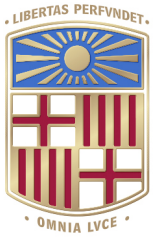


UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Esquemes de compartició de secrets amb corbes el·líptiques

Autor: Adrián Gutiérrez Silva

Director: Dr. Luís Víctor Dieulefait
Realitzat a: Departament d' Àlgebra

Barcelona, 17 de gener de 2024

Abstract

In this thesis, we provide a didactic introduction to pairing-based cryptography with elliptic curves, following the premises and methodologies outlined in Lawrence C. Washington's book *Elliptic Curves, Number Theory, and Cryptography*. We introduce the algebraic structure of the curve and subsequently, we delve into the key concept of pairing, exploring its applications in the field of computer security.

The distinctive element of this work is the presentation and analysis of a cryptographic secret sharing scheme titled *Conjunctive Hierarchical Multi-Secret Sharing Scheme using Elliptic Curves*, developed by Mohan Chintamani, Prabal Paul, and Laba Sa. With this contribution, we delve into the properties of elliptic curves and pairing, providing a deeper understanding of contemporary cryptographic techniques and their applications.

Resum

En aquesta tesi donem una introducció didàctica a la criptografia basada en emparellaments amb corbes el·líptíques seguint les premisses i metodologies establertes al llibre *Elliptic Curves, Number Theory, and Cryptography* de Lawrence C. Washington. Presentem l' estructura algebraica de la corba i seguidament, ens endinsem en el concepte clau d' emparellament, explorant les seves aplicacions en el marc de la seguretat informàtica.

L'element distintiu d'aquest treball és la presentació i anàlisi d'un esquema criptogràfic de compartició de secrets titulat *Conjunctive Hierarchical Multi-Secret Sharing Scheme using Elliptic Curves*, elaborat per Mohan Chintamani, Prabal Paul i Laba Sa. Amb aquesta contribució, aprofundim en les propietats de les corbes el·líptiques i el pairing, proporcionant una comprensió més profunda de les tècniques criptogràfiques contemporànies i les seves aplicacions.

2020 Mathematics Subject Classification. 11T71 , 11G05, 14G50, 14H52, 94A60

Agraïments

Vull agrair en primer lloc al professor Luís Dieulefait, per la confiança i la passió que m'ha transmès des del dia que vam començar a treballar i pels infinits aclariments pacients que m'han permès completar aquesta tesi.

Agraeixo també a la meva família i a totes les persones que m'estimen per haver-me ajudat en aquest procés, ja que directa o indirectament, han contribuït a constuir el meu camí.

Finalment, i encara que és impossible imaginar la quantitat de persones realment involucrades en la meva formació acadèmica, vull agraïr el seu esforç.

A totes aquelles que han viscut creient que l'educació és un dret universal.

Índex

1 Introducció

Aprofitarem el capítol d'introducció per donar un apropament informal als conceptes més bàsics de la criptografia. El lector familiritzat amb els continguts pot avançar directament al següent apartat. No pretenem en aquest capítol donar una definició rigurosa de conceptes criptogràfics clau com el de *funció unidireccional* o *complexitat computacional*. Dirigim al lector interessat a [6] per trobar un manual complet de criptografia moderna.

1.1 L' esquema criptogràfic bàsic

L' Alice vol enviar un missatge , que anomenem **text net**, a en Bob. Per tal de que sigui confidencial, l'Alice l'encripta per obtenir el **text encriptat**. Quan en Bob rep el text encriptat, el desencripta i recupera el text net. Per tal d'encriptar el missatge, Alice utilitza una **clau d'encriptació**. En Bob utilitza una **clau de desencriptació** per llegir el text encriptat. És evident que la clau de desencriptació s'ha de mantenir en secret per asegurar la confidencialitat.

Hi ha dos tipus bàsics d'encriptació. La **criptografia simètrica**, on la clau d'encriptació i la clau de desencriptació són les mateixes. En aquest cas, Alice i Bob necessiten trobar una manera d'establir una clau. Per exemple, Bob podria enviar un missatger a Alice diversos dies abans. Llavors, quan sigui el moment d'enviar el missatge, tots dos tindran la clau. És evident que això és impracticable en moltes situacions. El *xifrat Cèsar* o les màquines *Enigma* són exemples clàssics de criptografia simètrica.

El *xifrat Cèsar*, que rep el seu nom en referència a l'emperador Juli Cèsar, i que segons Suetoni, l'utilitzava per protegir els seus missatges estratègics militars.

> *Si havia de dir alguna cosa confidencial, ho escrivia utilitzant el xifrat, és a dir, canviant l'ordre de les lletres de l'alfabet, de manera que cap paraula es pogués entendre. Si algú vol descodificar-ho i entendre'n el significat, ha de substituir la quarta lletra de l'alfabet, és a dir, la D per la A, i així amb les altres.*
>
> Suetoni, vida dels dotze Cèsars.

L'altre tipus d'encriptació és la **criptografia asimètrica**. En aquest cas, Alice i Bob no necessiten tenir contacte prèviament. Bob genera dues claus alhora, una anomenada **clau pública** , que compartirà amb tothom, i un altre anomenada **clau privada**, que serà secreta. Quan l'Alice vol enviar-li un missatge, utilitzarà la clau pública del Bob per encriptar-lo. Ara, només el Bob amb la corresponent clau privada pot llegir el missatge. Tothom pot encriptar missatges pel Bob, però només ell els pot llegir. Com que tothom coneix la clau pública del Bob, volem que deduir la clau privada a partir de la clau pública sigui extremadament difícil.

Generalment, els sistemes asimètrics són més lents que els bons sistemes simètrics. Per tant, és usual utilitzar un sistema asimètric per establir una clau que després es farà servir en un sistema simètric. La millora de la velocitat és important quan es transmeten quantitats massives de dades.

1.2 Funcions unidireccionals

La criptografia moderna es basa en la diferència entre algoritmes eficients d'encriptació destinats als usuaris legítims i la inviabilitat computacional de la desencriptació per part de l'adversari. Això requereix disposar d'algoritmes amb certes propietats especials de duresa computacional. D'aquestes, potser la més bàsica és una funció unidireccional. De manera informal, una funció és unidireccional si és fàcil de calcular però és difícil d'invertir. En concret ens interessen certs tipus de funcions unidireccionals, anomenades *funcions parany (trapdoor functions)*. Aquestes funcions unidireccionals tenen la particularitat de que en el cas de coneixer un extra d'informació especial (clau privada) poden ser invertides fàcilment.

Si adoptem un llenguatge lleugerament més matemàtic, podríem dir que el problema bàsic de la criptografia és el d'establir una parella de funcions (o algoritmes) que juguin el paper d'encriptació-desencriptació. Més formalment, si anomenem:

- CE, CD a les clau d'encriptació-desencriptació respectivament.
- m al missatge net a transmetre.
- x al missatge encriptat.
- $\mathcal{E}$ a la funció d'encriptació. Que rep un missatge pla m i una clau d'encriptació CE i encripta el missatge (en funció de CE).

$$(m, CE) \longrightarrow \mathcal{E}(m, CE).$$

- $\mathcal{D}$ a la funció de desencriptació.

  Que rep un missatge encriptat x i una clau de desencriptació CD i el desencripta (en funció de CD).

$$(x, CD) \longrightarrow \mathcal{D}(x, CD).$$

Volem aconseguir que aquesta parella de funcions compleixin certes condicions sobre els elements prèviament definits, com per exemple:

- Volem que $\mathcal{E}(m, CE) = x$ sigui ilegible, és dir que llegint x no es puguir saber res de m.
- Volem que $\mathcal{D}(\mathcal{E}(m, CE), CD) = m$, és dir que la funció de desencriptació efectivament retorni el valor m original.

$$(m, CE) \xrightarrow{\mathcal{E}} \mathcal{E}(m, CE) \xrightarrow{\mathcal{D}} \mathcal{D}(\mathcal{E}(m, CE), CD) = m.$$

  (En argot matemàtic diríem que les funcions $\mathcal{E}$ i $\mathcal{D}$ són inverses la una de l'altre.)

- Volem que només es pugui recuperar m coneixent CD, és dir que si desencriptem amb una clau diferent $CD' \neq CD$, aleshores $\mathcal{D}(\mathcal{E}(m, CE), CD') \neq m$.

$$(m, CE) \xrightarrow{\mathcal{E}} \mathcal{E}(m, CE) \xrightarrow{\mathcal{D}} \mathcal{D}(\mathcal{E}(m, CE), CD') = m' \neq m$$

- Volem que $\mathcal{E}$ sigui una *funció unidireccional*, és dir, que és fàcil de calcular $\mathcal{E}(m, CE)$ coneixent m, però que coneixent $\mathcal{E}(m, CE)$, recuperar m sigui computacionalment inviable (si no coneixem la CD corresponent a CE). Si adoptem un llenguatge més tècnic, volem que les funcións d' encriptació i desencriptació es puguin computar en un temps polinomial (si coneixem la clau secreta), però que en el cas contrari la funció de desencriptació funcioni en un temps més lent.

  Tot i que es creu àmpliament que les funcions unidireccionals existeixen, i hi ha diverses funcions unidireccionals candidates conjecturades que s'utilitzen àmpliament, actualment no sabem com demostrar matemàticament que existeixin realment. Per tant, a la pràctica, es dissenyen esquemes criptogràfics assumint que es disposa d'una funció unidireccional. De fet, es pot demostrar que la prova de la existència d'una funció unidireccional resoldria un dels problemas del mileni, en concret demostrant que $\mathcal{P} \neq \mathcal{NP}$.

  Alguns exemples de problemes considerats unidireccionals són:

  - *Factorització.* Es conjectura que la funció $f : (x, y) \longmapsto xy$ és una funció unidireccional. Fins ara, els algoritmes de factorització més ràpids demostrats tenen un temps d'execució $L(n)\sqrt{2}$, on $L(n) = e^{\sqrt{\log n \log\log n}}$.
  - *El problema del logaritme discret.* Sigui p un primer. El grup multiplicatiu $\mathcal{Z}_p^* = \{x < p \mid (x, p) = 1\} \mod p$ és cíclic, de manera que

    $$\mathcal{Z}_p^* = \{g^i \mod p \mid 1 \leq i \leq p-1\}$$

    per a algun generador $g \in \mathcal{Z}_p^*$. Es conjectura que la funció $f : (p, g, x) \mapsto (g^x \mod p, p, g)$, on p és un primer i g és un generador per a $\mathcal{Z}_p^*$, és una funció unidireccional. Calcular $f(p, g, x)$ es pot fer en temps polinomial. No obstant això, la solució provada més ràpida per al seu invers, és l'algoritme del càlcul de l'índex, amb un temps d'execució esperat de $L(p)\sqrt{2}$.

En aquest treball, discutirem un criptosistema de compartició de secrets basat en corbes el·líptiques, especialment en el problema del logaritme discret per a corbes el·líptiques (ECDLP).

Potser algú es pregunti per què les corbes el·líptiques s'utilitzen en situacions criptogràfiques. La raó és que les corbes el·líptiques proporcionen una seguretat equivalent als sistemes clàssics utilitzant menys bits. Per exemple, a [10] s'estima a que una clau de 4096 bits per RSA ofereix el mateix nivell de seguretat que una de 313 bits en un sistema de corbes el·líptiques.

Observació 1.1. Al llarg d'aquesta tesi, estem treballant sota la hipòtesi de que un possible atacant al nostre criptosistema compta només amb eines de computació clàssica. Existeixen algoritmes quàntics eficients que resolen el problema del logaritme discret. Tanmateix, en la actualitat RSA i ECDLP es continuen utilitzant, ja que no existeixen ordinadors quàntics potents.

2 Corbes el·líptiques

En general, anomenem corba el·líptica a tota corba algebraica projectiva definida sobre un cos K, de gènere 1, no singular, de manera que hi ha com a mínim un punt K.

No pretenem amb aquest treball donar una definició tècnica i rigorosa de la corba el·líptica, sinó que treballarem en un escenari més simple, estàndard en la pràctica de la criptografia de corbes el·líptiques.

2.1 L' equació de Weierstrass

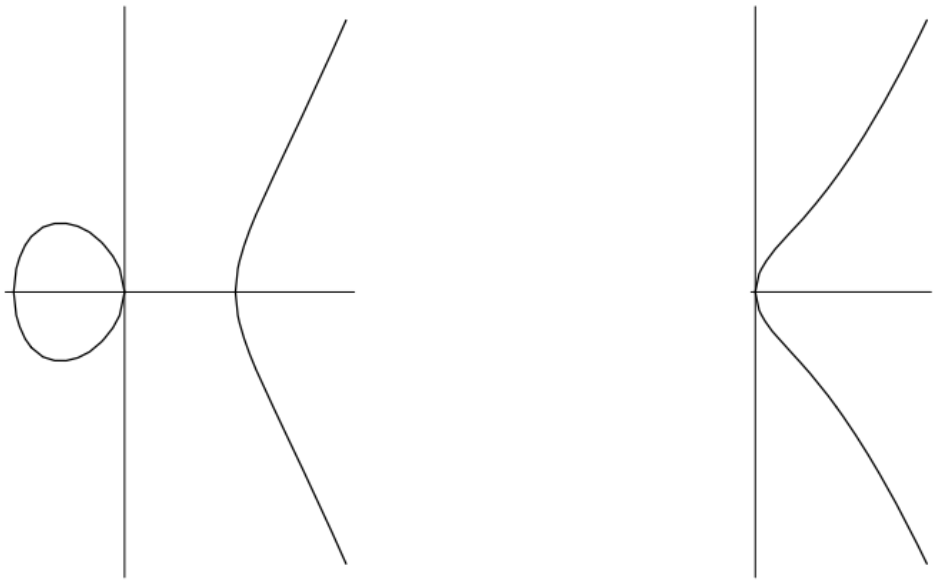
Al llarg d'aquest treball considerarem que una corba el·líptica E és la gràfica d' una equació de la forma:

$$y^2 = x^3 + Ax + B, \tag{2.1}$$

on A, B pertànyen a algun cos K, x, y tenen coordenades en un cos L extensió de K i $4A^3 + 27B^2 \neq 0$. Aquesta és l' **equació de Weierstrass** d' una corba el·líptica.

