UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Logaritme discret i pairings en corbes el·líptiques amb aplicacions a la criptografia

Autor: Bernadí Rosselló Gelabert

Director: Dr. Luis Víctor Dieulefait
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 20 de juny de 2021

Abstract

Cryptography is based on practically unsolvable problems computationally. We will study elliptic curves and the discrete logarithm problem that is defined over these curves. We will see some ways to take advantage of this problem to obtain encoding systems and finally we will see 2 ways to attack the curve reducing the discrete logarithm problem over elliptic curves to the discrete logarithm problem over finite fields.

Resum

La criptografia es basa en problemes pràcticament irresolubles computacionalment. En aquest treball estodiarem les corbes el·líptiques i el problema del logaritme discret que es defineix sobre aquestes corbes. Veurem unes quantes maneres d'aprofitar aquest problema per obtenir xifrats i finalment veurem 2 maneres d'atacar la corba reduint el problema del logaritme discret sobre corbes el·líptiques al problema del logaritme discret sobre cossos finits.

Índex

1 Introducció **1**

2 Corbes el·líptiques **3**

2.1 Grup sobre una corba 4

2.2 Isogènies 7

2.3 Weil pairing 10

2.4 Corbes el·líptiques sobre cossos finits 14

2.5 Corbes hiperel·líptiques 17

3 Xifrats **19**

3.1 ECDLP 19

3.2 Protocols d'acord de clau 19

3.2.1 ECDH 20

3.2.2 ElGamal 22

3.2.3 Massey-Omura 23

3.2.4 ECDSA 23

3.2.5 Firma BLS 25

4 Atacs a la corba **26**

4.1 Reducció del logaritme el·líptic 26

4.2 Reducció del cas corba supersingular 27

4.3 Atac GHS 28

4.3.1 Mètode càlcul d'índex 29

5 Conclusions **31**

1 Introducció

La criptografia s'ha usat durant molts anys sobretot amb fins bèlics. Ja des de l'edat romana existien diferents tipus de xifrats per tal d'aconseguir fer arribar un missatge als teus aliats de manera segura, com per exemple el xifrat de Juli Cèsar. També hi ha altres xifrats clàssics com els criptosistemes afins (monoalfabètic com el de Cèsar) o d'altres polialfabètics, com el xifrat de Vigènere.

La diferència essencial entre els xifrats clàssics i els moderns és que els primers són segurs solament si es manté el procediment i les claus en secret. En canvi en els xifrats moderns les claus segueixen sent privades però els procediments són públics. Els procediments, al ser tan complicats computacionalment, no deixaran que un atacant amb una quantitat arbitrària de text xifrat dedueixi les nostres claus i, per tant, llegir el missatge original.

Dins la criptografia moderna es poden distingir dos subgrups de criptosistemes: els de *clau privada* o *simètrics* i els de *clau pública* o *asimètrics*. Als de clau privada només l'emissor i el receptor coneixen la clau usada en el missatge i aquesta serveix tant per xifrar-lo com per desxifrar-lo. En els de clau pública cada usuari té una clau pública i una altra de privada. Qualsevol altre usuari que vulgui enviar-li un missatge a l'usuari usarà la seva clau pública i aquest utilitzarà la seva clau privada per desxifrar el missatge. Observam que l'avantatge d'aquest darrer tipus de xifrat és que els usuaris no s'han de posar prèviament d'acord en quina clau secreta hauran d'utilitzar entre ells. Degut a aquesta dificultat de desxifrar el missatge encara que es conegui el mètode de xifrat anomenem aquestes funcions de xifrat com a funcions trampa.

Segons W. Diffie i M. Hellman tot algoritme de clau pública ha de complir les següents propietats de complexitat computacional:

1. Qualsevol usuari pot calcular les seves pròpies claus pública i privada en temps polinomial.
2. L'emisor pot xifrar el seu missatge amb la clau pública del receptor en temps polinomial.
3. El receptor pot desxifrar el missatge xifrat amb la clau privada en temps polinomial.
4. El criptoanalista que intenti averiguar la clau privada mitjançant la pública es trobarà amb un problema intractable.
5. El criptoanalista que intenti desxifrar un missatge xifrat tenint la clau pública es trobarà amb un problema intractable.

Diffie i Hellman van rebre el 2015 el premi Turing "Per contribucions fonamentals a la criptografia moderna".

Aquí es presenta de forma general un esquema per la construcció d'un criptosistema de clau pública:

1. Agafar un problema díficil P, a poder ser, intractable.
2. Agafar un subproblema de P fàcil $P_{\text{fàcil}}$ que es resolgui en temps polinomial, preferiblement en temps lineal.

3. Transformar el problema $P_{\text{fàcil}}$ de manera que el problema resultant $P_{\text{difícil}}$ no es pareixi a $P_{\text{fàcil}}$ però sí al problema original P.

4. Publicar el problema $P_{\text{difícil}}$ i la manera en que aquest ha de ser usat, constituint això la clau pública. La informació sobre com es pot recuperar el problema $P_{\text{fàcil}}$ a partir del $P_{\text{difícil}}$ es manté en secret i això constitueix la clau privada.

Alguns dels sistemes públics amb més transcendència són per exemple els: RSA, de Rabin, de Merkle-Hellman, de McEliece, de ElGamal o basats en curves el·líptiques. En aquest treball ens centrarem en aquests dos darrers sistemes. [3, 5]

2 Corbes el·líptiques

A continuació descriurem les corbes que seran objecte d'estudi per ajudar-nos amb les seves aplicacions a la criptografia seguint els llibres [1, 2, 6].

Primer de tot triem el cos K sobre el que definirem la corba. Una corba el·líptica sobre K és una corba projectiva algebraica de gènere 1 que tingui al menys un punt sobre K.

Aquestes corbes es poden definir sobre qualsevol cos K. Si la característica de K és diferent de 2 i 3, mitjançant un canvi de variable podem escriure l'equació de la corba com:

$$y^2 = x^3 + ax + b \tag{2.1}$$

Si el cos K es de característica 2 aleshores es pot escriure com:

$$y^2 + cy = x^3 + ax + b$$

o de la forma:

$$y^2 + xy = x^3 + ax^2 + b$$

I en el cas que K sigui de característica 3 es pot escriure de la forma:

$$y^2 = x^3 + ax^2 + bx + c$$

On en tots els casos $a, b, c \in K$.

Donada aquesta equació (on el membre de la dreta no té cap arrel doble) definim el conjunt de punts de la corba C sobre K com els parells (x, y) tals que x i y són solució de l'equació i pertànyen a K junt amb el punt $\mathcal{O}$. Ho denotarem com:

$$C(K) = \{P = (x, y) \in C : x, y \in K\} \cup \mathcal{O}$$

On $\mathcal{O}$ el definirem millor en el següent apartat però és el punt a l'infinit de la corba. Aquí veim que la corba sempre té almenys el neutre ja que aquest té coordenades sobre K.

També podem definir els punt de la corba C però sobre la clausura algebraica del cos K sobre el qual està definida la corba: $\overline{K}$.

$$C(\overline{K}) = \{P = (x, y) \in C : x, y \in \overline{K}\} \cup \mathcal{O}$$

De moment definirem una sèrie de quantitats donada una corba escrita en la forma de Weierstrass, ja que tota corba admet aquesta forma:

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Si $char(K) \neq 2$ aleshores podem fer un canvi de variable $y \to (y - a_1x - a_3)/2$ i ens queda una eqüació de la forma

$$C : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

$$
\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_2a_3 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= c_4^3/\Delta
\end{aligned}
$$

On a part dels coeficients de C hem definit Δ el *discriminant* de l'equació de Weierstrass i j la *j-invariant* de la corba C.

Proposició 2.1. *1. Segons el discriminant podem classificar una corba donada amb la equació de Weierstrass de la següent manera:*

(a) No-singular si, i només si $\Delta \neq 0$

(b) Amb un node si, i només si $\Delta = 0$ *i* $c_4 \neq 0$

(c) Amb una cúspide si , i només si $\Delta = 0$ *i* $c_4 = 0$

2. Dues corbes el·líptiques (és a dir no-singulars) són isomorfes si tenen el mateix j-invariant.

3. Sigui $j_0 \in \overline{K}$*. Llavors existeix una corba el·líptica definida sobre* $\overline{K}$ *amb j-invariant igual a* j_0*.*

2.1 Grup sobre una corba

Donada la corba C, ens interessarà el grup creat pels punts sobre aquesta. Per això mateix definirem el neutre de C.

Primer de tot escriurem la corba en la forma de Weierstrass:

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

I ara farem ús de la geometria projectiva per a definir el punt que ens interessa. Homogeneïtzem i ens queda l'equació:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Aquí fent $Z = 0$ veiem que l'únic punt a l'infinit és el punt $[0 : 1 : 0]$. Aquest punt serà el que definirem com el neutre $\mathcal{O}$.

Ara definirem una suma de punts dins C geomètricament. Siguin P i Q punts a C, definirem la suma $P + Q$. Primer de tot agafem P i Q i fem la recta que passa pels dos punts, agafem el 3r punt de intersecció amb la cúbica i feim la recta que passa per $\mathcal{O}$. El punt on intersequi aquesta darrera recta amb la corba el·líptica serà el punt $P + Q$.

Feim ara la suma dels punts de manera numèrica ja que per criptografia ens convé poder calcular els punts de manera numèrica i no només geomètricament.

Feim el cas en que K té característica diferent de 2 i 3: primer de tot hem de tenir en compte que donada una recta que passi per dos punts de la nostra cúbica C, aquesta recta intersecarà C a un altre punt (això darrer s'ha d'agafar amb pinces de moment).

Siguin $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ veurem quin és el tercer punt d'intersecció $S = (x_3, y_3)$. Primer de tot mirarem el cas en que P i Q són diferents i la recta R que passa a través d'ells no és vertical.

Això ens diu que R és de la forma

$$y = mx + n \tag{2.2}$$

On

$$m = \frac{y_2 - y_1}{x_2 - x_1} \qquad\qquad n = y_1 - mx_1$$

Ara per obtenir el punt d'intersecció de R amb C substituirem 2.2 a 2.1 i obtindrem

$$x^3 - (mx + n)^2 + ax + b = 0$$

D'aquí les tres arrels seran els números x_1, x_2 i x_3. I com $x_1 + x_2 + x_3 = m^2$ obtenim

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

I la segona coordinada la podem obtenir fent

$$y_3 = mx_3 + n$$

Però hem de tenir en compte que el nostre punt resultant $P + Q$ serà el punt

$$P + Q = (x_3, -y_3)$$

Si la recta entre els punts P i Q és vertical, aleshores R es pot escriure com $x = u$. Si homogeneïtzem la recta ens queda com $X = UZ$ i veiem que passa pel punt $\mathcal{O}$. Així que direm que el tercer punt d'interseció serà $\mathcal{O}$. Ara en coordenades projectives sabem que $[0 : -1 : 0] = [0 : 1 : 0] = \mathcal{O}$ i per tant $\mathcal{O}$ serà la suma dels dos punts.

