Morfismos, Vol. 21, No. 2, 2017, pp. 17–31

Criptografía de curva elíptica en campos de característica 3 *

Edgar González Fernández [1] Feliú D. Sagols [2]

Resumen

Se reúnen los elementos matemáticos involucrados en la construcción de sistemas criptográficos basados en curvas elípticas sobre campos finitos de característica tres, como son: la identificación de polinomios irreducibles en el anillo de polinomios $\mathbb{F}_3[X]$, la aritmética en $\mathbb{F}_{3^n}$ y en curvas elípticas en forma Hessiana. Usando un algoritmo de conteo basado en el método de Satoh [12], adecuado para característica 3, decidimos si el grupo de puntos en la curva tiene un subgrupo cíclico adecuado. Estos elementos pueden ayudar a la implementación de los esquemas de ElGamal y DSA.

2010 Mathematics Subject Classification: 11T71, 14H52.
Keywords and phrases: Criptografía, curvas elípticas, característica 3.

1. Introducción

Desde la invención de la criptografía de clave pública, se han propuesto diversos algoritmos para garantizar una comunicación segura entre dos o más entidades mediante un canal que podría ser inseguro. Estos algoritmos abordan dos de los principales problemas que pueden afectar la seguridad de la información:

*Este trabajo es un resumen de la tesis "Criptosistemas de curva elíptica en campos de característica 3" que presentó el primer autor para obtener el grado de Maestría en Ciencias del Departamento de Matemáticas del CINVESTAV, Trabajo presentado el 14 de diciembre de 2012.

[1]Los autores agradecen a ABACUS-CINVESTAV, CONACyT apoyo EDOMEX-2011-C01-165873.

[2]Trabajo parcialmente soportado por el CONACyT bajo el contrato No. 240211

[3]Trabajo parcialmente soportado por el SNI bajo el contrato No. 7008.

- *El problema de la distribución de claves.* Si las entidades interesadas no tienen la posibilidad de acordar previamente una clave mediante un canal seguro, entonces podría comprometerse la comunicación si la clave es recuperada por una entidad ajena. Además, en un grupo de n entidades que requieren comunicarse entre sí, se requiere distribuir $n(n-1)/2$ claves distintas.

- *El problema de la firma.* Una vez establecida la comunicación, se desea verificar que la información recibida proviene realmente de la entidad con la cual deseamos comunicarnos.

Dos de los algoritmos más utilizados en la actualidad son el *protocolo de Diffie-Hellman* para el establecimiento de claves, y el *algoritmo de firma digital DSA*. Estos algoritmos están basados en el Problema del Logaritmo Discreto (PLD) en un grupo arbitrario. Inicialmente se propuso el grupo multiplicativo de $\mathbb{Z}/(p\mathbb{Z})$ para implementar esquemas criptográficos. Posteriormente Koblitz [9] y Miller [11] de forma independiente propusieron el uso del grupo aditivo en el conjunto de puntos de una curva elíptica para implementar estos algoritmos. Desde entonces se han realizado estandarizaciones y recomendaciones muy precisas para el caso de curvas elípticas definidas sobre campos primos o binarios (véase [5] y [2]), algo que aún no se tiene para campos de característica 3 (u otros campos de característica chica).

En [8, 4.4-5] se muestra una variedad de sistemas de cifrado basados en curvas elípticas, así como esquemas de firma digital, basados principalmente en el problema del logaritmo discreto en curvas elípticas. Algunos de ellos presentan sólo algunas modificaciones al sistema básico de ElGamal.

El presente artículo se estructura como sigue. En la Sección 2 definimos los objetos matemáticos que hacen posible la implementación de un sistema criptográfico basado en el problema del logaritmo discreto en curvas elípticas y establecemos la nomenclatura a utilizar. A continuación, en la Sección 3 introducimos los algoritmos que facilitan el manejo de la aritmética en campos de característica tres. Lo mismo hacemos en la Sección 4 para hacer posible la aritmética en curva elípticas sobre campos de característica tres de manera eficiente. Finalmente, exponemos el algoritmo de conteo propuesto en [7], el cual es una adaptación del algoritmo de Satoh [12] a característica tres, lo cuál nos permite realizar una búsqueda de curvas apropiadas para uso criptográfico.

2. Preliminares

Damos a continuación algunas definiciones básicas e introducimos la nomenclatura a utilizar en el resto del artículo.

2.1. Campos finitos

Denotamos por $\mathbb{F}_q$ al campo finito de q elementos, por lo que q debe considerarse como una potencia de un primo. En lo consiguiente $q = 3^n$ para algún entero $n > 0$. El anillo de polinomios con coeficientes en $\mathbb{F}_q$ será denotado por $\mathbb{F}_q[X]$. Consideraremos las extensiones de grado n de $\mathbb{F}_q$ como un anillo cociente $\mathbb{F}_q[X]/(p(X))$, donde $p \in \mathbb{F}_q[X]$ es un polinomio irreducible de grado n. Así los elementos de $\mathbb{F}_{q^n}$ se consideran como polinomios de grado a lo más $n-1$ con coeficientes en $\mathbb{F}_q$, y la aritmética queda definida mediante la aritmética usual en $\mathbb{F}_q[X]$ módulo $p(X)$.