Hi han altres equacions que descriuen corbes el·líptiques que poden ser transformades en l' equació de Weierstrass amb canvis de variable. Tanmateix hi han algunes equacions més generals per contextos més amplis que no poden ser transformades en l'equació de Weierstrass, com per exemple quan treballem sobre un cos de característica 2. Nosaltres treballarem únicament al context de l' equació de Weierstrass.

En general, és difícil representar gràficament les corbes el·líptiques sobre la majoria de cossos. Tanmateix, és útil per la intuició pensar-ne en termes de gràfiques sobre els nombres reals.



$(a) \quad y^2 = x^3 - x$ $(b) \quad y^2 = x^3 + x$

Figura 1: Dues corbes el·líptiques sobre $\mathbb{R}$

Observació 2.1. És possible demostrar que una corba descrita per l' equació de Weierstrass és no-singular si i només si $4A^3+27B^2 \neq 0$. Aquesta condició és equivalent a que l' equació $x^3 + Ax + B = 0$ no tingui cap arrel repetida. Per una demostració rigorosa d' aquest resultat, veure [5, Cap. 3, Prop. 1.4]

Definició 2.2 (Corba el·líptica)**.** *Sigui K un cos amb característica $\neq 2, 3$,L un cos extensió de K i $A, B \in K$ constants tals que $4A^3 + 27B^2 \neq 0$. Definim el conjunt de punts de la nostra corba el·líptica com:*

$$E(L) := \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}.$$

Per raons tècniques, és útil afegir un punt a l'infinit a una corba el·líptica. Al següent apartat, entendrem aquest fet amb més formalitat.

Tanmateix per facilitar el concepte a la resta del treball considerarem que el punt (∞, ∞), generalment denotat simplement per ∞, és un símbol formal que compleix certes propietats computacionals. Intuitivament, considerarem que ∞ està situat alhora als extrems superior i inferior de l'eix y. És a dir, imaginem que els extrems de l'eix y s' embolcallen i es troben (potser en algun lloc a la part posterior darrere de la pàgina) en el punt ∞. . Per exemple, direm que una recta passa per ∞ quan aquesta recta és vertical (i.e., $x =$ constant). Potser el punt ∞ sembli una mica estrany, però veurem que incloure'l té conseqüències molt útils.

No obstant això, si estem treballant amb un cos diferent dels nombres reals, no hi ha cap ordre significatiu dels elements i, per tant, distingir una part superior i una part inferior de l'eix y no té gaire sentit. A més, com hem disposat que dues línies verticals es trobin en ∞, per simetria, si es troben a la part superior de l'eix y, també haurien de trobar-se a la part inferior. Però dues línies haurien d'intersecar-se només en un punt, així que el "∞ superior" i el "∞ inferior" han de ser els mateixos. En qualsevol cas, aquesta serà una propietat útil de ∞.

2.2 L'espai projectiu i el punt a l'infinit.

Recordem que tot i que per simplicitat a la resta del treball considerarem la corba el·líptica com una corba afí, amb un punt extra (∞) amb propietats especials, realment la corba el·líptica és una corba definida a l'espai projectiu.

En concret és el conjunt de zeros al pla projectiu d'un **polinomi homogeni** de tres variables sobre un cos K, i de gènere 1, tal que com a mínim un punt de K és solució.

Recordem que el **pla projectiu** P_K^2 sobre K es defineix mitjançant les classes d'equivalència de les ternes (x, y, z) amb $x, y, z \in K$ i almenys un dels x, y, z diferent de zero. Dos triples (x_1, y_1, z_1) i (x_2, y_2, z_2) es diuen equivalents si existeix un element no nul $\lambda \in K$ tal que

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2).$$

Ho escrivim com $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. La classe d'equivalència d'un triple depèn només de les relacions entre x, y i z, per tant, la classe d'equivalència de (x, y, z) es denota $(x : y : z)$.

Si $(x : y : z)$ és un punt amb $z = 0$, aleshores $(x : y : z) = (x/z : y/z : 1)$. Aquests són els punts "finits"a P_K^2. No obstant això, si $z = 0$, llavors dividir per z s'ha de considerar com donar ∞ en qualsevol de les coordenades x o y, i per tant els punts $(x : y : 0)$ s'anomenen els "punts a l'infinit"a P_K^2.

El **pla afí** bidimensional sobre K sovint es denota

$$A_K^2 = \{(x, y) \in K \times K\}.$$

Tenim una inclusió $A_K^2 \hookrightarrow P_K^2$ donada per

$$(x, y) \mapsto (x : y : 1)$$

. D'aquesta manera, el pla afí es pot identificar amb els punts finits a P_K^2.

Definició 2.3. *Un polinomi és homogeni de grau n si és una suma de termes de la forma* $ax^i y^j z^k$ *amb* $a \in K$ *i* $i + j + k = n$

Per exemple, $F(x, y, z) = 2x^3 - 5xyz + 7yz^2$ és homogeni de grau 3.

Observació 2.4. Si un polinomi F és homogeni de grau n, aleshores es fàcil veure que $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ per a tot $\lambda \in K$. Això implica que si F és homogeni de cert grau, i $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, llavors $F(x_1, y_1, z_1) = 0$ si i només si $F(x_2, y_2, z_2) = 0$. Per tant, un zero de F a P_K^2 no depèn de la elecció del representant per a la classe d'equivalència, de manera que el conjunt de zeros de F a P_K^2 està ben definit. Si $F(x, y, z)$ és un polinomi arbitrari en x, y, z, llavors no podem parlar d'un punt de F a P_K^2 ja que això depèn del representant (x, y, z) de la classe d'equivalència.

Si $f(x, y)$ és un polinomi en x i y, llavors el podem fer homogeni inserint potències apropiades de z. Per exemple, en el cas de la corba el·líptica, si $f(x, y) = y^2 - x^3 - Ax - B$, aleshores obtenim el polinomi homogeni $F(x, y, z) = y^2 z - x^3 - Axz^2 - Bz^3$.

Si F és homogeni de grau n, aleshores

$$F(x, y, z) = z^n f(x/z, y/z)$$

i tenim que

$$f(x, y) = F(x, y, 1)$$

Ara podem entendre millor què significa que dues línies paral·leles es trobin a l'infinit. Siguin

$$y = mx + b_1, \quad y = mx + b_2$$

dues línies no verticals paral·leles amb $b_1 \neq b_2$, aquestes tenen les formes homogènies

$$y = mx + b_1 z, \quad y = mx + b_2 z$$

Quan resolem les equacions per trobar-ne la intersecció, obtenim $z = 0$ i $y = mx$. Com no podem tenir totes les coordenades x, y, z iguals a 0, hem de tenir $x \neq 0$. Per tant, podem dividir per x i trobar que la intersecció de les dues línies és

$$(x : mx : 0) = (1 : m : 0).$$

De manera similar, si $x = c_1$ i $x = c_2$ són dues línies verticals diferents, s'intersequen en el punt $(0 : 1 : 0)$, que és un dels punts a l'infinit a P_K^2.

Ara observem la corba el·líptica E donada per $y^2 = x^3 + Ax + B$. La seva forma homogènia és $y^2 z = x^3 + Axz^2 + Bz^3$. Els punts (x, y) a la corba original corresponen als punts $(x : y : 1)$ a la versió projectiva. Per veure quins punts a E es troben a l'infinit, posem $z = 0$ i obtenim $0 = x^3$. Per tant, $x = 0$, i y pot ser qualsevol nombre no nul (recordem que $(0 : 0 : 0)$ no està permès). Rescalant per y trobem que $(0 : y : 0) = (0 : 1 : 0)$ és l'únic punt a l'infinit a E. Com hem mencionat abans, $(0 : 1 : 0)$ es troba a cada línia vertical de manera que totes les línies verticals s'intersequen amb E en aquest punt a l'infinit. A més, com que $(0 : 1 : 0) = (0 : -1 : 0)$, considerem els extrems superior i inferior de l'eix y com el mateix.

Hi ha situacions on utilitzar coordenades projectives facilitat els càlculs a les corbes el·líptiques, no obstant això, per els propòsits d'aquest treball sempre treballarem amb coordenades afins, ja que al homogeneïtzar la corba, és dir, al prendre les coordenades $x = X/Z, y = Y/Z$, podem expressar "quasi" tota la corba amb només dues coordenades, cosa que ens facilita molt el càlcul i a més, en el procés només perdem un punt, el punt de l'infinit de la direcció vertical. Tractarem doncs aquest punt a l'infinit com un cas especial quan sigui necessari.

2.3 La llei de grup

Cap al 250 d.C el matemàtic Diofant d' Alexandria construí un mètode que serviria d' inspiració pel que a continuació definirem com a suma de punts d' una corba el·líptica. El mètode de Diofant utilitza punts coneguts sobre la corba per generar-ne de nous, també sobre la corba.

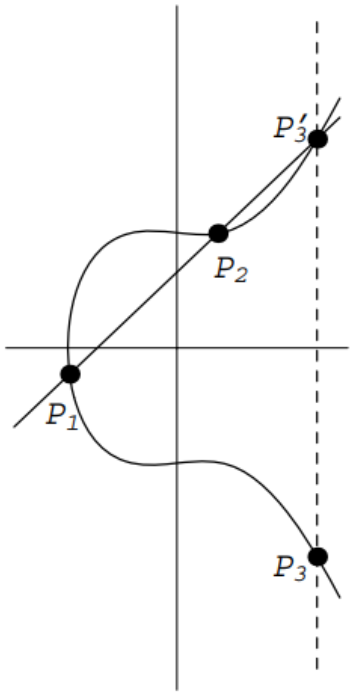


Figura 2: Suma de punts a una corba el·líptica

Començem amb dos punts: P_1, P_2 en una corba el·líptica E donada per l'equació $y^2 = x^3 + Ax + B$. Traçem la recta L que passa per P_1 i P_2 i trobem la intersecció de L amb E en un tercer punt P_3'. Reflectim P_3' a través de l'eix x (és dir, canviem el signe de la coordenada y) per obtenir P_3. Definim doncs

$$P_1 + P_2 = P_3.$$

Observació 2.5. Podríem denotar millor aquesta operació com $P_1 +_E P_2$, però optem per la notació més simple ja que mai sumarem punts sumant coordenades.

A la següent secció examinarem amb més detall aquest procés. Aportem prèviament un resultat que utilitzarem a la definició formal de la suma.

Problema 2.6. Sigui (x, y) un punt a una corba el·líptica donada per l' equació $y^2 = x^3 + Ax + B$. Veiem que si $y = 0$, aleshores $3x^2 + A \neq 0$. *(Indicació: Recordeu quina és la condició per a que x sigui una arrel múltiple.)*

Solució. Per començar, recordem que per a qualsevols nombres a,b,c, tenim:

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc. \quad (1)$$

Resoldrem el problema per reducció a l' absurd. Suposem que $(x, 0)$ és un punt de la corba el·líptica i que $3x^2 + A = 0$. Aleshores, x ha de ser solució de l' equació:

$$x^3 + Ax + B = 0.$$

Siguin α, β, γ les solucions d' aquesta equació cúbica. Sabem que són totes tres diferents ja que són arrels d' una corba el·líptica. Per l' equació (1), tenim:

$$\alpha + \beta + \gamma = 0 \quad (2)$$
$$\alpha\beta + \alpha\gamma + \beta\gamma = A \quad (3)$$

Suposem sense perdre generalitat que $x = \alpha$. Aleshores, per la hipòtesi inicial tenim que $A = -3\alpha^2$. Reordenant l' equació (2), podem escriure $\gamma = -(\alpha + \beta)$, i subsitituint γ a l' equacio (3), podem veure que:

$$\alpha\beta - (\alpha+\beta)\alpha - (\alpha+\beta)\beta = -3\alpha^2.$$

Simplificant l' equació, podem resoldre l' equació de segon grau sobre α:

$$2\alpha^2 - \beta\alpha - \beta^2 = 0,$$

que té com a solucions $\alpha = \beta$ i $\alpha = \frac{-\beta}{2}$. Al primer cas, veiem clarament com tenim una solució repetida, i en el segon $\alpha = \frac{-\beta}{2} \Rightarrow \gamma = -(\frac{-\beta}{2} + \beta) = \frac{-\beta}{2} = \alpha$. En tot cas arribem a una contradicció, ja que no pot haver arrels repetides.

2.3.1 Suma de punts a una corba el·líptica

Descriurem ara la construcció de l' algoritme de la suma. El lector que només estigui interessat en l' implementació computacional de l' algoritme pot avançar al següent punt.

Suposem que volem sumar dos punts

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$$

sobre una corba el·líptica E donada per l' equació $y^2 = x^3 + Ax + B$. Considerem diferents casos:

- Suposem primer que $P_1 \neq P_2$ i que cap dels dos punts és ∞. Traçem la recta L que passa per P_1 i P_2. La seva pendent és:

  $$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

  Si $x_1 = x_2$ la recta L és vertical. Considerarem aquest cas més endavant.

  Suposem doncs que $x_1 \neq x_2$. Podem escriure l' equació de L com:

  $$y = m(x - x_1) + y_1$$

  Per trobar la intersecció amb E, substituim y a la equació de E:

  $$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

  Reordenant termes tenim una equació de la forma

  $$x^3 - m^2x^2 + \ldots = 0.$$

  Les tres arrels d'aquesta cúbica es corresponen amb els 3 punts d' interesseció de L amb E.