Si agafem $P = Q$ aleshores agafarem la recta com la recta tangent a C en P i el 3r punt d'intersecció normalment. L'equació ens quedaria de la forma

$$x_3 = m^2 - 2x_P \qquad\qquad m = \frac{3x_P^2 + a}{2y_P}$$
$$y_3 = mx_3 + n \qquad\qquad n = y_P - mx_P$$

On hem obtingut la m per derivació directe de 2.1.

Es té estructura de grup amb el procediment? La resposta és sí.

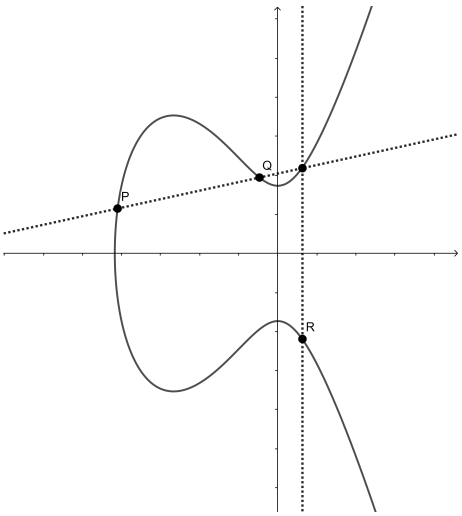

Figura 1: Suma de dos punts P i Q diferents.

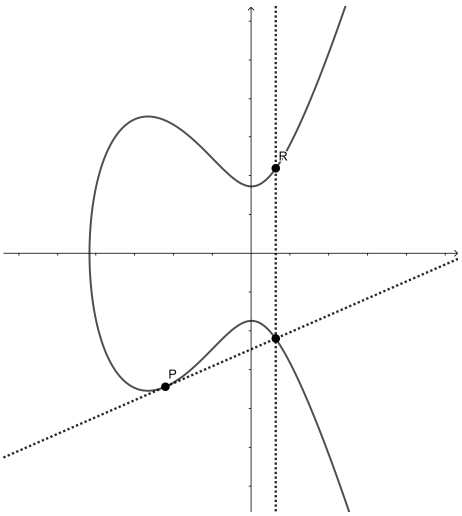

Figura 2: Suma de dos punts iguals $2P$.

Clarament de la definició

$$C(K) = \{P = (x, y) \in C : x, y \in K\} \cup \mathcal{O}$$

veim que el neutre pertany a la corba.

Ara $P + \mathcal{O} = P$, unim el punt de l'infinit amb $P = (x, y)$, que sabem que interseca el punt $P^* = (x, -y)$ a la corba i ara la suma dels dos punts l'obtenim unint el punt P^* amb el punt $\mathcal{O}$ i agafant la intersecció amb la corba el·líptica: $P = (x, y)$.

Per la manera simètrica amb la que hem definit la suma de dos punts $P+Q$, clarament $P + Q = Q + P$.

I abans hem vist que si la recta entre dos punts és vertical, és a dir, $P = (x, y)$ i $P^* = (x, -y)$, aleshores $P + P^* = \mathcal{O}$, ja que la recta entre P i P^* interseca $\mathcal{O}$ i quan feim la recta de $\mathcal{O}$ amb $\mathcal{O}$ aquesta és la mateixa recta de l'infinit i el punt $\mathcal{O}$ té multiplicitat 3.

També es podria veure que si tenim tres punts P, Q i R colinears que pertanyen a $C(K)$, aleshores $P + Q + R = \mathcal{O}$.

Amb tot això definirem també

$$mP = P + \cdots + P \text{ (m termes) per } m > 0$$

$$mP = -m(-P) \text{ per } m < 0 \qquad\qquad 0P = \mathcal{O}$$

I el grup de torsió

$$C[m] = \{P \in C(\overline{K}) : mP = \mathcal{O}\}$$

Es pot veure que si la característica del cos K és 0, aleshores

$$\#C[m] = m^2$$

En canvi si la característica del cos K no és coprimer amb m, $C[m]$ és més petit.

El *subgrup de torsió de* C és el conjunt de punts d'ordre finit.

$$C_{tors} = \bigcup_{m=1}^{\infty} C[m]$$

Si la corba està definida sobre K, $C_{tors}(K)$ denotarà els punts d'ordre finit a $C(K)$.

2.2 Isogènies

Agafem $K[x]$ l'anell de polinomis sobre x. L'ideal definit per una corba C és descriu com

$$I(C) = \{f \in \overline{K}[x] : f(P) = 0 \text{ per tot } P \in C\}$$

I podem escriure també

$$I(C/K) = \{f \in K[x] : f(P) = 0 \text{ per tot } P \in C\}$$

Amb això podem definir un domini d'integritat

$$K[C] = \frac{K[x]}{I(C/K)}$$

Al ser un domini d'integritat, existeix el seu cos quocient $K(C)$ i es diu *el cos quocient de* C/K. $\overline{K}[C]$ i $\overline{K}(C)$ es defineixen canviant la K per $\overline{K}$.

Siguin C_1 i C_2 corbes el·líptiques. Una isogènia és un morfisme

$$\phi : C_1 \to C_2$$

tal que $\phi(\mathcal{O}) = \mathcal{O}$. Una isogènia satisfà $\phi(C_1) = C_2$ o bé $\phi(C_1) = \{\mathcal{O}\}$. Direm que dues corbes són isògenes si existeix una isogènia tal que $\phi(C_1) = C_2$.

Una isogènia indueix una injecció de cossos quocients fixant K:

$$\begin{aligned} \phi^* : K(C_2) &\to K(C_1) \\ \phi^* f &= f \circ \phi \end{aligned}$$

Teorema 2.2. *Siguin C_1/K, C_2/K corbes el·líptiques i $\phi : C_1 \to C_2$ una isogènia distinta de 0 definida sobre K. Aleshores $K(C_1)$ és una extensió finita de $\phi^* K(C_2)$.*

Donades les corbes i la isogènia del teorema, definirem el grau de ϕ com $deg\ [0] = 0$ o altrament direm que ϕ és finita i direm

$$deg\ \phi = [\overline{K}(C_1) : \phi^* \overline{K}(C_2)]$$

Si el grau d'una isogènia és 1 aleshores és un isomorfisme.

Definició 2.3. *Les propietats de separabilitat, inseparabilitat i purament inseparable de ϕ estan definides per la corresponent propietat de l'extensió finita $\overline{K}(C_1)/\phi^*\overline{K}(C_2)$.*

Com les corbes el·líptiques són grups, les aplicacions entre elles formen grups

$$Hom(C_1, C_2) = \{\text{isogènies } \phi : C_1 \to C_2\}$$

$Hom(C_1, C_2)$ és un grup sota l'adició

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

Tenim també

$$End(C) = Hom(C, C)$$

amb composició

$$(\phi\psi)(P) = \phi(\psi(P))$$

$End(C)$ es coneix com *l'anell d'endomorfismes de C* i els elements invertibles de $End(C)$ formen *el grup d'automorfismes de C*. Si les corbes estan definides sobre K aleshores ens podem fixar en les isogènies definides sobre K, denotant-ho com

$$Hom_K(C_1, C_2) \qquad End_K(C) \qquad Aut_K(C)$$

Exemple 2.4. Sigui una corba C donada en la forma de Weierstrass i $q = p^r$ on p és la característica del cos K. El morfisme de Frobenius és

$$\begin{aligned} \phi_q : E &\to E^{(q)} \\ (x, y) &\to (x^q, y^q) \end{aligned}$$

on $E^{(q)}$ es defineix elevant els coeficients de l'equació a q.

Exemple 2.5. Per cada $m \in \mathbb{Z}$ la multiplicació per m és una isogènia

$$[m] : C \to C$$

Proposició 2.6. *1. Sigui C/K una corba el·líptica i $m \in \mathbb{Z}$, $m \neq 0$. Aleshores la aplicació de multiplicació per m,*

$$[m] : C \to C$$

no és constant.

2. Siguin C_1 i C_2 corbes el·líptiques. El grup d'isogènies

$$Hom_K(C_1, C_2)$$

és un $\mathbb{Z}$-mòdul lliure de torsió.

3. *Sigui C una corba el·líptica. Aleshores $End(C)$ és un anell no necessàriament commutatiu de característica 0 sense divisors del zero.*

Normalment, si $char(K) = 0$, $End(C) \cong \mathbb{Z}$. Si $End(C)$ té més elements que $\mathbb{Z}$ deim que C té multiplicació complexa. D'altra banda, si K és un cos finit, $End(C)$ té sempre més elements que $\mathbb{Z}$.

Ara definirem el dual d'una isogènia. Agafem una isogènia $\phi : C_1 \to C_2$ de grau m. Aleshores existeix una única isogènia $\hat{\phi} : C_2 \to C_1$ tal que

$$\hat{\phi} \circ \phi = [m]$$

A aquesta isogènia $\hat{\phi}$ li direm la isogènia dual de ϕ.

Teorema 2.7. *Sigui ϕ una isogènia de grau m*

$$\phi : C_1 \to C_2$$

1. *Aleshores*

$$\hat{\phi} \circ \phi = [m] \qquad \text{sobre } C_1$$
$$\phi \circ \hat{\phi} = [m] \qquad \text{sobre } C_2$$

2. *Sigui $\lambda : E_2 \to E_3$ una altra isogènia, aleshores*

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

3. *Sigui $\psi : C_1 \to C_2$ una altra isogènia, aleshores*

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

4. *Per tot $m \in \mathbb{Z}$*

$$\hat{[m]} = [m] \qquad i \qquad deg\ [m] = m^2$$

5.

$$deg\ \hat{\phi} = deg\ \phi$$

6.

$$\hat{\hat{\phi}} = \phi$$

Exemple 2.8. Sigui K un cos de característica distinta de 2, i $a,\ b \in K$ amb $b \neq 0$ i $r = a^2 - 4b \neq 0$. Considerem les corbes el·líptiques

$$C_1 :\ y^2 = x^3 + ax^2 + bx$$
$$C_2 : Y^2 = X^3 - 2aX^2 + rX$$

Ara considerem les isogènies

$$\phi :\ C_1 \to C_2 \qquad\qquad \hat{\phi} :\ C_2 \to C_1$$
$$(x, y) \to \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\right) \qquad (X, Y) \to \left(\frac{Y^2}{4X^2}, \frac{Y(r - X^2)}{8X^2}\right)$$

Es pot observar que si composem les dues isogènies ens queda $\hat{\phi} \circ \phi = [2]$ sobre C_1 i $\phi \circ \hat{\phi} = [2]$ sobre C_2.

