$	7	$7P$	$12P + 7(3P) = 7P$	H	U
o	$1P$	9	$9P$	$1P + 9(3P) = 2P$	W	C
s	$5P$	5	$5P$	$5P + 5(3P) = 7P$	S	H
a	$0P$	10	$10P$	$0P + 10(3P) = 4P$	K	R
v	$8P$	8	$8P$	$8P + 8(3P) = 6P$	V	G
e	$4P$	11	$11P$	$4P + 11(3P) = 11P$	L	Y
r	$4P$	10	10	$4P + 10(3P) = 8P$	X	I
l	$11P$	7	$7P$	$11P + 7(3P) = 6P$	H	T
i	$8P$	5	$5P$	$8P + 5(3P) = 10P$	F	X
b	$1P$	1	$1P$	$1P + 1(3P) = 4P$	B	R
r	$4P$	8	$8P$	$4P + 8(3P) = 2P$	V	C
o	$1P$	11	$11P$	$1P + 11(3P) = 8P$	Y	I
s	$5P$	9	$9P$	$5P + 9(3P) = 6P$	W	G

Así el mensaje cifrado es:
"UD GW HU WC SH KR VG LY XI HT FX BR VC YI WG"

Para descifrar el mensaje se requiere la llave privada, la cual en este caso es $a = 3$.

γ	δ	γ	δ	β	m	$t.c$
U	D	7P	3P	10(7P)=5P	3P+5P=8P	v
G	S	6P	5P	10(6P)=8P	5P+8P=0P	a
H	U	7P	7P	10(7P)=5P	7P+5P=12P	m
W	C	9P	2P	10(9P)=12P	2P+12P=1P	o
S	H	5P	7P	10(5P)=11P	7P+11P=5P	s
K	R	10P	4P	10(10P)=9P	4P+9P=0P	a
V	G	8P	6P	10(8P)=2P	6P+2P=8P	v
L	Y	11P	11P	10(11P)=6P	11P+6P=4P	e
X	I	10P	8P	10(10P)=9P	8P+9P=4P	r
H	T	7P	6P	10(7P)=5P	6P+5P=11P	l
F	X	5P	10P	10(5P)=11P	10P+11P=8P	i
B	R	1P	4P	10(1P)=10P	4P+10P=1P	b
V	C	8P	2P	10(8P)=2P	2P+2P=4P	r
Y	I	11P	8P	10(11P)=6P	8P+6P=1P	o
W	G	9P	6P	10(9P)=12P	6P+12P=5P	s

Obteniendo de la última columna el texto original "vamosaverlibros."
■

En base al algoritmo se verán algunos de los puntos que se deben tener en cuenta para la implementación.

Problema 1 En la generación de llaves se debe seleccionar una curva que satisfaga ciertas propiedades, principalmente que sobre el grupo de puntos racionales no sea factible resolver el problema del logaritmo discreto, además como en las implementaciones se usan computadoras es deseable que la curva se maneje sobre un campo de característica 2.

Problema 2 Se debe escoger un punto P de tal forma que su orden s sea lo más grande posible, este es el grupo cíclico a utilizar en el esquema.

Problema 3 La llave privada a es un número entero aleatorio en el intervalo $[2, s-1]$, por lo que se debe contar con un generador de números pseudoaleatorios confiable. Además en el cifrado, para cada bloque a cifrar se debe generar un número aleatorio también.

Problema 4 Para generar la llave pública, así como en el proceso de cifrar y descifrar la información se requiere de sumar varias veces el mismo punto por lo que sera necesario algoritmos eficientes para realizar este proceso.

Al considerar las alternativas del problema 1 se analiza cuándo es factible resolver el problema del logaritmo discreto en las curvas elípticas, lo cual se hará en la sección 3.1. El análisis de este problema conduce al surgimiento de las llamadas curvas de Koblitz [**23**], [**27**].

Una vez que se han determinado qué tipos de curvas son buenas en el sentido del problema 1, se deben seleccionar aquellas que satisfagan el problema 2. Para esto sólo se debe de seleccionar un campo apropiado para que tenga un subgrupo cíclico de orden suficientemente grande.

Para solucionar el problema 3 existen diferentes generadores de números pseudoaleatorios, entre los cuales destacan el congruencial lineal, LFRS, el Blum-Blum-Shub y el Blum-Micali [**13**], [**30**].

El generador congruencial lineal, está basado en la generación de números mediante la fórmula de recurrencia $x_n \equiv ax_{n-1} + c \mod m$. El principal problema es determinar los parámetros de forma adecuada [**2**]. Sin embargo para los sistemas criptográficos no es recomendable ya que con una cadena de longitud considerable se puede predecir los resultados, dejando de ser así pseudoaleatoria [**13**]. Esto mismo sucede con los generadores LFSR (linear feedback shift register), los cuales se pueden resolver mediante el algoritmo de Berlekamp-Massey [**5**], [**31**].

Los generadores Blum-Blum-Shub y Blum-Micali, aunque para los aspectos criptográficos no son del todo eficientes teóricamente son muy importantes y son la base para los algoritmos usados. La idea central en que basan su seguridad estos generadores son los residuos cuadráticos en el primer caso y en el problema del logaritmo discreto en el segundo [**13**], [**30**].

En cuanto al problema 4, la estructura que se desprende de las curvas de Koblitz permite determinar de manera eficiente el doble de un punto, logrando con esto una aritmética eficiente en las operaciones requeridas [**41**].

Capítulo 3

Curvas Elípticas en Criptografía

El impulso de la criptografía de curvas elípticas, trajo como consecuencia, principalmente, el estudio del problema del logaritmo discreto sobre el grupo de puntos racionales de una curva elíptica y la búsqueda de buenas curvas elípticas para su uso en criptografía. En el trabajo de Menezes, Okamoto y Vanstone [**27**], se reduce el PLD sobre curvas elípticas al PLD sobre campos finitos, en los cuales es más fácil resolver el PLD, para cierto tipo de curvas. Neal Koblitz publicó un artículo [**23**], en el cual describe las curvas no-supersingulares apropiadas, sobre campos de característica 2, las cuales actualmente se conocen como curvas de Koblitz, y son utilizadas para aplicaciones criptográficas.

3.1. El Problema del Logaritmo Discreto.

El problema del logaritmo discreto (PLD) es de vital importancia en varios esquemas criptográficos, en especial los que aquí se presentan. El resolver el PLD implica para la criptografía determinar qué grupos no son seguros y sobre qué grupos se pueden implementar esquemas confiables; en tanto para el criptoanálisis implica conocer qué esquemas son vulnerables para poder recuperar la información utilizada.

Como se ha mencionado, el uso de curvas elípticas en criptografía en un principio se debió a la fortaleza del problema del logaritmo discreto, por lo que es importante estudiarlo. Dado un grupo conmutativo finito $\mathbb{G}$ y dados dos elementos $\alpha, \beta \in \mathbb{G}$, en general no es sencillo determinar si existe un entero x tal que:

$$\alpha^x = \beta \tag{58}$$

Sin embargo, si se supone que $\mathbb{G}$ es un grupo cíclico y α es un generador del grupo, entonces se garantiza la existencia de $x \in \mathbb{N}$ tal que satisface (58), aún así, no es fácil determinar su valor. Se puede definir el logaritmo discreto base α en $\mathbb{G}$ como:

(59) $$\log_\alpha \beta = x \text{ si } \alpha^x = \beta \text{ y además } 0 \leq x < o(\mathbb{G})$$

donde $o(\mathbb{G})$ denota el orden del grupo.

Al problema de encontrar dicha x se le llama "El Problema del Logaritmo Discreto"(PLD), el cual es un problema abierto. Si bien es cierto que existen algunos algoritmos para resolver este problema, en general no determinan la solución en tiempo real.

3.1.1. Métodos para resolver el PLD

Una primera idea para resolver el problema es tomar al generador y empezar a calcular sus potencias hasta encontrar el elemento deseado, pero esto no es factible para grupos de orden grande. Existen varias alternativas para determinar el logaritmo discreto, entre las que destacan por su simplicidad el método "Baby-Step Giant-Step" y el método "ρ de Pollard", además se pueden mencionar el metodo "lambdaz el método de curvas elípticas [**40**], entre otros. En los métodos que aquí se presentan se considera al grupo cíclico $\mathbb{G}$ de orden n y a α un generador de este.

3.1.1.1. Método Paso-Pequeño Paso-Grande. (Baby-Step Giant-Step)

Este método se divide en dos partes [**28**], pasos pequeños y pasos grandes. En el primero de ellos se crea una base de datos los cuales permiten, en la segunda parte, realizar comparaciones para obtener el valor del logaritmo. Para explicar el funcionamiento se observa el siguiente hecho.

Sea $m = \lceil \sqrt{n} \rceil$ y sea $x = \log_\alpha \beta$ entonces existen i, j enteros únicos tales que $x = mj + i$ con $0 \leq i < m$, lo cual implica que $0 \leq j < m$. Con esto se tiene que:

(60) $$\beta = \alpha^x = \alpha^{mj+i} = \alpha^{mj}\alpha^i$$

De donde se sigue:

(61) $$\beta\alpha^{-mj} = \alpha^i$$

Conn base en esta observación el primer paso, es obtener la lista de las m parejas de la forma (i, α^i), con $i = 0, \ldots, m-1$ y almacenarla.

El segundo paso, naturalmente, consiste en que para cada $j = 0, \ldots, m-1$, se obtiene el valor de $\beta\alpha^{-mj}$ y se compara con cada una de las segundas entradas en la lista. De esta forma, se obtiene la primera entrada cuando son iguales y el valor de la j en la que se logró. Es decir, si $\beta\alpha^{-mj} = \alpha^i$ para algún i entonces $\log_\alpha \beta = i + jm$.

Ejemplo 3.1.

Considere $\mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$, *que es un grupo cíclico de orden* 12 *y* 2 *es un generador del grupo. Se desea determinar* $\log_2 5$ *y* $\log_2 7$.

Solución. Se procede como sigue:

1. $n = o(\mathbb{Z}_{13}^*) = 12$ con lo cual $m = \lceil\sqrt{12}\rceil = \lceil 3.46\rceil = 4$
2. Se obtiene la lista de 4 parejas
   si $i = 0$ como $2^0 = 1$, entonces $(0,1)$
   si $i = 1$ como $2^1 = 2$, y así $(1,2)$
   si $i = 2$ como $2^2 = 4$, de esta forma $(2,4)$
   si $i = 3$ como $2^3 = 8$, con lo cual se tiene $(3,8)$
3. Así $2^{-m} = 2^{-4} = 9$
4. Para $\log_2 5$ se obtiene
   para $j = 0$ como $5 * 9^0 = 5 * 1 = 5$, el cual no esta en las segundas entradas de la lista preliminar.
   para $j = 1$ como $5 * 9^1 = 5 * 9 = 6$, el cual no esta en las segundas entradas de la lista preliminar.
   para $j = 2$ se tiene $5 * 9^2 = 5 * 3 = 2$, el cual es la segunda entrada de $i = 1$.
5. Así $\log_2 5 = 1 + 4 * 2 = 9$
6. Para $\log_2 7$ se obtiene
   para $j = 0$ se tiene $7 * 9^0 = 7 * 1 = 7$, el cual no esta en las segundas entradas de la lista preliminar.
   para $j = 1$ se tiene $7 * 9^1 = 7 * 9 = 11$, el cual no esta en las segundas entradas de la lista preliminar.
   para $j = 2$ se tiene $7 * 9^2 = 7 * 3 = 8$, el cual es la segunda entrada de $i = 3$.
7. Así $\log_2 7 = 3 + 4 * 2 = 11$

■

Si se resuelven estos dos problemas por el método usual, es decir, elevar el generador hasta encontrar el número que se desea, se habrían requerido 18 multiplicaciones y 20 comparaciones; sin embargo, mediante este método se hicieron 4 multiplicaciones y una inversión para

los valores predefinidos y 2 más para cada logaritmos, además de 9 y 11 comparaciones respectivamente, teniendo así 8 multiplicaciones, una inversión y 20 comparaciones. Notando así el significativo ahorro de operaciones, no así las comparaciones, las cuales en este caso se conservan, sin embargo no representa mucho tiempo de cómputo.

Ejemplo 3.2.

Considere la curva elíptica del ejemplo 1.8 $x^3+xz^2+z^3+y^2z+yz^2$ *sobre* $\mathbb{F}_{2^3}$ *cuyos puntos son:*

$$\mathbb{G} = \{(0:1:0),(\alpha:0:1),(\alpha:1:1),(\alpha^2:1:1),(\alpha^2:0:1),(\alpha^3:\alpha:1),$$
$$(\alpha^3:\alpha^3:1),(\alpha^4:0:1),(\alpha^4:1:1),(\alpha^5:\alpha^4:1),(\alpha^5:\alpha^5:1),(\alpha^6:\alpha^2:1),$$
$$(\alpha^6:\alpha^6:1)\}$$

Es fácil ver que un generador del grupo es: $\gamma = (\alpha:0:1)$. *Se desea determinar* $\log_\gamma(\alpha^3:\alpha:1)$ *y* $\log_\gamma(\alpha^4:1:1)$.

Solución.

Para determinar $\log_\gamma(\alpha^3:\alpha:1)$ y $\log_\gamma(\alpha^4:1:1)$, se procede como sigue:

1. $n = O(\mathbb{G}) = 13$ con lo cual $m = \lceil\sqrt{13}\rceil = \lceil 3.6\rceil = 4$
2. Se obtiene la lista de 4 parejas
   si $i = 0$ como $0(\alpha:0:1) = (0:1:0)$, entonces se tiene $(0,(0:1:0))$
   si $i = 1$ como $1(\alpha:0:1) = (\alpha:0:1)$, y así $(1,(\alpha:0:1))$
   si $i = 2$ como $2(\alpha:0:1) = (\alpha^5:\alpha^4:1)$, entonces $(2,(\alpha^5:\alpha^4:1))$
   si $i = 3$ como $3(\alpha:0:1) = (\alpha^4:0:1)$, de esta forma $(2,(\alpha^4:0:1))$
3. Así $-m(\alpha:0:1) = -4(\alpha:0:1) = (\alpha^2:0:1)$
4. Para $\log_\gamma(\alpha^3:\alpha:1)$ se obtiene
   para $j = 0$ como
   $(\alpha^3:\alpha:1) + 0(\alpha^2:0:1) = (\alpha^3:\alpha:1) + (0:1:0) = (\alpha^3:\alpha:1)$, el cual no esta en las segundas entradas de la lista preliminar.
   Para $j = 1$ como $(\alpha^3:\alpha:1) + 1(\alpha^2:0:1) = (\alpha:0:1)$, el cual es la segunda entrada de $i = 1$.
5. Así $\log_\gamma(\alpha^3:\alpha:1) = 1 + 4 * 1 = 5$
6. Para $\log_\gamma(\alpha^4:1:1)$ se obtiene
   para $j = 0$ como $(\alpha^4:1:1) + 0(\alpha^2:0:1) = (\alpha^4:1:1)$, el cual no está en las segundas entradas de la lista preliminar.
   para $j = 1$ como $(\alpha^4:1:1) + 1(\alpha^2:0:1) = (\alpha^6:\alpha^2:1)$, el cual no está en las segundas entradas de la lista preliminar.

para $j = 2$ como
$(\alpha^4 : 1 : 1) + 2(\alpha^2 : 0 : 1) = (\alpha^4 : 1 : 1) + (\alpha^3 : \alpha : 1) = (\alpha^5 : \alpha^4 : 1)$, el cual es la segunda entrada de $i = 2$.

7. Así $\log_\gamma (\alpha^4 : 1 : 1) = 2 + 4 * 2 = 10$.

■

Si se resuelven estos dos problemas por el método usual, es decir, elevar el generador hasta encontrar el número que se desea, se habrían requerido 13 sumas y 15 comparaciones. Mediante este método se hicieron 4 sumas y una inversión para los valores predefinidos y 1 y 2 más para cada logaritmo respectivamente, además de 5 y 10 comparaciones respectivamente, teniendo así 3 sumas, una inversión y 15 comparaciones. Notando así el significativo ahorro de operaciones, no así las comparaciones, las cuales en este caso, como en el anteriormente analizado, se conservan, sin embargo no representa mucho tiempo de computo.

3.1.1.2. Método ρ de Pollard. Este método tiene la ventaja sobre el anterior que no requiere tener una lista previa de resultados. La idea detrás del algoritmo es encontrar dos parejas de números enteros tales que:

$$\alpha^{a_i}\beta^{b_i} = \alpha^{a_j}\beta^{b_j} \tag{62}$$

Con lo cual se tendrá que:

$$\beta^{b_i - b_j} = \alpha^{a_j - a_i} \tag{63}$$

$$(b_i - b_j)\log_\alpha \beta \equiv a_j - a_i \mod n \tag{64}$$

El método ρ de Pollard [**28**] consiste en lo siguiente: dado un grupo finito cíclico $\mathbb{G}$ de orden n y un generador α, se desea determinar $x = \log_\alpha \beta$, para esto se define una partición, S_1, S_2 y S_3 de similar tamaño, teniendo en cuenta que $1 \notin S_2$ y en base a esta se definen las sucesiones:

$$x_i = \begin{cases} \beta x_{i-1}, & x_{i-1} \in S_1 \\ x_{i-1}^2, & x_{i-1} \in S_2 \\ \alpha x_{i-1}, & x_{i-1} \in S_3 \end{cases}$$

$$a_i = \begin{cases} a_{i-1}, & x_{i-1} \in S_1 \\ 2a_{i-1}, & x_{i-1} \in S_2 \\ a_{i-1} + 1, & x_{i-1} \in S_3 \end{cases}$$

$$b_i = \begin{cases} b_{i-1} + 1, & x_{i-1} \in S_1 \\ 2b_{i-1}, & x_{i-1} \in S_2 \\ b_{i-1}, & x_{i-1} \in S_3 \end{cases}$$

Se calcula esta sucesión hasta que $x_i = x_{2i}$ y considerando entonces: $r = b_i - b_{2i}$ y $s = a_{2i} - a_i$ teniendo así que la solución x satisface la congruencia $rx \equiv s \mod n$.

Ejemplo 3.3. *Considerando el ejemplo 3.1, se desea determinar* $\log_2 5$ *y* $\log_2 7$, *mediante el método de la* ρ *de Pollard.*

Solución. Para obtener los logaritmos pedidos se procede como sigue:

1. Se crea la partición de $\mathbb{Z}_{13}^*$
   - $S_1 = \{1, 2, 3, 4\}$
   - $S_2 = \{5, 6, 7, 8\}$
   - $S_3 = \{9, 10, 11, 12\}$
2. La sucesión para $\log_2 5$ queda definida por:
$$x_i = \begin{cases} 5x_{i-1}, & x_{i-1} \in S_1 \\ x_{i-1}^2, & x_{i-1} \in S_2 \\ 2x_{i-1}, & x_{i-1} \in S_3 \end{cases}$$
3. Los valores obtenidos en las sucesiones son:

i	x_i	a_i	b_i
1	5	0	1
2	12	0	2
3	11	1	2
4	9	2	2
5	5	3	2
6	12	6	4
7	11	7	4
8	9	8	4

4. $r = b_4 - b_8 = 2 - 4 = -2 = 10$ y $s = a_8 - a_4 = 8 - 2 = 6$
5. Luego la solución debe satisfacer: $10x \equiv 6 \mod 12$, cuyas soluciones son $x = 3, 9$
6. Ahora sólo falta comprobar cuál de las dos es la correcta
   - $\alpha^3 = 2 * 2 * 2 = 8$ no se cumple la ecuación original.
   - $\alpha^9 = 8 * 8 * 8 = 5$ si se cumple la ecuación original.
7. La sucesión, para $\log_2 7$, queda definida por:
$$x_i = \begin{cases} 7x_{i-1}, & x_{i-1} \in S_1 \\ x_{i-1}^2, & x_{i-1} \in S_2 \\ 2x_{i-1}, & x_{i-1} \in S_3 \end{cases}$$
8. Los valores obtenidos en las sucesiones son:

i	x_i	a_i	b_i
1	7	0	1
2	10	0	2
3	7	1	2
4	10	2	4

9. $r = b_2 - b_4 = 2 - 4 = -2 = 10$ y $s = a_4 - a_2 = 2 - 0 = 2$
10. Luego la solución debe satisfacer: $10x \equiv 2 \mod 12$, cuyas soluciones son $x = 5, 11$
11. Ahora sólo falta verificar cuál de las dos es la correcta
    - $\alpha^5 = 6$ no se cumple la ecuación.
    - $\alpha^{11} = 7$ si se cumple la ecuación.

    Así $log_2 5 = 9$ y $log_2 7 = 11$

■

Ejemplo 3.4.

