Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional

Unidad Zacatenco

Departamento de Computación

Estudio y Análisis de Emparejamientos Bilineales Definidos sobre Curvas Ordinarias con Alto Nivel de Seguridad

Tesis que presenta

Laura Fuentes Castañeda

Para obtener el grado de

Maestro en Ciencias en Computación

Director de la tesis

Dr. Francisco Rodríguez Henríquez

México, Distrito Federal **Diciembre 2011**

Esta tesis se la dedico a mi hermosa madre Yolanda Castañeda por todo el amor que me ha brindado y por estar a mi lado en cada segundo de mi vida; a mi admirable padre Raúl Fuentes quien ha sido mi ejemplo a seguir y a quien le debo todo lo que he logrado; y a mi protector hermano David Fuentes porque siempre encuentra la manera de hacerme sonreír.

Agradecimientos

Deseo comenzar agradeciendo a mis abuelitos *Paula Solis* y *Domingo Castañeda*, quienes son la base de mi familia, por su amor incondicional, por todos los valores que desde niña me han inculcado y por impulsarme a alcanzar mis metas.

Quisiera agradecerle con mucho cariño a *Réne Henríquez García*, a quien siempre llevo presente en mi corazón y mi mente, por escucharme, apoyarme y por convertir cada momento a mi lado, en un recuerdo invaluable e inolvidable.

Les agradezco también a todos los amigos con quienes conviví durante estos dos años, especialmente a mi mejor amiga Cynthia, quien siempre ha estado conmigo y con quien he compartido momentos de felicidad y tristeza. Además, agradezco a mi amiga Lil María y a mis amigos Cuauhtemoc, Alejandro, Luis y Armando, por haber hecho tan amena y divertida la maestría.

A mis amigas de toda la vida: Sandy, Jessica, Monse y Paty; por su amistad incondicional y sus valiosos consejos.

Agradezco con sinceridad a mi asesor, el doctor Francisco Rondríguez Henríquez, por sus enseñanzas y por haberme guiado durante estos dos años.

A mis revisores, la Dra. María de Lourdes López García y el Dr. Carlos Artemio Coello Coello, así como al profesor Alfred Menezes y a su estudiante Edward Knapp, por sus contribuciones en mi trabajo de tesis.

A Sofía Reza por su amabilidad y paciencia.

A mi hermoso país natal México, le estaré eternamente agradecida representándolo siempre con orgullo.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT) por haberme brindado el apoyo económico, a partir del cual he culminado mis estudios de postgrado en tan distinguible institución.

Al CINVESTAV, quien se ha convertido en mi *alma mater*, por permitirme crecer en el ámbito personal, académico y científico.

Resumen

Actualmente los emparejamientos bilineales sobre curvas elípticas han sido utilizados como una primitiva en la construcción de nuevos protocolos criptográficos. Con el objetivo de hacer práctico el uso de estos protocolos, en los últimos años diversos trabajos de investigación se han enfocado en el diseño e implementación eficiente y segura de los emparejamientos bilineales.

En general, un emparejamiento bilineal está definido como la proyección $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, donde $\mathbb{G}_1$ y $\mathbb{G}_2$ son grupos cíclicos escritos de manera aditiva, formados por puntos en una curva elíptica E de orden r y $\mathbb{G}_T$ es un grupo cíclico escrito de manera multiplicativa, formado por los elementos de orden r del campo finito $\mathbb{F}_{p^k}$, tal que r es un número primo y k es el grado de encajamiento de $E/\mathbb{F}_p$.

En esta tesis se muestran las estimaciones referentes al desempeño de los emparejamientos *óptimos ate* y *óptimos de Weil* en su versión serial y paralela con 192 bits de seguridad, sobre las siguientes familias de curvas elípticas amables con los emparajeramientos: BN (Barreto-Naehrig), BW-12 (Brezing-Weng), KSS-18 (Kachisa-Schaefer-Scott) y BLS-24 (Barreto-Lynn-Scott).

Además, se presentan dos nuevos métodos basados en *rejillas* que mejoran de manera significativa el cómputo de la "exponenciación final" y el cómputo de la "función picadillo hacia el grupo $\mathbb{G}_2$". Los resultados obtenidos a partir de ambos métodos son los más eficientes reportados hasta el momento.

Abstract

Nowadays, the bilinear pairings over elliptic curves have been used as a primitive in the construction of new insteresting cryptographic protocols. With the aim of making these protocols practical, in the recent years a lot of research towards the efficient and secure design and implementation of the pairings have been done.

Roughly speaking, a bilinear pairing is defined by the mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additively written cyclic groups, comprised by all the points of order r in an elliptic curve E, and $\mathbb{G}_T$ is multiplicatively written cyclic group, comprised by all the elements of order r in the finite field $\mathbb{F}_{p^k}$, such that r is a large prime number and k is the embedding degree of $E/\mathbb{F}_p$.

In this work, it's presented the estimated computational costs of the *optimal ate* and *optimal Weil* pairings in a sequential and parallel implementation at a 192-bit security level, over the following families of pairing-friendly elliptic curves: BN (Barreto-Naehrig), BW-12 (Brezing-Weng), KSS-18 (Kachisa-Schaefer-Scott) y BLS-24 (Barreto-Lynn-Scott).

Moreover, a new *lattice*-based methods for computing the "final exponentiation" and the "hashing to $\mathbb{G}_2$", are presented. These novel methods are the most efficient so far.

Índice

Lista de Algoritmos

Capítulo 1

Introducción

Sin lugar a dudas, todo nuestro
conocimiento comienza con la experiencia

Immanuel Kant

El constante crecimiento de las comunicaciones ha promovido el desarrollo de aplicaciones como el cómputo nube, redes sociales, transacciones, firmas y dinero electrónico, que requieren de intercambio y acceso seguro a la información a través de servicios de seguridad, tales como:

- **Confidencialidad.** Garantiza que la información sólo puede ser leída o manipulada por las entidades autorizadas.
- **Integridad.** Asegura que la información no sea modificada por alguna entidad no autorizada, es decir, que permanezca íntegra.
- **Autenticación.** Garantiza que una entidad es quien dice ser.
- **No Repudio.** Evita que una entidad que ha transmitido un mensaje, se retracte de haberlo hecho.
- **Disponibilidad.** La información debe estar disponible para las entidades autorizadas en el formato y tiempo adecuados.

Para hacer uso de estos servicios de seguridad, por lo general es necesario emplear esquemas criptográficos que permitan establecer la comunicación entre dos o más entidades de forma segura, a través de un canal de comunicación inseguro.

En esta tesis abordaremos el estudio de la criptografía basada en emparejamientos que actualmente es el centro de atención de muchos investigadores, ya que ha dado pie al desarrollo de nuevos protocolos criptográficos.

1.1. Criptografía

La criptografía (del griego *kriptos* que significa ocultar y *graphos* que significa escritura) ha sido empleada durante miles de años con el objetivo de proveer comunicaciones confiables sobre canales inseguros. Hoy en día, la criptografía puede ser clasificada en simétrica y asimétrica.

1.1.1. Criptografía Simétrica

La criptografía simétrica o de llave privada es la más antigua, y debido a su eficiencia es útil para cifrar gran cantidad de información; su característica principal consiste en que utiliza una misma llave para cifrar y descifrar los datos.

Los esquemas de cifrado simétrico se dividen en cifradores por flujo de datos y cifradores por bloques:

- **Cifradores por flujo de datos**. Realizan el cifrado de la información bit a bit.
- **Cifradores por bloques**. Como su nombre lo indica, procesan los datos por grupos de bits de longitud fija llamados bloques.

Por otra parte, el hecho de utilizar una misma llave para el cifrado y descifrado de la información, trae como consecuencia los siguientes problemas:

Distribución de llaves. En un grupo de n entidades, si una entidad desea comunicarse con cada una de las $n-1$ entidades restantes, deberá manejar $n-1$ llaves distintas. En total el número de llaves requeridas es de $n(n-1)/2$.

Intercambio de llaves. Si dos entidades se encuentran físicamente en lugares distintos, surge el problema de como intercambiar las llaves de manera segura.

1.1.2. Criptografía Asimétrica

La criptografía asimétrica o de llave pública es el área de interés de ésta tesis, y se basa en problemas matemáticos difíciles de resolver. A diferencia de la criptografía simétrica, se utiliza un par de llaves para cifrar y descifrar la información, llamadas llave pública y llave privada, respectivamente. La llave privada es conocida únicamente por la entidad propietaria mientras que la llave pública es conocida por todos los usuarios, de tal manera que para un grupo de n entidades, sólo se requieren dos llaves por cada entidad.

A pesar de que la criptografía asimétrica dio pie a la elaboración de nuevos protocolos criptográficos, tiene la desventaja de que el tamaño de las llaves es mayor y las operaciones de cifrado y descifrado son considerablemente más costosas que las involucradas en criptografía simétrica. Además, el hecho de contar con una llave pública requiere que una tercera entidad *"confiable"* determine que dicha llave es de quien se dice ser, evitando problemas como la usurpación de la identidad.

1.2. Antecedentes

La criptografía asimétrica fue introducida por los investigadores Whit Diffie y Martin Hellman en 1976 [18], quienes propusieron una manera interesante de resolver el problema de intercambio de llaves y cuyo trabajo fue considerado como el desarrollo más impactante en la criptografía. Dos años después, en 1978, Rivest, Shamir y Adleman dieron a conocer en [43] el primer esquema de llave pública: RSA, el cual está basado en el problema matemático de factorización.

Posteriormente en 1985 Neal Koblitz y Victor Miller propusieron, de manera independiente, el uso de curvas elípticas para el diseño de criptosistemas de llave pública, cuya seguridad radica en el problema del logaritmo discreto. [25].

En los últimos años se ha puesto gran interés en el uso de emparejamientos bilineales en criptografía. A pesar de que éstos fueron introducidos desde 1948 por André Weil, fue hasta los años 90's que Menezes, Okamoto y Vanstone los utilizaron como un ataque al problema del logaritmo discreto en curvas elípticas, reduciéndolo al problema del logaritmo discreto en campos finitos, cuya complejidad es menor [36].

Debido a sus características, actualmente los emparejamientos bilineales han sido estudiados y empleados en nuevos protocolos criptográficos tales como: Diffie-Hellman tripartito, criptografía basada en la identidad [13], firmas cortas [14], entre otros. A continuación se describe, de manera general, la criptografía basada en la identidad que es una de las aplicaciones más novedosas que han surgido a partir de los emparejamientos bilineales.

1.2.1. Criptografía Basada en la Identidad

El concepto de criptografía basada en la identidad fue introducido en 1984 por Shamir, quien propuso la idea de que una cadena arbitraria, como la dirección de correo electrónico o un número telefónico, podrían servir como llave pública en un esquema de criptografía asimétrica.

La idea principal consiste en que si Alicia desea enviar un mensaje confidencial a la dirección de correo electrónico de Beto (betito@company.com), basta con utilizar la cadena *"betito@company.com"* como llave publica para cifrar el mensaje. De esta manera, cuando Beto recibe el correo electrónico cifrado, contacta a una tercera entidad llamada "Generador de llaves privadas", con quien se autentifica y obtiene su llave privada, a partir la cual descifra el mensaje de Alicia.

1.3. Estado del arte

En los últimos años diversos investigadores han presentado implementaciones en software de emparejamientos bilineales, la mayoría enfocándose en niveles de seguridad de 128 bits. Por un lado hay quienes han optado por utilizar arquitecturas multinúcleo para la implementación eficiente de los emparejamientos bilineales sobre curvas elípticas, tal es el caso de Aranha *et al.* [4] quienes reportaron el cómputo del emparejamiento η_T en 3.02 millones de ciclos sobre curvas supersingulares definidas en el campo $\mathbb{F}_{2^{1223}}$. Otro ejemplo es el presentado en [12], en donde se llevó a cabo la implementación en un procesador Intel Core i7 del emparejamiento η_T sobre curvas supersingulares definidas en el campo $\mathbb{F}_{3^{509}}$, en 5.4 millones de ciclos.

Tomando en cuenta las principales implementaciones realizadas sobre emparejamientos bilineales en curvas elípticas ordinarias, encontramos el artículo [39] publicado por Naehrig *et al.*, en el cual se presenta los detalles de una implementación que computa el emparejamiento *óptimo ate* sobre una curva BN de 257 bits, en 4.47 millones de ciclos, lo que fue considerado como un nuevo record en velocidad para el cálculo de emparejamientos bilineales.

Sin embargo, Jean-Luc Beuchat et al., encontraron en [11] una manera más eficiente que la propuesta por Naehrig, de computar el emparejamiento *óptimo ate* sobre curvas BN de 257 bits en tan sólo 2.33 millones de ciclos. Por primera vez, fue reportado el cálculo de un emparejamiento en menos de un mili segundo. Este nuevo resultado fue superado unos meses después por Aranha *et al.*, quienes reportaron el emparejamiento *óptimo ate* sobre curvas BN con 128 bits de seguridad, en 1.703 millones de ciclos.

Cabe mencionar que estas implementaciones sobre curvas ordinarias son secuenciales. Por otra parte, Aranha *et al.* [3] paralelizaron el ciclo de MIller e implementaron el emparejamiento *óptimo ate* sobre curvas BN con 128 bits de seguridad, con una acelaración de 1.23 veces más rápido que la versión secuencial, utilizando un procesador Intel Core i5. Además, motivados por el hecho de que la exponenciación final no se puede paralelizar, Aranha *et al.* [3] estudiaron e implementaron el emparejamiento *óptimo de Weil* con una aceleración de 1.25 veces más rápido que el emparejamiento *óptimo ate* sobre 8 núcleos.

En cuanto a implementaciones con 192 bits de seguridad, Luis Dominguez *et al.* [41] presentaron un tutorial de *Magma*, en donde describen la implementación de los emparejamientos de Tate, ate y R-ate sobre curvas KSS con grado de encajamiento $k = 18$. Además se describen algunas optimizaciones realizadas y la selección de parámetros en este tipo de curvas.

Ahora que se ha demostrado que los emparejamientos bilineales pueden ser computados de manera eficientemente con 128 bits de seguridad, los investigadores han puesto sus expectativas en el cálculo de emparejamientos con 192 bits de seguridad.

1.4. Arquitecturas multinúcleo

Un microprocesador multinúcleo es un componente integrado por dos o más procesadores independientes llamados "núcleos". Algunos ejemplos son los siguientes:

- Procesadores de dos núcleos: AMD Phenom II X2, Intel Core Duo.
- Procesadores de cuatro núcleos: AMD Phenom II X4, Intel 2010 core line. Este último incluye tres niveles de procesadores de cuatro núcleos: i3, i5, i7.
- Procesadores de seis núcleos: AMD Phenom II X6, Intel Core i7 Extreme Edition 980X.
- Procesadores de ocho núcleos: AMD FX-8150.

Los núcleos pueden o no compartir la memoria cache, para lo cual es posible utilizar métodos de comunicación entre los núcleos internos y la memoria compartida. Por otra parte, la principal ventaja de una plataforma multinúcleo es que permite a los desarrolladores particionar el trabajo en los distintos núcleos, lo cual trae como consecuencia una aceleración en el rendimiento de la aplicación. Por ejemplo, en una arquitectura de dos núcleos, idealmente se espera que el factor de aceleración de una aplicación sea dos veces más rápido que su versión secuencial.

1.5. Organización de la Tesis

El contenido de la tesis ha sido organizado en seis capítulos: el capítulo 2 introduce al lector en el tema mediante la definición de conceptos generales que son indispensables para su comprensión.

Posteriormente, dado que es de nuestro profundo interés, los capítulos 3 y 4 tocan a detalle el tema de curvas elípticas y emparejamientos bilienales, describiendo tanto los principales conceptos, como los algoritmos utilizados durante el desarrollo de la tesis. Además en el capítulo 4 también se mencionan dos de las principales aportaciones realizadas, las cuales representan una mejora en

los problemas de la "exponenciación final" y la "función *picadillo* hacia el grupo $\mathbb{G}_2$", en emparejamientos bilineales sobre curvas elípticas ordinarias.

En el capitulo 5 se determina la selección de parámetros y se muestran las estimaciones realizadas y los resultados obtenidos durante la tesis, para finalmente concluir con el capítulo 6 donde se recalcan algunos puntos importantes en el trabajo a futuro.

Capítulo 2

Conceptos Básicos

Todas las verdades son fáciles de entender
una vez que han sido descubiertas; el problema es descubrirlas

Galileo Galilei

Las estructuras algebraicas como los grupos abelianos, anillos, campos finitos, entre otros, son los "ladrillos" con los cuales se construyen los emparejamientos bilineales. En este capítulo se definen las principales propiedades de dichas estructuras; además, se introduce el concepto de grupo ciclotómico y rejilla, los cuales, en los últimos años, han sido objeto de estudio en la implementación eficiente de los emparejamientos bilineales.

2.1. Grupo

Un **grupo** $(\mathbb{G}, \star, e)$ es un objeto matemático abstracto, conformado por un conjunto $\mathbb{G}$, un elemento identidad $e \in \mathbb{G}$ y una operación binaria $\star : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$, con las siguientes propiedades:

(I) La operación $\star$ es cerrada sobre los elementos del conjunto $\mathbb{G}$, es decir,

$$\forall a, b \in \mathbb{G},\ a \star b \in \mathbb{G}.$$

(II) El elemento identidad "e" es único y para todo $a \in \mathbb{G}$, se cumple que

$$a \star e = e \star a = a.$$

(III) La operación $\star$ es asociativa sobre los elementos de $\mathbb{G}$, es decir, dados $a,\ b,\ c \in \mathbb{G}$, entonces

$$a \star (b \star c) = (a \star b) \star c.$$

(IV) Para todo $a \in \mathbb{G}$ existe un único elemento $\bar{a} \in \mathbb{G}$, llamado el inverso de a, tal que

$$a \star \bar{a} = \bar{a} \star a = e.$$

(V) El grupo es llamado **abeliano** si la operación $\star$ es conmutativa, es decir, si $\forall\ a, b \in \mathbb{G}$, se satisface la igualdad

$$a \star b = b \star a.$$

Un grupo se denota por $\mathbb{G} = (\mathbb{G}, \star, e)$ y se abrevia como $\mathbb{G}$; esta notación implica que $\mathbb{G}$ es un **conjunto** de elementos que **forma un grupo** bajo la operación $\star$, donde e es el elemento identidad. Además, dado un elemento $g \in \mathbb{G}$, en este capítulo se utilizara $\star^m(g)$ para denotar la aplicación de m veces el operador $\star$ sobre el elemento g, tal que $m \in \mathbb{Z}^+$.

A continuación se mencionan algunas definiciones asociadas a los grupos:

Definición 2.1 *(Orden del grupo). El* ***orden*** *de un grupo $(\mathbb{G}, \star, e)$ está definido como el número de elementos en el conjunto $\mathbb{G}$. Los grupos pueden tener orden finito o infinito.*

Definición 2.2 *(Orden de un elemento del grupo). Sea $\mathbb{G} = (\mathbb{G}, \star, e)$ un grupo, el* ***orden*** *de $g \in \mathbb{G}$ es el menor entero positivo r, tal que $\star^r(g) = e$.*

> ***Ejemplo 1.*** Dado $\mathbb{G} = (\mathbb{G}, \star, e)$, sea $g \in \mathbb{G}$ un elemento de orden 3, entonces:
>
> $$\star^3(g) = g \star g \star g = e, \quad \text{y} \quad \star^i(g) \neq e, \text{ para } 0 \leq i < 3.$$

Además, sea $\mathbb{G}$ un grupo de orden finito $n \in \mathbb{Z}^+$, $\forall\ g \in \mathbb{G}$ el orden de g divide al orden del grupo, lo cual implica que $\star^n(g) = e$.

Definición 2.3 *(Generador del grupo). Dado el grupo $\mathbb{G} = (\mathbb{G}, \star, e)$, se dice que $g \in \mathbb{G}$ es un* ***generador*** *del grupo, si para cada $h \in \mathbb{G}$ existe $i \in \mathbb{Z}^+$, tal que $h = \star^i(g)$.*

Definición 2.4 *(Grupo Cíclico). Un grupo $\mathbb{G} = (\mathbb{G}, \star, e)$ es* ***cíclico****, si existe al menos un generador $g \in \mathbb{G}$. Al grupo cíclico generado por g se denota como $\mathbb{G} = \langle g \rangle$.*

El número de elementos generadores en un grupo cíclico finito $\mathbb{G} = (\mathbb{G}, \star, e)$ de orden n, está definido como $\varphi(n)$, donde $\varphi(\cdot)$ denota la función indicatriz de Euler[1]. Por lo tanto si $\mathbb{G}$ es de orden primo p, entonces $\mathbb{G}$ tiene $\varphi(p) = p - 1$ generadores, es decir, $\forall g \in \mathbb{G}$ tal que $g \neq e$, $\mathbb{G} = \langle g \rangle$.

Cabe mencionar que las notaciones más utilizadas en grupos son la aditiva y la multiplicativa, las cuales se describen a continuación.

Notación aditiva

Si un grupo es escrito de manera aditiva utilizando "+" para denotar la operación de grupo, entonces el elemento identidad es comunmente denotado por "0" y el inverso aditivo de $a \in \mathbb{G}$ es "$-a$". Además, sea $m \in \mathbb{Z}^+$, la aplicación de m veces el operador $+$ sobre a, se denota como "ma".

> ***Ejemplo 2.*** El conjunto finito $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ forma al grupo abeliano $(\mathbb{Z}_n, +, 0)$ de orden n, definido bajo la suma módulo n. Específicamente si $n = 4$, entonces la operación de grupo se aplica sobre los elementos de $\mathbb{Z}_4$, tal y como se muestra en la siguiente **tabla de Cayley**[2]:

[1] Sea n un entero positivo, $\varphi(n)$ se define como el número de enteros positivos menores o iguales a n que son primos relativos con n.

[2] Las tablas de Cayley describen la estructura de un grupo finito mostrando todos los posibles productos o sumas entre los elementos del grupo.

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Por otra parte, $(\mathbb{Z}_4, +, 0)$ es cíclico con $\varphi(4) = 2$ generadores: "3" y "1".

$$\begin{aligned} 3 &\equiv 3 \mod 4 \\ 3+3 &\equiv 2 \mod 4 \\ 3+3+3 &\equiv 1 \mod 4 \\ 3+3+3+3 &\equiv 0 \mod 4 \end{aligned} \qquad \begin{aligned} 1 &\equiv 1 \mod 4 \\ 1+1 &\equiv 2 \mod 4 \\ 1+1+1 &\equiv 3 \mod 4 \\ 1+1+1+1 &\equiv 0 \mod 4 \end{aligned}$$

Notación multiplicativa

Cuando el grupo es escrito de manera multiplicativa, la operación de grupo se denota como " $\cdot$ "; además "1" y " a^{-1} " representan al elemento identidad y al inverso multiplicativo de $a \in \mathbb{G}$, respectivamente. La aplicación de $m \in \mathbb{Z}^+$ veces el operador " $\cdot$ " sobre a, se denota como " a^m ".

Ejemplo 3. Dado un entero positivo n, se define a $\mathbb{Z}_n^*$ como el conjunto compuesto por los elementos en $\mathbb{Z}_n$ diferentes a cero, que son primos relativos con n, es decir,

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \text{mcd}(a, n) = 1\}.$$

$(\mathbb{Z}_n^*, \cdot, 1)$ es un grupo abeliano de orden $\varphi(n)$ que opera bajo la multiplicación módulo n. La siguiente tabla de Cayley describe la estructura del grupo en el caso particular cuando $n = 10$, donde $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$:

$\odot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$(\mathbb{Z}_{10}^*, \cdot, 1)$ es un grupo cíclico con $\varphi(4) = 2$ generadores: "3" y "7".

$$\begin{aligned} 3 &\equiv 3 \mod 10 \\ 3 \cdot 3 &\equiv 9 \mod 10 \\ 3 \cdot 3 \cdot 3 &\equiv 7 \mod 10 \\ 3 \cdot 3 \cdot 3 \cdot 3 &\equiv 1 \mod 10 \end{aligned} \qquad \begin{aligned} 7 &\equiv 7 \mod 10 \\ 7 \cdot 7 &\equiv 9 \mod 10 \\ 7 \cdot 7 \cdot 7 &\equiv 3 \mod 10 \\ 7 \cdot 7 \cdot 7 \cdot 7 &\equiv 1 \mod 10 \end{aligned}$$

Ejemplo 4. Del mismo modo, si p es un número primo, el conjunto $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ de orden $p - 1$, forma al grupo cíclico finito $(\mathbb{Z}_p^*, \cdot, 1)$.

2.1.1. Subgrupos

Dado el grupo $(\mathbb{G}, \star, e)$, sea $\mathbb{H}$ un subconjunto de $\mathbb{G}$, si $\mathbb{H}$ forma un grupo bajo la operación $\star$ con "e" como elemento identidad, entonces se dice que $(\mathbb{H}, \star, e)$ es un subgrupo de $(\mathbb{G}, \star, e)$. A continuación se definen tres teoremas relevantes en teoría de grupos:

Teorema 2.1 ***(Teorema de Lagrange)*** *[48] . Sea $\mathbb{G} = (\mathbb{G}, \star, e)$ un grupo abeliano finito y sea $\mathbb{H} = (\mathbb{H}, \star, e)$ un subgrupo de $\mathbb{G}$, entonces el orden de $\mathbb{H}$ divide al orden de $\mathbb{G}$.*

Teorema 2.2 *[48, Teorema 8.6]. Sea $\mathbb{G} = (\mathbb{G}, \star, e)$ un grupo abeliano y sea m un número entero, el conjunto*

$$\mathbb{G}\{m\} = \{a \in \mathbb{G} \mid \star^m (a) = e\},$$

forma un subgrupo de $\mathbb{G}$, definido como $(\mathbb{G}\{m\}, \star, e)$.

Ejemplo 5. Dado el conjunto $\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, tal que $(\mathbb{Z}_{13}^*, \cdot, 1)$ es un grupo abeliano de orden 12, los conjuntos:

$$\begin{array}{rcccl}
\mathbb{Z}_{13}^*\{2\} & = & \{1, 12\} & = & \{a \in \mathbb{Z}_{13}^* \mid a^2 = 1\}, \\
\mathbb{Z}_{13}^*\{3\} & = & \{1, 3, 9\} & = & \{a \in \mathbb{Z}_{13}^* \mid a^3 = 1\}, \\
\mathbb{Z}_{13}^*\{4\} & = & \{1, 5, 8, 12\} & = & \{a \in \mathbb{Z}_{13}^* \mid a^4 = 1\}, \\
\mathbb{Z}_{13}^*\{5\} & = & \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} & = & \{a \in \mathbb{Z}_{13}^* \mid a^5 = 1\}, \\
\mathbb{Z}_{13}^*\{6\} & = & \{1, 3, 4, 9, 10, 12\} & = & \{a \in \mathbb{Z}_{13}^* \mid a^6 = 1\} \\
\cdots\cdots & & & &
\end{array}$$

forman subgrupos de $(\mathbb{Z}_{13}^*, \cdot, 1)$. La siguiente tabla de Cayley describe la estructura del subgrupo $(\mathbb{Z}_{13}^*\{4\}, \cdot, 1)$:

$\odot_{13}$	1	5	8	12
1	1	5	8	12
5	5	12	1	8
8	8	1	12	5
12	12	8	5	1

Teorema 2.3 *[48, Teorema 8.7]. Sea $\mathbb{G} = (\mathbb{G}, \star, e)$ un grupo abeliano y sea m un número entero tal que*

$$\star^m(\mathbb{G}) = \{\star^m(a) \mid a \in \mathbb{G}\},$$

entonces $\star^m(\mathbb{G}) = (\star^m(\mathbb{G}), \star, e)$ es un subgrupo de $\mathbb{G}$.

Ejemplo 6. Retomando el ejemplo anterior, dado el grupo abeliano $(\mathbb{Z}_{13}^*, \cdot, 1)$, aplicando el Teorema 2.3 para $m = 9$, obtenemos que:

$$(\mathbb{Z}_{13}^*)^9 = \{a^9 \mid a \in \mathbb{Z}_{13}^*\} = \{1, 5, 8, 12\}$$

ya que:

$$\begin{aligned}
1^9 &\equiv 1 \mod 13\\
2^9 &\equiv 5 \mod 13\\
3^9 &\equiv 1 \mod 13\\
4^9 &\equiv 12 \mod 13\\
5^9 &\equiv 5 \mod 13\\
6^9 &\equiv 5 \mod 13\\
7^9 &\equiv 8 \mod 13\\
8^9 &\equiv 8 \mod 13\\
9^9 &\equiv 1 \mod 13\\
10^9 &\equiv 12 \mod 13\\
11^9 &\equiv 8 \mod 13\\
12^9 &\equiv 12 \mod 13
\end{aligned}$$

Por lo tanto, $((\mathbb{Z}_{13}^*)^9,\ \cdot\ , 1) \cong (\mathbb{Z}_{13}^*\{4\}, \cdot, 1)$ es un subgrupo de $(\mathbb{Z}_{13}^*,\ \cdot\ , 1)$. Aplicando el mismo procedimiento para $2 \leq m \leq 6$, obtenemos los conjuntos:

$$\begin{aligned}
(\mathbb{Z}_{13}^*)^2 &= \{1, 3, 4, 9, 10, 12\}\\
(\mathbb{Z}_{13}^*)^3 &= \{1, 5, 8, 12\}\\
(\mathbb{Z}_{13}^*)^4 &= \{1, 3, 9\}\\
(\mathbb{Z}_{13}^*)^5 &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}\\
(\mathbb{Z}_{13}^*)^6 &= \{1, 12\}
\end{aligned}$$

los cuales corresponden con los obtenidos en el Ejemplo 5.

Una observación muy interesante de los Ejemplos 5 y 6 es la siguiente: Dado que el orden del grupo $(\mathbb{Z}_{13}^*,\ \cdot\ , 1)$ se puede factorizar como $12 = (4)(3)$, entonces:

$$\begin{aligned}
(\mathbb{Z}_{13}^*)^4 &= \mathbb{Z}_{13}^*\{3\}\\
(\mathbb{Z}_{13}^*)^3 &= \mathbb{Z}_{13}^*\{4\}
\end{aligned}$$

y de la misma forma, dado que $12 = (6)(2)$:

$$\begin{aligned}
(\mathbb{Z}_{13}^*)^6 &= \mathbb{Z}_{13}^*\{2\}\\
(\mathbb{Z}_{13}^*)^2 &= \mathbb{Z}_{13}^*\{6\}
\end{aligned}$$

En general, dado el grupo $\mathbb{G} = (\mathbb{G}, \cdot, 1)$, si el orden del grupo se factoriza como $(c)(r)$, entonces

$$\{a^c \mid a \in \mathbb{G}\} = \{a \in \mathbb{G} \mid a^r = 1\};$$

análogamente, si el grupo es escrito de manera aditiva, es decir $\mathbb{G} = (\mathbb{G}, +, 0)$, se cumple que

$$\{ca \mid a \in \mathbb{G}\} = \{a \in \mathbb{G} \mid ra = 0\}.$$

En la implementación de protocolos basados en emparejamientos, esta observación es relevante para la solución del problema conocido como *"Función picadillo hacia el grupo* $\mathbb{G}_2$*"*, el cual se detallará en la Sección 4.8.

2.1.2. Clase Lateral

Sea $\mathbb{H} = (\mathbb{H}, \star, e)$ un subgrupo de $\mathbb{G} = (\mathbb{G}, \star, e)$, para todo $a, b \in \mathbb{G}$ se escribe $a \equiv b \pmod{\mathbb{H}}$, si $a \star \bar{b} \in \mathbb{H}$, donde $\bar{b}$ es el inverso de b. A la expresión " $\equiv \pmod{\mathbb{H}}$ " se le conoce como **relación de equivalencia** y divide al grupo $\mathbb{G}$ en **clases de equivalencia**.

Dado $a \in \mathbb{G}$, $[a]_{\mathbb{H}}$ denota la clase de equivalencia que contiene al elemento "a", la cual está definida como:

$$[a]_{\mathbb{H}} = a \star \mathbb{H} = \{a \star h \mid h \in \mathbb{H}\},$$

es decir, $x \in [a]_{\mathbb{H}} \iff x \equiv a \pmod{\mathbb{H}}$.

Las clases de equivalencia son llamadas **"las clases laterales de $\mathbb{H}$ en $\mathbb{G}$"**. El conjunto de todas las clases laterales está denotado como $\mathbb{G}/\mathbb{H}$ y forma un grupo $(\mathbb{G}/\mathbb{H}, \star, [e]_{\mathbb{H}})$, donde

$$[a]_{\mathbb{H}} \star [b]_{\mathbb{H}} = [a \star b]_{\mathbb{H}},$$

el cual es llamado **"el grupo cociente de $\mathbb{G}$ módulo $\mathbb{H}$"**.

Ejemplo 7. Dado el conjunto $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, tal que $\mathbb{G} = (\mathbb{Z}_6, +, 0)$ es un grupo abeliano bajo la suma módulo 6, por el Teorema 2.3 se cumple que $\mathbb{H} = (3\mathbb{Z}_6, +, 0)$ es un subgrupo de $\mathbb{G}$, donde $3\mathbb{Z}_6 = \{0, 3\}$.

Las clases laterales de $\mathbb{H}$ en $\mathbb{G}$ son:

$$\begin{array}{rcccl} [0]_{\mathbb{H}} & = & 0 + 3\mathbb{Z}_6 & = & \{0, 3\} \\ [1]_{\mathbb{H}} & = & 1 + 3\mathbb{Z}_6 & = & \{1, 4\} \\ [2]_{\mathbb{H}} & = & 2 + 3\mathbb{Z}_6 & = & \{2, 5\} \end{array}$$

ya que $[3]_{\mathbb{H}} = [0]_{\mathbb{H}}$, $[4]_{\mathbb{H}} = [1]_{\mathbb{H}}$ y $[5]_{\mathbb{H}} = [2]_{\mathbb{H}}$. El grupo abeliano $\mathbb{G}/\mathbb{H} = (\{[0]_{\mathbb{H}}, [1]_{\mathbb{H}}, [2]_{\mathbb{H}}\}, +, [0]_{\mathbb{H}})$ está representado a partir de la siguiente tabla de Cayley:

$+$	$[0]_{\mathbb{H}}$	$[1]_{\mathbb{H}}$	$[2]_{\mathbb{H}}$
$[0]_{\mathbb{H}}$	$[0]_{\mathbb{H}}$	$[1]_{\mathbb{H}}$	$[2]_{\mathbb{H}}$
$[1]_{\mathbb{H}}$	$[1]_{\mathbb{H}}$	$[2]_{\mathbb{H}}$	$[0]_{\mathbb{H}}$
$[2]_{\mathbb{H}}$	$[2]_{\mathbb{H}}$	$[0]_{\mathbb{H}}$	$[1]_{\mathbb{H}}$

Tal y como se puede observar, $\mathbb{G}/\mathbb{H}$ es un grupo con la misma estructura que $(\mathbb{Z}_3, +, 0)$:

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Por lo tanto, se dice que $\mathbb{G}/\mathbb{H} \cong (\mathbb{Z}_3, +, 0)$.

2.1.3. Problema del logaritmo discreto en Grupos

En esta sección se utiliza la notación multiplicativa de un grupo para definir el problema del logaritmo discreto (PLD).

Definición 2.5 *(Problema del logaritmo discreto). Dado un grupo abeliano* $\mathbb{G} = (\mathbb{G}, \cdot, 1)$ *y un generador* $g \in \mathbb{G}$*, el problema del logaritmo discreto consiste en encontrar la solución a la ecuación* $g^x = h \in \mathbb{G}$*, denotada como* $x = \log_g(h)$*.*

Análogamente, si el grupo es escrito de manera aditiva $(\mathbb{G}, +, 0)$, se busca encontrar el valor de x en la ecuación $xg = h$, donde $g, h \in \mathbb{G}$. A continuación se describen dos problemas derivados del PLD.