2.2. Curvas elípticas

Dado un campo K algebraicamente cerrado y elementos $a_i \in K$, $i = 1, 2, 3, 4, 6$, una *curva elíptica afín* está formada por el conjunto de puntos en el plano K^2 que satisfacen una *ecuación de Weierstrass* no singular

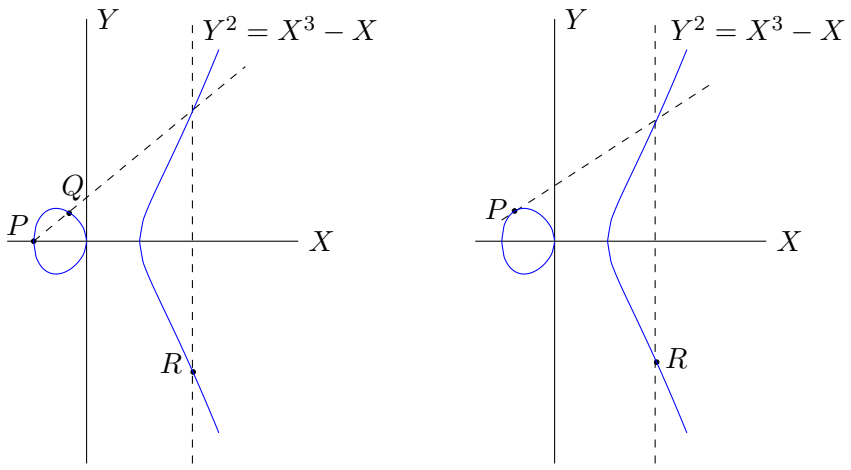
$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1}$$

Para fines prácticos, una curva elíptica puede definirse aún cuando K no es un campo algebraicamente cerrado. En el caso de $\mathbb{F}_q$ basta con pedir que los coeficientes a_i sean elementos de $\mathbb{F}_q$. Denotamos mediante $E_{\mathbb{F}_q}$ al conjunto de puntos con entradas en $\mathbb{F}_q$ que yacen en la curva, los cuales llamaremos $\mathbb{F}_q$-*puntos racionales*, o únicamente puntos racionales.

Mediante las siguientes reglas podemos definir la operación que hace de los puntos en una curva elíptica un grupo conmutativo.

1. **Identidad**. Se agrega un punto $\mathcal{O}$, conocido como puntos al infinito que sirve como neutro.

2. **Inverso**. El inverso (aditivo) del punto $P = (x, y)$ será $-P = (x, -y)$. Si $Q = -P$ entonces $P + Q = \mathcal{O}$.



(a) Suma (b) Doblado

Figura 1: Suma de puntos en una curva elíptica afín

3. **Suma**. Si $P = (x_1, y_1)$, $Q = (x_2, y_2)$ son puntos en la curva con $P \neq \pm Q$ entonces existe un tercer punto de intersección. La reflexión sobre el eje x (como se muestra en la figura 1(a)) será el punto $R = P + Q$.

4. **Doblado**. Por último, si $P = Q$ entonces se tomará la recta tangente sobre P y $P + Q = 2P = R$, como puede verse en la figura 1(b).

En este grupo el PLD consiste de lo siguiente: dados dos puntos $P, Q \in E$ encontrar un entero k tal que $P = kQ$ siempre que éste exista. Afortunadamente el conjunto de puntos racionales en una curva también forma un grupo conmutativo y el PLD se define de manera similar para una pareja de puntos $P, Q \in E_{\mathbb{F}_q}$.

En general denotaremos por E tanto a la curva elíptica como a la ecuación que la define. Con esto en mente, y con la finalidad de abordar el algoritmo de conteo a tratar en la Sección 5, definimos los siguientes objetos. Una *función racional* es una función de la forma f/g donde f y g son elementos del anillo cociente $\mathbb{F}_q[X, Y]/(E)$. Una *isogenia* entre dos curvas E_1 y E_2 es una función $\alpha : E_1 \to E_2$ dada por $\alpha(P) = (\alpha_1(P), \alpha_2(P))$ donde α_1 y α_2 son funciones racionales y se cumple además que α es un homomorfismo de grupos. Finalmente denotamos por $\mathrm{End}(E)$ como el grupo de *endomorfismos* de una curva, esto

es, el conjunto de isogenias de una curva en si misma.

