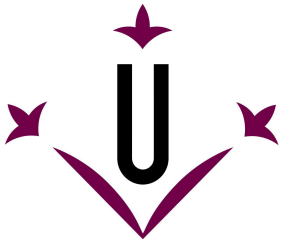
Universitat de Lleida

Volcans d'Isogènies de Corbes El·líptiques: aplicacions Criptogràfiques en Targetes Intel·ligents

Rosana Tomàs Cuñat



Universitat de Lleida

Escola Politècnica Superior

Departament de Matemàtica

Volcans d'Isogènies de Corbes El·líptiques: aplicacions Criptogràfiques en Targetes Intel·ligents

Memòria presentada per optar al grau de
doctora per la Universitat de Lleida
per

Rosana Tomàs Cuñat

Dirigida per

Josep M. Miret Biosca
Universitat de Lleida

Daniel Sadornil Renedo
Universidad de Cantabria

Programa de doctorat en Enginyeria

Lleida, març de 2011

A totes aquelles persones que m'han deixat prematurament
i hauria volgut que fossin amb mi en aquests moments.

"- Durant quant de temps vols que siguin secrets aquells missatges? -li va preguntar Randy en l'últim missatge abans d'abandonar Sant Francisco-. Cinc anys? Deu anys? Vint-i-cinc anys?

[...]

- Vull que segueixin sent secrets mentre els homes siguin capaços del mal. "

Neal Stephenson, *Kriptonomicon*

"La intel·ligència consisteix no només en el coneixement, sinó també en la destresa d'aplicar els coneixements en la pràctica."

Aristòtil

"D'entre totes les grandeses de les matemàtiques, la demostració és la que, evidentment, premia l'enginy dels investigadors.

[...]

Cap investigació humana pot dir-se ciència si no pot demostrar-se matemàticament."

Leonardo da Vinci, *"Tractat de la pintura"*

Resum

D. Kohel, i més endavant M. Fouquet i F. Morain, van estudiar l'estructura dels volcans de ℓ–isogènies d'una corba el·líptica sobre un cos finit, sent ℓ un primer qualsevol, i van donar algorismes per anar des del terra fins al cràter del volcà. Seguint aquests treballs, en aquesta tesi estudiem noves propietats dels volcans de ℓ–isogènies. Així, caracteritzem l'altura d'un volcà de ℓ–isogènies d'una corba el·líptica sobre un cos finit $\mathbb{F}_q$ a partir de les valoracions ℓ–àdiques del cardinal de la corba i de $q-1$, i analitzem detalladament el cas $\ell = 3$. D'altra banda, per a volcans anomenats regulars donem, segons l'estructura del subgrup de ℓ–Sylow de la corba, el nivell on està ubicada dins del volcà.

Utilitzant aquest estudi, hem dissenyat un algorisme que genera, a partir d'una corba donada, un llistat de corbes isògenes a la corba inicial de forma ordenada segons el grau ℓ de la isogènia. Amb aquest objectiu, introduïm el concepte ℓ–cordillera, estructura formada per tots els ℓ–volcans sobre un mateix cos, per a un primer ℓ. Així, per recórrer tota una ℓ–cordillera saltarem d'un ℓ–volcà a un altre considerant isogènies de grau un primer ℓ', diferent de ℓ.

En un vessant més pràctic, hem treballat en l'ús de la criptografia el·líptica en dispositius com les targetes intel·ligents. Més concretament, ens hem centrat en els atacs que pateixen aquests dispositius, com els *Zero-Value Points* (ZVP), presentats per L. Goubin i ampliats per T. Akishita i T. Takagi. En aquesta tesi, proposem una contramesura a aquests atacs, seguint la línia de la proposada per N. Smart. La contramesura està basada en l'ús d'una variant de l'algorisme esmentat anteriorment que busca corbes resistents recorrent les ℓ–cordilleres de la corba inicial.

Finalment, estudiem el comportament d'aquests atacs considerant corbes el·líptiques donades en el model d'Edwards. A diferència de les corbes el·líptiques expressades mitjançant l'equació de Weierstraß, les corbes d'Edwards no són vulnerables als atacs ZVP.

Resumen

D. Kohel, y más adelante M. Fouquet y F. Morain, estudiaron la estructura de los volcanes de ℓ–isogenias de una curva elíptica sobre un cuerpo finito, siendo ℓ un primo cualquiera, y propusieron algoritmos para ir desde el suelo hasta el cráter del volcán. Siguiendo estos trabajos, en esta tesis, estudiamos propiedades de los volcanes de ℓ–isogenias. Así, caracterizamos la altura de un volcán de ℓ–isogenias de una curva elíptica sobre un cuerpo finito $\mathbb{F}_q$ a partir de las valoraciones ℓ–ádicas del cardinal de la curva y de $q-1$, analizando en detalle el caso $\ell = 3$. Por otro lado, para los volcanes llamados regulares damos, según la estructura del subgrupo de ℓ–Sylow de la curva, el nivel donde está ubicada dentro del volcán.

Utilizando este estudio, hemos diseñado un algoritmo que genera, a partir de una curva dada, un listado de curvas isógenas a la curva inicial de forma ordenada según el grado ℓ de la isogenia. Con este objetivo, introducimos el concepto de ℓ–cordillera, estructura formada por todos los ℓ–volcanes sobre un mismo cuerpo, para un primo ℓ dado. Así, para recorrer toda una ℓ–cordillera, saltaremos de un ℓ–volcán a otro, considerando isogenias de grado un primo ℓ', diferente de ℓ.

En una vertiente más práctica, hemos trabajado en el uso de la criptografía elíptica en dispositivos como las tarjetas inteligentes. Más concretamente, nos hemos centrado en los ataques que sufren estos dispositivos, como los ataques *Zero-Value Points* (ZVP), presentados por L. Goubin y ampliados por T. Akishita y T. Takagi. En esta tesis, proponemos una contramedida a estos ataques, siguiendo la línea de la propuesta por N. Smart. La contramedida está basada en el uso de una variante del algoritmo mencionado anteriormente que busca curvas resistentes recorriendo las ℓ–cordilleras de la curva inicial.

Finalmente, estudiamos el comportamiento de estos ataques considerando curvas elípticas dadas en el modelo de Edwards. A diferencia de las curvas elípticas expresadas mediante la ecuación de Weierstraß, las curvas de Edwards no son vulnerables a los ataques ZVP.

Abstract

D. Kohel and later M. Fouquet and F. Morain studied the structure of volcanoes of ℓ–isogenies of an elliptic curve over a finite field, being ℓ any prime number. They also proposed algorithms to go from the floor to the crater of a volcano. Following these works, in this thesis we studied some properties of the ℓ–isogeny volcanoes. Thus, we characterized the height of an ℓ–isogeny volcano of an elliptic curve over a finite field $\mathbb{F}_q$ from the ℓ–adic valuations of the cardinality of the curve and $q-1$, analyzing the case $\ell = 3$ in detail. On the other hand, for the so-called regular volcanoes, we give the level where a curve is located inside the volcano, according to the structure of its ℓ–Sylow subgroup.

From this study, we have designed an algorithm that generates, from a given curve, a list of curves isogenous to the initial one, in an organized manner, according to the degree ℓ of the isogeny. With this objective, we introduce the concept of ℓ–cordillera, a structure consisting of all the ℓ–volcanoes over a field, for a given prime ℓ. Thus, in order to explore a whole ℓ–cordillera, we jump from an ℓ–volcano to another, considering isogenies of degree a prime ℓ' different from ℓ.

In a more practical aspect, we worked on the use of elliptic curve cryptography on devices such as smart cards. More specifically, we focused on the attacks suffered by these devices, such as the Zero-Value Point (ZVP) attacks, which were presented by L. Goubin and extended by T. Akishita and T. Takagi. In this thesis, we propose a countermeasure to these attacks, along the lines of the one proposed by N. Smart. The countermeasure is based on the use of a variant of the algorithm mentioned above, that searches for strong curves exploring the ℓ–cordilleras of the initial curve.

Finally, we studied the behavior of these attacks considering elliptic curves given in the Edwards model. Unlike elliptic curves expressed by the Weierstraß equation, Edwards curves are not vulnerable to ZVP attacks.

Agraïments

Als meus directors de tesi, Josep M. Miret i Daniel Sadornil, per la seva generositat en brindar-me l'oportunitat de comptar amb la seva capacitat i experiència científica en un marc de confiança, afecte i amistat, fonamentals per a la concreció d'aquest treball i. sobretot, per la seva permanent disposició i ajuda desinteressada.

A Francesc Giné, Ramiro Moreno, Jordi Pujolàs, Francesc Sebé, Francesc Solsona, Concepció Roig, Magda Valls i a la resta de membres del seminari de cripto-paral·lelisme, pels seus valuosos suggeriments i per les seves encertades aportacions durant el desenvolupament d'aquest treball.

A Juan Tena per la seva generositat científica i les seves valuoses crítiques en discutir els resultats d'aquest treball.

Als projectistes que han anat ajudant a implementar aquestes idees, molt especialment a Javier Valera i a Rubén Arias.

A tots els companys de l'EPS i als del Departament de Matemàtica per la seva calidesa i pel seu continu i afectuós alè.

Al meu espòs, Santi, pel seu afecte, paciència, comprensió i constant estímul.

Als meus pares, germà i família per brindar-me una llar càlida, ensenyar-me que la perseverança i l'esforç són el camí per assolir objectius, acompanyar-me en tots els moments importants de la meva vida i contagiar-me la seva fortalesa d'esperit, per ensenyar-me més que ningú les coses veritablement importants i fer-me créixer com a persona.

A tots els meus amics per tots els moments memorables, divertits i agradables que m'han donat, també per les seves rialles i el seu suport a cada moment, especialment al Rubén i al Ioannis, pel seu suport incondicional que m'ofereixen sempre.

A tots els professors que han sabut transmetre'm el coneixement necessari i donar-me les eines necessàries per arribar a aquesta meta.

I a totes aquelles persones que d'una manera o d'una altra han col·laborat o participat en l'elaboració d'aquesta tesi faig extensiu el meu més sincer agraïment.

Índex

Índex de Figures

Índex de Taules

Índex d'Algorismes

Capítol 1

Introducció

Aquesta tesi s'emmarca en l'àmbit de la criptografia amb corbes el·líptiques i el seu ús en targetes intel·ligents. Es donen solucions per millorar l'eficiència d'aquests dispositius en les seves funcions criptogràfiques i es proposen nous mètodes per evitar atacs en aquests tipus de dispositius.

1.1 Contextualització

En plena era de les telecomunicacions, cada cop són més els dispositius que incorporen microxips per millorar el seu funcionament per donar més usos de l'aparell a l'usuari.