- **Problema computacional de Diffie-Hellman**. Dado el grupo cíclico $\mathbb{G} = (\mathbb{G}, \cdot, 1)$, tal que $\mathbb{G} = \langle g \rangle$ y dados dos elementos $h_1, h_2 \in \mathbb{G}$, el problema computacional de Diffie-Hellman consiste en calcular
$$g^{\log_g(h_1)\cdot\log_g h_2}.$$
- **Problema de decisión de Diffie-Hellman**. Dados los elementos g, g^a, g^b, b^c en el grupo $\mathbb{G} = \langle g \rangle$, donde $a, b, c \in \mathbb{Z}^+$, se tiene que determinar si acaso $g^{ab} = g^c$.

2.2. Anillos

Un anillo conmutativo con unidad está conformado por un conjunto R y dos operaciones binarias: "+" y " $\cdot$ ", que satisfacen las siguientes propiedades:

(I) $(R, +, 0)$ es un grupo abeliano.

(II) La operación " $\cdot$ " es asociativa, es decir, $\forall\ a, b, c \in R$ se cumple que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(III) La multiplicación se distribuye sobre la suma, es decir, $\forall\ a, b, c \in R$, se cumple que
$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{y} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

(IV) Existe una identidad multiplicativa, es decir, existe un elemento $1_R \in R$, tal que $1_R \cdot a = a \cdot 1_R = a$, para todo $a \in R$.

(V) La multiplicación es conmutativa. Para todo $a, b \in R, a \cdot b = b \cdot a$.

2.3. Campos

Formalmente un campo es una estructura algebraica $(\mathbb{F}, +, \cdot\ 0, 1)$ conformada por un conjunto $\mathbb{F}$ y dos operaciones binarias: adición y producto, que satisfacen las siguientes propiedades:

(I) $\mathbb{F}^+ = (\mathbb{F}, +, 0)$ es un grupo abeliano con el "0" como unidad aditiva.

(II) $\mathbb{F}^* = (\mathbb{F} - \{0\},\ \cdot\ , 1)$ es un grupo abeliano con el "1" como unidad multiplicativa.

(III) El producto se distribuye a ambos lados de la suma, es decir,

$$(a+b)\cdot c = a\cdot b + a\cdot c,$$

para todo $a, b, c \in \mathbb{F}$.

Cabe mencionar que un campo finito $(\mathbb{F}_p, +, \cdot, 0, 1)$ se suele abreviar como $\mathbb{F}_p$.

Definición 2.6 *(Característica de un campo). Dado el campo $\mathbb{F}$, sea $n \in \mathbb{Z}^+$, se dice que n es la característica de $\mathbb{F}$, si n es el menor entero positivo tal que $n \cdot 1 = \sum_{i=0}^{n-1} 1 = 0$. En caso de que no exista tal entero n, se dice que $\mathbb{F}$ es de característica 0.*

Dado un campo $\mathbb{F}$, si $\mathbb{F}$ es de característica 0, entonces $\mathbb{F}$ es un campo infinito. Del mismo modo, sea p un número primo, si la característica de $\mathbb{F}$ es p, entonces $\mathbb{F}$ es finito. Por lo tanto, el conjunto $\mathbb{F}_p = \{0, 1, 2, \ldots, p-2, p-1\}$ define un **campo finito** $(\mathbb{F}_p, +, \cdot, 0, 1)$ bajo las operaciones de suma y producto módulo p.

Ejemplo 8. Dado el conjunto $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, se cumple que:

- $\mathbb{F}_7^+ = (\mathbb{F}_7, +, 0)$ y $\mathbb{F}_7^* = (\mathbb{F}_7 - \{0\}, \cdot, 1)$ son grupos abelianos de orden "7" y "6", respectivamente.

$\oplus_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\odot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- Las operaciones "+" y " $\cdot$ " son distributivas. Por ejemplo:

$$(6+3)\cdot 2 \;=\; 2\cdot 6 + 2\cdot 3 \;=\; 4 \mod 7$$

Por lo tanto, $\mathbb{F}_7 = (\mathbb{F}_7, +, \cdot, 0, 1)$ es un campo finito.

2.3.1. Extensión de un campo finito

Definición 2.7 *(Polinomio irreducible). Dado un polinomio $f(z)$ no constante de grado $n \in \mathbb{N}$, se dice que $f(z)$ es **irreducible**, si no puede factorizarse como el producto de polinomios de grado menor a n.*

El conjunto de polinomios en la variable z con coeficientes en $\mathbb{F}_p$, está denotado por $\mathbb{F}_p[z]$. Dado un número $n \in \mathbb{N}$, el conjunto finito compuesto por los polinomios en $\mathbb{F}_p[z]$ de grado menor a $n-1$, es decir,

$$\{a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \cdots + a_2 z^2 + a_1 z + a_0 \;\mid\; a_i \in \mathbb{F}_p\},$$

forma un "campo finito de característica p", denotado por $\mathbb{F}_{p^n}$, bajo las operaciones "+" y " $\cdot$ " módulo $f(z)$, donde $f(z)$ es un polinomio irreducible de grado n. De esta manera, el campo $\mathbb{F}_{p^n}$ es de orden p^n y puede ser representado como:

$$\mathbb{F}_{p^n} = \mathbb{F}_p[z]/f(z) \cong \text{ los polinomios en } \mathbb{F}_p[z] \bmod f(z).$$

Ejemplo 9. Dado el polinomio irreducible $f(z) = z^2+z+1$, el campo finito $\mathbb{F}_{2^2}$ es expresado en función de $f(z)$ y $\mathbb{F}_2[z]$:

$$\mathbb{F}_{2^2} = \mathbb{F}_2[z]/(z^2+z+1) = \{bz+a \mid a,b \in \mathbb{F}_2\} = \{0,1,z,z+1\},$$

es decir, $\mathbb{F}_{2^2}$ es el campo finito de orden $2^2 = 4$ formado por los polinomios en $\mathbb{F}_2[z]$ módulo z^2+z+1.

La estructura de los grupos abelianos $\mathbb{F}^+_{2^2}$ y $\mathbb{F}^*_{2^2}$ escritos de manera aditiva y multiplicativa, respectivamente, es descrita a través de las siguientes tablas de Cayley:

$\oplus_{z^2+z+1}$	0	1	z	$z+1$
0	0	1	z	$z+1$
1	1	0	$z+1$	z
z	z	$z+1$	0	1
$z+1$	$z+1$	z	1	0

$\odot_{z^2+z+1}$	1	z	$z+1$
1	1	z	$z+1$
z	z	$z+1$	1
$z+1$	$z+1$	1	z

Como se puede observar, el campo finito $\mathbb{F}_{2^2} = (\{0,1,x,x+1\},+,\cdot,0,1)$ contiene al campo primo $\mathbb{F}_2 = (\{0,1\},+,\cdot,0,1)$, ya que $\{0,1\} \subset \{0,1,x,x+1\}$.

Por otro lado, dos conceptos importantes en campos finitos son la "cerradura algebraica" y la "norma de un elemento":

Definición 2.8 *(Cerradura algebraica de un campo finito $\mathbb{F}_p$). Sea p un número primo, la cerradura algebraica del campo finito $\mathbb{F}_p$, denotada por $\bar{\mathbb{F}}_p$, es el conjunto infinito de todas sus extensiones, es decir,*

$$\bar{\mathbb{F}}_p = \bigcup_{m \geq 1} \mathbb{F}_{p^m}$$

Definición 2.9 *(Norma). Sea p un número primo y sea $n \in \mathbb{N}$, los conjugados de $a \in \mathbb{F}_{p^n}$ son los elementos a^{p^i}, donde $0 \leq i \leq n-1$. La **norma** de a, denotada por $|a|$, es el producto de todos los conjugados de a, es decir,*

$$|a| = \prod_{i=0}^{n-1} a^{p^i}.$$

2.4. Torres de Campo

Con el objetivo de hacer más eficiente la aritmética en $\mathbb{F}_{p^n}$, Baktir y Sunar propusieron en [5] la idea de expresar a $\mathbb{F}_{p^n} = \mathbb{F}_p[z]/f(z)$ como una extensión del campo finito $\mathbb{F}_q$, donde $q = p^m$, tal que $m|n$:

$$\begin{aligned} \mathbb{F}_{p^n} &= \mathbb{F}_q[v]/h(v) \quad \text{, donde } h(v) \in \mathbb{F}_q[v] \text{ es de grado } n/m \\ \mathbb{F}_q &= \mathbb{F}_p[u]/g(u) \quad \text{, donde } g(u) \in \mathbb{F}_p[u] \text{ es de grado } m. \end{aligned}$$

A esta representación se le conoce con el nombre de **torre de campos**.

Como se puede observar, la estructura de la torre de campos depende directamente del valor de n. Particularmente, dados los enteros positivos "a" y "b", se dice que **un campo finito $\mathbb{F}_{p^n}$ es *"amable"* con los emparejamientos** si $n = 2^a 3^b$, tal que $\mathbb{F}_{p^n}$ se puede representar a través de a extensiones cuadráticas y b extensiones cúbicas de un campo base [24].

Además, para todo $n = 2^a 3^b$, si $4 \nmid n$ entonces la torre de campos se puede construir mediante binomios irreducibles. Por el contrario, si $n \equiv 0 \mod 4$, se requiere que $p^n \equiv 1 \mod 4$ para utilizar esta misma representación [35, Teorema 3.75].

> ***Ejemplo 10.*** Sea $p = 97$, el campo finito $\mathbb{F}_{p^6}$ se puede expresar como una extensión cúbica del campo $\mathbb{F}_{p^2}$:
>
> $$\begin{aligned} \mathbb{F}_{p^6} &= \mathbb{F}_{p^2}[v]/(v^3 - u) \\ \mathbb{F}_{p^2} &= \mathbb{F}_p[u]/(u^2 + 5) \end{aligned}$$
>
> donde $-u$ y 5 no tienen residuos cuadráticos ni residuos cúbicos en $\mathbb{F}_{p^2}$ y $\mathbb{F}_p$, respectivamente.

En las siguientes secciones se describe la aritmética de torres de campo sobre extensiones cuadráticas y cúbicas de un campo finito *"amable"* con los emparejamientos $\mathbb{F}_q$, donde $q = p^m$ para $m > 0$. Cabe mencionar que los símbolos $\oplus$, $\ominus$, $\otimes$ y $\oslash$ han sido utilizados para denotar la adición, sustracción, multiplicación y división en el campo $\mathbb{F}_q$, respectivamente.

2.4.1. Aritmética en la extensión cuadrática de un campo finito

La extensión cuadrática de campo finito $\mathbb{F}_q$ está representada como:

$$\mathbb{F}_{q^2} = \mathbb{F}_q[u]/(u^2 - \beta), \tag{2.1}$$

donde $u^2 - \beta$ es un binomio irreducible en $\mathbb{F}_q[u]$, y $\beta \in \mathbb{F}_q$.

Adición

Dados dos elementos a y $b \in \mathbb{F}_{q^2}$, el cálculo de $a + b$ es implementado a partir del Algoritmo 2.1 el cual requiere de 2 sumas en el campo $\mathbb{F}_q$.

Algoritmo 2.1 Adición en el campo $\mathbb{F}_{q^2}$

Entrada: $a = (a_0 + a_1 u), \quad b = (b_0 + b_1 u) \in \mathbb{F}_{q^2}$.
Salida: $c = a + b \in \mathbb{F}_{p^n}$.
1: $c_0 \leftarrow a_0 \oplus b_0$;
2: $c_1 \leftarrow a_1 \oplus b_1$;
3: **return** $c = c_0 + c_1 u$;

Multiplicación

La multiplicación de dos elementos $a, b \in \mathbb{F}_{q^2}$, definida como:

$$(a_0 + a_1 u) \cdot (b_0 + b_1 u) = (a_0 b_0 + a_1 b_1 \beta) + (a_0 b_1 + a_1 b_0) u,$$

es implementada eficientemente a través del método de Karatsuba-Ofman, donde

$$(a_0 b_1 + a_1 b_0) = (a_0 + a_1) \cdot (b_0 + b_1) - a_0 b_0 - a_1 b_1.$$

Algoritmo 2.2 Multiplicación de $a \cdot b$ en el campo $\mathbb{F}_{q^2}$

Entrada: $a = (a_0 + a_1 u), \quad b = (b_0 + b_1 u) \in \mathbb{F}_{q^2}$.
Salida: $c = a \cdot b \in \mathbb{F}_{q^2}$.
1: $v_0 \leftarrow a_0 \otimes b_0$;
2: $v_1 \leftarrow a_1 \otimes b_1$;
3: $c_0 \leftarrow v_0 \oplus \beta v_1$;
4: $c_1 \leftarrow (a_0 \oplus a_1) \otimes (b_0 \oplus b_1) \ominus v_0 \ominus v_1$
5: **return** $c = c_0 + c_1 u$;

El Algoritmo 2.2 requiere en total 3 multiplicaciones y 5 sumas en el campo $\mathbb{F}_q$, así como 1 m_β, donde m_β denota el producto de un elemento $a_0 \in \mathbb{F}_q$ por la constante β de la Ecuación (2.1).

Cálculo de cuadrado

En el caso particular en el que $\beta = 1$, es decir, $u^2 = -1$, la operación a^2, donde $a \in \mathbb{F}_{q^2}$, es calculada de forma análoga al método complejo de elevación al cuadrado, a través de la siguiente identidad:

$$(a_0 + a_1 u)^2 \quad = (a_0 + a_1) \cdot (a_0 - a_1) + 2 a_0 a_1 u. \tag{2.2}$$

El Algoritmo 2.3 está basado en la Ecuación (2.2) y cálcula $(a_0 + a_1 u)^2$ independientemente del valor de β, con un costo de $2m_\beta$, 2 multiplicaciones y 5 sumas en el campo $\mathbb{F}_q$.

Algoritmo 2.3 Elevación al cuadrado en el campo $\mathbb{F}_{q^2}$

Entrada: $a = (a_0 + a_1 u) \in \mathbb{F}_{q^2}$.
Salida: $c = a^2 \in \mathbb{F}_{q^2}$.
1: $v_0 \leftarrow a_0 \ominus a_1$;
2: $v_3 \leftarrow a_0 \ominus \beta a_1$;
3: $v_2 \leftarrow a_0 \otimes a_1$;
4: $v_0 \leftarrow (v_0 \otimes v_3) \oplus v_2$;
5: $c_1 \leftarrow v_2 \oplus v_2$;
6: $c_0 \leftarrow v_0 \oplus \beta v_2$
7: **return** $c = c_0 + c_1 u$;

Inversión

El inverso de un elemento en el grupo multiplicativo del campo finito $\mathbb{F}_{q^2}$, es calculado mediante la siguiente identidad:

$$(a_0 + a_1 z)^{-1} = \frac{a_0 - a_1 z}{(a_0 - a_1 z) \cdot (a_0 + a_1 z)} = \frac{a_0 - a_1 z}{a_0^2 - a_1^2 \beta}.$$

con un costo de $1m_\beta$, 2 multiplicaciones, 2 cuadrados, 2 sumas y 1 inversión en el campo $\mathbb{F}_q$.

Algoritmo 2.4 Inversión en el campo $\mathbb{F}_{q^2}$

Entrada: $a = (a_0 + a_1 u) \in \mathbb{F}_{q^2}$.
Salida: $c = a^{-1} \in \mathbb{F}_{q^2}$.
1: $v_0 \leftarrow a_0^2$;
2: $v_1 \leftarrow a_1^2$;
3: $v_0 \leftarrow v_0 \ominus \beta v_1$;
4: $v_1 \leftarrow v_0^{-1}$;
5: $c_0 \leftarrow a_0 \otimes v_1$;
6: $c_1 \leftarrow -a_1 \otimes v_1$;
7: **return** $c = c_0 + c_1 u$;

2.4.2. Aritmética en la extensión cúbica de un campo finito

La extensión cúbica del campo finito $\mathbb{F}_q$ está representada por los polinomios en $\mathbb{F}_q[w]$, reducidos módulo el polinomio irreducible $w^3 - \beta \in \mathbb{F}_q[w]$, es decir:

$$\mathbb{F}_{q^3} = \mathbb{F}_q[w]/(w^3 - \beta). \tag{2.3}$$

Adición

La adición de dos elementos en $a, b \in \mathbb{F}_{q^3}$ es calculada a partir del Algoritmo 2.5, el cual tiene un costo de 3 sumas en el campo $\mathbb{F}_q$.

Algoritmo 2.5 Adición en el campo $\mathbb{F}_{q^3}$

Entrada: $a = (a_0 + a_1 w + a_2 w^2), \quad b = (b_0 + b_1 w + b_2 w^2) \in \mathbb{F}_{q^3}$.
Salida: $c = a + b \in \mathbb{F}_{p^n}$.
1: $c_0 \leftarrow a_0 \oplus b_0$;
2: $c_1 \leftarrow a_1 \oplus b_1$;
3: $c_2 \leftarrow a_2 \oplus b_2$;
4: **return** $c = c_0 + c_1 w + c_2 w^2$;

Multiplicación

El producto de dos elementos en la extensión cúbica del campo $\mathbb{F}_q$ se calcula nuevamente a través del método de Karatsuba-Ofman, con un costo de 2 multiplicaciones por β, 6 multiplicaciones y 15 sumas en el campo $\mathbb{F}_q$.

Algoritmo 2.6 Multiplicación de $a \cdot b$ en el campo $\mathbb{F}_{q^3}$

Entrada: $a = (a_0 + a_1 w + a_2 w^2), \quad b = (b_0 + b_1 w + b_2 w^2) \in \mathbb{F}_{q^3}$.
Salida: $c = a \cdot b \in \mathbb{F}_{q^3}$.
1: $v_0 \leftarrow a_0 \otimes b_0$;
2: $v_1 \leftarrow a_1 \otimes b_1$;
3: $v_2 \leftarrow a_2 \otimes b_2$;
4: $c_0 \leftarrow ((a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \ominus v_1 \ominus v_2)\beta \oplus v_0$;
5: $c_1 \leftarrow (a_0 \oplus a_1) \otimes (b_0 + b_1) \ominus v_0 \ominus v_1 \oplus \beta v_2$;
6: $c_2 \leftarrow (a_0 \oplus a_2) \otimes (b_0 \oplus b_2) \ominus v_0 \ominus v_2 \oplus v_1$;
7: **return** $c = c_0 + c_1 w + c_2 w^2$;

Cálculo de cuadrado

J. Chung y M. Hasan presentaron en su artículo "Asymmetric Squaring Formulae" [16] una fórmula para computar cuadrados eficientemente. A partir de estos resultados, el Algoritmo 2.7 calcula $a^2 \in \mathbb{F}_{q^3}$ con un costo de $2m_\beta$, 2 multiplicaciones, 3 cuadrados y 10 sumas en el campo $\mathbb{F}_q$.

Algoritmo 2.7 Elevación al cuadrado en el campo $\mathbb{F}_{q^3}$

Entrada: $a = (a_0 + a_1 w + a_2 w^2) \in \mathbb{F}_{q^3}$.
Salida: $c = a^2 \in \mathbb{F}_{q^3}$.
1: $v_4 \leftarrow 2(a_0 \otimes a_1)$;
2: $v_5 \leftarrow a_2^2$;
3: $c_1 \leftarrow (\beta v_5 \oplus + v_4)$;
4: $v_2 \leftarrow v_4 \ominus v_5$;
5: $v_3 \leftarrow a_0^2$;
6: $v_4 \leftarrow a_0 \ominus a_1 \oplus a_2$;
7: $v_5 \leftarrow 2(a_1 \otimes a_2)$;
8: $v_4 \leftarrow v_4^2$;
9: $c_0 \leftarrow \beta v_5 \oplus v_3$;
10: $c_2 \leftarrow (v_2 \oplus v_4 \oplus v_5 \ominus v_3)$;
11: **return** $c = c_0 + c_1 w + c_2 w^2$;

Inversión

El Algoritmo 2.8 está basado en el método descrito por Scott en [45], en el cual se requiere precalcular los valores temporales

$$A = a_0^2 - \beta a_1 a_2, \quad B = \beta a_2^2 - a_0 a_1, \quad C = a_1^2 - a_0 a_2, \quad F = \beta a_1 C + a_0 A + \beta a_2 B,$$

tal que la operación

$$(a_0 + a_1 w + a_2 w^2)^{-1} = (A + Bw + Cw^2)/F,$$

es calculada con un costo de $4m_\beta$, 9 multiplicaciones, 3 cuadrados, 5 sumas y un inverso en el campo $\mathbb{F}_q$.

Algoritmo 2.8 Inversión en el campo $\mathbb{F}_{q^3}$

Entrada: $a = (a_0 + a_1 w + a_2 w^2) \in \mathbb{F}_{q^3}$.
Salida: $c = a^{-1} \in \mathbb{F}_{q^3}$.

1: $v_0 \leftarrow a_0^2$;
2: $v_1 \leftarrow a_1^2$;
3: $v_2 \leftarrow a_2^2$;
4: $v_3 \leftarrow a_0 \otimes a_1$;
5: $v_4 \leftarrow a_0 \otimes a_2$;
6: $v_5 \leftarrow a_1 \otimes a_2$;
7: $A \leftarrow v_0 \ominus \beta v_5$;
8: $B \leftarrow \beta v_2 \ominus v_3$;
9: $C \leftarrow v_1 \ominus v_4$;
10: $v_6 \leftarrow a_0 \otimes A$;
11: $v_6 \leftarrow v_6 \oplus (\beta a_2 \otimes B)$;
12: $v_6 \leftarrow v_6 \oplus (\beta a_1 \otimes C)$;
13: $F \leftarrow 1/v_6$;
14: $c_0 \leftarrow A \otimes F$;
15: $c_1 \leftarrow B \otimes F$;
16: $c_2 \leftarrow C \otimes F$;
17: **return** $c = c_0 + c_1 w + c_2 w^2$;

2.4.3. Resumen de Costos

La siguiente tabla muestra en resumen el costo de las operaciones básicas sobre extensiones cuadráticas y cúbicas del campo finito $\mathbb{F}_q$, donde 'M', 'S', Á', Í', denotan una multiplicación, cuadrado, suma e inversión en el campo $\mathbb{F}_q$.

Operación	**Costo en** $\mathbb{F}_{q^2}$	**Costo en** $\mathbb{F}_{q^3}$
Suma	2A	2A
Multiplicación	3M+5A+m_β	6M + 15A+2m_β
Cuadrado	2M+5A+2m_β	2M+3S+10A+2m_β
Inversión	2M+2S+2A+I+m_β	9M+3S+5A+4m_β

Tabla 2.1: Costo de la aritmética en la extensión cuadrática y cúbica de un campo finito

2.5. Grupo Ciclotómico

Definición 2.10 *(Raíces de la unidad). Dado $n \in \mathbb{N}$, las raíces n-ésimas de la unidad son las n soluciones del polinomio $z^n - 1 = 0$, las cuales están denotadas por z_j.*

$$z^n - 1 = \prod_{j=0}^{n-1} (z - z_j).$$

El conjunto de las raíces n-ésimas de la unidad denotado como μ_n, forma un grupo cíclico

$$\mu_n = (\mu_n, \cdot, 1).$$

Definición 2.11 *(Raíces primitivas de la unidad). Sea $z^* \in \mu_n$, se dice que z^* es una raíz "primitiva" de la unidad, si y sólo si $\mu_n = \langle z^* \rangle$. Sea $\varphi(\cdot)$ la función indicatriz de Euler, μ_n tiene $\varphi(n)$ raíces primitivas.*

Ejemplo 11. Sea $\mathbb{C}$ el conjunto de los números complejos, las raíces cuartas de la unidad forman al grupo cíclico

$$\mu_4 = (\{1, i, -1, -i\}, \ \cdot \ , 1),$$

donde i y $-i$ son raíces primitivas, ya que $\mu_4 = \langle i \rangle$ y $\mu_4 = \langle -i \rangle$, como se muestra a continuación:

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1$$

$$-i^1 = -i, \quad -i^2 = -1, \quad -i^3 = i, \quad -i^4 = 1$$

Definición 2.12 *(Polinomio ciclotómico). El n-ésimo polinomio ciclotómico $\Phi_n(z)$ tiene grado $\varphi(n)$ y está definido como se muestra a continuación:*

$$\Phi_n(z) = \prod_{l=0}^{\varphi(n)-1} (z - z_l^*)$$

donde z_l^* son las raíces n-ésimas primitivas de la unidad.

Dado que las raíces de $\Phi_n(z)$ forman un subconjunto de μ_n, donde μ_n es el conjunto de raíces del polinomio $z^n - 1$, entonces $\Phi_n(z) | z^n - 1$.

Definición 2.13 *(Grupo ciclotómico). Sea p un número primo y sea $\mathbb{F}_{p^n}^*$ el grupo multiplicativo de un campo finito de característica p, el n-ésimo grupo ciclotómico $\mathbb{G}_{\Phi_n(p)}$ es un subgrugo de $\mathbb{F}_{p^n}^*$, definido por:*

$$\mathbb{G}_{\Phi_n(p)} = (\{\alpha \in \mathbb{F}_{p^n}^* | \alpha^{\Phi_n(p)} = 1\}, \ \cdot \ , 1)$$

Ejemplo 12. Dados los elementos $f, \alpha \in \mathbb{F}_{p^{12}}^*$, tal que $\alpha = f^{(p^{12}-1)/\Phi_{12}(p)}$, entonces α es un elemento en el grupo ciclotómico $\mathbb{G}_{\Phi_{12}(p)}$, ya que:

$$\alpha^{\Phi_{12}(p)} = \alpha^{p^4 - p^2 + 1} = f^{(p^{12}-1)} = 1$$

2.5.1. Cuadrados en el grupo ciclotómico $G_{\Phi_n(p)}$.

Como se mostrará en el capítulo 4, en la implementación de emparejamientos bilineales es necesario calcular la operación α^2, donde $\alpha \in \mathbb{G}_{\Phi_n(p)}$.

Particularmente se han estudiado los trabajos de Granger y Scott [24], así como el de Karabina [31], los cuales están enfocados en campos finitos $\mathbb{F}_{p^n}$, *amables* con los emparejamientos, donde

$n = 2^a 3^b$ para $a,\ b \in \mathbb{Z}^+$. De este modo, $\mathbb{F}_{p^n}$ es expresado como una extensión cúbica de una extensión cuadrática,

$$\begin{aligned} \mathbb{F}_{p^n} &= \mathbb{F}_{q^2}[z]/z^3 - \gamma, \quad \text{para } q = p^{2^{a-1}3^{b-1}}. \\ \mathbb{F}_{q^2} &= \mathbb{F}_q[w]/w^2 - \xi. \end{aligned} \tag{2.4}$$

Es decir, un elemento α en el grupo $\mathbb{F}^*_{p^n}$ es representado como

$$\begin{gathered} \alpha = (a + bz + cz^2)\ , \ \text{donde} \\ a = (a_0 + a_1 w), \quad b = (b_0 + b_1 w) \ \text{ y } \ c = (c_0 + c_1 w), \end{gathered} \tag{2.5}$$

tal que $a, b, c \in \mathbb{F}_{q^2}$ y $a_i, b_i, c_i \in \mathbb{F}_q$, para $i \in \{0, 1\}$.

Cuadrados de Granger y Scott

La forma tradicional de implementar la operación $\alpha^2 \in \mathbb{F}^*_{p^n}$ es:

$$\begin{aligned} \alpha^2 &= (a + bz + cz^2)^2 \\ &= (a^2 + 2bc\gamma) + (2ab + c^2\gamma)z + (2ac + b^2)z^2. \end{aligned} \tag{2.6}$$

No obstante, los autores demostraron que si α es un elemento en $\mathbb{G}_{\Phi_n(p)}$, es decir, $\alpha^{\Phi_n(p)} = \alpha^{p^{n/3} - p^{n/6} + 1} = 1$, entonces a, b y c satisfacen las siguientes identidades:

$$\begin{aligned} bc &= a^2 - \bar{a}/\gamma \\ ab &= c^2\gamma - \bar{b} \\ ac &= b^2 - \bar{c} \end{aligned}$$

donde $\bar{a}$, $\bar{b}$ y $\bar{c}$ son los conjugados de a, b y c respectivamente.

Sustituyendo los valores bc, ab y ac en la Ecuación (2.6), obtenemos que la operación α^2 es calculada con un costo de 3 cuadrados y 12 sumas en el campo $\mathbb{F}_{q^2}$, como se muestra a continación:

$$\alpha^2 = (3a^2 - 2\bar{a}) + (3c^2\gamma + 2\bar{b})z + (3b^2 - 2\bar{c}).$$

Cuadrados de Karabina o cuadrados comprimidos

El algoritmo propuesto por Karabina para el cálculo de $\alpha^2 = (a + bz + cz^2)$ (Ecuación (2.5)) requiere de tres bloques principales:

1. El elemento α es comprimido por la función $\mathcal{C}$:

$$\mathcal{C}(\alpha) = (b_0 + b_1 w)z + (c_0 + c_1 w)z^2$$

2. Se calcula $\mathcal{C}(\alpha^2) = (B_0 + B_1 w)z + (C_0 + C_1 w)z^2$ a través de las siguientes igualdades:

$$B_0 = 2b_0 + 3((c_0 + c_1)^2 - c_0^2 - c_1^2), \qquad B_1 = 3(c_0^2 + c_1^2\xi) - 2b_1,$$

$$C_0 = 3(b_0^2 + b_1^2\xi) - 2c_0, \qquad C_1 = 2c_1 + 3(b_0 + b_1)^2 - b_0^2 - b_1^2).$$

Esta operación requiere de 6 cuadrados y 22 sumas en el campo $\mathbb{F}_q$.

3. Se calcula $\alpha^2 = \mathcal{D}(\mathcal{C}(\alpha^2)) = (A_0 + A_1 w) + (B_0 + B_1 w)z + (C_0 + C_1 w)z^2$ con un costo adicional de 3 cuadrados, 3 multiplicaciones, 11 sumas y 1 inverso en el campo $\mathbb{F}_q$:

$$\left\{ \begin{array}{lll} A_1 = \frac{C_1^2\xi + 3C_0^2 - 2B_1}{4B_0}, & A_0 = (2A_1^2 + B_0C_1 - 3B_1C_0)\xi + 1 & \text{si } B_0 \neq 0 \\ A_1 = \frac{2C_0C_1}{B_1}, & A_0 = (2A_1^2 - 3B_1C_0)\xi + 1 & \text{si } B_0 = 0 \end{array} \right\}$$

Debido a la descompresión $\mathcal{D}(\mathcal{C}(\alpha^2))$, el método de Karabina tiene un costo computacional mayor al algoritmo propuesto por Granger y Scott. No obstante, cuando se requiere del cómputo de α^{2^i} para $0 \leq i$, el uso de cuadrados comprimidos conlleva un ahorro significativo.

2.5.2. Exponenciación en el grupo ciclotómico

En general, sea $\mathbb{G} = (\mathbb{G}, \cdot, 1)$ un grupo cíclico finito escrito de manera multiplicativa, y sea g un generador de $\mathbb{G}$, la exponenciación g^x, donde x es un número entero, es calculada expresando al exponente x como un número binario $x = \sum_{i=0}^{\ell} x_i 2^i$, tal que

$$g^x = g^{\sum_{i=0}^{\ell} x_i 2^i} = \prod_{i=0}^{\ell} g^{x_i 2^i} = \prod_{i=0}^{\ell} [g^{2^i}]^{x_i} = \prod_{x_i=1} g^{2^i},$$

En total esta operación requiere de $\ell = \log_2(x)$ cuadrados y $w_H(x)$ multiplicaciones, donde $w_H(x)$ denota el peso de Hamming de x. Si $g \in \mathbb{G}_{\Phi_n(p)}$ el método de Karabina se puede aplicar para el cómputo eficiente de g^x, a través de los siguientes pasos:

1. Se obtiene la representación con signo del entero $x = \sum_{i=0}^{\ell} 2^i x_i$, tal que $x_i = \{0, 1, -1\}$.
2. Se computa $\mathcal{C}(g^{2^i})$ para $0 \leq i \leq \ell$ y se almacenan los valores $h_j = \mathcal{C}(g^{2^i})$ cuando el bit $x_i \neq 0$.
3. Se descomprimen los valores h_j almacenados, es decir, $\mathcal{D}(\mathcal{C}(g^{\pm 2^i}))$ si $x_i \neq 0$.
4. Finalmente se calcula $g^x = \prod g^{\pm 2^i}$ si $x_i \neq 0$.

2.6. Rejilla (*Lattice*)

En esta sección comenzaremos por definir, de una manera general, los conceptos básicos que son esenciales en el estudio de las *rejillas*[3], entre estas definiciones se incluye la de *"espacio vectorial"*, que para propósitos de este capítulo, nos enfocaremos únicamente en considerar *espacios vectoriales* contenidos en $\mathbb{R}^m$, para algún entero positivo m.

Definición 2.14 *(Espacio Vectorial). Un espacio vectorial V es un subconjunto de $\mathbb{R}^m$, el cual es cerrado bajo la operación de suma y bajo la multiplicación escalar por elementos en $\mathbb{R}$, es decir:*

$$\forall\ w_1, w_2 \in V\ \ y\ \ \forall\ \alpha_1, \alpha_2 \in \mathbb{R}, \text{ se cumple que: } \alpha_1 w_1 + \alpha_2 w_2 \in V$$

El conjunto de vectores $w_1, w_2, \ldots, w_n \in V$ es *linealmente independiente*, si la única forma en que se satisfaga la siguiente igualdad:

$$\alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_n w_n = 0,$$

es si y sólo si $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

[3]En este trabajo han sido empleadas las *rejillas* en el cómputo eficiente de los emperejamientos bilineales, sin entrar en detalles acerca de su construcción y definición. En el caso de requerir mayor información del tema, se pueden consultar las referencias [34, 28].

Definición 2.15 *(Base de un espacio vectorial). La base de V es el conjunto de vectores linealmente independientes $v_1, \ldots, v_n$, tales que, todo vector $w \in V$ puede ser representado como una combinación lineal de v_i, es decir:*

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n,$$

donde $\alpha_i \in \mathbb{R}$, para $1 \leq i \leq n$.

Definición 2.16 *(Rejilla). Sea $v_1, \ldots, v_n \in \mathbb{R}^m$ la base del espacio vectorial V, la **rejilla** L generada por dicha base, es el conjunto de vectores formados por la combinación lineal de $v_1, ..., v_n$ con coeficientes en $\mathbb{Z}$, es decir $L \subset V$.*

> ***Ejemplo 13.*** Supongamos que $v_1 = (5.3,\ 1.9,\ 8.1)$, $v_2 = (3,\ 6.2,\ 2)$ y $v_3 = (1.4,\ 7,\ 1)$ son la *base* de la *rejilla* L, entonces $w_1 = (6.7,\ 8.9,\ 9.1)$, $w_2 = (5.1,\ 9.7,\ 8.1)$ y $w_3 = (11.3,\ 14.3,\ 12.1)$ son vectores en L, ya que:
>
> $$\begin{aligned} w_1 &= v_1 + v_3 \\ w_2 &= v_1 - v_2 + 2v_3 \\ w_3 &= v_1 + 2v_2 \end{aligned}$$
>
> y por el contrario, el vector $w_4 = 2.8v_1$ no pertenece a la *rejilla*, debido a que $2.8 \notin \mathbb{Z}$.