2.3 Weil pairing

El *grup de divisors d'una corba C*. El denotarem per $Div(C)$ i és un grup abelià generat pels punts de C. Un divisor $D \in Div(C)$ és una suma

$$D = \sum_{P \in C} n_P(P)$$

amb $n_P \in \mathbb{Z}$ i $n_P = 0$ per tot punt excepte per un conjunt finit. El *grau de D* està definit per

$$deg\ D = \sum_{P \in C} n_P$$

El conjunt de *divisors de grau 0* forma un subgrup del grup de divisors i el denotarem per

$$Div^0(C) = \{D \in Div(C) : deg\ D = 0\}$$

Assumim que la corba C és $\mathcal{C}^1$ i agafam $f \in \overline{K}(C)^*$. Podem associar a f el divisor $div(f)$ com

$$div(f) = \sum_{P \in C} ord_P(f)(P)$$

On $ord_P(f)$ és l'ordre de P a f segons si P és un pol o un zero de la funció f. És a dir, si P és un pol d'ordre n, llavors $ord_P(f) = -n$ i si P és un zero d'ordre m, $ord_P(f) = m$.

Diem que un divisor és principal si és de la forma $D = div(f)$ per alguna $f \in \overline{K}(C)^*$. Dos divisors D_1, D_2 són linealment equivalents si $D_1 - D_2$ és principal, i ho denotam per $D_1 \sim D_2$

Un divisor $D = \sum_{P \in C} n_P(P) \in Div(C)$ és positiu, denotat com $D \geqslant 0$, si $n_P \geqslant 0$ per tot $P \in C$. De manera que podem dir, donats dos divisors D_1,$D_2 \in Div(C)$ que

$$D_1 \geqslant D_2$$

per indicar que $D_1 - D_2$ és positiu.

Amb aquestes desigualtats podem resumir els zeros i pols d'una funció dient, per exemple

$$div(f) \geqslant m(Q) - n(P)$$

amb el que deim que f té un zero d'ordre al menys m a Q, que té un pol d'ordre com a molt n a P i que a la resta de punts és regular.

Proposició 2.9. *Sigui C una corba el·líptica, per cada divisor $D \in Div^0(C)$ existeix un únic punt $P \in C$ tal que*

$$D \sim (P) - (\mathcal{O})$$

D'aquí es pot veure que si C és una corba el·líptica i $D = \sum_{P \in C} n_P(P) \in Div(C)$. Aleshores D és principal si, i només si $\sum n_P = 0$ i $\sum [n_P]P = \mathcal{O}$.

A continuació agafarem un enter m co-primer amb $p = char(K)$ si $p > 0$. Agafem $T \in C[m]$, aleshores existeix una funció $f \in \overline{K}(C)$ tal que

$$div(f) = m(T) - m(\mathcal{O})$$

Ara amb un T' amb $m(T') = T$ hi ha igualment una funció $g \in \overline{K}(C)$ tal que

$$div(g) = m^*(T) - m^*(\mathcal{O}) = \sum_{R \in C[m]} (T' + R) - (R)$$

On m^* és el dual de m i ens envia un divisor (P) al sumatori dels divisors (Q) tal que $mQ = P$.

S'observa que les funcions $f \circ [m]$ i g^m tenen el mateix divisor, així, multiplicant f per un element de $\overline{K}^*$ podem assumir que

$$f \circ [m] = g^m$$

Ara agafem un altre punt $S \in C[m]$ (pot ser $S = T$). Per qualsevol punt $X \in C$,

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

I amb això podem definir un emparellament

$$e_m : C[m] \times C[m] \to \mu_m = \text{arrels } m\text{-èssimes de la unitat}$$

definint

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

on X és qualsevol punt de la corba tal que $g(X + S)$ i $g(X)$ estan definits i són distints de zero. Encara que g està definida llevat d'un element de $\overline{K}^*$, $e_m(S, T)$ no depèn d'aquesta elecció. Aquest emparellament és el *Weil e_m-pairing.*

Proposició 2.10. *El Weil e_m-pairing és:*

1. *Bilineal:*
$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_1)$$
2. *Alternant: $e_m(T, T) = 1$, en particular $e_m(S, T) = e_m(T, S)^{-1}$*
3. *No-degenerat: Si $e_m(S, T) = 1$ per tot $S \in C[m]$, aleshores $T = \mathcal{O}$.*
4. *Invariant Galois: Per tot $\sigma \in G_{\overline{K}/K}$,*
$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma)$$
5. *Compatible: Si $S \in C[mm']$ i $T \in C[m]$, aleshores*
$$e_{mm'}(S, T) = e_m([m']S, T)$$

Sempre existeixen punts $S, T \in C[m]$ tals que $e_m(S,T)$ és una arrel primitiva m-èssima de la unitat. En particualr, si $C[m] \subset C(K)$, aleshores $\mu_m \subset K^*$.

Demostració propietats [2]:

1. Linealitat en el primer factor:

$$e_m(S_1+S_2,T) = \frac{g(X+S_1+S_2)}{g(X+S_1)}\frac{g(X+S_1)}{g(X)} = e_m(S_2,T)e_m(S_1,T)$$

Hem usat que per $e_m(S_2,T) = g(Y+S_2)/g(Y)$ podem agafar el valor de Y com $Y = X+S_1$.

Per la linealitat en el segon factor agafem funcions $f_1, f_2, f_3, g_1, g_2, g_3$ com hem fet per T_1, T_2 i $T_3 = T_1+T_2$. Agafem $h \in \overline{K}(C)$ amb divisor

$$div(h) = (T_1+T_2) - (T_1) - (T_2) + (\mathcal{O})$$

aleshores

$$div(f_3/f_2f_1) = m\ div(h)$$

i

$$f_3 = cf_1f_2h^m$$

per algun $c \in \overline{K}^*$. Composem ara amb el mapa de multiplicació per m, usem $f_i \circ [m] = g_i^m$ i agafem les arrels m-èssimes per trobar

$$g_3 = c' g_1 g_2 I(h \circ [m])$$

Ara

$$\begin{aligned} e_m(S,T_1+T_2) = \frac{g_3(X+S)}{g_3(X)} &= \frac{g_1(X+S)g_2(X+S)h([m]X+[m]S)}{g_1(X)g_2(X)h([m]X)} \\ &= e_m(S,T_1)e_m(S,T_2) \end{aligned}$$

2. Per l'anterior propietat tenim

$$e_m(S+T,S+T) = e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T)$$

així que basta veure que $e_m(T,T) = 1$ per tot $T \in C[m]$. Per tot $P \in C$, sigui $\tau_P : C \to C$ el mapa de translació per P, és a dir: $\tau_P(Q) = Q+P$. Aleshores

$$div\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m\sum_{i=0}^{m-1}([1-i]T) - ([-i]T) = \mathcal{O}$$

Com $\prod_{i=0}^{m-1} f\circ\tau_{[i]T}$ és constant, is agafem algun $T' \in C[m]$ amb $[m]T' = T$, aleshores $\prod_{i=0}^{m-1} f \circ \tau_{[i]T'}$ és també constant, perquè la seva m-potència és el producte d'adalt de f's. Avaluant el producte de g's a X i a $X+T'$ es té

$$\prod_{i=0}^{m-1} g(X+[i]T') = \prod_{i=0}^{m-1} g(X+[i+1]T')$$

Ara cancelant els termes iguals tenim

$$g(X) = g(X+[m]T') = g(X+T)$$

i d'aquí

$$e_m(T,T) = g(X+T)/g(X) = 1$$

3. Si $e_m(S,T)=1$ per tot $S \in C[m]$, aleshores $g(X+S)=g(X)$ per tot $S \in C[m]$, i $g = h \circ [m]$ per alguna funció $h \in \overline{K}(C)$. Però llavors

$$(h \circ [m])^m = g^m = f \circ [m]$$

per tant $f = h^m$. D'aquí

$$m\ div(h) = div(f) = m(T) - m(\mathcal{O})$$

i

$$div(h) = (T) - (\mathcal{O})$$

4. Sigui $\sigma \in G_{\overline{K}/K}$. Si $f,\ g$ són funcions per T com fins ara, aleshores clarament $f^\sigma,\ g^\sigma$ són les corresponent funcions per T^σ. Per tant

$$e_m(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = \left(\frac{g(X+S)}{g(X)}\right)^\sigma = e_m(S,T)^\sigma$$

5. Agafant $f,\ g$ com abans, tenim

$$div(f^{m'}) = mm'(T) - mm'(\mathcal{O})$$

i

$$(g \circ [m'])^{mm'} = (f \circ [mm'])^{m'}$$

Ara de les definicions de $e_{mm'}$ i e_m,

$$e_{mm'} = \frac{g \circ [m'm](X+S)}{g \circ [m'](X)} = \frac{g(Y + [m']S)}{g(Y)} = e_m([m']S, T)$$

Lema 2.11. ([7]) *Sigui $C(\mathbb{F}_q)$ una corba el·líptica tal que $C[n] \subseteq C(\mathbb{F}_q)$ i n és coprimer amb q. Sigui $P \in C[n]$, aleshores P_1 i P_2 estan a la mateixa classe lateral de $< P >$ a $C[n]$ si i només si $e_n(P,P_1) = e_n(P,P_2)$.*

Prova:

Si $P_1 = P_2 + kP$ aleshores

$$e_n(P,P_1) = e_n(P,P_2)e_n(P,P)^k = e_n(P,P_2)$$

ja que $e_n(P,P) = 1$.

Ara si $e_n(P,P_1) = e_n(P,P_2)$, suposem que P_1 i P_2 estan a distintes classes laterals de $< P >$ a $C[n]$. Podem escriure $P_1 - P_2 = a_1P + a_2Q$ on P i Q són generadors de $C[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ i $a_2Q \neq \mathcal{O}$. Ara sigui $b_1P + b_2Q$ un punt qualsevol de $C[n]$, tenim

$$e_n(a_2Q, b_1P + b_2Q) = e_n(a_2Q, P)^{b_1} e_n(Q,Q)^{a_2b_2} = e_n(P, a_2Q)^{-b_1}$$

Si $e_n(P, a_2Q) = 1$ tenim per la no-degeneració de e_n que $a_2Q = \mathcal{O}$, el qual està en contradicció amb el que hem dit abans. Per tant, com $e_n(P, a_2Q) \neq 1$ ens quedaria

$$e_n(P,P_1) = e_n(P,P_2)e_n(P,P)^{a_1} e_n(P,Q)^{a_2} = e_n(P,P_2)e_n(P,Q)^{a_2} \neq e_n(P,P_2)$$

La qual cosa està en contradicció amb les hipòtesis del teorema.