Considere la curva elíptica $x^3+xz^2+z^3+y^2z+yz^2$ *sobre* $\mathbb{F}_{2^3}$ *donde* $\alpha^3 + \alpha + 1 = 0$ *los puntos de la curva son:*

$$\mathbb{G} = \{(0:1:0), (\alpha:0:1), (\alpha:1:1), (\alpha^2:1:1), (\alpha^2:0:1), (\alpha^3:\alpha:1), (\alpha^3:\alpha^3:1),$$

$$(\alpha^4:0:1), (\alpha^4:1:1), (\alpha^5:\alpha^4:1), (\alpha^5:\alpha^5:1), (\alpha^6:\alpha^2:1), (\alpha^6:\alpha^6:1)\}$$

y un generador del grupo es: $\gamma = (\alpha : 0 : 1)$. *Se desea determinar* $\log_\gamma (\alpha^3 : \alpha : 1)$ *y* $\log_\gamma (\alpha^4 : 1 : 1)$.

Solución.

Se procede como sigue:

1. Se crea la partición de $\mathbb{G}$
    - $S_1 = \{(0:1:0)(\alpha:0:1)(\alpha:1:1)(\alpha^2:1:1)(\alpha^2:0:1)\}$
    - $S_2 = \{(\alpha^3:\alpha:1), (\alpha^3:\alpha^3:1), (\alpha^4:0:1), (\alpha^4:1:1)\}$
    - $S_3 = \{(\alpha^5:\alpha^4:1), (\alpha^5:\alpha^5:1), (\alpha^6:\alpha^2:1), (\alpha^6:\alpha^6:1)\}$
2. La sucesión para $\log_\gamma (\alpha^3 : \alpha : 1)$ queda definida por:
$$x_i = \begin{cases} (\alpha^3:\alpha:1) + x_{i-1}, & x_{i-1} \in S_1 \\ 2x_{i-1}, & x_{i-1} \in S_2 \\ (\alpha:0:1) + x_{i-1}, & x_{i-1} \in S_3 \end{cases}$$
3. Los valores obtenidos en las sucesiones son:

i	x_i	a_i	b_i
1	$(\alpha^3 : \alpha : 1)$	0	1
2	$(\alpha^4 : 1 : 1)$	0	2
3	$(\alpha^6 : \alpha^6 : 1)$	0	4
4	$(\alpha^3 : \alpha^3 : 1)$	1	4
5	$(\alpha^4 : 0 : 1)$	2	8
6	$(\alpha^6 : \alpha^2 : 1)$	4	16
7	$(\alpha^6 : \alpha^6 : 1)$	5	16
8	$(\alpha^3 : \alpha^3 : 1)$	6	16

4. $r = b_4 - b_8 = 4 - 16 = -12 = 1$ y $s = a_8 - a_4 = 6 - 1 = 5$
5. La solución debe satisfacer: $1x \equiv 5 \mod 13$ así que $x = 5$
6. La sucesión para $\log_\gamma (\alpha^4 : 1 : 1)$ queda definida por:

$$x_i = \begin{cases} (\alpha^4 : 1 : 1) + x_{i-1}, & x_{i-1} \in S_1 \\ 2x_{i-1}, & x_{i-1} \in S_2 \\ (\alpha : 0 : 1) + x_{i-1}, & x_{i-1} \in S_3 \end{cases}$$

7. Los valores obtenidos en las sucesiones son:

i	x_i	a_i	b_i
1	$(\alpha^4 : 1 : 1)$	0	1
2	$(\alpha^6 : \alpha^6 : 1)$	0	2
3	$(\alpha^3 : \alpha^3 : 1)$	1	2
4	$(\alpha^4 : 0 : 1)$	2	4
5	$(\alpha^6 : \alpha^2 : 1)$	4	8
6	$(\alpha^6 : \alpha^6 : 1)$	5	8
7	$(\alpha^3 : \alpha^3 : 1)$	6	16
8	$(\alpha^4 : 0 : 1)$	12	16

8. $r = b_2 - b_4 = 4 - 16 = -12 = 1$ y $s = a_4 - a_2 = 12 - 2 = 10$
9. La solución debe satisfacer: $x \equiv 10 \mod 13$, así que $x = 10$

■

3.1.2. El mapeo de Weil

El principal motivo para utilizar el grupo de puntos racionales de una curva elíptica sobre un campo finito $\mathbb{K}$, es que el orden del grupo puede ser mayor a la cardinalidad del campo y la aritmética se realiza en el campo, es decir, se tiene un grupo adecuado y las operaciones se realizan de forma sencilla. Además, si el PLD sobre el campo finito (PLDCF) se puede resolver, esto no indica que el PLD sobre la curva elíptica (PLDCE) sea soluble.

En algunos casos es posible transformar o reducir el PLDCE al PLDCF, lo cual implica que si el PLDCF se puede resolver el PLDCE

también sea soluble. Si es posible resolver el PLDCE entonces el esquema no tendrá ninguna seguridad por lo cual dicha curva no será apropiada para la criptografía. Para lograr esta simplificación se utiliza el hecho (1.9) que dice:

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \tag{65}$$

donde $n_2 \mid n_1$ y las propiedades de los mapeos bilineales no degenerados, como el de Weil, que junto con el de Tate, y recientemente el de Ate, son los más importantes definidos sobre curvas elípticas.

Definición 3.5. *Weil Pairing*

El Mapeo de Weil sobre la curva elíptica $E(\mathbb{F}_q)$ se define como el mapeo bilineal del m-ésimo grupo de torsión de E ($E[m]$) al grupo de las raíces m-ésimas de la unidad en una extensión de $\mathbb{F}_q$ denotado como μ_m. Aquí se debe considerar a m y q primos relativos.

$$e_m : E[m] \times E[m] \to \mu_m$$

dado por:

$$e_m(S,T) = \frac{g(X+S)}{g(X)} \tag{66}$$

donde:

$E[m] = \{P \in E(\overline{\mathbb{F}_q}) | mP = P_\infty\}$.

g es una función racional sobre E que depende de $T \in E[m]$ es tal que g no tiene ceros ni polos en X y $X+S$.

La construcción de g se puede encontrar en [**40**]. Las propiedades esenciales del mapeo de Weil se enuncian en el siguiente teorema.

Teorema 3.6. *Sean $S_1, S_2, S, T_1, T_2, T \in E[m]$. Entonces se cumple que*

1. $e_m(S_1 + S_2, T) = e_m(S_1, T) e_m(S_2, T)$
2. $e_m(S, T_1 + T_2) = e_m(S, T_1) e_m(S, T_2)$
3. $e_m(S, S) = 1$
4. $e_m(S, T) = e_m(T, S)^{-1}$
5. *Si $e_m(S, T) = 1$ para toda $S \in E[m]$ entonces $T = P_\infty$.*

Existe una definición alternativa al mapeo de Weil que se denota como e', la cual en realidad no es equivalente [**25**]. Sin embargo se cumple la siguente relación entre ellas:

$$e(S,T) = e'(T,S) \tag{67}$$

La definición alternativa es usada en la mayoría de las ocasiones ya que su evaluación es más eficiente. La definición alternativa se da en [**28**] y en la definición 5.1, la cual se da para curvas hiperelípticas.

3.1.3. Reducción del PLDCE al PLDCF

Como se ha mencionado, la principal fortaleza del esquema de cifrado ElGamal, es el PLD. Si se puede reducir el PLDCE al PLDCF, se debilita el esquema por lo que es importante saber cuando sucede esto. Los siguientes resultados dan a conocer los tipos de curvas en los que esto es posible.

Teorema 3.7. *Sea $P, T \in E(\mathbb{F}_q)$ de orden n_1 y sean $l \in \mathbb{Z}$, $R = lP$. Si $e_{n_1}(R,T) = (e_{n_1}(P,T))^{l'}$ entonces $l' \equiv l \mod n'$ donde n' es un divisor de n_2, donde n_1, n_2 son como en la ecuación (65).*

DEMOSTRACIÓN. Sea $G \in E(\mathbb{F}_q)$ un elemento de orden n_2, luego existen $c, d \in \mathbb{Z}$ tales que $T = cP + dG$ entonces

$$e_{n_1}(P,T)^{n_2} = e_{n_1}(P,P)^{cn_2} e_{n_1}(P, dn_2 G) = e_{n_1}(P, P_\infty) = 1$$

así pues el orden n' de $e_{n_1}(P,T)$, divide a n_2, además

$$e_{n_1}(P,T)^{l'} = e_{n_1}(R,T) = e_{n_1}(lP,T) = e_{n_1}(P,T)^{l}$$

entonces $l' \equiv l \mod n'$ donde n' es un divisor de n_2

□

El resultado anterior da un algoritmo para reducir el PLDCE al PLDCF.

Algoritmo 3.8. *Aproximación a la reducción del PLDCE*

Entrada: *$P \in E(\mathbb{F}_q)$ de orden n_1 y $R \in E[n_1]$*
Salida: *l' tal que $l' \equiv l \mod n'$ donde $R = lP$ y $n' \mid n_2$.*

1. *Seleccionar aleatoriamente $T \in E(\mathbb{F}_q)$*
2. *Calcular $\alpha = e_{n_1}(P,T)$ y $\beta = e_{n_1}(R,T)$*
3. *Obtener $l' = log_\alpha(\beta)$ en $\mathbb{F}_q$*

Si bien este procedimiento no da exactamente el valor del logaritmo, si reduce los valores en los que se debe de buscar. Para garantizar que se obtiene sólo un valor basta pedir que el orden de α sea n. Esto se puede lograr debido al siguiente resultado.

Teorema 3.9. *Sea $P \in E(\mathbb{F}_q)$ un punto de orden n. Entonces existe $Q \in E[n]$ tal que $e_n(P,Q)$ es una raíz n-ésima primitiva de la unidad.*

DEMOSTRACIÓN. Sea $P \in E(\mathbb{F}_q)$ un punto de orden n y $Q \in E[n]$ arbitrario. Se define el carácter $e_P(Q) = e_n(P, Q)$. Entonces la imagen de e_P es un subgrupo de las raíces n-ésimas de la unidad. Supongamos que la imagen es el grupo de las raíces m-ésimas de la unidad, con lo cual $m \mid n$. Por otro lado se tiene que

$$1 = (e_P(Q))^m = e_n(mP, Q)$$

al ser Q arbitrario, esto indica que $mP = P_\infty$, es decir, $n \mid m$, por ende $m = n$. □

Algoritmo 3.10. *Reducción del PLDCE*

Entrada: $P \in E(\mathbb{F}_q)$ *de orden* n *y* $R \in E[n]$.
Salida: l *tal que* $R = lP$.

1. *Determinar el entero* k *más pequeño tal que* $E[n] \subset E(\mathbb{F}_{q^k})$.
2. *Encontrar* $Q \in E[n]$ *tal que* $\alpha = e_n(P, Q)$ *tiene orden* n.
3. *Calcular* $\beta = e_n(R, Q)$.
4. *Obtener* $l = log_\alpha(\beta)$ *en* $\mathbb{F}_{q^k}$.

Este algoritmo tiene dos grandes inconvenientes, en los dos primeros pasos. El primero es como encontrar k y el segundo determinar Q tal que $\alpha = e_n(P, Q)$ tenga orden n.

El primer problema se puede resolver con facilidad para las curvas supersingulares, los valores que puede tomar t se derivan del teorema de Hasse que indica que $|t| \leq 2\sqrt{q}$; en tanto el segundo problema se resuelve mediante aspectos probabilísticos.

Antes de clasificar las curvas supersingulares, se enuncian algunas proposiciones que ayudan a esto y sus pruebas se pueden encontrar en [**39**].

Proposición 3.11. *Sean* $\mathbb{F}_q$ *un campo finito de característica* p *y* E *un curva elíptica sobre* $\mathbb{F}_q$.

- *Si* $p \nmid n$ *entonces* $E(\mathbb{F}_q)[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.
- *Si* $n = p^s$ *y* E *es supersingular entonces* $E(\mathbb{F}_q)[n] = \{P_\infty\}$.
- *Si* $n = p^s$ *y* E *es no-supersingular entonces* $E(\mathbb{F}_q)[n] \cong \mathbb{Z}_n$.

Proposición 3.12. *Sean* $E(\mathbb{F}_{p^m})$ *una curva elíptica cuyo grupo de puntos racionales tiene orden* $p^m + 1 - t$ *y* $n \in \mathbb{N}$ *tal que* $p \nmid n$. *Si* $E(\overline{\mathbb{F}}_{p^m})[n] \subset E(\mathbb{F}_{p^m})$ *entonces* $n^2 \mid (p^m + 1 - t)$ *y además* $n \mid (p^m - 1)$.

Proposición 3.13. *Sea $E(\mathbb{F}_{p^m})$ una curva elíptica cuyo grupo de puntos racionales tiene orden $p^m + 1 - 2\sqrt{q}$. Si $n \in \mathbb{N}$ y $p \nmid n$, entonces $E(\overline{\mathbb{F}}_{p^m})[n] \subset E(\mathbb{F}_{p^m})$ sí y sólo si $n^2 \mid (p^m + 1 - 2\sqrt{q})$ y $n \mid (p^m - 1)$.*

La estructura de $E(\mathbb{F}_q)$ supersingular se da en el siguiente lema.

Lema 3.14. *La estructura de grupo para las curvas elípticas supersingulares está dado por:*

- *Si $t^2 = q, 2q$, o $3q$ entonces $E(\mathbb{F}_q)$ es cíclico.*
- *Si $t = \pm 2\sqrt{q}$ entonces $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}\mp 1} \oplus \mathbb{Z}_{\sqrt{q}\mp 1}$*
- *Si $t = 0$ y $q \not\equiv 3 \mod 4$ entonces $E(\mathbb{F}_q)$ es cíclico*
- *Si $t = 0$ y $q \equiv 3 \mod 4$ entonces $E(\mathbb{F}_q)$ es cíclico o $E(\mathbb{F}_q) \cong \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$*

donde t es como en el teorema de Hasse.

DEMOSTRACIÓN. Sea $n \in \mathbb{N}$. Si n es tal que $p \mid n$ con lo cual $E(\overline{\mathbb{F}}_q)[n] = \{P_\infty\}$, en caso contrario, $p \nmid n$, entonces tendremos lo siguiente:

Suponga que $t^2 = \alpha q$ donde $\alpha = 0, 1, 2, 3$ y sea $E(\mathbb{F}_q)$ una curva elíptica de orden $q + 1 - t$ y $E(\overline{\mathbb{F}}_q)[n] \subset E(\mathbb{F}_q)$ lo cual implica que:

$n^2 \mid (q + 1 - t)$ y $n \mid (q - 1)$ esto indica que $mcd(n, q) = 1$
y de aquí se llega a que:

$t^2 = q^2 + 1 + 2q - n^2 r = \alpha q$

$q^2 + 1 + 2q - \alpha q = n^2 r$

$(4 - \alpha)q = n^2 r - q^2 + 2q - 1 = n^2 r - (q - 1)^2 = n^2 s$

de aquí se tiene que $n^2 \mid (4 - \alpha)q$ y como $mcd(n^2, q) = 1$ de aquí se sigue $n^2 \mid (4 - \alpha)$ así pues si $\alpha = 1, 2, 3$, entonces $n = 1$ si $\alpha = 0$ entonces $n = 1, 2$

Si $\alpha = 0$ y $q \not\equiv 3 \mod 4$ y como $n^2 \mid (q + 1)$ se obtiene $n = 1$

Si $\alpha = 0$ y $q \equiv 3 \mod 4$ entonces $n = 1, 2$

En el caso en que n sólo puede tomar el valor de 1 se tiene que el grupo es cíclico y en el caso en que n puede tomar el valor de 2 entonces el grupo sera isomorfo a $\mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$

En el caso en que $\alpha = 4$ se tiene que $|E(\mathbb{F}_q)| = q + 1 \mp 2\sqrt{q}$ si $n = \sqrt{q}\mp 1$ entonces $|E(\mathbb{F}_q)| = n^2$ entonces $E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n \cong E(\mathbb{F}_q)[n]$ □

Una clasificación de las curvas supersingulares [**28**] se da en el cuadro 1. El sentido de la última columna es que $E(\mathbb{F}_{q^k}) \cong \mathbb{Z}_{cn_1} \oplus \mathbb{Z}_{cn_1}$

	t	Est de $E(\mathbb{F}_q)$	n_1	k	tipo	c
I	0	cíclico	$q+1$	2	$(q+1, q+1)$	1
II[1]	0	$\mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$	$\frac{q+1}{2}$	2	$(q+1, q+1)$	2
III	$\pm\sqrt{q}$	cíclico	$q+1 \mp \sqrt{q}$	3	$(\sqrt{q^3}\pm 1, \sqrt{q^3}\pm 1)$	$\sqrt{q}\pm 1$
IV[2]	$\pm\sqrt{2q}$	cíclico	$q+1 \mp \sqrt{2q}$	4	(q^2+1, q^2+1)	$q \pm \sqrt{2q}+1$
V[3]	$\pm\sqrt{3q}$	cíclico	$q+1 \mp \sqrt{3q}$	6	(q^3+1, q^3+1)	$(q+1)(q \pm \sqrt{3q}+1)$
VI	$\pm 2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}\mp 1} \oplus \mathbb{Z}_{\sqrt{q}\mp 1}$	$\sqrt{q} \mp 1$	1	$(\sqrt{q} \mp 1, \sqrt{q} \mp 1)$	1

CUADRO 1. Clasificación de las curvas Supersingulares

Lema 3.15. *Sea $E(\mathbb{F}_q)$ una curva supersingular tal que $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ donde $n_2 \mid n_1$. Entonces $E(\mathbb{F}_q)[n_1] \subset E(\mathbb{F}_{q^k})$ donde n_1 y k son como en el cuadro 1.*

DEMOSTRACIÓN. Se analiza cada caso.

Caso I

Se tiene que $|E(\mathbb{F}_q)| = q+1$ y $|E(\mathbb{F}_{q^2})| = q^2+1-2q$. Esto indica que $E(\mathbb{F}_{q^2}) \cong \mathbb{Z}_{q+1} \oplus \mathbb{Z}_{q+1}$ y así se tiene que $E(\mathbb{F}_q)[q+1] \subset E(\mathbb{F}_{q^2})$.

Caso II[1]

Se tiene que $|E(\mathbb{F}_q)| = q+1$ y $|E(\mathbb{F}_{q^2})| = q^2+1-2q$. Esto indica que $E(\mathbb{F}_{q^2}) \cong \mathbb{Z}_{q+1} \oplus \mathbb{Z}_{q+1}$ y como $q+1 = \frac{q+1}{2}(2)$ se cumple que $E(\mathbb{F}_q)[q+1] \subset E(\mathbb{F}_{q^2})$.

Caso III

Se tiene que $|E(\mathbb{F}_q)| = q+1 \mp \sqrt{q}$ lo cual implica que $|E(\mathbb{F}_{q^2})| = q^2+1+q$ y además $|E(\mathbb{F}_{q^3})| = q^3+1 \pm 2\sqrt{q^3} = (\sqrt{q^3}\pm 1)^2$ y como $(\sqrt{q^3}\pm 1) = (q \mp \sqrt{q}+1)(\sqrt{q}\pm 1)$ y $(q^3-1) = (\sqrt{q^3}-1)(\sqrt{q}+1)$. Esto indica que $E(\mathbb{F}_q)[q \mp \sqrt{q^3}+1] \subset E(\mathbb{F}_{q^3})$.

Caso IV[2]

Se tiene que $|E(\mathbb{F}_q)| = q+1\pm\sqrt{2q}$ y $|E(\mathbb{F}_{q^2})| = q^2+1$, y $|E(\mathbb{F}_{q^3})| = q^3+1\pm\sqrt{2q^3}$ así como $|E(\mathbb{F}_{q^4})| = q^4+1+2q^2$. Esto indica que $E(\mathbb{F}_{q^4}) \cong \mathbb{Z}_{q^2+1} \oplus \mathbb{Z}_{q^2+1}$ y como $q^2+1 = (q+1+\sqrt{2q})(q+1-\sqrt{2q})$, por lo que $E(\mathbb{F}_q)[q+1\pm\sqrt{2q}] \subset E(\mathbb{F}_{q^4})$.