Aunque se puede definir la ley de grupo mediante operaciones aritméticas en $\mathbb{F}_q$ a partir de la ecuación de Weierstrass, la representación Hessiana, que introduciremos en la Sección 4, no ayudará a definir de forma más eficiente la aritmética en estas curvas. Para esto, definimos una *curva elíptica proyectiva* como el conjunto de puntos en el espacio proyectivo $P^2(K)$ que satisfacen una *ecuación de Weierstrass proyectiva*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \quad (2)$$

Para poder implementar de manera exitosa un criptosistema de curva elíptica debemos establecer los procedimientos mediante los cuales se desarrollará la aritmética en curvas elípticas. Iniciamos con los elementos necesarios para definir la aritmética en $\mathbb{F}_q$.

3. Aritmética en $\mathbb{F}_{3^n}$

Como ya hemos mencionado, utilizaremos la representación polinomial dada por $\mathbb{F}_{3^n} \cong \mathbb{F}_3[X]/(p(X))$, con $p \in \mathbb{F}_3[X]$ de grado n irreducible, para definir la aritmética en campos de característica 3. Debemos entonces ser capaces de verificar cuando un polinomio es irreducible.

3.1. Polinomios irreducibles

Es importante poder encontrar polinomios irreducibles adecuados para que la aritmética en $\mathbb{F}_{3^n}$ sea eficaz para propósitos prácticos. Algunas de las pruebas más comunes para decidir cuando un polinomio es irreducible pueden encontrarse en [6]. Mencionamos una de ellas a continuación.

Algoritmo 1 Prueba de irreductibilidad de Ben-Or

Entrada: Polinomio $f \in \mathbb{F}_q[X]$ de grado n
Salida: f es irreducible o f es reducible

1: **para** $i = 1$ hasta $\lceil n/2 \rceil$ **hacer**
2: $\quad g = \text{mcd}(f, X^{q^i} - X)$
3: $\quad$ **si** $g \neq 1$ **entonces**
4: $\quad\quad f$ es reducible y detenemos el algoritmo
5: f es irreducible

Para poder construir polinomios irreducibles de grado alto de manera

rápida, podemos utilizar un criterio que emplea polinomios primitivos [10, Teorema 3.63].

Proposición 3.1.1. *Un polinomio* $f(X) = \sum_{i=0}^{n} a_i X^i$ *sobre* $\mathbb{F}_q$ *es primitivo si y sólo* $F(X) = \sum_{i=0}^{n} a_i X^{q^i-1}$ *es irreducible sobre* $\mathbb{F}_q$.

Para determinar si un polinomio irreducible es primitivo basta verificar que su orden no es un divisor propio de $q^n - 1$, por lo que se tiene el siguiente criterio.

Proposición 3.1.2. *Supongamos que* $f(X)$ *es un polinomio irreducible de grado* n *sobre* $\mathbb{F}_q$ *y* $q^n - 1 = p_1^{r_1} \dots p_k^{r_k}$, *donde* $p_1, \dots p_k$ *son primos distintos. Entonces* $f(X)$ *es primitivo sobre* $\mathbb{F}_q$ *si y sólo si*

$$X^{(q^n-1)/p_i} \not\equiv 1 \ mod\ f(X)$$

para cada $i = 1, \dots, k$.

Por ejemplo, para $q = 3$ y $n = 3$, tenemos que $q^n - 1 = 3^3 - 1 = 26 = 13 \cdot 2$. El polinomio $f(X) = X^3 - X + 1$ es irreducible sobre $\mathbb{F}_3$. Tenemos $X^{13} \equiv -1 \mod f(X)$ y por la tanto $X^2, X^{13} \not\equiv 1 \mod f(X)$. Así $f(X)$ es primitivo. Además por Proposición 3.1.1 se tiene que $X^{26} - X^2 + 1$ es irreducible, obteniendo así un trinomio para representar al campo con 3^{26} elementos.

3.2. Aritmética

La aritmética en $\mathbb{F}_3$ puede efectuarse de manera simple si utilizamos una representación alternativa mediante el conjunto $\{1, 0, -1\}$. Se tiene la ventaja que las operaciones de suma y multiplicación son efectuadas de manera casi idéntica a como se hace en $\mathbb{Z}$, salvo por la regla $1 + 1 = -1$. Esto nos ayuda a evitar la reducción módulo 3 y agiliza el cálculo de las operaciones en $\mathbb{F}_3[X]$, pues éstas también se pueden llevar a cabo de manera muy similar a lo realizado en $\mathbb{Z}[X]$.

La multiplicación en el anillo de polinomios $\mathbb{F}_3[X]$ puede efectuarse de manera eficiente mediante el algoritmo de Karatsuba-Ofman que se muestra a continuación.