Uno de los problemas fundamentales en Rejillas, consiste en encontrar el vector $w \in L$ con la menor norma euclidiana [4] $\|w\|$. Dada la base $v_1, ..., v_n$ de L, el algoritmo LLL de Lenstra, Lenstra y Lovasz [34], obtiene n vectores $w_i \in L$ de m dimensiones, tales que:

$$\|w_i\| = \left(\sum_{j=0}^{m-1} |w_{ij}|^2 \right)^{1/2} \quad \text{es mínima.}$$

2.7. Morfismos

Un **morfismo** es una proyección entre dos estructuras matemáticas. Existen diferentes tipos de morfismos:

- Monomorfismo. Un monomorfismo de X a Y está denotado como $f : X \to Y$. Para todos los morfismos $g_1, g_2 : Z \to X$, se cumple que $f \circ g_1 = f \circ g_2$.
- Isomorfismo. $f : X \to Y$ es un isomorfismo, si existe un morfismo $g : Y \to X$.
- Endomorfismo. Es un morfismo de un objeto matemático a sí mismo.
- Automorfismo. Es un endomorfismo invertible, es decir, es un isomorfismo a sí mismo.

[4] Dado un vector $v = (v_1, v_2, \ldots, v_n)$, la norma euclidiana de v, también conocida como la magnitud del vector, está denotada por $\|v\|$ y definida como $\|v\| = \sqrt{v_1^2 + v_2^2 + \cdots + v_n^2}$.

2.8. Eigenespacio

El concepto de eigenespacio es utilizado en la definición de emparejamientos, por lo tanto, a continuación se muestra una definición general e informal de dicho concepto:

Los vectores propios o **eigenvectores** de un operador lineal son los vectores no nulos que, cuando son transformados por el operador, dan lugar a la multiplicación de sí mismos por un escalar λ, el cual es llamado valor propio o **eigenvalor**. El **eigenespacio-**λ de un operador lineal, es el conjunto de eigenvectores con valor propio λ.

Capítulo 3

Curvas Elípticas e Introducción a los Emparejamientos Bilineales

Todos somos aprendices de un
oficio donde ninguno llega a ser maestro

Ernest Hemingway

La primera sección de este capítulo tiene el objetivo de introducir al lector en el área de las curvas elípticas, mediante la definición de conceptos básicos referentes al tema. Posteriormente, se describe una introducción a los emparejamientos bilineales, en donde se muestra la importancia de las curvas elípticas y campos finitos, para mantener el nivel de seguridad deseado en el cómputo del emparejamiento.

3.1. Curvas Elípticas

Una **curva elíptica** E **sobre un campo** $\mathbb{F}$, denotada como $E/\mathbb{F}$, en el *espacio afín*, está definida por la ecuación de Weierstrass:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.1}$$

donde $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. Sea $\text{char}(\mathbb{F})$ la característica del campo $\mathbb{F}$ [Definición 2.6], si $\text{char}(\mathbb{F}) \neq 2, 3$, el cambio admisible de variables [25]:

$$(x, y) \rightarrow \left(\frac{x - 3a_1^2 - 12a_2}{36}, \ \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24} \right)$$

transforma a $E/\mathbb{F}$ en una curva elíptica definida por la ecuación

$$y^2 = x^3 + ax + b, \tag{3.2}$$

con discriminante $\Delta = -16(4a^3 + 27b^2)$, la cual es conocida como la ecuación simplificada de Weierstrass [25], donde $a, b \in \mathbb{F}$.

> ***Ejemplo 14.*** La gráfica correspondiente a la curva elíptica $E : y^2 = x^3 + ax + b$ definida sobre el campo de los números reales $\mathbb{R}$ es la siguiente:

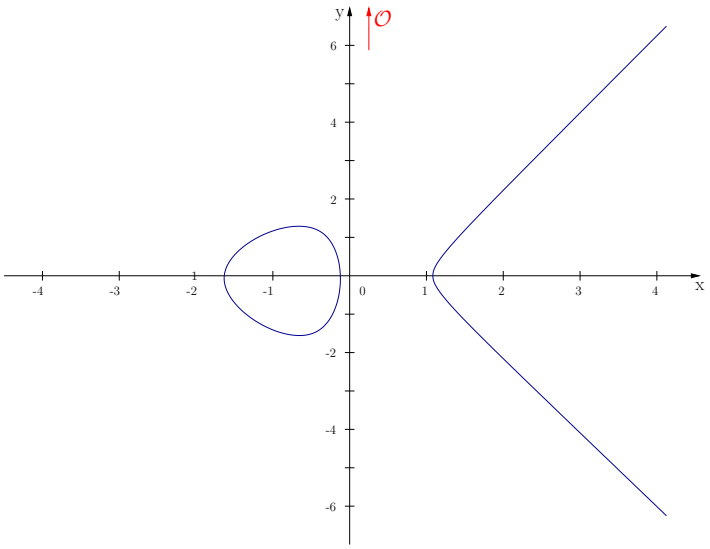


Figura 3.1: Curva elíptica sobre el campo de los reales $\mathbb{R}$.

3.1.1. Puntos en la curva elíptica

Definición 3.1 *(Punto al infinito). El punto correspondiente a (∞, ∞) es llamado el **punto al infinito** y está denotado por $\mathcal{O}$. El punto al infinito se encuentra en el extremo inferior y superior del eje de las ordenadas, de tal manera que la línea vertical al punto $P = (x, y)$ interseca a $\mathcal{O}$.*

Sea $\bar{\mathbb{F}}$ la cerradura algebráica de $\mathbb{F}$, dada la curva elíptica $E/\mathbb{F}$ definida por la Ecuación (3.2), el conjunto de los **puntos en la curva** $E/\mathbb{F}$ es:

$$E(\bar{\mathbb{F}}) = \{(x, y) \mid x, y \in \bar{\mathbb{F}},\ y^2 - x^3 - ax - b = 0\} \cup \{\mathcal{O}\}.$$

Además, para cualquier campo $\mathbb{F}'$, tal que $\mathbb{F} \subseteq \mathbb{F}' \subset \bar{\mathbb{F}}$, el conjunto de los **$\mathbb{F}'$-puntos racionales** de la curva elíptica se define como:

$$E(\mathbb{F}') = \{(x, y) \mid x, y \in \mathbb{F}',\ y^2 - x^3 - ax - b = 0\} \cup \{\mathcal{O}\}$$

y **forma un grupo abeliano escrito de manera aditiva**, donde $\mathcal{O}$ es el elemento identidad. De esta manera, en las siguientes secciones utilizaremos la notación $E(\mathbb{F}')$ para refirirnos al grupo abeliano y no sólo al conjunto de los $\mathbb{F}'$-puntos racionales de $E/\mathbb{F}$.

3.1.2. Suma de puntos

Dada una curva elíptica $E/\mathbb{F}$, la suma de dos puntos P y $Q \in E(\mathbb{F})$, denotada por $P + Q$, es calculada como se describe a continuación:

1. Si $P = Q$, se traza la recta tangente a la curva elíptica en el punto P, denotada como $\ell_{P,P}$. En caso contrario, es decir, si $P \neq Q$, se traza la recta secante a la curva elíptica en los puntos P y Q, la cual está denotada por $\ell_{P,Q}$.

2. Ambas rectas $\ell_{P,P}$ y $\ell_{P,Q}$ intersecan un tercer punto denominado $-R$, el cual se refleja sobre el eje de las abscisas, obteniendo el punto $R = P + Q$ (Figuras 3.2 y 3.3). El punto $-R$ tiene coordenadas $(x_R, -y_R)$, de tal manera que $R + (-R) = \mathcal{O}$.

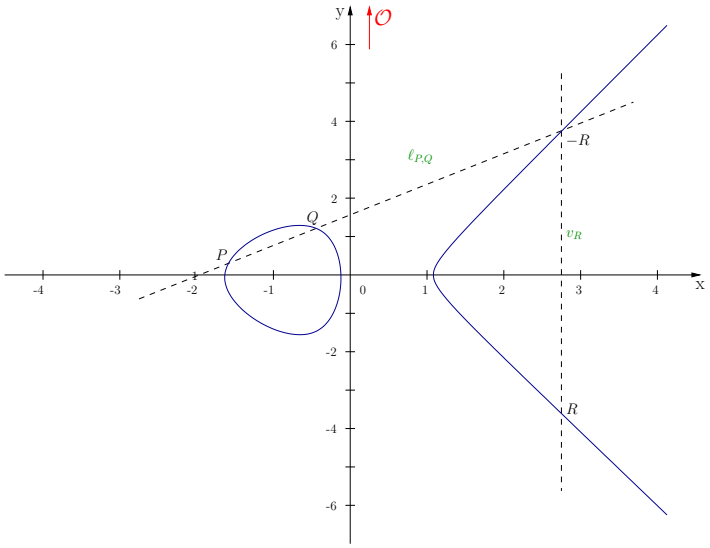


Figura 3.2: Suma de $P + Q$ en el campo de los reales $\mathbb{R}$.

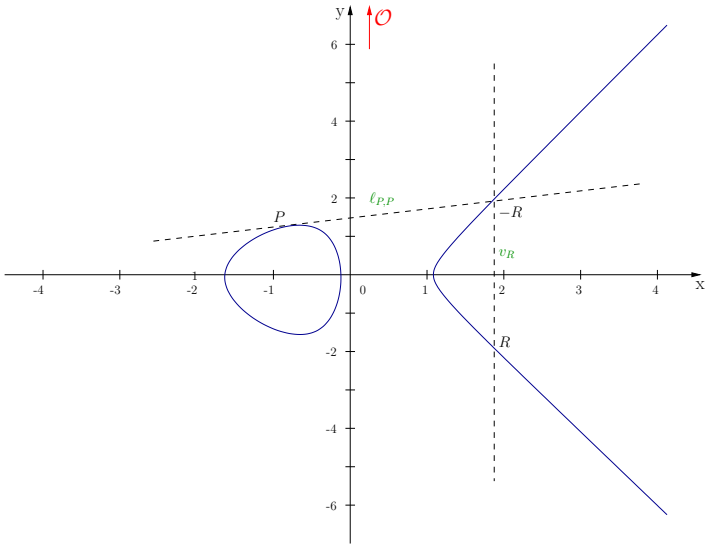


Figura 3.3: Suma de $P + P = 2P$ en el campo de los reales $\mathbb{R}$.

Con el objetivo de brindar una explicación más detallada de la suma de puntos, a continuación se describe el cálculo de $P+Q \in E(\mathbb{F})$ a través de ecuaciones, donde $E : y^2 = x^3+ax+b$, para $Q \neq P$ y $Q \neq -P$.

Partiendo de la ecuación de la recta $\ell_{P,Q}$, la cual está definida como:

$$y = m(x - x_P) + y_P, \quad \text{donde} \quad m = \frac{y_Q - y_P}{x_Q - x_P}, \tag{3.3}$$

se calcula la intersección de $\ell_{P,Q}$ en $E/\mathbb{F}$, igualando la Ecuación (3.3) con la ecuación de la curva elíptica, es decir:

$$(m(x - x_P) + y_P)^2 = x^3 + ax + b.$$

Desarrollando la ecuación anterior, obtenemos que:

$$x^3 - m^2x^2 + (a + 2x_Pm^2 - 2y_Pm)x + (b - x_P^2m^2 + 2x_Py_Pm - y_P^2) = 0.$$

Las tres raíces de este polinomio son las tres coordenadas, en el eje de las abscisas, de los puntos en los cuales la recta $\ell_{P,Q}$ interseca a la curva $E/\mathbb{F}$, es decir: x_P, x_Q y x_R. Por lo tanto:

$$x^3 - m^2x^2 + ux - v = (x - x_P)(x - x_Q)(x - x_R), \tag{3.4}$$

donde $u = a + 2x_Pm^2 - 2y_Pm$ y $v = b - x_P^2m^2 + 2x_Py_Pm - y_P^2$. Desarrollando la parte derecha de la Ecuación(3.4), obtenemos la siguiente igualdad:

$$x^3 - m^2x^2 + ux - v = x^3 + (-x_R - x_Q - x_P)x^2 + (x_Qx_R + x_Px_R + x_Px_Q)x - (x_Px_Qx_R),$$

de la cual se deduce que $-m^2 = -x_R - x_Q - x_P$ y por ende:

$$x_R = m^2 - x_Q - x_P.$$

Finalmente a partir de la Ecuación(3.3), se calcula $y_R = m(x_P - x_R) - y_P$ para obtener el punto $R = (x_R, y_R) = P + Q$.

En el caso particular cuando $Q = -P$, la suma de puntos $P + Q = \mathcal{O}$. Por otra parte, si $Q = P$, entonces $P + P = 2P$ es calculado de manera similar al método previamente descrito, tal y como se muestra en el Algoritmo 3.1.

Algoritmo 3.1 Suma de Puntos

Entrada: Coeficientes a, b de la curva elíptica $E : y^2 + ax + b$.
Puntos $P = (x_P, y_P)$ y $Q = (x_Q, y_Q) \in E(\mathbb{F})$.
Salida: $R = P + Q$.

1: **if** $P = \mathcal{O}$ **then**
2: **return** $R \leftarrow Q$;
3: **end if**
4: **if** $Q = \mathcal{O}$ **then**
5: **return** $R \leftarrow P$;
6: **end if**
7: **if** $x_P \neq x_Q$ **then**
8: $\lambda \leftarrow (y_P - y_Q)/(x_P - x_Q)$;
9: Ir al paso **18**;
10: **end if**
11: **if** $y_P \neq y_Q$ **then**
12: **return** $R \leftarrow \mathcal{O}$;
13: **end if**
14: **if** $y_Q = 0$ **then**
15: **return** $R \leftarrow \mathcal{O}$;
16: **end if**
17: $\lambda \leftarrow (3x_Q^2 + a)/2y_Q$;
18: $x_R \leftarrow \lambda^2 - x_P - x_Q$;
19: $y_R \leftarrow (x_Q - x_R)\lambda - y_Q$;
20: **return** $R \leftarrow (x_R, y_R)$

3.1.3. Espacio proyectivo

Una curva elíptica E sobre un campo $\mathbb{F}$, en el *espacio proyectivo*, está definida por la ecuación homogénea de Weierstrass:

$$E : y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3.5}$$

donde $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. Al igual que en el *espacio afín*, si la característica del campo es distinta a 2 ó 3, $E/\mathbb{F}$ se transforma en una curva elíptica definida por la ecuación [25]:

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{3.6}$$

Como se puede observar, la ecuación anterior se puede obtener sustituyendo $x = \frac{X}{Z}$ y $y = \frac{Y}{Z}$ en la Ecuación(3.2), donde $Z \neq 0$. Por lo tanto un punto (X, Y, Z) en el espacio proyectivo, corresponde al punto $(x = \frac{X}{Z}, y = \frac{Y}{Z})$ en el espacio afín, mientras que el punto al infinito $\mathcal{O}$ está definido como $(0, 1, 0)$.

Por otra parte, la suma de puntos $P + Q \in E(\mathbb{F})$, se realiza utilizando la misma metodología, con un costo de cómputo distinto:

Espacio	Costo de $P + Q$	Costo de $2P = P + P$
Afín	1I, 2M, 1S	1I, 2M, 2S
Proyectivo	12M, 2S	7M, 3S

donde "M", "S", "I", denota la multiplicación, cuadrado e inverso en el campo $\mathbb{F}$. Si la razón $I/M \geq 8$, entonces el costo de cómputo es menor en el espacio proyectivo.

En las siguientes secciones nos referiremos a $E/\mathbb{F}$ como una curva elíptica en el espacio afín, donde $\mathbb{F}$ es un campo de característica diferente a 2 y 3.

3.2. Curvas elípticas sobre campos finitos

Sea p un número primo y sea $q = p^n$, donde $n \in \mathbb{Z}^+$, dado un campo finito $\mathbb{F}_q$ de característica p, los $\mathbb{F}_q$-puntos racionales de una curva elíptica forman un grupo **finito** $E(\mathbb{F}_q)$, tal que para todo $P = (x_P, y_P) \in E(\mathbb{F}_q)$, $x_P, y_P \in \mathbb{F}_q$.

> ***Ejemplo 15.*** Dada la curva elíptica $E/\mathbb{F}_{23} : y^2 = x^3 + x$, la gráfica correspondiente al conjunto finito de los $\mathbb{F}_{23}$ -puntos racionales de E se muestra en la Figura 3.4.
>
> $E(\mathbb{F}_{23})$ es un grupo abeliano, donde cada punto tiene un inverso y la suma de dos puntos $P + Q \in E(\mathbb{F}_{23})$. Por ejemplo:
>
> - Dado que $-5 \mod 23 \equiv 18$, el punto $(13, 5)$ es el inverso de $(13, 18)$.
> - $(9, 5)+(20, 19) = (19, 22) \in E(\mathbb{F}_{23})$, los cual se puede comprobar utilizando las ecuaciones de suma de puntos, explicadas en la Sección 3.1.2:
>
> $$\begin{aligned} m &= \frac{19 - 5}{20 - 9} \mod 23 = 18 \\ x' &= 18^2 - 20 - 9 \mod 23 = 19 \\ y' &= 18(9 - 19) - 5 \mod 23 = 22 \end{aligned}$$

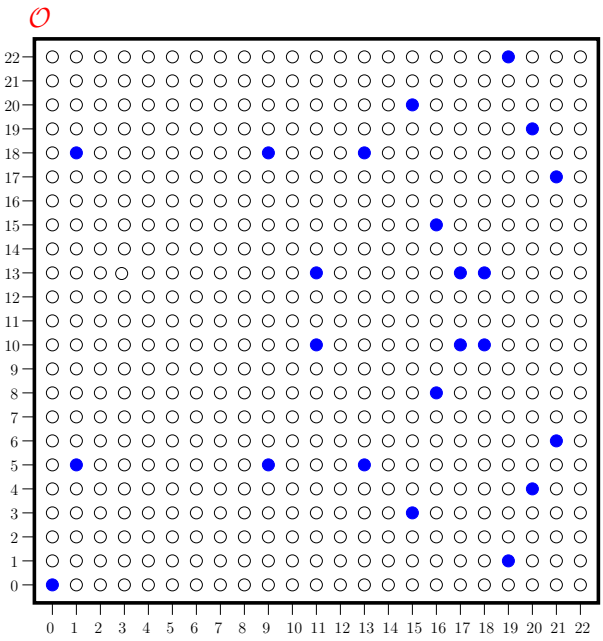


Figura 3.4: Curva elíptica sobre el campo finito $\mathbb{F}_{23}$

3.2.1. Orden de la curva elíptica

Sea p un número primo y sea $q = p^n$ para algún entero positivo n. Dado el campo finito $\mathbb{F}_q$ y una curva elíptica $E/\mathbb{F}_q$, el orden del grupo $E(\mathbb{F}_q)$, denotado por $\#E(\mathbb{F}_q)$, está definido por el teorema de Hasse como se describe a continuación:

Teorema 3.1 *[25, Teorema 3.7]. Sea E una curva elíptica definida sobre el campo $\mathbb{F}_q$, entonces*

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

Alternativamente, se puede escribir $\#E(\mathbb{F}_q) = q + 1 - t$, donde $|t| \leq 2\sqrt{q}$. El parámetro "t" se define como la *traza* de E sobre $\mathbb{F}_q$ y dado que t es relativamente más pequeño que q, $\#E(\mathbb{F}_q) \approx q$.

Dada una curva elíptica $E/\mathbb{F}_q$ con $q = p^n$ y $\#E(\mathbb{F}_q) = q + 1 - t$, se dice que $E/\mathbb{F}_q$ es **supersingular** [50] si p divide a t. Dicho en otras palabras, E es supersingular si y sólo si $t \equiv 0 \mod p$, lo cual es cierto si y sólo si $\#E(\mathbb{F}_q) \equiv 1 \mod p$; de otra forma, la curva es llamada **ordinaria**.

Supongamos que E está definida sobre el campo $\mathbb{F}_q$, sea $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$, tal que $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$, entonces $E(\mathbb{F}_q)$ es un subgrupo de $E(\mathbb{F}_{q^m})$. El orden de $E(\mathbb{F}_{q^m})$ se puede determinar a partir de la traza de $E(\mathbb{F}_q)$. El caso más simple es para una curva elíptica $E/\mathbb{F}_p$, donde $\#E(\mathbb{F}_p) = p + 1 - t$. El orden de $E(\mathbb{F}_{p^2})$ es determinado por la siguiente igualdad:

$$\#E(\mathbb{F}_{p^2}) = p^2 + 1 - (t^2 - 2p).$$

En general, dada la curva elíptica $E/\mathbb{F}_p$, el orden del grupo finito $E(\mathbb{F}_{p^m})$ para $m \in \mathbb{Z}^+$, es calculado mediante el siguiente algoritmo:

Algoritmo 3.2 Cálculo de $\#E(\mathbb{F}_{p^m})$, para una curva elíptica E definida sobre el campo $\mathbb{F}_p$

Entrada: m, p, t, tal que $\#E(\mathbb{F}_p) = p + 1 - t$.
Salida: $\#E(\mathbb{F}_{p^m})$.

1: $\tau_0 \leftarrow 2$
2: $\tau_1 \leftarrow t$;
3: **for** $i = 1$ to $m - 1$ **do**
4: $\quad \tau_{i+1} \leftarrow t \cdot \tau_i - p \cdot \tau_{i-1}$
5: **end for**
6: $q \leftarrow p^m$
7: $\tau \leftarrow \tau_m$
8: **return** $q + 1 - \tau$;

3.2.2. Puntos de torsión

Dada una curva elíptica $E/\mathbb{F}_p$, sea $\bar{\mathbb{F}}_p$ la cerradura algebráica de $\mathbb{F}_p$ [Definición 2.8], para cualquier entero positivo r, definimos el conjunto de los puntos de torsión r de $E(\bar{\mathbb{F}}_p)$, denotado como $E(\bar{\mathbb{F}}_p)[r]$, como el conjunto de puntos en $E(\bar{\mathbb{F}})$ de orden r:

$$E(\bar{\mathbb{F}}_p)[r] = \{P \in E(\bar{\mathbb{F}}_p) | rP = \mathcal{O}\}.$$

Sea $n \in \mathbb{Z}^+$, el conjunto de los F_{p^n}-puntos racionales de torsión r, para $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subset \bar{\mathbb{F}}_p$, denotado por $E(\mathbb{F}_{p^n})[r]$, es entonces:

$$E(\mathbb{F}_{p^n})[r] = \{P \in E(\mathbb{F}_{p^n}) | rP = \mathcal{O}\}.$$

3.2.3. Grado de encajamiento

Definición 3.2 *(Grado de encajamiento). Para dos números primos p y r, dado un campo finito $\mathbb{F}_p$, considérese una curva elíptica $E/\mathbb{F}_p$ tal que $\#E(\mathbb{F}_p) = h \cdot r$, donde $h \in \mathbb{Z}^+$. Sea k un entero positivo, se dice que k es el* grado de encajamiento *de $E/\mathbb{F}_p$ con respecto a p y r, si k es el menor entero positivo tal que:*

$$r | p^k - 1.$$

Sea $\Phi_k(\cdot)$ el k-ésimo polinomio ciclotómico, por definición se cumple que $\Phi_k(p) | p^k - 1$ y por lo tanto $r | \Phi_k(p)$[1]. Dado que $p \equiv t - 1 \mod r$, donde t es la traza de E sobre $\mathbb{F}_p$, alternativamente el grado de encajamiento puede ser definido como el menor entero positivo k, tal que:

$$r | \Phi_k(t - 1).$$

3.2.4. Curva enlazada (*Twist*)

Definición 3.3 *(Invariante-j). Dada la curva elíptica $E : y^2 = x^3 + ax + b$, el invariante-j de E, está denotado por $j(E)$ y definido como*

$$j = -1728 \frac{(4a)^3}{\Delta},$$

[1] La definición del polinomio ciclotómico se puede encontrar en la Sección 2.5.

donde $\Delta = -16(4a^3 + 27b^2)$ *es el discrimintante de la curva. El invariante-j determina la clase de isomorfismo de* E.

Definición 3.4 *(Curva enlazada) Sean* E *y* E' *dos curvas elípticas, se dice que* E' *es la curva* enlazada *de* E*, si y sólo si* E *y* E' *tienen el mismo invariante-j y son isomórficas sobre la cerradura algebraica de un campo finito* $\mathbb{F}_p$.

En particular, dada la curva elíptica $E/\mathbb{F}_p$ con grado de encajamiento k, si el grupo finito $E(\mathbb{F}_p)$ tiene un subgrupo de orden primo r, Hess *et al.* [26] demostraron que existe una curva *enlazada* E' de E, definida sobre el campo $\mathbb{F}_{p^{k/d}}$, donde $d|k$, con $r|\#E'(\mathbb{F}_{p^{k/d}})$, tal que E y E' son isomórficas[2] sobre $\mathbb{F}_{p^k}$, es decir,

$$\phi : E'(\mathbb{F}_{p^{k/d}}) \rightarrow E(\mathbb{F}_{p^k}),$$

donde $d \in \mathbb{Z}^+$, se define como el grado de la curva enlazada E'.

3.2.5. Endomorfismo de Frobenius

Definición 3.5 *(Endomorfismo de Frobenius). Sea* $E/\mathbb{F}_p$ *una curva elíptica con grado de encajamiento* k *y sea* $E(\mathbb{F}_p)$ *el grupo de los* $\mathbb{F}_p$*-puntos racionales en* $E/\mathbb{F}_p$*, tal que* $E(\mathbb{F}_p)$ *tiene un subgrupo de orden primo* r*. El endomorfismo de Frobenius actúa sobre* $E(\mathbb{F}_{p^k})$ *de la siguiente manera:*

$$\pi : E(\mathbb{F}_{p^k}) \rightarrow E(\mathbb{F}_{p^k}),$$

tal que

$$\pi(X, Y) = (X^p, Y^p) \in E(\mathbb{F}_{p^k}).$$

Sea t la traza de E sobre $\mathbb{F}_p$, $\sigma(u) = u^2 - tu + p$ es el polinomio característico del endomorfismo de Frobenius, es decir, para todo punto $Q \in E(\mathbb{F}_{p^k})$ se satisface la igualdad

$$\pi^2(Q) - t\pi(Q) + pQ = \mathcal{O}. \tag{3.7}$$

Del mismo modo, si $\sigma(u)$ se factoriza modulo r, entonces

$$\sigma(u) = (u - 1)(u - p) \mod r.$$

Por lo tanto, existen dos conjuntos de puntos en $E(\mathbb{F}_{p^k})[r]$ definidos como $\{P \in E(\mathbb{F}_{p^k})[r] \mid \pi(P) = P\}$ y $\{Q \in E(\mathbb{F}_{p^k})[r] \mid \pi(Q) = pQ\}$, los cuales corresponden con el eigenespacio-1 y el eigenespacio-p de π actuando sobre $E(\mathbb{F}_{p^k})[r]$[3], respectivamente [7].

Formalmente, el grupo cíclico $E(\mathbb{F}_p)[r]$ es el eigenespacio-1 de π, ya que para todo punto $P = (x, y) \in E(\mathbb{F}_p)$ se cumple que $(x^p, y^p) = (x, y)$. Por otra parte, si la curva elíptica $E/\mathbb{F}_p$ tiene una curva *enlazada* $E'/\mathbb{F}_{p^{k/d}}$ de grado d, con $r|\#E'(\mathbb{F}_{p^{k/d}})$, tal que E y E' son isomórficas bajo $\phi : E'(\mathbb{F}_{p^{k/d}}) \rightarrow E(\mathbb{F}_{p^k})$, Barreto *et al.* [7] demostraron que el eigenespacio-p de π es el subgrupo de $E(\mathbb{F}_{p^k})[r]$, formado por el conjunto

$$\phi(E'(\mathbb{F}_{p^{k/d}})[r]) = \{\phi(Q') \mid Q' \in E'(\mathbb{F}_{p^{k/d}})[r]\}.$$

[2] Una definición general de isomorfismo se encuentra en la Sección 2.7.
[3] En la Sección 2.8 esta definido, de una manera general, el concepto de eigenespacio.

3.3. Introducción a los emparejamientos Bilineales

Sean $\mathbb{G}_1 = (\mathbb{G}_1, +, 0)$, $\mathbb{G}_2 = (\mathbb{G}_2, +, 0)$ y $\mathbb{G}_T = (\mathbb{G}_T, \cdot, 1)$ grupos cíclicos de orden primo $r \in \mathbb{Z}^+$, un emparejamiento bilineal está definido como la proyección:

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T.$$

con las siguientes características:

- **No degenerado**. Se dice que un emparejamiento es *no degenerado*, si para todo $a \in \mathbb{G}_1$ existe un elemento $c \in \mathbb{G}_2$, tal que $\hat{e}(a, c) \neq 1$ y $a, c \neq 0$.
- **Bilinealidad**. Dados los elementos $a, b \in \mathbb{G}_1$ y $c, d \in \mathbb{G}_2$, donde $a, b, c, d \neq 0$, esta propiedad implica que $\hat{e}(a + b, c) = e(a, c) \cdot \hat{e}(b, c)$ y del mismo modo, $\hat{e}(a, c + d) = \hat{e}(a, c) \cdot \hat{e}(a, d)$. Por lo tanto,
$$\hat{e}(a + a, c) = \hat{e}(a, c + c) = \hat{e}(a, c) \cdot \hat{e}(a, c)$$
y en general, para todo $m \in [1, r - 1]$ se cumple que
$$\hat{e}(ma, c) = \hat{e}(a, mc) = \hat{e}(a, c)^m.$$
- En la práctica se requiere que exista un algoritmo capaz de computar eficientemente $\hat{e}(a, c)$.

Considérese una curva elíptica ordinaria $E/\mathbb{F}_p$ con grado de encajamiento k y un grupo $E(\mathbb{F}_p)$ de orden $h \cdot r = p + 1 - t$, donde r es un número primo y $h \in \mathbb{Z}^+$. Dada la curva *enlazada* E' de grado d tal que $E'(\mathbb{F}_{p^{k/d}})$ tiene un subgrupo de orden r, supongamos que E y E' son isomórficas sobre el campo $\mathbb{F}_{p^k}$, es decir, $\phi : E'(\mathbb{F}_{p^{k/d}}) \to E(\mathbb{F}_{p^k})$.

Bajo estas condiciones, estamos interesados en emparejamientos bilineales sobre los grupos $\mathbb{G}_1$, $\mathbb{G}_2$ y $\mathbb{G}_T$, tales que:

- $\mathbb{G}_1$ es el eigenespacio-1 de π en $E(\mathbb{F}_{p^k})$, es decir, es el grupo cíclico escrito de manera aditiva, formado por los puntos de torsión r en la curva elíptica $E(\mathbb{F}_p)$.
- $\mathbb{G}_2$ es el eigenespacio-p de π en $E(\mathbb{F}_{p^k})$. Sea $Q' \in E'(\mathbb{F}_{p^{k/d}})[r]$, tal que $\mathbb{G}'_2 = \langle Q' \rangle$ y sea $Q = \phi(Q')$, entonces $\mathbb{G}_2$ es el grupo cíclico generado por el punto Q, es decir, $\mathbb{G}_2 = \langle Q \rangle$.
- $\mathbb{G}_T$ es un subgrupo de $\mathbb{F}^*_{p^k}$, escrito de manera multiplicativa, el cual está formado por el conjunto de las r-ésimas raíces primitivas de la unidad en el grupo cíclico $\mathbb{F}^*_{p^k}$ [Definición 2.11]. Al grupo $\mathbb{G}_T$ lo denotaremos como $\mathbb{F}^\times_{p^k}$.

3.4. Seguridad en los emparejamientos

Un criptosistema basado en emparejamientos es considerado seguro, si el problema del logaritmo discreto es computacionalmente inviable, tanto en el subgrupo $\mathbb{F}^\times_{p^k}$, como en el grupo formado por los puntos de torsión r en la curva elíptica E.

El mejor ataque conocido para solucionar el problema del logaritmo discreto en el grupo $E[r]$ es el algoritmo paralelizado de Pollard rho, cuya complejidad es $\mathcal{O}(\sqrt{r})$ [40, 42]. Por otra parte, sea $\mathbb{F}_{p^k}$ un campo finito de característica p con p^k elementos, el mejor ataque conocido en el grupo $\mathbb{F}^\times_{p^k}$ es el cálculo de índices, cuya complejidad es subexponencial con respecto a la cardinalidad del

campo, es decir, $\mathcal{O}(\exp(1{,}92 \cdot (\ln p^k)^{1/3} \cdot (\ln \ln p^k)^{2/3}))$ [1].

Por lo tanto la seguridad del emparejamiento se mide con respecto a $\log_2(r)$ y $\log_2(p^k)$. La relación entre ambos parámetros está definida por $k \cdot \rho$, donde $\rho = \log_2(p)/\log_2(r)$, y dada la complejidad de los ataques, se requiere que $\log_2(p^k)$ sea significativamente mayor a $\log_2(r)$. En la Tabla 3.1, Freeman *et al.* [20] proporcionan una aproximación del grado de encajamiento y del tamaño en bits de p y r, necesarios para obtener distintos niveles de seguridad.

Nivel de seguridad (bits)	**Longitud en bits del orden** r $\log_2(r)$	**Longitud en bits de** p^k $\log_2(p^k)$	**Grado de encajamiento** k $\rho \approx 1$	$\rho \approx 2$
80	160	960 - 1280	6 - 8	3 - 4
112	224	2200 - 3600	10 - 16	5 - 8
128	256	3000 - 5000	12 - 20	6 - 10
192	384	8000 - 10000	20 - 26	10 - 13
256	512	14000 - 18000	28 - 36	14 - 18

Tabla 3.1: Parámetros necesarios para obtener un nivel de seguridad deseado [20]

De acuerdo con la Tabla 3.1, las curvas elípticas requeridas en la implementación de protocolos basados en emparejamientos, deben poseer un subgrupo de orden primo r "grande" y grado de encajamiento k relativamente "pequeño". Si se satisfacen ambas condiciones, se dice que las curvas son "*amables*" con los emparejamientos.

3.5. Curvas *amables* con los emparejamientos

Freeman *et al.* en su artículo "A taxonomy of pairing-friendly curves" [20] dan una definición formal de las curvas *amables* con los emparejamientos.

Definición 3.6 *Sea E una curva elíptica ordinaria definida sobre el campo finito primo $\mathbb{F}_p$. Se dice que E es "amable con los emparejamientos" si las siguientes condiciones se satisfacen:*

- *Existe un número primo r tal que $r \geq \sqrt{p}$ y $r|\#E(\mathbb{F}_p)$.*
- *El grado de encajamiento k de la curva elíptica $E/\mathbb{F}_p$ con respecto a r es menor que* $\log_2(r)/8$.

Este tipo de curvas son construidas a través del método de multiplicación compleja [23]. En éste método se fija el grado de encajamiento k y posteriormente se computan los enteros p, r y t, los cuales deben satisfacer seis condiciones principales:

1. p debe ser un número primo.
2. r debe ser un número primo tal que $r \geq \sqrt{p}$.
3. t debe ser primo relativo con p.
4. r debe dividir a $p + 1 - t$.
5. k debe ser el menor entero positivo tal que $r|\Phi_k(t-1)$.

6. Para $D \in \mathbb{Z}^+$ y $f \in \mathbb{Z}$, se debe satisfacer la ecuación:

$$4p - t^2 = Df^2, \tag{3.8}$$

la cual es conocida por el nombre de *ecuación CM* y garantiza que $t \leq 2\sqrt{p}$, donde D es el *discriminante CM* [20].

Bajo estas condiciones se define una curva elíptica ordinaria E sobre el campo $\mathbb{F}_p$ con grado de encajamiento k y $\#E(\mathbb{F}_p) = p + 1 - t$, tal que $r|\#E(\mathbb{F}_p)$. Además la ecuación de la curva es determinada a partir del valor de D en la Ecuación (3.8), los casos más comunes son [10]:

- Si $D = 1$, la ecuación de la curva es $E : y^2 = x^3 + ax$.
- Si $D = 3$, la ecuación de la curva es $E : y^2 = x^3 + b$.

Por otra parte, si el grado de encajamiento k es un número par, la curva elíptica E será isomórfica a la curva *enlazada* E' de grado $d = 2$. No obstante, dependiendo del valor del discriminante CM, E' puede ser de grado $d > 2$.