Caso V[3]

[1]sólo se da cuando $q \equiv 3 \mod 4$

[2]sólo se da cuando $q = 2^{2s+1}$

[3]solo se da cuando $q = 3^{2s+1}$

[3]sólo se da cuando $q = 3^{2s+1}$

Se tiene que $|E(\mathbb{F}_q)| = q+1\mp\sqrt{3q}$ y $|E(\mathbb{F}_{q^2})| = q^2+1-q$, $|E(\mathbb{F}_{q^3})| = q^3+1$, $|E(\mathbb{F}_{q^4})| = q^4+1+q^2$ y $|E(\mathbb{F}_{q^5})| = q^5+1\pm\sqrt{3q^5}$, así como $|E(\mathbb{F}_{q^6})| = q^6+1+2q^3 = (q^3+1)^2$ y puesto que $(q^3+1) = (q+1)(q^2-q+1) = (q+1)((q+1)^2-3q) = (q+1)(q+1-\sqrt{3q})(q+1+\sqrt{3q})$. Esto indica que $E(\mathbb{F}_{q^4}) \cong \mathbb{Z}_{q^2+1} \oplus \mathbb{Z}_{q^2+1}$ y como $q^2+1 = (q+1+\sqrt{2q})(q+1-\sqrt{2q})$ así se tiene que $E(\mathbb{F}_q)[q+1\pm\sqrt{3q}] \subset E(\mathbb{F}_{q^6})$.

Caso VI

Se tiene que $|E(\mathbb{F}_q)| = q+1\mp 2\sqrt{q}$. Esto indica que $E(\mathbb{F}_q) \cong \mathbb{Z}_{q\mp1} \oplus \mathbb{Z}_{q\mp1} \oplus \mathbb{Z}_{q+1} \cong E(\mathbb{F}_q)[\sqrt{q}\mp 1]$ y así $E(\mathbb{F}_q) = E(\mathbb{F}_q)[\sqrt{q}\mp 1]$. □

En base a esto construimos el siguiente algoritmo para resolver el problema del logaritmo discreto para curva elípticas.

Algoritmo 3.16. *del PLDCES*

Entrada : $P \in E(\mathbb{F}_q)$, $n = o(P)$, $o(E)$ *y* $R \in \langle P\rangle$
Salida: l *tal que* $R = lP$

1. *Determinar los valores de* k *y de* c *según el cuadro 1*
2. *Escoger aleatoriamente* $Q' \in E(\mathbb{F}_{q^k})$
3. *Calcular* $Q = \frac{cn_1}{n}Q'$
4. *Determinar* $\alpha = e_n(P,Q)$ *y* $\beta = e_n(R,Q)$
5. *Calcular* $l' = log_\alpha\beta$ *en* $\mathbb{F}_{q^k}$
6. *Si* $l'P = R$ *entonces* $l = l'$ *si no regresar al paso 2.*

Observaciones.

Si se conocen los valores de q y el orden de $E(\mathbb{F}_q)$ entonces se puede determinar fácilmente a qué clase pertenece y por consiguiente conocer los valores de n_1, k y c.

La probabilidad de que α tenga orden n es $\frac{\phi(n)}{n}$, esto se debe a que hay n clases laterales de $\langle P\rangle$ y hay $\phi(n)$ elementos de orden n. En las aplicaciones se utilizan grupos de orden primo y grande, así la probabilidad es $\frac{n-1}{n} \approx 1$.

Recordando el problema 1, al final del capítulo anterior, se buscan curvas en las cuales no sea posible reducir el PLDCE al PLDCF a un campo finito y además se pueda realizar aritmética eficiente. De esta manera en primera instancia las curvas deben ser no supersingulares. Además debe de estar definida sobre una extensión de $\mathbb{F}_2$, para fines de implementaciones. La búsqueda de estas curvas llevó a la definición de las curvas de Koblitz.

3.2. Curvas de Koblitz

Recordemos de la sección (1.2) que una curva elíptica se puede expresar mediante la forma normal de Weierstrass dada por:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{68}$$

Cuando estemos sobre un campo de característica 2 se ha visto en (11), (12), que la forma normal de Weierstrass se puede reducir a:

$$E : y^2 + xy = x^3 + a_2x^2 + a_6 \tag{69}$$

con $\Delta = a_6$ y $j = 1/a_6$, si $a_1 \neq 0$, $a_6 \neq 0$ y

$$E : y^2 + a_3y = x^3 + a_4x + a_6 \tag{70}$$

con $\Delta = a_3^4$ y $j = 0$, si $a_1 = 0$, $a_3 \neq 0$.

Como se ha mencionado, las curvas supersingulares son malas para propósitos criptográficos basados en el PLD. Esto indica que es conveniente identificar cuáles curvas son de este tipo. El siguiente lema nos ayuda a este fin. El resultado se probará sólo para curvas sobre campos de característica 2, para el caso general se puede consultar [**39**].

Lema 3.17. *Sea $E(\mathbb{F}_{p^m})$ una curva elíptica, con $p \not\equiv 1 \mod 3$, entonces $j = 0$ si y sólo si la curva es supersingular.*

DEMOSTRACIÓN. Sea E sobre $(\mathbb{F}_{2^m})$ una curva elíptica, si $j_E \neq 0$ entonces es de la forma dada en (69). Luego si $(x_0, y_0) \in E(\mathbb{F}_q)$ se cumple que:

$$y_0^2 + x_0y_0 = x_0^3 + a_2x_0^2 + a_6 \tag{71}$$

y además $(x_0, y_0 + x_0)$ es también un elemento de $E(\mathbb{F}_{2^m})$,

$$(y_0 + x_0)^2 + x_0(y_0 + x_0) = x_0^3 + a_2x_0^2 + a_6 \tag{72}$$

$$y_0^2 + x_0^2 + x_0y_0 + x_0^2 = x_0^3 + a_2x_0^2 + a_6 \tag{73}$$

$$y_0^2 + x_0y_0 = x_0^3 + a_2x_0^2 + a_6 \tag{74}$$

De esta manera los elementos de $E(\mathbb{F}_{2^m})$ vienen dadas por pares, si $y_0 \neq y_0 + x_0$, pero esto ocurre siempre y cuando $x_0 \neq 0$. Cuando $x_0 = 0$

el punto $(0, \sqrt{a_6})$ es un punto racional de la curva, ya que $\sqrt{a_6}$ siempre tiene solución para $a_6 \in \mathbb{F}_{2^m}^*$, además se tiene el punto al infinito, por lo cual $|E(\mathbb{F}_{2^m})| = 2l$ para alguna l y como $|E(\mathbb{F}_{2^m})| = 2^m + 1 - t$, entonces $t = 2^m + 1 - |E(\mathbb{F}_2^m)| = 2(2^{m-1} - l) + 1$, con lo que $2 \nmid t$, es decir, $E(\mathbb{F}_2^m)$ es no-supersingular.

Por otro lado si el j-invariante es cero entonces la curva es como en (70). Si (x_0, y_0) es elemento de $E(\mathbb{F}_{2^m})$, se cumple que:

$$y_0^2 + a_3 y_0 = x_0^3 + a_4 x_0 + a_6 \tag{75}$$

y además $(x_0, y_0 + a_3)$ es también elemento de $E(\mathbb{F}_{2^m})$,

$$(y_0 + a_3)^2 + a_3(y_0 + a_3) = x_0^3 + a_4 x_0 + a_6 \tag{76}$$

$$y_0^2 + a_3^2 + a_3 y_0 + a_3^2 = x_0^3 + a_4 x_0 + a_6 \tag{77}$$

$$y_0^2 + a_3 y_0 = x_0^3 + a_4 x_0 + a_6 \tag{78}$$

De esta manera los elementos de $E(\mathbb{F}_{2^m})$ vienen dadas por pares, si $y_0 \neq y_0 + a_3$ lo cual ocurre siempre y cuando $a_3 \neq 0$, como $a_3^4 = \Delta \neq 0$ entonces todas las soluciones vendrán por pares, además del punto al infinito, es decir, $|E(\mathbb{F}_{2^m})| = 2l + 1$ para alguna l y como $|E(\mathbb{F}_{2^m})| = 2^m + 1 - t$, entonces $t = 2^m + 1 - |E(\mathbb{F}_{2^m})| = 2^m + 1 - 2l - 1 = 2(2^{m-1} - l)$, con lo que $2|t$, es decir, $E(\mathbb{F}_{2^m})$ es supersingular.

□

Definición 3.18. *El automorfismo de Frobenius sobre el conjunto de puntos racionales de una curva elíptica $E(\mathbb{F}_{p^s})$ está dado por:*

$$\tau(x, y) = (x^p, y^p) \tag{79}$$

y

$$\tau(P_\infty) = P_\infty \tag{80}$$

Una consideración importante es que dada una curva elíptica $E(\mathbb{F}_q)$ de cardinalidad $q+1-t$ y dado el automorfismo de Frobenius τ entonces se cumple la relación:

$$\tau^2(P) - t\tau(P) + qP = P_\infty \text{ con } P \in E(\overline{\mathbb{F}}_q) \tag{81}$$

es decir:

$$qP = t\tau(P) - \tau^2(P) \text{ con } P \in E(\overline{\mathbb{F}}_q) \tag{82}$$

Ahora bien como se requiere hacer aritmética eficiente y el automorfismo de Frobenius es prácticamente libre, se tiene que la suma de q veces un elemento se simplifica a t adiciones. Por esta razón se buscan curvas con t pequeño. Al valor de t se le llama traza de Frobenius.

3.2.1. Curvas anómalas

El valor más pequeño, en valor absoluto, que puede tomar t es de 0. Esto implica que $qP = -\tau^2(P)$, es decir, la adición de un punto q veces es libre y por tanto se puede realizar aritmética en $E(\mathbb{F}_q)$ de forma muy eficiente. Sin embargo si $t = 0$ esto indica que $E(\mathbb{F}_q)$ es supersingular y no satisface los requerimientos de estos propósitos. Luego el siguiente paso es buscar curvas con $t = \pm 1$.

Definición 3.19. *Una curva elíptica $E(\mathbb{F}_q)$ se dice "anómala" si tiene q elementos. Su " curva deformada" es una curva $\widetilde{E}(\mathbb{F}_q)$ tal que tiene $q + 2$ elementos.*

Si la curva $E(\mathbb{F}_q) : y^2 = x^3 + a_2x^2 + a_6$ esta definida sobre un campo de característica diferente a 2 entonces su curva anómala es de la forma $E(\mathbb{F}_q) : \beta y^2 = x^3 + a_2x^2 + a_6$ donde β es un residuo no cuadrático de $\mathbb{F}_q$, [**23**].

Por ejemplo si consideramos $E(\mathbb{F}_5) : y^2 = x^3 + 3x + 1$, esta es una curva anómala pues las soluciones son: $(0,1), (0,4)(1,0), (2,0), P_\infty$. La "curva deformada" asociada a $E(\mathbb{F}_5)$ es una curva de la forma $\widetilde{E}(\mathbb{F}_5)$: $\beta y^2 = x^3 + 3x + 1$ donde $\beta \in \{2,3\}$ y como:

$C_2(\mathbb{F}_5) : 2y^2 = x^3 + 3x + 1 = \{(1,0), (2,0), (3,0), (4,1), (4,4), P_\infty\}$

$C_3(\mathbb{F}_5) : 3y^2 = x^3+3x+1 = \{(1,0), (2,0), (3,2), (3,3), (4,2), (4,3), P_\infty\}$

luego $\widetilde{E}(\mathbb{F}_5) : 3y^2 = x^3 + 3x + 1$.

Por otro lado, existen $2(2^{m-1} - 1)$ curvas no-supersingulares sobre $\mathbb{F}_2^m$ [1] y son de la forma

$y^2 + xy = x^3 + ax^2 + b$ donde $b \in \mathbb{F}_{2^m}^*$ y $a \in \{0, \gamma\} \subset \mathbb{F}_{2^m}$ y $tr_{\mathbb{F}_2}(\gamma) = 1$

así pues si $E : y^2 + xy = x^3 + ax^2 + b$ es una curva anómala entonces la curva deformada asociada es de la forma $E : y^2 + xy = x^3 + cx^2 + b$ con $tr(b) \neq tr(c)$

Teorema 3.20. *Sea E una curva elíptica anómala sobre $\mathbb{F}_q$ y $\widetilde{E}$ su curva deformada, entonces:*

1. *Si P es un punto de E o de $\widetilde{E}$ entonces qP se determina mediante la adición de dos puntos, que se obtienen fácilmente a partir de P.*
2. *Si $q = 2$ entonces $2^l P$ se expresa como la adición de dos puntos, que se obtienen fácilmente a partir de P con $l = 1, 2, 3, 4$.*

DEMOSTRACIÓN.

1. $qP = \pm\tau(P) - \tau^2(P)$
2. $2 = \pm\tau - \tau^2$

$4 = \pm 2\tau - 2\tau^2 = \pm(\pm\tau - \tau^2)\tau - 2\tau^2 = \tau^2 \mp \tau^3 - 2\tau^2 = \mp\tau^3 - \tau^2$

$8 = (\pm\tau - \tau^2)(\mp\tau^3 - \tau^2) = -\tau^4 \mp \tau^3 \pm \tau^5 + \tau^4 = \mp\tau^3 \pm \tau^5$

$16 = (\mp\tau^3 - \tau^2)^2 = \tau^6 \pm 2\tau^5 + \tau^4 = \tau^6 \pm (\pm\tau - \tau^2)\tau^5 + \tau^4)$
$= \tau^6 + \tau^6 \mp \tau^7 + \tau^4$
$= 2\tau^6 \mp \tau^7 + \tau^4$
$= (\pm\tau - \tau^2)\tau^6 \mp \tau^7 + \tau^4$
$= \pm\tau^7 - \tau^8 \mp \tau^7 + \tau^4$
$= \tau^4 - \tau^8$

□

3.2.2. Curvas anómalas sobre extensiones

Los puntos racionales en una curva anómala, $E(\mathbb{F}_q)$, o en la curva deformada asociada, $\widetilde{E}(\mathbb{F}_q)$, tienen la gran ventaja de que cumplen la relación $\tau^2(P) \pm \tau(P) + qP = P_\infty$ según sea el caso. Sin embargo esto sucede también para cualquier $P \in E(\overline{\mathbb{F}}_q)$ o $P \in \widetilde{E}(\overline{\mathbb{F}}_q)$, es decir, la relación se cumple para cualquier $P \in E(\mathbb{F}_q^m)$ o $P \in \widetilde{E}(\mathbb{F}_q^m)$ según sea el caso.

En cuanto al número de puntos racionales en estas curvas sabemos que se pueden determinar mediante la sucesión $V_0 = 2$, $V_1 = t = \pm 1$, $V_m = V_1 V_{m-1} - qV_{m-2}$ [41]. Además como $E(\mathbb{F}_q) \subset E(\mathbb{F}_{q^m})$ se sigue que $|E(\mathbb{F}_q)|$ divide a $|E(\mathbb{F}_{q^m})|$, como se buscan curvas elípticas con algún subgrupo de orden primo y esto nos indica que el orden de los grupos tienen como factor q ó $q+2$, respectivamente, se da la siguiente definición.

Definición 3.21. *Sea $E(\mathbb{F}_q)$ una curva de orden n, entonces se dice que $E(\mathbb{F}_{q^m})$ tiene orden casi-primo si el orden de esta es hp donde p es un primo, y h es un factor "pequeño" .*

En lo sucesivo el factor h tomará el valor de q o $q+2$, según sea el caso. Este valor recibe el nombre de *cofactor.*

En el campo de los binarios $\mathbb{F}_2$ tenemos sólo dos curvas no-supersingulares:

$$E_0 : y^2 + xy = x^3 + 1 \tag{83}$$

$$E_1 : y^2 + xy = x^3 + x^2 + 1 \tag{84}$$

El conjunto de puntos racionales son:

$E_0(\mathbb{F}_2) = \{(0:1:0), (0:1:1), (1:0:1), (1:1:1)\}$
$E_1(\mathbb{F}_2) = \{(0:1:0), (0:1:1)\}$

Así E_1 es una curva anómala y E_0 es su curva deformada asociada.

Los primeros valores de $(m, |E_1|, \frac{|E_1|}{2})$ para los que $E_1(\mathbb{F}_{2^m})$ tiene orden casi primo son: $(3, 14, 7)$, $(5, 22, 11)$, $(7, 142, 71)$, $(11, 1982, 991)$, $(17, 131174, 65587)$, $(19, 525086, 262543)$, $(23, 8393806, 4196903)$, además de los valores de m: 101, 107, 109, 113, 163, 283, 311, 331, 347, 359, 701, 1153, 1597, 1621, 2063, 2437, 2909, 3319, 6011.

Los primeros valores de $(m, |E_0|, \frac{|E_0|}{4})$ para los que el orden de $E_1(\mathbb{F}_{2^m})$ es casi primo son: $(2, 8, 2)$, $(5, 44, 11)$, $(7, 116, 29)$, $(9, 508, 127)$, $(13, 8012, 2003)$, $(19, 523492, 130873)$, $(23, 8383412, 2095853)$, $(41, 2199025563772, 549756390943)$, $(83, 967140655692318486674275 6, 241785163923079621668568 9)$, $(97, 158456325028528296935114828764, 396140812571320742667787071 91)$, además de los valores de m: 103, 107, 131, 233, 239, 277, 283, 349, 409, 571, 1249, 1913, 2221, 2647, 3169, 3527, 4349, 5333, 5903, 5923, 6701.

Estos valores, al igual que los siguientes se obtienen mediante una rutina implementada en Mathematica 5.1.

En el campo $\mathbb{F}_4$ tenemos 6 curvas no-supersingulares, de las cuales 2 son anómalas:

$$E_\alpha : y^2 + xy = x^3 + \alpha \tag{85}$$

$$E_{\alpha^2} : y^2 + xy = x^3 + \alpha^2 \tag{86}$$

y sus curvas deformadas son:

$$\widetilde{E}_\alpha : y^2 + xy = x^3 + \alpha x^2 + \alpha \tag{87}$$

$$\widetilde{E}_{\alpha^2} : y^2 + xy = x^3 + \alpha x^2 + \alpha^2 \tag{88}$$

donde $\alpha^2 + \alpha + 1 = 0$

El conjunto de puntos racionales son:
$E_\alpha = \{(0:1:0), (0:\alpha^2:1), (\alpha:1:1), (\alpha:\alpha^2:1)\}$
$E_{\alpha^2} = \{(0:1:0), (0:\alpha:1), (\alpha^2:1:1), (\alpha^2:\alpha:1)\}$
$\widetilde{E}_\alpha = \{(0:1:0), (0:\alpha^2:1), (1:\alpha:1), (1:\alpha^2:1), (\alpha^2:0:1), (\alpha^2:\alpha^2:1)\}$
$\widetilde{E}_{\alpha^2} = \{(0:1:0), (0:\alpha:1), (1:0:1), (1:1:1), (\alpha:1:1), (\alpha, \alpha^2)\}$

Los primeros valores de $(m, |E|, \frac{|E|}{4})$ para los que $E_\alpha(\mathbb{F}_{4^m})$ y $E_{\alpha^2}(\mathbb{F}_{4^m})$ tienen orden casi primo son:
$(3, 76, 19)$, $(5, 964, 241)$, $(7, 16636, 4159)$, $(17, 17180108884, 4295027221)$, $(37, 1888946593145781753888 4, 472236648286445438 4721)$, $(43, 773712524553188241781368 76, 193428131138297060445342 19)$, además de los valores de m: 67, 79, 163, 3359.

Los primeros valores de $(m, |E|, \frac{|E|}{6})$ para los que $\widetilde{E}_\alpha(\mathbb{F}_{4^m})$ y $\widetilde{E}_{\alpha^2}(\mathbb{F}_{4^m})$ tienen orden casi primo son:
$(5, 1086, 181)$, $(7, 16134, 2689)$, $(31, 461168601413335805 4, 768614335688893009)$, $(59, 3323069989462289673990344999453266 14, 553844998243714945665057499908877 69)$, además de los valores de m: 167, 227, 379, 1163, 3359.

En el campo $\mathbb{F}_8$ considerando $\gamma^3 = \gamma + 1$ su curva anómala y su deformada son:

$$E : y^2 + xy = x^3 + \gamma \tag{89}$$

$$\widetilde{E} : y^2 + xy = x^3 + x^2 + \gamma \tag{90}$$

El conjunto de puntos racionales son:

$$E = \{(0:1:0), (0:\gamma^4:1), (\gamma^2:\gamma:1), (\gamma^2:\gamma^4:1), (\gamma^5:0:1), (\gamma^5:\gamma^5:1), (\gamma^6:1:1), (\gamma^6:\gamma^2:1)\}$$
$$\widetilde{E} = \{(0:1:0), (0:\gamma^4:1), (1:\gamma^2:1), (1:\gamma^4:1), (\gamma:\gamma^2:1), (\gamma:\gamma^4:1), (\gamma^3:\gamma^4:1), (\gamma^3:\gamma^6:1), (\gamma^4:1:1), (\gamma^4:\gamma^5:1)\}$$

Los primeros valores de $(m, |E|, \frac{|E|}{8})$ para los que $E(\mathbb{F}_{8^m})$ tiene orden casi primo son: $(3, 536, 67)$, $(19, 144115187899137176, 18014398487392147)$,

(23, 590295810319300609336, 73786976289912576167), además de los valores de m: 139, 167, 751, 1489, 1979, 3391.