El paso tres de este algoritmo se calcula de manera recursiva, usando el mismo algoritmo de Karatsuba-Ofman o mediante el algoritmo usual. Como se ha observado al inicio de la sección, el campo finito $\mathbb{F}_{3^n}$ puede considerarse como el cociente $\mathbb{F}_3[X]/(p(X))$ con p irreducible. Para adaptar el algoritmo de multiplicación al campo finito $\mathbb{F}_{3^n}$, el paso cuatro

Algoritmo 2 Algoritmo de multiplicación polinomial de Karatsuba-Ofman

Entrada: Polinomios $f(X)$, $g(X)$ de grado k
Salida: Multiplicación de f y g
1: $l = \lceil \frac{k}{2} \rceil$
2: Expresar $f(X) = (X^l f_1 + f_0)$ y $g(X) = (X^l g_1 + g_0)$ con g_i y h_i de grado menor que l
3: Calcular $a = f_0 g_0$, $b = f_1 g_1$, $c = (f_1 + f_0)(g_1 + g_0)$
4: El resultado es $a + (c - a - b)X^l + bX^{2l}$

se modifica ligeramente, aplicando un reducción módulo p si el resultado de la multiplicación tiene grado mayor o igual a n.

Otra operación importante dentro la aritmética de campos finitos es la potenciación. Aprovechando la estructura de $\mathbb{F}_{3^n}$, podemos evaluar $f(X)^n$ expresando a n como una suma de potencias de 3 con coeficientes en $\{0, 1, 2\}$. Por ejemplo $17 = 3^3 + 2 \cdot 3 + 2$ por lo que $f(X)^{17} = f(X)^{3^2} f(X)^{2 \cdot 3} f(X)^2$. Para evitar el cálculo de múltiples cuadrados, podemos almacenar el valor de $f(X)^2$ y reutilizarlo para calcular $\left(f(X)^2\right)^3$.

Por último, para realizar el cálculo de inversos se puede utilizar el Algoritmo de Euclídes extendido. El Algoritmo de Euclídes para polinomios nos sirve para calcular el máximo común divisor de dos polinomios f, g. Si f es irreducible y el grado de g es menor que el grado de f entonces $\gcd(f, g) = 1$, y podemos encontrar polinomios r, s tales que

$$r(X)f(X) + s(X)g(X) = 1,$$

por lo tanto $s(X)g(X) \equiv 1 \bmod f(X)$, es decir, s será el inverso de g en $\mathbb{F}_3[X]/(f(X))$.

Además de la representación polinomial de campos finitos, existen representaciones mediante bases normales, esto es, mediante un conjunto de elementos $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ los cuales forman una base de $\mathbb{F}_{q^n}$ como espacio vectorial sobre $\mathbb{F}_q$ y tales que $\alpha_i = \alpha_1^{q^i}$ para cada $i = 1, \ldots, n$. Entonces un elemento $a \in \mathbb{F}_{q^n}$ se expresa como una combinación lineal de los elementos α_i.

Para revisar con más a detalle este enfoque, puede consultarse [1], donde se detallan métodos para la implementación en software de la aritmética en campos finitos de característica 3 utilizando tanto la representación polinomial como la representación mediante bases normales,

donde además se concluye que la representación polinomial es preferible para la implementación en software.

4. Aritmética en curvas elípticas sobre $\mathbb{F}_{3^n}$

Consideremos una ecuación de Weierstrass no singular dada por (2) sobre un campo K. Si la característica de K es distinta de 2 entonces la curva puede transformarse a una de las siguientes:

$$E_1 : Y^2Z = X^3 + aX^2Z + cZ^3, \quad a \neq 0, c \neq 0 \tag{3}$$

$$E_2 : Y^2Z = X^3 + bXZ^2 + cZ^3, \quad b \neq 0, c \neq 0. \tag{4}$$

Las curvas elípticas que puede transformarse en la forma (3) son llamadas *ordinarias*, mientras que aquellas que pueden transformarse en la forma (4) son conocidas como *supersingulares*. Usualmente se utilizan curva ordinarias para fines criptográficos. Es el caso de implementaciones del algoritmo ElGamal y para el intercambio seguro de claves mediante el protocolo de Diffie-Hellman, aunque existen algoritmos en los cuales las curvas supersingulares son preferibles, por ejemplo, en criptosistemas basados en identidad (véase [4]).

Aunque las fórmulas para la operación de grupo se simplifican al transformar la curva expresada mediante la fórmula general (2) a alguna de las mencionadas anteriormente, existen representaciones que hacen más ágiles las implementaciones prácticas.

4.1. Forma Hessiana de una curva elíptica

Consideremos un elemento $d \in \mathbb{F}_q$ donde q es una potencia de 3. La representación Hessiana de una curva elíptica es una ecuación de la forma

$$E_d : X^3 + Y^3 + Z^3 = dXYZ, \quad d \neq 0. \tag{5}$$

De acuerdo con [14] una curva escrita en esta forma puede ser llevada a una en la forma normal de Weierstrass mediante el cambio de variables

$$X \to d(X + Y),\ Y \to d(X - Y),$$

con lo que conseguimos una ecuación normal de Weierstrass de la forma $Y^2Z = X^3 + X^2Z - d^{-3}Z^3$, la cual es ordinaria.