Un exemple d'aquests dispositius són les targetes intel·ligents, que són una evolució de les targetes amb banda magnètica, utilitzades des dels vuitanta per fer diverses transaccions bancàries o emmagatzemar, de forma totalment insegura, dades del seu propietari. Aquesta mancança de seguretat va fer que hi hagués una evolució cap a les targetes intel·ligents, targetes que incorporen un microxip que proporciona seguretat a les dades que emmagatzema.

Amb aquesta nova generació de targetes se n'han multiplicat els usos, tant els que es donen en el sector bancari, com els que s'han incorporat en altres sectors com el sanitari o el de l'administració amb el DNI electrònic.

El problema que ens trobem, amb aquest gran ventall d'usos d'aquests dispositius, és que cada cop és més important donar una forta seguretat a les dades emmagatzemades, proporcionant, així, a l'usuari la tranquil·litat i la

confiança que la seva privacitat no es veurà alterada. L'opció per mantenir la privacitat i la seguretat de les dades recau en l'ús de la criptografia.

A la pràctica ens trobem amb dos tipus de criptografia. D'una banda, la criptografia simètrica, basada en una clau coneguda únicament per l'emissor i el receptor, que s'utilitza indistintament per xifrar i desxifrar el missatge. D'altra banda, la criptografia asimètrica, que utilitza un parell de claus, una de pública coneguda per tothom i una de privada que només coneix el receptor del missatge. En aquest cas, l'emissor xifra el missatge amb la clau pública i el receptor, amb la clau privada, desxifra de forma ràpida el missatge rebut. Amb aquest escenari, qualsevol pot xifrar un missatge, però solament el receptor, que és l'únic que coneix la clau privada, podrà desxifrar el missatge. En la criptografia simètrica, com que tant l'emissor com el receptor coneixen la clau, ambdos poden accedir a la informació. Cal, llavors, distribuir totes les claus possibles per a comunicacions entre totes les parelles emissor-receptor. Aquest últim fet provoca que el nombre de claus sigui massa gran en comparació amb el nombre d'usuaris.

Aquest últim tipus de criptosistemes basen la seva seguretat en l'enorme dificultat que comporta la resolució d'un problema matemàtic que, per la seva magnitud, és gairebé impossible de resoldre a la pràctica, tot i que coneixent alguna dada més, aquest mateix problema redueix considerablement el seu nivell de dificultat computacional.

La majoria dels criptosistemes de clau pública utilitzen, principalment, el problema de la factorització de nombres enters (IFP) i el del logaritme discret (DLP). El problema de la factorització d'enters utilitza el fet que és relativament fàcil realitzar el càlcul de potències o productes de nombres considerablement grans, si bé els processos inversos resulten molt costosos. Per tant, la seguretat d'aquests criptosistemes es troba en el fet que no existeix un mètode eficient per factoritzar nombres enters grans. D'entre els criptosistemes que es troben en aquest grup destaquem el criptosistema RSA [RSA78] i el Rabin-Williams [Rab79, Wil80]. Per la seva banda, el logaritme discret sobre un grup cíclic finit (G^*) basa la seva seguretat en el fet que tampoc hi ha cap mètode eficient per resoldre l'equació $y = g^x$, on g és un generador del grup i y, un element del grup. Els criptosistemes més usats d'aquest tipus són l'intercanvi

de claus Diffie-Hellman [DH76] i el criptosistema ElGamal [EG85].

El principal problema que comporten aquests criptosistemes és que en els últims anys han anat apareixent mètodes que resolen aquests problemes matemàtics en temps subexponencials, com és el cas de l'algorisme Index Calculus per al DLP sobre el grup multiplicatiu d'un cos finit [SS98]. Així mateix, l'evolució i el desenvolupament dels processadors fan possible realitzar els càlculs necessaris per poder desxifrar un missatge, sense conèixer la clau, de forma més ràpida. És a dir, el que fa un parell de dècades era costós, en un futur podria ser possible. Una solució per continuar treballant amb aquest tipus de criptosistemes sense tenir problemes de seguretat és anar augmentant la grandària de la clau, i augmentar també el temps de xifrat i el cost computacional de l'algorisme.

Una altra solució més interessant és la proposada per N. Koblitz [Kob87] i V. Miller [Mil86] en els anys 80, que van introduir l'ús de les corbes el·líptiques amb fins criptogràfics, i van basar la seva seguretat en el problema del logaritme discret sobre el grup de punts d'una corba el·líptica sobre un cos finit. Fins ara no s'ha trobat cap atac similar a l'Index Calculus per a corbes el·líptiques, de manera que utilitzant corbes el·líptiques es necessitaran claus de menor grandària per garantir la mateixa seguretat, cosa que fa que aquests criptosistemes siguin més adequats per a l'ús en dispositius amb recursos molt limitats.

Així, tot i que els xifratges de clau pública ofereixen la seguretat necessària per emmagatzemar dades, en el cas de les targetes intel·ligents, el microxip que porten incrustat té greus mancances de potència, així com de memòria, i els criptosistemes convencionals, com el RSA, per oferir un bon nivell de seguretat, demanen una mida de claus massa grans per ser guardades en aquests microxips. Per tant, la solució es troba buscant altres criptosistemes en què donar una forta seguretat sigui més "econòmic", sobretot pel que fa a memòria, i això passa per l'ús de criptosistemes basats en corbes el·líptiques.

A part del problema amb les restriccions que comporta l'ús de targetes intel·ligents tenim, també, els que comporta l'escenari on es treballa. En l'entorn on s'utilitzen les targetes intel·ligents ens trobem altres tipus de perills, altres atacs criptogràfics que provenen de fuites del mateix xip que poden donar informació, i trencar el criptosistema de la targeta. Aquesta informació

es coneix com informació *Side-Channel* i els atacs que fan ús d'aquest tipus d'informació s'anomenen atacs *Side-Channel*.

La informació *Side-Channel* que obté un atacant es pot deure a diverses fonts: pot obtenir-se informació sabent la potència consumida en cada moment, el temps que tarda en fer una acció o, fins i tot, analitzant diverses traces d'aquest tipus d'informació per deduir què fa la targeta en cada moment i quins nombres utilitza.

Depenent del tipus d'informació *Side-Channel* que s'utilitza podem parlar de diferents atacs: atacs de potència de consum [CJRR03, MOP06], *Simple* i *Differential Power Analysis* [KJJ99], atacs de temps [Sch00] i atacs electromagnètics [QS01] que alhora es poden dividir en *Simple* i *Differential Electromagnetic Attacks* (SEMA i DEMA) (vegis [CF05]).

Una solució per millorar l'eficiència en els criptosistemes implementats en les targetes intel·ligents és l'ús de criptografia el·líptica en comptes de la convencional. Això proporciona la seguretat que es demana en l'actualitat, i fa factible que s'emmagatzemin les claus dins la targeta sense gaires complicacions ni impediments. Però dins de la criptografia el·líptica tenim un handicap, i és que no totes les corbes el·líptiques definides sobre un cos finit proporcionen el mateix nivell de seguretat; en altres paraules, no totes les corbes d'un cos són segures. Això es deual fet que la seguretat d'una corba el·líptica ve donada pel seu cardinal, ja que per evitar l'atac de Pohlig-Hellman [PH78] cal que la factorització del cardinal tingui un factor primer gran de la mida del cos.

Ara bé, si dos corbes, definides sobre un mateix cos, tenen el mateix cardinal, se sap que tenen presumiblement la mateixa seguretat [JMV05] i [BSS05] (Chap. VIII, Weil descent attacks). Però el fet de calcular el cardinal d'una corba és una operació costosa, per tant, no és factible que cada cop que necessitem una corba el·líptica segura en busquem una a l'atzar i calculem el seu cardinal. Una opció més econòmica seria trobar corbes isògenes. A més, hi ha atacs del tipus Side-Channel que demanen que les corbes compleixin una sèrie de condicions per no ser atacades i, encara que dos corbes tinguin el mateix cardinal, podem dir que una és més segura que l'altra envers aquest tipus d'atacs.

A partir d'una corba el·líptica podem calcular corbes isògenes amb isogènies de graus petits diferents i, per tant, corbes que tenen el mateix cardinal que la corba inicial. De fet, el teorema de Tate [Tat66] assegura que totes les corbes el·líptiques sobre un cos finit amb el mateix cardinal es poden construir mitjançant isogènies. Els càlculs necessaris per obtenir una corba isògena són ràpids i, normalment, una corba té moltes isògenes, fet que fa que tinguem un bon registre de corbes segures a partir d'una d'inicial que també ho sigui.

Per obtenir corbes isògenes a partir d'una de donada hi ha diverses maneres de fer-ho: podem calcular-les mitjançant les fórmules de Vélu [Vél71], que fa ús dels polinomis de divisió, o calcular-les utilitzant polinomis modulars [BSS99].

A fi de calcular l'anell d'endomorfismes d'una corba el·líptica sobre un cos finit, D. Kohel [Koh96] va adonar-se que les isogènies de grau ℓ entre corbes el·líptiques es podien mapejar en un graf anomenat, per la seva peculiar forma, volcà de ℓ-isògenes o ℓ-volcà. M. Fouquet i F. Morain [FM02], seguint amb el treball començat per D. Kohel, donen un algorisme per trobar l'altura d'aquests grafs d'isogènies racionals de grau ℓ mitjançant polinomis modulars. J. Miret, R. Moreno, D. Sadornil, J. Tena i M. Valls donen en [MMS$^+$06], per al cas $\ell = 2$, un algorisme per trobar l'altura del volcà i per recórrer el cràter usant les fórmules de Vélu per al càlcul de les equacions de les corbes. Així mateix, per aquest cas $\ell = 2$ proven la relació existent entre el nivell del ℓ-volcà on està situada la corba i l'estructura del seu subgrup de ℓ-Sylow. Més recentment, G. Bisson i A. Sutherland [BS10] dissenyen algorismes per determinar l'anell d'endomorfismes d'una corba el·líptica a partir de la relació anterior. I S. Ionica i A. Joux [IJ10] caracteritzen el caràcter ascendent, horitzontal o descendent d'una ℓ-isogènia a partir d'un *pairing* definit en el subgrup de ℓ-Sylow de la corba. Cal dir que J. Miret, R. Moreno, A. Rio i M. Valls donen en [MMRV05, MMRV09] algorismes eficients per determinar el subgrup de ℓ-Sylow d'una corba el·líptica.

Tornant a l'entorn de la criptografia el·líptica en targetes intel·ligents, existeixen diverses contramesures als SCA utilitzats en la criptografia de corbes el·líptiques [CF05], com ara fer sempre en cada pas la suma i el doblat del punt, aleatoritzar les coordenades (projectives, Jacobianes,...), i agafar un escalar aleatori k, entre altres. Així com veiem que mitjançant aquest tipus

de criptografia ens quedava solucionat el problema de les mancances pròpies d'aquests aparells, no ens solucionen, a primera vista, els atacs *Side-Channel*.