Los primeros valores de $(m, |E|, \frac{|E|}{10})$ para los que $\widetilde{E}(\mathbb{F}_{8^m})$ tiene orden casi primo son: (7, 2094410, 209441), (11, 8589762730, 858976273), (19, 144115188252574570, 14411518825257457), además de los valores de m: 47, 59.

En base a todo esto se da la siguiente definición:

Definición 3.22. *Una curva de Koblitz es una curva de orden casi primo definida sobre un campo de característica 2, dada por alguna de los siguientes polinomios:*

$$E_0 : y^2 + xy = x^3 + 1 \tag{91}$$

$$E_1 : y^2 + xy = x^3 + x^2 + 1 \tag{92}$$

Capítulo 4

Criptosistemas IBE

Las curvas que no fueron apropiadas para los esquemas usados antes del año 2000 , junto con las herramientas que propiciaron esto fueron utilizados por Boneh y Franklin para proponer su esquema de cifrado [**6**]. Además utilizaron las ideas del IBE propuestas por Shamir en 1984 [**37**] y le dieron un nuevo impulso a la criptografía de curvas elípticas. Estas ideas se presentan en el presente capítulo y se generalizan, con otros esquemas, al caso de la variedad jacobiana de una curva hiperelíptica definida sobre campos finitos, en el siguiente capítulo.

4.1. Definición del IBE

Los criptosistemas basados en una identidad "IBE" (Identity-based encryption) es una variante del esquema de llave pública [**37**]. En cierto sentido se puede decir que es una forma general del esquema de llave pública.

En el esquema IBE, al igual que en el cifrado de llave pública, se tienen parámetros de uso privado, y otros de dominio público; y el esquema debe de garantizar que no se puedan obtener los parámetros privados a partir de los parámetros públicos y del algoritmo para cifrar ó firmar la información.

La diferencia entre un esquema de llave pública y un esquema IBE, radica en que si dos entidades desean compartir información cifrada, usando llave pública sólo bastará que estas entidades acuerden el esquema a seguir y dar a conocer sus llaves públicas, en tanto con un esquema IBE tendrán que acudir a una tercera entidad quien será responsable de generar las llaves que utilizarán, como se muestra en la figura 1

La tercera entidad, conocida como *responsable* o *autoridad* deberá tener la confianza de todos los usuarios del algoritmo, pues esta estará encargada de mantener en secreto parámetros privados del algoritmo.

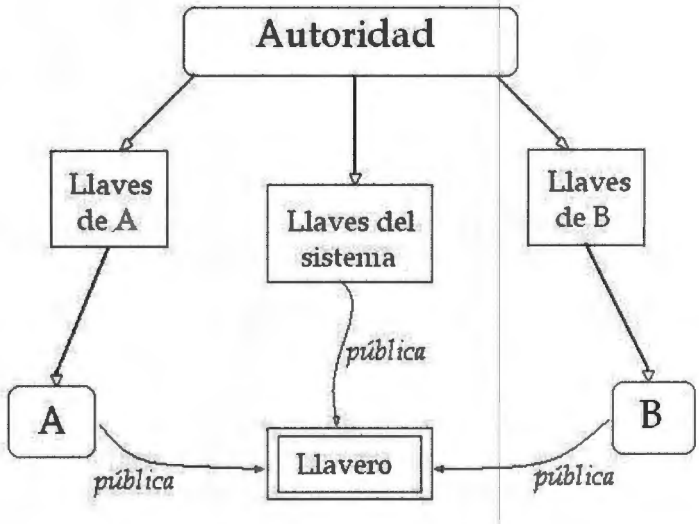

FIGURA 1. Generación de llaves en el esquema IBE

El esquema general de estos sistemas es el siguiente:

Esquema 4.1. *Esquema IBE*

- ***Inicio*** *El responsable del sistema (la autoridad) genera un par de llaves, (x,y), conocidas como la llave maestra y el parámetro del sistema que son valores secretos y públicos respectivamente.*
- ***Generación de llaves*** *El responsable le asigna un parámetro de identificación, ID_A, al usuario A y se crea la llave secreta s_A.*
- ***Cifrado*** *Cuando B quiere mandar el mensaje m a A se usa el ID_A para obtener el cifrado c_A.*
- ***Descifrado*** *A puede recuperar m a partir de c_A y con la ayuda de s_A.*

Los cifrados que utilizan este esquema están basados principalmente en los problemas Diffie-Hellman, como lo son el problema computacional y el problema de decisión, entre otros que se desprenden de estos, así como de las funciones bilineales. Los esquemas de cifrados más destacados son el Boneh-Franklin IBE, el Waters IBE y el Boneh-Boyen IBE [**9**], [**34**].

Las funciones bilineales, que se usan en estos esquemas requieren de otra propiedad que es la no degeneración. Estas funciones son conocidas como *"pairings"*, aquí se les denominará mapeos bilineales no degenerados o simplemente mapeos bilineales.

Definición 4.2. *Dados los grupos* $\mathbb{G}$, $\widehat{\mathbb{G}}$ *(aditivos) y* $\widetilde{\mathbb{G}}$ *(multiplicativo) se define un "pairing" como un mapeo bilineal no-degenerado*

$$e : \mathbb{G} \times \widehat{\mathbb{G}} \longrightarrow \widetilde{\mathbb{G}} \tag{93}$$

Esto quiere decir que para $P, Q \in \mathbb{G}$ y $R, S \in \widehat{\mathbb{G}}$

- *Bilinealidad*
  $e(P+Q, R) = e(P, R)e(Q, R)$
  $e(P, R+S) = e(P, R)e(P, S)$
- *No degeneración*
  Si $P \in \mathbb{G}$ entonces $e(P, 0_{\widehat{\mathbf{G}}}) = 1_{\widetilde{\mathbf{G}}}$ y si $e(P, R) = 1_{\widetilde{\mathbf{G}}}$ para cualquier $R \in \widehat{\mathbb{G}}$ entonces $P = 0_{\mathbf{G}}$

Ejemplo 4.3. *Un ejemplo de estas formas bilineales se puede dar de la siguiente forma: sean* g, $\widehat{g}$ *y* $\widetilde{g}$, *generadores de los grupos* $\mathbb{G}$, $\widehat{\mathbb{G}}$ *y* $\widetilde{\mathbb{G}}$, *respectivamente, entonces se define* $e(ag, b\widehat{g}) = \widetilde{g}^{ab}$.

En la gran mayoría de los casos, para las aplicaciones criptográficas se consideran sólo dos grupos tomando a $\widehat{\mathbb{G}} = \mathbb{G}$, bajo esta consideración se dice que un mapeo es simétrico si $e(P, Q) = e(Q, P)$, como el mapeo de Tate, y se dice que es asimétrico si se satisface que $e(P, Q) = e(Q, P)^{-1}$, como el de Weil.

Si se considera un mapeo e, asimétrico y $\mathbb{G} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ entonces existen $U, V \in \mathbb{G}$ tal que si $P, Q \in \mathbb{G}$, existen $a, b, c, d \in \mathbb{Z}$ con la propiedad de que $P = aU + bV$ y $Q = cU + dV$ de tal forma que a la pareja $(P, Q) \in \mathbb{G} \times \mathbb{G}$ esta asociada a la matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ teniéndose de esta forma:

$$\begin{aligned} e(P, Q) &= e(aU + bV, cU + dV) \\ &= e(U, U)^{ac} e(U, V)^{ad-bc} e(V, V)^{bd} \end{aligned} \tag{94}$$

además en el caso en que se tenga que $e(U, U) = e(V, V) = 1_{\widetilde{\mathbf{G}}}$ el mapeo se reducirá a $e(P, Q) = e(U, V)^{det(A)} = \omega^{det(A)}$ donde ω es un generador de $\widetilde{\mathbb{G}}$, el mapeo de Weil es un ejemplo de mapeo con estas propiedades y esto permite una evaluación más eficiente, aunque no es la óptima [9].

4.1.1. Esquema Boneh-Franklin

Este esquema fue publicado en el 2003 por Dan Boneh y Matt Franklin en SIAM Journal of Computing [6]. La importancia de este trabajo es que es el primero en el cual se presenta el esquema IBE utilizando curvas elípticas y mapeos bilineales. A partir de este trabajo la

investigación en esta dirección se desarrolló rápidamente. La estructura es la siguiente:

Esquema 4.4. *Boneh-Franklin IBE*

- ***Inicio***
  - *Dados los grupos finitos cíclicos* $\mathbb{G}$, *y* $\widetilde{\mathbb{G}}$ *del mismo orden* p *primo y* $k = |p|_2$
  - *Se selecciona* g *un generador de* $\mathbb{G}$
  - *Definir funciones hash (compresión)*
    - $H_1 : \mathbb{F}_2^k \to \mathbb{G}$ $\qquad H_2 : \widetilde{\mathbb{G}} \to \mathbb{F}_2^k$
    - $H_3 : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{Z}_p^*$ $\qquad H_4 : \mathbb{F}_2^k \to \mathbb{F}_2^k$
  - *Seleccionar aleatoriamente* $x \in \mathbb{Z}_p^*$
  - *Calcular* $y = g^x$
  - *Parámetro público del sistema* $(g, y, H_1, H_2, H_3, H_4)$
  - *Llave maestra* (x)
- ***Generación de llaves particulares al usuario A***
  - *Elegir un elemento* $a \in \mathbb{F}_2^k$
  - *Obtener* $ID_A = h_A = H_1(a)$ *(llave pública)*
  - *Calcular* $s_A = h_A^x$ *(llave privada)*
- ***Cifrado de un mensaje para el usuario A***
  - *El mensaje a enviar es* $m \in \mathbb{F}_2^k$
  - *Generar aleatoriamente* $\sigma \in \mathbb{F}_2^k$
  - *Obtener* $r = H_3(\sigma, m)$
  - *Calcular* $C_1 = g^r$ *y* $C_2 = \sigma \oplus H_2(e(h_A, y)^r)$
  - *Calcular* $C_3 = m \oplus H_4(\sigma)$
- ***Descifrado de un mensaje recibido por el usuario A***
  Dado $C = (C_1, C_2, C_3)$ *y conocida la llave secreta* s_A
  - *Recuperar* $\sigma = C_2 \oplus H_2(e(s_A, C_1))$
  - *Recuperar el mensaje* $m = C_3 \oplus H_4(\sigma)$

Es fácil ver que sí se recupera el mensaje. Esto se sigue de que $C_3 = m \oplus H_4(\sigma)$ con lo cual se tiene:

$$\begin{aligned} C_3 \oplus H_4(\sigma) &= m \oplus H_4(\sigma) \oplus H_4(\sigma) \\ &= m \end{aligned} \tag{95}$$

Además de que se está recuperando adecuadamente σ ya que

$$\begin{aligned} e(s_A, C_1) &= e(h_A^x, g^r) \\ &= e(h_A, y)^r \end{aligned} \tag{96}$$

Ejemplo 4.5. *Para este ejemplo se considerará a los grupos* $\mathbb{G} = \mathbb{Z}_{29}$ *y* $\widehat{\mathbb{G}} = \mu_{29}$, *con lo cual* $p = 29$, *y* $k = 5$. *Se seleccionan* $g = 21$ *y* $\widehat{g} = \zeta_1^2$ *como generadores de* $\mathbb{Z}_{29}$ *y* μ_{29} *respectivamente, se define la función*

bilineal dada por: $e(tg, sg) = \widehat{g}^{ts}$. *Además de considerar las siguientes funciones de compresión:*

$H_1 : \mathbb{F}_2^5 \to \mathbb{Z}_{29}$ *dada por:* $(x_0, x_1, x_2, x_3, x_4) \mapsto \sum_{i=0}^{4} x_i * 2^i \pmod{29}$

$H_2 : \mu_{29} \to \mathbb{F}_2^5$ *dada por:* $\zeta_1^n \mapsto P(n_2)$ *y* $P(x_0, x_1, x_2, x_3, x_4) = (x_1, x_3, x_0, x_2, x_4)$

$H_3 : \mathbb{F}_2^5 \times \mathbb{F}_2^5 \to \mathbb{Z}_{29}^*$ *dada por:* $\overline{x} \mapsto \sum_{i=0}^{9} x_i * 2^i \mod 28$

y la función de permutación:

$H_4 : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ *dada por:* $\overline{l} \mapsto (x * \sum l_i 2^i)_2$

Considérese que se obtiene aleatoriamente $x = 13$ *y así* $y = 13(21) = 12 \mod 29$. *Luego el parámetro del sistema (público) es* $(g, y) = (21, 12)$ *y la llave maestra (privada) es* $x = 13$. *Se desea cifrar "NO".*

Solución.

Para obtener los parámetros de un usuario se obtiene de forma aleatoria $a = 01010 \in \mathbb{F}_2^5$ y se calcula $h_A = H_1(01010) = 10$ y además se tiene que $s_A = 13(10) = 14$ teniendo así que la llave pública del usuario es $h_A = 10$ y la llave privada es $s_A = 14$.

Cifrado, se tiene que el campo $\mathbb{F}_{2^5}$ tiene 32 elementos, por lo cual se debe considerar un alfabeto con 32 elementos, consideremos el alfabeto español con la siguiente asignación A=0, B=1, $\cdots$, Z=26, Á=27, É=28, Í=29, Ó=30, Ú=31, como se desea cifrar "NO", es decir, 01101, 01111 en $\mathbb{F}_2^5$; generando aleatoriamente $\sigma_0 = 10001$ y $\sigma_1 = 10110$ se obtiene $r_0 = H_3(10001, 01101)$ y $r_1 = H_3(10110, 01111)$

M	$m \in \mathbb{F}_2^5$	σ	r	C_1	$e(h_a, y)^r$	H_2	C_2	$H_4(\sigma)$	C_3	(c_1, c_2, c_3)
N	01101	10001	21	6	ζ_1^{28}	10110	00111	10010	11111	(G,H,U)
O	01111	10110	19	22	ζ_1^{6}	01010	11100	11001	10110	(V,É,V)

Teniendo así que el mensaje cifrado es GHU VEV.

Para recuperar el mensaje, teniendo en cuenta que $s_A = 14$ se hacen los siguientes cálculos:

C_1	C_2	C_3	$e(s_A, C_1)$	H_2	σ	H_4	m	m
6	00111	11111	ζ_1^{28}	10110	10001	10010	01101	n
22	11100	10110	ζ_1^{6}	01010	10110	11001	01111	o

Recuperando así el mensaje original *NO*.

■

4.1.2. Esquema Boneh-Boyen

El esquema presentado por Boneh y Boyen [8], tiene la ventaja sobre el anterior que no requiere de definir funciones adicionales como son las de compresión que son necesarias en el esquema anterior, sin embargo si se obtienen algunos inversos que dependiendo del grupo que se utilize puede significar un costo significativo de cómputo. El esquema es el siguiente:

Esquema 4.6. *Boneh-Boyen IBE*

- ***Inicio***
  - *Dados los grupos cíclicos finitos* $\mathbb{G}$, *y* $\widehat{\mathbb{G}}$ *del mismo orden* p *primo.*
  - $e : \mathbb{G} \times \mathbb{G} \to \widehat{\mathbb{G}}$ *una función bilineal*
  - *Se selecciona* g *un generador de* $\mathbb{G}$
  - *Se generan aleatoriamente* $x, y \in \mathbb{Z}_p^*$
  - *Se obtiene* $X = g^x$ *y* $Y = g^y$
  - *El parámetro del sistema es* (g, X, Y)
  - *La llave maestra es* (x, y).
- ***Generación de llaves***
  - *Se elige un* $v \in \mathbb{Z}_p^*$ *como ID.*
  - *El usuario selecciona aleatoriamente* $r \in \mathbb{Z}_p$
  - *Se obtiene* $K = g^{\frac{1}{v+x+ry}}$
  - *La llave secreta será* $d = (r, K)$
- ***Cifrado***
  - *El mensaje a cifrar es* $m \in \widehat{\mathbb{G}}$
  - *Se selecciona aleatoriamente* $s \in \mathbb{Z}_p^*$.
  - *Se obtienen los valores de* $C_1 = g^{sv}X^s$, $C_2 = Y^s$, $C_3 = e(g,g)^s m$
  - *El mensaje cifrado es la tripleta:* $C = (C_1,\ C_2,\ C_3)$
- ***Descifrado*** *Dada la tripleta* $C = (C_1, C_2, C_3)$
  - *Se calcula* $z = e(C_1 C_2^r, K)$
  - *Se obtiene* $m = \frac{C_3}{z}$

Se puede verificar fácilmente que el mensaje se recupera de forma correcta, para esto solo basta con ver que $z = e(g,g)^s$.

$$z = e(C_1 C_2^r, K) = e(g^{sv}X^s(Y^s)^r, g^{\frac{1}{v+x+ry}}) = e(g^{sv}(g^x)^s((g^y)^s)^r, g)^{\frac{1}{v+x+ry}} \tag{97}$$

por lo tanto

$$z = e(g^{sv+sx+sry}, g)^{\frac{1}{v+x+ry}} = e(g,g)^s \tag{98}$$

Aunque el esquema, definido originalmente está planteado para grupos de orden primo, en general no es requisito indispensable para el correcto funcionamiento, pero sí para una mejor implementación.

Ejemplo 4.7.

Para este ejemplo, al igual que en el ejemplo (4.5) se consideraran a los grupos $\mathbb{G} = \mathbb{Z}_{29}$ *y* $\widehat{\mathbb{G}} = \mu_{29}$, *con lo cual* $p = 29$, *y a los generadores* $g = 21$ *y* $\widehat{g} = \zeta_1^2$ *de* $\mathbb{Z}_{29}$ *y* μ_{29} *respectivamente y la función bilineal dada por:* $e : (kg, sg) \mapsto \widehat{g}^{ks}$. *Luego obtenemos aleatoriamente* $x = 13$ *y* $y = 11$ *y se calcula* $X = 13(21) = 12$ *y* $Y = 11(21) = 28$.

Así pues el parámetro del sistema (público) es $(g, X, Y) = (21, 12, 28)$ *y la llave maestra (privada) es* $(x, y) = (13, 11)$. *Se desea cifrar SI.*

Solución.

Para obtener los parámetros de un usuario se obtiene de forma aleatoria $v = 8 \in \mathbb{Z}_{29}^*$ y $r = 5 \in \mathbb{Z}_{29}$ y se calcula $K = \frac{1}{v+x+ry} g = \frac{1}{8+13+(5)(11)}(21) = \frac{21}{18} = 6$, teniendo así que la llave pública del usuario es $v = 8$ y la llave privada es $(r, K) = (5, 6)$.

Cifrado: Tenemos que el grupo es de orden 29 por lo cual se debe elegir un alfabeto con 29 elementos, consideremos el alfabeto español junto con " " y ".", asignando " " = 0, "." = 28 y los demás en el orden habitual. Supónganse que se desea cifrar "SI", es decir, ζ^{20}, ζ^9 en μ_{29}; generando aleatoriamente $s_S = 23$ y $s_I = 9$, se tiene que:

M	μ_{29}	s	sv	svg	sX	$svg + sX$	sY	$e(g,g)^s$	$e(g,g)^s m$	c
S	ζ^{20}	23	10	7	15	22	6	ζ_1^{17}	ζ^8	h
I	ζ^9	9	14	4	21	25	20	ζ_1^{18}	ζ^{27}	z

teniendo así que el mensaje cifrado es $(22, 6, \zeta_1^8)(25, 20, \zeta_1^{27}) = RTH\ PHZ$.

Para recuperar el mensaje, teniendo en cuenta que $r = 5$ y $K = 17$ se hacen los siguientes cálculos:

C_1	C_2	C_3	rC_2	$C_1 + rC_2$	$e(C_1 + rC_2, K)$	$\frac{C_3}{e(C_1 C_2^r, K)}$	m
22	6	ζ^8	$5(\ 6) = \ 1$	23	$e(23, 6) = \zeta^{17}$	$\zeta^{8-17} = \zeta^{-9}$	s
25	20	ζ^{27}	$5(20) = 13$	9	$e(\ 9, 6) = \zeta^{14}$	$\zeta^{27-18} = \zeta^9$	i

Recuperando así el mensaje original *SI.*

■

4.2. Firma digital

4.2.1. Firma de Boneh-Boyen

El esquema de firma digital presentado por Boneh y Boyen [7], al igual que el esquema de cifrado, está basado en los mapeos y en lo problemas Diffie-Hellman, el esquema de firma es el siguiente:

Esquema 4.8.