Teorema 2.12. *Existeix un punt $Q \in C[n]$ tal que $e_n(P,Q)$ és una arrel n-èssima de la unitat.*

Prova: Sigui $Q \in C[n]$ aleshores tenim

$$e_n(P,Q)^n = e_n(P,nQ) = e_n(P,\mathcal{O}) = 1$$

Per tant $e_n(P,Q)$ és una arrel n-èssima de la unitat.

Hi ha n classes laterals de $< P >$ a $C[n]$ i per l'anterior lema es dedueix que a mesura que Q varia sobre aquests representants de les classes, $e_n(P,Q)$ varia sobre les n distintes arrels n-èssimes.

Teorema 2.13. *Sigui $Q \in C[n]$ tal que $e_n(P,Q)$ és una arrel primitiva n-èssima de la unitat. Definim $f : < P > \to \mu_n$ definida per $f(R) = e_m(R,Q)$. Aleshores f és un morfisme de grups.*

2.4 Corbes el·líptiques sobre cossos finits

Sigui C una corba el·líptica escrita en la forma de Weierstrass sobre un cos K de q elements i característica $p > 0$, volem saber la quantitat de punts que hi ha a $C(K)$ o el que és el mateix, un més dels punts $(x,y) \in K^2$ que són solució de

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Com cada valor de x té dos possibles valors per la y, el natural seria pensar que el nombre de punts a $E(K)$ és $2q+1$. No obstant, hem de tenir en compte que una "equació quadràtica aleatòria" té un 50% de probabilitat de ser resoluble a K, per tant s'esperaria que la correcta magnitud fós q.

E. Artin va conjecturar el següent teorema, que va ser provat per Hasse el 1930.

Teorema 2.14. *Sigui C/K una corba el·líptica definida sobre un cos amb q elements. Aleshores*

$$|\#C(K) - q - 1| \leqslant 2\sqrt{q}$$

Ara veurem una aplicació del resultat anterior. Sigui $K = \mathbb{F}_q$ amb q imparell i un polinomi cúbic amb arrels distintes a $\overline{K}$

$$f(x) = ax^3 + bx^2 + cx + d \in K[x]$$

I amb això definim $\chi : K^* \to \{\pm 1\}$ de manera que $\chi(t) = 1$ si, i només si t és un quadrat a K^*. Direm que $\chi(0) = 0$.

Ara usarem la funció χ per contar els K-punts racionals sobre la corba el·líptica

$$E : y^2 = f(x)$$

Cada $x \in K$ correspondrà a 0, 1 o 2 punts $(x,y) \in E(K)$ depenent de si $f(x)$ no és un quadrat, és 0, o és un quadrat distint de 0 sobre K. Usem ara aquesta funció per comptar els punts a $E(K)$, tenint en compte que hi ha un punt a l'infinit.

$$\#E(K) = 1 + \sum_{x \in K} (\chi(f(x)) + 1) = 1 + q + \sum_{x \in K} \chi(f(x))$$

Comparant aquest resultat amb el teorema anterior demostrat per Hasse veim que

$$|\sum_{x\in K}\chi(f(x))| \leqslant 2\sqrt{q}$$

Aquesta desigualtat ens diu que a mesura que passem per els elements $x \in K$ els valors d'un polinomi cúbic $f(x)$ tendeixen a estar igualment repartits entre quadrats i no-quadrats.

Teorema 2.15. *Sigui K un cos perfecte de característica p i C/K una corba el·líptica. Per cada enter $r \geqslant 1$, siguin*

$$\phi_r : C \to C^{p^r} \quad i \quad \hat{\phi}_r : C^{p^r} \to C$$

el p^r-mapa de Frobenius i el seu dual.

1. *Les següents propietats són equivalents*
   (a) $C[p^r] = 0$ *per tot* $r \geqslant 1$.
   (b) $\hat{\phi}_r$ *és purament inseparable per tot* $r \geqslant 1$.
   (c) *El mapa* $[p] : C \to C$ *és purament inseparable i* $j(C) \in \mathbb{F}_{p^2}$
2. *Si les propietats de l'anterior apartat no es donen, aleshores per tot* $r \geqslant 1$

$$C[p^r] = \mathbb{Z}/p^r\mathbb{Z}$$

Si C té les propietats donades al primer apartat, deim que C és supersingular.

Exemple 2.16. Agafem el cos $\mathbb{F}_{17}$ i la corba $y^2 = x^3 + 10x + 2$. Els 22 punts que formen part de la corba són

$$\begin{aligned} C(\mathbb{F}_{17}) = \{&\mathcal{O}, (0,6), (0,11), (1,8), (1,9), (2,8), (2,9), (3,5),\\ &(3,12), (4,2), (4,15), (8,4), (8,13), (11,7), (11,10),\\ &(13,0), (14,8), (14,9), (15,5), (15,12), (16,5), (16,12)\} \end{aligned}$$

Observam que aquesta corba té 22 punts sobre $\mathbb{F}_{17}$ i es compleix el teorema de Hasse

$$|22 - 17 - 1| = 4 \leqslant 2\sqrt{17} = 8.246$$

Podem comprovar també que fent la suma de dos punts de $C(\mathbb{F}_{17})$ ens dóna un altre punt dins $C(\mathbb{F}_{17})$.

Per exemple $(3,5) + (11,10) = (1,9)$.

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{10-5}{11-3} = \frac{5}{8} = 5 \cdot 8^{-1} = 5 \cdot 15 = 75 = 7 \pmod{17}$$

$$n = y_1 - mx_1 = 5 - 7 \cdot 3 = 1 \pmod{17}$$

$$x_3 = m^2 - x_1 - x_2 = 7^2 - 3 - 11 = 35 = 1 \pmod{17}$$

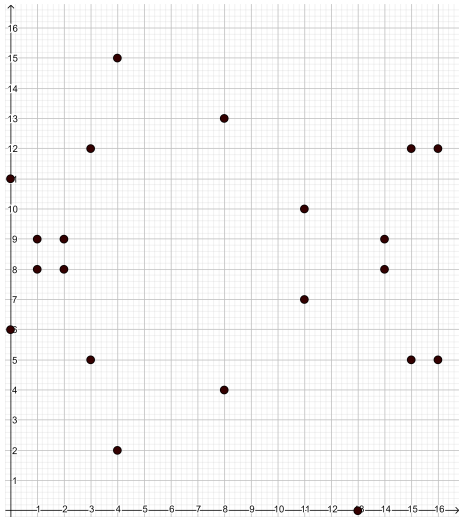

Figura 3: Representació dels punts sobre $y^2 = x^3 + 10x + 2$ a $\mathbb{F}_{17}$

$$y_3 = mx_3 + n = 7 \cdot 1 + 1 = 8 \pmod{17}$$

I el punt serà el $-(1, 8) = (1, -8) = (1, 9)$

Fem ara el punt $2(0, 11) = (4, 15)$

$$m = \frac{3x_P^2 + a}{2y_P} = \frac{3 \cdot 0^2 + 10}{2 \cdot 11} = \frac{10}{22} = \frac{10}{5} = 10 \cdot 7 = 70 = 2 \pmod{17}$$

$$n = y_P - mx_P = 11 - 2 \cdot 0 = 11 \pmod{17}$$

$$x_3 = m^2 - 2x_P = 2^2 - 2 \cdot 0 = 35 = 4 \pmod{17}$$

$$y_3 = mx_3 + n = 2 \cdot 4 + 11 = 2 \pmod{17}$$

I el punt serà el $-(4, 2) = (4, -2) = (4, 15)$

Després del teorema provat per Hasse, en lo referent a l'ordre del grup sobre la corba el·líptica es va arribar al següent lema:

Lema 2.17. *Existeix una corba d'ordre $q + 1 - t$ sobre $\mathbb{F}_q$ on $q = p^m$ si i només si es té una de les següents condicions:*

1. *$t \not\equiv 0 \pmod{p}$ i $t^2 \leqslant 4q$*
2. *m és imparell i es té una de les següents:*
   - *(a) $t = 0$*
   - *(b) $t^2 = 2q$ i $p = 2$*
   - *(c) $t^2 = 3q$ i $p = 3$*

3. m és parell i es té una de les següents:

(a) $t^2 = 4q$

(b) $t^2 = q$ *i* $p \not\equiv 1 \pmod 3$

(c) $t = 0$ *i* $p \not\equiv 1 \pmod 4$

Es diu que una corba és superesingular si p divideix t. De l'anterior resultat podem deduir que una corba és supersingular si i només si $t^2 = 0,\ q,\ 2q,\ 3q$ o $4q$. El següent lema ens dóna l'estructura de grup d'una corba supersingular. $\mathbb{Z}_n$ és el grup cíclic de n elements.

Lema 2.18. *Sigui* $\#C(\mathbb{F}_q) = q + 1 - t$

1. *Si* $t^2 = q,\ 2q$ *o* $3q$, *aleshores* $C(\mathbb{F}_q)$ *és cíclic.*
2. *Si* $t^2 = 4q$ *aleshores:*
   si $t = 2\sqrt{q}$, $C(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$
   si $t = -2\sqrt{q}$, $C(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$
3. *Si* $t = 0$ *i* $q \not\equiv 3 \pmod 4$, $C(\mathbb{F}_q)$ *és cíclic.*
   Si $t = 0$ *i* $q \equiv 3 \pmod 4$, *aleshores o* $C(\mathbb{F}_q)$ *és cíclic o* $C(\mathbb{F}_q) \cong \mathbb{Z}_{(q+1)/2}$

La corba C la podem veure també com una corba sobre una extensió K de $\mathbb{F}_q$; $C(\mathbb{F}_q)$ és un subgrup de $C(K)$. A partir de les conjectures de Weil podem calcular $\#C(\mathbb{F}_{q^k})$ a partir de $\#C(\mathbb{F}_q)$ de la següent manera.

Sigui $\#C(\mathbb{F}_q) = q+1-t$, aleshores $\#C(\mathbb{F}_{q^k}) = q^k + 1 - \alpha^k - \beta^k$, on α i β són números complexes determinats per la factorització $1 - tT + qT^2 = (1 - \alpha T)(1 - \beta T)$.