D'altra banda, L. Goubin [Gou03] troba un altre atac que es denomina *Zero-Value Point* (ZVP) que sols funciona per a criptografia el·líptica. Aquest atac es basa en el fet que els punts amb alguna coordenada nul·la permeten obtenir certa informació de la clau. N. Smart [Sma90] hi troba una solució mitjançant l'ús d'isogènies. T. Akishita i T. Takagi [AT03, AT04] amplien l'atac de Goubin i busquen solucions usant corbes isògenes com N. Smart.

Cal dir, finalment, que buscant mètodes més eficients i segurs per a la criptografia amb corbes el·líptiques en targetes intel·ligents recentment s'ha proposat incorporar un altre model de corbes el·líptiques, les corbes d'Edwards [Edw07], que resulten més eficients en cost, com s'ha vist en els treballs de D. Bernstein i T. Lange [BL07, BL09].

1.2 Objectius

Els mètodes proposats per N. Smart i T. Akishita i T. Takagi [Sma90, AT03, AT04] per evitar atacs ZVP no són del tot eficients quan el grau de les isogènies es fa gran. En aquest cas, perden molta de l'eficàcia que ens donava l'ús d'aquesta criptografia en aquests dispositius. Per tant, es presenten dos problemes clars. D'una part, trobar corbes bones criptogràficament i, en segon lloc, evitar els atacs ZVP.

Per aquest motiu, en aquesta tesi es pretén obtenir un gran ventall de corbes el·líptiques utilitzant la construcció de ℓ-volcans per intentar, alhora, trobar un mètode més eficient per obtenir corbes resistents als atacs ZVP utilitzant aquesta construcció de volcans.

Seguint aquest camí, els objectius que s'han pretès aconseguir amb aquesta tesi se centren en dos aspectes.

El primer, de caràcter més analista, ha estat el fet de buscar més informació de les corbes el·líptiques mitjançant els volcans d'isogènies, que, com ja s'ha dit, ens agrupen corbes el·líptiques definides en un mateix cos i que comparteixen també el cardinal. En altres paraules, gràcies a la construcció dels volcans de corbes el·líptiques podem obtenir un registre ampli de corbes el·líptiques,

presumiblement amb el mateix nivell de seguretat.

El segon aspecte té un caràcter més pràctic, i és el fet d'utilitzar els resultats obtinguts per trobar corbes segures a atacs específics de certs entorns, com els que ens trobem en les targetes intel·ligents. En aquests, no sols es necessita una corba el·líptica que compleixi les restriccions de seguretat que el protocol criptogràfic exigeix, sinó que també hi ha altres restriccions que vénen donades perquè sigui segura envers els atacs que poden sorgir per les condicions de l'entorn on s'utilitzen aquests dispositius.

1.3 Contribucions

El caràcter multidisciplinar d'aquesta tesi ha permès enfocar el treball d'investigació des dos punts de vista, un de més enfocat a resultats teòrics i un altre de més centrat en el seu ús pràctic d'aquests.

Pel que fa al primer objectiu que ens vam proposar, en l'article *Volcanoes of ℓ-isogenies of elliptic curves over finite fields: the case $\ell = 3$* [MST+07] s'ha continuat l'estudi de les propietats dels volcans d'isogènies de corbes el·líptiques iniciat en les tesis de D. Kohel [Koh96], M. Fouquet [Fou01] i D. Sadornil [Sad04]. Així, es determina el nivell del volcà de ℓ-isogènies on es troba la corba en termes del subgrup de ℓ-Sylow de la corba. A més hem dissenyat un algorisme que, donada un corba el·líptica $E/\mathbb{F}_q$ i un primer ℓ, retorna l'altura h i la mida del cràter c del ℓ-volcà on pertany aquesta corba, així com el nivell k on es troba aquesta corba inicial. I per al cas $\ell = 3$, es fa un estudi de tots els 3-volcans sobre un cos finit $\mathbb{F}_p$ per a diferents primers petits p.

Seguint amb aquest primer objectiu, també es volia tenir un ampli ventall de corbes el·líptiques sobre un cos finit amb el mateix cardinal. Això s'ha plantejat a l'article *Exploiting Isogeny Cordillera Structure to Obtain Cryptographically Good Elliptic Curves* [MST+08], on es dóna un procediment per obtenir totes les classes d'isomorfia de corbes el·líptiques sobre un cos finit que tenen un mateix cardinal. Per fer-ho s'ha definit el terme *cordillera*. Aquest terme fa referència, per a un primer ℓ, al graf de tots els volcans de ℓ-isògenes de corbes definits sobre un mateix cos finit i amb un mateix cardinal. Per aconseguir-ho, s'ha ideat un algorisme que, a partir d'una corba donada, ens

generi les corbes de la seva cordillera sense necessitat d'anar calculant-ne els cardinals.

Pel que fa a l'aspecte pràctic que també s'ha volgut abarcar, ens vam centrar a voler millorar, utilitzant criptografia amb corbes el·líptiques, les aplicacions de dispositius amb fortes restriccions computacionals i de memòria. Més concretament ens vam centrar en les targetes intel·ligents, on l'ús de la criptografia el·líptica limitaria menys aquestes restriccions. Malauradament, en aquests dispositius apareixen uns altres tipus d'atacs que no són considerats en la criptografia més estàndard.

Així, en *On Avoiding ZVP-Attacks Using Isogeny Volcanoes* [MST+09], s'ha proposat l'ús de l'algorisme presentat en [MST+08] per obtenir corbes criptogràficament segures que alhora fossin resistents als atacs ZVP. Això es fa mitjançant una cerca exhaustiva d'una corba segura a partir de la construcció de cordilleres de volcans. Aquesta cerca d'una corba resistent a aquests atacs és més eficient que els mètodes existents proposats per N. Smart, T. Akishita i T. Takagi [Sma90, AT03, AT04]. A la vegada, dóna la possibilitat de buscar corbes que, a més, siguin resistents a altres condicions que quedaven per tractar amb els mètodes inicials.

De la mateixa manera, en *Curvas de Edwards y ataques basados en puntos de valor cero* [MST+10], s'introdueix com a contramesura dels atacs ZVP l'ús d'un altre model de corba el·líptica anomenades corbes d'Edwards. Aquestes són totalment resistents als atacs ZVP coneguts, i fan que no quedin condicions sense tractar com en les solucions anteriors [Sma90, AT03, AT04, MST+09].

Seguint en aquesta línia, i com a possible treball futur, es podria passar a un altre model de corbes anomenades *twist d'Edwards* [BMB+09, DS08], ja que aquestes amplien el nombre de corbes el·líptiques en forma de Weierstraß equivalents entre si.

Un altre possible treball futur seria intentar paral·lelitzar els algorismes donats, ja que es podria, mitjançant un clúster, obtenir un registre molt més ampli de corbes el·líptiques amb el mateix cardinal i en molt menys temps.

1.4 Estructura

Aquesta tesi consta de sis capítols dividits de la següent manera:

- Capítol 2 - *Corbes el·líptiques:* Comencem aquesta memòria de tesi amb un capítol dedicat a les nocions preliminars de corbes el·líptiques i càlcul d'isogènies necessàries per realitzar les contribucions que es presenten. També hi introduïm les notacions i eines necessàries per al desenvolupament d'aquest treball.

- Capítol 3 - *Targetes intel·ligents i criptografia el·líptica:* En aquest capítol es presenten l'evolució històrica i el funcionament de les targetes intel·ligents. Així mateix, es mostren els avantatges que aquests dispositius ofereixen, tant en les seves aplicacions com en l'emmagatzematge d'informació necessària, que, a més, he de ser segura. Per aquest motiu, les targetes intel·ligents tenen implementada una sèrie de protocols criptogràfics i de seguretat. No obstant això, aquests protocols són molts cops insuficients davant dels diferents atacs que han anat sorgint a mesura que va passant el temps.

- Capítol 4 - *Volcans d'isogènies de corbes el·líptiques:* Seguint en la línia del treball realitzat per D. Sadornil en la seva tesis [Sad04], en aquest capítol es dóna una forma de caracteritzar l'altura d'un ℓ-volcà sobre un cos $\mathbb{F}_p$ a partir de les valoracions ℓ-àdiques de $q-1$ i del cardinal de les corbes. També es presenta un algorisme que no solament ens dóna l'altura del volcà, sinó el nivell en què es troba una determinada corba dins d'aquest volcà, així com la mida del seu cràter. Aquests paràmetres són útils per poder estudiar els volcans i poder fer una classificació segons la seva morfologia.

- Capítol 5 - *Cordilleres de volcans:* Aquí es presenta un procediment per obtenir un ampli registre de corbes utilitzant el concepte de cordillera de volcans de corbes el·líptiques. Més concretament es dóna un algorisme que obté tots els volcans de ℓ-isogènies que formen una cordillera, obtenint així totes les corbes sobre un cos finit que comparteixen cardinal.

- Capítol 6 - *Corbes resistents als atacs ZVP:* En aquest capítol estudiem l'atac ZVP, un atac enfocat a targetes intel·ligents i centrat en criptografia sobre corbes el·líptiques. Perquè siguin factibles aquests atacs, les corbes el·líptiques usades en els criptosistemes han de complir un seguit de condicions. Per fer-ho, hem dissenyat un nou algorisme que ens dóna, de forma més ràpida i eficient, que amb els mètodes existents, corbes el·líptiques segures enfront aquests atacs específics per aconseguir que la targeta intel·ligent sigui més resistent. El fet que el procediment sigui més eficient ens permet tractar altres condicions per evitar els atacs ZVP, condicions mencionades però no tractades per T. Akishita i T. Takagi [AT03, AT04]. Finalment, hem estudiat aquestes condicions usant corbes d'Edwards. Aquestes corbes resulten resistents a totes les condicions sobre atacs ZVP que fan vulnerables les corbes el·líptiques donades en forma de Weierstraß.

Capítol 2

Corbes el·líptiques

L'ús de les corbes el·líptiques en criptografia va ser una idea proposada, alhora, per V . Miller [Mil86] i N. Koblitz [Kob87] la segona meitat dels vuitanta. L'ús de la corbes el·líptiques com a tècnica criptogràfica té cada vegada més acceptació, ja que presenta diversos avantatges respecte a criptosistemes com el RSA [RSA78] o ElGamal multiplicatiu [EG85]. La principal és que es pot arribar a una seguretat equiparable a la d'aquests criptosistemes usant claus de grandària molt menor.

Abans d'endinsar-nos en l'estudi de les corbes el·líptiques dins de la criptografia s'introduiran alguns conceptes bàsics sobre aquest tipus de corbes cúbiques: les seves característiques i les seves propietats, així com alguns resultats.