- *Generación de Llaves para el usuario B*
  - *Dados* $(\mathbb{G}, \widehat{\mathbb{G}}, p, k = |p|_2)$
  - *Elegir* $g \in \mathbb{G}$ *un generador.*
  - *Obtener aleatoriamente* $x_b, y_b \in \mathbb{Z}_p^*$
  - *Calcular* $u_b = g^{x_b}$ *y* $v_b = g^{y_b}$
  - *La llave pública será* (g, u_b, v_b) *y la privada* (x_b, y_b).
- *Firma*
  - *Conocida la llave secreta* (x_b, y_b) *y un mensaje* $m \in \mathbb{Z}_p^*$
  - *Seleccionar aleatoriamente* $r \in \mathbb{Z}_p^*$
  - *Calcular* $\sigma = g^{\frac{1}{x_b+m+y_b r}}$
  - *La firma es* (σ, r)
- *Validación*
  - *Se conoce la llave pública* (g, u, v), *el mensaje* m *y su firma* (σ, r)
  - *Calcular* $f_1 = e(\sigma, ug^m v^r)$
  - *Obtener* $f_2 = e(g, g)$
  - *Si* $f_1 = f_2$ *entonces la firma es válida*

Efectivamente f_1 debe de ser igual a f_2 ya que:

$$
\begin{aligned}
f_1 = e(\sigma, ug^m v^r) &= e(\sigma, g^{x_b} g^m g^{y_b r}) \\
&= e(g^{\frac{1}{x_b+m+y_b r}}, g^{x_b+m+y_b r}) \\
&= e(g, g) = f_2
\end{aligned} \tag{99}
$$

Ejemplo 4.9.

Supónganse que se desea firmar el mensaje enviado en el ejemplo (4.7), de igual forma se toma $\mathbb{G} = \mathbb{Z}_{29}$ *y* $\widehat{\mathbb{G}} = \mu_{29}$, *con lo cual* $p = 29$. *Sean* $g = 21$ *y* ζ_1 *generadores de* $\mathbb{Z}_{29}$ *y* μ_{29} *respectivamente, se considera*

la función bilineal dada por: $e : (k, s) \mapsto \zeta^{10*k*s}$, *teniendo en este caso que* $e(21, 21) = \zeta^2$.

Solución.

Se generan aleatoriamente la llave privada del usuario B $x_B = 3$ y $y_B = 20$, y se obtiene su llave pública $u_B = (3)21 = 5$ y $v_B = (20)21 = 14$, teniendo así la llave privada $(x_B, y_B) = (3, 20)$ y la llave pública $(u_B, v_B) = (5, 14)$.

Se desea firmar el mensaje cifrado en (4.7), es decir, "$RTD\ PHO$" $= (19, 21, 4, 17, 8, 16)$, usando la función hash definida en (2.6), usando a "$V = 23$" como valor inicial, entonces se tiene la sucesión:

- $h_0 = 23$,
- $h_1 = g(23, 19) = 23 * 19 + 23 + 19 = 15$,
- $h_2 = g(15, 21) = 15 * 21 + 15 + 21 = 3$,
- $h_3 = g(3, 4) = 3 * 4 + 3 + 4 = 19$,
- $h_4 = g(19, 17) = 19 * 17 + 19 + 17 = 11$,
- $h_5 = g(11, 8) = 11 * 8 + 11 + 8 = 20$,
- $h_6 = g(20, 16) = 20 * 16 + 20 + 16 = 8$,

así pues el mensaje es "H" $= 8$.

Se selecciona aleatoriamente $r = 12$ y se obtiene $s = 3+8+20*12 = 19$ y como $s \in \mathbb{Z}_{29}^*$ y además $s^{-1} = 26$ se obtiene $\sigma = (26)21 = 24$ teniendo que la firma es $(24, 12) = WL$, es decir, se envía:

"$RTD\ PHO\ WL$"

Para verificar la firma se calcula

$$f_1 = e(\sigma, ug^m v^r) = e(24, 5 + (8)21 + (12)14) = e(24, 22) = \zeta^2$$

y como coinciden los valores de f_1, y $e(21, 21)$, entonces la firma es válida.

■

Capítulo 5

El IBE y las curvas hiperelípticas

El esquema IBE, es un caso especial de los esquemas de llave pública, su principal característica es la existencia de una autoridad que es la encargada de asignar las llaves a la vez que es quien protege la llave maestra del sistema.

Los problemas Diffie-Hellman juegan un papel trascendente en la fortaleza para estos esquemas. Adicionalmente existen los co-problemas. Los mapeos bilineales no degenerados, *pairings*, más conocidos son el de Weil y el de Tate, y recientemente se han creado el mapeo Eta y el Ate, los cuales provienen del mapeo de Tate. Todos estos mapeos esencialmente se definen sobre subgrupos del m-ésimo grupo de torsión al grupo de las raices m-ésimas de la unidad. Los mapeos son definidos tradicionalmente sobre curvas elípticas.

Se verá como usarlo en curvas de género mayor a 1, para aplicar los esquema IBE, y se darán algunos ejemplos con grupos de orden pequeño.

5.1. Los problemas de Diffie-Hellman

Los problemas de Diffie-Hellman son muy importantes para la criptografía IBE. La intratabilidad de los problemas propicia la fortaleza en los esquemas, contra ataques de critptoanálisis.

Para definir estos problemas, esencialmente se requiere un grupo (aditivo) $\mathbb{G}$. Además se necesita un grupo (multiplicativo) $\widetilde{\mathbb{G}}$ y un mapeo bilineal e para el problema bilineal. Los problemas son los siguientes:

1. *El Problema Computacional Diffie-Hellman* (CDHP):
   Dados $P, aP, bP \in \mathbb{G}$ obtener abP.
2. *El Problema de Decisión Diffie-Hellman* (DDHP):
   Dados $P, aP, bP, cP \in \mathbb{G}$ Decidir si $abP = cP$.

3. *El Problema Gap Diffie-Hellman* (GDHP):
   Resolver el CDHP en $\mathbb{G}$ resolviendo el DDHP usando algún algoritmo.
4. *El Problema Bilineal Diffie-Hellman* (BDHP):
   Dados $P, aP, bP, cP \in \mathbb{G}$ y un mapeo bilineal $e : \mathbb{G} \times \mathbb{G} \mapsto \widetilde{\mathbb{G}}$ obtener $e(P,P)^{abc}$

De forma similar se pueden definir problemas similares a estos, llamados co-problemas, los cuales son más generales al considerar dos o tres grupos, $\mathbb{G}$, $\widehat{\mathbb{G}}$, $\widetilde{\mathbb{G}}$, dependiendo del problema. La intratabilidad de estos problemas de igual forma sirven como base en la seguridad de cifrados.

1. Co-CDHP:
   Dados $P, aP \in \mathbb{G}$ y $Q \in \widehat{\mathbb{G}}$ obtener aQ
2. Co-DDHP:
   Dados $P, aP \in \mathbb{G}$ y $Q, bQ \in \widehat{\mathbb{G}}$, donde P y Q son del mismo orden, Decidir si $a = b$ módulo el orden de P.
3. Co-GDHP:
   Resolver el Co-CDHP en $\mathbb{G}, \widehat{\mathbb{G}}$ resolviendo el Co-DDHP mediante algún algoritmo.
4. Co-BDHP:
   Dados $P, aP, bP, \in \mathbb{G}$, $Q \in \widehat{\mathbb{G}}$ y un mapeo bileneal $e : \mathbb{G} \times \widehat{\mathbb{G}} \mapsto \widetilde{\mathbb{G}}$ calcular $e(P,Q)^{ab}$

En la verificación que se realiza para comprobar que el mensaje se está recuperando, tanto en el esquema de Boneh-Franklin como en el de Boneh-Boyen, se puede ver claramente la importancia de que este último problema sea intratable computacionalmente.

5.2. Mapeos bilineales

Debido a que la gran mayoría de los cifrados del tipo IBE basan su seguridad en el problema bilineal de Diffie-Hellman, en esta sección se veran cuáles son las diferencias al utilizar la jacobiana.

El mapeo de Weil está definido sobre el m-ésimo grupo de torsión de una curva elíptica, pero en la definición a cada punto se le asocia un divisor, por lo que no hay problema en extender la definición a curvas hiperelípticas, usando la definición alternativa [**28**], [**25**].

Definición 5.1. *El Mapeo de Weil sobre la curva hiperelíptica $C(\mathbb{F}_q)$ se define como el mapeo bilineal del m-ésimo grupo de torsión de $\mathcal{J}$ ($\mathcal{J}[m]$)*

al grupo de las raíces m-ésimas de la unidad. Aquí se debe considerar que m y q son primos relativos.

$$e_m : \mathcal{J}[m] \times \mathcal{J}[m] \to \mu_m \tag{100}$$

dado por:

$$e_m(S,T) = \frac{f_A(B)}{f_B(A)} \tag{101}$$

donde $S,T \in \mathcal{J}[m]$, $A,B \in Div(C)$ *y* $f_A, f_B \in Div(\mathbb{F}(C))^*$ *tales que* $A \sim (S)$, $B \sim (T)$, $div(f_A) = mA$, $div(f_B) = mB$ *y A,B tienen soporte ajeno.*

El mapeo extendido de Weil conserva todas las propiedades, y la demostración de estas son iguales que en el caso de las curvas elípticas con la excepción del caso de la no degeneración.

Para verificar que el mapeo es no degenerado sólo basta considerar una extensión adecuada, es decir, una extensión $\mathbb{F}_{q^k}$ tal que $m|q^k - 1$ y $m^2|\#\mathcal{J}(C(\mathbb{F}_{q^k}))$.

5.3. El mapeo de Tate

Junto con el mapeo de Weil, el mapeo de Tate es otro de los más utilizados, además a últimas fechas se han definido varios mapeos basado en este último, como lo son el Eta y el Ate.

En esta sección se considerara que

$$\left(\mathbb{F}_{q^k}^*\right)^m = \{x^m : x \in \mathbb{F}_{q^k}^*\}. \tag{102}$$

Definición 5.2. *Considerando la notación anterior y a m un entero tal que este es coprimo con p (la característica del campo). El mapeo de Tate*

$$\langle \cdot, \cdot \rangle_m : \mathcal{J}[m] \times \frac{\mathcal{J}(\mathcal{C})}{m\mathcal{J}(\mathcal{C})} \to \frac{\mathbb{F}_{q^k}^*}{\left(\mathbb{F}_{q^k}^*\right)^m} \tag{103}$$

está definido por:

$$\langle P, Q \rangle_m = G(D) \tag{104}$$

donde G es una función racional tal que $div(G) = mP$, *k es el menor entero que satisface* $m|q^k - 1$ *y* $m^2|\#\mathcal{J}(\mathcal{C}(\mathbb{F}_{q^k}))$, *y D es un divisor en la clase de P tal que* $supp(P) \cap supp(D) = \emptyset$.

Una observación interesante es que el mapeo de Weil se puede definir a partir del mapeo de Tate, para esto es necesario realizar primero las siguientes observaciones.

En la implementación de los algoritmos de cifrado es necesario conocer con exactitud cuál es el representante con el que se trabaja por lo cuál se aprovecha el hecho de que

$$\frac{\mathcal{J}(\mathcal{C})}{m\mathcal{J}(\mathcal{C})} \cong \mathcal{J}[m] \tag{105}$$

y al considerar a $\mathbb{F}_{q^k}^* / \left(\mathbb{F}_{q^k}^*\right)^m \cong \mu_m$, el mapeo reducido de Tate es:

$$\begin{aligned} \langle \cdot, \cdot \rangle_m : \mathcal{J}[m] \times \mathcal{J}[m] &\to \mu_m \\ \langle P, Q \rangle_m &= G(D)^{(q^k-1)/m} \end{aligned} \tag{106}$$

Esta definición es la que se utilizará en lo sucesivo, y recordando el mapeo de Weil se tiene que

$$e_m(P,Q) = \frac{G_A(B)}{G_B(A)} = \frac{\langle P, Q \rangle_m}{\langle Q, P \rangle_m} \tag{107}$$

relacionando así los dos mapeos más importantes.

Teorema 5.3. *El mapeo de Tate satisface las siguientes propiedades:*

1. *Es bilineal.*
2. *Es no degenerado. i.e.* $\langle P, Q \rangle \neq 1$ *para algunos* P, Q,
3. *Es compatible.*

DEMOSTRACIÓN.

1. Es bilineal.
   Sean $S \in \mathcal{J}[m], T = \sum_{P \in \mathcal{C}} m_P P, R = \sum_{P \in \mathcal{C}} n_P P \in \mathcal{J}(\mathcal{C})/m\mathcal{J}(\mathcal{C})$ divisores, tales que $supp(S) \cap supp(T)$, $supp(S) \cap supp(R)$ y f una función racional para la cual se cumple que $div(f) = mS$, entonces

   $$\begin{aligned} \langle S, T + R \rangle_m &= \prod_{P \in \mathcal{C}} f(P)^{m_P + n_P} \\ &= \prod_{P \in \mathcal{C}} f(P)^{m_P} \prod_{P \in \mathcal{C}} f(P)^{n_P} \\ &= \langle S, T \rangle_m \langle S, R \rangle_m \end{aligned}$$

   Ahora bien, si $S, T \in \mathcal{J}[m], R \in \mathcal{J}(\mathcal{C})/m\mathcal{J}(\mathcal{C})$ son divisores, tales que $supp(S) \cap supp(R)$, $supp(T) \cap supp(R)$ y f_T, f_S son funciones racionales tales que $div(f_T) = mT, div(f_S) = mS$, entonces de aquí se tiene que $div(f_T \cdot f_S) = m(S + T)$ y

   $$\begin{aligned} \langle S + T, R \rangle_m &= (f_T \cdot f_S)(R) \\ &= f_T(R) \cdot f_S(R) \\ &= \langle T, R \rangle_m \langle S, R \rangle_m \end{aligned}$$

2. Es no degenerado.

   Sea $P \in \mathcal{J}[m]$ como el mapeo de Weil es no degenerado entonces existe $Q \in \mathcal{J}[m]$ tal que $e_m(P,Q) \neq 1$, si $x \in \mu_m$ es un generador entonces existen enteros a, b, c tales que $0 < a < m$, $0 \leq b, c < m$ y $e_m(P,Q) = x^a$, $\langle P,Q\rangle_m = x^b$, $\langle Q,P\rangle_m = x^c$, con lo que se tiene $x^a = \frac{x^b}{x^c}$, es decir, $a + c \equiv b \mod m$ de esta forma si $b = 0$ entonces $c \neq 0$ y $\langle Q,P\rangle_m \neq 1$ y si $b \neq 0$ entonces $\langle P,Q\rangle_m \neq 1$ y así el mapeo es no degenerado.
3. Es compatible.

   Sea $S \in \mathcal{J}[m]$, $T \in \mathcal{J}[m \cdot n]$ dos divisores y sean f_{mn}, f_m funciones racionales para las que se cumple que $div(f_{mn}) = mnS$ y $div(f_m) = mS$, entonces $div(f_{mn}) = div(f_m^n)$ lo cual implica

   $$\langle S,T\rangle_{m\cdot n} = f_{mn}(T) = f_m^n(T) = f_m(nT) = \langle S,nT\rangle_m$$

   la segunda igualdad se sostiene por que T es un divisor de grado cero.

□

Ejemplo 5.4. *Sea C una curva hiperelíptica dada por:*

$$v^2 + u^7 + u^6 + u^5 + u^2 + 1 = 0$$

sobre $\mathbb{F}_{3^3}$, y considere que x es tal que $x^3 - x + 1 = 0$, luego $P = (1,1) - P_\infty$ y $Q = (x,x^2) - (1,2)$ son dos divisores en la jacobiana.

La representación de estos divisores en términos de funciones racionales está dada por:

$$P = (1,1) - P_\infty = div(u - 1, 1) \quad Q = (x,x^2) - (1,2) = (u - x, x^2)$$

utilizando el algoritmo 1.44 se tiene que su orden es 26, y se observa en estos cálculos que los grupos generados son diferentes, de esta forma se puede garantizar la no degeneración del mapeo de Weil y por ende la no degeneración del mapeo de Tate.

Para obtener la función racional G tal que $div(G) = 26P$ sólo basta encontrar una función que satisfaga $G(1,1) = 0$ y $N(G) = (u-1)^{26}$, si

$$G(u,v) = \begin{array}{c} u^{13} + u^{11} + u^8 - u^7 + u^6 - u^5 + u^3 - u^2 + u - 1 - \\ v(-u^9 + u^8 + u^7 + u^6 - u^3 - u^2 - u) \end{array}$$

cumple con la condición, de esta forma se puede obtener

$$\langle P,Q\rangle_{26} = (G(Q))^{\frac{27-1}{26}} = G((x,x^2) - (1,2)) = \frac{G(x,x^2)}{G(1,2)} = \frac{x^6}{1} = x^6.$$

5.4. Curvas hiperelípticas y mapeos bilineales

Un aspecto importante en la evaluación de estos mapeos es la selección de los representante para que tenga soporte ajeno, para conseguir esto tenemos el siguiente teorema.

Teorema 5.5. *Sea C un curva hiperelíptica y sean P, Q divisores reducidos de dicha curva, entonces existen divisores A, B tales que $A \sim P$ y $B \sim Q$ y además $supp(A) \cap supp(B) = \emptyset$.*

DEMOSTRACIÓN. Sea C una curva hiperelíptica de género g, definida sobre $\mathbb{F}_q$ considérese que los divisores se encuentran en $\mathbb{F}_{q^k}$ y además $q^k \geq 2g + 1$, y considérese que los divisores son de la forma

$$P = \sum_{P_i \in C \setminus \{P_\infty\}} m_i P_i - mP_\infty$$

$$Q = \sum_{P_i \in C \setminus \{P_\infty\}} n_i P_i - nP_\infty$$

Luego existe $x_\infty \in \mathbb{F}_{q^k}$ tal que $supp(A) \cap supp(div(u - x_\infty)) = \emptyset$ y $supp(B) \cap supp(div(u - x_\infty))$, y además existe y_∞ tal que $supp(A) \cap supp(div(v - y_\infty)) = \emptyset$ y $supp(B) \cap supp(div(v - y_\infty))$.

Así pues, $\frac{(u-x_\infty)^g}{v-y_\infty}$ es un parámetro uniformizante de P_∞, y además

$$P \sim P' = P - mdiv\left(\frac{(u - x_\infty)^g}{v - y_\infty}\right)$$

Si $R = (x_r, y_r) \in C_1 = supp(P') \cap supp(Q)$ es un punto ordinario, luego $u - x_r$ es un parámetro uniformizante de R. Luego

$$Q \sim Q' = Q - \sum_{P_i \in C_1} -n_i div(u - x_i)$$

Si $S = (x_s, y_s) \in C_2 = supp(P') \cap supp(Q')$ es un punto especial, luego $v - y_s$ es un parámetro uniformizante de S. Luego

$$Q' \sim Q'' = Q' - \sum_{P_i \in C_2} -n_i div(v - y_i)$$

De esta forma se tiene que $supp(P') \cap supp(Q'') = \emptyset$. Definiendo $A = P'$ y $B = Q''$, se tiene lo deseado.

□

En la selección de la curva a utilizar es necesario poder garantizar que tiene subgrupos de determinado orden, por lo cuál es necesario

conocer el número de elementos en la jacobiana, para obtener el número de elementos se realiza el siguiente análisis.

Para las curvas hiperelípticas se tiene la siguiente relación [**29**]

$$e^{\sum_{r\geq 1} M_r \frac{t^r}{r}} = \frac{P(t)}{(1-t)(1-qt)} \tag{108}$$

donde:

M_r: es el número de puntos racionales en $C(\mathbb{F}_{q^r})$ y $P(t)$ es un polinomio de grado $2g$ con coeficientes en $\mathbb{Z}$, en particular este polinomio es de la forma:

$$P(t) = 1 + a_1 t + \cdots + a_g t^g + q a_{g-1} t^{g+1} + \cdots + q^g t^{2g} \tag{109}$$

Determinar este polinomio es posible conociendo el número de puntos racionales sobre $\mathbb{F}_q$, $\mathbb{F}_q^2$, $\cdots$ $\mathbb{F}_q^g$. Esto se logra tomando el logaritmo natural en (108) obteniendo:

$$\sum_{r\geq 1} M_r \frac{t^r}{r} = \ln P(t) + \sum_{r\geq 1} \frac{t^r}{r} + \sum_{r\geq 1} \frac{(qt)^r}{r} \tag{110}$$

y calculando la derivada en $t = 0$, en los tres primeros casos se obtiene:

$$M_1 = a_1 + q + 1 \tag{111}$$

$$M_2 = 2a_2 - a_1^2 + q^2 + 1 \tag{112}$$

$$M_3 = 3a_3 - 6a_1 a_2 a_1^3 + q^3 + 1 \tag{113}$$

Por el teorema fundamental del álgebra este polinomio se puede factorizar de forma única como:

$$P(t) = \prod_{i=1}^{g} (1 - \alpha_i t)(1 - \overline{\alpha_i} t) \tag{114}$$

y además se cumple que $|\alpha_i| = \sqrt{q}$.