  En aquest cas ja coneixem dues de les arrels, concretament x_1 i x_2, ja que P_1 i P_2 són punts tant a L com a E. Per tant, podríem factoritzar la cúbica per obtenir el tercer valor de x. Però hi ha una manera més fàcil. Com hem vist al problema (2.6), si tenim un polinomi cúbic $x^3 + ax^2 + bx + c$ amb arrels r, s, t, llavors

  $$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \ldots.$$

  Aleshores,

  $$r + s + t = -a.$$

  Si coneixem dues arrels r, s, podem recuperar la tercera com $t = -a - r - s$. En el nostre cas,

  $$t = m^2 - x_1 - x_2$$

  i obtenim

  $$x_3' = m^2 - x_1 - x_2$$

  substituint x_3 a L

  $$y_3' = m(x_3 - x_1) + y_1.$$

  Hem trobat P_3'. El reflectim a través de l'eix x per obtenir el punt $P_3 = (x_3, y_3)$:

  $$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1.$$

- En el cas on $x_1 = x_2$ però $y_1 \neq y_2$, la recta L que conté P_1, P_2 és vertical. Aleshores L interseca amb E en ∞, per definició. Reflectant ∞ a través de l'eix x estem un altre cop a ∞, també les propietats que hem enunciat abans. Aleshores, en aquest cas
$$P_1 + P_2 = \infty$$

- $P_1 = P_2 = (x_1, y_1)$. Quan dos punts en una corba són molt propers, la recta que passa per ells s'aproxima a una recta tangent. Aleshores, quan els dos punts coincideixen, considerem la recta L que passa per ells com la recta tangent. La diferenciació implícita ens permet trobar la pendent m de L:
$$2y\frac{dy}{dx} = 3x^2 + A \Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$
Si $y_1 = 0$, llavors la recta L és vertical i establim $P_1 + P_2 = \infty$ com abans. (Com hem vist al problema 2.6, sabem que $3x_1^2 + A \neq 0$)

Aleshores, suposem que $y_1 \neq 0$. L'equació de L és
$$y = m(x - x_1) + y_1,$$
com abans. Intersequem amb E i obtenim l'equació cúbica
$$0 = x^3 - m^2x^2 + \dots.$$
Aquest cop, només coneixem una arrel, és a dir, x_1, però és una arrel doble ja que L és tangent a E a P_1. Per tant, procedint com abans, obtenim P_3:
$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1.$$

- Finalment, suposem que $P_1 \neq P_2$ i que $P_2 = \infty$. La recta que passa per P_1 i ∞ és una línia vertical que interseca E en el punt P_1', que és la reflexió de P_1 respecte a l'eix x. Quan reflectim P_1' a través de l'eix x per obtenir $P_3 = P_1 + P_2$, tornem a obtenir P_1. Per aquest motiu
$$P_1 + \infty = P_1$$
per a tots els punts P_1 a E. És clar que estenem això per incloure $\infty + \infty = \infty$.

Resumim el desenvolupament anterior:

LLEI DE GRUP

Sigui E una corba el·líptica definida per $y^2 = x^3 + Ax + B$. Siguin $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$ punts a E amb $P_1, P_2 \neq \infty$. Definim $P_1 + P_2 = P_3 = (x_3, y_3)$ com segueix:

1. Si $x_1 = x_2$, llavors
$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{amb} \quad m = \frac{y_2 - y_1}{x_2 - x_1}.$$
2. Si $x_1 = x_2$, però $y_1 \neq y_2$, aleshores $P_1 + P_2 = \infty$.
3. Si $P_1 = P_2$ i $y_1 \neq 0$, llavors
$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{amb} \quad m = \frac{3x_1^2 + A}{2y_1}.$$
4. Si $P_1 = P_2$ i $y_1 = 0$, aleshores $P_1 + P_2 = \infty$.

A més, definim
$$P + \infty = P$$
per a tots els punts P sobre E.

Teorema 2.7. *Els punts de E amb l' operació previament definida formen un grup abelià amb ∞ com element neutre.*

Demostració. Notem que quan P_1, P_2 tenen coordenades en un cos L que conté A, B, aleshores el punt $P_1 + P_2$ també té coordenades en L. Tenim doncs que $E(L)$ és tancat sota la operació definida.

La propietat conmutativa es dedueix trivialment per la fòrmula i pel fet de que la recta entre P_1, P_2 és la mateixa que entre P_2 i P_1. El punt ∞ és l'element neutre per definició. Sigui P' el punt simètric a P respecte l'eix x. Aleshores $P + P' = \infty$ i P' és l'invers de P.

No provarem l'associativitat de la suma. Aquesta és la propietat més difícil de demostrar i no forma part de l' objetiu d'aquest treball. La propietat pot ser verificada simplement computant les formules. Aquesta demostració es torna molt llarga i farragosa ja que hem d' anar considerar diferents casos, depenent de si $P_1 = P_2$, $P_1 + P_2 = P_3$, etc.. Per veure una demostració en detallada veure [[1], Cap 2.4] $\square$

2.3.2 El problema del logaritme discret a la corba el·líptica

Una corba el·líptica sobre un cos finit té un nombre finit de punts. En aquest cas $E(K)$ és un grup abelià finit. Aquests tipus de grups tenen aplicacions criptogràfiques interesants.

Notació 1. *Sigui P un punt en una corba el·líptica i k un nombre enter, definim kP de la següent manera:*

1. *Si $k > 0$, aleshores: $kP := P + P + \ldots + P$ amb k sumands.*
2. *Si $k < 0$, aleshores: $kP := (-P) + (-P) + \ldots + (-P)$ amb $|k|$ sumands.*

Per computar kP per un k gran, és ineficient computar kP simplement sumant P amb si mateix k vegades. Tanmateix, podem calcular kP ràpidament amb el procediment a continuació.

Suposem que per exemple volem calcular $19P$. Computem doncs:

$$2P, \quad 4P = 2P + 2P, \quad 8P = 4P + 4P,$$

$$16P = 8P + 8P, \quad 19P = 16P + 2P + P.$$

En una corba el·líptica sobre un cos qualsevol, pot sorgir la dificultat de que si k és molt gran, la mida de les coordenades dels punts creix ràpidament. Tanmateix, treballant amb cos finit com per exemple $E(\mathbb{F}_p)$, aquest problema desapareix, ja que podem anar reduint *mod* p a cada pas.

Algoritme per calcular el múltiple enter d'un punt

Sigui k un enter positiu i P un punt en una corba el·líptica. L' algoritme següent calcula kP.

1. Comencem amb $a = k$, $B = \infty$, $C = P$.
2. Si a és parell, fem $a = a/2$, i $B = B$, $C = 2C$.
3. Si a és senar, fem $a = a - 1$, i $B = B + C$, $C = C$.
4. Si $a \neq 0$, tornem al pas 2.
5. Sortida B.

La sortida B és kP. L' algoritme permet calcular el resultat en un temps $O(log(n))$.

Per un altre costat, si treballem amb un cos finit gran, per exemple $E(\mathbb{F}_q)$, per un q gran, donats els punts P i kP, és molt difícil determinar el valor de k. Aquest és el **problema del logaritme discret sobre corbes el·líptiques**.

Observació 2.8. Més generalment, sigui G un grup qualsevol que denotarem multiplicativament i $a, b \in G$. Suposem que sabem que $a^k = b$ per algun enter k. En aquest context, *el problema del logaritme discret* és també trobar k. No es coneix cap algoritme que pugui resoldre aquest problema en temps polinomial, per tant es considera intractable.

Observació 2.9. Al llarg d'aquesta tesi, estem treballant sota la hipòtesi de que un possible atacant al nostre criptosistema compta només amb eines de computació clàssica. Existeixen algoritmes eficients que resolen el problema del logaritme discret al context de la computació quàntica.

Proposició 2.10. *L' operació de multiplicació per un nombre enter és distributiva respecte de la suma d'enters i respecte la suma de punts. És a dir es compleix que*

1. *Siguin a, b un nombres enters i P un punt d'una corba el·líptica E, aleshores*

$$(a+b)P = aP + bP.$$

   Suposem que $a + b > 0$. Clarament veiem que

$$(a+b)P = P + \overset{a+b}{\dots} + P = P + \overset{a}{\dots} + P + \overset{b}{\dots} + P = aP + bP.$$

   El cas on $a + b < 0$ es veu de manera anàloga.

2. *Sigui a un nombre enter i P, Q punts d'una corba el·líptica E, aleshores*

$$a(P+Q) = aP + aQ.$$

   Demostració. Demostrarem aquest resultat per inducció.

   Trivialment veiem que pel cas inicial $n = 1$, tenim que $1(P + Q) = 1P + 1Q$. Suposem cert que $n(P + Q) = nP + nQ$. Veiem aleshores que

$$(n+1)(P+Q) = n(P+Q) + (P+Q) = nP + nQ + P + Q.$$

   I ara per la conmutativitat de la suma de punts

$$nP + nQ + P + Q = nP + P + nQ + Q = (n+1)P + (n+1)Q.$$

□

2.4 Divisors

En aquesta secció donarem una introducció als conceptes clau de divisor i de funció d'una corba el·líptica. No és l' objectiu d'aquest treball donar la definició exhaustiva i rigorosa que aquests conceptes requereixen. Aquests dos conceptes seràn essencials posteriorment a l'hora de definir l'emparellament de Weil.

Definició 2.11. *Sigui E una corba el·líptica definida sobre un cos K. Per a cada punt $P \in E(\overline{K})$, definim el símbol formal $[P]$. Un divisor D a E és una combinació lineal* ***finita*** *d'aquests símbols amb coeficients enters:*

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

Per tant, un divisor és un element del grup abelià lliure generat pels símbols $[P]$. El grup de divisors es denota com a $\mathrm{Div}(E)$.

Definició 2.12. *Definim les funcions grau i suma d'un divisor com:*

$$\mathrm{gr}(\sum_j a_j[P_j]) = \sum_j a_j \in \mathbb{Z}$$
$$\mathrm{sum}(\sum_j a_j[P_j]) = \sum_j a_j P_j \in E(\overline{K}).$$

La funció suma simplement utilitza la llei de grup a E per operar els punts que estan dins dels símbols. Els divisors de grau 0 formen un subgrup important de $\mathrm{Div}(E)$, denotat com a $\mathrm{Div}^0(E)$. La funció suma dóna un homomorfisme

$$\mathrm{sum} : \mathrm{Div}^0(E) \to E(\overline{K}).$$

Es clar que siguin D, E dos divisors qualsevol, tenim que

$$\mathrm{sum}(D+E) = \mathrm{sum}(\sum_j a_j[P_j] + \sum_i b_i[P_i]) = \sum_j a_j P_j + \sum_i b_i P_i = \mathrm{sum}(D) + \mathrm{sum}(E)$$

L' objectiu d'aquesta secció serà demostrar que el nucli d' aquest homomorfisme està format pels divisors de funcions (**Divisors principals**). (*Teorema 2.22*).

Definició 2.13. *Una funció f a E és una funció racional de la forma*

$$f(x,y) = \frac{P(x,y)}{Q(x,y)}$$

On P i Q són polinomis en dues variables de l'anell $\overline{K}[x,y]$ i $Q \neq 0$, tals que f està definida en almenys un punt de $E(\overline{K})$ diferent de ∞. A més, considerarem que les funcions a E poden prendre valors a $\overline{K} \cup \infty$.

Per exemple, la funció racional $1/(y^2 - x^3 - Ax - B)$ no seria una funció a E.

Observació 2.14. Falta un detall tècnic a l'hora de definir funcions a E. Mostrem un exemple per ilustrar la situació. Considerem l'equació $y^2 = x^3 - x$ d'una corba el·líptica. La funció $f(x, y) = \frac{x}{y}$ no està definida a $(0, 0)$. No obstant això, a E,

$$\frac{x}{y} = \frac{y}{x^2 - 1},$$

la qual si està definida i pren el valor 0 a $(0, 0)$. Es pot demostrar que sempre es pot transformar una funció d'aquesta manera per obtenir una expressió dóna un valor únivoc a $K \cup \{\infty\}$.

Diem que una funció té un **zero** en un punt P si pren el valor 0 a P, i té un **pol** en P si pren el valor ∞ a P. Sigui P un punt. Es pot demostrar que existeix una funció u_P, anomenada **uniformitzadora** a P, amb $u(P) = 0$ i tal que qualsevol funció $f(x, y)$ es pot escriure en la forma

$$f = u_P^r \cdot g \quad \text{amb} \quad r \in \mathbb{Z} \quad \text{tal que} \quad g(P) \neq 0, \infty.$$

Definim **l'ordre** de f a P com

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

Definició 2.15. *Suposem que f és una funció a E, no idènticament 0. Definim el **divisor** de f com*

$$\mathrm{div}(f) = \sum_{P \in E(\overline{K})} \mathrm{ord}_P(f)[P] \ \in \mathrm{Div}(E).$$

La següent proposició ens permet asegurar que aquesta suma sempre serà finita i en conclusió, el divisor d'una funció està ben definit. Aquest es un resultat avançat de corbes algebraiques que no demostrarem.

Proposició 2.16. *Sigui E una corba el·líptica i f una funció en E diferent de 0.*

1. *f té un nombre finit de zeros i pols.*
2. *$\mathrm{gr}(div(f)) = 0$.*
3. *Si f no té zeros ni pols, és dir, si $div(f) = 0$, aleshores f és constant.*

Observació 2.17. Anomenem **divisors principals** als divisors de funcions. Per com hem definit els divisors de les funcions, és fàcil comprobar que siguin f, g dues funcions a E, es compleix que

$$\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g) \qquad \mathrm{div}(f/g) = \mathrm{div}(f) - \mathrm{div}(g)$$

Recordem que un zero d'ordre 1 de la funció f és un pol (un zero d' ordre -1) de la funció $1/f$.

A continuació haurem de presentar 3 resultats per tal de facilitar la demostració del teorema 2.22.

Lema 2.18. *Sigui P_1 i P_2 polinomis a $\overline{K}[t]$ sense arrels en comú. Suposem que existeixen quatre parelles (a_i, b_i), $1 \leq i \leq 4$, amb $a_i, b_i \in \overline{K}$ que compleixen:*

1. *Per a cada i, almenys un dels a_i, b_i és diferent de zero.*
2. *Si $i \neq j$, llavors no existeix $c \in \overline{K}^\times$ tal que $(a_i, b_i) = (ca_j, cb_j)$.*
3. *$a_i P_1 + b_i P_2$ és un quadrat d'un polinomi per a $1 \leq i \leq 4$.*

Aleshores P_1, P_2 són polinomis constants.