2.5 Corbes hiperel·líptiques

Aquestes corbes són més generals que les corbes el·líptiques, és fàcil veure que aquestes només són un cas particular.

Aquí seguirem l'article [8].

Sigui $K = \mathbb{F}_q$ el cos finit de q elements i $\overline{K} = \bigcup_{n \geqslant 1} \mathbb{F}_{q^n}$ la seva clausura algebraica. Una corba hiperel·líptica C de gènere g està definida per una equació del tipus

$$y^2 + h(x)y = f(x)$$

on h i $f \in K[x]$, el grau de f és $\deg f = 2g + 1$ i $\deg h \leqslant g$.

Sigui L una extensió del cos K. El conjunt de punts L-racionals són el conjunt

$$C(L) = \{(x, y) :\ x,\ y \in L,\ y^2 + h(x)y = f(x)\} \cup \{\infty\}$$

L'oposat d'un punt $P = (x, y) \in C(L)$ és $-P = (x, -y - h(x))$ $(-\infty = \infty)$. En aquestes corbes no hi ha en general una llei de grup natural definida sobre $C(L)$, expecte en el cas de les corbes el·líptiques, que són el cas on $g = 1$, és a dir, on $\deg f = 3$.

El grup D^0 de divisors de grau zero de C és el conjunt de sumes formals $D = \sum_{P \in C(\overline{K})} n_P P$, amb $n_P \in \mathbb{Z}$, només un nombre finit dels $n_P \neq 0$ i tal que $\sum n_P = 0$. D^0 és un grup sota l'addició $\sum_{P \in C} n_P P + \sum_{P \in C} m_P P = \sum_{P \in C} (n_P + m_P) P$.

El cos de funcions denotat per $K(C)$ és el cos de fraccions del domini d'integritat de polinomis $K[x,y]/(y^2 + h(x)y - f(x))$. Sigui $f \in K(C)$, el divisor de f és $\mathrm{div} f = \sum_{P \in C(\overline{K})} n_P(f) P$, on $n_P(f)$ denota la multiplicitat de P com a arrel de f. El grup $\mathrm{Prin}_K = \{\mathrm{div}(f) : f \in K(C)\}$ és subgrup de D^0.

Definició 2.19. *El jacobià de C sobre K és el grup quocient $J_C(K) = D^0_K / Prin_K$.*

$J_C(K)$ és un grup finit. Un teorema de Weil implica $(\sqrt{q}-1)^{2g} \leqslant \# J_C(K) \leqslant (\sqrt{q}+1)^{2g}$ així que $\# J_C(K) \approx q^g$. Si D_1 i D_2 estan a la mateixa classe d'equivalència escrivim $D_1 \sim D_2$. Cada classe d'equivalència té un únic divisor en forma reduïda, és a dir $\sum_{P \in C} n_P P - \sum_{P \in C} n_P \mathcal{O}$, tal que $n_P \geqslant 0$ per tot P, si $n_P \geqslant 1$ i $P \neq -P$ aleshores $n_{-P} = 0$, $n_P = 0$ o 1 si $P = -P$ i $\sum n_P \leqslant g$.

Aquest divisor es pot representar de manera única per un parell de polinomis $a,\ b \in K[x]$, on $\deg b < \deg a \leqslant g$, a és mònic i $a | (b^2 + bh - f)$. Escrivim $D = \mathrm{div}\ (a,b)$ per dir $D = \mathrm{m.c.d.}(\mathrm{div}(a), \mathrm{div}(b - v))$, on el m.c.d. de dos divisors es defineix com $\sum_{P \in C} \min(n_P, m_P) P - \sum_{P \in C} \min(n_P, m_P)\, \mathcal{O}$. El grau de D és $\deg a$.

3 Xifrats

3.1 ECDLP

En aquesta secció treballarem sobre el logaritme discret en corbes el·líptiques o logaritme el·líptic (ECDLP o *Elliptic Curve Discrete Logarithm Problem*). En aquest problema es fonamenta la criptografia basada en corbes el·líptiques. Ens basarem en [4].

Al 1985, Neal Kobitz i Victor Miller van proposar cadascú de manera independent l'ús de corbes el·líptiques en criptografia. Desde llavors aquesta criptografia s'ha utilitzat en camps tant diversos com els sistemes de xifrat i desxifrat de dades, generació i verificació de firmes digitals, factorització d'enters, estudi de primalitat...

De la mateixa manera que els problemes de factorització i del logaritme discret, no es coneix cap algoritme que resolgui eficientment el logaritme el·líptic en tots els casos. Com veurem hi ha certs casos en que aquestes corbes són més dèbils davant possibles atacs. No obstant això s'estima que el logaritme el·líptic és el més difícil dels tres problemes mencionats, per això es considera que la criptografia basada en corbes el·líptiques és la que proporciona els criptosistemes més resistents.

El problema del logaritme discret és el següent:

Definició 3.1. *Sigui G un grup cíclic finit i a, $b \in G$. Aleshores el problema del logaritme discret és trobar un n tal que $a^n = b$. Direm que $n = \log_a b$.*

I el problema del logaritme el·lítpic és:

Definició 3.2. *Donada una corba C definida sobre un cos finit $\mathbb{F}_q$ i un punt P obtingut a partir d'un generador G d'ordre n, el problema del logaritme el·líptic és trobar $k \in \{0, 1, \ldots, n-1\}$ tal que $P = kG$. L'anomenarem $k = \log_G P$*

Els cossos finits $\mathbb{F}_q$ només existeixen si q és de la forma $q = p^m$. A més, per un valor de m existeix un únic cos, llevat d'isomorfismes, amb cardinal p^m.

En general la criptografia basada en corbes el·líptiques utilitza dos tipus de cossos $\mathbb{F}_q$: els $\mathbb{F}_p$ i els $\mathbb{F}_{2^m}$.

Si el cos és de la forma $\mathbb{F}_p$ se'l denomina cos finit primer i en aquests casos el cos és isomorf a $\mathbb{Z}/p\mathbb{Z}$. Als cossos de la forma $\mathbb{F}_{2^m}$ se'ls denomina cossos finits binaris. En aquest cas es pot representar un element $a \in \mathbb{F}_{2^m}$ com una cadena de bits $a = (a_{m-1}a_{m-2}\ldots a_2a_1)$ on els $a_i = 0, 1$.

La longitud d'una corba el·líptica i de les claus associades a la corba es poden calcular a partir del tamany del cos finit sobre les que estan definides. Aquesta longitud ha de ser interpretada com el número de bits necessaris per representar l'enter p en corbes sobre cossos primers (el valor $\lceil \log_2 p \rceil$), mentre que en el cas de corbes sobre cossos binaris aquesta longitud coincideix amb el valor m.

3.2 Protocols d'acord de clau

Passem a veure ara uns sistemes usats per acordar una clau de manera pública però sense que un usuari no desitjat pugui saber-la.

3.2.1 ECDH

Aquest és el protocol de Diffie-Hellman, ECDH (*Elliptic Curve Diffie-Hellman key agreement protocol*). En aquest cas suposarem que es volen posar en contacte dos usuaris **U** i **V**.

Abans de tot els dos usuaris s'han de posar d'acord sobre quin cos finit $\mathbb{F}_q$ treballaran, quina corba el·líptica C usaran i quin generador del grup G triaran.

Passos:

1. **U** determina un número secret aleatori u i calcula el punt de la corba uG. **U** envia uG a **V**.
2. **V** genera un altre número aleatori secret v i calcula també vG i l'envia a **U**.
3. Ara **U** pot calcular el punt $u(vG)$ i **V** pot calcular el punt $v(uG)$.
4. Ara **U** i **V** han calculat el mateix punt de la corba: $u(vG) = v(uG) = (uv)G$ que no podia ser precalculat per ningun dels dos abans d'iniciar el protocol.

Ara **U** i **V** poden usar aquest punt que han calculat com a clau o com a semilla per generar una clau a partir d'ell.

Si un adversari volgués calcular el punt a partir de la conversació entre **U** i **V** es trobaria amb que ha de calcular uvG a partir de uG i vG. Aquest problema es coneix com el problema de Diffie-Hellman (DHP o *Diffie-Hellman Problem*). Hauria de ser capaç de determinar u a partir de uG però això és el problema del logaritme discret sobre una corba el·líptica que assumim irressoluble.

Exemple 3.3. Agafem la corba $y^2 = x^3 + 33x + 51$ definida sobre $\mathbb{F}_{71}$, que té ordre $n = 67$. Agafem el punt generador $G = (57, 18)$ que necessàriament té ordre 67 ja que 67 és primer.

Ara **U** determina el número $u = 12$ i calcula $uG = 12(57, 18) = (33, 21)$. **V** fa el mateix amb $v = 62$, $vG = 62(57, 18) = (32, 47)$. A continuació s'envien mútuament els punts sobre la corba que han generat i els dos podran calcular

$$uvG = 12 \cdot 62(57, 18) = 12(32, 47) = 62(33, 21) = (43, 26)$$

No obstant això hi ha un atac a aquest tipus de criptografia que es coneix com el "Man in the Middle Attack"o l'home d'enmig.

Aquest atac es basa en la capacitat d'un atacant **A** que pugui no només interceptar les transmissions entre **U** i **V** si no que a més és capaç de reemplaçar els valor que s'envien per un altre que hagi triat ell.

Passos:

1. **U** determina un número secret aleatori u i calcula el punt de la corba uG i l'intenta enviar a **V**.
2. **A** intercepta el missatge i en lloc d'enviar el punt uG a **V** envia el punt aG on a és un enter de la seva elecció.

3. **V** determina un punt vG de la corba amb v un número aleatori i l'intenta enviar a **U**.

4. **A** novament intercepta el missatge i torna a enviar el punt aG a **U**.

5. Ara seguint l'anterior protocol **U** calcularia el punt $u(aG)$ i **V** calcularia el punt $v(aG)$.

D'aquesta manera **A** pot calcular els dos punts que han calculat finalment **U** i **V**, que s'han quedat amb dues claus que no coincideixen encara que ells no ho saben.

Amb aquest atac **A** pot conèixer tots els missatges que es volen enviar **U** i **V** entre ells i, a més, si vol pot canviar el missatge. És a dir **U** podria haver enviat un missatge m a **V** i **A** en saber el missatge canviar-lo per un altre missatge $\overline{m}$ que ell prefereixi, controlant d'aquesta manera les comunicacions.

Aquest protocol de Diffie-Hellman es pot considerar d'una ronda, ja que els dos usuaris **U** i **V** només han de mandar i rebre informació una vegada.