2.1 Definicions bàsiques

Una corba el·líptica E sobre un cos $\mathbb{K}$ ve definida per una equació del tipus següent:

$$E/\mathbb{K} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

amb $a_i \in \mathbb{K}$, anomenada *equació de Weierstraß*. Aquesta equació ha de satisfer que el seu discriminant, Δ, sigui no nul per de manera que la corba no tingui

punts singulars. L'expressió del discriminant ve donada per:

$$\Delta = 9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2, \tag{2.2}$$

en què els b_i vénen definits en funció dels valors a_i de la forma següent:

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,\ b_8 = (b_2b_6 - b_4^2)/4.$$

Sempre que el cos $\mathbb{K}$ no tingui característica 2 ni 3, es pot fer un canvi de variable que transforma l'equació de Weierstraß (2.1) en el que es coneix com l'equació reduïda de Weierstraß, que queda de la manera següent:

$$E/\mathbb{K} : y^2 = x^3 + ax + b, \tag{2.3}$$

amb a, $b \in \mathbb{K}$ i, on ara, el seu discriminant ve donat per:

$$\Delta = -16(4a^3 + 27b^2).$$

Juntament amb el discriminant d'una corba, se'n pot definir un altre paràmetre, el *j–invariant* de la corba. Aquest paràmetre ve donat, si la corba està definida mitjançant la forma de Weierstraß, per l'expressió:

$$j_E = \frac{b_2^2 - 24b_4}{\Delta}. \tag{2.4}$$

L'equació d'una corba el·líptica, així com els punts que satisfan aquesta equació, es pot representar en diferents sistemes de coordenades. Es poden representar mitjançant coordenades en el pla afí, $\mathbb{A}^2(\mathbb{K})$, com hem vist fins ara, o mitjançant coordenades en el pla projectiu, $\mathbb{P}^2(\mathbb{K})$. En l'espai projectiu, els punts vénen donats amb la forma $(X : Y : Z)$, a diferència de l'espai afí, on són de la forma (x, y), entenent que les tres components X, Y i Z no poden ser nul·les a la vegada i que:

$$(X : Y : Z) \sim (X' : Y' : Z') \Leftrightarrow \exists \lambda \in \mathbb{K}^*$$

de manera que

$$X = \lambda X',\ Y = \lambda Y',\ Z = \lambda Z'.$$

Així, podem representar l'equació de Weierstraß en coordenades projectives reemplaçant la coordenada x per X/Z i y per Y/Z. Fent aquest canvi, l'equació (2.1) en el pla projectiu s'expressarà de la manera següent:

$$E/\mathbb{K} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \qquad (2.5)$$

Aquesta és la forma més comuna de treballar amb un sistema de coordenades projectives, però no és l'única representació possible de punts en l'espai projectiu. La forma general ve donada per dos paràmetres constants, c i d, que ens determinen en quina representació treballem. En aquesta forma general, podem passar de coordenades afins a qualsevol sistema de projectives ponderades de la forma següent:

$$x \longmapsto \frac{X}{Z^c} \quad \text{i} \quad y \longmapsto \frac{Y}{Z^d}.$$

En cas anterior, considerat l'habitual quan es parla de coordenades projectives, aquests paràmetres prenen valor $c = 1$ i $d = 1$, però en l'àmbit criptogràfic no és l'única representació que s'utilitza, també es parla de les coordenades jacobianes. En aquestes coordenades projectives, els paràmetres prenen com a valor $c = 2$ i $d = 3$. En el sistema jacobià, l'equació (2.1) queda de la forma:

$$E/\mathbb{K} : Y^2 + a_1XYZ + a_3YZ^3 = X^3 + a_2X^2Z^2 + a_4XZ^4 + a_6Z^6. \qquad (2.6)$$

Aquestes corbes, en l'espai projectiu, sempre passen pel punt $(0 : 1 : 0)$, que anomenarem punt de l'infinit i denotarem per $\mathcal{O}_E$.

Denotarem per $E(\mathbb{K})$ el conjunt de punts $(X : Y : Z)$ que satisfan l'equació de la corba $E/\mathbb{K}$. En cas d'un sistema de coordenades afí, hem d'afegir-hi el punt $\mathcal{O}_E$.

Es diu que dos corbes $E/\mathbb{K}$ i $E'/\mathbb{K}$ són *isomorfes* si hi existeix un isomorfisme, és a dir, una aplicació bijectiva:

$$\begin{aligned}(u,r,s,t) : E &\longrightarrow E' \\ (x,y) &\longmapsto (x',y')\end{aligned}$$

donada per la transformació afí:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u^2 & 0 \\ su^2 & u^3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix},$$

amb $u \in \mathbb{K}^*$ i r, s, $t \in \mathbb{K}$.

Es pot veure que dos corbes E i E' definides sobre el mateix cos $\mathbb{K}$ mitjançant una equació (2.3):

$$\begin{aligned}E/\mathbb{K} : y^2 &= x^3 + ax + b \\ E'/\mathbb{K} : y^2 &= x^3 + a'x + b'\end{aligned}$$

són isomorfes si, i només si, existeix $c \in \mathbb{K}^*$, de manera que $a' = c^4 a$ i $b' = c^6 b$. En aquest cas, l'isomorfisme ve definit per:

$$(x,y) \longmapsto (c^2 x, c^3 y).$$

En cas que el cos $\mathbb{K}$ sigui algebraicament tancat, aleshores es pot afirmar que dos corbes el·líptiques definides sobre aquest cos $\mathbb{K}$ són isomorfes, si, i només si, tenen el mateix j–invariant. En un cos no algebraicament tancat, sols és cert un sentit d'aquesta implicació: dos corbes isomorfes tenen el mateix j–invariant. El fet de tenir dos corbes amb el mateix j–invariant no implica, però, que aquestes siguin isomorfes.

2.2 Llei de grup

Sigui $E(\mathbb{K})$ el conjunt de punts d'una corba el·líptica E definida sobre $\mathbb{K}$. Es pot definir una suma de punts sobre $E(\mathbb{K})$ que el dota d'estructura de grup abelià amb neutre el punt $\mathcal{O}_E$ [HMV03, MVOV96].

Aquesta suma de punts es pot definir de forma geomètrica utilitzant el *mètode de la corda-tangent*. Per calcular el punt suma de dos punts P i Q de $E(\mathbb{K})$ es traça la recta que passa per aquests dos punts; aquesta interseca en un tercer punt al qual denotarem com S. El resultat, doncs, de $P+Q$ és el punt R que s'obté en intersecar la corba amb la paral·lela a l'eix d'ordenades pel punt S. En cas que $P=Q$, és a dir, que vulguem doblar un punt, es traça la recta tangent al punt que es vol doblar. Aquesta recta, com en cas anterior, intersecarà en un nou punt S (Figura 2.1).

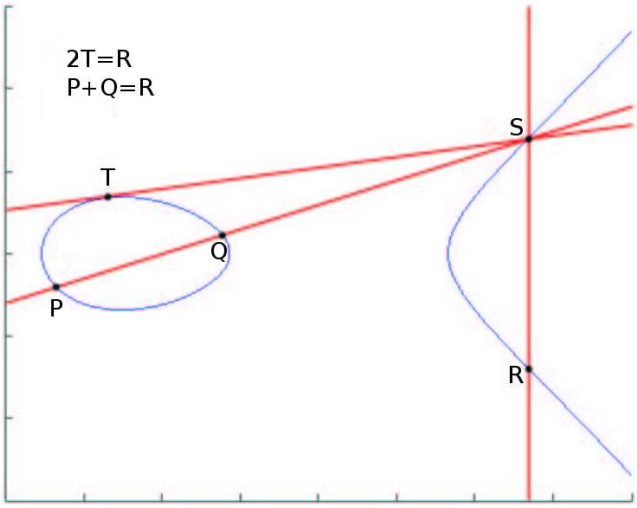


Figura 2.1: Mètode de la corda-tangent

Analíticament, les operacions vénen determinades depenent de les coordenades en què es treballa. Així, en cas de les coordenades representades en forma afí, si l'equació de la corba és:

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

trobem que el punt resultant de la suma, $R = (x_3, y_3)$, es pot expressar en termes de les coordenades dels punts $P = (x_1, y_1)$ i $Q = (x_2, y_2)$, quan $P+Q \neq \mathcal{O}_E$, i les seves coordenades vénen donades per les expressions següents:

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1, \tag{2.7}$$

amb $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ en cas que $x_1 \neq x_2$, i $\lambda = \frac{3x_1 + a}{2y_1}$ si $x_1 = x_2$ i $y_1 \neq 0$.

Si el que es vol és fer el doblat del punt, és a dir, en cas que $P = Q$, aleshores les coordenades del punt doblat vénen donades per les següents expressions:

$$x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1, \tag{2.8}$$

Però les coordenades afins no són les úniques amb què es pot treballar. Aquestes altres coordenades són les projectives i les jacobianes. En tots dos tipus, els punts vénen donats per tres coordenades $P = (X : Y : Z)$ i es pot passar a coordenades afins amb uns canvis simples. En cas que es treballi amb punts representats mitjançant coordenades projectives, obtenim que els punts equivalents en coordenades afins són, si $Z \neq 0$, $(X/Z, Y/Z)$, mentre que si els punts estan representats amb coordenades jacobianes, els punts afins són $(X/Z^2, Y/Z^3)$ [CMO98]. L'avantatge de treballar amb coordenades projectives o jacobianes sobre un cos finit és que s'evita el càlcul d'inversos modulars.

Quan es treballa en coordenades projectives, el punt $(X : Y : Z)$ pertany a la corba si satisfà l'equació:

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Les coordenades de $R = P + Q = (X_3 : Y_3 : Z_3)$, amb $P \neq Q$, vénen donades en termes de $P = (X_1 : Y_1 : Z_1)$ i $Q = (X_2 : Y_2 : Z_2)$ per:

$$X_3 = vA, \quad Y_3 = u(v^2X_1Z_2 - A) - v^3Y_1Z_2, \quad Z_3 = v^3Z_1Z_2, \tag{2.9}$$

on $u = Y_2Z_1 - Y_1Z_2$, $v = X_2Z_1 - X_1Z_2$ i $A = u^2Z_1Z_2 - v^3 - 2v^2X_1Z_2$. I, en cas que es fes el doblat d'un punt, seria:

$$X_3 = 2hs, \quad Y_3 = w(4B - h) - 8Y_1^2s^2, \quad Z_3 = 8s^3, \tag{2.10}$$

on $w = aZ_1^2 + 3X_1^2$, $s = Y_1Z_1$, $B = X_1Y_1s$ i $h = w^2 - 8B$.