Demostració. Aquesta es una demostració bastant llarga i principalment calculística amb poc interès pel nostre treball. Veure [1], Lema 11.6] per una demostració completa. □

Lema 2.19. *Considerem una corba el·líptica E sobre un cos amb característica $\neq 2$. Considerem la corba donada per l' equació*

$$y^2 = x^3 + Ax + B.$$

Sigui t un variable. No existeixen funcións racionals no constants $X(t), Y(t) \in \overline{K}(t)$ tal que

$$Y(t)^2 = X(t)^3 + AX(t) + B.$$

Demostració. Factoritzem el polinomi cúbic com

$$x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3),$$

on $e_1, e_2, e_3 \in \overline{K}$ són diferents. Suposem que $X(t)$ i $Y(t)$ existeixen i no són constants. Escrivim

$$X(t) = \frac{P_1(t)}{P_2(t)}, \quad Y(t) = \frac{Q_1(t)}{Q_2(t)}.$$

Podem assumir que $P_1(t), P_2(t)$ no tenen arrels comunes, i que $Q_1(t), Q_2(t)$ no tenen arrels comunes. Substituint a l'equació per E obtenim

$$Q_1(t)^2 P_2(t)^3 = Q_2(t)^2 \ (P_1(t)^3 + AP_1(t)P_2(t)^2 + BP_2(t)^3).$$

Com que el costat dret és un múltiple de $Q_2(t)^2$, també ho ha de ser el costat esquerre. Com que Q_1, Q_2 no tenen arrels comunes, P_2^3 ha de ser un múltiple de Q_2^2.

Una arrel comuna de P_2 i $P_1^3 + AP_1P_2^2 + BP_2^3$ seria una arrel de P_1^3. Com que P_1 i P_2 no tenen arrels comunes, això és impossible. Per tant, Q_2^2 ha de ser un múltiple de P_2^3. Per tant, P_2^3 i Q_2^2 són múltiples l'un de l'altre, per tant són múltiples constants l'un de l'altre. Ajustant P_1 i Q_1 si cal, podem assumir que $P_2^3 = Q_2^2$.

Cancel·lant aquestes dues expresions del càlcul obtenim

$$Q_1^2 = P_1^3 + AP_1P_2^2 + BP_2^3.$$

Per altra banda, com que

$$\Big(\frac{P_1}{P_2}\Big)^3 + A\Big(\frac{P_1}{P_2}\Big) + B = (\frac{P_1}{P_2} - e_1)(\frac{P_1}{P_2} - e_2)(\frac{P_1}{P_2} - e_3)$$

Multiplicant tota l' expresió per P_2^3 veiem que

$$P_1^3 + AP_1P_2^2 + BP_2^3 = (P_1 - e_1P_2)(P_1 - e_2P_2)(P_1 - e_3P_2)$$

Suposem ara que $i \neq j$ i que $P_1 - e_iP_2$ i $P_1 - e_jP_2$ tenen una arrel comuna que anomenarem r. Llavors, r és arrel de

$$e_j(P_1 - e_iP_2) - e_i(P_1 - e_jP_2) = (e_j - e_i)P_1$$

i de

$$(P_1 - e_iP_2) - (P_1 - e_jP_2) = (e_j - e_i)P_2.$$

Com que $e_j - e_i \neq 0$, això significa que r és una arrel comuna de P_1 i P_2, la qual cosa és una contradicció. Per tant, $P_1 - e_iP_2$ i $P_1 - e_jP_2$ no tenen arrels comunes quan $i \neq j$. Com que el producte

$$(P_1 - e_1P_2)(P_1 - e_2P_2)(P_1 - e_3P_2)$$

és el quadrat d'un polinomi, cada factor ha de ser el quadrat d'un polinomi a $\overline{K}[t]$ (podria semblar que cada factor és una constant multiplicada pel quadrat, però totes les constants són quadrats al cos algebraicament tancat $\overline{K}$, per tant es poden absorbir dins dels quadrats de polinomis).

Com que $P_2^3 = Q_2^2$, trobem que P_2 també ha de ser el quadrat d'un polinomi.

Ara, podem veure que tenim 2 polinomis P_1, P_2 i les 4 parelles

$$(1, -e_1), \quad (1, -e_2), \quad (1, -e_3), \quad (0, 1)$$

que satisfan les condicions del lema 2.18, i aleshores, P_1 i P_2 han de ser constants. En conseqüència, també $X(t) = P_1(t)/P_2(t)$ ha de ser constant, en contradicció amb la hipòtesi inicial. D'aquesta forma completem la demostració.

□

Lema 2.20. *Siguin $P, Q \in E(\overline{K})$. Suposem que existeix una funció h de E tal que*

$$\mathrm{div}(h) = [P] - [Q].$$

Aleshores $P = Q$.

Demostració. Suposem que $P \neq Q$ i que $\mathrm{div}(h) = [P] - [Q]$. Llavors, per a qualsevol constant c, la funció $h - c$ té un pol simple a Q i, per tant, per la Proposició 2.16, té exactament un zero, el qual ha de ser simple.

Sigui f qualsevol funció a E. Si f no té cap zero o pol a Q, aleshores

$$g(x,y) = \prod_{R \in E(\overline{K})} (h(x,y) - h(R))^{\mathrm{ord}_R(f)}$$

té el mateix divisor que f (ja que estem suposant que $\mathrm{ord}_Q(f) = 0$, el factor per $R = Q$ es defineix com 1). L'únic a comprovar és que els pols de $h(x,y)$ a Q s'anul·len. Cada factor té un pol a $(x,y) = Q$ d'ordre $\mathrm{ord}_R(f)$ (o una arrel si $\mathrm{ord}_R(f) < 0$). Com que $\sum_R \mathrm{ord}_R(f) = 0$, aquests es cancel·len.

Com que f i g tenen el mateix divisor, el quocient f/g no té zeros ni pols, i per tant és constant per la proposició 2.16. D'aquí veiem que f és una funció racional de h.

Si f té una arrel o un pol a Q, el factor per $R = Q$ en el producte anterior no està definit. No obstant això, $f \cdot h^{\mathrm{ord}_R(f)}$ no té zeros ni pols a Q. El raonament anterior mostra que, per tant, és una funció racional de h, així que el mateix es manté per f.

Hem demostrat que cada funció a $E(\overline{K})$ és una funció racional de h. En particular, x i y són funcions racionals de h. El lema 2.19 mostra que això és impossible. Aquesta contradicció significa que hem de tenir $P = Q$.

□

Lema 2.21. *Siguin P_1, P_2 dos punts sobre una corba el·líptica. Aleshores existeix una funció racional g tal que:*

$$[P_1] + [P_2] = [P_1 + P_2] + [\infty] + \mathrm{div}(g).$$

Demostració. Sigui L la recta amb equació $ax + by + c = 0$ que conté els punts P_1, P_2. Suposem que P_3 és el tercer punt a E que pertany a la recta $ax+by+c = 0$. Aleshores la funció

$$f(x,y) = ax + by + c$$

té zeros a P_1, P_2, P_3. Si $b \neq 0$, llavors f té un pol triple a ∞. Per tant, per la proposició 2.16

$$\mathrm{div}(ax + by + c) = [P_1] + [P_2] + [P_3] - 3[\infty].$$

La recta que passa per $P_3 = (x_3, y_3)$ i $-P_3$ és $x - x_3 = 0$. El divisor de la funció $x - x_3$ és

$$\mathrm{div}(x - x_3) = [P_3] + [-P_3] - 2[\infty].$$

Per tant,

$$\mathrm{div}\left(\frac{ax + by + c}{x - x_3}\right) = \mathrm{div}(ax + by + c) - \mathrm{div}(x - x_3) = [P_1] + [P_2] - [-P_3] - [\infty].$$

Com que $P_1 + P_2 = -P_3$, podem reescriure la darrera equació com

$$[P_1] + [P_2] = [P_1 + P_2] + [\infty] + \mathrm{div}\left(\frac{ax + by + c}{x - x_3}\right)$$

□

Teorema 2.22. *Sigui E una corba el·líptica. Sigui D un divisor a E amb $gr(D) = 0$. Aleshores existeix una funció f a E tal que*

$$\mathrm{div}(f) = D$$

si i només si

$$sum(D) = \infty$$

.

Demostració. Considerem el divisor

$$D = \sum_{j=1}^{k} a_j[P_j] \quad a_j \in \mathbb{Z},$$

Fent abús de notació, si reordenem els termes positius i negatius, podem reescriure el divisor D de la forma següent

$$D = [P_1] + \ldots + [P_p] - ([Q_1] + \ldots + [Q_n]).$$

On $p + n = \sum a_j$ i considerant que poden haver punts repetits en els casos on $a_j \neq -1, 1$.

Al lema anterior, acabem hem demostrat que el divisor $[P_1] + [P_2]$ es pot substituir per $[P_1 + P_2] + [\infty] + \mathrm{div}(g)$, per alguna funció racional g.

Aleshores

$$[P_1] + [P_2] + [P_3] = [P_1 + P_2] + [\infty] + \mathrm{div}(g_1) + [P_3] =$$

$$[P_1 + P_2 + P_3] + 2[\infty] + \mathrm{div}(g_1) + \mathrm{div}(g_2) =$$

$$[P_1 + P_2 + P_3] + 2[\infty] + \mathrm{div}(g_1 \cdot g_2))$$

D'aquesta manera, aplicant aquest resultat iterativament, podem veure que existeixen punts P, Q, una funció racional G (per ser producte de funcions racionals) , i un nombre enter m tal que el divisor D es pot reescriure com

$$D = [P] - [Q] + m[\infty] + \mathrm{div}(G).$$

Observem també que la igualtat

$$[P_1] + [P_2] = [P_1 + P_2] + [\infty] + \mathrm{div}(g)$$

Ens permet veure que

$$\mathrm{div}(g) = [P_1] + [P_2] - [P_1 + P_2] - [\infty.]$$

I aplicant la funció suma veiem que

$$\mathrm{sum}(\mathrm{div}(g)) = P_1 + P_2 - (P_1 + P_2) - \infty = \infty.$$

Ara, com que la funció

$$G = g_1 \cdot g_2 \dots g_{(p+m-2)}$$

és producte de funcions racionals i $\text{sum}(\text{div}(g_i)) = \infty$ per a cada i, podem veure que

$$\text{div}(G) = \sum_{i=1}^{p+m-2} \text{div}(g_i) \quad \Rightarrow \quad \text{sum}(\text{div}(G)) = \sum_{i=1}^{p+m-2} \text{sum}(\text{div}(g_i)) = \infty$$

Recordem que no hi ha cap problema al distribuir la funció sum al sumatori de divisors, degut a la condició de homomorfisme d' aquesta funció. A més, degut a la proposició 2.16, sabem que $\text{gr}(\text{div}(G)) = 0$.

Recuperant el divisor D

$$D = [P] - [Q] + m[\infty] + \text{div}(G)$$

veiem que

$$0 = \text{gr}(D) = 1 - 1 + m + 0 = m.$$

Aleshores podem veure que el divisor original té la forma

$$D = [P] - [Q] + \text{div}(G).$$

Finalment, veiem que

$$\text{sum}(D) = P - Q + \text{sum}(\text{div}(G)) = P - Q + \infty = P - Q.$$

Suposem ara que $\text{sum}(D) = \infty$. Llavors $P - Q = \infty$, així que $P = Q$ i $D = \text{div}(G)$.

Recíprocament, suposem que $D = \text{div}(f)$ per a alguna funció f.

Aleshores

$$\text{div}(f) = [P] - [Q] + \text{div}(G) \quad \Rightarrow \quad [P] - [Q] = \text{div}(f/G).$$

Prenent $h := f/G$, el lema 2.20 ens diu que en aquesta situació, $P = Q$, i aleshores $\text{sum}(D) = \infty$. Això completa la demostració.

□

Corołari 2.23. *La aplicació*

$$\text{sum} : \text{Div}^0(E)/(\textit{divisors principals}) \longrightarrow E(\overline{K})$$

és un isomorfisme de grups.

Demostració. Degut a que $\text{sum}([P] - [\infty]) = P$, l' aplicació és exhaustiva. El teorema 2.22 ens diu que el nucli d'aquesta aplicació està format exactament pels divisors de funcions (*divisors principals*). □

Exemple 2.24. La demostració del teorema 2.22 ens dóna un algoritme per trobar una funció amb un divisor concret (de grau 0 i suma igual a ∞). Considerem la corba el·líptica E sobre $\mathbb{F}_{11}$ donada per l'equació

$$y^2 = x^3 + 4x.$$

Sigui

$$D = [(0,0)] + [(2,4)] + [(4,5)] + [(6,3)] - 4[\infty].$$

D té grau 0 i un càlcul senzill mostra que $\mathrm{sum}(D) = \infty$. Per tant, pel teorema 2.22, D és el divisor d'una funció.

Trobem la funció. La recta que passa per $(0,0)$ i $(2,4)$ és $y - 2x = 0$. Trobem la intersecció amb E i veiem que és tangent a $(2,4)$

$$\mathrm{div}(y - 2x) = [(0,0)] + 2[(2,4)] - 3[\infty].$$

La recta vertical que passa per $(2,4)$ és $x - 2 = 0$, i

$$\mathrm{div}(x - 2) = [(2,4)] + [(2,-4)] - 2[\infty].$$

Per tant,

$$D = [(2,-4)] + \mathrm{div}\left(\frac{y-2x}{x-2}\right) + [(4,5)] + [(6,3)] - 3[\infty].$$

De manera similar, tenim

$$[(4,5)] + [(6,3)] = [(2,4)] + [\infty] + \mathrm{div}\left(\frac{y+x+2}{x-2}\right),$$

que dóna

$$D = [(2,-4)] + \mathrm{div}\left(\frac{y-2x}{x-2}\right) + [(2,4)] + \mathrm{div}\left(\frac{y+x+2}{x-2}\right) - 2[\infty].$$

Com que ja hem calculat $\mathrm{div}(x-2)$, utilitzem això per concloure que

$$D = \mathrm{div}(x-2) + \mathrm{div}\left(\frac{y-2x}{x-2}\right) + \mathrm{div}\left(\frac{y+x+2}{x-2}\right) = \mathrm{div}\Big(\frac{(y-2x)(y+x+2)}{x-2}\Big).$$

Aquesta funció es pot simplificar. El numerador és

$$\begin{aligned}(y-2x)(y+x+2) &= y^2 - xy - 2x^2 + 2y - 4x \\ &= x^3 - xy - 2x^2 + 2y \qquad (\text{doncs} \quad y^2 = x^3 + 4x) \\ &= (x-2)(x^2 - y)\end{aligned}$$

I aleshores,

$$D = \mathrm{div}(x^2 - y).$$

2.5 El grup de torsió

Els punts de torsió, és dir els punts d'ordre finit, tenen un paper fonamental en l'estudi de les corbes el·líptiques. Aquests seràn crucials per entendre el concepte central del treball, l'emparellament de Weil.