Finalmente la curva *enlazada* E' se define sobre el campo $\mathbb{F}_{p^{k/d}}$ y dependiendo del valor de d, se puede determinar la ecuación de la curva e isomorfismo bajo el cual está definido, tal y como se muestra en la Tabla 3.2, donde $\xi \in \mathbb{F}_{p^{k/d}}$ no debe tener raíz cuadrada ni raíz cúbica en $\mathbb{F}_{p^{k/d}}$.

Discriminante D	**Grado de la curva *enlazada*** d	**Ecuación de la curva** $E'(\mathbb{F}_{p^{k/d}})$	**Isomorfismo sobre** $\mathbb{F}_{p^k}$ $\phi_d : E' \to E$
-	2	$E' : Y^2 = X^3 + a/\xi^2 X + b/\xi^3$	$(X, Y) \to (X, Y\xi^{1/2})$
3	3	$E' : Y^2 = X^3 + b/\xi$	$(X, Y) \to (X\xi^{1/3}, Y\xi^{1/2})$
1	4	$E' : Y^2 = X^3 + a/\xi X$	$(X, Y) \to (X\xi^{1/2}, Y\xi^{3/4})$
3	6	$E' : Y^2 = X^3 + b/\xi$	$(X, Y) \to (X\xi^{1/3}, Y\xi^{1/2})$

Tabla 3.2: Características de la curva *enlzada* E' [26]

3.5.1. Familias de Curvas Elípticas

Buniakowski y Schinzel [33] encontraron que la evaluación de un polinomio no constante $g(z)$, puede generar infinitos números primos si y sólo si $g(z)$ satisface las siguientes condiciones:

- El polinomio $g(z)$ debe ser irreducible.
- Sea $g(z)$ un polinomio de grado m, el coeficiente correspondiente al término z^m debe ser un entero positivo.
- $g(n) \in \mathbb{Z}$ para un número infinito de $n \in \mathbb{Z}$.
- Existen dos número enteros n_1 y n_2, tales que $\gcd(g(n_1), g(n_2)) = 1$.

A partir de estas características se definen los polinomios $p(z)$ y $r(z)$ que representan a los parámetros primos p y r respectivamente, dando lugar a que la traza t de $E/\mathbb{F}_p$, sea expresada como $t(z)$. De esta manera, las *"Familias de Curvas Elípticas"* son parametrizadas por la terna $(p(z), r(z), t(z))$ y construidas mediante las condiciones 3-6 del método descrito previamente.

Con base en la Ecuación (3.8), se dice que una familia de curvas elípticas es completa si existe un polinomio $f(z)$ tal que

$$4p(z) - t(z)^2 = Df(z)^2, \tag{3.9}$$

en caso contrario es llamada dispersa [20]. En particular, debido a sus características, las familias completas de curvas elípticas BN (Barreto-Naehrig), BW (Brezing-Weng), KSS (Kachisa-Schaefer-Scott) y BLS (Barreto-Lynn-Scott), han sido estudiadas y consideradas en la implementación eficiente de los emparejamientos bilineales con 192 bits de seguridad, lo cual está directamente relacionado con el grado de encajamiento y el tamaño en bits de $p = p(z_0)$ y $r = r(z_0)$, para $z \in \mathbb{Z}$.

Familia de Curvas Elípticas	k	$\rho = \frac{\log_2(p)}{\log_2(r)}$	$\log_2(r)$	$\log_2(p)$	$\log_2(p^k)$
BN	12	1.00	640	640	7680
BW	12	1.49	427	640	7680
KSS	18	1.33	384	512	9216
BLS	24	1.25	384	480	11520

Tabla 3.3: Familias de Curvas Elípticas para 192 bits de seguridad

Curvas BN

La familia BN [8] tiene grado de encajamiento $k = 12$ y define curvas elípticas de orden primo r, es decir, $\#E(\mathbb{F}_p) = r$. La característica del campo, el orden del grupo y la traza de Frobenius se encuentran parametrizados por:

$$\begin{aligned} p(z) &= 36z^4 + 36z^3 + 24z^2 + 6z + 1 \\ r(z) &= 36z^4 + 36z^3 + 18z^2 + 6z + 1 \\ t(z) &= 6z^2 + 1 \end{aligned}$$

La Ecuación (3.9) se cumple para $f(z) = 6z^2 + 4z + 1$ y $D = 3$; por lo tanto, dado $z_0 \in \mathbb{Z}$, si $p = p(z_0)$ y $r = r(z_0)$ son números primos, la ecuación de la curva es $E/\mathbb{F}_p : y^2 = x^3 + b$ y es isomórfica a la curva *enlazada* de grado $d = 6$, definida como $E'/\mathbb{F}_{p^2} : Y^2 = X^3 + b/\xi$, donde los elementos $b \in \mathbb{F}_p$ y $\xi \in \mathbb{F}_{p^2}$ no tienen residuos cuadráticos ni residuos cúbicos en $\mathbb{F}_p$ y $\mathbb{F}_{p^2}$, respectivamente.

Curvas BW-12

Las curvas BW [15] forman parte de las *familias ciclotómicas*, las cuales deben su nombre a que el parámetro $r(z)$ es el k-ésimo polinomio ciclotómico. Sea k el grado de encajamiento, dependiendo del valor de i en la congruencia $k \equiv i \mod 6$, se pueden proponer distintas familias de curvas elípticas.

En el caso particular en que $k = 12$, donde $k \equiv 0 \mod 6$, la terna $(p(z),\ r(z),\ t(z))$ así como el polinomio $f(z)$, están definidos por las siguientes igualdades:

$$\begin{aligned} p(z) &= \frac{1}{3}(z-1)^2(z^4 - z^2 + 1) + z \\ r(z) &= \Phi_{12}(z) = z^4 - z^2 + 1 \\ t(z) &= z + 1 \\ f(z) &= \frac{1}{3}(z-1)(2z^2 - 1) \end{aligned}$$

Al igual que la familia BN, las curvas BW son de la forma $E/\mathbb{F}_p : y^2 = x^3 + b$ y son isomórficas a la curva *enlazada* $E'/\mathbb{F}_{p^2}$ de grado 6, es decir, $E'(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^{12}})$.

Curvas KSS-18

Kachisa *et al* [30] propusieron familias de curvas elípticas con grado de encajamiento $k = 8$, 16, 18, 32, 36 y 40, de las cuales, aquella con $k = 18$ es adecuada para matener la seguridad de 192 bits balanceada en ambos lados del emparejamiento.

$$\begin{aligned} p(z) &= \frac{1}{21}(z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 + 343z^2 + 1763z + 2401) \\ r(z) &= \frac{1}{343}(z^6 + 37z^3 + 343) \\ t(z) &= \frac{1}{7}(z^4 + 16z + 7) \\ f(z) &= \frac{1}{21}(5z^4 + 14z^3 + 94z + 259) \end{aligned}$$

En las curvas KSS-18 el discriminante CM es $D = 3$, pero a diferencia de las familias BN y BW-12, la curva E' *enlazada* a E está definida sobre el campo $\mathbb{F}_{p^3}$.

Curvas BLS-24

La *familia ciclotómica* BLS [6] está parametrizada por:

$$\begin{aligned} p(z) &= \frac{1}{3}(z-1)^2(z^8 - z^4 + 1) + z \\ r(z) &= \Phi_{24}(z) = z^8 - z^4 + 1 \\ t(z) &= z + 1 \\ f(z) &= (z-1)(2z^4 - 1)/3 \end{aligned}$$

y fue considerada por su alto grado de encajamiento. La principal desventaja de las curvas BLS-24 es que E' se define sobre el campo $\mathbb{F}_{p^4}$, lo cual implica que la aritmética en la curva *enlazada* E', sea más compleja en comparación con la aritmética asociada a las familias de curvas elípticas descritas previamente.

Capítulo 4

Emparejamientos Bilineales

Nunca percibimos lo que está hecho,
sólo vemos lo que queda por hacer

Marie Curie

A partir de los conceptos definidos previamente, la primera sección de este capítulo tiene el objetivo de mostrar a los emparejamientos bilineales desde una perspectiva matemática. Posteriormente se define el algoritmo con el cual son computados eficientemente y se describen dos de las principales aportaciones realizadas a los problemas de *"Exponenciación final"* y *"Función picadillo hacia el grupo* $\mathbb{G}_2$*"*, en emparejamientos bilineales.

A continuación se proporciona la notación que será utilizada a lo largo del capítulo.

Notación:

- $\mathbb{G}_1$, $\mathbb{G}_2$ y $\mathbb{G}_T$ son los grupos finitos de orden primo r involucrados en la definición de los emparejamientos bilineales. $\mathbb{G}_1$ y $\mathbb{G}_2$ están escritos de manera aditiva, mientras que $\mathbb{G}_2$ está escrito de manera multiplicativa [Sección 3.3].
- $q = p^n$, donde p es un número primo y $n \in \mathbb{Z}^+$.
- $\mathbb{F}_p$ es un campo finito de característica p [Sección 2.3].
- $\bar{\mathbb{F}}_p$ es la cerradura algebráica del campo $\mathbb{F}_p$ [Definición 2.8].
- $\mathbb{F}_q$ es una extensión del campo $\mathbb{F}_p$, tal que $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \bar{\mathbb{F}}_p$.
- $E/\mathbb{F}_p : y^2 = x^3 + ax + b$, es una curva elíptica definida por la ecuación simplificada de Weierstrass, donde $a, b \in \mathbb{F}_p$ [Sección 3.1].
- $E(\bar{\mathbb{F}}_p)$ es el conjunto de puntos en la curva elíptica $E/\mathbb{F}_p$ [Sección 3.1.1].
- $E(\mathbb{F}_q)$ es el grupo abeliano escrito de manera aditiva, formado por el conjunto finito de los $\mathbb{F}_q$-puntos racionales de la curva elíptica $E/\mathbb{F}_q$.
- El grupo finito $E(\mathbb{F}_p)$ tiene orden $h \cdot r = p + 1 - t$ para algún entero positivo h, donde r denota un número primo y t denota la traza de E sobre $\mathbb{F}_p$ [Sección 3.2.1].

- k es el grado de encajamiento de $E/\mathbb{F}_p$ [Definición 3.2].
- $E'/\mathbb{F}_{p^{k/d}}$ es la *curva enlazada* a $E/\mathbb{F}_p$ de grado d. El grupo $E'(\mathbb{F}_{p^{k/d}})$ es isomórfico a $E(\mathbb{F}_{p^k})$ bajo $\phi : E' \to E$ [Definición 3.4].
- $\mathbb{G}_{\Phi_k(\cdot)}$ es el k-ésimo grupo ciclotómico [Definición 2.13].
- π denota el endomorfismo de Frobenius [Definición 3.5].
- $(p(z), r(z), t(z))$ es una familia de curvas elípticas, donde $p = p(z_0)$, $r = r(z_0)$ y $t = t(z_0)$ para algún número entero z_0.

4.1. Funciones racionales de la curva elíptica

Dada una curva elíptica E definida sobre un campo finito $\mathbb{F}_q$, donde $q = p^n$ y $n \in \mathbb{Z}^+$, sea $\bar{\mathbb{F}}_q$ la cerradura algebraica de $\mathbb{F}_q$, se dice que $f(x, y)$ es una función racional en $E/\mathbb{F}_q$, si existe un punto $P = (x_P, y_P) \in E(\bar{\mathbb{F}}_q)$, tal que $f(x_P, y_P) \neq \infty$. El conjunto de funciones racionales en $E/\mathbb{F}_q$ está denotado por $\bar{\mathbb{F}}_q(E)$ y para todo $f \in \bar{\mathbb{F}}_q(E)$ se cumple que $f(P)$ es un elemento en el conjunto $\{\bar{\mathbb{F}}_q \cup \infty\}$ [50].

Sean P y Q puntos en la curva elíptica $E/\mathbb{F}$, una función racional $f \in \bar{\mathbb{F}}_q(E)$ tiene un **cero** en P y un **polo** en Q, si y sólo si $f(P) = 0$ y $f(Q) = \infty$, respectivamente. En general, la evaluación de f en un punto P puede ser representada a partir de la siguiente igualdad:

$$f(P) = (u(P))^m \cdot g(P)$$

donde $m \in \mathbb{Z}$, $u(P) = 0$ y $g(P) \neq 0, \infty$. Por lo que si $m > 0$ entonces f tiene un cero en P y si $m < 0$ entonces f tiene un polo en P. Cabe mencionar que $u(P)$ es llamada la función *"uniformadora"* y el número entero m es el **orden** de f en P, denotado como:

$$\mathrm{ord}_P(f) = m.$$

4.2. Divisores

Sea $E/\mathbb{F}_q$ una curva elíptica, a cada punto $P \in E(\bar{\mathbb{F}}_q)$ se le asigna el símbolo formal $[P]$. Un divisor $\mathcal{D}$ sobre $E/\mathbb{F}_q$, es una combinación lineal finita de dichos símbolos con coeficientes en $\mathbb{Z}$ [50].

$$\mathcal{D} = \sum_j a_j [P_j], \qquad a_j \in \mathbb{Z}.$$

Las operadores que definen a un divisor son:

- El grado.
$$\deg\left(\sum_j a_j [P_j]\right) = \sum_j a_j \in \mathbb{Z}$$
- La suma.
$$\mathrm{sum}\left(\sum_j a_j [P_j]\right) = \sum_j a_j P_j \in E$$

- El soporte.

$$\text{supp}\left(\sum_j a_j[P_j]\right) = \{P_j \in E | a_j \neq 0\}$$

4.2.1. Divisores principales

Un divisor $\mathcal{D}$ sobre la curva elíptica $E/\mathbb{F}_q$ con $\deg(\mathcal{D}) = 0$ y $\text{sum}(\mathcal{D}) = \mathcal{O}$, es llamado **"principal"** si existe una función racional $f \in \bar{\mathbb{F}}_q(E)$, tal que $\mathcal{D} = \text{div}(f)$, donde

$$\text{div}(f) = \sum_{P_j \in E} \text{ord}_{P_j}(f)[P_j].$$

Ejemplos de divisores principales son los correspondientes a las funciones racionales $\ell_{P,P}$ y $\ell_{P,Q}$ [1], las cuales denotan a la recta tangente a E en el punto P y a la recta secante a E en los puntos P y Q, respectivamente.

$$\text{div}(\ell_{P,P}) = 2[P] + [-2P] - 3[\mathcal{O}]$$
$$\text{div}(\ell_{P,Q}) = [P] + [Q] + [-(P+Q)] - 3[\mathcal{O}]$$

En general, dadas las funciones f y $g \in \bar{\mathbb{F}}_q(E)$, los divisores principales cumplen con las siguientes propiedades:

- $\text{div}(f \cdot g) = \text{div}(f) + \text{div}(g)$.
- $\text{div}(f/g) = \text{div}(f) - \text{div}(g)$.
- La función f es una constante, si y sólo si $\text{div}(f) = 0$.

Una función racional f puede ser evaluada en un divisor $\mathcal{D} = \sum_j a_j[P_j]$, a través de la siguiente fórmula:

$$f(\mathcal{D}) = \prod_{P_j \in supp(\mathcal{D})} f(P_j)^{a_j},$$

de tal manera que, para todo $n \in \mathbb{Z}$,

$$f(\mathcal{D})^n = f(n\mathcal{D}), \tag{4.1}$$

donde $n\mathcal{D} = \sum_j n \cdot a_j[P_j]$. A continuación se mencionan tres conceptos que serán de utilidad en la definición de emparejamientos bilineales:

Definición 4.1 *(Reciprocidad de Weil) [37]. Sea $E/\mathbb{F}_q$ una curva elíptica y sean $f, g \neq 0$ funciones racionales en $\bar{\mathbb{F}}_q(E)$ con soportes disjuntos, entonces:*

$$f(div(g)) = g(div(f))$$

Definición 4.2 *(Relación de equivalencia). Dos divisores $\mathcal{D}_1$ y $\mathcal{D}_2$ son linealmente equivalentes, $\mathcal{D}_1 \sim \mathcal{D}_2$, si y sólo si $\mathcal{D}_1 - \mathcal{D}_2$ es un divisor principal, es decir,*

$$\mathcal{D}_1 - \mathcal{D}_2 = div(f), \quad o\ bien \quad \mathcal{D}_1 = \mathcal{D}_2 + div(f)$$

Definición 4.3 *(Función de Miller) [37]. Una función de Miller de longitud $s \in \mathbb{Z}$ denotada por $f_{s,R}$, es una función racional en $\bar{\mathbb{F}}_q(E)$ con divisor $div(f_{s,R}) = s[R] - [sR] - (s-1)[\mathcal{O}]$.*

[1] En la Sección 3.1.2. se puede encontrar la definición de las rectas $\ell_{P,P}$ y $\ell_{P,Q}$, así como sus ecuaciones.

Lema 4.1 *Sea $f_{s,R}$ una función de Miller y sea v_R la línea vertical que corta a la curva elíptica E en el punto R, para todo $a, b \in \mathbb{Z}$ se cumple que:*

(I) $f_{a+b,R} = f_{a,R} \cdot f_{b,R} \cdot \ell_{aR,bR}/v_{(a+b)R}$

(II) $f_{ab,R} = f_{b,R}^{a} \cdot f_{a,bR}$

(III) $f_{1,R} = c$, *donde c es una constante, por ejemplo $c = 1$.*

4.3. Emparejamiento de Weil

Definición 4.4 *(Emparejamiento de Weil) [37]. Sea $r > 1$ un número entero y sean $\mathcal{D}_1$ y $\mathcal{D}_2$ divisores en una curva elíptica E con soportes disjuntos, es decir,*

$$supp(\mathcal{D}_1) \cap supp(\mathcal{D}_2) = \emptyset,$$

existen dos funciones racionales f_1 y f_2 en E, tales que $div(f_1) = r\mathcal{D}_1$ y $div(f_2) = r\mathcal{D}_2$. El emparejamiento de Weil definido como

$$e_W(\mathcal{D}_1, \mathcal{D}_2) = \frac{f_1(\mathcal{D}_2)}{f_2(\mathcal{D}_1)},$$

es un emparejamiento bilineal no degenerado.

Específicamente, dados los puntos $P \in \mathbb{G}_1$ y $Q \in \mathbb{G}_2$, f_1 y f_2 son funciones racionales en $\mathbb{F}_{p^k}(E)$ con divisores $\mathrm{div}(f_1) = r[P] - r[\mathcal{O}]$ y $\mathrm{div}(f_2) = r[Q] - r[\mathcal{O}]$, respectivamente, tal que $\mathcal{D}_1 \sim [P] - [\mathcal{O}]$ y $\mathcal{D}_2 \sim [Q] - [\mathcal{O}]$. Por lo tanto, el cálculo de $f_i(\mathcal{D}_j)$ toma valores en el grupo multiplicativo $\mathbb{F}_{p^k}^*$ y además, a través de la reciprocidad de Weil, se cumple que

$$\left(\frac{f_1(\mathcal{D}_2)}{f_2(\mathcal{D}_1)}\right)^r = \frac{f_1(r\mathcal{D}_2)}{f_2(r\mathcal{D}_1)} = \frac{f_1(\mathrm{div}(f_2))}{f_2(\mathrm{div}(f_1))} = 1,$$

es decir, $g = e_W(\mathcal{D}_1, \mathcal{D}_2)$ es un elemento en el subgrupo de las r-ésimas raíces primitivas de la unidad en $\mathbb{F}_{p^k}^*$.

En los últimos años se han hecho distintas mejoras a los emparejamientos bilineales, por un lado se ha demostrado que el cálculo de $f_1(\mathcal{D}_2)$ puede ser reemplazado por $f_1(Q)$ y del mismo modo $f_2(\mathcal{D}_1)$ es sustituido por $f_2(P)$. Por otro lado, si P y Q son puntos de torsión r, entonces

$$\mathrm{div}(f_1) = r[P] - r[\mathcal{O}] = r[P] - [rP] - (r-1)[\mathcal{O}]$$

y

$$\mathrm{div}(f_2) = r[Q] - r[\mathcal{O}] = r[Q] - [rQ] - (r-1)[\mathcal{O}]$$

es decir, f_1 y f_2 se pueden expresar como las funciones de Miller $f_{r,P}$ y $f_{r,Q}$. Finalmente,

$$\begin{aligned} e_W : \mathbb{G}_1 \times \mathbb{G}_2 &\to \mathbb{G}_T, \\ (Q, P) &\mapsto \frac{f_{r,P}(Q)}{f_{r,Q}(P)} \end{aligned} \tag{4.2}$$

4.4. Emparejamiento de Tate

Definición 4.5 *(Emparejamiento de Tate) [7]. Dados los puntos $P \in \mathbb{G}_1$ y $Q \in \mathbb{G}_2$, consideremos al divisor $\mathcal{D}_Q \sim [Q] - [\mathcal{O}]$ y a la función de Miller $f_{r,P}$. El emparejamiento de Tate no degenerado y bilineal está definido como:*

$$\hat{t} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T,$$
$$(P, Q) \mapsto f_{r,P}(Q)^{(p^k-1)/r} \tag{4.3}$$

Sea $g = f_{r,P}(Q)$ un elemento en el grupo multiplicativo $\mathbb{F}^*_{p^k}$, a diferencia del emparejamiento de Weil, $\hat{t}(P, Q)$ requiere del cómputo de una exponenciación final, tal que

$$(g^{(p^k-1/r)})^r = 1$$

es decir, $g = \hat{t}(P, Q)$ es un elemento en el subgrupo de las r-ésimas raíces primitivas de la unidad en $\mathbb{F}^*_{p^k}$.

4.4.1. Emparejamiento ate

Dada una curva elíptica $E/\mathbb{F}_p$ con grado de encajamiento k, sea $E(\mathbb{F}_p)$ el grupo de los $\mathbb{F}_p$-puntos racionales de $E/\mathbb{F}_q$, con orden $\#E(\mathbb{F}_q) = h \cdot r = p + 1 - t$, donde t la traza de E sobre $\mathbb{F}_p$. Dados dos puntos $P \in E(\mathbb{F}_p)[r]$ y $Q \in E'(\mathbb{F}_{p^{k/d}})[r]$, el emparejamiento *ate* [26] está definido como

$$\hat{a}(Q, P) = f_{t-1,Q}(P)^{(p^k-1)/r}, \tag{4.4}$$

se deriva del emparejamiento de Tate de la siguiente manera [49]: para todo $m \in \mathbb{Z}^+$ tal que $r \nmid m$, se cumple que

$$\hat{t}(Q, P)^m = f_{r,Q}(P)^{m\cdot(p^k-1)/r} \in \mathbb{F}^*_{p^k}$$

es un emparejamiento bilineal no degenerado. Utilizando el Lema 4.1(II) y dado que $rQ = \mathcal{O}$,

$$f^m_{r,Q}(P) = f_{mr,Q}(P). \tag{4.5}$$

Por definición, en las familias de curvas elípticas $r|(p^k - 1)$ [Definición 3.2]; por lo tanto, si λ es un entero positivo tal que $\lambda \equiv p \mod r$, entonces $\lambda^k - 1 \equiv p^k - 1 \mod r$ y como consecuencia $\lambda^k - 1$ es un múltiplo de r. Con base en esta observación, sustituimos $mr = \lambda^k - 1$ en la Ecuación (4.5) y obtenemos que

$$f_{mr,Q}(P) = f_{\lambda^k-1,Q}(P) = f_{\lambda^k,Q}(P),$$

Considerando que para todo punto $Q \in E'[r]$ se satisface que $\lambda^i Q = p^i Q$ y utilizando repetidamente el Lema 4.1(II), $f_{\lambda^k,Q}(P)$ es expresado como se muestra a continuación:

$$f_{\lambda^k,Q}(P) = \prod_{i=0}^{k-1} f_{\lambda,Q}(P)^{\lambda^{k-1-i}p^i} = f_{\lambda,Q}(P)^{\sum_{i=0}^{k-1}\lambda^{k-1-i}p^i}$$

Finalmente λ es sustituida por $t - 1$ ya que, por el teorema de Hasse, $t - 1 \equiv p \mod r$, es decir,

$$\hat{t}(Q, P)^m = f_{t-1,Q}(P)^{c\cdot(p^k-1)/r}$$

donde $c = \sum_{i=0}^{k-1} \lambda^{k-1-i}p^i$ y $r \nmid c$. Dado que $\hat{t}(Q, P)$ está bien definido, $f_{t-1,Q}(P)^{(p^k-1)/r}$ (Ecuación (4.4)) es un emparejamiento bilineal no degenerado [49].

4.5. Emparejamientos óptimos

Sea $f_{s,R}$ la función de Miller de longitud $s \in \mathbb{Z}$, los emparejamientos bilineales definidos bajo la metodología de Weil y Tate, son de la forma

$$\frac{f_{s,P}(Q)}{f_{s,Q}(P)}$$

y

$$f_{s,P}(Q)^{\frac{p^k-1}{r}}$$

respectivamente. La función de Miller $f_{s,R}$ es calculada mediante el algoritmo de Miller, el cual será descrito en la Sección 4.6; en general este algoritmo requiere de $\log_2(s)$ iteraciones para ser computado. De acuerdo con Vercauteren [49], un emparejamiento bilineal es considerado *"óptimo"* si puede ser computado con $\log_2(r)/\varphi(k) + \varepsilon(k)$ iteraciones del algoritmo de Miller, donde $\varepsilon(k) \leq \log_2(k)$.

Basados en la Ecuación (4.5), en los últimos años diversos investigadores se han apoyado en el uso de *rejillas*[2] para encontrar múltiplos de r, tales que $f_{mr,R}$ defina un emparejamiento *"óptimo"*.

4.5.1. Emparejamiento óptimo ate

Definición 4.6 *(Función Extendida de Miller). Dado un número entero $s \in \mathbb{Z}$, existe un polinomio $h(x) = \sum_{i=0}^{n} h_i x^i$, tal que $h(s) \equiv 0 \mod r$, para un número entero n. Sea $f_{r,R}$ la función de Miller de longitud r y sea $m = h(s)/r$ con $r \nmid m$, para todo punto $R \in E[r]$ se satisface la siguiente igualdad:*

$$f_{r,R}^m = f_{mr,R} = f_{\sum_{i=0}^{n} h_i s^i, R}.$$

Aplicando repetidamente el Lemma 4.1(1) obtenemos que:

$$f_{r,R}^m = \prod_{i=1}^{n} f_{s^i,R}^{h_i} \cdot \left(\prod_{i=0}^{n} f_{h_i, s^i R} \cdot \prod_{i=0}^{n-1} \frac{\ell_{c_{i+1}R, h_i s^i R}}{v_{c_i R}} \right), \tag{4.6}$$

donde $c_i = \sum_{j=i}^{n} h_j s^j$. La expresión entre paréntesis es llamada **"función extendida de Miller"**, *la cual está denotada como $\mathbf{f_{s,h,R}}$ y es una función racional de la curva elíptica E con divisor $div(f_{s,h,R}) = \sum_{i=0}^{n} h_i([s^i R] - [\mathcal{O}])$.*

A partir de esta definición, Vercauteren demostró en [49] que si el polinomio $h(x)$ es evaluado en p y $h(p) \equiv 0 \mod r$, entonces la proyección:

$$\begin{aligned} a_{opt} : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mathbb{G}_T, \\ (Q, P) &\mapsto (f_{p,h,Q}(P))^{(p^k-1)/r} \end{aligned} \tag{4.7}$$

define un emparejamiento bilineal no degenerado.

Con base en la Ecuación (4.6), para que a_{opt} sea *"óptimo"* se requiere que el polinomio $h(p)$ tenga coeficientes h_i, tales que

$$\log_2(h_i) \approx \log_2(r)/\varphi(k).$$

[2] En la Sección 2.6. se encuentra una explicación general del algoritmo *LLL*.

El método a partir del cual se obtiene $h(p)$ es el siguiente: se construye la matriz M cuyas filas representan a los polinomios $h'_i(p) = a^i - p^i$ que cumplen con la congruencia $h'_i(p) \equiv 0 \mod r$, como se muestra a continuación:

$$M = \begin{array}{c} \begin{matrix} p^0 & p^1 & p^2 & \cdots & p^{\varphi(k)-1} \end{matrix} \\ \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -p & 1 & 0 & \cdots & 0 \\ -p^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ -p^{\varphi(k)-1} & 0 & 0 & \cdots & 1 \end{pmatrix} \end{array} \dashrightarrow \begin{array}{ccc} r & \equiv 0 & \mod r \\ -p+p & \equiv 0 & \mod r \\ -p^2+p^2 & \equiv 0 & \mod r \\ \vdots & \vdots & \vdots \\ -p^{\varphi(k)-1}+p^{\varphi(k)-1} & \equiv 0 & \mod r \end{array}$$

De esta manera, cualquier combinación lineal de las filas de M corresponde a un polinomio $h'(p)$ que es múltiplo de r. Además, si las filas son representadas como vectores $v_0, v_1, \ldots, v_{\varphi(k)-1}$ linealmente independientes que forman la base de una *rejilla* L, a partir del algoritmo $LLL(M)$ se obtienen los vectores $w_i \in L$ con norma euclideana mínima y los cuales están asociados a un polinomio

$$h'_{w_i}(p) = w_{i,0} + w_{i,1}p + w_{i,2}p^2 + \cdots + w_{\varphi(k)-1}p^{\varphi(k)-1}$$

tal que $h'_{w_i}(p) \equiv 0 \mod r$, donde $0 \leq i < \varphi(k)$.

Sea w_0 el vector con menor norma euclidiana en la *rejilla* L, por el teorema de Minkowski [38] se satisface que $\max_j |w_{0,j}| \leq r^{1/\varphi(k)}$. Es decir, el polinomio $h'_{w_0}(p)$ tiene coeficientes $w_{0,j}$ tales que:

$$\log_2(w_{0,j}) \leq \log_2(r)/\varphi(k).$$

Por lo tanto si $h(p) = h'_{w_0}(p)$, entonces a_{opt} es un emparejamiento *"óptimo"* ate. En las siguientes secciones se muestran los resultados obtenidos de aplicar este método, sobre las familias de curvas elípticas estudiadas durante la tesis, las cuales están parametrizadas por la terna $(p(z), r(z), t(z))$.

Curvas BN

En la familia Barreto-Naherig, $h(p) = (6z+2) + p - p^2 + p^3$ es el polinomio característico del emparejamiento óptimo ate, el cual está definido como:

$$a_{BN}(Q,P) = (f_{6z+2,Q}(P) \cdot \ell_{[6z+2]Q,pQ}(P) \cdot \ell_{[6z+2+p]Q,-p^2Q}(P))^{(p^{12}-1)/r} \tag{4.8}$$

Curvas KSS-18

En la familia de curvas KSS con grado de encajamiento $k = 18$, el vector con menor norma euclideana en la *rejilla* L, es $[z, 3, 0, 1, 0, 0]$, el cual está asociado al polinomio $h(p) = z + 3p + p^3$.

$$a_{KSS}(Q,P) = (f_{z,Q}(P) \cdot f^p_{3,Q}(P) \cdot \ell_{zQ,3pQ}(P))^{(p^{18}-1)/r} \tag{4.9}$$

Curvas BW-12 y BLS-24

Las familias de curvas ciclotómicas con grado de encajamiento $k \equiv 0 \mod 6$, tienen la particularidad de que la traza de Frobenius está parametrizada por $t(x) = x + 1$. Con base en la definición de Vercauteren, el emparejamiento ate sobre curvas BW-12 y BLS-24 es "optimo".

$$a_{BW}(Q, P) = (f_{z,Q}(P))^{(p^{12}-1)/r} \tag{4.10}$$

$$a_{BLS}(Q, P) = (f_{z,Q}(P))^{(p^{24}-1)/r} \tag{4.11}$$

4.5.2. Emparejamiento óptimo de Weil

Siguiendo la misma metodología de Vercauteren, Hess en su artículo *"Pairing Lattices"* [27] define distintas variantes del emparejamiento de Weil. Sin embargo, en esta tesis nos enfocamos en la siguiente observación: si $f_{s,h,R}$ es un **emparejamiento óptimo ate** sin la exponenciación final, entonces para $e = k/d$, la proyección

$$\begin{aligned} w_{opt} : \mathbb{G}_1 \times \mathbb{G}_2 &\to \mathbb{G}_T, \\ (P, Q) &\mapsto \prod_{i=0}^{e-1} \left(\frac{f_{s,h,p^i P}(Q)}{f_{s,h,Q}(p^i P)} \right)^{p^{e-1-i}} \end{aligned} \tag{4.12}$$

es un **emparejamiento óptimo de Weil** no degenerado.

4.6. Ciclo de Miller

Sea $E(\bar{\mathbb{F}}_p)$ el conjunto de puntos en la curva elíptica $E/\mathbb{F}_p$, dados dos puntos $T, R \in E/\mathbb{F}_p$, para el cálculo de la función de Miller $f_{s,T}(R)$ no es necesario construir a $f_{s,T}$ explícitamente como una función racional en x e y, basta con evaluarla en los puntos del soporte de $D_R \sim [R] - [\mathcal{O}]$. Sea $n = \log_2(s)$, si el parámetro s es expresado en base binaria, $s = \sum_{i=0}^{n} s_i 2^i$, por regla de Horner se cumple que:

$$s = s_0 + 2(s_1 + 2(s_2 + \cdots + 2(s_{n-2} + 2(s_{n-1} + 2(s_n))))),$$

es decir, el número entero s se puede expresar a partir de los valores temporales c_i, como se muestra a continuación:

$$\begin{aligned} & c_n &&= && s_n \\ & c_{n-1} &&= && s_{n-1} + 2(c_n) \\ & c_{n-2} &&= && s_{n-2} + 2(c_{n-1}) \\ & c_{n-3} &&= && s_{n-3} + 2(c_{n-2}) \\ & \vdots && && \vdots \\ & c_1 &&= && s_1 + 2(c_2) \\ s = \quad & c_0 &&= && s_0 + 2(c_1), \end{aligned}$$

de tal manera que $f_{s,T}(R) = f_{s_0+2(c_1),T}(R)$.

Por lo tanto, sea $f_{c_n,T}(R) = f_{1,T}(R) = 1$, la función de Miller $f_{s,T}(R)$ es calculada aplicando repetidamente el Lema 4.1, como se muestra a continuación:

$$f_{s_i+2c_{(i+1)},P} = \left\{ \begin{array}{lll} f_{c_{i+1},P}^2 \cdot \frac{\ell_{(c_{i+1})P,(c_{i+1})P}}{v_{2(c_{i+1})P}} & \text{si} & s_i = 0 \\ f_{c_{i+1},P}^2 \cdot \frac{\ell_{(c_{i+1})P,(c_{i+1})P}}{v_{2(c_{i+1})P}} \cdot \frac{\ell_{2(c_{i+1})P,P}}{v_{c_iP}} & \text{si} & s_i = 1 \end{array} \right\}. \tag{4.13}$$

Además, Barreto *et al.* [7, Teorema 2] demostraron que las líneas verticales $v_{2(c_{i+1})P}$ y v_{c_iP}, pueden ser excluidas de la igualdad (4.13), dando como resultado el Algoritmo 4.1, el cual requiere de las variables temporales $\tilde{T} \in E(\bar{\mathbb{F}}_p)$ y $f \in \mathbb{F}_{p^k}^*$. Cabe mencionar que dependiendo del emparejamiento que se este computando, el cálculo de $f_{s,T}(R)$ se puede realizar a partir del Algoritmo 4.1 para $T \in \mathbb{G}_1$ y $R \in \mathbb{G}_2$, o bien, para $T \in \mathbb{G}_2$ y $R \in \mathbb{G}_1$.

Algoritmo 4.1 Algoritmo de Miller para curvas elípticas

Entrada: $s \in \mathbb{Z}$ y $T, R \in E(\bar{\mathbb{F}}_p)$, tal que $T \neq R$
Salida: $f_{s,T}(R)$.