Si volem es pot estendre a 3 usuaris **U**, **V** i **W**. Seleccionen públicament una corba C, d'ordre n i un generador G de la corba.

Ara els 3 usuaris tendrien la seva respectiva clau secreta: **U** generaria u, **V** generaria v i **W** generaria w. Amb tot això els usuaris haurien de fer dues rondes.

A la 1a ronda:

1. **U** envia a **V** uG, **V** envia a **W** vG i **W** envia a **U** wG.

2. **U** envia a **V** $u(wG)$, **V** envia a **W** $v(uG)$ i **W** envia a **U** $w(vG)$.

3. Ara els tres usuaris poden calcular $uvwG$.

Un atacant hauria de poder calcular $uvwG$ donats G, uG, vG, wG, uvG, vwG i uwG, que es suposa que és un problema no més fàcil que el problema de Diffie-Hellman.

A continuació el que ens demanem és si és possible fer un acord de clau entre les tres parts en una única ronda. La resposta la va donar Joux i la trobarem en els emparellaments bilineals.

Usarem un emparellament bilineal que anirà dels elements de la nostra corba al corresponent grup cíclic i amb això establirem el protocol següent en una ronda:

1. Els tres usuaris **U**, **V** i **W** eligeixen aleatòriament enters u, v i w i envien el respectiu valor uG, vG i wG a les altres dues parts.

2. Ara cada un pot calcular:

$$\mathbf{U}\text{: } \psi(vG, wG)^u = \psi(G, G)^{uvw}$$

$$\mathbf{V}\text{: } \psi(uG, wG)^v = \psi(G, G)^{uvw}$$

$$\mathbf{W}\text{: } \psi(uG, vG)^w = \psi(G, G)^{uvw}$$

Ara el que comparteixen els tres és un element del grup multiplicatiu d'arribada, no un punt sobre la corba.

Per extendre aquest protocol a r usuaris necessitariem una apicació multilineal computable, és a dir una aplicació definida de: $\psi_r : C^{r-1} \to C^*$, on C és la corba el·líptica i C^* el grup multiplicatiu al que aniriem amb la aplicació multilineal.

El que voldriem fer seria, donats G, a_1G, a_2G, ...,a_rG, calcular

$$\psi_r(G, G, \ldots, G)^{a_1 a_2 \ldots a_r}$$

Aquestes aplicacions pareixen possibles per a $r = 3$, però per a $r > 3$ un treball de Boneh i Silverberg ha mostrat algunes evidències de que no és possible construir aquest tipus d'aplicacions.

3.2.2 ElGamal

Ara per aquest sistema necessitarem una corba C, un generador G de la corba d'ordre n i una relació que es conegui públicament entre un possible missatge a transmetre m i un punt de la corba P_m. Ara veurem com hauria de fer un usuari **U** per enviar-li el missatge m a **V**.

Passos:

1. **V** agafa aleatòriament un valor v (amb $0 < v < n$) i dóna a conèixer la seva clau pública: $V = vG$.

2. Ara **U** vol enviar el missatge m a **V**. Mirarà a la llista pública quin punt P_m correspon al missatge i després triarà un valor u aleatori (amb $0 < u < n$) i enviarà el parell de punts $(uG, P_m + uV)$ a **V**.

3. En haver rebut els punts, l'usuari **V** podrà recuperar el punt P_m que representa el missatge m multiplicant el punt uG per el valor v, amb el que obtindrà $v(uG) = u(vG) = uV$ i ho podrà restar de $P_m + uV$ obtenint així $(P_m + uV) - uV = P_m$.

Exemple 3.4. Treballem sobre la corba $y^2 = x^3 + 40x + 7$ definidia sobre $\mathbb{F}_{61}$ amb ordre $n = 61$ de l'element generador $(10, 59)$.

Si **U** volgués enviar el missatge "Compra 50 camions" a la seva empresa **V** amb clau privada $v = 27$ i clau pública el punt $V = (46, 27)$, primer hauria de consultar la llista de missatges i punts associats, suposem que el punt P_m associat al nostre missatge és $P_m = (60, 24)$. **U** primer obtindria un valor aleatori, per exemple $u = 18$ i calcularia:

$$uG = 18(10, 59) = (37, 30)$$

$$P_m + uV = (60, 24) + 18(46, 27) = (60, 24) + (7, 9) = (8, 31)$$

Després **U** mandaria a **V** el criptograma format pel parell de punts $((37, 30), (8, 31))$. I ara per recuperar el punt P_m **V** hauria de realitzar els següents càlculs:

$$P_m = (P_m + uV) - uV = (P_m + uV) - u(vG) = (P_m + uV) - v(uG)$$

$$= (8, 31) - 27(37, 30) = (8, 31) - (7, 9) = (8, 31) + (7, 52) = (60, 24)$$

3.2.3 Massey-Omura

Per aquest sistema la preparació és quasi la mateixa que per la d'ElGamal: una corba el·líptica C definida sobre un cos $\mathbb{F}_q$ i una llista que relacioni els possibles missatges a enviar m amb un punt de la corba P_m. Ara no necessitem d'un generador de la corba. Veiem que hauria de fer un usuari **U** per enviar un missatge a **V**.

Passos:

1. **U** generaria un enter aleatori u tal que $0 < u < n$ on n és l'ordre de la corba. Hauria de cercar el punt P_m corresponent al missatge m que vol enviar i calcular el punt uP_m i enviar-lo a **V**.
2. Ara, **V** generaria un altre enter aleatori v amb $0 < v < n$ i tornaria el punt vuP_m a **U**.
3. Ara **U** retransmetrà de tornada el punt $u^{-1}vuP_m = vP_m$, amb u^{-1} l'invers de u mòdul n.
4. Ara l'usuari **V** pot obtenir el punt P_m calculant $v^{-1}vP_m = P_m$ i obtenint així el missatge m.

En aquest procediment s'hauria d'anar alerta: si l'ordre de la corba n no fós primer ens hauriem d'assegurar que u i v fossin coprimers amb n per tal que existissin els seus respectius inversos.

Exemple 3.5. Considerem ara la corba $y^2 = x^3 + 32x + 44$ definida sobre $\mathbb{F}_q$ amb $n = 59$.

Si ara **U** vol enviar el missatge "compra una central elèctrica"a **V**, primer hauria de consultar a la llista pública de relacions entre missatges i punts de la corba i determinaria el punt $P_m = (5, 16)$, per exemple. Suposem que aleatòriament genera també l'enter $u = 20$ i envia a **V** el punt $uP_m = 20(5, 16) = (34, 33)$.

V ha rebut el punt i ha generat l'enter $v = 23$ i envia a **U** el punt $v(uP_m) = 23(34, 33) = (22, 9)$. **U** envia de tornada el punt $u^{-1}(vuP_m) = 3(22, 9) = (20, 56)$, ja que $u^{-1} = 20^{-1} = 3 \pmod{59}$.

V ja pot calcular el punt original de la corba fent $v^{-1}(vP_m) = 18(20, 56) = (5, 16)$, ja que $v^{-1} = 23^{-1} = 18 \pmod{59}$. I amb aquest punt P_m recupera el missatge original m.

Un dels desavantatges teòrics dels sistemes d'ElGamal i Massey-Omura és el finit nombre de missatges a xifrar, limitat per el nombre de punts a la corba. La limitació és teòrica degut a que es poden triar corbes amb un nombre de punts molt elevat.

La utilitat d'aquests sistemes està limitada a entorns tancats on els possibles missatges estiguin prèviament estipulats.

3.2.4 ECDSA

Aquest és un protocol de firma digital (ECDSA, *Elliptic Curve Digital Signature Algorith*). És el protocol anàleg al sistema de firma digital DSA (*Digital Signature Algorithm*).

Per aquest protocol s'usarà: una corba el·líptica C, el cos finit $\mathbb{F}_q$, el generador del grup de la corba G, el parell de claus privada i pública del firmant **U**, (u, uG) i del verificador **V**, (v, vG) i una funció resum $\mathcal{H}$ o funció *hash*.

Una funció resum és una aplicació $\mathcal{H} : M \to N$ que té com a entrada una cadena de M i les converteix en una cadena de longitud normalment fixa en N. Es pot dir que actua com una projecció del conjunt M sobre el conjunt N.

El protocol té dues parts que es separen en dos algoritmes: el d'elaboració de la firma i el de verificació de la firma.

Passos del protocol d'elaboració:

1. **U** calcula el resum del missatge m fent $\mathcal{H}(m) = \tilde{m}$.
2. **U** genera un número aleatori k tal que $0 < k < n - 1$ on n és l'ordre de G i calcula $kG = (x_1, y_1)$ i $r = x_1 \pmod{n}$. Si $r = 0$ s'escull un altre valor de k.
3. **U** determina $k^{-1} \pmod{n}$ i calcula $s = k^{-1}(\tilde{m} + ur) \pmod{n}$.
4. La firma de **U** per el resum del missatge m és el parell (r, s).

Ara vegem el procés de verificació de la firma una vegada **V** ha rebut el missatge a verificar i la firma.

Passos del protocol de verificació:

1. **V** calcula el resum del missatge m: $\mathcal{H}(m) = \tilde{m}$.
2. **V** comprova que els enters r i s estan a l'interval $[1, n - 1]$.
3. **V** determina el valor $s^{-1} \pmod{n}$ i calcula $z_1 = \tilde{m}s^{-1} \pmod{n}$ i $z_2 = rs^{-1} \pmod{n}$.
4. Després, **V** determina $z_1G + z_2uG = (x_0, y_0)$.
5. Finalment, **V** accepta la firma com a vàlida si, i només si $r = x_0 \pmod{n}$.

El procés és correcte donat que, si denotem per $(P)_x$ la primera coordenada del punt $P \in C$ es té el següent:

$$x_0 = (z_1G + z_2uG)_x = (\tilde{m}s^{-1}G + rs^{-1}uG)_x = ((\tilde{m} + ru)s^{-1}G)_x$$
$$= (kG)_x = x_1 \pmod{n} = r$$

Exemple 3.6. Agafem la corba $y^2 = x^3 + 3x + 42$ definida sobre el cos $\mathbb{F}_{89}$, on l'ordre de la corba és 79, agafem com a generador el punt $G = (69, 80)$. La clau privada de l'usuari **U** és $u = 23$ i la clau pública és $23G = 23(69, 80) = (70, 35)$.