Definició 2.25. *Sigui E una corba el·líptica definida sobre un cos K. Sigui n un nombre natural. Definim el subgrup de n-torsió com:*

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}$$

Remarquem que els punts de $E[n]$ tenen coordenades en la clausura algebraica $\overline{K}$.

Problema 2.26. Calculem explícitament els primers grups de torsió per intuir la seva estructura. Recordem que sempre estem considerant que treballem sobre cossos amb característica $\neq 2, 3$.

Podem expressar la corba E de la forma

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

amb $e_1, e_2, e_3 \in \overline{K}$. Un punt P satisfà $2P = \infty$ si i només si la recta tangent a P és vertical. És fàcil veure que això significa que $y = 0$, així que

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

Com a grup abstracte, és isomorf a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Ara mirem $E[3]$. Un punt P satisfà $3P = \infty$ si i només si $2P = -P$. Això significa que la coordenada x de $2P$ és igual a la coordenada x de P (les coordenades y difereixen en signe).

En equacions, això esdevé

$$m^2 - 2x = x, \quad \text{on} \quad m = \frac{3x^2 + A}{2y}.$$

Utilitzant el fet que $y^2 = x^3 + Ax + B$, trobem que

$$(3x^2 + A)^2 = 12x(x^3 + Ax + B).$$

Això es simplifica a

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

El discriminant d'aquest polinomi és $-6912(4A^3 + 27B^2)^2$, que és diferent de zero. Per tant, el polinomi no té arrels múltiples. Hi ha 4 valors diferents de x (a $\overline{K}$), i cada x produeix dues valors de y, així que tenim vuit punts d'ordre 3. Com que ∞ també pertany a $E[3]$, veiem que $E[3]$ és un grup d'ordre 9 en què cada element és d'ordre 3. Concloem en que

$$E[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3.$$

L'estructura general ve descrita pel següent resultat.

Teorema 2.27. *Sigui E una corba el·líptica sobre un cos K i n un nombre natural. Si la característica de K no divideix a n o és 0, aleshores*

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Demostració. La prova d'aquest resultat és calculísticament molt extensa i no tan interessant per l'objectiu del nostre treball . Veure [1, Cap 3] per una demostració completa d'aquest teorema. □

Observació 2.28. Si n és un nombre natural tal que la característica de K no divideix a n, aleshores si escollim una base β_1, β_2 de $E[n]$, podem escriure tot element P de $E[n]$ de la forma

$$P = a_1\beta_1 + a_2\beta_2,$$

on a_1, a_2 són nombres enters determinats únicament mod n.

2.6 L'emparellament de Weil

Sigui E una corba el·líptica definida sobre un cos K amb car$(K)= k$. Considerem un nombre natural n tal que $k \nmid n$. Aleshores a la secció anterior hem vist que

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Considerem ara el conjunt de les arrels $n-$èssimes de la unitat, és dir

$$\mu_n = \{x \in \overline{K} \mid x^n = 1\}$$

Com que la característica de K no divideix a n, sabem que l' equació $x^n = 1$ té totes les arrels diferents, i en conseqüència, μ_n és un grup cíclic d'ordre n.

En aquest context, l' objectiu d'aquesta secció és construir una aplicació bilineal

$$e_n : E[n] \times E[n] \to \mu_n.$$

2.6.1 Construcció de *l'emparellament de Weil*

Sigui $T \in E[n]$. Segons el Teorema 2.22, existeix una funció f a E tal que

$$\text{div}(f) = n[T] - n[\infty].) \tag{2.2}$$

Escollim $T' \in E[n^2]$ tal que $nT' = T$. Farem servir el Teorema 2.22 per demostrar que existeix una funció g tal que

$$\text{div}(g) = \sum_{R \in E[n]} ([T' + R] - [R]).$$

Per poder aplicar el teorema, hem de verificar que la suma dels punts al divisor és ∞. Això es dedueix del fet que hi ha n^2 punts R a $E[n]$.

$$\text{sum}(g) = \sum_{R \in E[n]} (T' + R) - R = \sum_{R \in E[n]} T' = n^2 T' = \infty,$$

doncs hem escollit $T' \in E[n^2]$. Notem que g no depèn de la elecció de T' ja que dues eleccions diferents per a T difereixen en un element $R \in E[n]$.

Sigui $f \circ n$ la funció que multiplica un punt per n, i després aplica f. Els punts $P = T' + R$ amb $R \in E[n]$ són els punts P amb $nP = T$. Es dedueix doncs que

$$\text{div}(f \circ n) = n \sum_{R \in E[n]} [T' + R] - n \sum_{R \in E[n]} [R] = \text{div}(g^n).$$

Aleshores, $f \circ n$ és un múltiple constant de g^n. Multiplicant f per una constant adequada, podem assumir que

$$f \circ n = g^n.$$

Aleshores, sigui $S \in E[n]$ i un punt qualsevol$P \in E(\overline{K})$.

$$g(P+S)^n = f(n(P+S)) = f(nP) = g(P)^n.$$

Això implica que

$$g(P+S)/g(P) \ \in \mu_n.$$

Definim ***l'aparellament de Weil*** (sobre el grup de n-torsió) com

$$e_n(S,T) = \frac{g(P+S)}{g(P)}.$$

Com que g es determina en funció a un múltiple escalar pel seu divisor, aquesta definició és independent de la elecció de g.

Observació 2.29. Es pot veure que de fet, $g(P+S)/g(P)$ és independent del punt P escollit. La prova d'això és prou tècnica i només donarem un croquis de la demostració: A la topologia de Zariski, la funció $g(P+S)/g(P)$ és contínua respecte P i E és un espai connex. Aleshores com que la imatge de la funció és un conjunt finit i discret, la funció $g(P+S)/g(P)$ ha de ser constant. Veure [1, Cap. 11.2].

Teorema 2.30. *Sigui E una corba el·líptica definida sobre un cos K i considerem un nombre natural n tal que la característica de K no divideix a n. Aleshores l'* ***emparellament de Weil*** *sobre el grup de n-torsió*

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

satisfà les següents propietats:

1. *e_n és bilineal en cada variable, és dir*

$$e_n(S_1+S_2,T) = e_n(S_1,T)\cdot e_n(S_2,T)$$

$$e_n(S,T_1+T_2) = e_n(S,T_1)\cdot e_n(S,T_2)$$

   per a cada $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. *e_n és no degenerat en cada variable. Això significa que si $e_n(S,T) = 1$ per a tot $T \in E[n]$, llavors $S = \infty$, i també que si $e_n(S,T) = 1$ per a tot $S \in E[n]$, llavors $T = \infty$.*

3. *$e_n(T,T) = 1$ per a tot $T \in E[n]$.*

4. *És alternant, és dir,*
   $e_n(T,S) = e_n(S,T)^{-1}$ per a tot $S, T \in E[n]$.

5. *És invariant Galois,*
   $e_n(\sigma S, \sigma T) = \sigma(e_n(S,T))$ per a tot automorfisme σ de $\mathrm{Gal}(\overline{K}/K)$.

Demostració. 1. Com que e_n és independent del punt P, podem calcular el pairing amb P i $P + S_1$ i veiem

$$\begin{aligned} e_n(S_1, T)e_n(S_2, T) &= \frac{g(P + S_1)}{g(P)} \frac{g(P + S_1 + S_2)}{g(P + S_1)} \\ &= \frac{g(P + S_1 + S_2)}{g(P)} \\ &= e_n(S_1 + S_2, T) \end{aligned}$$

Això prova la linealitat a la primera variable.

Ara, suposem $T_1, T_2, T_3 \in E[n]$ amb $T_1 + T_2 = T_3$. Per cada $1 \leq i \leq 3$, considerem f_i, g_i les funcions corresponents per definir $e_n(S, T_i)$. Pel teorema 2.22, sabem que existeix una funció h tal que

$$\mathrm{div}(h) = [T_3] - [T_1] - [T_2] + [\infty].$$

L' equació (2.2) de la construcció de les f_i, ens permet veure que

$$\mathrm{div}\Big(\frac{f_3}{f_1 f_2}\Big) = n\mathrm{div}(h) = \mathrm{div}(h^n).$$

Aleshores, ha d'existir una constant $c \in \overline{K}^{\times}$ tal que

$$f_3 = c f_1 f_2 h^n.$$

Això implica que

$$g_3 = c^{1/n}(g_1)(g_2)(h \circ n).$$

La pròpia definició de e_n implica

$$e_n(S, T_1 + T_2) = \frac{g_3(P + S)}{g_3(P)} = \frac{g_1(P + S)g_2(P + S)h(n(P + S)}{g_1(P)g_2(P)h(nP)} = e_n(S, T_1)e_n(S, T_2),$$

ja que $nS = \infty$, i en conseqüència, $h(n(P + S)) = n(nP)$. Queda doncs provada la linealitat a la segona variable.

2. Suposem que $T \in E[n]$ és tal que $e_n(S,T) = 1$ per a tot $S \in E[n]$. Això significa que $g(P+S) = g(P)$ per a tot P i per a tot $S \in E[n]$. Es pot demostrar que aleshores, existeix una funció h tal que $g = h \circ n$. (*Per una prova completa, podeu veure* [1, Prop. 9.34], [5, Teorema 4.10b]). Aleshores

$$(h \circ n)^n = g^n = f \circ n.$$

Com que la multiplicació per n és exhaustiva a $E(\overline{K})$, tenim $h^n = f$. Per tant,

$$n \operatorname{div}(h) = \operatorname{div}(f) = n[T] - n[\infty],$$

així que $\operatorname{div}(h) = [T] - [\infty]$. Segons el Teorema 2.22, tenim $T = \infty$. Això demostra la meitat de (2), la no degeneració en l'altre variable surt directment assumint la propietat (4), que provarem més endavant. Suposem doncs que $e_n(S,T) = 1$ per a tot $T \in E[n]$, aleshores en particular, $e_n(T,S)^{-1} = 1 \implies e(T,S) = 1$ per a tot T i acabem de provar que aleshores $S = \infty$.

3. Considerem τ_{jT} com la representació d'afegir jT, de manera que $f \circ \tau_{jT}$ denota la funció $P \mapsto f(P + jT)$. El divisor de $f \circ \tau_{jT}$ és $n[T - jT] - n[-jT]$. Per tant,

$$\operatorname{div}\left(\prod_{j=0}^{n-1} f \circ \tau_{jT}\right) = \sum_{j=0}^{n-1} (n[(1-j)T] - n[-jT]) = 0.$$

Això significa que $\prod_{j=0}^{n-1} f \circ \tau_{jT}$ és constant. La n-èssima potència de la funció $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ és el producte anterior de f compost amb la multiplicació per n, per tant, també és constant. Ja que

$$\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n = \prod_{j=0}^{n-1} f \circ n \circ \tau_{jT'} = \prod_{j=0}^{n-1} f \circ \tau_{jT} \circ n \quad (\text{ja que } nT' = T),$$

Com que hem demostrat que aquest darrer producte és constant, es dedueix que $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ és constant (tornem a utilitzar la connexió de E en la topologia de Zariski). Aleshorea, té el mateix valor a P i $P+T$, de manera que

$$\sum_{j=0}^{n-1} g(P + T' + jT') = \sum_{j=0}^{n-1} g(P + jT').$$

Cancel·lant els termes comuns (suposem que P està triat de manera que tots els termes són finits i no nuls) obtenim

$$g(P + nT') = g(P).$$

Com que $nT' = T$, tenim que

$$e_n(T,T) = \frac{g(P+T)}{g(P)} = 1$$

.

4. Utilitzant (1) i (3) veiem que

$$1 = e_n(S+T, S+T) = e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T) = e_n(S,T)e_n(T,S).$$

Per tant, $e_n(T,S) = e_n(S,T)^{-1}$.

5. Sigui σ un automorfisme de $\mathrm{Gal}(\overline{K}/K$. Llavors, clarament com per hipòtesi f té un zero en $T = (x_0, y_0)$, tenim que

$$f(x_0, y_0) = \frac{P(x_0, y_0)}{Q(x_0, y_0)} = 0$$

Si apliquem σ, tenim que

$$(f(x_0, y_0))^\sigma = f^\sigma(\sigma(x_0), \sigma(y_0)) = \sigma(0) = 0$$

(Denotem f^σ per indicar la funció racional a la qual hem aplicat σ al seus coeficients). Aleshores podem veure que

$$\mathrm{div}(f^\sigma) = n[\sigma T] - n[\infty]$$

i de manera similar construim g^σ. Per tant, f^σ, g^σ són les funcions corresponents a la construcció de l'emparellament per σT, i aleshores

$$\sigma(e_n(S,T)) = \frac{\sigma(g(P+S))}{\sigma(g(P))} = \frac{g^\sigma(\sigma P + \sigma S)}{g^\sigma(\sigma P)} = e_n(\sigma S, \sigma T).$$

□

Corołari 2.31. *Sigui T_1, T_2 una base de $E[n]$. Aleshores $e_n(T_1, T_2)$ és una n-èssima arrel primitiva de la unitat.*

Demostració. Suposem que $e_n(T_1, T_2) = \xi$ amb $\xi^d = 1$. Aleshores, $e_n(T_1, dT_2) = 1$. També $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$. (Aplicant (1) i (3)).