4.2. Aritmética en curvas en forma Hessiana

Sean $P = (x_1, y_1, z_1)$ y $Q = (x_2, y_2, z_2)$ dos puntos en E_d. La ley de grupo de una curva elíptica en forma Hessiana está definida por las siguientes reglas:

- El elemento identidad está dado por $\mathcal{O} = (1, -1, 0)$.
- El inverso de P es $-P = (y_1, x_1, z_1)$.
- Si $P \neq Q$ y $P, Q \neq \mathcal{O}$ la suma está dada por $P + Q = (x_3, y_3, z_3)$ donde

$$\begin{aligned} x_3 &= y_1^2 x_2 z_2 - y_2^2 x_1 z_1, \\ y_3 &= x_1^2 y_2 z_2 - x_2^2 y_1 z_1, \\ z_3 &= z_1^2 x_2 y_2 - z_2^2 x_1 y_1. \end{aligned} \tag{6}$$

- si $P = Q$ entonces $P + Q$ está dada por

$$\begin{aligned} x_3 &= y_1(z_1 - x_1)^3, \\ y_3 &= x_1(y_1 - z_1)^3, \\ z_3 &= z_1(x_1 - y_1)^3. \end{aligned} \tag{7}$$

Suponiendo que $z_1 = 1$ en (6), podemos calcular $P + Q$ mediante 10 multiplicaciones y 3 sumas en $\mathbb{F}_q$:

- **M**: $O_1 = y_1 x_2$
- **M**: $O_2 = y_1 z_2$
- **M**: $O_3 = x_1 y_2$
- **M**: $O_4 = x_1 z_2$
- **M**: $O_5 = O_1 O_2$
- **M**: $O_6 = O_3 O_4$
- **M**: $O_7 = x_2 y_2$
- **M**: $O_8 = O_3 y_2$
- **M**: $O_9 = O_1 x_2$
- **M**: $O_{10} = O_2 O_4$
- **A**: $x_3 = O_{11} = O_5 - O_8$
- **A**: $y_3 = O_{12} = O_6 - O_9$
- **A**: $z_3 = O_{13} = O_7 - O_{10}$

En cuanto a (7), podemos expresar a z_3 como

$$z_3 = -z_1 \left[(z_1 - x_1) + (y_1 - z_1)\right]^3$$

con lo cuál requerimos de calcular

- **A**: $O_1 = z_1 - x_1$
- **A**: $O_2 = y_1 - z_1$
- **C**: $O_3 = O_1^3$
- **C**: $O_4 = O_2^3$
- **A**: $O_5 = O_3 + O_4$
- **M**: $x_3 = O_6 = y_1 O_3$
- **M**: $y_3 = O_7 = x_1 O_4$
- **M**: $z_3 = O_8 = -z_1 O_5$

4.3. El grupo formal de una curva elíptica

Consideremos una curva elíptica en forma Hessiana E_d sobre $\mathbb{F}_q$ y las funciones racionales $\tau = \frac{X+Y}{Y}$ y $\omega = \frac{Z}{Y}$. Notemos que el punto $(0,0)$ del plano afín (τ, ω) corresponde al punto $(1,-1,0)$ de nuestro espacio proyectivo original. Dividiendo la ecuación (5) entre Y^3, esta queda como

$$(\tau - 1)^3 + \omega^3 + 1 = d(\tau - 1)\omega.$$

Despejando a ω del lado derecho de la ecuación y sustituyendo sucesivamente en el lado izquierdo obtenemos una serie de potencias ω en $\mathbb{Z}[d^{-1}][[\tau]]$ como sigue

$$\omega = -3d^{-1}\tau + 3d^{-1}\tau^2 - d^{-1}\tau^3 + \dots. \tag{8}$$

La ecuación afín $x^3 + y^3 + 1 = dxy$ donde $x = X/Z$ y $y = Y/Z$ puede expresarse en términos del *parámetro formal* τ, pues $x = (\tau - 1)/\omega$, $y = 1/\omega$. Con esto, la ley de grupo de E_d puede expresarse en términos de τ, y el conjunto de puntos (τ, ω) forma un grupo conocido como *el grupo formal de* E_d.