Per firmar el missatge m, que suposem que el seu resum és $\tilde{m} = 63$, **U** eligeix de manera aleatòria el valor $k = 14$ i calcula $kG = 14(69, 80) = (67, 39)$ i per tant $r = 67 \pmod{79} = 67$. A continuació, **U** determina

$$k^{-1} = 14^{-1} \pmod{79} = 17 \pmod{79}$$

$$s = k^{-1}(\tilde{m} + ur) \pmod{n} = 17(63 + 23 \cdot 67) \pmod{79} = 13 \pmod{79}$$

Això ens deixa amb la firma $(r, s) = (67, 13)$.

Per a verificar la firma del missatge, **V** necessita la clau pública $uG = (70, 35)$, calcular el resum $\tilde{m} = 63$ del missatge, comprovar que $r = 67$ i $s = 13$ estan a l'interval $[1, n-1] = [1, 78]$ i calcular el valor

$$s^{-1} = 13^{-1} \pmod{79} = 73 \pmod{79}$$

Ara **V** ha de determinar els valors

$$z_1 = \tilde{m}s^{-1} \pmod{n} = 63 \cdot 73 \pmod{79} = 17 \pmod{79}$$

$$z_2 = rs^{-1} \pmod{n} = 67 \cdot 73 \pmod{79} = 72 \pmod{79}$$

Després de calcular

$$z_1G + z_2uG = 17(69, 80) + 72(70, 35) = (31, 72) + (79, 13) = (67, 39)$$

V acceptarà la firma ja que $r = 67 = (z_1G + z_2uG)_x \pmod{n}$.

3.2.5 Firma BLS

Aquest protocol és per crear una firma però fent ús novament dels emparellaments bilineals. Boneh, Lynn i Shacham van proposar el primer esquema de firma en el que aquesta es reduïa a un sol enter i per aquest motiu la coneixem com a firma curta.

El protocol es coneix com esquema de firma BLS(*Boneh-Lynn-Shacham scheme*). Per aquesta firma necessitem una corba C, un generador G del grup sobre la corba, un emparellament bilineal ψ sobre la corba i una funció resum $\mathcal{H}$ que vagi d'una cadena de bits a la corba $C\backslash\{\mathcal{O}\}$.

La clau pública de **U** és $U = uG$ on $u \in [1, n-1]$ és la seva clau privada i un enter aleatori.

Generació de la firma:

1. **U** calcula $\mathcal{H}(m) = \tilde{m}$.
2. **U** determina la seva firma com $S = u\tilde{m}$.

Ara un usuari **V** que conegui la clau pública de **U** pot verificar la firma S amb el següent algoritme:

1. **V** calcula $\mathcal{H}(m) = \tilde{m}$.
2. **V** determina $g_1 = \psi(G, S)$ i $g_2 = \psi(U, \tilde{m})$.
3. **V** accepta la firma com a vàlida si, i només si $g_1 = g_2$.

Amb el protocol anterior es té

$$g_1 = \psi(G, S) = \psi(G, u\tilde{m}) = \psi(G, \tilde{m})^u = \psi(uG, \tilde{m}) = \psi(U, \tilde{m}) = g_2$$

Per falsificar la firma de **U** sobre el missatge m un atacant hauria de calcular $S = u\tilde{m}$, donats G, U i $\tilde{m} = \mathcal{H}(m)$. Això és el cas del problema de Diffie-Hellman sobre C que es considera intractable, fent que aquest esquema per a la firma sigui segur.

4 Atacs a la corba

En aquesta secció veurem alguns atacs a la corba el·líptica. Hi ha dos tipus de mètodes: els generals i els específics. [4]

Els atacs generals valen per qualsevol tipus de corba, en canvi els específics aprofiten les característiques especials que tenen algunes corbes.

Un exemple d'atac general és el de força bruta o de cerca exhaustiva: consisteix en provar tots els valors G, $2G$, $3G\ldots$ fins a trobar el k tal que $P = kG$. De mitja s'hauran de provar $n/2$ multiplicacions d'un escalar pel punt G i en el pitjor dels casos es necessitarien n multiplicacions.

El tamany de l'ordre del generador de les corbes utilitzades habitualment en criptografia fa inviable l'ús d'aquesta tècnica. Un atacant que pogués realitzar un billó de multiplicacions per segon, necessitaria millons d'anys per determinar un únic logaritme.

4.1 Reducció del logaritme el·líptic

Ara veurem una reducció del logaritme el·líptic sobre la corba a logaritmes discrets sobre cossos finits. [7]

Agafem una corba C definida sobre $\mathbb{F}_q$ amb estructura de grup $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ amb $n_2 | \, n_1$. Sigui $P \in C[n]$ un punt d'ordre n i assumim que coneixem n. Ara volem trobar donat un R, l'enter $l \in [0, n-1]$ tal que $R = lP$.

Per tal de resoldre el problema del logaritme discret en lloc del logaritme el·líptic usarem el *Weil Pairing*. Del fet que $e_n(P, P) = 1$ deduïm que $R \in < P >$ si i només si $nR = \mathcal{O}$ i $e_n(P, R) = 1$. Com aquestes condicions es poden comprovar en temps polinomial assumim que, donats P i R, $R \in < P >$.

Amb el següent algoritme trobam informació parcial sobre l:

Input: un element $P \in C(\mathbb{F}_q)$ d'ordre màxim n_1 i $R = lP$.

Output: Un enter $l' = l \pmod{n'}$, on $n' | n_2$.

Algoritme:

1. Agafam un punt aleatori $T \in C(\mathbb{F}_q)$
2. Computam $\alpha = e_{n_1}(P, T)$ i $\beta = e_{n_1}(R, T)$
3. Computam l', el logaritme discret de β en base α a $\mathbb{F}_q$.

L'algoritme calcula $l' \equiv l \pmod{n'}$:

Sigui n' l'ordre de α, n' divideix n_2 per les següents raons. Sigui $G \in C(\mathbb{F}_q)$ un element d'ordre n_2 tal que els elements P i Q generen $C(\mathbb{F}_q)$ i sigui $T = c_1 P + c_2 Q$. Aleshores

$$\alpha^{n_2} = e_{n_1}(P, T)^{n_2} = e_{n_1}(P, P)^{c_1 n_2} e_{n_1}(P, c_2 n_2 G) = e_{n_1}(P, \mathcal{O}) = 1$$

I ara:

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

Podem determinar l' calculant el logaritme discret de β en base α a $\mathbb{F}_q$.

Com hi ha n_2 classes laterals de $< P >$ a $C(\mathbb{F}_q)$, la probabilitat de que $n' = n_2$ és $\phi(n_2)/n_2$.

Ara donarem un algoritme per trobar l mòdul n amb $R = lP$.

Input: un element $P \in C(\mathbb{F}_q)$ d'ordre n i $R \in < P >$.

Output: Un enter l tal que $R = lP$.

Algoritme:

1. Determinar l'enter k més petit tal que $C[n] \subseteq C(\mathbb{F}_{q^k})$
2. Trobar $Q \in C[n]$ tal que $\alpha = e_n(P, Q)$ té ordre n.
3. Computem $\beta = e_n(R, Q)$.
4. Computem l, el logaritme discret de β en base α sobre $\mathbb{F}_{q^k}$.

L'algoritme és correcte ja que:

$$\beta = e_n(R, Q) = e_n(lP, Q) = e_n(P, Q)^l = \alpha^l$$

Aquest algoritme, encara que és correcte, no ens val sempre, ja que en general necessita un temps exponencial. No es dona cap mètode per determinar k o trobar Q. Veurem ara què passa en el cas de les corbes el·líptiques supersingulars.

4.2 Reducció del cas corba supersingular

En el cas de les corbes supersingulars, veurem que la reducció necessita un temps probabilístic polinomial, el que ens dóna un temps probabilístic subexponencial per resoldre els logaritmes el·líptics en aquestes corbes. [7]

Pel que hem vist a la secció de corbes el·líptiques sobre cossos finits sabem que, sent $C(\mathbb{F}_q)$ una corba el·líptica amb $q = p^m$ i $\#C(\mathbb{F}_q) = q + 1 - t$, aleshores només hi ha les següents possibilitats:

1. $t = 0$ i $C(\mathbb{F}_q) \cong \mathbb{Z}_q$.
2. $t = 0$ i $C(\mathbb{F}_q) \cong \mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$ (i $q \equiv 3 \pmod 4$).
3. $t^2 = q$ i m és parell.
4. $t^2 = 2q$ i $p = 2$ i m és imparell.
5. $t^2 = 3q$ i $p = 3$ i m és imparell.
6. $t^2 = 4q$ i m és parell.

Sigui P un punt d'ordre n a $C(\mathbb{F}_q)$. Com $n_1 | (q + 1 - t)$ i $p | t$, tenim m.c.d.$(n_1, q) = 1$. Aplicant la conjectura de Weil i el lema de les estructures dels grups de les corbes el·líptiques es pot determinar el menor enter k tal que $C[n_1] \subseteq C(\mathbb{F}_{q^k})$, i per tant $C[n] \subseteq C(\mathbb{F}_{q^k})$. Per cada tipus de corba la estructura de $C(\mathbb{F}_{q^k})$ és de la forma $\mathbb{Z}_{cn_1} \oplus \mathbb{Z}_{cn_1}$ per un c apropiat. A la taula s'adjunta informació sobre els distints tipus de corba.

Informació sobre les corbes						
Tipus	t	Estructura grup	n_1	k	Tipus $C(\mathbb{F}_{q^k})$	c
1	0	Cíclic	$q+1$	2	$(q+1, q+1)$	1
2	0	$\mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$	$(q+1)/2$	2	$(q+1, q+1)$	2
3	$\pm\sqrt{q}$	Cíclic	$q+1 \mp \sqrt{q}$	3	$(\sqrt{q^3} \pm 1, \sqrt{q^3} \pm 1)$	$\sqrt{q} \pm 1$
4	$\pm\sqrt{2q}$	Cíclic	$q+1 \mp \sqrt{2q}$	4	(q^2+1, q^2+1)	$q \pm \sqrt{2q} + 1$
5	$\pm\sqrt{3q}$	Cíclic	$q+1 \mp \sqrt{3q}$	6	(q^3+1, q^3+1)	$(q+1)(q \pm \sqrt{3q} + 1)$
6	$\pm 2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}\mp 1} \oplus \mathbb{Z}_{\sqrt{q}\mp 1}$	$\sqrt{q} \mp 1$	1	$(\sqrt{q} \mp 1, \sqrt{q} \mp 1)$	1

Ara donem l'algoritme de reducció pel cas de les corbes el·líptiques supersingulars:

Input: Un element P d'ordre n en una corba supersingular $C(\mathbb{F}_q)$, i $R \in < P >$.