Sigui ara $S \in E[n]$. Aleshores $S = aT_1 + bT_2$ per determinats nombres enters a, b. Aleshores

$$e_n(S, dT_2) = e_n(T_1, T_2)^a e_n(T_2, dT_2)^b = 1.$$

Com aquesta igualtat es compleix per a tot S, aplicant (2) podem veure que $dT_2 = \infty$. Això és cert si i només si $n \mid d$ i aleshores ξ és arrel primitiva n-èssima de la unitat. □

Corołari 2.32. *Si $E[n] \subseteq E(K)$, aleshores $\mu_n \subseteq K$.*

Recordem que en principi, els punts de $E[n]$ tenen coordenades en $E(\overline{K})$.

Demostració. Ara, considerem qualsevol automorfisme $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Sigui T_1, T_2 una base de $E[n]$. Com que estem suposant que T_1, T_2 tenen coordenades en K, tenim que $\sigma T_1 = T_1$ i $\sigma T_2 = T_2$. Aplicant el corolari anterior, veiem $e_n(T_1, T_2) = \xi$, on ξ és una n-èssima arrel primitiva de la unitat. Aleshores

$$\xi = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\xi).$$

El teorema fonamental de la teoria de Galois ens diu que si hi ha un element $\xi \in \overline{K}$ queda fixat per a tot automorfisme $\sigma \in \mathrm{Gal}(\overline{K}/K)$, aleshores $\xi \in K$. Com que ξ era una arrel primitiva de la unitat, directament veiem que $\mu_n \subset K$.

(Detall tècnic: L'extensió $\overline{K}/K$ no té perquè ser finita. Per aquest fet, aplicar la teoria de Galois no és tan fàcil com podria semblar. Realment, el teorema fonamentalde a teoria de Galois només implica que en aquest cas ξ viu a una extensió purament inseparable de K. Però, una $n-$èssima arrel primitiva de la unitat genera una extensió $K(\zeta_n)/K$ que en el nostre cas, com que $\mathrm{car}(K) \nmid n$, sí que és separable. Trivialment, també és normal i per tant efectivament és una extensió Galoisiana i podem concluir que $\xi \in K$.)

□

3 Esquemes de compartició de secrets

Anomenem esquemes de compartició de secrets (també anomenat divisió de secrets) a mètodes per distribuir un secret entre un conjunt d' usuaris, de manera que cap usuari tingui cap informació intel·ligible sobre el secret, però quan un nombre suficient d'usuaris treballen junts, el secret es pot reconstruir. El *Distribuïdor (Dealer)* és l'encarregat de generar i repartir el secret.

Els esquemes de compartició de secrets són ideals per emmagatzemar informació altament sensible. Exemples pràctics poden ser claus d'encriptació, codis de llançament de míssils o comptes bancaris numerats. Cadascuna d'aquestes peces d'informació ha de mantenir-se altament confidencial, ja que la seva exposició podria ser desastrosa; no obstant això, també és crític que no es perdin. Per aquest motiu, són útils en situacions on alguns participants poden estar fora de servei, doncs encara que alguns participants no siguin disponibles el secret es pot reconstruir si hi ha prou participants restants. A més distribueixen l' autoritat i la presa de decisions, proporcionant seguretat contra participants que puguin obrar de forma maliciosa.

Definició 3.1 (Fragment)**.** *Anomenem fragment (del secret) a la part d' informació privada que rep cada usuari que participa en l' esquema.*

Definició 3.2 (Subconjunt autoritzat i estructura d'accés)**.** *Un subconjunt d'usuaris capaç de reconstruir el secret s'anomena subconjunt autoritzat i la col·lecció de tots els subconjunts autoritzats s'anomena estructura d'accés.*

Definició 3.3 (Nombre llindar)**.** *Sigui t un nombre natural. Direm que t és el nombre llindar de l' esquema si qualsevol subconjunt de com a mínim t usuaris formen un subconjunt autoritzat.*

Observació 3.4. Cap fragment pot donar informació significativa del secret. Més específicament, sigui t el nombre llindar d' un esquema amb secret S, la probabilitat d' endevinar S coneixent $t-1$ fragments del secret ha de ser igual a la probabilitat d' endevinar-lo no coneixent-ne cap. Naturalment, aquesta probabilitat ha de ser negligible.

3.1 Esquema jeràrquic conjuntiu de compartició de multi-secrets

L'esquema de Chintamani, Paul i Sa [2] que presentarem a continuació aporta una sèrie de propietats importants respecte d' altres esquemes coneguts, a saber-ne:

1. És un esquema multi-secrets, és dir, es poden compartir diversos secrets entre els usuaris de manera que qualsevol subconjunt autoritzat d'usuaris pugui recuperar tots els secrets. No obstant això, qualsevol subconjunt no autoritzat d'usuaris no obté cap informació sobre cap dels secrets.

2. Permet establir diferents rangs d' autoritat, dividint els usuaris en diferents graus de jerarquia.

3. És verificable, és dir, els usuaris poden utilitzar informació pública per comprovar si la informació compartida per un altre usuari és vàlida.

4. A més, el distribuïdor de l' esquema no necessita un canal segur, ja que distribueix el fragments ja encriptats i de manera pública.

A continuació, definim formalment quins són els subconjunts autoritzats de l' esquema de Chintamani et al.

Definició 3.5 (Estructura d'accés jeràrquica conjuntiva)**.** *Sigui U un conjunt de n usuaris dividit en m nivells disjunts $L_1, L_2, \ldots, L_m$. Definim: L_i com a nivell superior a L_j si $i < j$. Sigui t_i el nombre llindar pel nivell L_i o superior, i $t_1 \leq t_2 \leq \ldots \leq t_m$. Aleshores, la estructura d'accés jeràrquica conjuntiva es defineix com:*

$$\Gamma = \{A \subseteq U : |A \cap (\bigcup_{j=1}^{m} L_j)| \geq t_i \text{ per tot } i, 1 \leq i \leq m.\}$$

Observació 3.6. L' adjectiu d' estructura conjuntiva vol dir que un conjunt d'usuaris pot reconstruir el secret si conté com a mínim t_i usuaris de estrictament cada nivell L_i o superior.

3.1.1 Preliminars

Abans de veure l' esquema, necessitarem presentar 2 resultats tècnics d' àlgebra lineal.

Proposició 3.7. *Siguin m_1, m_2, i t enters positius. Suposem que coneixem b_1, b_2, ..., $b_{m_1} \in \mathbb{F}_l$. Si $t > m_1$, llavors existeix una matriu A de $m_1 \times t$ i una matriu B de $m_2 \times t$ tal que qualsevol conjunt de t files de la matriu M,*

$$M = \begin{bmatrix} A \\ B \end{bmatrix},$$

forma una submatriu invertible de M, i el sistema $AX = \begin{pmatrix} b_1 & b_2 & \ldots & b_{m_1} \end{pmatrix}^T$ té diferents solucions $X \in \mathbb{F}^t$.

Demostració. Suposem que trobem una matriu M de $(m_1 + m_2) \times t$ tal que qualsevol conjunt de t files de M formi una submatriu invertible. Deixem que M sigui

$$M = \begin{bmatrix} A \\ B \end{bmatrix},$$

on A és una submatriu de $m_1 \times t$ i B és una submatriu de $m_2 \times t$. Com que $t > m_1$, el rang d'A és m_1. Es segueix que el sistema $AX = \begin{bmatrix} b_1 & b_2 & \dots & b_{m_1} \end{bmatrix}^T$ té diferents solucions, com es requeria.

□

Proposició 3.8. *Siguin m_1, m_2 i t enters positius amb $t \leq m_1$. Suposem que coneixem b_1, b_2, ..., $b_{m_1} \in \mathbb{F}_l$. Per a qualsevol enter t' que satisfaci $m_1 < t' \leq m_1 + m_2$, existeix una matriu M,*

$$M = \begin{bmatrix} A & A' \\ B & B' \end{bmatrix},$$

on A i B són matrius de mida $m_1 \times t$ i $m_2 \times t$ respectivament, A' i B' són matrius de mida $m_1 \times (t' - t)$ i $m_2 \times (t' - t)$, respectivament. A més, les primeres t columnes de qualsevol conjunt de t files de M formen una submatriu invertible, i el sistema $AX = \begin{pmatrix} b_1 & b_2 & \dots & b_{m_1} \end{pmatrix}^T$ té diferents solucions.

Demostració. Com abans, seleccionem les matrius A i B de mida $m_1 \times t$ i $m_2 \times t$, respectivament, de manera que qualsevols t files de la matriu

$$\begin{bmatrix} A \\ B \end{bmatrix}$$

formin una submatriu invertible. Com que $t \leq m_1$, la dimensió de l'espai de columnes d'A és t. Sigui $v_1, v_2, \dots, v_t \in \mathbb{F}_l^{m_1}$ els vectors columna d'A. Sigui W un subespai de $\mathbb{F}_l^{m_1}$ tal que $< v_1, v_2, \dots, v_t > + W = \mathbb{F}_l^{m_1}$ i la dimensió de W és $m_1 - t$. Segons la hipòtesi sobre t', tenim $t' - t \geq m_1 - t$. Així doncs, podem seleccionar vectors columna $w_1, w_2, \dots, w_{t'-t} \in \mathbb{F}_l^{m_1}$ que generin W.

Ara, sigui A' sigui la matriu formada pels vectors columna $w_1, w_2, \dots, w_{t'-t}$ i sigui B' qualsevol matriu de mida $m_2 \times (t' - t)$. Com que les columnes de les matrius A i A' generen tot $\mathbb{F}_l^{m_1}$, tenim que el rang de $\begin{bmatrix} A & A' \end{bmatrix}$ és m_1. Per tant, el sistema $\begin{bmatrix} A & A' \end{bmatrix} X = \begin{bmatrix} b_1 & b_2 & \dots & b_{m_1} \end{bmatrix}^T$ té diferents solucions. Definint $M = \begin{bmatrix} A & A' \\ B & B' \end{bmatrix}$, tenim el resultat desitjat.

□

Observació 3.9. A l'article original de Chintamani et al. treballen amb un tipus de matrius anomenades *matrius generadores d' un codi de màxima distància separable (Matrius MDS).* Aquestes matrius definides amb paràmetres $[n, k, d]$ tenen la propietat de que qualsevols k files formen una submatriu invertible. La demostració d'aquest resultat queda lluny del tema d' aquest treball i la podem trobar a ([8, Teorema 2.4.3]). La generació d' aquestes matrius es pot implementar amb les llibreries de *SageMath.*

3.2 Implementació del protocol

Com que l'esquema treballa amb corbes el·líptiques i emparellaments bilineals, recordem breument la seva definició.

Considerem un cos finit $\mathbb{F}_q$ amb característica $\neq 2, 3$. Sabem que aleshores podem descriure una corba el·líptica E com la gràfica de la equació:

$$E : y^2 = x^3 + ax + b.$$

Recordem que aquestes corbes són no singulars, és dir, corbes tals que $16(4a^3+27b^2) \neq 0$. El grup $E(\mathbb{F}_q)$ és la col·lecció de punts de $\mathbb{F}_q$ sobre la corba el·líptica més el punt a l'infinit O que és l'element identitat del grup.

Definició 3.10. *Sigui el nombre de punts a $E(\mathbb{F}_q)$ un múltiple de l, on l és un nombre primer i $mcd(l, q) = 1$. Definim el grau d'incrustació (embedding degree) de $E(\mathbb{F}_q)$ amb respecte a l com el nombre natural k més petit tal que $l \mid q^k - 1$.*

Notació 2. *Sigui k el grau d'incrustació de $E(\mathbb{F}_q)$ sobre l. Escriurem $E[l]$ per indicar la col·lecció de punts de l-torsió a $E(\mathbb{F}_{q^k})$.*

Notació 3. *Sigui k el grau d'incrustació de $E(\mathbb{F}_q)$ sobre l. Escriurem μ_l per indicar el subgrup d'ordre l del grup multiplicatiu $\mathbb{F}^*_{q^k}$.*

Es poden definir molts tipus d'emparellaments bilineals utilitzant corbes el·líptiques i molts poden ser aplicables a aquest mateix esquema. En el nostre exemple, treballarem amb l'emparellament de Weil.

L' emparellament de Weil e és una aplicació $e : E[l] \times E[l] \to \mu_l$ definida al capítol 2. Aquesta aplicació pot ser implementada eficientment amb l' algoritme de Miller [3].

Observació 3.11. És necessari en la majoria de casos extendre el cos $E(\mathbb{F}_q)$ a $E(\mathbb{F}_{q^k})$ perquè l'emparellament no sigui degenerat. Això es dona perquè $\mu_n \subseteq \mathbb{F}^*_q$ si i només si $l \mid q - 1$.

3.2.1 Preparació i distribució dels fragments

Considerem una corba el·líptica E sobre un cos finit $\mathbb{F}_q$, on $q = p^r$ per a algun $r \in \mathbb{N}$ i p és un nombre primer gran. Siguin $P, P' \in E(\mathbb{F}_{q^k})$ punts d'ordre l, on l és un nombre primer i k és el grau d'embedding de $E(\mathbb{F}_q)$. Suposem que l és prou gran com perquè el problema del logaritme discret de la corba el·líptica (ECDLP) sigui difícil de resoldre.

Considerem e l'emparellament de Weil, definit al primer capítol:

$$e : E[l] \times E[l] \to \mu_l$$

Considerem l' estructura d' accés Γ de la definició 3.5 i suposem que hi ha un conjunt U de n usuaris i un Distribuïdor de confiança D. El Distribuïdor té l'autoritat per generar i publicar tots els paràmetres de l'esquema. Els usuaris es divideixen en m nivells disjunts $L_1, L_2, \ldots, L_m$.

Sigui $|L_i| = n_i$ i t_i el llindar per al nivell L_i o superior per a $i = 1, 2, \ldots, m$. El nivell superior és L_1 i L_m és el nivell més baix. Assumim que $t_1 \leq t_2 \leq \ldots \leq t_m$. Suposem que hi ha s secrets, diguem-ne $K_1, K_2, \ldots, K_s$, que es compartiran entre els usuaris. El Distribuïdor fa P públic.