1: $s = \sum_{i=0}^{n} s_i 2^i$, donde $s_i \in \{0,1\}$ y $s_n = 1$;
2: $\tilde{T} \leftarrow T$, $f \leftarrow 1$;
3: **for** $i = n-1$ down to 0 **do**
4: $\quad f \leftarrow f^2 \cdot \ell_{\tilde{T},\tilde{T}}(R)$; $\tilde{T} \leftarrow 2\tilde{T}$;
5: $\quad$ **if** $s_i = 1$ **then**
6: $\quad\quad f \leftarrow f \cdot \ell_{\tilde{T},T}(R)$; $\tilde{T} \leftarrow \tilde{T} + T$;
7: $\quad$ **end if**
8: **end for**
9: **return** f;

A las sentencias que van de los puntos 3 al 8 en el Algoritmo 4.1, se les conoce con el nombre de *ciclo de Miller* y en los últimos años diversos investigadores se han enfocado en paralelizarlo y optimizarlo, haciendo más eficiente la aritmética de curvas elípticas y reduciendo el tamaño de s, como es el caso de los emparejamientos óptimos.

4.6.1. Aritmética en el ciclo de Miller

Aritmética de curvas elípticas

La aritmética de curvas elípticas en el ciclo de Miller, es implementada eficientemente utilizando coordenadas proyectivas [Sección 3.1.3]. Las familias de curvas elípticas en la Tabla 3.3 están definidas bajo la ecuación $E : y^2 = x^3 + b$ cuya forma proyectiva es $Y^2Z = X^3 + bZ^3$. Dependiendo del emparejamiento, la aritmética de curvas elípticas se puede realizar en $E/\mathbb{F}_p$, o bien, en la curva enlazada $E'/\mathbb{F}_{p^{k/d}}$, definida por la ecuación en su forma proyectiva $E' : Y^2Z = X^3 + b'Z^3$, donde $b' \in \mathbb{F}_{p^{k/d}}$.

Sea $\tilde{T} = (X_1, Y_1, Z_1)$ un punto en el conjunto $E(\bar{\mathbb{F}}_p)[r]$, por definición el cálculo de $2\tilde{T} = (X_3, Y_3, Z_3)$ requiere del cómputo de la recta tangente a $E/\mathbb{F}_p$ en el punto $\tilde{T}$, denotada por $\ell_{\tilde{T},\tilde{T}}$ [Sección 3.1.2].

Por lo tanto sea $R = (x_R, y_R)$ un punto en $E(\bar{\mathbb{F}}_p)[r]$, el cálculo de $\ell_{\tilde{T},\tilde{T}}(R)$ y $2\tilde{T}$ (línea 4 del Algoritmo 4.1) se puede realizar de manera simultánea a partir del Algoritmo 4.2, donde:

$$\ell_{T,T}(R) = 3X_1^2 x_R - 2Y_1 Z_1 y_R + 3bZ_1^2 - Y_1^2 \in \mathbb{F}_{p^k}^*$$

$$X_3 = \tfrac{X_1 Y_1}{2}(Y_1^2 - 9bZ_1^2) \qquad Y_3 = \left[\tfrac{1}{2}(Y_1^2 + 9bZ_1^2)\right] - 27b^2 Z_1^4 \qquad Z_3 = 2Y_1^3 Z_1$$

Del mismo modo, dado el punto $T = (X_2, Y_2, Z_2)$, el Algoritmo 4.3 calcula la recta secante a los puntos $\tilde{T}$ y T en la curva elíptica $E/\mathbb{F}_p$ y la suma de $\tilde{T}+T = (X_3, Y_3, Z_3)$ (línea 6 del Algoritmo 4.1), tales que

$$\ell_{\tilde{T},T}(R) = \lambda y_R - \alpha x_R + (\alpha X_2 - \lambda Y_2)$$

$$X_3 = \lambda(\lambda^2 + Z_1\alpha^2 - 2X_1\lambda^2) \qquad Y_3 = \alpha(3X_1\lambda^2 - \lambda^3 - Z_1\alpha^2) - Y_1\lambda^3 \qquad Z_3 = Z_1\lambda^3,$$

donde $\alpha = Y_1 - Y_2 Z_1$ y $\lambda = X_1 - X_2 Z_1$.

Independientemente del tipo de emparejamiento, la aritmética de curvas elípticas requiere de la aritmética en los campos $\mathbb{F}_p$ y $\mathbb{F}_{p^{k/d}}$. La Tabla 4.1 muestra el costo de los Algoritmos 4.2 y 4.3, donde m, s, a denotan una multiplicación, cuadrado y suma en el campo $\mathbb{F}_p$; $\hat{m}, \hat{s}, \hat{a}$ denotan una multiplicación, cuadrado y suma en el campo $\mathbb{F}_{p^{k/d}}$, $\hat{M}$ denota una multiplicación de un elemento en $\mathbb{F}_p$ por un elemento en $\mathbb{F}_{p^{k/d}}$, m_b y $m_{b'}$ denotan una multiplicación por las constantes b y b', respectivamente.

Operación	**Costo** $T, \tilde{T} \in \mathbb{G}_1$ y $R \in \mathbb{G}_2$	**Costo** $T, \tilde{T} \in \mathbb{G}_2$ y $R \in \mathbb{G}_1$
Doblado de un punto y evaluación de la línea tangente. $\ell_{\tilde{T},\tilde{T}}(R)$ y $2\tilde{T}$	$3m + 6s + 17a + 2\hat{M} + m_b$	$3\hat{m} + 6\hat{s} + 17\hat{a} + 2\hat{M} + m_{b'}$
Suma de un punto y evaluación de la línea secante. $\ell_{\tilde{T},T}(R)$ y $\tilde{T} + T$	$11m + 2s + 9a + 2\hat{M} + m_b$	$11\hat{m} + 2\hat{s} + 9\hat{a} + 2\hat{M} + m_{b'}$

Tabla 4.1: Costo de la aritmética de curvas elípticas en el ciclo de Miller

Algoritmo 4.2 Cálculo de la recta tangente y doblado de un punto en coordenadas proyectivas

Entrada: $T = (X_1, Y_1, Z_1), \quad R = (x_R, y_R) \in E(\bar{\mathbb{F}}_p)[r]$
Salida: $2T, \quad \ell_{T,T}(Q)$.

1: $A \leftarrow X_1 \cdot Y_1/2$
2: $B \leftarrow Y_1^2$
3: $C \leftarrow Z_1^2$
4: $D \leftarrow 3Z_1^2$
5: $E \leftarrow Db'$
6: $F \leftarrow 3E$
7: $G \leftarrow (B+F)/2$
8: $H \leftarrow (Y_1+Z_1)^2 - (B+C)$
9: $I \leftarrow E - B$
10: $X_3 \leftarrow A \cdot (B-F)$
11: $Y_3 \leftarrow G^2 - 3E^2$
12: $Z_3 \leftarrow B \cdot H$
13: $l_0 \leftarrow Ib'$
14: $l_1 \leftarrow H \cdot y_Q$
15: $l_2 \leftarrow 3X_1^2 \cdot x_Q$
16: **return** $2T = (X_3, Y_3, Z_3)$ y $\ell_{T,T}(Q) = l_0 + l_1 + l_2$,

Algoritmo 4.3 Cálculo de la recta secante y suma de puntos en coordenadas proyectivas

Entrada: $T = (X_1, Y_1, Z_1), \quad P = (X_2, Y_2, Z_2), \quad R = (x_R, y_R) \in E(\bar{\mathbb{F}}_p)[r]$
Salida: $T + P, \quad \ell_{T,P}(Q)$.

1: $A \leftarrow X_1 - Z_1 \cdot X_2$
2: $B \leftarrow Y_1 - Z_1 \cdot Y_2$
3: $C \leftarrow A^2$
4: $X_3 \leftarrow C \cdot X_1$
5: $C \leftarrow A \cdot C$
6: $D \leftarrow B^2 \cdot Z_1$
7: $D \leftarrow C + D - 2X_3$
8: $X_3 \leftarrow X_3 - D$
9: $T_1 \leftarrow B \cdot X_3$
10: $Y_3 \leftarrow T_1 - C \cdot Y_1$
11: $X_3 \leftarrow A \cdot D$
12: $Z_3 \leftarrow C \cdot Z_1$
13: $l_0 \leftarrow (B \cdot X_2) - (A \cdot Y_2)$
14: $l_1 \leftarrow A \cdot y_Q$
15: $l_2 \leftarrow -B \cdot x_Q$
16: **return** $2T = (X_3, Y_3, Z_3)$ y $\ell_{T,T}(Q) = l_0 + l_1 + l_2$,

Aritmética de campos finitos

El cálculo de $\ell_{\tilde{T},\tilde{T}}(R)$ y $\ell_{\tilde{T},T}(R)$ definen un elemento en el grupo $\mathbb{F}_{p^k}^*$ escrito de manera multiplicativa, con la mitad de sus coeficientes iguales a 0. En general, el producto de un elemento $f \in \mathbb{F}_{p^k}$ por $\ell_{\tilde{T},\tilde{T}}$ (líneas 4 y 6 del Algoritmo 4.1) se denomina "multiplicación dispersa" y al producto de dos líneas se le conoce como "multiplicación muy dispersa" [11].

Particularmente en esta tesis estamos trabajando con dos tipos de multiplicaciones dispersas y muy dispersas:

- ***Multiplicación dispersa y muy dispersa cuando el campo*** $\mathbb{F}_{p^k}$ ***se representa como una extensión cuadrática de una extensión cúbica y*** $d|k$ ***para*** $d = 6$.

  Suponiendo que se está utilizando la siguiente torre de campos:

$$\begin{aligned} \mathbb{F}_{p^k} &= \mathbb{F}_{p^{k/2}}[v]/v^2 - \xi \\ \mathbb{F}_{p^{k/2}} &= \mathbb{F}_{p^{k/6}}[u]/u^3 - \beta \end{aligned}$$

  En un emparejamiento de la forma $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, dados los puntos $\tilde{T} \in \mathbb{G}_1$ y $R \in \mathbb{G}_2$, el elemento $a = \ell_{\tilde{T},\tilde{T}}(R) \in \mathbb{F}_{p^k}$ está representado como:

$$a = (a_{0,0} + 0u + 0u^2) + (a_{1,0} + a_{1,1}u + 0u^2)v.$$

  Por otro lado, en un emparejamiento de la forma $\mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T$, dados los puntos $\tilde{T} \in \mathbb{G}_2$ y $R \in \mathbb{G}_1$, el elemento $a = \ell_{\tilde{T},\tilde{T}}(R) \in \mathbb{F}_{p^k}$ está representado como:

$$a = (a_{0,0} + a_{0,1}u + 0u^2) + (0 + a_{1,1}u + 0u^2)v.$$

  Como se puede observar, en ambos casos el elemento $a = \ell_{\tilde{T},\tilde{T}}(R) \in \mathbb{F}_{p^k}$ tiene tres de sus coeficientes iguales a cero y por lo tanto utilizando el algoritmo de Karatsuba, el costo es independiente del emparejamiento, como se muestra en la siguiente tabla, donde $\hat{m}$, $\hat{a}$ denotan una multiplicación y una suma en $\mathbb{F}_{p^{k/d}}$.

Operación	**Costo**
Multiplicación *dispersa*	$13\hat{m} + 29\hat{a}$
Multiplicación *muy dispersa*	$7\hat{m} + 14\hat{a}$

Tabla 4.2: Costo de la multiplicación *dispersa* y *muy dispersa* cuando el campo $\mathbb{F}_{p^k}$ es representado como una extensión cuadrática de una extensión cúbica

- ***Multiplicación dispersa y muy dispersa cuando el campo*** $\mathbb{F}_{p^k}$ ***se representa como una extensión cúbica de una extensión cuadrática y*** $d|k$ ***para*** $d = 6$.

  En este caso, suponiendo que se está utilizando la siguiente torre de campos:

$$\begin{aligned} \mathbb{F}_{p^k} &= \mathbb{F}_{p^{k/3}}[v]/v^3 - \xi \\ \mathbb{F}_{p^{k/3}} &= \mathbb{F}_{p^{k/6}}[u]/u^2 - \beta \end{aligned}$$

  Nuevamente, en un emparejamiento de la forma $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, dados los puntos $\tilde{T} \in \mathbb{G}_1$ y $R \in \mathbb{G}_2$, el elemento $a = \ell_{\tilde{T},\tilde{T}}(R) \in \mathbb{F}_{p^k}$ está representado como:

$$a = (a_{0,0} + a_{0,1}u) + (a_{1,0} + 0u)v + (0 + 0u)v^2.$$

Por otro lado, en un emparejamiento de la forma $\mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T$, dados los puntos $\tilde{T} \in \mathbb{G}_2$ y $R \in \mathbb{G}_1$, el elemento $a = \ell_{\tilde{T},\tilde{T}}(R) \in \mathbb{F}_{p^k}$ está representado como:

$$a = (a_{0,0} + a_{0,1}u) + (a_{1,0} + 0u)v + (0 + 0u)v^2.$$

Utilizando el algoritmo de Karatsuba, a continuación se muestra el costo de la multiplicación *dispersa* y *muy dispersa*, donde $\hat{m}$, $\hat{a}$ denotan una multiplicación y una suma en $\mathbb{F}_{p^{k/d}}$.

Operación	Costo
Multiplicación dispersa	$13\hat{m} + 34\hat{a}$
Multiplicación muy dispersa	$7\hat{m} + 15\hat{a}$

Tabla 4.3: Costo de la multiplicación *dispersa* y *muy dispersa* cuando el campo $\mathbb{F}_{p^k}$ es representado como una extensión cúbica de una extensión cuadrática

4.7. Exponenciación final

Como se ha visto en las secciones anteriores, los emparejamientos bilineales basados en la metodología de Tate requieren del cómputo de la exponenciación final $f^{(p^k-1)/r} \in \mathbb{F}_{p^k}^{\times}$, la cual tiene un costo considerable. Por ejemplo, con base en la Tabla 3.3, en una implementación sobre curvas KSS-18 con 192 bits de seguridad, se requiere que $\log_2(r) \approx 384$ y $\log_2(p) \approx 512$. Utilizando el método de exponenciación binaria, el costo de calcular $f^{(p^k-1)/r}$ es de aproximadamente 8832 cuadrados y 4416 multiplicaciones en el campo $\mathbb{F}_{p^k}$.

Sin embargo el aparente alto costo de la exponenciación final puede ser reducido drásticamente utilizando la representación de $(p^k - 1)/r$ como el producto de dos exponentes [**?**]:

$$\frac{(p^k - 1)}{r} = \frac{(p^k - 1)}{\Phi_k(p)} \cdot \frac{\Phi_k(p)}{r} \tag{4.14}$$

donde $\Phi_k(p)$ es el k-ésimo polinomio ciclotómico evaluado en p. Las familias de curvas elípticas que han sido estudiadas en el desarrollo de esta tesis (BN, BW-12, KSS-18 y BLS-24)[3], tienen la característica de que el grado de encajamiento k puede ser representado como $2^a 3^b$, tal que $a, b \geq 1$ y lo cual implica que $6|k$. El k-ésimo polinomio ciclotómico Φ_k cuando $6|k$, tiene la siguiente estructura [24]:

$$\Phi_{2^a 3^b}(z) = z^{2 \cdot 2^{a-1} 3^{b-1}} - z^{2^{a-1} 3^{b-1}} + 1, \tag{4.15}$$

es decir,

$$\Phi_k(p) = p^{k/3} - p^{k/6} + 1.$$

Por otra parte, el primer exponente $(p^k - 1)/\Phi_k(p)$ en la Ecuación (4.14), es expresado como:

$$(p^k - 1)/\Phi_k(p) = (p^{k/2} - 1) \cdot \left(\frac{p^{k/2} + 1}{\Phi_k(p)} \right).$$

Sustituyendo $\Phi_k(p)$ en la ecuación anterior y realizando un poco de álgebra, obtenemos la siguiente igualdad:

$$(p^k - 1)/\Phi_k(p) = (p^{k/2} - 1) \cdot (p^{k/6} + 1) \tag{4.16}$$

[3]La definición de las familias de curvas elípticas BN, BW-12, KSS-18 y BLS-24 se encuentra en la Sección 3.5.1.

Al cálculo de $g = f^{(p^{k/2}-1)(p^{k/6}+1)} \in \mathbb{F}_{p^k}$, se le conoce como **"*la parte fácil de la exponenciación final*"** debido a que únicamente requiere de la aplicación de dos operadores de Frobenius, dos multiplicaciones y una inversión en $\mathbb{F}_{p^k}$. Cabe mencionar que esta operación trae consigo diversas ventajas:

- El inverso multiplicativo de g se vuelve equivalente a una conjugación.

  Esto sucede debido a que $p^k - 1 = (p^{k/2} - 1) \cdot (p^{k/2} + 1)$, de tal manera que siendo f un elemento en $\mathbb{F}_{p^k}$ cuyo orden no divide a $p^{k/2} - 1$, si $g' = f^{p^{k/2}-1}$, entonces

  $$(g')^{p^{k/2}+1} = (f)^{(p^{k/2}-1)p^{k/2}+1} = 1 \quad \text{y por lo tanto} \quad (g')^{p^{k/2}} = 1/g'.$$

  Finalmente, por las propiedades del operador de Frobenius, se cumple que $(g')^{p^{k/2}} = (\bar{g'})$, donde $(\bar{g'})$ denota la conjugación de g'.

- El elemento $g = f^{(p^k-1)/\Phi_k(p)}$ se vuelve parte del k-ésimo grupo ciclotómico $G_{\Phi_k(p)}$ [Definición 2.13], ya que $g^{\Phi_k(p)} = (f^{(p^k-1)/\Phi_k(p)})^{\Phi_k(p)} = 1$.

- g se vuelve unitario, es decir, su norma $|g| = 1$ [Definición 2.9].

Finalmente, de acuerdo con la Ecuación (4.14), es necesario computar la exponenciación $g^{\Phi_k(p)/r} \in \mathbb{F}_{p^k}^{\times}$. Esta operación es llamada **"*la parte difícil de la exponenciación final*"**, debido a que su costo computacional es considerablemente mayor.

4.7.1. Parte *difícil* de la exponenciación final

Tomando como referencia el trabajo de Scott *et al.* [46], para las distintas familias de curvas elípticas, el exponente $d = \Phi_k(p)/r$ es parametrizado por un polinomio $d(z)$, y representado en base $p(z)$, tal que $d = d(z_0)$ y $p = p(z_0)$ para algún entero z_0:

$$d(z) = \sum_{i=0}^{\varphi(k)-1} \lambda_i(z) p^i(z) \tag{4.17}$$

donde $\varphi(\cdot)$ es la función indicatriz de Euler.

Los polinomios $\lambda_i(z)$ en la Ecuación (4.17), son de grado menor a $\deg(p(z))$ con coeficientes $\lambda_{(i,j)} \in \mathbb{Z}$, donde $\deg(p(z))$ denota el grado del polinomio $p(z)$.

$$\lambda_i(z) = \sum_{j=0}^{\deg(p(z))-1} \lambda_{(i,j)} z^j$$

Utilizando esta representación polinomial del exponente d, la operación $g^{d(z)}$ es implementada de la siguiente manera:

$$g^{d(z)} = g^{\sum_{i,j} \lambda_{(i,j)} z^j p^i} = \prod_{i,j} g^{\lambda_{(i,j)} z^j p^i}$$

donde $0 \leq i < \varphi(k)$ y $0 \leq j < \deg(p(x))$.

Siguiendo el método de Scott *et al.*, los valores temporales g^{z^j} son calculados y posteriormente

se les aplica el operador de Frobenius $(g^{z^j})^{p^i}$. Finalmente, a través del método de Olivos [29], se calcula $\prod (g^{z^j p^i})^{\lambda_{(i,j)}}$ mediante la cadena de adición vectorial formada por los distintos exponentes $\lambda_{(i,j)} \in \mathbb{Z}$.

Una de las principales aportaciones de esta tesis fue hacer más eficiente la parte *difícil* de la exponenciación final. El método propuesto está basado en la observación de que siendo $\mathbb{F}_{p^k}^{\times}$ un grupo cíclico, existe un múltiplo d' de d tal que $g^{d'} \in \mathbb{F}_{p^k}^{\times}$ y $g^{d'} \neq 1$, si y sólo si $r \nmid d'$ [21] [4].

Por lo tanto el problema se reduce a encontrar un múltiplo d' de d tal que $g \mapsto g^{d'}$ sea computado con un costo menor a $g \mapsto g^d$. Siendo $d = d(z)$ y dado que $g^{r(z)d(z)} = 1$, el múltiplo $d'(z)$ es expresado como la combinación lineal de $d(z)$, $zd(z)$, $\ldots$, $z^{\deg(r(z))-1}d(z)$, los cuales son representados mediante la Ecuación (4.17).

La matriz M es construida de manera que cada una de sus filas contenga los coeficientes $\lambda_{(i,j)} \in \mathbb{Z}$ correspondientes a los polinomios $d(z)$, $zd(z)$, $\ldots$, $z^{\deg(r(z))-1}d(z)$, es decir

$$\begin{bmatrix} d(z) \\ zd(z) \\ \vdots \\ z^{\deg(r(z))-1}d(z) \end{bmatrix} = M \cdot \left(\begin{bmatrix} 1 \\ p(z) \\ \vdots \\ p(z)^{\varphi(k)-1} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ z \\ \vdots \\ z^{\deg(p(z))-1} \end{bmatrix} \right)$$

donde $\otimes$ denota el producto de Kronecker.

Considerando a las filas de la matriz M como vectores $v_\ell \in \mathbb{Z}^m$, donde $m = \varphi(k) \cdot \deg(p(z))$ y $0 \leq \ell < \deg(r(z))$, el algoritmo $LLL(M)$ es ejecutado, dando como resultado un vector v' generado por la combinación lineal de los vectores v_ℓ cuya norma euclidiana $\|v'\|$ es mínima.

Finalmente, siendo $d'(z)$ el múltiplo de $d(z)$ correspondiente al vector v'

$$d'(z) = v' \cdot \left(\begin{bmatrix} 1 \\ p(z) \\ \vdots \\ p(z)^{\varphi(k)-1} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ z \\ \vdots \\ z^{\deg(p(z))-1} \end{bmatrix} \right)$$

la exponenciación $g^{d'(z)}$ es implementada a través de cadenas de adición, con un costo menor al de $g^{d(z)}$. A continuación es descrito a detalle el método propuesto para el caso particular de las familias de curvas elípticas BN, BW-12, KSS-18 y BLS-24. Del mismo modo, en el Apéndice A se puede encontrar la descripción del método para las familias Freeman-10 y KSS-8.

[4] Este trabajo fue realizado en colaboración con el profesor Alfred Menezes y Edward Knapp de la Universidad de Waterloo.

Curvas BN

En las curvas Barreto-Naehrig, el exponente $d(z) = (p(z)^4 - p(z)^2 + 1)/r(z)$ es expresado como

$$\begin{aligned} d(z) = & -36z^3 - 30z^2 - 18z - 2 \\ & + (-36z^3 - 18z^2 - 12z + 1)p(z) \\ & + (6z^2 + 1)p(z)^2 \\ & + p(z)^3. \end{aligned}$$

De acuerdo con el método descrito previamente, la matriz $M_{16\times 4}$ es construida de manera que

$$\begin{bmatrix} d(z) \\ zd(z) \\ 6z^2d(z) \\ 6z^3d(z) \end{bmatrix} = M \cdot \left(\begin{bmatrix} 1 \\ p(z) \\ p(z)^2 \\ p(z)^3 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ z \\ z^2 \\ z^3 \end{bmatrix} \right).$$

Si $z^\ell d(z)$ tiene coeficientes en $\mathbb{R}$, es necesario aplicar la multiplicación por un escalar que permita construir a la matriz M con elementos en $\mathbb{Z}$ (por ejemplo $6z^2d(z)$ y $6z^3d(z)$). Por lo tanto, al ejecutar el algoritmo $LLL(M)$ obtenemos el vector

$$v' = (1, 6, 12, 12, 0, 4, 6, 12, 0, 6, 6, 12, -1, 4, 6, 12),$$

que corresponde al múltiplo $d'(z) = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \lambda_3 p^3 = (12z^3 + 6z^2 + 2z)d(z)$, donde

$$\begin{aligned} \lambda_0(z) &= 1 + 6z + 12z^2 + 12z^3 \\ \lambda_1(z) &= 4z + 6z^2 + 12z^3 \\ \lambda_2(z) &= 6z + 6z^2 + 12z^3 \\ \lambda_3(z) &= -1 + 4z + 6z^2 + 12z^3. \end{aligned}$$

La exponenciación $g^{d'(z)}$ es implementada eficientemente a través de los valores temporales

$$g \mapsto g^z \mapsto g^{2z} \mapsto g^{4z} \mapsto g^{6z} \mapsto g^{6z^2} \mapsto g^{12z^2} \mapsto g^{12z^3},$$

los cuales requieren de 3 exponenciaciones a la z potencia, 3 cuadrados y 1 multiplicación en $\mathbb{F}_{p^{12}}$. Finalmente, sea $a = g^{12z^3} \cdot g^{6z^2} \cdot g^{6z}$ y $b = a \cdot (g^{2z})^{-1}$, la exponenciación $g^{d'(z)}$ es computada con un costo total de 3 aplicaciones del operador de Frobenius, 3 exponenciaciones a la z potencia, 10 multiplicaciones en $\mathbb{F}_{p^{12}}$ y 3 cuadrados en el grupo $\mathbb{G}_{\Phi_{12}(p)}$, como se muestra a continuación:

$$g^{d'(z)} = [a \cdot g^{6z^2} \cdot g] \cdot [b]^p \cdot [a]^{p^2} \cdot [b \cdot g^{-1}]^{p^3} \in \mathbb{F}^{\times}_{p^{12}}.$$

Curvas BW-12

En el caso particular de las *familias ciclotómicas*, dado que $r(z) = \Phi_k(z)$, no existe un múltiplo $d'(z)$ de $d(z) = \Phi_k(p)/r(z)$, tal que $g \mapsto g^{d'(z)}$ sea calculado con un costo menor a $g \mapsto g^{d(z)}$. Sin embargo, es posible disminuir el número de multiplicaciones en el campo $\mathbb{F}_{p^{12}}$ mediante el uso de valores temporales. Sea $d(z) = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \lambda_3 p^3$, donde

$$\begin{aligned} \lambda_0 &= z^5 - 2z^4 + 2z^2 - z + 3 \\ \lambda_1 &= z^4 - 2z^3 + 2z - 1 \\ \lambda_2 &= z^3 - 2z^2 + z \\ \lambda_3 &= z^2 - 2z + 1, \end{aligned}$$

se computan los elementos

$$g \to g^{-2} \to g^{z} \to g^{2z} \to$$
$$g^{z-2} \to g^{z^2-2z} \to g^{z^3-2z^2} \to g^{z^4-2z^3} \to g^{z^4-2z^3+2z} \to g^{z^5-2z^4+2z^2},$$

y posteriormente se implementa la exponenciación $g^{d(z)}$ como:

$$g^{z^5-2z^4+2z^2} \cdot (g^{z-2})^{-1} \cdot g \cdot (g^{z^4-2z^3+2z} \cdot g^{-1})^{p} \cdot (g^{z^3-2z^2} \cdot g^{z})^{p^2} \cdot (g^{z^2-2z} \cdot g)^{p^3}$$

utilizando 5 exponenciaciones por z, 3 aplicaciones del operador Frobenius, 10 multiplicaciones en $\mathbb{F}_{p^{12}}$ y 2 cuadrados en el grupo $\mathbb{G}_{\Phi_{12}(p)}$.

Curvas KSS-18

En la familia de curvas KSS con grado de encajamiento $k = 18$, la matriz entera M es construida de la siguiente manera:

$$\begin{bmatrix} 3d(z) \\ (3/7)zd(z) \\ (3/49)z^2d(z) \\ (3/49)z^3d(z) \\ (3/49)z^4d(z) \\ (3/49)z^5d(z) \end{bmatrix} = M \left(\begin{bmatrix} 1 \\ p(z) \\ p(z)^2 \\ p(z)^3 \\ p(z)^4 \\ p(z)^5 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ z \\ z^2 \\ z^3 \\ z^4 \\ z^5 \\ z^6 \\ z^7 \end{bmatrix} \right).$$

Después de ejecutar el algoritmo $LLL(M)$, el vector v' con menor norma euclideana, es el correspondiente al múltiplo $d'(z) = \frac{3z^2}{49}d(z) = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \lambda_3 p^3 + \lambda_4 p^4 + \lambda_5 p^5$, donde

$$\begin{aligned}
\lambda_0 &= z^6 + 5z^5 + 7z^4 + 21z^3 + 108z^2 + 147z, \\
\lambda_1 &= -5z^5 - 25z^4 - 35z^3 - 98z^2 - 505z - 686, \\
\lambda_2 &= -z^7 - 5z^6 - 7z^5 - 19z^4 - 98z^3 - 133z^2 + 6, \\
\lambda_3 &= 2z^6 + 10z^5 + 14z^4 + 35z^3 + 181z^2 + 245z, \\
\lambda_4 &= -3z^5 - 15z^4 - 21z^3 - 49z^2 - 254z - 343, \\
\lambda_5 &= z^4 + 5z^3 + 7z^2 + 3.
\end{aligned}$$

Utilizando el método de Olivos, construimos la cadena de adición

$$\begin{aligned}
&\{1, 2, 3, 5, 6, 7, 10, 14, 15, 19, 21, 25, 35, \underline{38}, 49, \underline{73}, \\
&\ 98, 108, 133, 147, 181, 245, 254, 343, \underline{490}, 505, 686\}
\end{aligned}$$

y computamos la exponenciación $g^{d'(z)}$ a través de 29 aplicaciones del operador de Frobenius, 7 exponenciaciones a la z potencia, 52 multiplicaciones en $\mathbb{F}_{p^{18}}$ y 8 cuadrados en $\mathbb{G}_{\Phi_{18}(p)}$.

Curvas BLS-24

Al igual que las curvas BW-12, no existe un múltiplo $d'(z)$ de $d(z)$, tal que el costo de computar $g \mapsto g^{d'(z)}$ sea menor al de $g \mapsto g^{d(z)}$. Sea $d(z) = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \lambda_3 p^3 + \lambda_4 p^4 + \lambda_5 p^5 + \lambda_6 p^6 + \lambda_7 p^7$,

tal que:

$$\begin{aligned}
\lambda_7 &= z^2 - 2z + 1,\\
\lambda_6 &= z^3 - 2z^2 + z = z\lambda_7,\\
\lambda_5 &= z^4 - 2z^3 + z^2 = z\lambda_6,\\
\lambda_4 &= z^5 - 2z^4 + z^3 = z\lambda_5,\\
\lambda_3 &= z^6 - 2z^5 + z^4 - z^2 + 2z - 1 = z\lambda_4 - \lambda_7,\\
\lambda_2 &= z^7 - 2z^6 + z^5 - z^3 + 2z^2 - z = z\lambda_3,\\
\lambda_1 &= z^8 - 2z^7 + z^6 - z^4 + 2z^3 - z^3 = z\lambda_2,\\
\lambda_0 &= z^9 - 2z^8 + z^7 - z^5 + 2z^4 - z^3 + 3 = z\lambda_1 + 3.
\end{aligned}$$

Calculando los valores temporales

$$\begin{aligned}
g^z \to g^{-2z} \to g^{-2z+1} \to g^{z^2} \to g^{\lambda_7}\\
g^{z\lambda_7} \to g^{z\lambda_6} \to g^{z\lambda_5} \to g^{z\lambda_4} \to g^{z\lambda_4-\lambda_7} \to g^{z\lambda_3} \to g^{z\lambda_2} \to g^{z\lambda_1} \to g^{z\lambda_1+3},
\end{aligned}$$

el costo de la parte difícil de la exponenciación final es 9 exponenciaciones a la z potencia, 7 aplicaciones del operador Frobenius, 12 multiplicaciones en $\mathbb{F}_{p^{24}}$ y 2 cuadrados en el grupo $\mathbb{G}_{\Phi_{24}(p)}$.

4.7.2. Comparación con el método de Scott *et al.*

En concreto, la Tabla 4.4 muestra la comparación de nuestro método con el de Scott *et al.*, para distintas familias de curvas elípticas *amables* con los emparejamientos, donde 'M'denota una multiplicación en $\mathbb{F}_{p^k}$ y 'S'denota un cuadrado en el k-ésimo grupo ciclotómico $G_{\Phi_k(p)}$ [5]. Cabe aclarar que ambos métodos requieren de $\deg(p(z)) - 1$ exponenciaciones a la z potencia, la cual es la operación más costosa de la exponenciación final.

Curva	Scott *et al.* [46]	Esta tesis [21]
BN	13M 4S	10M 3S
Freeman	14M 2S	12M 2S
KSS-8	31M 6S	26M 7S
KSS-18	62M 14S	52M 8S
BW-12	-	10M 2S
BLS-24	-	12M 2S

Tabla 4.4: Comparación entre los resultados obtenidos y los reportados por Scott *et al.* para el cálculo de la exponenciación final

4.8. Función picadillo hacia el grupo $\mathbb{G}_2$

El uso de protocolos basados en emparejamientos sólo puede ser práctico si es es posible computar eficientemente todas las operaciones involucradas en dichos protocolos. Sin embargo, la mayoría de las implementaciones en el estado del arte, sólo consideran la velocidad en el cómputo del emparejamiento como una métrica, sin tener en cuenta otras primitivas importantes, tales como la

[5] Los algoritmos estudiados para el cálculo de cuadrados en el grupo ciclotómico $G_{\Phi_k(p)}$, se encuentran descritos en la Sección 2.5.

generación de puntos aleatorios en una curva elíptica o el problema conocido como *"Picadillo al grupo $\mathbb{G}_2$"*.

En esta tesis se ha abarcado ambos problemas: El cómputo eficiente de los emparejamiento bilineales y en particular, la solución eficiente al problema del *"picadillo al grupo $\mathbb{G}_2$"*, el cual se describe a continuación:

Definición del Problema

Con base en la definición del grupo $\mathbb{G}_2$ presentada en la Sección 3.3, un elemento $Q \in \mathbb{G}_2$ es un punto de torsión r en el grupo $E(\mathbb{F}_{p^k})[r]$, tal que $\pi(Q) = pQ$, donde π es el endomorfismo de Frobenius, k es el grado de encajamiento y r es un número primo. El problema del *"picadillo al grupo $\mathbb{G}_2$"* consiste en encontrar un punto $Q \in \mathbb{G}_2$ a partir de un punto aleatorio en $E(\mathbb{F}_{p^k})$.

Dada la existencia de las curvas enlazadas [Definición 3.4], si el grupo $E'(\mathbb{F}_{p^{k/d}})[r]$ es isomórfico a $E(\mathbb{F}_q)[r]$, entonces el problema se reduce a encontrar un punto Q' en $E'(\mathbb{F}_{p^{k/d}})[r]$, donde $E'/\mathbb{F}_{p^{k/d}}$ es la curva enlazada de grado $d \in \{2, 3, 4, 6\}$.

Solución

Sea $E'(\mathbb{F}_{p^{k/d}})$ un grupo abeliano finito de orden $\#E'(\mathbb{F}_{p^{k/d}}) = c \cdot r$, donde "$c$" es un número compuesto definido como el *cofactor* de la curva enlazada. A partir de los Teoremas 2.1, 2.2 y 2.3 de la Sección 2.1.1, sabemos que

$$\{c\tilde{Q} \mid \tilde{Q} \in E'(\mathbb{F}_{p^{k/d}})\} = \{Q' \in E'(\mathbb{F}_{p^{k/d}}) \mid rQ' = \mathcal{O}\},$$

es decir, al tomar un punto aleatorio $\tilde{Q}$ de la curva enlazada y multiplicarlo por el cofactor c, obtenemos un punto Q' de torsión r en $E'(\mathbb{F}_{p^{k/d}})[r]$. La solución es sencilla, sin embargo, c es un número considerablemente grande, lo que provoca que esta solución sea costosa. A continuación se muestran las dos soluciones más eficientes hasta el momento para realizar el cómputo del problema descrito.