En base a esta factorización se puede definir la siguiente sucesión

$$N_r = \prod_{i=1}^{g} |(1 - \alpha_i^r)|^2 \tag{115}$$

La importancia de esta sucesión es que determina el número de clases en la jacobiana asociada a la curva C, es decir, $N_r = \#\mathcal{J}(\mathbb{F}_{q^r})$; de esta forma se tiene que $N_1 = P(1)$.

Corolario 5.6. *Con la notación arriba descrita se tiene que*

$$(q^{r/2} - 1)^{2g} \leq N_r \leq (q^{r/2} + 1)^{2g} \tag{116}$$

Las ecuaciones (114) y (115) se pueden reescribir como:

$$P(t) = \prod_{i=1}^{g} (1 - a_i t + q t^2) \tag{117}$$

y

$$N_r = \prod_{i=1}^{g} (1 - V_{i,r} + q^r) \tag{118}$$

respectivamente; donde $a_i = \alpha_i + \overline{\alpha_i}$ y $V_{i,r} = \alpha_i^r + \overline{\alpha_i}^r$

Lema 5.7. *De acuerdo con la notación anterior se tiene que*

$$V_{i,r} = V_{i,1} V_{i,r-1} - q V_{i,r-2} \tag{119}$$

con $r \geq 2$

DEMOSTRACIÓN. Nótese que $V_{i,0} = 2$ y $V_{i,1} = a_i$, ahora para $r = 2$ se tiene que

$$V_{i,1} V_{i,1} - q V_{i,0} = (\alpha_i + \overline{\alpha_i})^2 - 2q = \alpha_i^2 + 2q + \overline{\alpha_i}^2 - 2q = V_{i,2}$$

y supongamos que la igualdad se satisface para cualquier $k < r$ entonces

$$\begin{aligned} V_{i,1} V_{i,r-1} - q V_{i,r-2} &= (\alpha_i + \overline{\alpha_i})(\alpha_i^{r-1} + \overline{\alpha_i}^{r-1}) - q(\alpha_i^{r-2} + \overline{\alpha_i}^{r-2}) \\ &= \alpha_i^r + q(\alpha_i^{r-2} + \overline{\alpha_i}^{r-2}) + \overline{\alpha_i}^r - q(\alpha_i^{r-2} + \overline{\alpha_i}^{r-2}) = V_{i,r} \end{aligned}$$

□

De esta forma se tiene que para determinar la cardinalidad de la jacobiana se requiere solamente la factorización real y no la compleja del polinomio $P(t)$.

Cuando se desea encontrar una curva con cierto tipo de orden, es posible ver cómo deben ser sus parámetros, y en base a estos buscar la curva adecuada. Por ejemplo, si se desea encontrar una curva hiperelíptica en la cual sea fácil evaluar $\langle \cdot, \cdot \rangle_m$, supongamos que $m = 13$ y se procede como sigue:

Primero se deben encontrar un primo p y un entero k tal que $m = 13 | p^k - 1$ esto es con la finalidad de establecer el campo $\mathbb{F}_{p^k}$ en el que se

a_1	a_2	a_3	M_1	M_2	M_3	$\exists$	N.C.
-2	4	2	2	14	50	N	-
-2	5	-2	2	16	44	N	-
-2	6	-6	2	18	38	S	81
-1	0	8	3	9	51	N	-
-1	1	4	3	11	42	S	81
-1	2	0	3	13	33	S	162
-1	3	-4	3	15	24	S	243
-1	4	-8	3	17	15	S	81
-1	5	-12	3	19	6	N	-
0	-2	6	4	6	46	N	-
0	-1	2	4	8	34	N	-
0	0	-2	4	10	22	S	486
0	1	-6	4	12	10	N	-
1	-2	-4	5	5	23	N	-
1	-1	-8	5	7	8	S	81

CUADRO 1. parámetros que pueden tener curvas con jacobiana de 26 elementos sobre $\mathbb{F}_3$

definirá la curva para poder garantizar que el mapeo sea no degenerado. En este caso si se toma $p = 3$ y $k = 3$ se cumple esto.

Así mismo, se debe tener en cuenta el género g deseado para la curva, sea $g = 3$, retomando la ecuación (116) en nuestro caso:

$$0.1539 = (3^{1/2} - 1)^6 \leq N_1 \leq (3^{1/2} + 1)^6 = 415.8409 \tag{120}$$

como es deseable que N_1 sea un múltiplo de 13 se tienen 31 opciones, aquí se considerá el caso en que $N_1 = 26$ es decir $P(1) = 26$. De esta forma se puede determinar un coeficiente de $P(t)$, pero además de las ecuaciones (111), (112) y (113) se pueden dar cotas que depende del rango permitido para los $M_i's$, aquí se tiene que:

$$1 \leq M_1 \leq 2q + 1 \tag{121}$$

$$M_1 \leq M_2 \leq 2q^2 + 1 \tag{122}$$

$$M_1 \leq M_3 \leq 2q^3 + 1 \tag{123}$$

En general se tiene que $M_s \leq M_r \leq 2q^r + 1$ donde s es el mayor divisor, menor a r, de r. De esta forma se pueden determinar los parámetros de la curva $(M_1, M_2 \ldots, a_1, a_2, \ldots)$.

En el caso que se analiza lo parámetros probables se muestran en el cuadro 1, en la penúltima columna de este cuadro se señala si existe un curva algebraica sobre $\mathbb{F}_3$ con dichos parámetros.

En este caso se seleccionaron los parámetros enmarcados, y de la lista de curvas obtenidas en el paso anterior se busca una que sea no singular. Obteniendo así la curva

$$C : v^2 + u^7 + u^6 + u^5 + u^2 + 1 \tag{124}$$

y además

$C(\mathbb{F}_3) = \{P_\infty, (1,1), (1,2)\}$

$C(\mathbb{F}_{3^2}) = \{P_\infty, (1,1), (1,2), (0,y^2), (0,y^6), (y,1), (y,2), (y^2,1), (y^2,2), (y^3,1), (y^3,2), (y^4,y^2), (y^4,y^6), (y^2,1), (y^2,2), (y^5,0), (y^6,1), (y^6,2), (y^7,0)\}$

$C(\mathbb{F}_{3^3}) = \{P_\infty, (1,1), (1,2), (x,x^2), (x,x^{15}), (x^3,x^6), (x^3,x^{19}), (x^7,x^2), (x^7,x^{15}), (x^9,x^5), (x^9,x^{18}), (x^{11},x^5), (x^{11},x^{18}), (x^{21},x^6), (x^{21},x^{19})\}$

Aquí se pueden observar que la ventaja de utilizar esquemas con el grupo generado por la jacobiana de una curva hiperelíptica, es el hecho de que la aritmética será sencilla, se utilizarán un campo con 9 elementos y el grupo será de orden 169. Sin embargo la gran desventaja de esto es encontrar una curva que cumpla con las características adecuadas.

5.5. Ejemplo

La curva.

Sea $\mathcal{C}$ la curva hiperelíptica sobre $\mathbb{F}_{3^3}$ ($\mathbb{F}_3[x]/ < x^3 - x + 1 >$) dada por:

$$F(u,v) = v^2 + u^7 + u^6 + u^5 + u^2 + 1. \tag{125}$$

Utilizando la ecuación 115, se calcula la cardinalidad de la jacobiana, obteniendo que $|\mathcal{J}(\mathcal{C}(\mathbb{F}_{3^3}))| = 12,506 = 2 \cdot 13^2 \cdot 37$.

Los grupos.

La factorización anterior indica que la jacobiana tiene dos subgrupos de orden 13. De esta forma se utiliza el mapeo reducido de Tate definido sobre el 13-grupo de torsión de $\mathcal{J}(\mathcal{C})$, además se considerará un alfabeto con 13 caracteres.

$$\{!, \#, \$, \%, \&, *, +, -, ?, @, \hat{}, \tilde{}, \square\}.$$

Los puntos $(1,1)$ y (x,x^2) son puntos racionales de la curva arriba descrita, y además es fácil ver que los divisores $(1,1)-P_\infty$ y $(x,x^2)-P_\infty$ tienen orden 26, y por ende el orden de los divisores $P = 2(1,1) - 2P_\infty$ y $Q = (x,x^2) + (1,1) - 2P_\infty$ es 13. De esta forma se considerarán los grupos $\mathbb{G} =< P >$, $\widehat{\mathbb{G}} =< Q >$ and $\widetilde{\mathbb{G}} = \mu_{13} \cong < x^2 > \subset \mathbb{F}_{3^3}^*$.

Para evaluar el mapeo de Tate en P, Q, los generadores de los grupos, es necesaria una función racional G tal que $div(G) = 13P$, además de un divisor tal que $supp(P) \cap supp(D) = \emptyset$ y $D \sim Q$.

En este caso se puede considerar a G como: $G(u,v) = u^{13} + u^{11} + u^8 - u^7 + u^6 - u^5 + u^3 - u^2 + u - 1 - v(-u^9 + u^8 + u^7 + u^6 - u^3 - u^2 - u)$, y el divisor D puede tomarse como $D = (x,x^2) - (1,2)$. Esto se debe a que $G(1,1) = 0$ y $N(G) = (u^2+u+1)^{13}$, junto con $Q = D + div(u-1)$.

Lo anterior implica que

$$
\begin{aligned}
\langle P,Q\rangle_{13} &= (G(D))^{\frac{27-1}{13}} \\
&= G((x,x^2)-(1,2))^2 \\
&= \frac{G(x,x^2)^2}{G(1,2)^2} \\
&= \frac{x^{12}}{1} = x^{12}.
\end{aligned} \tag{126}
$$

La Asignación.

Para realizar la implementación es necesario tener una asignación entre el alfabeto y los grupos a utilizar, esto se realiza conforme a la siguiente tabla.

alfabeto	G	$\widehat{\mathbb{G}}$	$\widetilde{\mathbb{G}}$
!	$P = (1+u+u^2, -1-u)$	$Q = (x+x^{22}u+u^2, x^{14}+x^9u)$	x^2
#	$2P = (1+u+u^3, -1)$	$2Q = (x^{14}+x^{16}u+x^7u^2+u^3, x^3u^2)$	x^4
$	$3P = (1+u+u^3, -u-u^2)$	$3Q = (x^3+x^{14}u+u^2, x^8+x^2u)$	x^6
%	$4P = (-1+u-u^2+u^3, -u^2)$	$4Q = (x^4+x^9u+u^2, x^{17}+x^{22}u)$	x^8
&	$5P = (-1+u-u^2+u^3, 1)$	$5Q = (x^8+x^7u+x^7u^2+u^3, x^5+x^{10}u+x^{17}u^2)$	x^{10}
*	$6P = (1+u^2+u^3, -1-u+u^2)$	$6Q = (1+x^{19}u+x^{12}u^2+u^3, x^{15}+x^8u+x^{22}u^2)$	x^{12}
+	$7P = (1+u^2+u^3, 1+u-u^2)$	$7Q = (1+x^{19}u+x^{12}u^2+u^3, x^2+x^{21}u+x^9u^2)$	x^{14}
-	$8P = (-1+u-u^2+u^3, -1)$	$8Q = (x^8+x^7u+x^7u^2+u^3, x^{18}+x^{23}u+x^4u^2)$	x^{16}
?	$9P = (-1+u-u^2+u^3, u^2)$	$9Q = (x^4+x^9u+u^2, x^4+x^9u)$	x^{18}
@	$10P = (1+u+u^3, u+u^2)$	$10Q = (x^3+x^{14}u+u^2, x^{21}+x^{15}u)$	x^{20}
^	$11P = (1+u+u^3, 1)$	$11Q = (x^{14}+x^{16}u+x^7u^2+u^3, x^{16}u^2)$	x^{22}
-	$12P = (1+u+u^2, 1+u)$	$12Q = (x+x^{22}u+u^2, x+x^{22}u)$	x^{24}
□	$13P = (1,0)$	$13Q = (1,0)$	x^{26}

La función hash.

En la implementación de la firma digital Boneh-Boyen es necesaria una función hash que tenga como entrada un vector con entradas en

$\widetilde{\mathbb{G}} =< x^2 >$, y su salida será un elemento de $\mathbb{Z}_p^* = \mathbb{Z}_{13}^*$, la cual definiremos como

$$Z(\overline{x}) = \left(\sum_{k=1}^{i} \log_{x^2}(x_k^{2k}) \right) \mod 13 \tag{127}$$

Donde $\overline{x} = (x_1, x_2, \ldots, x_i)$ con $x_k \in \widetilde{\mathbb{G}}$.

Inicio.

Un par de elementos aleatorios son generados, $a = 12$, $b = 7 \in \mathbb{Z}_{13}^*$, y se calculan los valores de $A = ag = 12P = (1 + u + u^2, 1 + u)$, $B = bg = 7P = (1 + u^2 + u^3, 1 + u - u^2)$. De esta forma se tiene que los parámetros privados del sistema son $(12, 7)$, en tanto que los parámetros públicos son $(P, 12P, 7P)$.

Generación de llaves.

Para crear las llaves del usuario $\mathcal{A}$, la autoridad genera aleatoriamente un par de elementos en $r \in \mathbb{Z}_{13}$ y $v \in \mathbb{Z}_{13}^*$, por ejemplo $r = 11$ y $v = 9$, y con estos valores se determina $K = (v + a + rb)^{-1}Q = 7^{-1}Q = 2Q = (x^{14} + x^{16}u + x^7u^2 + u^3, x^3u^2)$. La llave secreta del usuario $\mathcal{A}$ es $d = (11, 2Q)$ y la pública es $v = 9$.

Cifrado.

Suponga que $\mathcal{B}$ desea enviar el mensaje &~, al usuario $\mathcal{A}$, entonces $\mathcal{B}$ seleciona un par de elementos aleatorios, $\in \mathbb{Z}_{13}^*$ por ejemplo 2, 10 y hace las operaciones necesarias para completar la siguiente tabla.

M	s	$s(vg + A)$	sB	$e(g, \widetilde{g})^s M$	C_1, C_2, C_3	m
& $\sim x^{10}$	2	$2(9P + 12P)$	$2(7P)$	$(x^{12})^2 x^{10}$	$3P, P, x^8$	$! %
~ $\sim x^{24}$	10	$10(9P + 12P)$	$10(7P)$	$(x^{12})^{10} x^{24}$	$2P, 5P, x^{14}$	#&+

De esta forma $\mathcal{B}$ envia el mensaje $! % #&+ al usuario $\mathcal{A}$.

Decifrado.

Si el usuario $\mathcal{A}$ recibe el mensaje $! % #&?, este con su llave secreta $(11, 2Q)$, recupera el mensaje de la siguiente manera:

C	C_1, C_2, C_3	$h = C_1 + rC_2$	$z =< h, K >$	$\frac{C_3}{z}$	m
$! %	$3P, P, x^8$	$3P + 11(P)$	$< P, 2Q >= (x^{12})^{1*2}$	$\frac{x^8}{x^{24}}$	&
#&+	$2P, 5P, x^{14}$	$2P + 11(5P)$	$< 5P, 2Q >= (x^{12})^{5*2}$	$\frac{x^{14}}{x^{16}}$	~

Recuperando así el mensaje original &~.

Firma digital Boneh-Boyen

Con los parámetros arriba considerados se procede como sigue:

Generación de llaves.

Un par de elementos aleatorios en $\mathbb{Z}_{13}^*$ son generados, por ejemplo $x_{\mathcal{B}} = 5, y_{\mathcal{B}} = 4$ y se obtienen los valores para $u_{\mathcal{B}} = x_{\mathcal{B}}\widetilde{g} = 5Q = (x^8 + x^7u + x^7u^2 + u^3, x^5 + x^{10}u + x^{17}u^2)$ y $v_{\mathcal{B}} = y_{\mathcal{B}}\widetilde{g} = 4Q = (x^4+x^9u+u^2, x^{17}+x^{22}u)$. La llave pública para el usuario $\mathcal{B}$ es $(5Q, 4Q)$ y su llave privada será $(5, 4)$.

La Firma.

El usuario $\mathcal{B}$, con su llave secreta $11, 19$ y el mensaje **$!% #&+** o visto como un vector en $< x^2 >^6$, $\overline{x} = (x^6, x^2, x^8, x^4, x^{10}, x^{14})$ se calcula $m = Z(\overline{x}) = 1 \in \mathbb{Z}_{13}^*$.

Así mismo se genera un elemento aleatorio, por ejemplo $r = 8$ y se calcula $(x_{\mathcal{B}} + m + y_{\mathcal{B}}r)^{-1} = (5 + 1 + 4 \cdot 8)^{-1} = (12)^{-1} = 12$, $\sigma = (x_{\mathcal{B}} + m + y_{\mathcal{B}}r)^{-1}g = 12P = (1 + u + u^2, 1 + u)$ obteniéndose finalmente que la firma es $(12P, 8)$ o **˜-**.

Verificación

Conocida la llave pública de $\mathcal{B}$ $(11Q, 19Q)$, el mensaje **$!% #&+** $\mapsto \overline{x} = (x^6, x^2, x^8, x^4, x^{10}, x^{14})$ se calcula $m = Z(\overline{x}) = 1$ y la firma **˜-**, i.e. $(12P, 8)$, se evalua el mapeo de Tate en $\langle \sigma, u_{\mathcal{B}} + m\widehat{g} + rv_{\mathcal{B}} \rangle_{13} = \langle 12P, 5Q + 1 \cdot Q + 8 \cdot 4Q \rangle_{13} = \langle 12P, 12Q \rangle_{13} = x^{12}$. Como esta evaluación es igual a $\langle P, Q \rangle_{13}$ la firma es correcta.

Conclusiones

Este trabajo presenta la construcción de un esquema criptográfico, utilizando el grupo generado por la jacobiana de una curva hiperelíptica, esta construcción parte de los esquemas existentes para curvas elípticas, las cuales son un caso particular de las curvas hiperelípticas. La generalización se da de forma natural observando las relaciones que se dan entre los grupos.

La construcción de esquemas sobre curvas hiperelípticas han sido poco explotadas, debido a que el problema del logaritmo no es tan fuerte, la ventaja del enfoque aquí presentado se da en que la fortaleza de este no radica en el PLD sino en el BDHP. Al ser poco explotadas estas ideas hay pocas referencias donde ver posibles implementaciones. Como resultado de la investigación realizada para esta tesis se público el trabajo "*Boneh-Boyen Encryption and Signature Scheme on the Jacobian of a Hyperelliptic Curve.*[en] C. Numerantium [**26**]. Además se dieron platicas en coloquios.

La idea para lograr la generalización parte de tres aspectos. El primer aspecto a considerar es el hecho de que las curvas elípticas son un caso particular de las curvas hiperelípticas y la relación que existe entre los puntos racionales de la curva elíptica y los divisores en la jacobiana de una curva hiperelíptica. Se muestra cómo están definidos estos grupos para posteriormente realizar los cálculos necesarios.

El segundo aspecto a considerar es el tipo de esquema que se utiliza, por lo cual se realizó una descripción de los esquemas más importantes que utilizan al grupo de los puntos racionales de una curva elíptica. Cabe mencionar que en muchos de los esquemas, en especial en los referentes a firmas digitales, es necesario el uso de funciones hash que sirven para estandarizar el tamaño de la información a utilizar.

De este estudio se desprenden que los dos tipos de curvas elípticas sirven para diferentes tipos de esquemas. Las no-supersingulares,

que fueron utilizadas durante mucho tiempo usando esquemas basados en la intratabilidad del problema del logaritmo discreto. En tanto las curvas supersingualres pueden ser utilizadas en esquemas que basan su fortaleza en el problema bilineal Diffie-Hellman.

El tercer aspecto que se considera, se desprende del problema bilineal Diffie-Hellman, el cual requiere de la definición de un mapeo bilineal. Para esto se analiza la forma de extender los mapeos bilineales definidos sobre los puntos racionales de una curva elíptica, al conjunto de divisores de la jacobiana de una curva hiperelíptica. Analizando los casos de los mapeos de Weil y de Tate.

Una vez que se tienen todos los aspectos anteriores, se pueden conjuntar para establecer las herramientas que definen un esquema criptográfico basados en los divisores sobre la jacobiana de una curva hiperelíptica. Además se ejemplifica comó se logra esto.

En el análisis de todo este proceso, también se logra observar que de forma teórica, los esquemas en algunos aspectos pueden utilizar un grupo $\mathbb{Z}_n$ sin la necesidad de que este sea de orden primo, lo cual conlleva a implementaciones menos eficientes.