Anomenem u_{ij} al j-èssim usuari del nivell L_i

Nivell L_1

- Considerem una matriu M_1 d'ordre $n_1 \times t_1$ tal que qualsevols t_1 files formin submatriu de M_1 invertible.
- El distribuïdor D tria t_1 nombres enters aleatoris $a_{11}, a_{12}, \ldots, a_{1t_1} \in [0, l-1]$ i computa
$$(b_{11} b_{12} \ldots b_{1n_1})^T = M_1 \cdot (a_{11} a_{12} \ldots a_{1t_1})^T$$
- Cada usuari u_{1j} del nivell L_1, tria $x_{1j} \in [1, l-1]$ aleatòriament i publica $x_{1j}P$.
- Aleshores, el distribuïdor D computa $b_{1j} x_{1j} P$ per a cada usuari u_{1j}, $j = 1, 2, \ldots, n_1$, i ho publica.
- Cada u_{1j} obtindrà el seu fragment $b_{1j}P$ calculant $x_{1j}^{-1}(b_{1j}x_{1j})P$.

Nivell L_i Cas 1 Suposem que $t_i > \sum_{k=1}^{i-1} n_k$.

- Considerem una matriu M_i d'ordre $(n_1 + n_2 + \ldots + n_i) \times t_i$ tal que qualsevol t_i files formin una matriu invertible.
- El distribuïdor D tria t_i valors $a_{i1}, a_{i2}, \ldots, a_{iti} \in [0, l-1]$ i computa
$$(b_{11} \ldots b_{1n_1} b_{21} \ldots b_{2n_2} \ldots b_{i1} \ldots b_{ini})^T = M_i \cdot (a_{i1} a_{i2} \ldots a_{iti})^T$$
de manera que b_{sj}, $s = 1, 2, \ldots, i-1$, $j = 1, 2, \ldots, n_s$, coincideixin amb els nivells anteriors. Això és possible gràcies a la Proposició 3.7.

- Cada usuari u_{ij} en el nivell L_i, tria $x_{ij} \in [1, l-1]$ aleatòriament i publica $x_{ij}P$ per $j = 1, 2, \ldots, n_i$.
- Després, el distribuïdor D computa $b_{ij}x_{ij}P$ per a cada u_{ij} i ho publica. Cada u_{ij} pot obtenir el seu fragment $b_{ij}P$ calculant $x_{ij}^{-1}(b_{ij}x_{ij})P$.

Nivell L_i Cas 2 Suposem que $t_i \leq \sum_{k=1}^{i-1} n_k$.

- Considerem una matriu M_i d'ordre $(n_1 + n_2 + \ldots + n_i) \times t_i'$, on $\sum_{k=1}^{i-1} n_k < t_i' \leq \sum_{k=1}^{i} n_k$, de manera que les primeres t_i columnes de qualsevols t_i files formin una submatriu invertible de M_i.
- El distribuïdor D tria t_i' valors $a_{i1}, a_{i2}, \ldots, a_{iti}, \ldots, a_{it_i'}$ de l'interval $[0, l-1]$ i computa

  $$(b_{11} \cdot \ldots \cdot b_{1n_1} \cdot \ldots \cdot bi_1 \cdot \ldots \cdot b_{ini})^T = M_i \cdot (a_{i1} \cdot a_{i2} \cdot \ldots \cdot a_{iti} \cdot \ldots \cdot a_{it_i'})^T,$$

  de manera que b_{sj} per a $s = 1, 2, \ldots, i-1$ i $j = 1, 2, \ldots, n_s$ coincideixin amb els nivells anteriors. Això és possible gràcies a la Proposició 3.8.
- Dels a_{ij} valors, per $j \in [1, t_i']$, el distribuidor publica $a_{iti+1} \cdot \ldots \cdot a_{it_i'}$
- Cada usuariu_{ij} del nivell L_i tria $x_{ij} \in [1, l-1]$ de manera aleatòria i publica $x_{ij}P$.
- Després, el distribuïdor D computa $b_{ij}x_{ij}P$ per a cada u_{ij} i ho publica. Cada usuari u_{ij} pot obtenir el seu fragment $b_{ij}P$ calculant $x_{ij}^{-1}(b_{ij}x_{ij})P$.

Ara que tots els fragments s'han repartit el distribuïdor D tria claus secretes $K_i \in [0, p-1]$ i sigui

$$Q = \sum_{j=1}^{m} a_{j1}P$$

calcula $v_i = e(P', i \cdot Q) + K_i$, per $1 \leq i \leq s$. Finalment, D publica v_i, $1 \leq i \leq s$, i M_j, $1 \leq j \leq m$.

Observació 3.12. Quan operem amb punts de la corba, per exemple sigui $P \in E(\mathbb{F}_q)$, $aP + bP$ indica l'operació del grup de punts de la corba el·líptica i no una suma convencional. A més, fem notar que per a qualsevol $P_1, P_2 \in E[l]$, $e(P_1, P_2) \in \mu_l \subseteq \mathbb{F}_{q^k}^* \subseteq \mathbb{F}_{q^k}$. També, per a $K \in [0, p-1]$, tenim $K \in \mathbb{F}_{q^k}$. Així doncs, $v = e(P_1, P_2) + K$ és a $\mathbb{F}_{q^k}$.

Observació 3.13. A l'article original de Chintamani et al. [2] $v_i = e(P, i \cdot Q) + K_i = e(P, aP) + K_i$ per algun $a \in \mathbb{F}_q$. En el nostre cas hem hagut de definir un punt auxiliar P' linealment independent de $P \in E[l]$ ja que amb l'emparellament de Weil

$$e(P, aP) = e(P, P)^a = 1^a = 1$$

per a tot $P \in E[l]$, la qual cosa degenararia l'esquema.

3.2.2 Reconstrucció dels secrets

Després de la distribució dels fragments, recordem que els elements públics de l'esquema són:

- $P, P' \in E[l]$
- $v_i = e(P', i \cdot Q) + K_i$, per a cada secret$1 \leq i \leq s$
- M_i, per a cada nivell $1 \leq i \leq m$
- $b_{ij}x_{ij}P$, per $1 \leq i \leq m$ $1 \leq j \leq n_i$
- $x_i jP$, per $1 \leq i \leq m$ $1 \leq j \leq n_i$
- A més, en els casos on $t_i \leq \sum_{k=1}^{i-1} n_k$, $\begin{pmatrix} a_{iti+1}P & \dots & a_{iti'}P \end{pmatrix}^T$ també són públics.

Sense pèrdua de generalitat, suposem ara que t_1 usuaris $u_{11}, u_{12}, \dots, u_{1t_1}$ del nivell L_1, $t_2 - t_1$ usuaris $u_{21}, u_{22}, \dots, u_{2(t_2-t_1)}$ del nivell L_2, $t_3 - t_2$ usuaris $u_{31}, u_{32}, \dots, u_{3(t_3-t_2)}$ del nivell L_3, ..., i $t_m - t_{m-1}$ usuaris $u_{m1}, \dots, u_{m(t_m-t_{m-1})}$ del nivell L_m col·laboren per reconstruir els secrets.

Nivell L_1 :

Els usuaris col·laboradors del nivell L_1 consideraran una submatriu M_1' de M_1 d'ordre t_1 corresponent als seus fragments i calcularan la seva inversa $M_1'^{-1}$. Això és possible, doncs per construcció, qualsevols t_1 files són invertibles

A continuació, els usuaris calculen:

$$M_1'^{-1} \cdot \begin{pmatrix} b_{11}P & b_{12}P & \dots & b_{1t_1}P \end{pmatrix}^T = \begin{pmatrix} a_{11}P & a_{12}P & \dots & a_{1t_1}P \end{pmatrix}^T$$

.

Ara podem calcular la resta recursivament:

Nivell L_i Cas 1

Els usuaris col·laboradors dels nivells $L_1 \dots L_i$ seleccionant les files corresponents als seus fragments poden trobar una $t_i \times t_i$ submatriu M_i' de M_i que és invertible per construcció i aleshores computar:

$$M_i'^{-1} \cdot \begin{pmatrix} b_{11}P & \dots & b_{1t_1}P & \dots & b_{i1} \dots & b_{i(t_i-t_{i-1})}P \end{pmatrix}^T = \begin{pmatrix} a_{i1}P & a_{12}P & \dots & a_{it_i}P \end{pmatrix}^T$$

Nivell L_i Cas 2

Considerem la $(n_1 + ... + n_i) \times t_i'$ matriu $M_i = \begin{bmatrix} A_i & A_i' \\ B_i & B_i' \end{bmatrix}$ (veure Proposició 3.8). En aquest cas, recordem que les dimensions de les submatrius serien:

$$dim(M_i) = \begin{bmatrix} (n_1 + \ldots + n_{i-1}) \times t_i & (n_1 + \ldots + n_{i-1}) \times (t_i' - t_i) \\ n_i \times t_i & n_i \times (t_i' - t_i) \end{bmatrix}$$

Els usuaris col·laboradors primer calculen

$$\begin{bmatrix} b'_{11}P \\ \vdots \\ b'_{1t_1}P \\ \vdots \\ b'_{i1}P \\ \vdots \\ b'_{i(t_i - t_{i-1})}P \end{bmatrix} = \begin{bmatrix} b_{11}P \\ \vdots \\ b_{1t_1}P \\ \vdots \\ b_{i1}P \\ \vdots \\ b_{i(t_i - t_{i-1})}P \end{bmatrix} - \begin{bmatrix} A_i'' \\ B_i'' \end{bmatrix} \begin{bmatrix} a_{i(t_i+1)}P \\ \vdots \\ a_{it_i'}P \end{bmatrix},$$

on A_i'' i B_i'' són les submatrius de A_i' i B_i', respectivament, corresponents als usuaris col·laboradors. Aleshores consideren una submatriu M_i' formada per les primeres t_i columnes de M_i corresponents als seus fragments i calculen:

$$M_i'^{-1} \cdot \begin{pmatrix} b'_{11}P & \ldots & b'_{i(t_i - t_{i-1})}P \end{pmatrix}^T = \begin{pmatrix} a_{i1}P & \ldots & a_{it_i}P \end{pmatrix}^T.$$

.

Quan els usuaris hagin repetit el procés a tots els nivells, aquests poden calcular $Q = \sum_{j=1}^{m} a_{j1}P$. Aleshores, computen els secrets $K_i = v_i - e(P', i \cdot Q)$ per a cada $1 \leq i \leq s$ i tots són revelats.

3.3 Anàlisi sobre la seguretat de l'esquema

La verificació dels fragments és essencial per evitar un problema, a saber-ne: Un usuari podria enviar fragments incorrectes al procés de reconstrucció. El usuaris poden comprovar si la informació distribuida es correcta gràcies a l'emparellament de Weil de la següent manera:

1. Cada usuari u_{ij} proporciona el seu suposat fragment $c_{ij}P$ amb una informació addicional $x_{ij}^{-1}P'$ per a la verificació.

2. Els altres usuaris col·laboradors poden verificar l'autenticitat de la part examinant la validesa de l'equació $e(x_{ij}^{-1}P', b_{ij}x_{ij}P) = e(P', c_{ij}P)$. L'equació anterior és veritable si i només si $c_{ij}P = b_{ij}P$ ja que:

$$e(x_{ij}^{-1}P', b_{ij}x_{ij}P) = e(P', b_{ij}P)^{x_{ij}^{-1}x_{ij}} = e(P', b_{ij}P)$$

.

La robustesa de l' esquema de Chintamani et al. [2] es fundamenta en 2 problemes intractables, a saber-ne:

1. *La unidireccionalitat de l' emparellament de Weil:*

   L' emparellament de Weil es eficientment computable per exemple amb l' algoritme de Miller [3]. L' unidireccionalitat es dona perquè donat $g \in \mu_l$ és difícil trobar $P, Q \in E[l]$ tals que $e(P, Q) = g$. A més, tot i conéixer P, trobar $Q \in E[l]$ tal que $e(P, Q) = g$ és difícil [9].

2. *El problema del logaritme discret*

   Donats els punts $P, aP \in E(K)$ d' una corba elíptica i $a \in \mathbb{Z}$, trobar el valor de a és conegut com el Problema del Logaritme Discret de la Corba El·líptica (ECDLP). Es creu que l'ECDLP és computacionalment inviable de resoldre per a una elecció adequada de la corba el·líptica E i dels punts a E.

Un possible atacant podria intentar aconseguir el secrets a través de diferents fonts d'informació pública. Recordem que per reconstruir tots els secrets hauríem de trobar el punt $Q \in E[l]$ tal que

$$Q = \sum_{i=1}^{m} a_{m1}P$$

Per fer això hauria de obtenir suficients fragments per la reconstrucció. Quan el distribuïdor reparteix els fragments $b_{ij}P$ als usuaris, l'adversari no els pot obtenir a partir de $b_{ij}x_{ij}P$ ja que equivaldria a resoldre un ECDLP. A més, pel mateix motiu, un adversari no pot obtenir la clau secreta dels usuaris x_{ij} a partir de $x_{ij}P$.

A més, la probabilitat d'endevinar els secrets és baixa. És clar que endevinar els coeficients a_{i1} és de $1/l$ i la probabilitat d' endevinar un dels secrets K_i és de $1/p$. Considerant que l, p són nombres primers grans, aquesta probabilitat es molt baixa.

Ara suposem que tot i no conéixer suficients fragments, un grup no autoritzat pretén aconseguir els secrets.

Aleshores en el millor cas, $t_i - 1$ o menys usuaris del nivell L_i colaboren per computar $a_{i1}P$. Aleshores poden formar un sistema de $t_i - 1$ equacions i t_i incògnites. En aquest cas la solució del sistema és una varietat lineal de dimensió 1 sobre el cos $\mathbb{F}_l$, és dir que tenim també l solucions, de manera que la probabilitat continua sent baixa.

Finalment, podem dir que encara que es doni la situació en que un atacant aconsegueixi un dels secrets K_i, no podria aconseguir-ne la resta, ja que encara que pot conéixer g tal que

$$g = e(P', iQ) = v_i - K_i,$$

invertir l'emparellament e per recuperar Q és molt difícil.