4.8.1. Método propuesto por Scott *et al* [47]

El orden del grupo $E'(\mathbb{F}_{p^{k/d}})$ se puede determinar a partir de la ecuación CM, bajo la cual se definen las curvas ordinarias *amables* con los emparejamientos [23]. Dada la curva elíptica $E/\mathbb{F}_p$, con base en la Ecuación (3.8) de la Sección 3.5, existe $\hat{f} \in \mathbb{Z}$ tal que:

$$4q - \hat{t}^2 = D\hat{f}^2,$$

donde D es el discriminante CM y $\hat{t}$ define la traza de E sobre $\mathbb{F}_{p^{k/d}}$, la cual es calculada a partir del Algoritmo 3.2.

Por el Teorema de Hasse, $\#E'(\mathbb{F}_{p^{k/d}}) = q + 1 - \tilde{t}$, donde $\tilde{t}$ es la traza de E' sobre $\mathbb{F}_{p^{k/d}}$ y cuyo valor depende del grado de la curva enlazada:

d	2	3	4	6
$\tilde{t}$	$-\hat{t}$	$(\pm 3\hat{f} - \hat{t})/2$	$\pm\hat{f}$	$(\pm 3\hat{f} + \hat{t})/2$

Tabla 4.5: Posibles valores de la traza t' de E' sobre $\mathbb{F}_q$.

Una vez determinado el orden del grupo, el cofactor es calculado como: $(q+1-\tilde{t})/r$.

Dado el isomorfismo $\phi\colon E'(\mathbb{F}_q) \to E(\mathbb{F}_{p^k})$, sea $\pi\colon E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k})$ el endomorfismo de Frobenius en E, Scott *et al.* [47] observaron que el endomorfismo $\psi : E'(\mathbb{F}_{p^{k/d}}) \to E'(\mathbb{F}_{p^{k/d}})$, definido como $\psi = \phi^{-1} \circ \pi \circ \phi$, puede ser utilizado para acelerar el cómputo de $\tilde{Q} \mapsto c\tilde{Q}$, donde ψ satisface la siguiente igualdad:

$$\psi^2(\tilde{Q}) - t\psi(\tilde{Q}) + p\tilde{Q} = \mathcal{O} \tag{4.18}$$

para todo $\tilde{Q} \in E'(\mathbb{F}_{p^{k/d}})$ [22, Teorema 1]. De esta manera, Scott *et al.* representaron al cofactor c como un polinomio en p y mediante la Ecuación (4.18), expresaron a c como un polinomio en ψ con coeficientes g_i menores a p. En las familias de curvas elípticas, este método es computado sobre los polinomios $p(z), r(z), t(z), c(z)$.

> ***Ejemplo 16.*** En las curvas BN, el cofactor de la curva enlazada $E'(\mathbb{F}_{p^2})$ está definido como $c(z) = 36z^4 + 36z^3 + 30z^2 + 6z + 1$. Utilizando el método de Scott *et al.*,
>
> $$c(z)\tilde{Q} = (36z^4 + 36z^3 + 30z^2 + 6z + 1)\tilde{Q} = \psi(6z^2\tilde{Q}) + 6z^2\tilde{Q} + \psi(\tilde{Q}) - \psi^2(\tilde{Q}).$$
>
> El costo del endomorfismo ψ es desdeñable; por lo tanto, el método de Scott *et al.* requiere de 2 multiplicaciones escalares por z y algunas sumas de puntos.

4.8.2. Método propuesto en esta tesis [21]

Comenzaremos por definir un teorema, el cual está basado en la observación de que dado un múltiplo c' del cofactor c, tal que $c' \not\equiv 0 \pmod{r}$, se cumple que $c'\tilde{Q} \in E(\mathbb{F}_{p^{k/d}})[r]$.

Teorema 4.1 *Supóngase que $E'(\mathbb{F}_{p^{k/d}})$ es un grupo cíclico y $p \equiv 1 \mod d$. Existe un polinomio $h(w) = h_0 + h_1 w + \cdots + h_{\varphi(k)-1} w^{\varphi(k)-1} \in \mathbb{Z}[w]$ tal que $h(\psi(\tilde{Q}))$ es un múltiplo de $c\tilde{Q}$, para todo $\tilde{Q} \in E(\mathbb{F}_{p^{k/d}})$, y $|h_i|^{\varphi(k)} \leq \#E'(\mathbb{F}_{p^{q/d}})/r$, donde $i \in \mathbb{Z}$.*

La prueba del teorema está basada en dos lemas principales:

Lema 4.2 *Sea d el grado de la curva enlazada E', si $p \equiv 1 \mod d$, entonces $\psi(\tilde{Q}) \in E'(\mathbb{F}_{p^{k/d}})$, para todo $\tilde{Q} \in E'(\mathbb{F}_{p^{k/d}})$.*

Prueba: Dado $\gamma \in \mathbb{F}_{p^k}$, tal que $\gamma^d \in \mathbb{F}_{p^{k/d}}$, el isomorfismo ϕ se define como $\phi(x, y) = (\gamma^2 x, \gamma^3 y)$, lo cual implica que $\psi(x, y) = (\gamma^{2(p-1)} x^p, \gamma^{3(p-1)} y^p)$. Además, si $\gamma^d \in \mathbb{F}_{p^{k/d}}$ y $p - 1 \equiv 0 \mod d$ entonces $\gamma^{p-1} \in \mathbb{F}_{p^{k/d}}$ y por lo tanto, $\psi(x, y) \in E'(\mathbb{F}_{p^{k/d}})$ para $(x, y) \in E'(\mathbb{F}_{p^{k/d}})$. □

Lema 4.3 *Sea $t^2 - 4p = Df^2$ y $\tilde{t}^2 - 4q = D\tilde{f}^2$, para algún valor de f y $\tilde{f}$, donde $q = p^{k/d}$ y D es el discriminante CM; sea además $\tilde{n} = \#E'(\mathbb{F}_{p^{k/d}})$, si se cumplen las condiciones:*

- $p \equiv 1 \mod d$,
- $mcd(\tilde{f}, \tilde{n}) = 1$,
- $E'(\mathbb{F}_{p^{k/d}})$ *es un grupo cíclico,*

entonces $\psi(\tilde{Q}) = a\tilde{Q}$ para todo $\tilde{Q} \in E'(\mathbb{F}_{p^{k/d}})$, donde:

$$a = (t \pm f(\tilde{t} - 2)/\tilde{f})/2.$$

Prueba: Dado que $E'(\mathbb{F}_{p^{k/d}})$ es cíclico y ψ es un endomorfismo en el grupo $E'(\mathbb{F}_{p^{k/d}})$, existe un número entero a, tal que $\psi(\tilde{Q}) = a\tilde{Q}$, para todo punto $\tilde{Q} \in E'(\mathbb{F}_{p^{k/d}})$. De esta manera, la identidad $\psi^2(\tilde{Q}) - t\psi(\tilde{Q}) + p\tilde{Q} = \mathcal{O}$ es escrita como $a^2 - ta + p = 0$; resolviendo la ecuación cuadrática, encontramos que:

$$a \equiv \frac{1}{2}(t \pm \sqrt{t^2 - 4p}) \equiv \frac{1}{2}(t \pm \sqrt{Df^2}) \equiv \frac{1}{2}(t \pm f\sqrt{D}) \mod \tilde{n}.$$

donde $\tilde{n} = \#E'(\mathbb{F}_{p^{k/d}})$. Sea $q = p^{k/d}$, por el teorema de Hasse, se cumple que $\tilde{n} = q + 1 - \tilde{t}$, es decir, $q \equiv t - 1 \mod \tilde{n}$; reduciendo módulo $\tilde{n}$, observamos que:

$$D\tilde{f}^2 = \tilde{t}^2 - 4q = \tilde{t}^2 - 4\tilde{t} + 4 = (\tilde{t} - 2)^2$$

y por lo tanto, $\sqrt{D} \equiv \pm(\tilde{t} - 2)/\tilde{f} \mod \tilde{n}$.

Sin perder generalidad, dado f y $\tilde{f}$, se cumple que $a = \frac{1}{2}(t + f\sqrt{D})$ y $\sqrt{D} \equiv (\tilde{t} - 2)/\tilde{f} \mod \tilde{n}$. Finalmente, dado que el orden del punto $\tilde{Q} \in E'(\mathbb{F}_{p^{k/d}})$ divide a $\tilde{n}$, entonces:

$$\psi(\tilde{Q}) = a\tilde{Q} = \left(\frac{1}{2}(t + f\sqrt{D})\right)\tilde{Q} = \left(\frac{1}{2}(t + f(\tilde{t} - 2)/\tilde{f})\right)\tilde{Q}.$$

□

Una vez calculado el valor de a, tal que $a\tilde{Q} = \psi(\tilde{Q})$, es necesario encontrar el polinomio $h \in \mathbb{Z}[w]$ con los menores coeficientes, tal que $h(a) = 0 \mod c$. Para esto, se procede a construir la matriz M cuyas filas representan a los polinomios $h_i(w) = w^i - a^i$, tal que $h_i(a) \equiv 0 \mod c$. De esta manera, cualquier combinación lineal de las filas de M corresponderá con un polinomio $h'(w)$ que satisface dicha condición.

Dado que el endomorfismo de Frobenius π actuando sobre $E(\mathbb{F}_{p^k})$ tiene orden k y dado que ψ es un endomorfismo restringido al grupo cíclico $E'(\mathbb{F}_{p^{k/d}})$, entonces ψ actuando sobre $E'(\mathbb{F}_{p^{k/d}})$ también tiene orden k. Además, dado que el número entero a satisface la congruencia $\Phi_k(a) \equiv 0 \mod \tilde{n}$, los polinomios $h(w) = w^i - a^i$ con $i \geq \varphi(k)$ pueden ser escritos como combinaciones lineales de de $w - a, \ldots, w^{\varphi(k)-1} - a^{\varphi(k)-1}$ módulo c, donde $\varphi(\cdot)$ es la función indicatriz de Euler. Por esta razón, únicamente son considerados los polinomios de grado menor a $\varphi(k)$.

$$\begin{array}{c} \\ M = \end{array} \begin{array}{c} \begin{array}{ccccc} a^0 & a^1 & a^2 & \cdots & a^{\varphi(k)-1} \end{array} \\ \begin{pmatrix} c & 0 & 0 & \cdots & 0 \\ -a & 1 & 0 & \cdots & 0 \\ -a^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ -a^{\varphi(k)-1} & 0 & 0 & \cdots & 1 \end{pmatrix} \end{array} \dashrightarrow \begin{array}{ccccc} c & \equiv & 0 & \mod c \\ -a + a & \equiv & 0 & \mod c \\ -a^2 + a^2 & \equiv & 0 & \mod c \\ \vdots & \vdots & & \vdots \\ -a^{\varphi(k)-1} + a^{\varphi(k)-1} & \equiv & 0 & \mod c \end{array}$$

Como se puede observar, la metodología es la misma que la utilizada en la definición de emparejamientos óptimos [Sección 4.5], es decir, las filas de la matriz M son vistas como vectores, los cuales forman la base de una *rejilla* L. Al aplicar el algoritmo $LLL(M)$, por el teorema de Minkowski [38], obtendremos un vector v formado por la combinación lineal de la base de L, el cual corresponde al polinomio h con coeficientes menores a $|c|^{1/\varphi(k)}$.

A continuación se describe el método para computar la función *picadillo* hacia el grupo $\mathbb{G}_2$ sobre las familias de curvas BN, BW-12, KSS-18 y BLS-24. Del mismo modo, la descripción del método empleado sobre las curvas Freeman-10 y KSS-8 se encuentra en el Apéndice B.

Curvas BN

En las curvas Barreto-Naehrig, el orden del grupo $\tilde{n} = \#E'(\mathbb{F}_{p^2})$ y la traza de E' sobre $\mathbb{F}_{p^2}$, se encuentran parametrizadas por:

$$\tilde{n} = (36z^4 + 36z^3 + 18z^2 + 6z + 1)(36z^4 + 36z^3 + 30z^2 + 6z + 1)$$
$$\tilde{t} = 36z^4 + 1$$

donde $\tilde{n}(x) = r(x)c(x)$. Utilizando el Lema 4.3, obtenemos que:

$$a(x) = -\frac{1}{5}(3456z^7 + 6696z^6 + 7488z^5 + 4932z^4 + 2112z^3 + 588z^2 + 106z + 6).$$

Una observación interesante es que $a(z) \equiv p(z) \mod r(z)$ y $\psi(Q') = a(z)Q' = p(z)Q'$ para todo $Q' \in \tilde{E}(\mathbb{F}_{p^2})[r]$. Siguiendo el método descrito anteriormente, construimos la *rejilla* reduciendo $-a(z)^i$ modulo $c(z)$:

$$\left[\begin{array}{c|ccc} c(z) & 0 & 0 & 0 \\ -a(z) & 1 & 0 & 0 \\ -a(z)^2 & 0 & 1 & 0 \\ -a(z)^3 & 0 & 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{c|ccc} 36z^4 + 36z^3 + 30z^2 + 6z + 1 & 0 & 0 & 0 \\ 48/5z^3 + 6z^2 + 4z - 2/5 & 1 & 0 & 0 \\ 36/5z^3 + 6z^2 + 6z + 1/5 & 0 & 1 & 0 \\ 12z^3 + 12z^2 + 8z + 1 & 0 & 0 & 1 \end{array}\right].$$

Para la *rejilla* construida a partir de esta matriz, encontramos que $h(w) = z + 3zw + zw^2 + w^3$. Reduciendo modulo $\tilde{n}$, encontramos que

$$h(a) = -(18z^3 + 12z^2 + 3z + 1)c(z)$$

y dado que $\mathrm{mcd}(18z^3 + 12z^2 + 3z + 1, r(x)) = 1$:

$$\tilde{Q} \mapsto z\tilde{Q} + \psi(3z\tilde{Q}) + \psi^2(z\tilde{Q}) + \psi^3(\tilde{Q}).$$

El cómputo de $\tilde{Q} \mapsto Q'$, donde $Q' \in E'(\mathbb{F}_{p^2})[r]$, tiene un costo de 1 doblado, 4 sumas de puntos, 1 multiplicación escalar por z y 3 aplicaciones del operador ψ.

Curvas BW-12

En las curvas BW-12 el cofactor se encuentra parametrizado como:

$$c(z) = \frac{1}{9}z^8 - \frac{4}{9}z^7 + \frac{5}{9}z^6 - \frac{4}{9}z^4 + \frac{2}{3}z^3 - \frac{4}{9}z^2 - \frac{4}{9}z + \frac{13}{9}$$

y es más eficiente computar la función *picadillo* al grupo $\mathbb{G}_2$ utilizando el método propuesto por Scott *et al.*, en donde

$$h(a) = (z^3 - z^2 - z + 4) + (z^3 - z^2 - z + 1)a + (-z^2 + 2z - 1)a^2,$$

de esta manera

$$\tilde{Q} \mapsto (z^3 - z^2 - z + 4)\tilde{Q} + \psi((z^3 - z^2 - z + 1)\tilde{Q}) + \psi^2((-z^2 + 2z - 1)\tilde{Q})$$

se calcula con un costo total de 6 sumas de puntos, 2 doblados, 3 multiplicaciones escalares por z y 3 aplicaciones del operador ψ.

Curvas KSS-18

En la familia de curvas KSS-18, el cofactor del grupo formado por los $\mathbb{F}_{p^3}$-puntos racionales de la curva enlazada $E'/\mathbb{F}_{p^3}$ de grado $d = 6$, está parametrizado como:

$$\begin{aligned} c(z) = \frac{1}{27}\big(&z^{18} + 15z^{17} + 96z^{16} + 409z^{15} + 1791z^{14} + 7929z^{13} + 27539z^{12} \\ &+ 81660z^{11} + 256908z^{10} + 757927z^9 + 1803684z^8 \\ &+ 4055484z^7 + 9658007z^6 + 19465362z^5 + 30860595z^4 \\ &+ 50075833z^3 + 82554234z^2 + 88845918z + 40301641\big). \end{aligned}$$

Construyendo la *rejilla*, obtenemos un vector correspondiente al múltiplo de $c(z)$:

$$h(a) = -\frac{3}{343}z(8z^3 + 147)c(z) = \lambda_0 + \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3 + \lambda_4 a^4 + \lambda_5 a^5,$$

donde

$$\begin{aligned} \lambda_0 &= 5z + 18 \\ \lambda_1 &= z^3 + 3z^2 + 1 \\ \lambda_2 &= -3z^2 - 8z \\ \lambda_3 &= 3z + 1 \\ \lambda_4 &= -z^2 - 2 \\ \lambda_5 &= z^2 + 5z. \end{aligned}$$

Construyendo la cadena de adición $\{1, 2, 3, 5, 8, \underline{10}, 18\}$, es posible computar $\tilde{Q} \mapsto Q'$, donde $Q' \in E'(\mathbb{F}_{p^3})[r]$, utilizando 2 doblados, 6 sumas, 3 multiplicaciones escalares por z y 5 aplicaciones del operador ψ.

Curvas BLS-24

Al igual que la familia BW-12, el método más eficiente de computar la función *picadillo* al grupo $\mathbb{G}_2$ sobre las curvas BLS-24, es el propuesto por Scott *et al.*, sin embargo, el Teorema 4.1 se sigue cumpliendo.

En estas familias de curvas, el cofactor se encuentra parametrizado como:

$$\begin{aligned} c(z) =& \frac{1}{81} \cdot z^{32} - 8z^{31} + 28z^{30} - 56z^{29} + 67z^{28} - 32z^{27} - 56z^{26} + \\ & 160z^{25} - 203z^{24} + 44z^{23} + 4z^{22} - 44z^{21} + 170z^{20} - 124z^{19} + 44z^{18} - 4z^{17} + \\ & 2z^{16} + 20z^{15} - 46z^{14} + 20z^{13} + 5z^{12} + 8z^{11} - 14z^{10} + 16z^9 - 101z^8 + 100z^7 + \\ & 70z^6 - 128z^5 + 70z^4 - 56z^3 - 44z^2 + 40z + 100 \end{aligned}$$

$$h(a) = 3c(z) = \lambda_0 + \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3 + \lambda_4 a^4 + \lambda_5 a^5 + \lambda_6 a^6$$

donde

$$\begin{aligned}
\lambda_0 &= -2z^8 + 4z^7 - 3z^5 + 3z^4 - 2z^3 - 2z^2 + z + 4 \\
\lambda_1 &= z^5 - z^4 - 2z^3 + 2z^2 + z - 1 \\
\lambda_2 &= z^5 - z^4 - z + 1 \\
\lambda_3 &= z^5 - z^4 - z + 1 \\
\lambda_4 &= -3z^4 + z^3 + 4z^2 + z - 3 \\
\lambda_5 &= 3z^3 - 3z^2 - 3z + 3 \\
\lambda_6 &= -z^2 + 2z - 1.
\end{aligned}$$

Utilizando el método descrito en [47], el costo total es de 21 sumas de puntos, 4 doblados, 8 multiplicaciones escalares por z y 6 aplicaciones del operador ψ.

4.8.3. Comparación con el método de Scott *et al.*

En la Tabla 4.6 se muestra una comparación de los resultados obtenidos en esta tesis con el trabajo de Scott *et al.* [47]. "A", "D" denotan la suma y doblado de puntos, mientras que , "Z" y "ψ" denotan una multiplicación escalar por el parámetro z y la aplicación del operador $\psi(\cdot)$, respectivamente.

Curva	Scott *et al.* [47]	Esta tesis [21]
BN	4A 2D 2Z 3ψ	4A 1D 1Z 3ψ
Freeman	20A 5D 3Z 4ψ	14A 4D 3Z 4ψ
KSS-8	22A 5D 5Z 2ψ	7A 3D 2Z 3ψ
KSS-18	59A 5D 7Z 4ψ	16A 2D 3Z 5ψ
BW-12	6A 3D 3Z 3ψ	-
BLS-24	21A 4D 8Z 6ψ	-

Tabla 4.6: Comparación entre los resultados obtenidos y los reportados por Scott *et al.* para el cálculo de la función picadillo hacia el grupo $\mathbb{G}_2$

Dado que la operación más costosa es la multiplicación escalar por z, en la mayoría de las familias de curvas elípticas, el método propuesto es considerablemente más eficiente que el presentado por Scott *et al.* [47].

Por ejemplo, en un emparejamiento sobre curvas BN con 128 bits de seguridad, se requiere que $\log_2(z) \approx 64$. Suponiendo que z tiene un peso de Hamming de 3 y utilizando un algoritmo de suma y doblado de puntos para la multiplicación escalar, el costo de computar zQ para $Q \in \mathbb{G}_2$ es de aproximadamente $63D + 2A$. Por lo tanto, el método propuesto para el cálculo de la función *picadillo* hacia el grupo $\mathbb{G}_2$ es aproximadamente dos veces más eficiente que el método de Scott *et al.*, como se muestra en la siguiente tabla:

Scott *et al.*	**Esta tesis**
$\approx 126\ D + 4\ A$	$\approx 63\ D + 2\ A$

Capítulo 5

Diseño y Estimaciones

Todo lo que puede ser contado no necesariamente cuenta;
todo lo que cuenta no necesariamente puede ser contado

Albert Einstein

Como se mencionó en la Sección 3.5.1, en las familias de curvas elípticas la terna $(p(z), r(z), t(z))$ define distintas curvas dependiendo del valor de z. La elección de z influye directamente en la seguridad y eficiencia en el cómputo de los emparejamientos bilineales; es por esta razón que en la primera sección de este capítulo, se muestran los costos relacionados con la selección del parámetro z, para las distintas familias de curvas elípticas estudiadas durante la tesis.

Posteriormente, a partir de estos costos, la segunda sección del capítulo contiene las estimaciones realizadas sobre implementaciones secuenciales y paralelas de los emparejamientos bilineales. Debido a la dificultad que existe en la paralelización de la función de Miller y la exponenciación final, la mayoría de los trabajos presentados en el estado del arte, se han enfocado en implementaciones secuenciales. Sin embargo, en esta tesis se ha decidido explorar la paralelización de la función de Miller, esperando que el trabajo realizado pueda beneficiar a los protocolos basados en emparejamientos sobre arquitecturas multinúcleo.

5.1. Selección de Parámetros

Después de realizar una búsqueda exhaustiva inteligente, seleccionamos cuidadosamente el parámetro z para las familias de curvas elípticas amables con los emparejamientos BN, BW-12, KSS-18 y BLS-24, que permitiera llevar a cabo el cómputo eficiente de los emparejamientos bilineales con 192 bits de seguridad. Los resultados obtenidos se muestran en la siguiente tabla:

Familia de Curvas Elípticas	**Parámetro** z	$\log_2(p)$	**Palabras de** p (64 bits)	$\log_2(r)$	**Ecuación de la Curva**
BN	$2^{158} - 2^{128} - 2^{68} + 1$	638	10	638	$E : y^2 = x^3 + 257$
BW-12	$-2^{107} + 2^{105} + 2^{93} + 2^5$	638	10	427	$E : y^2 = x^3 + 15$
KSS-18	$2^{64} - 2^{61} + 2^{56} - 2^{13} - 2^7$	507	8	375	$E : y^2 = x^3 + 13$
BLS-24	$-2^{48} + 2^{27} - 2^{24} + 2^{19} - 1$	479	8	384	$E : y^2 = x^3 + 1$

Tabla 5.1: Selección del parámetro z para la definición de curvas ordinarias.

5.1.1. Costo computacional de la aritmética de torre de campos

Uno de los principales criterios que fue considerado en la selección del parámetro z, es que $p = p(z)$ defina un campo finito $\mathbb{F}_{p^k}$ *amable* con los emparejamientos para las distintas familias de curvas elípticas, donde k es el grado de encajamiento [Sección 2.4]. De esta manera, $\mathbb{F}_{p^k}$ es representado mediante extensiones cuadráticas y cúbicas de un campo base, utilizando binomios irreducibles.

A continuación se muestra la definición y costo de la torre de campo, así como el costo de las principales operaciones involucradas en el cálculo de los emparejamientos bilineales para las distintas familias de curvas elípticas estudiadas durante la tesis. Estos costos fueron obtenidos a partir de las Tablas 2.1, 4.1, 4.2 y 4.3; así como de los Algoritmos 2.1 al 2.8 del Capítulo 2 y los Algoritmos 4.2 y 4.3 para la suma y doblado de puntos.

Es importante mencionar que el costo de la exponenciación por z se estimó utilizando el método descrito en la Sección 2.5.1; por otra parte, el costo del operador de Frobenius depende directamente del valor de p y se estimo utilizando el método descrito en la referencia [11].

Curvas BN y BW-12

Las curvas correspondientes a las familias BN y BW-12 propuestas en la Tabla 5.1, tienen la característica de que $\log_2(p) \approx 640$ y además, ambas tienen grado de encajamiento $k = 12$. Lo anterior permite que la estructura general de la torre de campos sea la misma para las curvas BN y BW-12.

$$\begin{aligned} \mathbb{F}_{p^2} &= \mathbb{F}_p[u]/(u^2 - \beta), \text{ donde } \beta \in \mathbb{F}_p. \\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^2}[v]/(v^3 - \xi), \text{ donde } \xi \in \mathbb{F}_{p^2}. \\ \mathbb{F}_{p^{12}} &= \mathbb{F}_{p^6}[w]/(w^2 - \gamma), \text{ donde } \gamma = v \end{aligned}$$

Para utilizar esta representación, se debe cumplir que β y ξ no tengan raíz cuadrada ni raíz cúbica en los campos finitos $\mathbb{F}_p$ y $\mathbb{F}_{p^2}$, respectivamente. El procedimiento para encontrar ambos parámetros es directo: basta con calcular raíces cuadradas y cúbicas recursivamente de β y ξ, hasta satisfacer la condición estipulada [32]. A continuación se muestra el valor de β y ξ obtenidos para ambas familias de curvas elípticas:

Familia de Curvas Elípticas	β	ξ
BN	-1	$u+1$
BW-12	-1	$u+2$

En la Tabla 5.2 se muestra el costo computacional de la aritmética en cada una de las extensiones de la torre de campos. Además la Tabla 5.3 proporciona el costo de las principales operaciones involucradas en el cálculo del emparejamiento.

Cabe señalar que m_{640}, s_{640}, a_{640}, i_{640} denotan el costo de una multiplicación, cuadrado, suma e inversión en $\mathbb{F}_p$, donde p es un número primo de 638 bits, distribuido en 10 palabras de 64 bits[1]. Además, $\tilde{m}$, $\tilde{s}$, $\tilde{a}$, $\tilde{i}$ denotan el costo de una multiplicación, cuadrado, suma e inversión en $\mathbb{F}_{p^2}$, respectivamente, mientras que m_β y m_ξ denotan una multiplicación por β y ξ.

[1] En las implementaciones en software, esta selección del tamaño de p permite el uso de la técnica llamada "*reducción displicente (lazzy reduction)*", como se recomienda en [2,9]

Campo	Suma	Multiplicación	Cuadrado	Inversión
$\mathbb{F}_{p^2}$	$2a_{640}$	$3m_{640} + 5a_{640} + m_\beta$	$2m_{640} + 5a_{640} + 2m_\beta$	$2m_{640} + 2s_{640} + 2a_{640} + i_{640} + m_\beta$
$\mathbb{F}_{p^6}$	$3\tilde{a}$	$6\tilde{m} + 15\tilde{a} + 2m_\xi$	$2\tilde{m} + 3\tilde{s} + 10\tilde{a} + 2m_\xi$	$9\tilde{m} + 3\tilde{s} + 5\tilde{a} + \tilde{i} + 4m_\xi$
$\mathbb{F}_{p^{12}}$	$6\tilde{a}$	$18\tilde{m} + 60\tilde{a} + 7m_\xi$	$12\tilde{m} + 45\tilde{a} + 6m_\xi$	$25\tilde{m} + 9\tilde{s} + 61\tilde{a} + \tilde{i} + 13m_\xi$
$\mathbb{G}_{\Phi_{12}(p)}$	$6\tilde{a}$	$18\tilde{m} + 60\tilde{a} + 7m_\xi$	$9\tilde{s} + 30\tilde{a} + 4m_\xi$	Conjugación

Tabla 5.2: Costo de la Aritmética en la torre de extensiones de campo de $\mathbb{F}_{p^{12}}$

Operación	Costo
Doblado de un punto y evaluación de la línea tangente. $\ell_{T,T}(P)$ y $2T$	$3\tilde{m} + 6\tilde{s} + 17\tilde{a} + 4m_{640} + m_\xi$
Suma de un punto y evaluación de la línea secante. $\ell_{T,Q}(P)$ y $T + Q$	$11\tilde{m} + 2\tilde{s} + 9\tilde{a} + 4m_{640} + m_\xi$
Multiplicación dispersa	$13\tilde{m} + 29\tilde{a} + 3m_\xi$
Multiplicación muy dispersa	$7\tilde{m} + 14\tilde{a}$

Operación	BN	BW-12
Exponenciación por z en el grupo $\mathbb{G}_{\Phi_{12}(p)}$	$69\tilde{m} + 957\tilde{s} + 3689\tilde{a} + \tilde{i} + 501m_\xi$	$75\tilde{m} + 645\tilde{s} + 2578\tilde{a} + \tilde{i} + 350m_\xi$
Operador de Frobenius p, p^3	$15m_{640}$	$15m_{640}$
Operador de Frobenius p^2	$10m_{640}$	$15m_{640}$

Tabla 5.3: Costo de las operaciones involucradas en el cómputo del emparejamiento sobre curvas BN y BW-12

Curvas KSS-18

Un elemento en el campo $\mathbb{F}_{p^{18}}$ puede ser representado utilizando la siguiente torre de campos:

$$\begin{aligned} \mathbb{F}_{p^3} &= \mathbb{F}_p[u]/(u^3 - \beta), \text{ donde } \beta = -6 \in \mathbb{F}_p, \\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^3}[v]/(v^2 - \xi), \text{ donde } \xi = u \in \mathbb{F}_{p^3}, \\ \mathbb{F}_{p^{18}} &= \mathbb{F}_{p^6}[w]/(w^3 - \gamma), \text{ donde } \gamma = v \end{aligned}$$

De manera similar a las curvas BN y BW-12, la Tabla 5.4 contiene el costo de la aritmética en las extensiones de la torre de campos. Dado que p es un número primo de 507 bits, distribuido en 8 registros de 64 bits (Tabla 5.1), hemos utilizado m_{512}, s_{512}, a_{612}, i_{512}, para denotar el costo de una multiplicación, cuadrado, suma e inversión en el campo $\mathbb{F}_p$. Además, $\bar{\bar{m}}$, $\bar{\bar{s}}$, $\bar{\bar{a}}$ y $\bar{\bar{i}}$ denotan el costo de las operaciones en el campo $\mathbb{F}_{p^3}$.

Campo	Suma	Multiplicación	Cuadrado	Inversión
$\mathbb{F}_{p^3}$	$3a_{512}$	$6m_{512} + 15a_{512} + 2m_\beta$	$2m_{512} + 3s_{512} + 10a_{512} + 2m_\beta$	$9m_{512} + 3s_{512} + 5a_{512} + i_{512} + 4m_\beta$
$\mathbb{F}_{p^6}$	$2\bar{a}$	$3\bar{m} + 5\bar{a} + m_\xi$	$2\bar{m} + 5\bar{a} + 2m_\xi$	$2\bar{m} + 2\bar{s} + 2\bar{a} + \bar{i} + m_\xi$
$\mathbb{F}_{p^{18}}$	$6\bar{a}$	$18\bar{m} + 60\bar{a} + 8m_\xi$	$12\bar{m} + 45\bar{a} + 10m_\xi$	$35\bar{m} + 2\bar{s} + 72\bar{a} + \bar{i} + 20m_\xi$
$\mathbb{G}_{\Phi_{18}(p)}$	$6\bar{a}$	$18\bar{m} + 60\bar{a} + 8m_\xi$	$6\bar{m} + 39\bar{a} + 7m_\xi$	Conjugación

Tabla 5.4: Costo de la Aritmética en la torre de extensiones de campo $\mathbb{F}_{p^{18}}$

Operación	Costo
Doblado de un punto y evaluación de la línea tangente. $\ell_{T,T}(P)$ y $2T$	$3\bar{m} + 6\bar{s} + 17\bar{a} + 6m_{512} + m_\xi$
Suma de un punto y evaluación de la línea secante. $\ell_{T,Q}(P)$ y $T + Q$	$11\bar{m} + 2\bar{s} + 9\bar{a} + 6m_{512} + m_\xi$
Multiplicación dispersa	$13\bar{m} + 34\bar{a} + 4m_\xi$
Multiplicación muy dispersa	$7\bar{m} + 15\bar{a} + 2m_\xi$
Exponenciación por z en el grupo $\mathbb{G}_{\Phi_{18}(p)}$	$99\bar{m} + 399\bar{s} + 1703\bar{a} + \bar{\bar{i}} + 234m_\xi$
Operador Frobenius	$5m_{512}$

Tabla 5.5: Costo de las operaciones involucradas en el cómputo del emparejamiento sobre curvas KSS-18

Curvas BLS-24

Un elemento en el campo finito $\mathbb{F}_{p^{24}}$ puede ser representado de diversas maneras; en este trabajo hemos utilizado la siguiente torre de campos:

$$\begin{aligned}
\mathbb{F}_{p^2} &= \mathbb{F}_p[u]/(u^2 + \beta), \text{ donde } \beta = 1 \in \mathbb{F}_p, \\
\mathbb{F}_{p^4} &= \mathbb{F}_{p^2}[v]/(v^2 + \xi), \text{ donde } \xi = u + 1 \in \mathbb{F}_{p^2}, \\
\mathbb{F}_{p^8} &= \mathbb{F}_{p^4}[w]/(w^2 + v) \\
\mathbb{F}_{p^{24}} &= \mathbb{F}_{p^8}[z]/(z^3 + w)
\end{aligned}$$

Las Tablas 5.6 y 5.7 muestran el costo de la aritmética en las extensiones de torres de campos y el costo de las operaciones involucradas en el cálculo del emparejamiento *óptimo ate*, respectivamente. A pesar de que el $\log_2(p) = 479$, los elementos del campo $\mathbb{F}_p$ son representados por 8 registros de 64 bits, como si se tratase de números de 512 bits. Del mismo modo que las curvas BN y BW-12, $\tilde{m}$, $\tilde{s}$, $\tilde{a}$, $\tilde{i}$ denotan la multiplicación, cuadrado, suma e inversión en el campo in $\mathbb{F}_{p^2}$, respectivamente.