En cas que es treballi amb coordenades jacobianes, el punt $(X : Y : Z)$ pertany a la corba si satisfà l'equació:

$$Y^2 = X^3 + aXZ^4 + bZ^6.$$

Les equacions de la suma en aquest tipus de coordenades són:

$$X_3 = -H^3 - 2U_1H^2 + R^2,\ Y_3 = -S_1H^3 + R(U_1H^2 - X_3),\ Z_3 = Z_1Z_2H, \quad (2.11)$$

amb $U_1 = X_1Z_2^2$, $U_2 = X_2Z_1^2$, $S_1 = Y_1Z_2^3$, $S_2 = Y_2Z_1^3$, $H = U_2 - U_1$ i $R = S_2 - S_1$. Mentre que el doblat d'un punt, $P = Q$, seria:

$$X_3 = T, \quad Y_3 = -8Y_1^4 + M(S - T), \quad Z_3 = 2Y_1Z_1, \quad (2.12)$$

amb $S = 4X_1Y_1^2$, $M = 3X_1^2 + aZ_1^4$ i $T = -2S + M^2$.

En la secció 2.11.2 es mostren els costos en realitzar aquestes operacions depenent del model de corba utilitzat. Així, segons les característiques que es vulguin, s'elegeix un model o bé un altre.

A partir de les operacions de suma i doblat es pot considerar la multiplicació d'un punt P per un escalar k com la suma de k vegades el punt P. Més precisament:

$$kP = \begin{cases} \overbrace{P + \cdots + P}^{k \text{ vegades}} & \text{si } k > 0, \\ \mathcal{O}_E & \text{si } k = 0, \\ \underbrace{(-P) + \cdots + (-P)}_{k \text{ vegades}} & \text{si } k < 0. \end{cases}$$

A la pràctica, per calcular kP no se suma k cops el punt P, sinó que s'utilitza l'algorisme de doblats successius que redueix considerablement el cost. El mètode emprat utilitza el valor en binari de $k = k_{n-1} \ldots k_0$. Comença per k_{n-1} i va tractant cada bit fins a arribar a k_0; així, si el bit i–èssim pren valor 0, aleshores l'algorisme fa el doblat del punt que ha obtingut en el pas anterior; en canvi, si pren valor 1 primer fa el doblat del punt anterior i a aquest nou punt li suma el punt inicial P. Així, aquest algorisme fa que calcular kP tingui un cost de l'ordre de $\log_2 k$.

2.3 Corbes el·líptiques sobre cossos finits

Fins ara hem parlat de corbes el·líptiques sobre un cos arbitrari $\mathbb{K}$. Com que en criptografia interessa treballar sobre cossos finits, en aquesta secció veurem algunes propietats de les corbes el·líptiques en cas que aquestes estiguin definides sobre un cos finit $\mathbb{F}_q$, on q és un primer o una potència d'un primer [Elk98, Ler97, Rüc87].

S'anomena *cardinal* d'una corba el·líptica E definida sobre $\mathbb{F}_q$ el nombre de punts $(x, y) \in \mathbb{F}_q^2$ pertanyents a $E(\mathbb{F}_q)$ juntament amb el punt de l'infinit $\mathcal{O}_E$, denotat com $\#E(\mathbb{F}_q)$. En criptografia, una corba el·líptica sobre un cos finit $\mathbb{F}_q$ és més o menys segura depenent de la mida q i de com sigui la factorització del seu cardinal. Per tant, és important conèixer el cardinal de la corba en la qual es treballa. Del cardinal d'una corba sobre un cos $\mathbb{F}_q$ en sabem, gràcies a H. Hasse [Has33], que es troba en l'anomenat interval de Hasse. Calcular, però, el cardinal, tot i que existeixen algorismes com el SEA [Sch85], resulta encara costós. Seguidament, introduïm l'endomorfisme de Frobenius d'una corba el·líptica.

Donada una corba el·líptica E sobre $\mathbb{F}_q$, es defineix l'*endomorfisme de Frobenius* de E com:

$$\begin{aligned} \pi : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ (x, y) &\longrightarrow (x^q, y^q) \end{aligned} \tag{2.13}$$

on $\overline{\mathbb{F}}_q$ és la clausura algebraica de $\mathbb{F}_q$. Aquest endomorfisme satisfà l'equació:

$$X^2 - tX + q = 0$$

on l'enter t s'anomena *traça* de l'endomorfisme de Frobenius de E.

Tenint en compte aquesta equació de l'endomorfisme de Frobenius, es pot enunciar la desigualtat de Hasse [Has33] com:

Teorema 2.1 (Desigualtat de Hasse)**.** *Sigui E una corba el·líptica definida sobre un cos finit $\mathbb{F}_q$, aleshores $\#E(\mathbb{F}_q) = q + 1 - t$, amb $|t| \leqslant 2\sqrt{q}$, sent t la traça de l'endomorfisme de Frobenius de E.*

Tanmateix, l'estructura del grup de punts de la corba, $E(\mathbb{F}_q)$, ve caracteritzada pel següent resultat [Cas66]:

Teorema 2.2 (Teorema de Cassels)**.** *Sigui E una corba el·líptica sobre $\mathbb{F}_q$ de manera que $\#E(\mathbb{F}_q) = m$. El grup de punts d'aquesta corba és isomorf o bé al grup cíclic $\mathbb{Z}/m\mathbb{Z}$, o bé al producte de dos grups cíclics $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$, on $m = m_1 \cdot m_2$, $m_1|m_2$ i $m_1|(q-1)$.*

D'altra banda, W. Waterhouse [Wat69] va demostrar que sobre un cos $\mathbb{F}_p$ existeixen corbes el·líptiques amb cadascun dels cardinals possibles de l'interval de Hasse, mentre que si es treballa sobre un $\mathbb{F}_q$, amb $q = p^n$, $n > 1$, aleshores hi ha alguns valors d'aquest interval que no poden donar-se mai. És més, Waterhouse va determinar els possibles cardinals en cas $\mathbb{F}_q$:

Teorema 2.3. *Existeix almenys una corba $E/\mathbb{F}_q$, $q = p^n$, amb cardinal $\#E(\mathbb{F}_q) = q + 1 - t$ únicament si es compleix algun dels següents casos:*

A. $t \not\equiv 0 \pmod{p}$ *i* $t^2 \leqslant 4q$,

B. *n és senar i*

  a) $t = 0$,

  b) $t^2 = 2q$ *i* $p = 2$,

  c) $t^2 = 3q$ *i* $p = 3$,

C. *n és parell i*

  a) $t^2 = 4q$,

  b) $t^2 = q$ *i* $p \not\equiv 1$,

  c) $t = 0$ *i* $p \not\equiv 1$.

Ara bé, no totes les corbes són bones per usar en criptografia el·líptica. Així, les anomenades *supersingulars* s'han de descartar per a usos criptogràfics quan ens basem en el problema del logaritme discret. Es diu que una corba $E/\mathbb{F}_q$

és supersingular quan p divideix t; veient el Teorema 2.1 i també el 2.3, es pot extreure que una corba és supersingular si, i només si, $t^2 = 0$, q, $2q$, $3q$ o $4q$. Altrament, es diu que la corba és *ordinària*.

En el grup de punts $E(\mathbb{F}_q)$ es poden considerar els anomenats subgrups de k–torsió, denotats com $E(\mathbb{F}_q)[k]$. Així, si fixem un enter k positiu, el subgrup $E(\mathbb{F}_q)[k]$ està format per tots els punts $P \in E(\mathbb{F}_q)$ de manera que $kP = \mathcal{O}_E$, és a dir, que tenen ordre k o bé un factor de k. D'altra banda, es denota com $E[k]$ el subgrup de k–torsió de la corba E definida sobre la clausura algebraica $\overline{\mathbb{F}}_q$.

Si ℓ és un primer diferent de la característica de $\mathbb{F}_q$, sempre i que el grup $E(\mathbb{F}_q)[\ell]$ no sigui trivial, es pot afirmar que $E(\mathbb{F}_q)[\ell]$ és cíclic i isomorf a $\mathbb{Z}/\ell\mathbb{Z}$, o bé és de rang 2, i aleshores tenim que $E(\mathbb{F}_q)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

Es defineix també el *subgrup de ℓ–Sylow* d'una corba el·líptica $E/\mathbb{F}_q$, $\mathcal{S}_\ell(E(\mathbb{F}_q))$, com el conjunt de tots els punts de $E(\mathbb{F}_q)$ que tenen ordre una potència de ℓ.

Si el subgrup $\mathcal{S}_\ell(E(\mathbb{F}_q)) \neq \{\mathcal{O}_E\}$, aleshores o bé és cíclic i isomorf a $\mathbb{Z}/\ell^n\mathbb{Z}$, $n \geqslant 1$, o bé de rang 2 i $\mathcal{S}_\ell(E(\mathbb{F}_q)) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}$, amb $n \geqslant r \geqslant 1$.

En la tesi de R. Moreno [Mor05], així com en [MMRV05, MMRV08], es donen algorismes per determinar l'estructura dels subgrups de Sylow, és a dir, per determinar els enters n i r, i generadors del subgrup.

2.4 Polinomis de divisió

En aquesta secció introduirem els polinomis de n–divisió que tenen la peculiaritat que les seves arrels ens donen les abscisses dels punts d'ordre n, és a dir, les abscisses dels punts d'n–torsió.

Donada una corba el·líptica E sobre un cos $\mathbb{K}$ d'equació (2.1), es defineixen els *polinomis de n–divisió*, $\psi_n(x, y) \in \mathbb{K}[x, y]$ amb $n \geqslant 1$ [Cas66] de forma recursiva de la manera següent:

$$\begin{aligned}
\psi_1(x,y) &= 1, \quad \psi_2(x,y) = 2y + a_1x + a_3, \\
\psi_3(x,y) &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\
\psi_4(x,y) &= (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 \\
&\quad +(b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2)\psi_2(x,y), \\
\psi_{2n+1}(x,y) &= \psi_{n+2}(x,y)\psi_n(x,y) - \psi_{n-1}(x,y)\psi_{n+1}^3(x,y), \ n \geq 2, \\
\psi_{2n}(x,y) &= \frac{\psi_n(x,y)(\psi_{n+2}(x,y)\psi_{n-1}^2(x,y) - \psi_{n-2}(x,y)\psi_{n+1}^2(x,y))}{\psi_2(x,y)}, \ n \geq 3,
\end{aligned} \tag{2.14}$$

definint el casos de $n = 0$ de la següent forma: $\psi_0(x,y) = 0$.