5. Conteo de puntos

El Teorema de Hasse establece una cota para el número de puntos racionales en una curva elíptica. Denotando por $|E_{\mathbb{F}_q}|$ a la cardinalidad de puntos en $E_{\mathbb{F}_q}$ se tiene que

$$q + 1 - 2\sqrt{q} < |E_{\mathbb{F}_q}| < q + 1 + 2\sqrt{q}.$$

Al entero t que satisface $t = q + 1 - |E_{\mathbb{F}_q}|$ se le conoce como la *traza de Frobenius*, ya que se relaciona con el *endomorfismo de Frobenius* , definido por $F(x, y) = (x^q, y^q)$, el cual cumple $F^2 - [t] \circ F + [q] = [0]$ ([13, Teorema V.2.3.1]), donde $[n]$ es el endomorfismo definido por la multiplicación por n. Continuamos esta sección desarrollando el algoritmo de conteo para curvas elípticas sobre $\mathbb{F}_{3^n}$, mismo que está enfocado en calcular $\mathrm{Tr}(F)$.

5.1. Levantamiento de una curva elíptica

Sea $\mathbb{Q}_3$ el campo de números 3-ádicos, $\mathbb{Q}_q$ una extensión no ramificada de grado n de $\mathbb{Q}_3$ y $\mathbb{Z}_q$ su anillo de enteros. Un *levantamiento* de una curva elíptica E_d con $d \in \mathbb{F}_q$, es una curva E_D con $D \in \mathbb{Z}_q$ y tal que $D \equiv d \bmod 3$. Si además $\mathrm{End}(E_d) \cong \mathrm{End}(E_D)$ entonces este levantamiento, conocido como el *levantamiento canónico*, es único [3].

Consideremos una curva elíptica E_d y el automorfismo de Frobenius $\sigma : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ dado por $\sigma(a) = a^3$ para todo $a \in \mathbb{F}_q$. Entonces σ induce una isogenia de curvas $E_d \longrightarrow E_{\sigma(d)}$ conocida como la *isogenia de Frobenius*.

Proposición 5.1.1. *Existe un único $\Sigma \in End(\mathbb{Q}_q)$ tal que el siguiente diagrama es conmutativo*

$$\begin{array}{ccc} \mathbb{Z}_q & \xrightarrow{\Sigma} & \mathbb{Z}_q \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{F}_q & \xrightarrow{\sigma} & \mathbb{F}_q \end{array}$$

donde π es la reducción módulo p. A la función Σ se le conoce como *sustitución de Frobenius*.

El algoritmo propuesto por Satoh en [12] está basado en el levantamiento canónico de una curva elíptica. Consideremos una curva E_d sobre $\mathbb{F}_q$. Si $q = 3^n$ entonces tenemos una colección de m curvas obtenidas al aplicar sucesivamente la isogenia de Frobenius $\sigma_i : E_{d_{3^i}} \longrightarrow E_{d_{3^{i+1}}}$. Tenemos así el siguiente diagrama conmutativo

$$\begin{array}{ccccccccc} \mathcal{E}_0 & \xrightarrow{\Sigma_0} & \mathcal{E}_1 & \xrightarrow{\Sigma_1} & \cdots & \xrightarrow{\Sigma_{n-2}} & \mathcal{E}_{n-1} & \xrightarrow{\Sigma_{n-1}} & \mathcal{E}_0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ E_d & \xrightarrow{\sigma_0} & E_{d^3} & \xrightarrow{\sigma_1} & \cdots & \xrightarrow{\sigma_{n-2}} & E_{d^{3^{n-1}}} & \xrightarrow{\sigma_{n-1}} & E_d \end{array}$$

donde Σ_i es la isogenia inducida por la sustitución de Frobenius y $\mathcal{E}_i$ es un levantamiento de $E_{d^{3^i}}$. Asimismo, obtenemos un endomorfismo $\mathcal{F} : \mathcal{E}_0 \longrightarrow \mathcal{E}_0$ dado por la composición $\Sigma_0 \circ \cdots \circ \Sigma_{n-1}$ el cual es el levantamiento del endomorfismo de Frobenius $F : E_d \longrightarrow E_d$ y cumple $Tr(F) = Tr(\mathcal{F})$.

El siguiente resultado, debido a Satoh [12], se aplicará al endomorfismo dual de $\mathcal{F}$ para poder calcular a traza de Frobenius.

Proposición 5.1.2. *Sea E una curva elíptica sobre K y sea $f \in End(\mathcal{E})$ de grado d. Sea τ el parámetro formal de $\mathcal{E}$ en $\mathcal{O}$ y asumamos que la reducción $\pi(f)$ de f* mód 3 *es separable y que $f(ker\pi) \subseteq ker\pi$. Sea c el*

coeficiente del término lineal del homomorfismo $\hat{f}$ inducido por f en el grupo formal de $\mathcal{E}$. Entonces $Tr(f) = c + d/c$.

Debido a que el endomorfismo de Frobenius no es separable, la proposición anterior no es válida para F. Sin embargo, el endomorfismo dual $\widehat{F}$ es separable siempre que la curva E sea ordinaria. Se tiene además que $Tr(\widehat{\mathcal{F}}) = Tr(\mathcal{F})$, por lo que al calcular $Tr(\widehat{\mathcal{F}})$ habremos obtenido el número de puntos contenidos en la curva E_d.