Output: Un enter l tal que $R = lP$.

Algoritme:

1. Determinem k i c a partir de la taula.
2. Agafem un punt aleatori $Q' \in C(\mathbb{F}_{q^k})$ i posam $Q = (cn_1/n)Q'$.
3. Computem $\alpha = e_n(P, Q)$ i $\beta = e_n(R, Q)$.
4. Feim el logaritme discret l' de β en base α a $\mathbb{F}_{q^k}$.
5. Comprovem que $l'P = R$. Si és així $l = l'$ i ja estem. Si no, l'ordre de α és menor que n i tornam al punt 2.

Lema 4.1. *Sigui G un grup abelià de tipus (cn, cn). Si els elements $\{\alpha_i\}$ són uniformement seleccionats de manera aleatòria sobre G, aleshores els elements $\{c\alpha_i\}$ estan uniformement distribuïts sobre els elements del subgrup G de tipus (n, n).*

Pel lema, Q és un punt aleatori sobre $C[n]$, i la probabilitat que l'element α tingui ordre n és de $\phi(n)/n$. Ja que hi ha $\phi(n)$ elements d'ordre n a $\mathbb{F}_{q^k}$ i hi ha n classes laterals de $< P >$ a $C[n]$.

4.3 Atac GHS

Veurem ara un atac basat en un algoritme donat per [8].

Siguin l i n enters tals que $q = 2^l$ i $K = \mathbb{F}_{q^n}$, considerem la corba el·líptica C definida sobre K per la equació

$$\mathrm{C} : y^2 + xy = x^3 + ax^2 + b, \quad a \in K,\, b \in K^*$$

Suposem que $\#C(K) = dr$ amb d petit: $d = 2$ o $d = 4$ i r primer. Per tant $r \approx q^n$. Sigui $b_i = \sigma^i(b)$ on $\sigma : K \to K$ és l'automorfisme de Frobenius $\sigma(\alpha) = \alpha^q$ i definim:

$$m(b) = \dim_{\mathbb{F}_2}(< (1, b_0^{1/2}), \ldots, (1, b_{n-1}^{1/2}) >)$$

Assumim que n és imparell o $m(b) = n$ o $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$. Gaundry, Hess i Smart van provar que es pot usar el mètode de l'atac del descens de Weil per reduir el problema del

logaritme el·líptic en el subgrup d'ordre r de $C(K)$ al logaritme discret en un subgrup d'ordre r de $J_C(K)$ d'una corba hiperel·líptica de gènere g definida sobre $\mathbb{F}_q$. Primer es construeix la restricció de Weil $W_{C/K}$ d'escalars de C, que és una varietat n-dimensional sobre $\mathbb{F}_q$. Després intersequem $W_{C/K}$ amb $n-1$ hiperplans per obtenir la corba hiperel·líptica H. Aquest algoritme de reducció es diu atac GHS al logaritme el·líptic. El gènere g de H és 2^{m-1} o $2^{m-1}-1$, on $m = m(b)$.

El problema del logaritme discret al subgrup d'ordre r de $J_H(K)$ es pot resoldre usant l'alogritme rho de Pollard, que té un temps esperat d'execució de $O(g^2 q^{n/2} \log^2 q/M)$ operacions de bits, on M és el número de processadors disponibles per a l'atac paral·lel. Tot i això, com la operació de grup es pot realitzar més ràpidament a $C(K)$ que a $J_H(K)$, és més eficient aplicar l'algoritme rho de Pollard directament a $C(K)$.

L'altra alternativa és usar algoritmes per calcular índexs, aquests algoritmes tenen un temps d'execució subexponencial per corbes de gènere gran. Per tant poden ser més interessants que l'algoritme rho de Pollard.

Per tal que l'atac GHS resolgui el logaritme el·líptic a $C(K)$, el logaritme discret hauria de ser tractable a $J_H(K)$ usant els algoritmes de càlcul d'índex. Es pot veure que $1 \leqslant m \leqslant n$, en general $m \approx n$, d'on $g \approx 2^{n-1}$ i $\#J_H(K) \approx q^{2^{n-1}}$ i l'atac GHS falla. L'atac GHS només tendrà èxit si la m és petita, més o menys $m \approx \log_2 n$, perquè llavors $g \approx n$ $\#J_H(K) \approx q^n$. Analitzant la fórmula per a $m(b)$ es va obtenir el següent resultat.

Teorema 4.2. *Sigui n primer imparell, sigui t l'ordre multiplicatiu de 2 (mod n), i sigui $s = (n-1)/t$. Aleshores:*

1. *$x^n + 1$ factoritza sobre $\mathbb{F}_2$ com $(x+1)f_1 f_2 \dots f_s$ on les f_i són distints polinomis irreductibles de grau t.*
2. *Sigui $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ el mapa de Frobenius $\sigma(x) = x^q$ i $a \in \mathbb{F}_{q^n}$ un element de traça 1. Definim $B = \{b \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q : (\sigma+1)f_i(\sigma)(b) = 0$ per algun $1 \leqslant i \leqslant s\}$. Aleshores per tot $b \in B$, les corbes el·líptiques $y^2 + xy = x^3 + b$ i $y^2 + xy = x^3 + ax^2 + b$ tenen $m(b) = t+1$.*
3. *$\#B = qs(q^t - 1)$.*

4.3.1 Mètode càlcul d'índex

Amb aquest mètode volem resoldre el problema del logaritme hiperel·líptic (HCDLP, *Hyperelliptic Curve Discrete Logarithm Problerm*), que és el següent:

Definició 4.3. *Sigui H una corba hiperel·líptica de gènere g sobre $K = \mathbb{F}_q$, $D_1 \in J_H(K)$, $r = ord(D_1)$ i $D_2 \in < D_1 >$, volem trobar $s \in [0, r-1]$ tal que $D_2 = sD_1$.*

Assumirem que r és primer i que $\#J_H(K) \approx r$.

Primer introduïm dues nocions:

Divisors primers: un divisor en forma reduïda $D = \mathrm{div}(a,b) \in J_H(K)$ es diu primer si a és irreductible sobre K. El conjunt de divisors primers de grau $\leqslant t$ es pot trobar de la següent manera: per cada polinomi mònic irreductible $a \in K[x]$ de grau $\leqslant t$, s'han de trobar les arrels de $y^2 + h(x)y - f(x)$ mòdul $a(x)$. Per cada arrel $b(x)$ (n'hi ha 0, 1 o 2), $\mathrm{div}(a,b)$ és un divisor primer.

Divisors "smooth": un divisor en forma reduïda $D = \operatorname{div}(a, b) \in J_H(K)$ es pot expressar com una suma de divisors primers de la següent manera: primer hem de factoritzar a en polinomis mònics irreductibles sobre K: $a = a_1^{e_1} a_2^{e_2} \cdots a_L^{e_L}$. Sigui $b_i = b \pmod{a_i}$ per $1 \leqslant i \leqslant L$. Aleshores $D = \sum_{i=1}^{L} e_i \operatorname{div}(a_i, b_i)$, D es diu que es *t-smooth* si $\max\{\deg a_i\} \leqslant t$.

Les idees principals de l'algoritme de càlcul d'índex de Enge-Gaundry són les següents:

1. Construïm una base $S = \{P_1, P_1, \ldots, P_w\}$ que consisteix en tots els divisors primers de grau $\leqslant t$ per alguna fita t.

2. Ara es fa una *random-walk* al grup de divisors reduïts, equivalent als divisors de la forma $\alpha D_1 + \beta D_2$ i guardem els divisors *t-smooth* trobats. Cada divisor *t-smooth* guarda una relació $\alpha_i D_1 + \beta_i D_2 \sim R_i = \sum_j e_{ij} P_j$.

3. Quan s'han trobat $w+1$ relacions diferents, es pot trobar amb àlgebra lineal mòdul r una combinació lineal no trivial $\sum_{i=1}^{w+1} \gamma_i (e_{i1}, e_{i2}, \ldots, e_{iw}) = (0, 0, \ldots, 0)$. Per tant $\sum_{i=1}^{w+1} \gamma_i R_i = 0$ i d'aquí tenim $\sum \gamma_i (\alpha_i D_1 + \beta_i D_2) = 0$ i

$$\log_{D_1} D_2 = -\frac{\sum \gamma_i \alpha_i}{\sum \gamma_i \beta_i} \pmod{r}$$

5 Conclusions

Les matemàtiques són d'utilitat en molts àmbits de la nostra vida i societat. Com es pot apreciar en aquest treball, on es pot veure que les usam per exemple per firmar documents a distància o comunicar-nos amb la seguretat que ens comunicam amb el destinatari que volem i no amb interlocutors no desitjats.

La criptografia s'ha usat des de fa molts anys sobretot per l'ús militar. És només més recentment que l'hem aplicada per altres fins i això és degut a la globalització de la nostra societat i a l'increment exponencial que estan tenint les noves tecnologies.

No obstant això, veiem que també hi ha la branca de la criptografia que consisteix en rompre aquests protocols, per la finalitat que és òbvia parlant des del punt de vista militar i per motius poc desitjats també des del punt de vista de les firmes electròniques i els pagaments en línia. Tot i això, de moment la criptografia evoluciona suficientment ràpid com perquè aquests mètodes que hi ha per trencar els sistemes es puguin evitar.

Per acabar, dir que m'ha resultat molt interessant veure com es pot aplicar una teoria que em resultava tan abstracte com pot ser la teoria de grups i teoria de cossos de l'àlgebra a un camp que té una utilitat tant del dia a dia com pot ser la criptografia.

Referències

[1] Silverman, J.H.; Tate, J.: *Rational points on elliptic curves,* 2a edició, Springer, 2015.

[2] Silverman, J.H.: *The arithmetic of elliptic curves,* 2a edició, Springer, 2009.

[3] Caballero, P.: *Introducción a la criptografía,* Rama, 1996.

[4] Gayoso, V.; Hernández, L.; Martín, A.: *Criptografía con curvas elípticas,* CSIC, 2018.

[5] Juher, D.: *Introducció a la criptografia,* Universitat de Girona, 2000.

[6] Schmitt, S.; Zimmer, H.G.: *Elliptic curves: a computational approach,* De Gruyter, 2008.

[7] Menezes, A.; Vanstone, S.: *Reducing elliptic curve logarithms to logarithms in a finite field,* IEEE Transactions on Information Theory, Vol. 39, pàg 1639-1646, 1993.

[8] Menezes, A.; Jacobson, M.: *Solving elliptic curve discrete logarithm problems using Weil descent,* Journal of the Ramanujan Mathematical Society, Vol. 16, pàg 231-260, 2001.