Veient les expressions (2.14) és fàcil observar que en els casos que n sigui un nombre parell, $\psi_n(x,y)$ és igual a un polinomi de variable x multiplicat per $\psi_2(x,y)$, és a dir, multiplicat per $2y + a_1x + a_3$, mentre que si n és senar, $\psi_n(x,y)$ mòdul l'equació de la corba serà un polinomi que únicament tindrà la variable x. Per tant, a partir d'aquestes propietats podem construir uns nous de polinomis $f_n(x)$, també anomenats de n–divisió, definits utilitzant sols la variable x. Aquests polinomis es defineixen a partir dels polinomis de n–divisió de dos variables $\psi_n(x,y)$ de la següent forma:

$$f_n(x) = \begin{cases} \frac{\psi_n(x,y)}{\psi_2(x,y)}, & \text{si } n \text{ és parell,} \\ \psi_n(x,y), & \text{altrament.} \end{cases}$$

Els polinomis de n–divisió $\psi_n(x,y)$ estan relacionats amb la multiplicació d'un punt $P = (x,y)$ de la corba el·líptica $E/\mathbb{K}$ per un escalar n i donen les coordenades d'aquest nou punt:

$$nP = \left(\frac{\phi_n(x,y)}{\psi_n^2(x,y)}, \ \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right),$$

on:

$$\begin{aligned}
\phi_n(x,y) &= x\psi_n^2(x,y) - \psi_{n-1}(x,y)\psi_{n+1}(x,y), \\
2\psi_n(x,y)\omega_n(x,y) &= \psi_{n+2}(x,y)\psi_{n-1}^2(x,y) - \psi_{n-2}(x,y)\psi_{n+1}^2(x,y).
\end{aligned}$$

Així, si E és una corba el·líptica definida sobre el cos finit $\mathbb{F}_q$, un punt $P = (x, y) \in E(\overline{\mathbb{F}}_q)$, amb $P \neq \mathcal{O}_E$, serà un punt de n–torsió, és a dir, $nP = \mathcal{O}_E$, si, i només si, $\psi_n(x, y) = 0$.

2.5 Isogènies de corbes el·líptiques

En aquesta secció donarem els conceptes bàsics sobre isogènies entre corbes el·líptiques, que són morfismes de corbes algebraiques que preserven l'estructura de grup [Sil86, Sil94, Gal99]. Comencem per la definició formal d'isogènia:

Definició 2.4. *Siguin E i E' dos corbes el·líptiques definides sobre un cos $\mathbb{K}$. S'anomena isogènia entre E i E' a un morfisme de corbes $\mathcal{I} : E/\mathbb{K} \to E'/\mathbb{K}$, de manera que $\mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$.*

Com a exemple d'isogènia tenim la isogènia *multiplicació per m*, denotada com $[m]$. Aquesta va d'una corba E a si mateixa i es defineix de la següent forma:

$$\begin{aligned} [m] : E/\overline{\mathbb{K}} &\to E/\overline{\mathbb{K}} \\ P &\to mP \end{aligned} \tag{2.15}$$

Qualsevol isogènia sobre la clausura algebràica $\mathcal{I}$ o és constant, i aleshores $\mathcal{I}(E) = \mathcal{O}_{E'}$, o és exhaustiva, i llavors $\mathcal{I}(E) = E'$. En aquest últim cas, es diu que E i E' són corbes isògenes.

Donada una isogènia $\mathcal{I}$ entre dos corbes el·líptiques E i E' sobre $\mathbb{K}$, es pot obtenir una immersió dels cossos de funcions racionals de les corbes definida per:

$$\begin{aligned} \mathcal{I}^* : \overline{\mathbb{K}}(E') &\hookrightarrow \overline{\mathbb{K}}(E) \\ f &\mapsto \mathcal{I}^* f = f \circ \mathcal{I} \end{aligned}$$

A partir d'aquesta immersió es pot definir el que es coneix com *grau de la isogènia* $\mathcal{I}$, com el grau de l'extensió $\overline{\mathbb{K}}(E)/\mathcal{I}^*(\overline{\mathbb{K}}(E'))$. Llavors $deg(\mathcal{I}) =$

$deg_s(\mathcal{I})deg_i(\mathcal{I})$, on deg_s i deg_i són els graus de separabilitat i inseparabilitat, respectivament, d'aquesta immersió.

Donada una isogènia $\mathcal{I}$ entre dos corbes, E i E', definides sobre un cos $\mathbb{K}$, aleshores $\forall P, Q \in E/\mathbb{K}$ tenim que $\mathcal{I}(P+Q) = \mathcal{I}(P) + \mathcal{I}(Q)$, és a dir, $\mathcal{I}$ conserva la llei de grup. A més, el conjunt $\mathcal{I}^{-1}(\mathcal{O}_E)$ és un subgrup finit de $E(\mathbb{K})$.

D'altra banda, si $G \subset E(\overline{\mathbb{K}})$ és un grup finit, llavors existeix una única corba el·líptica E' i una isogènia separable $\mathcal{I}_G : E \longrightarrow E'$ de manera que $Ker\mathcal{I}_G = G$. En aquest cas E' es denota com E/G. Si E està definida sobre $\mathbb{K}$ i G és un grup racional, és a dir, invariant per l'acció de Galois $Gal(\overline{\mathbb{K}}/\mathbb{K})$, aleshores la corba E/G i la isogènia $\mathcal{I}_G$ estan definides sobre $\mathbb{K}$.

Si $\mathcal{I} : E \longrightarrow E'$ és una isogènia de grau m, aleshores existeix una única isogènia $\widehat{\mathcal{I}} : E' \longrightarrow E$ de grau m, de manera que:

$$\begin{cases} \widehat{\mathcal{I}} \circ \mathcal{I} = [m] & \text{en } E \\ \mathcal{I} \circ \widehat{\mathcal{I}} = [m] & \text{en } E' \end{cases}$$

La isogènia $\widehat{\mathcal{I}}$ es coneix com *isogènia dual* de $\mathcal{I}$.

Basant-se en el cardinal, tenim el següent resultat de Tate:

Teorema 2.5. *[Tat66] Dos corbes E i E' definides sobre un cos finit $\mathbb{F}_q$ són isògenes si, i només si, tenen el mateix cardinal.*

Aquest resultat és molt important per a aquesta tesi perquè ens permet trobar corbes amb el mateix cardinal que una de donada mitjançant el càlcul d'isogènies.

2.6 Fórmules de Vélu

En aquesta secció donarem les fórmules de Vélu que expressen, a partir d'una corba el·líptica inicial i un subgrup del seu grup de punts, els coeficients de la corba el·líptica isògena determinada per aquest subgrup. Així, donada una corba el·líptica $E/\mathbb{K}$ definida mitjançant l'equació:

$$E/\mathbb{K} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

i un subgrup Galois invariant $G \subseteq E(\overline{\mathbb{K}})$, J. Vélu [Vél71] va donar expressions per a les coordenades del punt imatge per la isogènia $\mathcal{I}_G$ d'un punt $P \in E(\mathbb{K})$:

$$\begin{cases} X = x(\mathcal{I}_G(P)) = \sum_{T\in G} x(P+T) - \sum_{T\in G\setminus\mathcal{O}_E} x(T) \\ Y = y(\mathcal{I}_G(P)) = \sum_{T\in G} y(P+T) - \sum_{T\in G\setminus\mathcal{O}_E} y(T) \end{cases}$$

Vélu va donar també l'equació de la corba E' isògena a E per $\mathcal{I}_G$ i les equacions de la isogènia $\mathcal{I}_G$. Per determinar aquestes expressions, J. Vélu va considerar els subconjunts R i S de forma que:

$$G\setminus E[2] = R \cup (-R), \quad R \cap (-R) = \emptyset \text{ i } S = (G \cap E[2])\setminus\{\mathcal{O}_E\}.$$

Si $f(x,y) = 0$, amb $f(x,y) = x^3 + a_2x^2 + a_4x + a_6 - (y^2 + a_1xy + a_3y)$, és l'equació de la corba E i $P = (x,y)$ és un punt de $E(\overline{\mathbb{K}})$, aleshores les derivades parcials de $f(x,y)$ respecte a x i y en P vénen donades per:

$$\begin{aligned} f_P^x &= \tfrac{\partial f(x,y)}{\partial x}(P) = 3x^2 + 2a_2x + a_4 - a_1y, \\ f_P^y &= \tfrac{\partial f(x,y)}{\partial y}(P) = -2y - a_1x - a_3. \end{aligned}$$

A partir d'aquestes expressions, J. Vélu va considerar, per cada punt $T \in R \cup S$, els següents elements de $\overline{\mathbb{K}}$:

$$\begin{aligned} t(T) &= \begin{cases} f_T^x, & \text{si } T \in S \\ 2f_T^x - a_1f_t^y = 6x(T)^2 + b_2x(T) + b_4, & \text{si } T \notin S \end{cases} \\ u(T) &= 4x(T)^3 + b_2x(T)^2 + 2b_4x(T) + b_6. \end{aligned}$$

i els paràmetres:

$$t = \sum_{T\in R\cup S} t(T) \quad \text{i} \quad \omega = \sum_{T\in R\cup S} (u(T) + x(T)t(T)).$$

Aleshores, la corba E' isògena a E per la isogènia $\mathcal{I}_G$ té equació:

$$E'/\mathbb{K} : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6',$$

on:

$$a'_1 = a_1, \quad a'_2 = a_2, \quad a'_3 = a_3, \quad a'_4 = a_4 - 5t \quad \text{i} \quad a'_6 = a_6 - b_2 t - 7\omega$$

A més, les coordenades del punt $\mathcal{I}_G(P) = (X, Y)$ tenen les expressions següents:

$$\begin{aligned} X &= x + \sum_{T \in R \cup S} \left(\frac{t(T)}{x - x(T)} + \frac{u(T)}{(x - x(T))^2} \right) \\ Y &= y - \sum_{T \in R \cup S} \left(u(T) \frac{2y + a_1 x + a_3}{(x - x(T))^3} \right. \\ &\quad \left. + t(T) \frac{a_1(x - x(T)) + y - y(T)}{(x - x(T))^2} + \frac{a_1 u(T) - f_T^x f_T^y}{(x - x(T))^2} \right) \end{aligned}$$

2.7 Polinomis modulars

En aquest apartat es presentaran els polinomis modulars, una altra eina per calcular les corbes isògenes d'una corba el·líptica donada (vegis [BSS99, BSS05, CL05]). Per definir-los, es treballarà amb corbes el·líptiques definides sobre $\mathbb{C}$ i s'utilitzaran els reticles. Passem a definir què s'entén per reticle:

Definició 2.6. *Un reticle L en el pla complex $\mathbb{C}$ és un subgrup discret de $\mathbb{C}$ generat per dos vectors, ω_1 i ω_2, linealment independents que es poden elegir amb la condició $Im(\frac{\omega_1}{\omega_2}) > 0$. Aquest reticle es denota com*

$$L(\omega_1, \omega_2) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

Si L és un reticle de $\mathbb{C}$, aleshores la sèrie definida com

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

convergeix normalment en cada compacte de $\mathbb{C} - L$. La suma d'aquesta sèrie es denomina funció de Weierstraß associada al reticle L. Aquesta funció és diferenciable i doblement periòdica, amb períodes ω_1 i ω_2.