Campo	Suma	Multiplicación	Cuadrado	Inversión
$\mathbb{F}_{p^2}$	$2a_{512}$	$3m_{512} + 5a_{512} + m_\beta$	$2m_{512} + 5a_{512} + 2m_\beta$	$2m_{512} + 2s_{512} + 2a_{512} + i_{512} + m_\beta$
$\mathbb{F}_{p^4}$	$2\tilde{a}$	$3\tilde{m} + 5\tilde{a} + m_\xi$	$2\tilde{m} + 5\tilde{a} + 2m_\xi$	$2\tilde{m} + 2\tilde{s} + 2\tilde{a} + \tilde{i} + m_\xi$
$\mathbb{F}_{p^8}$	$4\tilde{a}$	$9\tilde{m} + 25\tilde{a} + 4m_\xi$	$6\tilde{m} + 15\tilde{a} + 4m_\xi$	$12\tilde{m} + 2\tilde{s} + 26\tilde{a} + \tilde{i} + 8m_\xi$
$\mathbb{F}_{p^{24}}$	$12\tilde{a}$	$54\tilde{m} + 210\tilde{a} + 26m_\xi$	$36\tilde{m} + 135\tilde{a} + 22m_\xi$	$111\tilde{m} + 2\tilde{s} + 316\tilde{a} + \tilde{i} + 60m_\xi$
$\mathbb{G}_{\Phi_{24}(p)}$	$12\tilde{a}$	$54\tilde{m} + 210\tilde{a} + 26m_\xi$	$18\tilde{m} + 93\tilde{a} + 5m_\xi$	Conjugación

Tabla 5.6: Costo de la Aritmética en la torre de extensiones de campo $\mathbb{F}_{p^{24}}$

Operación	Costo
Doblado de un punto y evaluación de la línea tangente. $\ell_{T,T}(P)$ y $2T$	$21\tilde{m} + 79\tilde{a} + 8m_{640} + 16m_{\xi}$
Suma de un punto y evaluación de la línea secante. $\ell_{T,Q}(P)$ y $T+Q$	$37\tilde{m} + 85\tilde{a} + 8m_{640} + 16m_{\xi}$
Multiplicación dispersa	$39\tilde{m} + 133\tilde{a} + 17m_{\xi}$
Multiplicación muy dispersa	$21\tilde{m} + 65\tilde{a} + 9m_{\xi}$
Exponenciación por z en el grupo $\mathbb{G}_{\Phi_{24}(p)}$	$881\tilde{m} + 2\tilde{s} + 4647\tilde{a} + \tilde{i} + 878m_{\xi}$
Operador Frobenius	$45m_{512}$

Tabla 5.7: Costo de las operaciones involucradas en el cómputo del emparejamiento sobre curvas BLS-24

5.2. Costo computacional del emparejamiento óptimo ate

En general, el emparejamiento *óptimo ate* se encuentra dividido en tres bloques principales: el ciclo de Miller [Sección 4.6], la evaluación de líneas adicionales al ciclo de Miller y la exponenciación final [Sección 4.7]. Con el objetivo de hacer una estimación del costo del emparejamiento *óptimo ate*, las siguientes tablas muestran el número de operaciones requeridas por familia (BN, BW-12, KSS-18 y BLS-24), para el cálculo de cada uno de estos bloques principales.

# de operaciones requeridas en el ciclo de Miller (C.M)					
Familia de Curvas Elípticas	**Doblado de un punto y evaluación de la línea tangente** $\ell_{T,T}(P)$ y $2T$	**Suma de puntos y evaluación de la línea secante** $\ell_{T,Q}(P)$ y $P+Q$	**Multiplicación dispersa en** $\mathbb{F}_{p^k}$	**Multiplicación muy dispersa en** $\mathbb{F}_{p^k}$	**Cálculo de cuadrados en** $\mathbb{F}_{p^k}$
BN	161	6	165	1	160
BW-12	107	3	108	1	106
KSS-18	64	4	66	1	63
BLS-24	48	4	50	1	47

Tabla 5.8: Número de operaciones requeridas en el ciclo de Miller para cada una de las familias de curvas elípticas

# de operaciones requeridas en las líneas finales (L.F)						
Familia de Curvas Elípticas	**Doblado de un punto y evaluación de la línea tangente** $\ell_{T,T}(P)$ y $2T$	**Suma de puntos y evaluación de la línea secante** $\ell_{T,Q}(P)$ y $P+Q$	**Mult. en** $\mathbb{F}_{p^k}$	**Cuadrado en** $\mathbb{F}_{p^k}$	**Mult. muy dispersa en** $\mathbb{F}_{p^k}$	**Operador Frobenius** $\mathbb{F}_{p^k}$
BN	-	2	1	-	1	4
BW-12	-	-	-	-	-	-
KSS-18	1	1	2	1	1	5
BLS-24	-	-	-	-	-	-

Tabla 5.9: Número de operaciones requeridas en el cálculo de las líneas adicionales al ciclo de Miller

# de operaciones requeridas en la exponenciación final (E.F)					
Familia de Curvas Elípticas	**Multiplicación en** $\mathbb{F}_{p^k}$	**Cuadrados en el grupo** $\mathbb{G}_{\Phi_k(p)}$	**Inversión en** $\mathbb{F}_{p^k}$	**Operador Frobenius**	**Exponenciación por** z_0
BN	12	3	1	4	3
BW-12	12	2	1	4	5
KSS-18	54	8	1	29	7
BLS-24	14	2	1	8	9

Tabla 5.10: Número de operaciones requeridas en la exponenciación final para cada una de las familias de curvas elípticas

Finalmente, la siguiente tabla contiene el costo total del emparejamiento *óptimo ate* en términos de operaciones en el campo $\mathbb{F}_{p^2}$ y $\mathbb{F}_{p^3}$, según sea el caso.

Costo total del emparejamiento *óptimo ate*							
Familia de Curvas Elípticas	**Extención del campo** n	Fase	**# Mult. en el campo** $\mathbb{F}_{p^n}$	**#Cuadrados en el campo** $\mathbb{F}_{p^n}$	**#Sumas en el campo** $\mathbb{F}_{p^n}$	**#Inversiones en el campo** $\mathbb{F}_{p^n}$	**#Mult. en el campo** $\mathbb{F}_p$
BN	2	C.M	$4621\tilde{m}$	$978\tilde{s}$	$14790\tilde{a}$	-	$668m_{640}$
		L.F	$47\tilde{m}$	$4\tilde{s}$	$92\tilde{a}$	-	$58m_{640}$
		E.F	$448\tilde{m}$	$2907\tilde{s}$	$11938\tilde{a}$	$4\tilde{i}$	$50m_{640}$
		Total	$5116\tilde{m}$	$3889\tilde{s}$	$26847\tilde{a}$	$4\tilde{i}$	$776m_{640}$
BW-12	2	C.M	$3037\tilde{m}$	$648\tilde{s}$	$9762\tilde{a}$	-	$440m_{640}$
		L.F	-	-	-	-	-
		E.F	$616\tilde{m}$	$3297\tilde{s}$	$13731\tilde{a}$	$6\tilde{i}$	$60m_{640}$
		Total	$3653\tilde{m}$	$3945\tilde{s}$	$23493\tilde{a}$	$6\tilde{i}$	$500m_{640}$
KSS-18	3	C.M	$1857\bar{\tilde{m}}$	$392\bar{\tilde{s}}$	$6218\bar{\tilde{a}}$	-	$408m_{512}$
		L.F	$80\bar{\tilde{m}}$	$8\bar{\tilde{s}}$	$206\bar{\tilde{a}}$	-	$27m_{512}$
		E.F	$1748\bar{\tilde{m}}$	$2795\bar{\tilde{s}}$	$15545\bar{\tilde{a}}$	$8\bar{\tilde{i}}$	$145m_{512}$
		Total	$3685\bar{\tilde{m}}$	$3195\bar{\tilde{s}}$	$21969\bar{\tilde{a}}$	$8\bar{\tilde{i}}$	$580m_{512}$
BLS-24	2	C.M	$4819\tilde{m}$	-	$17192\tilde{a}$	-	$416m_{512}$
		L.F	-	-	-	-	-
		E.F	$8832\tilde{m}$	$20\tilde{s}$	$45265\tilde{a}$	$10\tilde{i}$	$360m_{512}$
		Total	$13651\tilde{m}$	$20\tilde{s}$	$62457\tilde{a}$	$10\tilde{i}$	$776m_{640}$

Tabla 5.11: Costo del emparejamiento óptimo ate para distintas familias con 192-bits de seguridad

5.2.1. Comparación del emparejamiento *óptimo ate* (Versión Secuencial)

A partir de la Tabla 5.11 no es posible hacer una comparación justa entre el desempeño de las distintas familias de curvas elípticas, debido principalmente a que tanto el campo base $\mathbb{F}_p$ como la extensión $\mathbb{F}_{p^n}$, para $n = \{2, 3\}$, varían dependiendo de la curva elíptica.

Una forma en la cual se puede llevar a cabo una comparación apropiada, es a través del número de multiplicaciones en el campo $\mathbb{F}_{p_{512}}$, donde p_{512} denota un número primo de 512 bits. Suponiendo

que se está empleando un multiplicador de complejidad cuadrática para el producto de dos números sobre los campos $\mathbb{F}_{p_{640}}$ y $\mathbb{F}_{p_{512}}$, podemos decir que:

$$m_{640} \approx (640/512)^2 \cdot m_{512} = 1.5625 \cdot m_{512}$$

Considerando además que $s_{512} \approx 0.8\, m_{512}$ e $i_{512} \approx 50 m_{512}$, la Tabla 5.12 muestra una comparación entre el costo de cómputo del emparejamiento *óptimo ate* sobre curvas BN, BW-12, KSS-18 y BLS-24 con 192 bits de seguridad. Como se puede observar, estas estimaciones predicen que la implementación sobre curvas BW-12 es más eficiente sobre todas las demás. Las curvas KSS-18 ocupan el segundo lugar, seguidas muy de cerca por las BN, mientras que la familia BLS-24 es la menos eficiente debido al elevado costo de la exponenciación final.

	Fase	**Multiplicación** en $\mathbb{F}_p$	**Multiplicación en** $\mathbb{F}_{p_{512}}$
BN	C.M.	$16487m_{640}$	$25761m_{512}$
	L.F.	$207m_{640}$	$323m_{512}$
	E.F.	$7422m_{640}$	$11597m_{512}$
	Total	$24116m_{640}$	$37681m_{512}$
BW-12	C.M.	$10847m_{640}$	$16949m_{512}$
	L.F	–	–
	E.F.	$8824m_{640}$	$13787m_{512}$
	Total	$19671m_{640}$	$\mathbf{30736m_{512}}$
KSS-18	C.M.	$13275m_{512}$	$13275m_{512}$
	L.F	$542m_{512}$	$542m_{512}$
	E.F	$23422m_{512}$	$23422m_{512}$
	Total	$37239m_{512}$	$37239m_{512}$
BLS-24	C.M.	$14873m_{512}$	$14873m_{512}$
	L.F		
	E.F	$27432m_{512}$	$27432m_{512}$
	Total	$42305m_{512}$	$42305m_{512}$

Tabla 5.12: Costo total del emparejamiento *óptimo ate* con 192 bits de seguridad

5.2.2. Versión paralela del emparejamiento óptimo ate

Aprovechando la existencia de las arquitecturas multinúcleo y las propiedades específicas de la función de Miller [Definición 4.3], Aranha *et al.* propusieron un método para la paralelización del computo de $f_{s,R}$, el cual se describe a continuación: primero se selecciona $s = 2^w s_1 + s_0$, donde $s_0 < 2^w$ y posteriormente, se aplica el Lema 4.1 (presentado en la sección Sección 4.2.1), para obtener:

$$f_{s,R} = f_{s1,R}^{2^w} \cdot f_{2^w,s_1R} \cdot f_{s_0,R} \cdot \ell_{2^w s_1 R, s_0 R}/v_{sR} \tag{5.1}$$

Si s_0 es un número relativamente pequeño, entonces el costo de la función de Miller $f_{s_0,R}$ se pude considerar desdeñable, al igual que el cálculo de las líneas en la Ecuación (5.1); por lo tanto, la función $f_{s,R}$ puede ser paralelizada, mediante el cómputo de $f_{s1,R}^{2^w}$ y $f_{2^w,s1R}$ en distintos procesadores.

Como se puede observar, el parámetro w debe ser seleccionado cuidadosamente con el objetivo de balancear el tiempo de cómputo entre las dos funciones de Miller. Los criterios bajo los cuales se selecciona w incluyen el peso de Hamming de s_1 (que determina el número de sumas en el ciclo de Miller para la primera función), y el costo de los w cuadrados que deben calcularse en $f_{s1,R}^{2^w}$, el

cual debe estar balanceado con el esfuerzo computacional requerido por la multiplicación escalar s_1R en la función $f_{2^w,s1R}$.

Cabe mencionar que no se ha podido encontrar ningún método efectivo para la paralelización de la exponenciación final, por lo cual, la siguiente sección se enfoca exclusivamente en la paralelización de la función de Miller. En el Apéndice C , se encuentran las Tablas C.1, C.2, C.3 y C.4 que muestran los resultados de aplicar dicho método a las distintas familias de curvas elípticas. A continuación se describe a detalle el procedimiento empleado en la familia de curvas BN.

Ejemplo sobre curvas BN

El emparejamiento *óptimo ate* sobre curvas BN requiere del cómputo de la función de Miller $f_{6z+2,Q}(P)$ [Sección 4.5.1]. Con base en la Tabla 5.1, en las familias de curvas Barreto-Naehrig se seleccionó el parámetro $z = 2^{158} - 2^{128} - 2^{68} + 1$, donde

$$s = 6z + 2 = 2^{160} + 2^{159} - 2^{130} - 2^{129} - 2^{70} - 2^{69} + 2^3,$$

se puede expresar como $s = 2^{69}(2^{91} + 2^{90} - 2^{61} - 2^{60} - 2^1 - 1) + 2^3$. A partir de la Ecuación (5.1), esta representación de s permite el cómputo del emparejamiento *óptimo ate* en dos núcleos, como se muestra a continuación:

$$\begin{aligned} &f_{2^{160}+2^{159}-2^{130}-2^{129}-2^{70}-2^{69}+2^3} \\ &= f^{2^{69}}_{2^{91}+2^{90}-2^{61}-2^{60}-2^1-1,R} \cdot f_{2^{69},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R} \cdot f_{8,R} \end{aligned}$$

cuyo factor de aceleración es de 1.34 (Tabla C.1). Para plataformas de más de dos núcleos, la Ecuación (5.1) se puede aplicar de manera recursiva, por ejemplo:

$$\begin{aligned} &f^{2^{69}}_{2^{91}+2^{90}-2^{61}-2^{60}-2^1-1,R} \\ &= f^{2^{69+46}}_{2^{45}+2^{44}-2^{15}-2^{14},R} \cdot f^{2^{69}}_{2^{46},[2^{45}+2^{44}-2^{15}-2^{14}]R} \cdot f^{2^{69}}_{-3,R}, \end{aligned}$$

además, dado que $2^{69} = 2^{32} \cdot 2^{37}$, utilizando el Lema 4.1(II) se obtiene que:

$$\begin{aligned} &f_{2^{69},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R} \cdot f_{8,R} \\ &= f^{2^{32}}_{2^{37},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R} \cdot f_{2^{32},[2^{128}+2^{127}-2^{98}-2^{97}-2^{38}-2^{37}]R} \cdot f_{8,R} \end{aligned}$$

De esta manera, las funciones racionales se pueden distribuir sobre cuatro núcleos con un factor de aceleración de 1.71. Finalmente, para una arquitectura de ocho núcleos, se obtienen las siguientes particiones:

$$\begin{aligned} &f^{2^{115}}_{2^{45}+2^{44}-2^{15}-2^{14},R} \cdot f^{2^{69}}_{-3,R} \\ &= f^{2^{146}}_{2^{14}+2^{13},R} \cdot f^{2^{115}}_{-2^{15}-2^{14},R} \cdot f^{2^{115}}_{2^{31},[2^{14}+2^{13}]R} \cdot f^{2^{69}}_{-3,R} \end{aligned}$$

$$\begin{aligned} &f^{2^{69}}_{2^{46},[2^{45}+2^{44}-2^{15}-2^{14}]R} \\ &= f^{2^{93}}_{2^{22},[2^{40}+2^{39}-2^{10}-2^9]R} \cdot f^{2^{69}}_{2^{24},[2^{62}+2^{61}-2^{32}-2^{31}]R} \end{aligned}$$

$$\begin{aligned} &f^{2^{32}}_{2^{37},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R} \\ &= f^{2^{50}}_{2^{19},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R} \cdot f^{2^{32}}_{2^{18},[2^{110}+2^{109}-2^{80}-2^{79}-2^{20}-2^{19}]R} \end{aligned}$$

$$f_{2^{32},[2^{128}+2^{127}-2^{98}-2^{97}-2^{38}-2^{37}]R} \cdot f_{8,R}$$
$$= f_{2^{17},[2^{128}+2^{127}-2^{98}-2^{97}-2^{38}-2^{37}]R}^{2^{15}} \cdot f_{2^{15},[2^{145}+2^{144}-2^{115}-2^{114}-2^{55}-2^{54}]R} \cdot f8, R$$

con un factor de aceleración de 1.88.

5.2.3. Comparación del emparejamiento *óptimo ate* (Versión Paralela)

Esta sección sólo se enfoca en presentar los resultados más relevantes, dejando en el Apéndice la descripción detallada del número de multiplicaciones que cada núcleo debe procesar, así como la aceleración obtenida conforme se aumenta el número de núcleos.

La Figura 5.1 muestra que las curvas con menor grado de encajamiento, son las que presentan un factor de aceleración mayor (BN y BW-12). Por otra parte, el dividir una función de Miller en dos, no implica dividir el número de operaciones a la mitad; las dificultades de paralelizar el algoritmo de Miller son tan altas que el factor de aceleración obtenido para 8 núcleos en curvas BN es de "2", el cual es el valor ideal para implementaciones en dos núcleos.

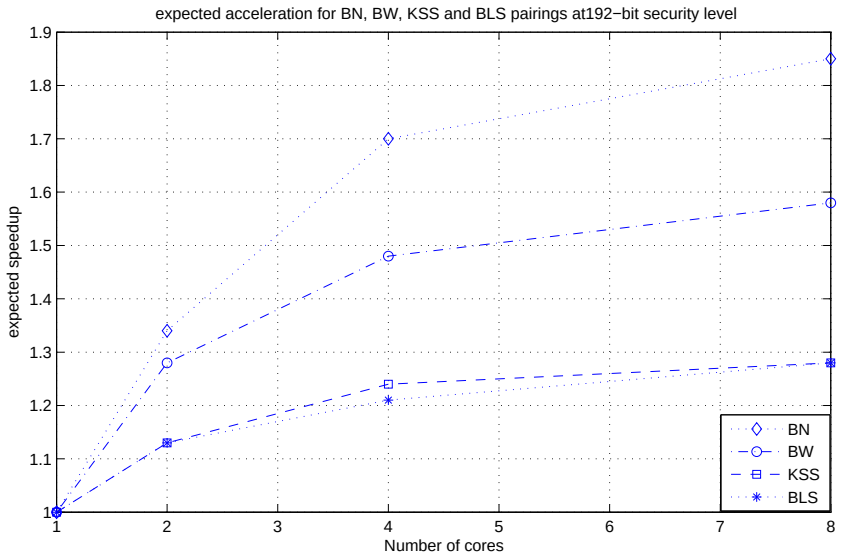


Figura 5.1: Aceleración estimada de la versión paralela del emparejamiento *óptimo ate* sobre las familias de curvas elípticas *amables* con los emparejamientos BN, BW-12, KSS-18 y BLS-24, con 192 bits de seguridad

Así mismo, la Tabla 5.13 muestra la comparación del costo de cómputo del emparejamiento *óptimo ate* entre las distintas familias de curvas elípticas, en términos de multiplicaciones de 512 bits, sobre 1, 2, 4 y 8 núcleos. Como se puede observar, las curvas BW-12 tienen la ventaja sobre las otras familias, independientemente del número de núcleos.

	Número de núcleos			
	1	**2**	**4**	**8**
BN	37358 m_{512}	27938 m_{512}	21992 m_{512}	20161 m_{512}
BW-12	**30736 $\mathbf{m_{512}}$**	**24098 $\mathbf{m_{512}}$**	**20731 $\mathbf{m_{512}}$**	**19464 $\mathbf{m_{512}}$**
KSS-18	36697 m_{512}	32480 m_{512}	29515 m_{512}	28543 m_{512}
BLS-24	42305 m_{512}	37400 m_{512}	35079 m_{512}	33004 m_{512}

Tabla 5.13: Comparación de la versión paralela del emparejamiento *óptimo ate*

5.3. Costo computacional del emparejamiento *óptimo de Weil*

De acuerdo con la definición de Vercauteren [Sección 4.5], los emparejamientos definidos bajo la metodología de Weil, sólo pueden ser *óptimos* en arquitecturas multinúcleo, debido a que requieren del cómputo de al menos dos funciones de Miller de igual magnitud. Además, en arquitecturas de dos núcleos la única forma de paralelizar el emparejamiento *óptimo de Weil* es que el numerador y el denominador se ejecuten independientemente en cada núcleo.

5.3.1. Paralelización del emparejamiento *óptimo de Weil*

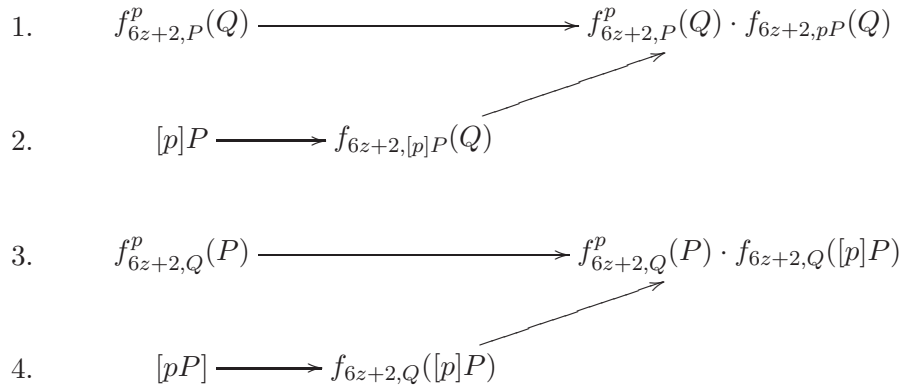
A continuación se describen los emparejamientos *óptimos de Weil* para las distintas familias de curvas elípticas (BN, BW-12, KSS-18 y BLS-24), los cuales fueron obtenidos directamente de la Ecuación (4.12). Es importante mencionar que en las siguientes secciones "P" denota un punto en el grupo abeliano $E(\mathbb{F}_p)$ y "Q" es un punto en $E'(\mathbb{F}_{p^{k/d}})$, ambos de orden primo r, donde E' es la curva enlazada de E.

Curvas BN

En el artículo [3], los autores propusieron dos versiones del emparejamiento *óptimo de Weil* sobre las curvas BN, enfocándose en una seguridad de 128 bits. Particularmente la versión a la que llamaron "emparejamiento β Weil" corresponde con el definido por la Ecuación (4.12), el cual se muestra a continuación:

$$\left(\frac{(f_{6z+2,P}\cdot \ell_{[6z+2]P,pP}\cdot \ell_{[6z+2+p]P,-p^2P})(Q)^p}{(f_{6z+2,Q}\cdot \ell_{[6z+2]Q,pQ}\cdot \ell_{[6z+2+p]Q,-p^2Q})(P)^p}\cdot\frac{(f_{6z+2,pP}\cdot \ell_{[6z+2]pP,p^2P}\cdot \ell_{[6z+2+p^2]P,-p^3P})(Q)}{(f_{6z+2,Q}\cdot \ell_{[6z+2]Q,pQ}\cdot \ell_{[6z+2+p]Q,-p^2Q})(pP)}\right)^{(p^6-1)(p^2+1)}$$

Sin tomar en cuenta las líneas $\ell_{[6z+2]R,pR}\cdot \ell_{[6z+2+p]R,-p^2R})$ para $R=\{P,Q\}$, el siguiente diagrama fue tomado de la referencia [3] y describe la ruta de ejecución en una arquitectura de cuatro núcleos.



En una arquitectura de ocho núcleos cada función de Miller $f_{6z+2,R}$ para $z = 2^{158} - 2^{128} - 2^{68} + 1.$, fue dividida en las funciones racionales

$$f_{2^{91}+2^{90}-2^{61}-2^{60}-2^1-1,R}^{2^{69}} \quad \text{y} \quad f_{2^{69},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R} \cdot f_{8,R},$$

a partir del método descrito en los emparejamientos *óptimos ate*.

Curvas BW-12

El emparejamiento *óptimo de Weil* sobre las curvas BW-12 está definido como se muestra a continuación:

$$\left(\frac{f_{z,Q}^p(P) \cdot f_{z,Q}([p]P)}{f_{z,P}^p(Q) \cdot f_{z,[p]P}(Q)} \right)^{(p^6-1)(p^2+1)}.$$

Una característica importante de las familias ciclotómicas es que $pP = zP$ para $P \in E(\mathbb{F}_p)[r]$, lo cual hace más eficiente su implementación. El siguiente diagrama ilustra la ruta de ejecución cuando las cuatro funciones presentes en el emparejamiento *óptimo de Weil* son computadas en una arquitectura de cuatro núcleos:

1. $f_{z,Q}(P) \longrightarrow f_{z,Q}^p(P) \longrightarrow f_{z,Q}^p(P) \cdot f_{z,Q}([p]P)$
2. $[p]P \longrightarrow f_{z,Q}([p]P)$
3. $f_{z,P}(Q) \longrightarrow f_{z,P}^p(Q) \longrightarrow f_{z,P}^p(Q) \cdot f_{z,[p]P}(Q)$
4. $[pP] \longrightarrow f_{z,[p]P}(Q)$

Considerando una arquitectura de ocho núcleos, cada una de las funciones $f_{z,R}$ para $R = \{P, Q\}$, es representada como el producto de dos funciones de Miller utilizando la estrategia descrita en la paralelización de los emparejamientos *óptimos ate*. De esta manera, de acuerdo con la Tabla C.1 del Apéndice C, $f_{z,R}$ para $z = -(2^{107} - 2^{105} - 2^{93} - 2^5)$ se divide en

$$f_{-(2^{53}-2^{51}-2^{39}),R}^{2^{54}} \cdot f_{2^5,R} \quad \text{y} \quad f_{2^{54},[-(2^{53}-2^{51}-2^{39})]R}.$$

Curvas KSS-18

El emparejamiento *optimo de Weil* correspondiente a la familia de curvas elípticas KSS con grado de encajamiento $k = 18$, definido por la Ecuación (4.12), es el siguiente:

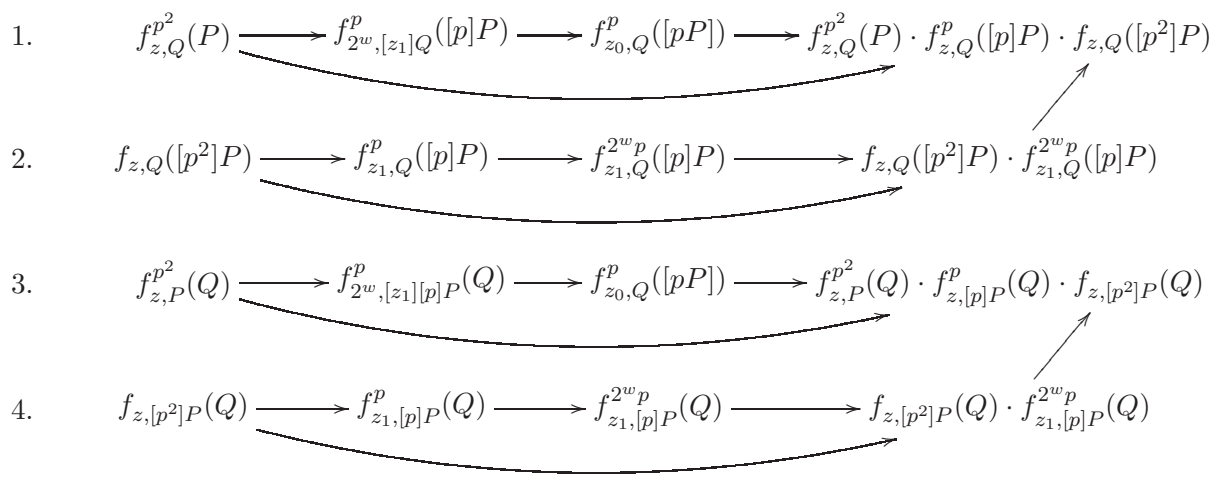
$$\left[\frac{(f_{z,Q} \cdot f_{3,Q}^p \cdot \ell_{[z]Q,[3p]Q})(P)^{p^2} \cdot (f_{z,Q} \cdot f_{3,Q}^p \cdot \ell_{[z]Q,[3p]Q})([p]P)^p \cdot (f_{z,Q} \cdot f_{3,Q}^p \cdot \ell_{[z]Q,[3p]Q})([p^2]P)}{(f_{z,P} \cdot f_{3,P}^p \cdot \ell_{[z]P,[3p]P})(Q)^{p^2} \cdot (f_{z,[p]P} \cdot f_{3,[p]P}^p \cdot \ell_{[xp]P,[3p^2]P})(Q)^p \cdot (f_{z,[p^2]P} \cdot f_{3,[p^2]P}^p \cdot \ell_{[xp^2]P,[3p^3]P})(Q)} \right]^{(p^9-1)(p^3+1)}.$$

Al igual que las otras familias de curvas elípticas, la paralelización del emparejamiento *óptimo Weil* es **directa** sobre arquitecturas de uno y dos núcleos. Sin embargo, para arquitecturas de más de dos núcleos, el punto importante a considerar son las seis funciones de Miller $f_{z,R}.$, para $R = P$ ó $R = Q$.

Particularmente en la implementación sobre una arquitectura de cuatro núcleos, el parámetro z se puede expresar como $z = 2^w z_1 + z_0$, de tal manera que la función $f_{z,R}$ puede ser computada haciendo uso del Lema 4.1, como se muestra en la Ecuación (5.1). Con base en la Tabla 5.1, si $z = 2^{64} - 2^{61} + 2^{56} - 2^{13} - 2^7$, una posible opción es fijar los parámetros w, z_1 y z_0 como:

$$w = 39 \qquad z_1 = 2^{25} - 2^{22} + 2^{17} \qquad z_0 = -2^{13} - 2^7.$$

Esta representación de z se aplica sobre dos de las seis funciones de Miller $f_{z,R}$. El siguiente diagrama ejemplifica la ruta de ejecución de cada núcleo:



Es importante mencionar que las seis funciones $(f^{p}_{3,R} \cdot \ell_{[z]R,[3p]R})^{p^i}$ y la exponenciación a $(p^9-1)\cdot(p^3+1)$, son implementadas al finalizar el proceso. Una observación interesante en el primer núcleo, es que la multiplicación escalar $[z_1]Q$ es obtenida a partir de la función $f^{p^2}_{z,Q}(P)$, sin ningún costo adicional.

Al igual que las curvas BW-12, en el caso de contar con una arquitectura de ocho núcleos, la mejor opción es dividir a cada una de las seis funciones de Miller en cuatro funciones racionales, utilizando la metodología descrita en los emparejamientos *óptimos ate*.

Curvas BLS-24

El emparejamiento *óptimo de Weil* definido para la familia de curvas BLS-24:

$$\left[\frac{f^{p^3}_{z,P}(Q) \cdot f^{p^2}_{z,[p]P}(Q) \cdot f^{p}_{z,[p^2]P}(Q) \cdot f_{z,[p^3]P}(Q)}{f^{p^3}_{z,Q}(P) \cdot f^{p^2}_{z,Q}([p]P) \cdot f^{p}_{z,Q}([p^2]P) \cdot f_{z,Q}([p^3]P)} \right]^{(p^{12}-1)\cdot(p^4+1)},$$

donde $[p]P = [z]P$, no permite muchas opciones de paralelización. La más sencilla y directa es la siguiente:

- 2 núcleos: Cada núcleo computa 4 funciones de Miller.
- 4 núcleos: Cada núcleo computa 2 funciones de Miller.
- 8 núcleos: Cada núcleo computa 1 función de Miller.

5.3.2. Comparación del emparejamiento *óptimo de Weil*

La Tabla 5.14 muestra un resumen del costo estimado de la implementación del emparejamiento *óptimo de Weil*, descrito previamente. Se estima que la implementación secuencial y multińucleo sobre curvas BW-12, sea la más eficiente.

	Número de núcleos			
	1	**2**	**4**	**8**
BN	98198 m_{512}	53690 m_{512}	27830 m_{512}	18409 m_{512}
BW-12	**64791 $\mathbf{m_{512}}$**	**35452 $\mathbf{m_{512}}$**	**18396 $\mathbf{m_{512}}$**	**11758 $\mathbf{m_{512}}$**
KSS-18	78128 m_{512}	44358 m_{512}	27025 m_{512}	18869 m_{512}
BLS-24	113313 m_{512}	62824 m_{512}	32401 m_{512}	16795 m_{512}

Tabla 5.14: Comparación del emparejamiento *óptimo de Weil* sobre distintas familias de curvas elípticas

5.4. Resultados

La Tabla 5.4 fue construida con el objetivo de llevar a cabo una comparación entre todas las estimaciones, tanto seriales como paralelas, de los emparejamientos óptimos considerados en este trabajo. Los factores de aceleración fueron calculados con respecto a la versión secuencial del emparejamiento *óptimo ate* sobre las curvas Barreto-Naehrig.

Como se puede observar, el emparejamiento *óptimo ate* sobre curvas BW-12 es el más eficiente en uno y dos núcleos, mientras que el emparejamiento *óptimo de Weil* en las mismas curvas, es el más eficiente en cuatro y ocho núcleos. Además, el factor de aceleración máximo obtenido en el estudio realizado es de 3.17 para ocho núcleos,

	Número de núcleos			
Aceleración estimada BN	**1**	**2**	**4**	**8**
Emp. Óptimo ate	1.00	1.34	1.70	1.85
Emp. Óptimo de Weil	0.38	0.70	1.34	2.03
Aceleración estimada BW12	**1**	**2**	**4**	**8**
Emp. Óptimo ate	**1.22**	**1.55**	1.80	1.91
Emp. Óptimo de Weil	0.58	1.05	**2.03**	**3.17**
Aceleración estimada KSS18	**1**	**2**	**4**	**8**
Emp. Óptimo ate	1.02	1.15	1.27	1.31
Emp. Óptimo de Weil	0.47	0.84	1.38	1.98
Aceleración estimada BLS24	**1**	**2**	**4**	**8**
Emp. Óptimo ate	0.88	0.99	1.07	1.13
Emp. Óptimo de Weil	0.33	0.60	1.15	2.22

Tabla 5.15: Estimación de la aceleración entre la versión paralela del emparejamiento *óptimo ate* y la versión paralela del emparejamiento *óptimo de Weil*. Todos estos factores fueron tomados con respecto a la versión secuencial del emparejamiento *óptimo ate* sobre curvas BN.

Capítulo 6

Conclusiones

La sabiduría humana está contenida
en estas dos palabras: Confiar y esperar

Alejandro Dumas

En esta tesis se llevó a cabo el análisis de los emparejamientos bilienales con 192 bits de seguridad y se propusieron dos métodos para el cálculo eficiente de la exponenciación final y la función *picadillo* hacia el grupo $\mathbb{G}_2$. Cabe mencionar que ambas propuestas están basadas en el método de *rejillas* que Vercauteren utilizó en [49] para la definición de emparejamientos *óptimos ate*, los cuales requieren de $\log_2(r)/\varphi(k)$ iteraciones del ciclo de Miller, donde $\varphi(\cdot)$ es la función indicatriz de Euler y k es el grado de encajamiento.

Para concluir con esta tesis, a continuación se hace un resumen de los principales resultados obtenidos, así como del trabajo que en un futuro puede ser desarrollado.

- En el cálculo de la exponenciación final se mostró que, para las distintas familias de curvas elípticas, existe un múltiplo $d'(z)$ de $d(z)$, donde $d(z) = \Phi_k(p(z))/r(z)$ y $r(z)$ no divide a $d'(z)$, tal que $g \mapsto g^{d'(z)}$ puede ser computado más eficientemente que $g \mapsto g^{d(z)}$. Para ello $d'(z)$ se representa en base $p(z)$ como $d'(z) = d'_0(z) + d'_1(z)p(z) + \cdots + d'_{\varphi(k)-1}(z)p(z)^{\varphi(k)-1}$.

- En cuanto al cálculo de la función *picadillo* hacia el grupo $\mathbb{G}_2$, se demostró a partir del Teorema 4.1, que existe un polinomio $h(w) = h_0 + h_1 w + \cdots + h_{\varphi(k)-1}w^{\varphi(k)-1} \in \mathbb{Z}[w]$ tal que todo punto $\tilde{Q} \in E'(\mathbb{F}_{p^{k/d}})$ puede ser proyectado a un punto Q' en el grupo $\mathbb{G}_2$ mediante el cómputo de $h(\psi(\tilde{Q}))$, donde $|h_i|^{\varphi(k)} \leq \#E'(\mathbb{F}_{p^{k/d}})/r$ para todo i.