En el análisis del presente trabajo, se da a conocer cómo extender las ideas de los criptosistemas que utilizan curvas elípticas para hacer uso de curvas hiperelípticas, además se describen algunas condiciones iniciales para determinar curvas hiperelípticas con un subgrupo de orden adecuado.

La ventaja de implementar el esquemas IBE usando la jacobiana de una curva hiperelíptica, al igual que considerar la extensión de un esquema de llave pública, es el hecho que la aritmética en los grupos es más eficiente. La desventaja de la implementación es que la búsqueda de la curva con las caracteristicas necesarias, no es fácil, aún cuando el grupo es pequeño.

En la descripción de los mapeos bilineales no degenerados, se consideraron los usados tradicionalmente, sin embargo últimamente se ha definido otros mapeos los cuales están relacionados, y el objetivo de los nuevos mapeos es tener una mejor evaluación, como lo son el Eta y el Ate. Una posible dirección en la cual se puede continuar este trabajo es cómo generalizar estos mapeos. Además de la búsqueda de algoritmos o tipos de curvas que permitan una aritmética más eficiente.

Apéndice A

Convergencia de Algoritmos

La convergencia de algoritmos es de gran importancia ya que esto nos indicará si el algoritmo en algún momento llegará a la solución del problema planteado o no. Desde el punto de vista computacional no basta con conocer si el algoritmo obtendrá la solución, sino que es importante conocer también el tiempo que se tardará en obtenerla.

La primera parte del problema, determinar si se llega a la solución o no, se enfoca principalmente desde el punto de vista de la lógica de programación y del análisis de error de aproximación.

La segunda parte del problema, determinar el tiempo de ejecución, permite comparar algoritmos que arrojen el mismo resultado, y además estimar cuando se tendrán resultados. Para determinar el tiempo se considera el número de operaciones que requiere el algoritmo.

A.1. Tiempo de ejecución.

Para estimar el tiempo que un algoritmo tardará en ejecutarse, es necesario estimar el número de operaciones que requiere y considerar el tiempo que requiere cada operación, es decir el problema es contar el número de operaciones a realizar. Por lo general cada ejecución con parámetros diferentes requiere un cantidad distinta de operaciones.

Una alternativa es contabilizar el número promedio de operaciones y otra es encontrar el máximo de operaciones a realizar. Una desventaja del primer caso es que en ocasiones no es tan sencillo de determinar, caso contrario al segundo, sin embargo en ocasiones el primero dará una idea más clara del tiempo requerido.

Ejemplo A.1. *En el método paso-pequeño paso-grande (3.1.1.1), para calcular m se realiza una operación $\lceil \sqrt{n} \rceil$ y en el primer paso se realizan m operaciones y otras tantas, cuando mucho en el segundo, así se tendrán $2m+1 \approx 2\sqrt{n}+1$ operaciones en el caso promedio se tendrán $m + \frac{m}{2} + 1 \approx \frac{3\sqrt{n}}{2} + 1$.*

En el caso de realizar la búsqueda del logaritmo de forma exahustiva, a lo más se requieren n multiplicaciones, en el caso promedio n/2. Si $n = 100$ *se observa con claridad la ventaja del método* 21 *vs.* 100 *ó* 16 *vs.* 50.

A.2. Notación O-grande

La notación O-grande sirve para comparar dos sucesiones, el número de operaciones requeridas por un algoritmo. Se puede ver como una sucesión, dependiente por lo general de la cantidad de datos, en el caso del PLD se considera el orden del grupo.

Definición A.2. *Sean* x_n *y* y_n *dos sucesiones, entonces se dice que* x_n *es O-grande de* y_n *si existen constantes* $c \in \mathbb{R}$ *y* $k \in \mathbb{N}$ *tales que*

$$|x_n| \leq c|y_n| \qquad \forall n \geq k$$

lo cual se denota como $x_n = O(y_n)$

Es fácil ver que esta notación satisface las siguientes propiedades: [20]

1. $\forall k > 0, \quad k \cdot f = O(f)$
2. Si $f = O(g)$ y $h = O(g)$ entonces $(f + g) = O(g)$
3. Si $f = O(g)$ y $g = O(h)$ entonces $f = O(h)$
4. $n^k = O(b^n) \quad \forall b > 1 \; y \; k \geq 0$
5. $\log_b(n) = O(n^k) \quad \forall b > 1 \; y \; k > 0$
6. Si $f = O(n^a)$ y $g = O(n^b)$ entonces $f + g = O(n^{\text{máx}(a,b)})$
7. Si $f = O(n^a)$ y $g = O(n^b)$ entonces $f \cdot g = O(n^{a+b})$

Computacionalmente, la notación O-grande, es utilizada para determinar el orden de los algoritmos, siendo los de principal uso las funciones n^k, $log_2(n)$ y 2^n, así como combinaciones de estas, gracias a que la notación puede ser utilizada para definir una relación de equivalencia.

Definición A.3. *Se dice que dos suceciones* x_n *y* y_n *son del mismo orden si*

$$x_n = O(y_n) \Leftrightarrow y_n = O(x_n) \tag{128}$$

Esta relación efectivamente es de equivalencia. Claramente es una relación simétrica y reflexiva, por definición; y la transitivdad se cumple de forma inmediata por la propiedad 3.

n	$\log_2(n)$	$\sqrt{n}$	n	$n\log_2(n)$	n^2	2^n
10	$4\times10^{-9}s$	$4\times10^{-9}s$	$10^{-8}s$	$4\times10^{-8}s$	$10^{-7}s$	$10^{-6}s$
10^2	$7\times10^{-9}s$	$1\times10^{-8}s$	$10^{-7}s$	$7\times10^{-7}s$	$10^{-5}s$	4×10^{13}a.
10^3	$1\times10^{-8}s$	$3.2\times10^{-8}s$	$10^{-6}s$	$1\times10^{-5}s$	$10^{-3}s$	*
10^4	$1.3\times10^{-8}s$	$1\times10^{-7}s$	$10^{-5}s$	$1.3\times10^{-4}s$	$10^{-1}s$	*
10^5	$1.7\times10^{-8}s$	$3.2\times10^{-7}s$	$10^{-4}s$	$1.7\times10^{-3}s$	$10s$	*
10^6	$2\times10^{-8}s$	$1\times10^{-6}s$	$10^{-3}s$	$2\times10^{-2}s$	$17min$	*
10^{30}	$1\times10^{-7}s$	$11.6dias$	3×10^{13}a.	*	*	*
10^{50}	$1.7\times10^{-7}s$	3.2×10^{7}a.	3×10^{33}a.	*	*	*

CUADRO 1. Tiempo de ejecución dependiendo del orden.

Ejemplo A.4. *La sucesión del número de operaciones del ejemplo A.1 es* $x_n = 2\sqrt{n}+1$, *y considérese la sucesión* $y_n = \sqrt{n}$. *Con esto se tiene que*

$$|\sqrt{n}| \leq 1|2\sqrt{n}+1| \qquad \forall n \leq 1$$

es decir $y_n = O(x_n)$ *y además*

$$|2\sqrt{n}+1| \leq 3|\sqrt{n}| \qquad \forall n \leq 1$$

De esta forma se dice que $2\sqrt{n}+1$ *y* $\sqrt{n}$ *son del mismo orden, o bien que* x_n *es de orden* $\sqrt{n}$.

En el cuadro 1 se despliegan los tiempos que una computadora actual tarda en ejecutar un algoritmo de cierto orden [**35**], lo cual puede disminuir con el avance computacional. En el cuadro se considera que el año tiene 365.25 dias, y son tiempos aproximados, lo cual muestra la importancia del orden. Tratar de resolver el problema del logaritmo discreto para grupos de orden 50 se vuelve impráctico con los métodos aquí expuestos.

Los tiempos reflejados para determinar la ejecución de un algoritmo, dan una idea del concepto de ejecución en tiempo real. Si se va a enviar un mensaje de importancia para las siguientes t horas, y el algoritmo para resolver el PLD tarda más de estas t horas entonces el PLD no se resolverá en tiempo real, en cambio si el algoritmo tarda menos de este tiempo, se puede decir que sí se resuelve.

Apéndice B

S-box Whirpool

Las diferentes representaciones del polinomio de permutación asociado a la S-Box, S, utilizada en la función Whirlpool son:

En la representación polinomial hexagesimal considerando p_8.

$$81 + A1x^{100} + A2x^{16} + A5x^{136} + A5x^{208} + A5x^{210} + A7x^{151} + A8x^{92} + A8x^{177} + A8x^{182} + A9x^{135} + A9x^{196} + A9x^{205} + AAx^{140} + AAx^{238} + ACx^{109} + 8Ax^{28} + 2Ax^{34} + 4Ax^{63} + 8Ax^{103} + Ax^{125} + 8Ax^{150} + Ax^{181} + 4Ax^{218} + 5Ax^{226} + B0x^{189} + B2x^{118} + B3x^{14} + B3x^{186} + B3x^{230} + B4x^{87} + B5x^{143} + B5x^{203} + B7x^{84} + B7x^{149} + B9x^{60} + BAx^{21} + BAx^{26} + BAx^{178} + BBx^{130} + BDx^{99} + 3Bx^{9} + 8Bx^{20} + 8Bx^{40} + 7Bx^{47} + Bx^{48} + 8Bx^{59} + 9Bx^{88} + 7Bx^{93} + 9Bx^{117} + 3Bx^{122} + 4Bx^{184} + 9Bx^{244} + C2x^{98} + C2x^{165} + C2x^{217} + C3x^{222} + C5x^{156} + C5x^{209} + C5x^{247} + C8x^{173} + C9x + C9x^{155} + CAx^{240} + CBx^{74} + CCx^{35} + CCx^{232} + CDx^{55} + CEx^{153} + 8Cx^{12} + 9Cx^{36} + 7Cx^{44} + 6Cx^{107} + 4Cx^{157} + Cx^{195} + 5Cx^{224} + 2Cx^{236} + D0x^{215} + D2x^{82} + D3x^{200} + D4x^{18} + D4x^{243} + D7x^{79} + D8x^{56} + D9x^{127} + D9x^{162} + DDx^{198} + DFx^{97} + 6Dx^{50} + 4Dx^{85} + 8Dx^{121} + Dx^{154} + Dx^{176} + Dx^{214} + 8Dx^{220} + Dx^{235} + 6Dx^{248} + E0x^{172} + E1x^{22} + E2x^{75} + E3x^{27} + E3x^{228} + E3x^{237} + E6x^{199} + E7x^{234} + E8x^{83} + E9x^{223} + EEx^{57} + EFx^{166} + 9Ex^{53} + 4Ex^{68} + Ex^{110} + 7Ex^{113} + Ex^{114} + 2Ex^{134} + 7Ex^{139} + Ex^{188} + 4Ex^{197} + 9Ex^{250} + F0x^{241} + F2x^{5} + F4x^{132} + F4x^{187} + F5x^{158} + F6x^{38} + F6x^{229} + F8x^{129} + F9x^{52} + F9x^{212} + FBx^{227} + FEx^{123} + FFx^{61} + FFx^{148} + Fx^{30} + 9Fx^{39} + 8Fx^{43} + 4Fx^{91} + 9Fx^{108} + 8Fx^{133} + 9Fx^{161} + 6Fx^{170} + 8Fx^{201} + 2Fx^{219} + Fx^{245} + 8Fx^{249} + D4x^{2} + 78x^{3} + D7x^{4} + 9Ax^{6} + 75x^{7} + 8Bx^{8} + CDx^{10} + 61x^{11} + 46x^{13} + 38x^{15} + 3x^{17} + 74x^{19} + 46x^{23} + 15x^{24} + 36x^{25} + 58x^{29} + 80x^{31} + 64x^{32} + 16x^{33} + 73x^{37} + 40x^{41} + 83x^{42} + 53x^{45} + 87x^{46} + 68x^{49} + 47x^{51} + 64x^{54} + 91x^{58} + 82x^{62} + 40x^{64} + 4x^{65} + E9x^{67} + F9x^{69} + 57x^{70} + EDx^{71} + 4x^{72} + 82x^{73} + 25x^{76} + 48x^{77} + 49x^{78} + 64x^{80} + 19x^{81} + 33x^{86} + 58x^{89} + 72x^{90} + 91x^{94} + 83x^{95} + 45x^{96} + 22x^{101} + 56x^{102} + 23x^{104} + 51x^{105} + 60x^{106} + 54x^{111} + 25x^{112} + 47x^{115} + 38x^{116} + 87x^{119} + 24x^{120} + 80x^{124} + 83x^{126} + 87x^{128} + 6x^{131} + 60x^{137} + 37x^{138} + 39x^{141} + 58x^{142} + 30x^{144} + 90x^{145} + 22x^{146} + 35x^{147} + 49x^{152} + 82x^{159} + 82x^{160} + 46x^{163} + 93x^{164} + 25x^{167} + 2x^{168} + 4x^{169} + 55x^{171} + 19x^{174} + 32x^{175} + 84x^{179} + 8x^{180} + 32x^{183} + 70x^{185} + 99x^{190} + 54x^{191} + 92x^{192} + 37x^{193} + 7x^{194} + 76x^{202} +$$

$27x^{204} + 90x^{207} + 45x^{211} + 29x^{213} + 29x^{216} + 16x^{221} + 89x^{225} + 97x^{231} + 27x^{233} + 51x^{239} + 94x^{242} + 74x^{246} + 65x^{251} + EBx^{252} + 4x^{253}$

Considerando a los coeficientes como potencias de β (raíz de p_8):

$\beta^{112} + \beta^{23}x + \beta^{41}x^2 + \beta^{78}x^3 + \beta^{170}x^4 + \beta^{213}x^5 + \beta^{146}x^6 + \beta^{21}x^7 + \beta^{237}x^8 + \beta^{120}x^9 + \beta^{12}x^{10} + \beta^{66}x^{11} + \beta^{49}x^{12} + \beta^{48}x^{13} + \beta^{171}x^{14} + \beta^{201}x^{15} + \beta^{209}x^{16} + \beta^{25}x^{17} + \beta^{41}x^{18} + \beta^{10}x^{19} + \beta^{237}x^{20} + \beta^{57}x^{21} + \beta^{89}x^{22} + \beta^{48}x^{23} + \beta^{141}x^{24} + \beta^{249}x^{25} + \beta^{57}x^{26} + \beta^{176}x^{27} + \beta^{222}x^{28} + \beta^{241}x^{29} + \beta^{113}x^{30} + \beta^{7}x^{31} + \beta^{195}x^{32} + \beta^{239}x^{33} + \beta^{142}x^{34} + \beta^{127}x^{35} + \beta^{35}x^{36} + \beta^{159}x^{37} + \beta^{173}x^{38} + \beta^{46}x^{39} + \beta^{237}x^{40} + \beta^{6}x^{41} + \beta^{247}x^{42} + \beta^{24}x^{43} + \beta^{115}x^{44} + \beta^{206}x^{45} + \beta^{13}x^{46} + \beta^{172}x^{47} + \beta^{238}x^{48} + \beta^{107}x^{49} + \beta^{133}x^{50} + \beta^{253}x^{51} + \beta^{214}x^{52} + \beta^{137}x^{53} + \beta^{195}x^{54} + \beta^{12}x^{55} + \beta^{251}x^{56} + \beta^{44}x^{57} + \beta^{165}x^{58} + \beta^{237}x^{59} + \beta^{60}x^{60} + \beta^{175}x^{61} + \beta^{192}x^{62} + \beta^{37}x^{63} + \beta^{6}x^{64} + \beta^{2}x^{65} + x^{66} + \beta^{245}x^{67} + \beta^{34}x^{68} + \beta^{214}x^{69} + \beta^{189}x^{70} + \beta^{117}x^{71} + \beta^{2}x^{72} + \beta^{192}x^{73} + \beta^{236}x^{74} + \beta^{95}x^{75} + \beta^{36}x^{76} + \beta^{226}x^{77} + \beta^{152}x^{78} + \beta^{170}x^{79} + \beta^{195}x^{80} + \beta^{193}x^{81} + \beta^{59}x^{82} + \beta^{11}x^{83} + \beta^{158}x^{84} + \beta^{145}x^{85} + \beta^{125}x^{86} + \beta^{20}x^{87} + \beta^{217}x^{88} + \beta^{241}x^{89} + \beta^{155}x^{90} + \beta^{136}x^{91} + \beta^{144}x^{92} + \beta^{172}x^{93} + \beta^{165}x^{94} + \beta^{247}x^{95} + \beta^{221}x^{96} + \beta^{90}x^{97} + \beta^{67}x^{98} + \beta^{109}x^{99} + \beta^{63}x^{100} + \beta^{101}x^{101} + \beta^{219}x^{102} + \beta^{222}x^{103} + \beta^{47}x^{104} + \beta^{208}x^{105} + \beta^{30}x^{106} + \beta^{250}x^{107} + \beta^{46}x^{108} + \beta^{220}x^{109} + \beta^{199}x^{110} + \beta^{143}x^{111} + \beta^{36}x^{112} + \beta^{167}x^{113} + \beta^{199}x^{114} + \beta^{253}x^{115} + \beta^{201}x^{116} + \beta^{217}x^{117} + \beta^{211}x^{118} + \beta^{13}x^{119} + \beta^{225}x^{120} + \beta^{197}x^{121} + \beta^{120}x^{122} + \beta^{88}x^{123} + \beta^{7}x^{124} + \beta^{105}x^{125} + \beta^{247}x^{126} + \beta^{96}x^{127} + \beta^{254}x^{128} + \beta^{116}x^{129} + \beta^{83}x^{130} + \beta^{26}x^{131} + \beta^{230}x^{132} + \beta^{24}x^{133} + \beta^{130}x^{134} + \beta^{135}x^{135} + \beta^{188}x^{136} + \beta^{30}x^{137} + \beta^{185}x^{138} + \beta^{167}x^{139} + \beta^{151}x^{140} + \beta^{154}x^{141} + \beta^{241}x^{142} + \beta^{42}x^{143} + \beta^{29}x^{144} + \beta^{51}x^{145} + \beta^{101}x^{146} + \beta^{39}x^{147} + \beta^{175}x^{148} + \beta^{158}x^{149} + \beta^{222}x^{150} + \beta^{205}x^{151} + \beta^{152}x^{152} + \beta^{111}x^{153} + \beta^{8}x^{154} + \beta^{23}x^{155} + \beta^{123}x^{156} + \beta^{16}x^{157} + \beta^{231}x^{158} + \beta^{192}x^{159} + \beta^{192}x^{160} + \beta^{46}x^{161} + \beta^{96}x^{162} + \beta^{48}x^{163} + \beta^{119}x^{164} + \beta^{67}x^{165} + \beta^{87}x^{166} + \beta^{18}x^{167} + \beta x^{168} + \beta^{2}x^{169} + \beta^{61}x^{170} + \beta^{150}x^{171} + \beta^{203}x^{172} + \beta^{196}x^{173} + \beta^{193}x^{174} + \beta^{194}x^{175} + \beta^{104}x^{176} + \beta^{144}x^{177} + \beta^{57}x^{178} + \beta^{140}x^{179} + \beta^{3}x^{180} + \beta^{51}x^{181} + \beta^{144}x^{182} + \beta^{194}x^{183} + \beta^{179}x^{184} + \beta^{202}x^{185} + \beta^{171}x^{186} + \beta^{230}x^{187} + \beta^{199}x^{188} + \beta^{242}x^{189} + \beta^{68}x^{190} + \beta^{143}x^{191} + \beta^{153}x^{192} + \beta^{185}x^{193} + \beta^{198}x^{194} + \beta^{200}x^{195} + \beta^{135}x^{196} + \beta^{34}x^{197} + \beta^{204}x^{198} + \beta^{160}x^{199} + \beta^{82}x^{200} + \beta^{24}x^{201} + \beta^{121}x^{202} + \beta^{42}x^{203} + \beta^{33}x^{204} + \beta^{135}x^{205} + x^{206} + \beta^{227}x^{207} + \beta^{188}x^{208} + \beta^{123}x^{209} + \beta^{188}x^{210} + \beta^{221}x^{211} + \beta^{214}x^{212} + \beta^{147}x^{213} + \beta^{8}x^{214} + \beta^{108}x^{215} + \beta^{147}x^{216} + \beta^{67}x^{217} + \beta^{37}x^{218} + \beta^{69}x^{219} + \beta^{197}x^{220} + \beta^{239}x^{221} + \beta^{216}x^{222} + \beta^{212}x^{223} + \beta^{131}x^{224} + \beta^{74}x^{225} + \beta^{19}x^{226} + \beta^{234}x^{227} + \beta^{176}x^{228} + \beta^{173}x^{229} + \beta^{171}x^{230} + \beta^{124}x^{231} + \beta^{127}x^{232} + \beta^{33}x^{233} + \beta^{81}x^{234} + \beta^{104}x^{235} + \beta^{240}x^{236} + \beta^{176}x^{237} + \beta^{151}x^{238} + \beta^{208}x^{239} + \beta^{73}x^{240} + \beta^{79}x^{241} + \beta^{38}x^{242} + \beta^{7}x^{243} + \beta^{217}x^{244} + \beta^{113}x^{245} + \beta^{10}x^{246} + \beta^{123}x^{247} + \beta^{133}x^{248} + \beta^{24}x^{249} + \beta^{137}x^{250} + \beta^{72}x^{251} + \beta^{235}x^{252} + \beta^{2}x^{253}$