Es defineix la sèrie:

$$G_k(L) = \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^k},$$

amb k un enter qualsevol de manera que $k > 2$, i L un reticle de $\mathbb{C}$. La sèrie $G_k(L)$ és absolutament convergent.

Donat un reticle L, se li pot associar una corba el·líptica definida sobre $\mathbb{C}$ d'equació:

$$E/\mathbb{C} : y^2 = 4x^3 - g_2(L)x - g_3(L) \tag{2.16}$$

on $g_2(L) = 60G_4(L)$ i $g_3(L) = 140G_6(L)$.

Recíprocament, donada una corba el·líptica sobre $\mathbb{C}$ d'equació $E/\mathbb{C} : y^2 = 4x^3 - a_2x - a_3$ existeix un reticle L amb $g_2(L) = a_2$ i $g_3(L) = a_3$. Si $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ és aquest reticle i prenem $\tau = \frac{\omega_1}{\omega_2}$, amb $Im(\tau) > 0$, aleshores, existeix un isomorfisme de grups entre el quocient de $\mathbb{C}$ pel reticle $L(1, \tau)$ i la corba E donat per:

$$\begin{array}{rcl} \psi : \mathbb{C} & \to & E \\ z & \mapsto & \begin{cases} (\wp_L(z), \wp'_L(z)) & \text{si } z \notin L \\ \mathcal{O}_E & \text{si } z \in L \end{cases} \end{array}$$

Així, es pot identificar una corba el·líptica sobre $\mathbb{C}$ amb $\mathbb{C}/L$.

El j–invariant de la corba el·líptica associada a $L(1, \tau)$, denotat com $j(\tau)$, ve donat per:

$$j(\tau) = 1728\frac{g_2^3(L)}{g_2^3(L) - 27g_3^3(L)}.$$

Aquest invariant té una expressió, coneguda amb el nom de *q–expansió* del j–invariant, donada per:

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geqslant 1} c_n q^n,$$

amb $q = e^{2\pi i \tau}$ i on els coeficients c_n es poden anar calculant recursivament.

Si considerem un element $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$ del grup

$$GL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) : \quad ad - bc > 0 \right\},$$

es defineix

$$j \circ \alpha(\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right),$$

que és el j–invariant de la corba el·líptica $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau')$ on $\tau' = \frac{a\tau+b}{c\tau+d}$.

Per a cada enter n es defineix

$$S_n^\star = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) : \ ad = n, \ d > 0, \ 0 < b < d, \ \gcd(a, b, d) = 1 \right\}.$$

En cas que n sigui primer, aleshores $\#S_n^\star = n + 1$.

Utilitzant les definicions prèvies podem relacionar les corbes isògenes amb el seu j–invariant a partir del teorema següent:

Teorema 2.7. *Siguin E i E' dos corbes el·líptiques definides sobre $\mathbb{C}$ amb j–invariants $j(E) = j(\tau) = j$ i $j(E') = j'$, i sigui n un enter. Llavors, existeix $\sigma \in S_n^\star$ de manera que*

$$j' = j \circ \sigma(\tau),$$

si, i només si, existeix una isogènia de E a E' amb nucli un subgrup cíclic de grau n.

Definició 2.8. *S'anomena polinomi modular d'ordre n el polinomi de grau $\#S_n^\star$ en x donat per:*

$$\Phi_n(x, j) = \prod_{\sigma \in S_n^\star} (x - j \circ \sigma).$$

Aquest polinomi, vist com a polinomi en dos variables $\Phi_n(x, y)$, és simètric. Vegem com a exemple el polinomi modular d'ordre 3:

$$\begin{aligned}\Phi_3(x,y) \;=\; & x^4 + 2232x^3y^2 - 1069956x^3y + 36864000x^3 + 8900222976000x^2y + \\ & y^4 + 2232x^2y^3 - 1069956xy^3 + 36864000y^3 + 8900222976000xy^2 + \\ & 452984832000000x^2 + 1855425871872000000000x + \\ & 452984832000000y^2 + 1855425871872000000000y - \\ & x^3y^3 + 2587918086x^2y^2 - 770845966336000000xy.\end{aligned}$$

Utilitzant la Definició 2.8 i el Teorema 2.7 es pot afirmar que existeix una isogènia de grau n de la corba E a la corba E' d'invariants j i j', respectivament, si, i només si, $\Phi_n(j,j') = 0$.

També es pot deduir que de cada corba el·líptica existeixen en la clausura algebraica $n+1$ isògenes de grau n (exceptuant isomorfismes) en cas que n sigui un nombre primer i $n\prod_{p|n}\left(1+\frac{1}{p}\right)$ en cas que n sigui producte de primers. Aquest valor és el grau de $\Phi_n(x,y)$ en x i en y.

Si treballem amb una corba el·líptica definida sobre un cos finit, $E/\mathbb{F}_q$, aleshores el nombre de corbes ℓ–isògenes a aquesta, amb ℓ primer, pot ser 0, 1, 2 o $\ell+1$ (vegis en [Koh96]).

2.8 Coeficients de les corbes ℓ–isògenes

Fins ara hem vist que donada una corba el·líptica E sobre un cos $\mathbb{F}_q$ es poden trobar mitjançant el polinomi modular de grau ℓ els j–invariants de les corbes ℓ–isògenes a aquesta. Ara veurem com a partir d'aquests j–invariants podem obtenir coeficients de les corbes ℓ–isògenes a $E/\mathbb{F}_q$.

Sigui $y^2 = x^3 + \tilde{a}x + \tilde{b}$ l'equació d'una corba $\tilde{E}$ que té j–invariant $\tilde{j}$, sent $\tilde{j}$ una arrel de $\phi_\ell(x,j)$, és a dir, el j–invariant de la corba isògena a E. A partir d'aquest j–invariant es pot construir l'equació de la corba $\tilde{E}$ definida en $\mathbb{F}_q$ de la següent manera [BSS99, BSS05]:

$$\overline{a} = -48a, \quad \overline{b} = 864b, \quad j' = -j\frac{\overline{b}}{\overline{a}}, \quad \tilde{j}' = -\frac{j'}{\ell}\frac{(\phi_\ell)_x(j,\tilde{j})}{(\phi_\ell)_y(j,\tilde{j})},$$
$$\tilde{a} = -\frac{(\tilde{j}')^2}{48\tilde{j}(\tilde{j}-1728)}, \quad \tilde{b} = -\frac{(\tilde{j}')^3}{864(\tilde{j})2(\tilde{j}-1728)}.$$

Aquestes expressions donen els coeficients d'una corba el·líptica a partir del seu j–invariant $\tilde{j}$, ℓ–isògena a $E/\mathbb{F}_q$.

2.9 Cossos quadràtics

Un *cos quadràtic* $\mathbb{K}$ és una extensió de grau 2 de $\mathbb{Q}$. Qualsevol cos quadràtic es pot escriure com $\mathbb{K} = \mathbb{Q}(\sqrt{\delta})$ amb $\delta \in \mathbb{Z}$ i lliure de quadrats. A més a més, es defineix el discriminant de $\mathbb{K}$ com:

$$d_{\mathbb{K}} = \begin{cases} 4\delta & \text{si } \delta \not\equiv 1 \mod 4, \\ \delta & \text{si } \delta \equiv 1 \mod 4. \end{cases}$$

En un cos quadràtic $\mathbb{K}$ hi ha l'automorfisme no trivial que a cada $\alpha = x + y\sqrt{\delta}$ li assigna el seu conjugat denotat com $\overline{\alpha} = x - y\sqrt{\delta}$. La norma i la traça de α es defineixen, aleshores, com:

$$\begin{aligned} N_{\mathbb{K}}(\alpha) &= \alpha \cdot \overline{\alpha} = x^2 - \delta y^2, \\ T_{\mathbb{K}}(\alpha) &= \alpha + \overline{\alpha} = 2x. \end{aligned} \tag{2.17}$$

Es diu que α és un enter algebraic, si $N_{\mathbb{K}}(\alpha)$ i $T_{\mathbb{K}}(\alpha) \in \mathbb{Z}$. D'aquesta forma, es defineix l'anell d'enters del cos $\mathbb{K}$ com:

$$\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{Q}(\sqrt{\delta}) \mid N_{\mathbb{K}}(\alpha), T_{\mathbb{K}}(\alpha) \in \mathbb{Z}\}.$$

L'anell d'enters $\mathcal{O}_{\mathbb{K}}$ d'un cos quadràtic $\mathbb{K}$ és un mòdul lliure de rang 2 amb base $\{1, \omega\}$, on:

$$\omega = \begin{cases} \sqrt{d} & \text{si } \delta \not\equiv 1 \mod 4, \\ \frac{1+\sqrt{d}}{2} & \text{si } \delta \equiv 1 \mod 4, \end{cases} \tag{2.18}$$

o per abreviar, $\omega = \frac{d+\sqrt{d}}{2}$, i d'aquesta manera serveix per als dos casos.

En l'anell d'enters d'un cos quadràtic $\mathbb{K}$, hi ha uns subanells $\mathcal{O}$ anomenats *ordres* del cos $\mathbb{K}$ que es defineixen de la manera següent:

Definició 2.9. *Un ordre $\mathcal{O}$ de $\mathbb{K}$ és un subanell finitament generat com a $\mathbb{Z}$–mòdul que compleix $\mathcal{O} \otimes \mathbb{Q} = \mathbb{K}$.*

Aquests subanells continguts en $\mathbb{K}$ són de la forma

$$\mathcal{O} = \mathbb{Z} \oplus f\omega\mathbb{Z},$$

amb ω definida mitjançant (2.18). Quan $f = 1$, aleshores $\mathcal{O} = \mathcal{O}_{\mathbb{K}}$. Aquest ordre s'anomena *ordre maximal* de $\mathbb{K}$, ja que és el més gran de tots els possibles ordres de $\mathbb{K}$.

Definició 2.10. *Donat un ordre $\mathcal{O} = \mathbb{Z} \oplus f\omega\mathbb{Z}$, l'índex $f = [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$, s'anomena* conductor de $\mathcal{O}$. *I l'enter $D = f^2 d_{\mathbb{K}}$ és el* discriminant *de l'ordre $\mathcal{O}$ sent $d_{\mathbb{K}}$ el discriminant de $\mathbb{K}$.*

Veiem també què s'entén com *àlgebra de quaternions* sobre $\mathbb{Q}$, una estructura que va ser introduïda per W. R. Hamilton el 1844 [Ham44].