- A partir de los puntos anteriores, concluimos que la solución óptima a los problemas de "reducción del ciclo de Miller", "exponenciación final" y "función *picadillo* hacia el grupo $\mathbb{G}_2$" están relacionadas por $\varphi(k)$.

- Por otra parte, con base en el estudio y análisis realizado sobre los emparejamientos bilineales, se llegó a la conclusión de que es equívoco pensar que, en una implementación, la mejor opción es trabajar con familias de curvas elípticas que mantienen la seguridad balanceada en ambos lados del emparejamiento.

Un claro ejemplo de esto último es la familia de curvas KSS-18, que de acuerdo con [20], es la ideal en una implementación con 192 bits de seguridad; sin embargo, hemos comprobado que las curvas BW-12 son superiores, al permitir una mayor eficiencia en el cómputo de los emparejamientos *óptimo ate* y *óptimo de Weil* con dicho nivel de seguridad.

- El cálculo de los emparejamientos bilineales depende de numerosos factores, lo cual implica que aún con los resultados obtenidos, nada nos absuelve de que exista otra familia de curvas elípticas ordinarias capaz de computar los emparejamientos bilineales con mayor eficiencia que la familia BW-12.
- La versión paralela del emparejamiento *óptimo de Weil* para las distintas familias de curvas elípticas (BN, BW-12, KSS-18, BLS-24), es más eficiente que la versión paralela del emparejamiento *óptimo ate* en arquitecturas de más de cuatro núcleos.
- El emparejamiento *óptimo de Weil* obtenido a partir de la Ecuación (4.12) no beneficia a las familias con alto grado de encajamiento, ya que el número de ciclos de Miller necesarios en el cómputo del emparejamiento aumenta conforme al grado de encajamiento.
- Los resultados presentados en esta tesis son "ideales", es necesario tener en cuenta que en una implementación están presentes otro tipo de factores como la sincronización de hilos.

6.1. Trabajo a futuro

- Es necesario realizar las estimaciones necesarias para la implementación con 256 bits de seguridad. Algunos trabajos como el de Costello *et al.* [17], estiman que las curvas BLS-24 son las más eficientes para el cálculo de los emparejamientos *óptimos ate* con dicho nivel de seguridad.
- Llevar a cabo las implementaciones necesarias para corroborar los resultados obtenidos en esta tesis.
- En el año 2006 Oliver Schirokauer en [44], enfocándose en las curvas BN, mostró que el problema del logaritmo discreto en $\mathbb{F}_p$ y $\mathbb{F}_{p^2}$ puede ser resuelto en menor tiempo si el número primo p tiene un peso de Hamming bajo. Además mencionó que estas ideas podrían extenderse al campo $\mathbb{F}_{p^{12}}$, reduciendo la seguridad en el grupo $\mathbb{G}_T$.

  En esta tesis no fueron considerados este tipo de ataques, de esta manera, es necesario realizar el análisis y estudio de los emparejamientos bilineales, suponiendo que el parámetro z ha sido elegido de manera aleatoria, lo cual asegura, en cierto modo, que el número primo $p = p(z)$ sea "aleatorio".

  Como consecuencia de esta selección, no pueden ser utilizados algunos algoritmos como el de Karabina [31] para el cálculo de cuadrados ciclotómicos. Por lo tanto, también es necesario realizar una nueva búsqueda de algoritmos para el cómputo eficiente de los emparejamientos bilineales.
- En altos niveles de seguridad como 256 bits, es recomendable definir otro tipo de emparejamientos *óptimos de Weil* que beneficien a las familias de curvas elípticas con alto grado de encajamiento, para ello se puede consultar la referencia [27].

Bibliografía

[1] Leonard M. Adleman and Ming-Deh A. Huang. Function Field Sieve Method for Discrete Logarithms over Finite Fields. *Inf. Comput.*, 151:5–16, May 1999.

[2] Diego Aranha, Koray Karabina, Patrick Longa, Catherine Gebotys, and Julio López. Faster Explicit Formulas for Computing Pairings over Ordinary Curves. In Kenneth Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 48–68. Springer Berlin / Heidelberg, 2011.

[3] Diego Aranha, Edward Knapp, Alfred Menezes, and Francisco. Rodriguez-Henriquez. Parallelizing the Weil and Tate Pairings. *Thirteenth IMA International Conference on Cryptography and Coding 2011 (to appear)*, 2011.

[4] Diego Aranha, Julio López, and Darrel Hankerson. High-Speed Parallel Software Implementation of the η_T Pairing. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010*, volume 5985 of *Lecture Notes in Computer Science*, pages 89–105. Springer Berlin / Heidelberg, 2010.

[5] Selcuk Baktir and Berk Sunar. Optimal Tower Fields. *IEEE Trans. Comput.*, 53:1231–1243, October 2004.

[6] Paulo Barreto, Ben Lynn, and Michael Scott. Constructing Elliptic Curves with Prescribed Embedding Degrees. In Stelvio Cimato, Giuseppe Persiano, and Clemente Galdi, editors, *Security in Communication Networks*, volume 2576 of *Lecture Notes in Computer Science*, pages 257–267. Springer Berlin / Heidelberg, 2003.

[7] Paulo Barreto, Ben Lynn, and Michael Scott. On the Selection of Pairing-Friendly Groups. In Mitsuru Matsui and Robert Zuccherato, editors, *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*, pages 17–25. Springer Berlin / Heidelberg, 2004.

[8] Paulo Barreto and Michael Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer Berlin / Heidelberg, 2006.

[9] Paulo S. L. M. Barreto, Michael Naehrig, Geovandro C. C. F. Pereira, and Marcos A. Simplício Jr. A Family of Implementation-Friendly BN Elliptic Curves, 2010. geovandro@larc.usp.br 14850 received 3 Aug 2010, last revised 29 Aug 2010.

[10] Naomi Benger and Michael Scott. Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography. In M. Hasan and Tor Helleseth, editors, *Arithmetic of Finite Fields*, volume 6087 of *Lecture Notes in Computer Science*, pages 180–195. Springer Berlin / Heidelberg, 2010.

[11] Jean-Luc Beuchat, Jorge González-Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez, and Tadanori Teruya. High-Speed Software Implementation of the Optimal Ate Pairing over BarretoâNaehrig Curves. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *Pairing-Based Cryptography - Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, pages 21–39. Springer Berlin / Heidelberg, 2010.

[12] Jean-Luc Beuchat, Emmanuel López-Trejo, Luis Martínez-Ramos, Shigeo Mitsunari, and Francisco Rodríguez-Henríquez. Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves. Cryptology ePrint Archive, Report 2009/276, 2009. http://eprint.iacr.org/.

[13] Dan Boneh and Matthew Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[14] Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weil Pairing. In *ASIACRYPT '01: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, pages 514–532, London, UK, 2001. Springer-Verlag.

[15] Friederike Brezing and Annegret Weng. Elliptic Curves Suitable for Pairing Based Cryptography. *Designs, Codes and Cryptography*, 37:133–141, 2005.

[16] Jaewook Chung and Anwar Hasan. Asymmetric Squaring Formulae. *Computer Arithmetic, IEEE Symposium on*, 0:113–122, 2007.

[17] Craig Costello, Kristin Lauter, and Michael Naehrig. Attractive Subfamilies of BLS Curves for Implementing High-Security Pairings. Cryptology ePrint Archive, Report 2011/465, 2011. http://eprint.iacr.org/.

[18] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, pages 644–654.

[19] David Freeman. Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465. Springer Berlin / Heidelberg, 2006.

[20] David Freeman, Michael Scott, and Edlyn Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *Journal of Cryptology*, 23:224–280, 2010.

[21] Laura Fuentes-Castaneda, Edward Knapp, and Francisco Rodríguez-Henríquez. Faster Hashing to $\mathbb{G}_2$. Presented in SAC, 2011.

[22] Steven Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves. *Journal of Cryptology*, 24:446–469, 2011.

[23] Shafi Goldwasser and Joe Kilian. Primality Testing Using Elliptic Curves, journal = J. ACM, volume = 46, issue = 4, month = July, issn = 0004-5411, pages = 450–472, numpages = 23, acmid = 320213, publisher = ACM, address = New York, NY, USA, year = 1999.

[24] Robert Granger and Michael Scott. Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions. In Phong Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 209–223. Springer Berlin / Heidelberg, 2010.

[25] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[26] F. Hess, N. Smart, Frederik Vercauteren, and Technische Universität Berlin. The Eta Pairing Revisited. *IEEE Transactions on Information Theory*, 52:4595–4602, 2006.

[27] Florian Hess. Pairing Lattices. In Steven Galbraith and Kenneth Paterson, editors, *Pairing-Based Cryptography - Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 18–38. Springer Berlin / Heidelberg, 2008.

[28] Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman. *An Introduction to Mathematical Cryptography*. Springer Publishing Company, Incorporated, 1 edition, 2008.

[29] Olivos Jorge. On Vectorial Addition Chains. *J. Algorithms*, 2(1):13–21.

[30] Ezekiel Kachisa, Edward Schaefer, and Michael Scott. Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field. In Steven Galbraith and Kenneth Paterson, editors, *Pairing-Based Cryptography - Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer Berlin / Heidelberg, 2008.

[31] Koray Karabina. Squaring in cyclotomic subgroups. Cryptology ePrint Archive, Report 2010/542, 2010. http://eprint.iacr.org/.

[32] Neal Koblitz and Alfred Menezes. Pairing-Based Cryptography at High Security Levels. In Nigel Smart, editor, *Cryptography and Coding*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36. Springer Berlin / Heidelberg, 2005.

[33] Serge Lang. Algebra. Springer, 2002.

[34] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[35] Rudolf Lidl and Harald Niederreiter. *Finite Fields (Encyclopedia of Mathematics and its Applications)*. Cambridge University Press, October 1996.

[36] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, New York, NY, USA, 1991. ACM.

[37] Victor Miller. The Weil Pairing, and Its Efficient Calculation. *Journal of Cryptology*, 17:235–261, 2004.

[38] H. Minkowski. *Geometrie der Zahlen*. Leipzig und erlin, Druck and Verlag von B.G. Teubner, 1910.

[39] Michael Naehrig, Ruben Niederhagen, and Peter Schwabe. New Software Speed Records for Cryptographic Pairings. Cryptology ePrint Archive, Report 2010/186, 2010. http://eprint.iacr.org/.

[40] Paul C. Van Oorschot and Michael J. Wiener. Parallel Collision Search with Cryptanalytic Applications. *Journal of Cryptology*, pages 1–28, 1996.

[41] Luis J Dominguez Perez, Ezekiel J Kachisa, and Michael Scott. Implementing Cryptographic Pairings: A Magma Tutorial. Cryptology ePrint Archive, Report 2009/072, 2009. http://eprint.iacr.org/.

[42] J. Pollard. Monte Carlo methods for Index Computation (mod p). *Mathematics of Computation*, 32:918–924, 1978.

[43] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, journal = Commun. ACM, volume = 21, number = 2, issn = 0001-0782, pages = 120–126, doi = http://doi.acm.org/10.1145/359340.359342, publisher = ACM, address = New York, NY, USA, year = 1978.

[44] Oliver Schirokauer. The Number Field Sieve for Integers of Low Weight. Cryptology ePrint Archive, Report 2006/107, 2006. http://eprint.iacr.org/.

[45] Michael Scott. Implementing Cryptographic Pairings. In Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto, editors, *Pairing-Based Cryptography - Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 177–196. Springer, 2007.

[46] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis Dominguez Perez, and Ezekiel Kachisa. On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves. In Hovav Shacham and Brent Waters, editors, *Pairing-Based Cryptography - Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*, pages 78–88. Springer Berlin / Heidelberg, 2009.

[47] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa. Fast Hashing to G2 on Pairing Friendly Curves. Cryptology ePrint Archive, Report 2008/530, 2008. http://eprint.iacr.org/.

[48] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, New York, NY, USA, 2005.

[49] Frederik Vercauteren. Optimal Pairings. *IEEE Trans. Inf. Theor.*, 56:455–461, January 2010.

[50] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, 2003.

Apéndice A

Exponenciación final sobre Curvas Freeman y KSS-8

A.1. Curvas Freeman

Las curvas Freeman [19] tienen grado de encajamiento $k = 10$ y están parametrizadas por z como se muestra a continuación:

$$r = r(z) = 25z^4 + 25z^3 + 15z^2 + 5z + 1$$
$$p = p(z) = 25z^4 + 25z^3 + 25z^2 + 10z + 3.$$

Para $d = \Phi_{10}(p)/r = (p^4 - p^3 + p^2 - p + 1)/r$ construimos la matriz M de dimensión 4×16, de la siguiente manera:

$$\begin{bmatrix} d(z) \\ zd(z) \\ 5z^2d(z) \\ 5x^3d(z) \end{bmatrix} = M \left(\begin{bmatrix} 1 \\ p(z) \\ p(z)^2 \\ p(z)^3 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ z \\ z^2 \\ z^3 \end{bmatrix} \right).$$

Los coeficientes de los polinomios en las filas de la matriz M forman la base de la *rejilla* L. Después de ejecutar el algoritmo LLL obtenemos el siguiente vector:

$$[1, -2, 0, -5, -1, -4, -5, -5, 1, 3, 5, 5, 2, 5, 5, 5],$$

el cual corresponde al múltiplo

$$d'(z) = (5z^3 + 5z^2 + 3z + 1)d(z) = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \lambda_3 p^3,$$

donde

$$\lambda_0(z) = 1 - 2z - 5z^3$$
$$\lambda_1(z) = -1 - 4z - 5z^2 - 5z^3$$
$$\lambda_2(z) = 1 + 3z + 5z^2 + 5z^3$$
$$\lambda_3(z) = 2 + 5z + 5z^2 + 5z^3,$$

De esta manera, para $g \in \mathbb{F}_{p^k}$, $g \mapsto g^{d'}$ puede ser computado en tres pasos:

1. Se calcula la cadena:

$$g \mapsto g^z \mapsto g^{2z} \mapsto g^{4z} \mapsto g^{5z} \mapsto g^{5z^2} \mapsto g^{5z^3},$$

2. Posteriormente se calculan los valores temporales A, B, C, D, como se muestra a continuación:

$$\begin{aligned} A &= g^{5z^3} \cdot g^{2z}, & B &= A \cdot g^{5z^2}, \\ C &= g^{2z} \cdot g, & D &= B \cdot g^z \cdot f, \end{aligned}$$

3. Finalmente, a partir de esto valores se calcula $g^{d'}$ como:

$$g^{d'} = [A^{-1} \cdot f] \cdot [B^{-1} \cdot C^{-1}]^p \cdot [D]^{p^2} \cdot [C \cdot D]^{p^3},$$

El costo total de computar $g^{d'}$ es de 3 exponenciaciones por z, 12 multiplicaciones en el campo $\mathbb{F}_{p^k}$ y 2 cuadrados en el grupo ciclotómico $\mathbb{G}_{\Phi_{10}(p)}$.

A.2. Curvas KSS-8

La familia de curvas elípticas KSS con grado de encajamiento $k = 8$ está parametrizada como:

$$\begin{aligned} r = r(z) &= \frac{1}{450}(z^4 - 8z^2 + 25), \\ p = p(z) &= \frac{1}{180}(z^6 + 2z^5 - 3z^4 + 8z^3 - 15z^2 - 82z + 125) \end{aligned}$$

y al igual que la familia BN, define curvas elípticas con orden primo r, es decir, $\#E(\mathbb{F}_p) = r$. Aplicando el método descrito en la Sección 4.7, se construye la matriz M de dimensión 4×24, como se muestra a continuación:

$$\begin{bmatrix} 6d(z) \\ (6/5)zd(z) \\ (6/5)z^2d(z) \\ (6/5)z^3d(z) \end{bmatrix} = M \left(\begin{bmatrix} 1 \\ p(z) \\ p(z)^2 \\ p(z)^3 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ z \\ z^2 \\ z^3 \\ z^4 \\ z^5 \end{bmatrix} \right).$$

Las filas de la matriz M corresponden con los múltiplos de $d(z) = \Phi_8(p(z))/r(z)$. Nuevamente los coeficientes de los polinomios en las filas de M forman la base de una *rejilla* L, de la cual, el vector en L con menor norma euclidiana corresponde al múltiplo $d'(z)$ de $d(z)$, definido como:

$$d'(z) = \frac{6z}{5}d(z) = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \lambda_3 p^3$$

para

$$\begin{aligned} \lambda_0 &= 2z^4 + 4z^3 + 5z^2 + 38z - 25 \\ \lambda_1 &= -z^5 - 2z^4 - z^3 - 16z^2 + 20z + 36 \\ \lambda_2 &= z^4 + 2z^3 - 5z^2 + 4z - 50 \\ \lambda_4 &= 3z^3 + 6z^2 + 15z + 72. \end{aligned}$$

El cálculo de $g^{d'}$ puede ser realizado a través del método de Scott *et al.* [46]. Primero se escribe $g^{d'}$ como:

$$g^{d'} = y_0^1\ y_1^2\ y_2^3\ y_3^4\ y_4^5\ y_5^6\ y_6^{15}\ y_7^{16}\ y_8^{20}\ y_9^{25}\ y_{10}^{36}\ y_{11}^{38}\ y_{12}^{50}\ y_{13}^{72}$$

donde

$$
\begin{aligned}
y_0 &= (1/g^{z^5} \cdot 1/g^{z^3})^p \cdot (g^{z^4})^{p^2} \\
y_1 &= g^{z^4} \cdot (1/g^{z^4})^p \cdot (g^{z^3})^{p^2} \\
y_2 &= (g^{z^3})^{p^3} \\
y_3 &= g^{z^3} \cdot (g^z)^{p^2} \\
y_4 &= g^{z^2} \cdot (g^z)^{p^2} \\
y_5 &= (g^{z^2})^{p^3} \\
y_6 &= (g^z)^{p^3} \\
y_7 &= (1/g^{z^2})^p \\
y_8 &= (g^z)^p \\
y_9 &= 1/g \\
y_{10} &= g^p \\
y_{11} &= g^z \\
y_{12} &= (1/g)^{p^2} \\
y_{13} &= g^{p^3}
\end{aligned}
$$

Estos valores temporales son computados a partir de g, g^z, ..., g^{z^5} utilizando multiplicaciones en $\mathbb{F}_{p^k}$ y operadores de Frobenius. Posteriormente se encuentra la cadena de adición que contenga las potencias de las variables temporales y_i, para lo cual es necesario incluir el número 10, como se muestra a continuación:

$$\{1, 2, 3, 4, 5, 6, \underline{10}, 15, 16, 20, 25, 36, 38, 50, 72\}.$$

Finalmente, a partir de esta cadena de adición y de los valores temporales y_i, es posible calcular $g^{d'}$ utilizando el método de Olivos [29], con un costo de 5 exponenciaciones por z, 26 multiplicaciones en $\mathbb{F}_{p^k}$ y 7 cuadrados en el grupo ciclotómico $\mathbb{G}_{\Phi_8(p)}$-

Apéndice B

Función *picadillo* hacia el grupo $\mathbb{G}_2$ sobre Curvas Freeman y KSS-8

B.1. Curvas Freeman

Las curvas Freeman forman parte de las familias dispersas de curvas elípticas [20] y su principal característica es que no cuentan con un discriminante CM fijo, por lo que el algoritmo propuesto no puede ser aplicado directamente a esta familia de curvas elípticas. Sin embargo, es posible utilizar un método similar al de la exponenciación final, calculando los múltiplos $c(z)$, $zc(z)$, $z^2c(z)$, $z^3c(z)$.

El resultado fue la siguiente cadena de adición correspondiente al múltiplo $h(a) = \lambda_0 + \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3$ de c, donde

$$\begin{aligned}
\lambda_0(z) &= 10z^3 + 5z^2 + 4z + 1\\
\lambda_1(z) &= -3z\\
\lambda_2(z) &= -10z^3 - 10z^2 - 8z - 3\\
\lambda_3(z) &= -5z^3 - 5z^2 - z\\
\lambda_4(z) &= -5z^3 + 2.
\end{aligned}$$

Utilizando la cadena de adición $\{1, 2, 3, 4, 5, 8, 10\}$, se puede calcular $h(a) \cdot \tilde{Q}$ utilizando 14 sumas de puntos, 4 doblados de puntos, 3 multiplicaciones escalares por z y 4 funciones ψ.

B.2. Curvas KSS-8

Las curvas KSS-8 tienen una curva enlazada E' de grado 4, donde el grupo finito $E'(\mathbb{F}_{p^2})$ tiene orden

$$\tilde{n}(z) = \frac{1}{72}(z^8 + 4z^7 + 6z^6 + 36z^5 + 34z^4 - 84z^3 + 486z^2 + 620z + 193)r(z).$$

Sea $c(z) = \tilde{n}(z)/r(z)$ después de realizar el trabajo descrito en la Sección 4.8, encontramos que el número entero a tal que $\psi(\tilde{Q}) = a\tilde{Q}$ para todo $\tilde{Q} \in E'(\mathbb{F}_{p^2})$, está definido como:

$$\begin{aligned}
a = \frac{1}{184258800}\big(&- 52523z^{11} - 174115z^{10} + 267585z^9 - 193271z^8\\
&- 325290z^7 + 15093190z^6 - 29000446z^5 - 108207518z^4\\
&+ 235138881z^3 + 284917001z^2 - 811361295z - 362511175\big).
\end{aligned}$$

Construyendo la *rejilla* correspondiente encontramos a la matriz

$$\left[\begin{array}{c|ccc} c(z) & 0 & 0 & 0 \\ -a(z) & 1 & 0 & 0 \\ -a(z)^2 & 0 & 1 & 0 \\ -a(z)^3 & 0 & 0 & 1 \end{array}\right]$$

encontramos que el vector con la menor norma euclidiana es el correspondiente al múltiplo

$$h(a) = \frac{1}{75}(z^2 - 25)c(z) = \lambda_0 + \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3$$

de c tal que $\lambda = (\lambda_0, \lambda_1, \lambda_2, \lambda_3) = (-z^2 - z, z - 3, 2z + 6, -2z - 4)$.

El cálculo de $h(a) \cdot \tilde{Q}$ es realizado de la siguiente manera: se computa $Q \mapsto zQ \mapsto (z+1)Q \mapsto (z^2+z)Q$ y $Q \mapsto 2Q \mapsto 4Q$, posteriormente se calculan los valores

$$\begin{aligned} \lambda_0 Q &= -(z^2 + z)Q \\ \lambda_1 Q &= (z+1)Q - 4Q \\ \lambda_2 Q &= 2(z+1)Q + 4Q \\ \lambda_3 Q &= -2(z+1)Q - 2Q \end{aligned}$$

y finalmente se calcula

$$h(a)Q = \lambda_0 Q + \psi(\lambda_1 Q) + \psi^2(\lambda_2 Q) + \psi^3(\lambda_3 Q)$$

con un costo total de 7 suma de puntos, 3 doblados de puntos, 2 multiplicaciones escalares por z y 3 funciones ψ.

Apéndice C

Resultados. Versión paralela del emparejamiento *óptimo ate*

Con el objetivo de llevar a cabo una implementación paralela de los emparejamientos *óptimos ate*, en la Sección 5.2.2 se describió el método propuesto por Aranha *et al.*, en el cual se toma ventaja de las propiedades de la función de Miller $f_{s,R}$, para expresarla como el producto de funciones racionales de menor longitud. Las dos principales desventajas de este método son:

- Esta representación de la función de Miller requiere del cómputo de operaciones adicionales. De tal manera que si la función $f_{s,R}$ tiene un costo c_f y es representada como el producto de n funciones racionales, el costo de cada una de estas funciones racionales es mayor que c_f/n.

- En el cómputo de los emparejamientos *óptimos ate*, la exponenciación final es el cuello de botella, debido principalmente a su alto costo y a que no se ha encontrado un método eficiente de paralelización.

En este apéndice se han incluido los resultados obtenidos de aplicar el método de Aranha *et al.* sobre las familias de curvas elípticas en las cuales se enfocó este trabajo (BN, BW-12, KSS-18 y BLS-24).

# de Núcleo	F. de Miller	Costo de F. de Miller	Costo Exp. Final	Costo Total	Aceleración
Secuencial					
Núcleo 1:	$f_{2^{160}+2^{159}-2^{130}-2^{129}-2^{70}-2^{69}+2^3,R}$	$16487m_{640}$	$7422m_{640}$	$23909m_{640}$	1.0
Costo en 2 núcleos					
Núcleo 1:	$f^{2^{69}}_{2^{91}+2^{90}-2^{61}-2^{60}-2^1-1,R}$	$10404m_{640}$			
Núcleo 2:	$f_{2^{69},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R} \cdot f_{8,R}$	$9185m_{640}$			
Costo estimado:		$10458m_{640}$	$7422m_{640}$	17880M	1.34
Costo en 4 núcleos					
Núcleo 1:	$f^{2^{115}}_{2^{45}+2^{44}-2^{15}-2^{14},R} \cdot f^{2^{69}}_{-3,R}$	$6491m_{640}$			
Núcleo 2:	$f^{2^{69}}_{2^{46},[2^{45}+2^{44}-2^{15}-2^{14}]R}$	$6481m_{640}$			
Núcleo 3:	$f^{2^{32}}_{2^{37},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R}$	$6177m_{640}$			
Núcleo 4:	$f_{2^{32},[2^{128}+2^{127}-2^{98}-2^{97}-2^{38}-2^{37}]R} \cdot f_{8,R}$	$6262m_{640}$			
Costo estimado:		$6653m_{640}$	$7422m_{640}$	14075M	1.70
Costo en 8 núcleos					
Núcleo 1:	$f^{2^{146}}_{2^{14}+2^{13},R} \cdot f^{2^{115}}_{-2^{15}-2^{14},R}$	$5003m_{640}$			
Núcleo 2:	$f^{2^{115}}_{2^{31},[2^{14}+2^{13}]R} \cdot f^{2^{69}}_{-3,R}$	$5103m_{640}$			
Núcleo 3:	$f^{2^{93}}_{2^{22},[2^{40}+2^{39}-2^{10}-2^9]R}$	$4264m_{640}$			
Núcleo 4:	$f^{2^{69}}_{2^{24},[2^{62}+2^{61}-2^{32}-2^{31}]R}$	$4638m_{640}$			
Núcleo 5:	$f^{2^{50}}_{2^{19},[2^{91}+2^{90}-2^{61}-2^{60}-2^1-1]R}$	$4593m_{640}$			
Núcleo 6:	$f^{2^{32}}_{2^{18},[2^{110}+2^{109}-2^{80}-2^{79}-2^{20}-2^{19}]R}$	$4676m_{640}$			
Núcleo 7:	$f^{2^{15}}_{2^{17},[2^{128}+2^{127}-2^{98}-2^{97}-2^{38}-2^{37}]R}$	$4750m_{640}$			
Núcleo 8:	$f_{2^{15},[2^{145}+2^{144}-2^{115}-2^{114}-2^{55}-2^{54}]R} \cdot f8, R$	$4919m_{640}$			
Costo estimado:		$5481m_{640}$	$7422m_{640}$	$12903m_{640}$	1.85

Tabla C.1: Aceleración estimada del emparejamiento *óptimo ate* con 192 bits de seguridad sobre las curvas BN parametrizadas por $z = 2^{158} - 2^{128} - 2^{68} + 1$.

# de Núcleo	F. de Miller	Costo de F. de Miller	Costo Exp. Final	Costo Total	Aceleración
Secuencial					
Núcleo 1:	$f_{-(2^{107}-2^{105}-2^{93}-2^5),R}$	$10847m_{640}$	$8824m_{640}$	$19671m_{640}$	1.0
Costo en 2 núcleos					
Núcleo 1:	$f^{2^{54}}_{-(2^{53}-2^{51}-2^{39}),R} \cdot f_{2^5,R}$	$6545m_{640}$			
Núcleo 2:	$f_{2^{54},[-(2^{53}-2^{51}-2^{39})]R}$	$6494m_{640}$			
Costo estimado:		$6599m_{640}$	$8824m_{640}$	$15423m_{640}$	1.28
Costo en 4 núcleos					
Núcleo 1:	$f^{2^{80}}_{-(2^{27}-2^{25}-2^{13}),R} \cdot f_{2^5,R}$	$4257m_{640}$			
Núcleo 2:	$f^{2^{54}}_{2^{26},[-2^{27}+2^{25}+2^{13}]R}$	$3865m_{640}$			
Núcleo 3:	$f^{2^{26}}_{2^{28},[-2^{53}+2^{51}+2^{39}]R}$	$4275m_{640}$			
Núcleo 4:	$f_{2^{26},[-2^{81}+2^{79}+2^{67}]R}$	$4282m_{640}$			
Costo estimado:		$4444m_{640}$	$8824m_{640}$	$13268m_{640}$	1.48
Costo en 8 núcleos					
Núcleo 1:	$(f^{2^{21}}_{-2^6+2^4,R} \cdot f_{2^{13},R})^{2^{80}}$	$3198m_{640}$			
Núcleo 2:	$f^{2^{80}}_{2^{21},[-2^6+2^4]R}$	$3199m_{640}$			
Núcleo 3:	$f^{2^{67}}_{2^{13},[-2^{27}+2^{25}+2^{13}]R} \cdot f_{2^5,R}$	$3182m_{640}$			
Núcleo 4:	$f^{2^{54}}_{2^{13},[-2^{40}+2^{38}+2^{26}]R}$	$2838m_{640}$			
Núcleo 5:	$f^{2^{39}}_{2^{15},[-2^{53}+2^{51}+2^{39}]R}$	$3131m_{640}$			
Núcleo 6:	$f^{2^{26}}_{2^{13},[-2^{68}+2^{66}+2^{54}]R}$	$3090m_{640}$			
Núcleo 7:	$f^{2^{13}}_{2^{13},[-2^{81}+2^{79}+2^{67}]R}$	$3207m_{640}$			
Núcleo 8:	$f_{2^{13},[-2^{94}+2^{92}+2^{80}]R}$	$3255m_{640}$			
Costo estimado:		$3633m_{640}$	$8824m_{640}$	$12457m_{640}$	1.58

Tabla C.2: Aceleración estimada del emparejamiento *óptimo ate* con 192 bits de seguridad sobre las curvas BW-12 parametrizadas por $z = -(2^{107} - 2^{105} - 2^{93} - 2^5)$

# de Núcleo	F. de Miller	Costo de F. de Miller	Costo Exp. Final	Costo Total	Aceleración
Secuencial					
Núcleo 1:	$f_{2^{64}-2^{61}+2^{56}-2^{13}-2^7,R}$	$13275m_{512}$	$23422m_{512}$	$36697m_{512}$	1.0
Costo en 2 núcleos					
Núcleo 1:	$f^{2^{39}}_{2^{25}-2^{22}+2^{17},R} \cdot f_{-2^{13}-2^7,R}$	$8950m_{512}$			
Núcleo 2:	$f_{2^{39},[2^{25}-2^{22}+2^{17}]R}$	$8889m_{512}$			
Costo estimado:		$9058m_{512}$	$23422m_{512}$	$32480m_{512}$	1.13
Costo en 4 núcleos					
Núcleo 1:	$f^{2^{43}}_{2^{21}-2^{18}+2^{13},R}$	$5568m_{512}$			
Núcleo 2:	$f^{2^{39}}_{2^4,[2^{21}-2^{18}+2^{13}]R} \cdot f_{-2^{13}-2^7,R}$	$5506m_{512}$			
Núcleo 3:	$f^{2^{19}}_{2^{20},[2^{25}-2^{22}+2^{17}]R}$	$5676m_{512}$			
Núcleo 4:	$f_{2^{19},[2^{45}-2^{42}+2^{37}]R}$	$5769m_{512}$			
Costo estimado:		$6093m_{512}$	$23422m_{512}$	$29515m_{512}$	1.24
Costo en 8 núcleos					
Núcleo 1:	$f^{2^{54}}_{2^{10}-2^7+2^2,R}$	$3654m_{512}$			
Núcleo 2:	$f^{2^{43}}_{2^{11},[2^{10}-2^7+2^2]R}$	$3840m_{512}$			
Núcleo 3:	$f^{2^{39}}_{2^4,[2^{21}-2^{18}+2^{13}]R}$	$2820m_{512}$			
Núcleo 4:	$f_{-2^{13}-2^7,R}$	$2578m_{512}$			
Núcleo 5:	$f^{2^{29}}_{2^{10},[2^{25}-2^{22}+2^{17}]R}$	$3936m_{512}$			
Núcleo 6:	$f^{2^{19}}_{2^{10},[2^{35}-2^{32}+2^{27}]R}$	$4116m_{512}$			
Núcleo 7:	$f^{2^{10}}_{2^9,[2^{45}-2^{42}+2^{37}]R}$	$4122m_{512}$			
Núcleo 8:	$f_{2^{10},[2^{54}-2^{51}+2^{46}]R}$	$4365m_{512}$			
Costo estimado:		$5121m_{512}$	$23422m_{512}$	$28543m_{512}$	1.28

Tabla C.3: Aceleración estimada del emparejamiento *óptimo ate* con 192 bits de seguridad sobre las curvas KSS-18 parametrizadas por $z = 2^{64} - 2^{61} + 2^{56} - 2^{13} - 2^7$.

# de Núcleo	F. de Miller	Costo de F. de Miller	Costo Exp. Final	Costo Total	Aceleración
Secuencial					
Núcleo 1:	$f_{-2^{48}+2^{27}-2^{24}+2^{19}-1,R}$	$14873m_{512}$	$27432m_{512}$	$42305m_{512}$	1.0
Costo en 2 núcleos					
Núcleo 1:	$f^{2^{19}}_{-2^{29}+2^8-2^5+1,R}$	$9806m_{512}$			
Núcleo 2:	$f_{2^{19},[-2^{29}+2^8-2^5+1]R}$	$7505m_{512}$			
Costo estimado:		$9968m_{512}$	$27432m_{512}$	$37400m_{512}$	1.13
Costo en 4 núcleos					
Núcleo 1:	$f^{2^{28}}_{-2^{20},R}$	$6758m_{512}$			
Núcleo 2:	$(f_{2^9,[-2^{20}]R} \cdot f_{2^8-2^5+1,R})^{2^{19}}$	$7161m_{512}$			
Núcleo 3:	$f^{2^9}_{2^{10},[-2^{29}+2^8-2^5+1]R}$	$5274m_{512}$			
Núcleo 4:	$f_{2^9,[-2^{39}+2^{18}-2^{15}+2^{10}]R}$	$5175m_{512}$			
Costo estimado:		$7647m_{512}$	$27432m_{512}$	$35079m_{512}$	1.21
Costo en 8 núcleos					
Núcleo 1:	$f^{2^{38}}_{-2^{10},R}$	$4158m_{512}$			
Núcleo 2:	$f^{2^{28}}_{2^{10},[-2^{10}]R}$	$4428m_{512}$			
Núcleo 3:	$f^{2^{19}}_{2^9,[-2^{20}]R}$	$4438m_{512}$			
Núcleo 4:	$f^{2^{19}}_{2^8-2^5+1,R}$	$3354m_{512}$			
Núcleo 5:	$f^{2^{14}}_{2^5,[-2^{29}+2^8-2^5+1]R}$	$3974m_{512}$			
Núcleo 6:	$f^{2^9}_{2^5,[-2^{34}+2^{13}-2^{10}+2^5]R}$	$4109m_{512}$			
Núcleo 7:	$f^{2^4}_{2^5,[-2^{39}+2^{18}-2^{15}+2^{10}]R}$	$4244m_{512}$			
Núcleo 8:	$f_{2^4,[-2^{44}+2^{23}-2^{20}+2^{15}]R}$	$4010m_{512}$			
Costo estimado:		$5572m_{512}$	$27432m_{512}$	$33004m_{512}$	1.28

Tabla C.4: Aceleración estimada del emparejamiento *óptimo ate* con 192 bits de seguridad sobre las curvas BLS-24 parametrizadas por $z = -2^{48} + 2^{27} - 2^{24} + 2^{19} - 1$