3.4 Un exemple de l'esquema

Donem un exemple de l' esquema utilitzant l'emparellament de Weil. Els càlculs realitzats per Chintamani et.al estàn realitzats amb l' eina *SageMath*.

Considerem una corba el·líptica $E\ :\ y^2 = x^3 + 4x + 15$ definida al cos finit $\mathbb{F}_{47}$. $E(\mathbb{F}_{47})$ té 37 punts. Busquem el mínim k tal que $37 \mid 47^k - 1$. En aquest cas $k = 3$.

Tenim doncs que $\mathbb{F}_{47^3}$ és una extensió finita de cosssos i $E(\mathbb{F}_{47^3})$ té 104044 punts. Sigui α un arrel del polinomi cúbic: $x^3 + x + 4$, irreduible sobre $\mathbb{F}_{47}$. Considerem:

1. El grup de torsió: $E[37] \subseteq E(\mathbb{F}_{47^3})$.
2. $P' = (1, 4) \subseteq E[37]$
3. $P = (24\alpha + 1, 22\alpha^2 + 10\alpha + 23) \subseteq E[37]$
4. $n_1 = 2\ , n_2 = 3\ , n_3 = 5$
5. $t_1 = 1,\ t_2 = 3,\ t_3 = 4$
6. Secrets: $K_1 = 8,\ K_2 = 15,\ K_3 = 22,\ K_4 = 11$.

Pel nivell L_1:

- Escollim la matriu: $M_1 = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ i un $(t_1 = 1)$ nombre enter a_{11} $a_{11} = 11 \in [0, 36]$.
- Computem $\begin{pmatrix} b_{11} & b_{12} \end{pmatrix}^T = M_1 \cdot \begin{pmatrix} a_{11} \end{pmatrix} = \begin{pmatrix} 33 & 7 \end{pmatrix}^T$.
- Aleshores, els fragments dels usuaris u_{11}, u_{12} són:
  - $33P = (\alpha^2 + 30\alpha + 40, 33\alpha^2 + 40\alpha + 28)$
  - $7P = (42\alpha^2 + 45\alpha + 19, 28\alpha^2 + 2\alpha + 6)$

  respectivament.

Nivell L_2 :

- Com que $t_2 > n_1$, escollim la matriu

$$M_2 = \begin{bmatrix} 4 & 6 & 1 \\ 2 & 5 & 8 \\ 1 & 0 & 9 \\ 5 & 2 & 10 \\ 7 & 3 & 11 \end{bmatrix}$$

  i $t_2 = 3$ nombres enters $a_{21} = 33$, $a_{22} = 32$, $a_{23} = 5 \in [0, 36]$.

- Computem
  $\begin{pmatrix} b_{11} & b_{12} & b_{21} & b_{22} & b_{23} \end{pmatrix}^T = M_2 \cdot \begin{pmatrix} a_{21} & a_{22} & a_{23} \end{pmatrix}^T = \begin{pmatrix} 33 & 7 & 4 & 20 & 12 \end{pmatrix}^T$.
  Destaquem que els nombresb_{11} i b_{12} es corresponen amb el nivell L_1.

- Aleshores, els fragments dels usuaris u_{21}, u_{22}, u_{23} són:

  - $4P = (\alpha^2 + 30\alpha + 40, 14\alpha^2 + 7\alpha + 19)$
  - $20P = (36\alpha^2 + 17\alpha + 11, 7\alpha^2 + 19\alpha + 20$
  - $12P = (7\alpha^2 + 29\alpha + 45, 26\alpha^2 + 6\alpha + 10)$

  respectivament.

Nivell L_3 :

- Com que $t_3 < n_1 + n_2$, sigui $t_3' = 6$.

- Escollim la matriu

$$M_3 = \begin{bmatrix} 3 & 1 & 5 & 7 & 1 & 9 \\ 2 & 4 & 9 & 3 & 6 & 1 \\ 5 & 2 & 11 & 7 & 10 & 2 \\ 1 & 1 & 2 & 3 & 5 & 7 \\ 2 & 9 & 6 & 15 & 12 & 16 \\ 10 & 0 & 3 & 1 & 2 & 4 \\ 4 & 5 & 1 & 7 & 2 & 9 \\ 3 & 2 & 8 & 0 & 5 & 3 \\ 1 & 7 & 11 & 12 & 10 & 4 \\ 4 & 8 & 9 & 2 & 3 & 1 \end{bmatrix}$$

  i $t_3' = 6$ nombres enters $a_{31} = 6$, $a_{32} = 25$, $a_{33} = 8$, $a_{34} = 19$, $a_{35} = 7$, $a_{36} = 20 \in [0, 36]$.

- Computem $\begin{pmatrix} b_{11} & b_{12} & b_{21} & b_{22} & b_{23} & b_{31} & b_{32} & b_{33} & b_{34} & b_{35} \end{pmatrix}^T =$
  $M_3 \cdot \begin{pmatrix} a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \end{pmatrix}^T = \begin{pmatrix} 33 & 7 & 4 & 20 & 12 & 12 & 3 & 5 & 18 & 5 \end{pmatrix}^T$

Destaquem que els nombres b_{11}, b_{12}, b_{21}, b_{22}, b_{23} es corresponen amb els dels nivells L_1, L_2.

- Aleshores, els fragments dels usuaris u_{31}, u_{32}, u_{33}, u_{34}, u_{35} són:
  - $12P = (7\alpha^2 + 29\alpha + 45, 26\alpha^2 + 6\alpha + 10)$,
  - $3P = (14\alpha^2 + 20\alpha + 21, 22\alpha^2 + 29\alpha + 40)$,
  - $5P = (4\alpha^2 + 9\alpha + 39, 14\alpha^2 + 42\alpha + 5)$,
  - $18P = (17\alpha^2 + 6\alpha + 22, 26\alpha^2 + 32\alpha + 10)$,
  - $5P = (4\alpha^2 + 9\alpha + 39, 14\alpha^2 + 42\alpha + 5)$

  Respectivament.

Ara computem:

- $Q = a_{11}P + a_{21}P + a_{31}P = 13P = (17\alpha^2 + 13\alpha + 4, 8\alpha^2 + 22\alpha + 9)$.
- $v_1 = e(P', Q) + K_1 = e(P', 13P) + 8 = 37\alpha^2 + 28\alpha + 12$,
- $v_2 = e(P', 2Q) + K_2 = e(P', 26P) + 15 = 28\alpha^2 + 7\alpha + 4$,
- $v_3 = e(P', 3Q) + K_3 = e(P', 2P) + 22 = 36\alpha^2 + 32\alpha + 23$,
- $v_4 = e(P', 4Q) + K_4 = e(P', 15P) + 11 = 42\alpha^2 + 5\alpha + 24$.

Publiquem $P, v_1, v_2, v_3, v_4, M_1, M_2, M_3$. El repartiment de fragments dels secrets ja està completat.

Reconstrucció dels secrets:

Ara suposem que els usuaris u_{11}, u_{21}, u_{23}, u_{32} col·laboren per reconstruir els secrets K_1, K_2, K_3 i K_4.

- **Nivell L_1 :** L' usuari u_{11} pot calcular el secret del nivell L_1, invertint la submatriu corresponent a la seva fila M_1 i tenim doncs que:

  $a_{11}P = 3^{-1}b_{11}P = 25(\alpha^2 + 30\alpha + 40, 33\alpha^2 + 40\alpha + 28) =$
  $(18\alpha^2 + 27\alpha + 12, 36\alpha^2 + 20\alpha + 32)$.

- **Nivell L_2 :** Els usuaris u_{11}, u_{21}, u_{23} utilitzant les files corresponents als seus fragments formen una 3×3 submatriu M_2' de M_2:

$$M_2' = \begin{bmatrix} 4 & 6 & 1 \\ 1 & 0 & 9 \\ 7 & 3 & 11 \end{bmatrix}$$

  agafant les files primera, tercera i quarta de M_2, i calculen la seva inversa:

$$M_2^{-1} = \begin{bmatrix} 24 & 19 & 26 \\ 36 & 0 & 27 \\ 22 & 35 & 30 \end{bmatrix}$$

Després, calculen

$$M_2^{-1} \cdot \begin{pmatrix} 33P & 4P & 12P \end{pmatrix}^T = \begin{pmatrix} (\alpha^2 + 30\alpha + 40, 33\alpha^2 + 40\alpha + 28) \\ (4\alpha^2 + 9\alpha + 39, 33\alpha^2 + 5\alpha + 42) \\ (4\alpha^2 + 9\alpha + 39, 14\alpha^2 + 42\alpha + 5) \end{pmatrix}$$

Així, el secret del nivell L_2 és: $a_{21}P = (\alpha^2 + 30\alpha + 40, 33\alpha^2 + 40\alpha + 28)$.

- **Nivell L_3 :** (Cas $t_3 < n_1 + n_2$)

  En el nivell L3, els usuaris u_{11}, u_{21}, u_{23}, u_{32} coneixen les entrades de les files corresponents de M_3. Com que $a_{35} = 7$ i $a_{36} = 20$ són públics, primer calculen:

$$\begin{aligned}
&b_{11}P - (a_{35}P + 9a_{36}P) = 31P = (18\alpha^2 + 42\alpha + 8, 40\alpha^2 + 18\alpha + 46), \\
&b_{21}P - (10a_{35}P + 2a_{36}P) = 5P = (4\alpha^2 + 9\alpha + 39, 14\alpha^2 + 42\alpha + 5), \\
&b_{23}P - (12a_{35}P + 16a_{36}P) = 15P = (31\alpha^2 + 10\alpha + 24, 11\alpha^2 + 23\alpha + 44), \\
&b_{32}P - (2a_{35}P + 9a_{36}P) = 31P = (18\alpha^2 + 42\alpha + 8, 40\alpha^2 + 18\alpha + 46).
\end{aligned}$$

  Després, prenen la 4×4 submatriu corresponent a les $t_3 = 4$ primeres columnes de les files corresponents als seus fragments

$$M_3' = \begin{bmatrix} 3 & 1 & 5 & 7 \\ 5 & 2 & 11 & 7 \\ 2 & 9 & 6 & 15 \\ 4 & 5 & 1 & 7 \end{bmatrix}$$

  de M_3 i calculen la seva inversa $M_3'^{-1} = \begin{bmatrix} 16 & 36 & 23 & 15 \\ 26 & 35 & 7 & 35 \\ 21 & 7 & 22 & 20 \\ 1 & 1 & 21 & 6 \end{bmatrix}$. Ara, tenim

$$M_3'^{-1} \cdot \begin{bmatrix} 31P \\ 5P \\ 15P \\ 31P \end{bmatrix} = \begin{pmatrix} (18\alpha^2 + 42\alpha + 8, 7\alpha^2 + 29\alpha + 1) \\ (7\alpha^2 + 29\alpha + 45, 21\alpha^2 + 41\alpha + 37) \\ (18\alpha^2 + 12\alpha + 8, \alpha^2 + 38\alpha + 44) \\ (17\alpha^2 + 6\alpha + 22, 21\alpha^2 + 15\alpha + 37) \end{pmatrix}.$$

  Així, el secret del nivell L_3 és: $a_{31}P = (18\alpha^2 + 42\alpha + 8, 7\alpha^2 + 29\alpha + 1)$.

Finalment, els usuaris u_{11}, u_{21}, u_{23}, u_{32} computen $Q = a_{11}P + a_{21}P + a_{31}P = 13P$ i reconstrueixen els secrets:

- $K_1 = v_1 - e(P', Q) = 8$,
- $K_2 = v_2 - e(P', 2Q) = 15$,
- $K_3 = v_3 - e(P', 3Q) = 22$,
- $K_4 = v_4 - e(P', 4Q) = 11$.

4 Conclusions

Al llarg d' aquest treball hem pogut completar algunes tasques importants.

Primer, hem introduit de manera relativament senzilla el concepte de corba el·líptica i la suma de punts de la corba, que ens han permès entendre algunes propietats bàsiques. Després hem presentat algunes eines fonamentals més avançades per a l'estudi de les corbes el·líptiques com el concepte de divisor, grup de torsió o funció a una corba el·líptica. Finalment i per tancar la primera meitat del treball, hem utilitzat tot aquest desenvolupament per a construir l'emparellament de Weil, un objecte fonamental en l'estudi de les corbes el·líptiques.

A la segona part del treball, hem pogut utilitzar tota la base teòrica de la primera part per a comprendre i presentar en detall un criptosistema avançat i innovador de compartició de secrets.

Referències

[1] Washington, Lawrence C. (2008) *Elliptic curves: number theory and cryptography*, 2nd edition, University of Maryland.

[2] Mohan Chintamani, Prabal Paul, Laba Sa (2023) *Conjuctive Hierarchichal Multi-Secret Sharing Scheme using Elliptic Curves*, The Indian National Science Academy.

[3] Miller, Victor S. (2004) *The Weil pairing, and it's efficient calculation,* J. Cryptology.

[4] Shamir, Adi (1979) *How to share a secret*, Programming techniques, Massachusetts Institute of Technology.

[5] Silverman, Joseph H. (1986) *The arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, Brown University.

[6] Shafi Goldwasser, Mihir Bellare (2008) *Lectures on Cryptography*, Massachusetts Institute of Technology.

[7] The Sage development team (2023) *Elliptic Curves, Release 10.2*

[8] W.C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press (2012).

[9] S.D Galbraith, F. Hess, F. Vercauteren (2008) *Aspects of pairing inversion*, IEEE Transactions of Information Theory, Vol. 54.

[10] I.F Blake, G. Seroussi, N.P. Smart. *Elliptic curves in cryptography*, volume 265, *London Mathematical Society Lecture Note Series*. Cambrige University Press. Cambridge, 2000.

[11] D. Boneh, N. Daswani. Experimenting with electronic commerce on PalmPilot. *Financial Cryptography '99*, volume 1648 of *Lecure Notes in Computer science.*, pàg 1-16, Springer-Verlag, Berlin 1999.