La técnica usada por Satoh consiste en obtener levantamientos de las isogenias duales $\widehat{\sigma}_i$ para cada i

$$\begin{array}{ccccccccc}
\mathcal{E}_0 & \xrightarrow{\widehat{\Sigma}_{n-1}} & \mathcal{E}_{n-1} & \xrightarrow{\widehat{\Sigma}_{n-2}} & \cdots & \xrightarrow{\widehat{\Sigma}_1} & \mathcal{E}_1 & \xrightarrow{\widehat{\Sigma}_0} & \mathcal{E}_0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
E_0 & \xrightarrow{\widehat{\sigma}_{n-1}} & E_{n-1} & \xrightarrow{\widehat{\sigma}_{n-2}} & \cdots & \xrightarrow{\widehat{\sigma}_1} & E_1 & \xrightarrow{\widehat{\sigma}_0} & E_0
\end{array}$$

las cuales son separables y por lo tanto satisfacen la proposición 5.1.2. Una vez calculados estos levantamientos, tenemos que

$$Tr(F) = Tr(\widehat{\mathcal{F}}) = \prod_{i=0}^{n-1} Tr(\widehat{\Sigma}_i). \tag{9}$$

5.2. Algoritmo de conteo

A continuación citamos algunos resultados presentados en [7] para conseguir levantamientos de $\widehat{\sigma}_i$ que aproximen suficientemente al levantamiento canónico.

Lema 5.2.1. *Dado un elemento $D_i \in \mathbb{Z}_q$ tal que $D_i \equiv d^{3^i} \bmod 3$, existe un único elemento $D_{i+1} \in \mathbb{Z}_q$ tal que*

$$(D_{i+1}+6)^3 - (D_{i+1}^2 + 3D_{i+1} + 9)D_i^3 = 0, \quad D_{i+1} \equiv d^{3^{i+1}} \bmod 3 \tag{10}$$

De acuerdo a [7, Corolario 1], la secuencia de curvas E_{D_i} se aproxima al levantamiento canónico, y la función $\phi_i : E_{D_{i+1}} \to E_{D_i}$ dada por

$$\phi_i(X,Y,Z) = \left(Y^2Z + Z^2X + X^2Y, Y^2X + Z^2Y + X^2Z, \frac{D_{i+1}+6}{D_i} XYZ\right)$$

define la isogenia dual inducida por la sustitución de Frobenius de los levantamientos $E_{D_i}, E_{D_{i+1}}$.

Considerando $\overline{\phi_i}$ como la reducción módulo 3 de ϕ_i, se puede ver que $\sigma_i \circ \overline{\phi_i} = [3]$, por lo tanto $\overline{\phi_i}$ es la isogenia dual $\widehat{\sigma}_i$ y entonces $\phi_i = \widehat{\Sigma}_i$.

Encontrando el valor de D_i que definen al levantamiento canónico de $E_{d^{3^i}}$ podremos calcular la traza de Frobenius.

La sucesión de curvas E_{D_i} representan una aproximación del levantamiento canónico $\mathcal{E}_i$ de $E_{d^{3^i}}$. Con esto, podemos finalmente calcular $\mathrm{Tr}(\widehat{\sigma}_i)$ a partir del grupo formal de $\mathcal{E}_i$ alrededor de $\mathcal{O}$ y el homomorfismo inducido por $\widehat{\Sigma}_i$.

Proposición 5.2.2. *Consideremos el parámetro formal $\tau = (Y+X)/Y$ del grupo formal de E_{D_i} en $\mathcal{O}$ y $\omega = Z/Y$. Sea c el coeficiente del término lineal del homomorfismo inducido por $\phi_i : E_{D_{i+1}} \to E_{D_i}$. Entonces $c = 1 + \dfrac{6}{D_{i+1}}$.*

Como hemos notado anteriormente, tenemos la igualdad $\widehat{\mathcal{F}} = \widehat{\Sigma}_{n-1} \circ \ldots \circ \widehat{\Sigma}_0$ por lo que podemos calcular $\mathrm{Tr}(F)$ a partir de cada una de las funciones $\widehat{\Sigma}_i$ mediante

$$\mathrm{Tr}(F) = \mathrm{Tr}(\widehat{F}) = \mathrm{Tr}(\widehat{\Sigma}_{n-1}) \cdots \mathrm{Tr}(\widehat{\Sigma}_0).$$

Entonces, de acuerdo a la conclusión de la proposición 5.2.2, la traza del endomorfismo de Frobenius está dada por

$$Tr(F) = \prod_{i=0}^{n-1} \left(1 + \frac{6}{D_{n+i}}\right) \bmod 3^n.$$

donde n debe ser elegido de tal manera que el entero $\mathrm{Tr}(F)$ esté completamente definido. Por el teorema de Hasse tenemos que $|\mathrm{Tr}(F)| \leq 2\sqrt{q}$, por lo que esta cota es suficiente para determinar $\mathrm{Tr}(F)$. Entonces m debe cumplir $3^n > 2\sqrt{q} = 2 \cdot 3^{n/2}$. Basta con tomar $m = \left\lceil \frac{n}{2} \right\rceil + 2$.