En la representación polinomial hexagesimal considerando q_8:

$$81+AFx+F6x^2+E3x^3+59x^4+B3x^5+91x^6+C4x^7+96x^8+3Fx^9+E7x^{10}+71x^{11}+D5x^{12}+7Ax^{13}+ADx^{14}+A0x^{15}+94x^{16}+41x^{17}+6Ex^{18}+BDx^{19}+90x^{20}+F9x^{21}+E9x^{22}+E8x^{23}+7Cx^{24}+69x^{25}+9Dx^{26}+50x^{27}+16x^{28}+7Fx^{29}+AFx^{30}+A6x^{31}+4Ax^{32}+BCx^{33}+EDx^{34}+F6x^{35}+97x^{36}+88x^{37}+FAx^{38}+C8x^{39}+37x^{40}+8Ax^{41}+7Fx^{42}+60x^{43}+36x^{44}+63x^{45}+97x^{46}+52x^{47}+4Ex^{48}+25x^{49}+FFx^{50}+1Bx^{51}+1Dx^{52}+5Ax^{53}+B5x^{54}+D6x^{55}+7Dx^{56}+BAx^{57}+15x^{58}+34x^{59}+1Fx^{60}+F1x^{61}+23x^{62}+Cx^{63}+84x^{64}+58x^{65}+7Dx^{66}+2Ex^{67}+BEx^{68}+C2x^{69}+FBx^{70}+DFx^{71}+33x^{72}+FAx^{73}+8Bx^{74}+92x^{75}+A3x^{76}+EAx^{77}+D3x^{78}+E3x^{79}+7x^{80}+41x^{81}+CCx^{82}+87x^{83}+D0x^{84}+43x^{85}+7Cx^{86}+AEx^{87}+9x^{88}+CDx^{89}+52x^{90}+B1x^{91}+1Ax^{92}+ECx^{93}+E1x^{94}+90x^{95}+46x^{96}+17x^{97}+FDx^{98}+8Cx^{99}+58x^{100}+9Dx^{101}+F5x^{102}+55x^{103}+BAx^{104}+58x^{105}+60x^{106}+16x^{107}+D1x^{108}+ECx^{109}+CAx^{110}+40x^{111}+C6x^{112}+C4x^{113}+6Fx^{114}+BAx^{115}+CDx^{116}+5Cx^{117}+DBx^{118}+ECx^{119}+39x^{120}+66x^{121}+24x^{122}+75x^{123}+8Cx^{124}+17x^{125}+F0x^{126}+23x^{127}+29x^{128}+DAx^{129}+B4x^{130}+BCx^{131}+40x^{132}+38x^{133}+C2x^{134}+D6x^{135}+F1x^{136}+29x^{137}+85x^{138}+99x^{139}+7x^{140}+FDx^{141}+6Cx^{142}+DFx^{143}+64x^{144}+75x^{145}+54x^{146}+63x^{147}+6Ex^{148}+64x^{149}+88x^{150}+50x^{151}+EEx^{152}+7Ex^{153}+D3x^{154}+F7x^{155}+31x^{156}+F2x^{157}+9Cx^{158}+23x^{159}+8Cx^{160}+D0x^{161}+3Cx^{162}+Ex^{163}+DFx^{164}+Ax^{165}+A8x^{166}+91x^{168}+88x^{169}+ADx^{170}+FBx^{171}+8Dx^{172}+4Ax^{173}+AEx^{174}+6Cx^{175}+C5x^{176}+F1x^{177}+8x^{178}+62x^{179}+E8x^{180}+42x^{181}+93x^{182}+FAx^{183}+D7x^{184}+DDx^{185}+4Cx^{186}+Bx^{187}+6Cx^{188}+49x^{189}+76x^{190}+44x^{191}+84x^{192}+6x^{193}+2Ax^{194}+17x^{195}+6Cx^{196}+ADx^{197}+3x^{198}+92x^{199}+1Cx^{200}+C3x^{201}+DBx^{202}+9Fx^{203}+D1x^{204}+F6x^{205}+ACx^{206}+CDx^{207}+BEx^{208}+14x^{209}+29x^{210}+EDx^{211}+CCx^{212}+A3x^{213}+CFx^{214}+60x^{215}+59x^{216}+E4x^{217}+2Cx^{218}+BBx^{219}+20x^{220}+6Dx^{221}+C1x^{222}+D8x^{223}+C8x^{224}+94x^{225}+F0x^{226}+9Fx^{227}+5Ax^{228}+25x^{229}+86x^{230}+EDx^{231}+69x^{232}+45x^{233}+95x^{234}+Ex^{235}+ADx^{236}+8Bx^{237}+7Bx^{238}+48x^{239}+3Ax^{240}+8Dx^{241}+B2x^{242}+E8x^{243}+4Ax^{244}+3Bx^{245}+80x^{246}+1Bx^{247}+EBx^{248}+9Bx^{249}+8Cx^{250}+78x^{251}+74x^{252}+90x^{253}$$

Considerando a los coeficientes como potencias de $\eta = \zeta^5 + 1$:

$$\eta^{32} + \eta^{252}x + \eta^{46}x^2 + \eta^{218}x^3 + \eta^{83}x^4 + \eta^{195}x^5 + \eta^{55}x^6 + \eta^{128}x^7 + \eta^4x^8 + \eta^{98}x^9 + \eta^{73}x^{10} + \eta^{44}x^{11} + \eta^{198}x^{12} + \eta^{248}x^{13} + \eta^{182}x^{14} + \eta^{23}x^{15} + \eta^{155}x^{16} + \eta^{52}x^{17} + \eta^{254}x^{18} + \eta^{170}x^{19} + \eta^{16}x^{20} + \eta^{36}x^{21} + \eta^{161}x^{22} + \eta^{135}x^{23} + \eta^{42}x^{24} + \eta^{178}x^{25} + \eta^{131}x^{26} + \eta^{153}x^{27} + \eta^{186}x^{28} + \eta^{78}x^{29} + \eta^{252}x^{30} + \eta^{212}x^{31} + \eta^{30}x^{32} + \eta^{85}x^{33} + \eta^{102}x^{34} + \eta^{46}x^{35} + \eta^{205}x^{36} + \eta^{191}x^{37} + \eta^{190}x^{38} + \eta^{22}x^{39} + \eta^{129}x^{40} + \eta^{247}x^{41} + \eta^{78}x^{42} + \eta^{69}x^{43} + \eta^{105}x^{44} + \eta^{210}x^{45} + \eta^{205}x^{46} + \eta^{92}x^{47} + \eta^{94}x^{48} + \eta^{160}x^{49} + \eta^{188}x^{50} + \eta^{235}x^{51} + \eta^{15}x^{52} + \eta^{59}x^{53} + \eta^{174}x^{54} + \eta^{86}x^{55} + \eta^{65}x^{56} + \eta^{244}x^{57} + \eta^{144}x^{58} + \eta^{12}x^{59} + \eta^{47}x^{60} + \eta^{166}x^{61} + \eta^{89}x^{62} + \eta^{204}x^{63} + \eta^{251}x^{64} + \eta^{181}x^{65} + \eta^{65}x^{66} + \eta^{96}x^{67} + \eta^{154}x^{68} + \eta^{165}x^{69} + \eta^{232}x^{70} + \eta^{39}x^{71} + \eta^{25}x^{72} + \eta^{190}x^{73} + \eta^{147}x^{74} + \eta^{228}x^{75} + \eta^{249}x^{76} + \eta^{206}x^{77} + \eta^{45}x^{78} + \eta^{218}x^{79} + \eta^{72}x^{80} + \eta^{52}x^{81} + \eta^{20}x^{82} + \eta^{19}x^{83} + \eta^{7}x^{84} + \eta^{231}x^{85} + \eta^{42}x^{86} + \eta^{207}x^{87} + \eta^{26}x^{88} + \eta^{162}x^{89} + \eta^{92}x^{90} + \eta^{68}x^{91} + \eta^{142}x^{92} + \eta^{136}x^{93} + \eta^{238}x^{94} + \eta^{16}x^{95} + \eta^{214}x^{96} + \eta^{226}x^{97} + \eta^{113}x^{98} + \eta^{84}x^{99} + \eta^{181}x^{100} + \eta^{131}x^{101} + \eta^{41}x^{102} + \eta^{234}x^{103} + \eta^{244}x^{104} + \eta^{181}x^{105} + \eta^{69}x^{106} + \eta^{186}x^{107} + \eta^{183}x^{108} + \eta^{136}x^{109} + \eta^{168}x^{110} + \eta^{240}x^{111} + \eta^{80}x^{112} + \eta^{128}x^{113} + \eta^{114}x^{114} + \eta^{244}x^{115} + \eta^{162}x^{116} + \eta^{221}x^{117} + \eta^{57}x^{118} + \eta^{136}x^{119} + \eta^{180}x^{120} + \eta^{150}x^{121} + \eta^{21}x^{122} + \eta^{81}x^{123} + \eta^{84}x^{124} + \eta^{226}x^{125} + \eta^{107}x^{126} + \eta^{89}x^{127} + \eta^{222}x^{128} + \eta^{127}x^{129} + \eta^{184}x^{130} + \eta^{85}x^{131} + \eta^{240}x^{132} + \eta^{192}x^{133} + \eta^{165}x^{134} + \eta^{86}x^{135} + \eta^{166}x^{136} + \eta^{222}x^{137} + \eta^{201}x^{138} + \eta^{97}x^{139} + \eta^{72}x^{140} + \eta^{113}x^{141} + \eta^{230}x^{142} + \eta^{39}x^{143} + \eta^{152}x^{144} + \eta^{81}x^{145} + \eta^{139}x^{146} + \eta^{210}x^{147} + \eta^{254}x^{148} + \eta^{152}x^{149} + \eta^{191}x^{150} + \eta^{153}x^{151} + \eta^{13}x^{152} + \eta^{223}x^{153} + \eta^{45}x^{154} + \eta^{171}x^{155} + \eta^{133}x^{156} + \eta^{63}x^{157} + \eta^{219}x^{158} + \eta^{89}x^{159} + \eta^{84}x^{160} + \eta^{7}x^{161} + \eta^{112}x^{162} + \eta^{197}x^{163} + \eta^{39}x^{164} + \eta^{33}x^{165} + \eta^{9}x^{166} + x^{167} + \eta^{55}x^{168} + \eta^{191}x^{169} + \eta^{182}x^{170} + \eta^{232}x^{171} + \eta^{130}x^{172} + \eta^{30}x^{173} + \eta^{207}x^{174} + \eta^{230}x^{175} + \eta^{185}x^{176} + \eta^{166}x^{177} + \eta^{120}x^{178} + \eta^{3}x^{179} + \eta^{135}x^{180} + \eta^{126}x^{181} + \eta^{253}x^{182} + \eta^{190}x^{183} + \eta^{49}x^{184} + \eta^{88}x^{185} + \eta^{56}x^{186} + \eta^{61}x^{187} + \eta^{230}x^{188} + \eta^{103}x^{189} + \eta^{11}x^{190} + \eta^{66}x^{191} + \eta^{146}x^{192} + \eta^{79}x^{193} + \eta^{14}x^{194} + \eta^{226}x^{195} + \eta^{230}x^{196} + \eta^{182}x^{197} + \eta^{209}x^{198} + \eta^{228}x^{199} + \eta^{67}x^{200} + \eta^{6}x^{201} + \eta^{57}x^{202} + \eta^{35}x^{203} + \eta^{183}x^{204} + \eta^{46}x^{205} + \eta^{106}x^{206} + \eta^{162}x^{207} + \eta^{154}x^{208} + \eta^{158}x^{209} + \eta^{222}x^{210} + \eta^{102}x^{211} + \eta^{20}x^{212} + \eta^{249}x^{213} + \eta^{76}x^{214} + \eta^{69}x^{215} + \eta^{83}x^{216} + \eta^{175}x^{217} + \eta^{56}x^{218} + \eta^{132}x^{219} + \eta^{115}x^{220} + \eta^{2}x^{221} + \eta^{227}x^{222} + \eta^{100}x^{223} + \eta^{22}x^{224} + \eta^{155}x^{225} + \eta^{107}x^{226} + \eta^{35}x^{227} + \eta^{59}x^{228} + \eta^{160}x^{229} + \eta^{101}x^{230} + \eta^{102}x^{231} + \eta^{178}x^{232} + \eta^{160}x^{233} + \eta^{8}x^{234} + \eta^{197}x^{235} + \eta^{182}x^{236} + \eta^{147}x^{237} + \eta^{176}x^{238} + \eta^{146}x^{239} + \eta^{140}x^{240} + \eta^{130}x^{241} + \eta^{208}x^{242} + \eta^{135}x^{243} + \eta^{30}x^{244} + \eta^{141}x^{245} + \eta^{110}x^{246} + \eta^{235}x^{247} + \eta^{37}x^{248} + \eta^{64}x^{249} + \eta^{64}x^{250} + \eta^{64}x^{251} + \eta^{10}x^{252} + \eta^{16}x^{253}$$

Bibliografía

[1] Angel Angel J., *Criptografía y Curvas Elípticas*, Tesis (Maestría), Departamento de Matematicas UAM-I (1998).

[2] Azarang M. R., García Dunna E., *Simulación y análisis de modelos estocasticos*, McGraw-Hill, (1996).

[3] Barreto P., *The pairing-based crypto lounge*, http://paginas.terra.com.br/informatica/paulobarreto/pblounge.html.

[4] Barreto P., Rijmen V., *The Whirlpool Hash Function*, http://paginas.terra.com.br/informatica/paulobarreto/WhirlpoolPage.html

[5] Berlekamp R., *Algebraic Coding Theory*, McGraw-Hill, NY, 1968.

[6] Boneh D., Franklin M., Identity-based encryption from the Weil pairing, SIAM Journal of computing, Vol 32 no.3 pp. 586-615, (2003).

[7] Boneh D. Boyen X., Short signatures without random oracles. In *Advances in Cryptolgy*-Eurocrypt 2004, LNCS, vol. 3027 pp. 56-73, Springer-Verlag, (2004)

[8] Boneh D. Boyen X., Efficient selective-ID secure identity-based encryption without random oracles. In *Advances in Cryptology*-Eurocrypt 2004, LNCS, vol. 3027, pp. 223-238, Springer-Verlag (2004)

[9] Boyen X., *A promenade through the new cryptography of bilinear pairings*, IEEE Information theory workshop, (2006).

[10] Buchmann J.A., *Introduction to cryptography*, Springer-Verlag, (2000).

[11] Caballero Gil P., *Introducción a la Criptografía*, Alfaomega, 2ed., (2003).

[12] Cantor D., *Computing in the jacobian of a hyperelliptic curve* Mathematics of Computation, Vol 48, pp 95-101 (1987).

[13] Diaz Santiago S., *Generación de sucesiones pseudoaleatorias criptográficamente fuertes*, Tesis (Maestría), Departamento de Matematicas UAM-I, (2005).

[14] ElGamal T., A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory Vol. 31, No. 4, pp. 469-472, (1985).

[15] Fulton W., *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley, (1989)

[16] Hankerson D., Menezes A., Vanstone S., *Guide to Elliptic curve cryptography*, Springer-Verlang, (2004).

[17] Johnston P., *JavaScript MD5*, http://pajhome.org.uk/crypt/md5/

[18] Lidl R., Niederreiter H., *Finite Fields*, Cambridge univ. Press, 2ed. (1997).

[19] Van Lint, J. H. and Van der Geer G., *Introduction to Coding Theory and Algebraic Geometry*, Birkhauser Boston, (1989).

[20] Kincaid D., Cheney W., *Análisis numérico*, Addison-Wesley Iberoamericana, (1994).

[21] Koblitz N., *Elliptic curve cryptosystem.*, Mathematics of Computation, vol 48, pp. 203-209, (1987).

[22] Koblitz N., *Hiperelliptic cryptosystems.*, Journal of Cryptology, vol 1, p. 139-150, (1989).

[23] Koblitz N., *CM-curves with good cryptographic properties*, Advances in Cryptology, CRYPTO'91, pp. 279-287, (1992).

[24] Koblitz N., *Algebraic Aspects of Cryptography.*, Springer-Verlang, 2ed., (1999).

[25] Maas M., *Pairing-Based Criptography*, Master Thesis, Department of Mathematics and Computing Science, Technische Universiteit Eindhoven, (2004).

[26] Martinez O., Tapia-Recillas H., *Boneh-Boyen Encryption and Signature Scheme on the Jacobian of a Hyperelliptic Curve*, C. Numerantium 188, pp. 65-74, (2007).

[27] Menezes A., Okamoto T., Vanstone S., *Reducing elliptic curve logarithms to logarithms in a finite field*, Annual ACM Symposium on Theory of Computing, pp. 80-89. ACM Press, (1991).

[28] Menezes A., *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, (1993).

[29] Menezes A., Wu Y., Zuccherato R., *An Elementary Introduction to Hyperelliptic Curves*, Technical Report CORR 96-19, University of Waterloo (1996)

[30] Menezes A., van Oorschot P., Vanstone S., Handbook of Applied Cryptography, CRC Press, (1997).

[31] Meza Moreno R., *El algoritmo de Berlekamp-Massey y decodificación de códigos BCH sobre el anillo* $\mathbf{Z}_{p^s}$, Tesis (Maestría), Departamento de Matemáticas UAM-I, (2007).

[32] Miller V., *Use of elliptic curves in cryptography*, Advances in cryptology-CRYPTO 85, pp. 417-426, (1986).

[33] National Bureau of Standards, *Data Encryption Standard*, Federal Information Processing Standard, U.S. Departament of Commerce, FIPS PUB 46, Washington, D.C., (1977)

[34] Okamoto T., *Cryptography based on bilinear maps*, LNCS vol. 3857, p 35-50, Springer-Verlag (2006)

[35] Rosen K., *Matemáticas Discretas y sus aplicaciones*, MacGrawHill, 6ed. (2006)

[36] Rivest R.L., Shamir A., Adlmeman L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol.21, No.2, pp. 120-126 (1978).

[37] Shamir A., Identy-based cryptosystems and signature schemes. In *Proceedings of Crypto'84*, LNCS, vol. 196, pp. 47-53, Springer-Verlag, (1984).

[38] Schneier B., *Applied Cryptography* 2 ed., John Wiley & Sons. (1996)

[39] Schoof R., *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory A 46 p. 183-211 (1987)

[40] Silverman J., *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, (1986).

[41] Solinas J., *Efficient Arithmetic on Koblitz Curves*, Designs Codes and Cryptography, 19, p. 195-249 (2000).

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Fecha : 08/04/2009
Página : 1/1

CONSTANCIA DE PRESENTACION DE EXAMEN DE GRADO

La Universidad Autónoma Metropolitana extiende la presente CONSTANCIA DE PRESENTACION DE EXAMEN DE GRADO de MAESTRO EN CIENCIAS (MATEMÁTICAS) del alumno OZIEL MARTINEZ DELGADO, matrícula 203381863, quien cumplió con los 132 créditos correspondientes a las unidades de enseñanza aprendizaje del plan de estudio. Con fecha diecisiete de abril del 2009 presentó la DEFENSA de su EXAMEN DE GRADO cuya denominación es:

CRIPTOGRAFIA DE CURVAS HIPERELIPTICAS BAJO EL ESQUEMA IBE

Cabe mencionar que la aprobación tiene un valor de 60 créditos y el programa consta de 192 créditos.

El jurado del examen ha tenido a bien otorgarle la calificación de:

Aprobar

JURADO

Presidente

DR. HORACIO TAPIA RECILLAS

Secretario

DR. RUBEN VAZQUEZ MEDINA

Vocal

DR. JOSE NOE GUTIERREZ HERRERA

Vocal

DRA. LAURA HIDALGO SOLIS

UNIDAD IZTAPALAPA
Coordinación de Sistemas Escolares
Av. San Rafael Atlixco 186, Col. Vicentina, México, DF, CP 09340 Apdo. Postal 555-320-9000
Tels. 5804-4880 y 5804-4883 Fax: 5804-4876