Para encontrar las raíces de las ecuaciones dadas por (10) puede utilizarse el método de Newton, utilizando como punto inicial cualquier levantamiento del elemento d^{3^i} correspondiente para satisfacer el lema de Hensel. El algoritmo de conteo utiliza el algoritmo 3 para calcular la traza de Frobenius t. El número de puntos se determina mediante la identidad $|E_{\mathbb{F}_q}| = q + 1 - t$.

Algoritmo 3 Cálculo de la Traza de Frobenius

Entrada: Curva elíptica en forma de Hasse con $d \in \mathbb{F}_q \setminus \mathbb{F}_{3^2}$ y un levantamiento $D_0 \in \mathbb{Z}_q$ de d.

Salida: Traza del endomorfismo de Frobenius.

1: $m \leftarrow \lceil \frac{n}{2} \rceil + 2$
2: **para** $i = 1$ hasta m **hacer**
3: $\quad D_{i+1} \leftarrow \text{Resolver}((X+6)^3 - (X^2+3X+9)D_i^3 = 0) \mod 3^i$
4: $t \leftarrow (1 + 6/D_m)$
5: **para** $i = m+1$ hasta $m+n-1$ **hacer**
6: $\quad D_{i+1} \leftarrow \text{Resolver}((X+6)^3 - (X^2+3X+9)D_i^3 = 0) \mod 3^m$
7: $\quad t \leftarrow t(1 + 6/D_i) \bmod 3^{m+1}$
8: **si** $t > 2\sqrt{3^n}$ **entonces**
9: $\quad t \leftarrow t - 3^m$

Edgar González Fernández
Departamento de Computación,
Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional,
Av. Instituto Politécnico Nacional 2508 San Pedro Zacatenco, Gustavo A. Madero,
07360 Ciudad de México, Distrito Federal,
egonzalez@computacion.cs.cinvestav.mx

Feliú D. Sagols Troncoso
Departamento de Matemáticas,
Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional,
Av. Instituto Politécnico Nacional 2508 San Pedro Zacatenco, Gustavo A. Madero,
07360 Ciudad de México, Distrito Federal,
fsagols@math.cinvestav.mx

Referencias

[1] Ahmadi, O., Hankerson, D., and Menezes, A. Software Implementation of Arithmetic in $\mathbb{F}_{3^m}$. In *First International Workshop on the Arithmetic of Finite Fields (WAIFI 2007) Proceedings* (Berlin, 2007), vol. 4547 of *Lecture Notes in Comput. Sci.*, Springer, pp. 85–102.

[2] Certicom. Standards For Efficient Cryptography (SEC 1 v2), Sept. 2009.

[3] Deuring, M. Die typen der multiplikatorringe elliptischer funktionen korper. *Abh. Math. Sem. Univ. Hamburg 14* (1941), 197–272.

[4] Galbraith, S. D. Supersingular curves in cryptography. In *Advances in Cryptology — ASIACRYPT 2001 Proceedings* (Berlin, 2001), Lecture Notes in Comput. Sci., Springer.

[5] Gallagher, P., Cameron F. Kerry, A. S., and Director, C. R. FIPS PUB 186-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS), 2009.

[6] Gao, S., and Panario, D. Tests and constructions of irreducible polynomials over finite fields. In *Selected Papers of a Conference Held at Rio de Janeiro, January 1997* (1997), Found. Comput. Math., Springer, pp. 346–361.

[7] Gustavsen, T. S., and Ranestad, K. A Simple Point Counting Algorithm for Hessian Elliptic Curves in Characteristic Three. *Appl. Algebra Eng. Commun. Comput. 17*, 2 (2006), 141–150.

[8] Hankerson, D., Menezes, A., and Vanstone, S. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004.

[9] Koblitz, N. Elliptic Curve Cryptosystems. *Math. Comp. 48* (1997), 203–209.

[10] Lidl, R., and Niederreiter, H. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, New York, NY, USA, 1986.

[11] Miller, V. Use of elliptic curves in cryptography. In *Advances in Cryptology — Crypto '85 Proceedings* (Berlin, 1986), vol. 218 of *Lecture Notes in Comput. Sci.*, Springer, pp. 417–426.

[12] Satoh, T. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 4 (2000), 247–270.

[13] Silverman, J. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[14] Smart, N. P., and Westwood, E. J. Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three. *Appl. Algebra Engrg. Comm. Comput.*, 13 (2003), 485–497.