Una àlgebra de quaternions sobre $\mathbb{Q}$ és una àlgebra de dimensió 4 de la forma:

$$\mathbb{K} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k,$$

on i^2, $j^2 \in \mathbb{Q}$, $i^2 < 0$, $j^2 < 0$, $k = ij = -ji$ i $k^2 = -i^2 j^2$.

2.10 Anell d'endomorfismes d'una corba el·líptica

Siguin $\mathcal{I}$ i $\mathcal{I}'$ dos isogènies entre les corbes el·líptiques E_1 i E_2 definides sobre un cos $\mathbb{K}$, és a dir, $\mathcal{I}, \mathcal{I}' \in Hom(E_1, E_2)$, aleshores tenim que $(Hom(E_1, E_2), +)$ té estructura de grup amb l'operació:

$$(\mathcal{I} + \mathcal{I}')(P) = \mathcal{I}(P) + \mathcal{I}'(P).$$

Tanmateix, el conjunt $End(E) = Hom(E, E)$ té estructura d'anell mitjançant l'operació suma anterior i com a operació producte la composició d'isogènies:

$$(\mathcal{I} \circ \mathcal{I}')(P) = \mathcal{I}(\mathcal{I}'(P)).$$

L'anell $(End(E), +, \circ)$ s'anomena anell d'endomorfismes de E. Aquest anell conté $\mathbb{Z}$ si s'identifica m amb la isogènia:

$$[m] : E \longrightarrow E$$

de manera que $[m]P = mP$ (vegis (2.15)).

Teorema 2.11. *L'anell d'endomorfismes d'una corba el·líptica E definida sobre un cos és isomorf a un dels anells següents:*

1. *L'anell d'enters $\mathbb{Z}$.*

2. *Un ordre en un cos quadràtic imaginari.*

3. *Un ordre en una àlgebra de quaternions.*

Donada una corba E definida sobre un cos finit, no és possible que $End(E)$ sigui isomorf a $\mathbb{Z}$. A més a més, si $End(E)$ és un ordre en una àlgebra de quaternions, aleshores E és supersingular.

Donada una corba ordinària E sobre un cos finit $\mathbb{F}_q$, amb $q = p^n$ i p primer, $\mathcal{O} = End(E)$ és un ordre del cos quadràtic

$$\mathbb{K} = \mathbb{Q}\left(\sqrt{t^2 - 4q}\right),$$

L'anell $\mathbb{Z}[\pi]$ generat per l'endomorfisme de Frobenius de E (vegis 2.13) també és un ordre $\mathbb{K}$ i se satisfan les següents inclusions d'ordres de $\mathbb{K}$:

$$\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{K}},$$

on $\mathcal{O}_{\mathbb{K}}$ és l'anell d'enters de $\mathbb{K}$.

2.11 Corbes d'Edwards

El 2007, H. M. Edwards [Edw07] va definir un nou tipus de model d'equacions per a algunes corbes el·líptiques; més concretament va provar que qualsevol corba el·líptica definida sobre un cos finit $\mathbb{F}_q$ de característica diferent de 2 és birracionalment equivalent (un canvi de variables donat per funcions racionals) sobre $\mathbb{F}_q$ o sobre una extensió de $\mathbb{F}_q$ a una corba amb equació:

$$x^2 + y^2 = c^2(1 + x^2y^2),$$

anomenada forma d'Edwards.

Posteriorment, D. Bernstein i T. Lange [BL07], amb la finalitat que aquesta transformació pogués realitzar-se sobre el cos base per a una família de corbes el·líptiques més àmplia, van estendre aquesta idea admetent un nou tipus d'equació, que per similitud també s'anomena forma d'Edwards. Així, es diu que una corba $F/\mathbb{F}_q$ està en forma d'Edwards si té per equació:

$$x^2 + y^2 = c^2(1 + dx^2y^2),$$

on $cd(1 - c^4d) \neq 0$.

Aquestes corbes, sobre els reals, tenen la següent forma:

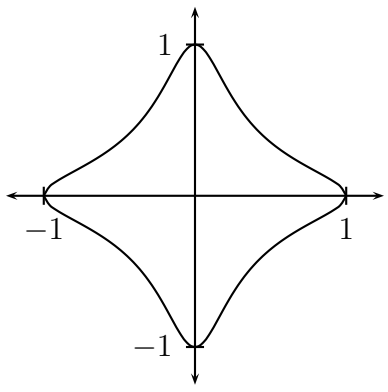


Figura 2.2: Corba d'Edwards $x^2 + y^2 = 1 - 20x^2y^2$ sobre $\mathbb{R}$

2.11.1 Llei de grup

Per a una corba d'Edwards $F/\mathbb{F}_q$ es pot definir, de manera anàloga a com es fa per a una corba el·líptica en forma de Weiertraß, una llei de grup. En aquesta, l'element neutre és $(0, c)$ i donat un parell de punts (x_1, y_1), $(x_2, y_2) \in F/\mathbb{F}_q$ la suma es defineix com:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \right).$$

Si d no és un residu quadràtic a $\mathbb{F}_q$, aquesta operació és completa i unificada, és a dir, per a qualsevol parell de punts la suma es pot realitzar d'aquesta manera i les mateixes expressions es poden aplicar independentment dels punts que es desitgi sumar i sense fer distinció per sumar dos punts diferents o calcular el doblat d'un punt [BL09].

A més, en aquestes corbes existeixen sempre un punt d'ordre 2, $(0, -c)$, i dos punts d'ordre 4, $(c, 0)$, i el seu oposat $(-c, 0)$. El fet de tenir punts d'ordre 2 i d'ordre 4 és una condició necessària perquè una corba el·líptica sigui equivalent a una corba d'Edwards. Més concretament, al voltant del 25% de les classes d'isomorfia de corbes el·líptiques sobre un cos finit es poden representar mitjançant una corba en forma d'Edwards sobre el mateix cos base. El següent teorema [BL07] mostra quines corbes el·líptiques són birracionalment equivalents a una corba d'Edwards.

Teorema 2.12. *Sigui $\mathbb{K}$ un cos finit de característica diferent de 2. Sigui E una corba el·líptica sobre $\mathbb{K}$ de manera que el grup $E(\mathbb{K})$ té un element d'ordre 4.*

1. *Existeix $d \in \mathbb{K} - \{0, 1\}$ de manera que la corba $x^2 + y^2 = 1 + dx^2y^2$ és birracionalment equivalent sobre $\mathbb{K}$ a E o a la seva twist quadràtica.*

2. *Si $E(\mathbb{K})$ té un únic punt d'ordre 2, llavors existeix un no quadrat $d \in \mathbb{K}$ de manera que la corba $x^2 + y^2 = 1 + dx^2y^2$ és birracionalment equivalent sobre $\mathbb{K}$ a E o a la seva twist quadràtica.*

3. *Si $\mathbb{K}$ és un cos finit i $E(\mathbb{K})$ té un únic punt d'ordre 2, llavors existeix un no quadrat $d \in \mathbb{K}$ de manera que la corba $x^2 + y^2 = 1 + dx^2y^2$ és birracionalment equivalent sobre $\mathbb{K}$ a E.*

En cas que una corba el·líptica sigui birracionalment equivalent a una corba d'Edwards, existeix una correspondència entre la llei de grup de la corba el·líptica i la suma en la corba d'Edwards (Teorema 3.2 en [BL07]).

Teorema 2.13. *Sigui $\mathbb{K}$ un cos de característica diferent de 2, i siguin $c, d, e \in \mathbb{K}^*$ amb $e = 1 - dc^4$. Suposem que d no és un quadrat i sigui la corba d'Edwards*

$$F/\mathbb{K} : x^2 + y^2 = c^2(1 + dx^2y^2).$$

Sigui la corba el·líptica d'equació

$$E/\mathbb{K} : (1/e)v^2 = u^3 + (4/e - 2)u^2 + u.$$

Per a cada $i \in \{1, 2, 3\}$ siguin (x_i, y_i) tres punts de $F(\mathbb{K})$ tals que $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$. Es defineix P_i de la forma següent: $P_i = \mathcal{O}$ (punt de l'infinit) si $(x_i, y_i) = (0, c)$; i $P_i = (u_i, v_i)$ si $x_i \neq 0$, on $u_i = (c + y_i)/(c - y_i)$ i $v_i = 2c(c + y_i)/((c - y_i)x_i)$. Llavors

$$P_i \in E(\mathbb{K}) \quad i \quad P_1 + P_2 = P_3.$$

Per tant, operacions sobre una corba el·líptica donada poden traslladar-se a operacions sobre una corba d'Edwards equivalent. A més, les operacions en una corba d'Edwards equivalent són computacionalment més eficients. Finalment, considerant l'aplicació inversa que transforma els punts de $F/\mathbb{K}$ en punts de $E/\mathbb{K}$, pot obtenir-se de manera fàcil el resultat en la corba el·líptica original.

2.11.2 Suma i doblat en corbes d'Edwards

Com ja s'ha comentat, una de les motivacions que fa que siguin interessants les corbes d'Edwards és el fet que aquestes operacions de suma i doblat de punts són més eficients que en cas general de corbes el·líptiques, i, per tant, ens resulta més econòmic realitzar els càlculs en la forma d'Edwards que en la de Weierstraß.

Anomenem M les multiplicacions que es realitzin, S els quadrats (de *squared*) i D multiplicar pel paràmetre d. Ara veurem, en les taules que vénen a continuació, quin és el gruix de càlculs per a cada operació que cal realitzar. Per deixar-ho tot en nombre de multiplicacions, M, s'ha agafat com a valor de S=0,8M i D=0,5M. Dit això, observem la comparativa de les operacions en les següents taules per corbes el·líptiques de la forma de Weierstraß amb coordenades Jacobianes (Jac), projectives (Proj) i corbes d'Edwards (Edw).

En la Taula 2.1 extreta de [BL07] es mostra la comparativa del nombre d'operacions que es realitzen per calcular la suma de dos punts diferents depenent si s'utilitzen coordenades jacobianes, projectives i corbes d'Edwards.

Coordenades	Suma	Suma en M
Jac	11M+5S	15M
Proj	12M+2S	13.6M
Edw	10M+1S+1D	11.3M

Taula 2.1: Comparativa de suma de dos punts

En la Taula 2.2 de [BL07] entren dos tipus nous de dades: són els que el paràmetre a de la corba el·líptica en forma reduïda de Weierstraß val -3. En aquest cas, les operacions de suma i doblat en una corba el·líptica en forma de Weierstraß es poden realitzar més ràpidament (vegis [BSS99, BSS05]). Tot i això, continuen sent més eficients els càlculs en forma d'Edwards

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{c(1 + dx_1^2y_1^2)}, \frac{y_1^2 - x_1^2}{c(1 - dx_1^2y_1^2)} \right)$$

que en altres models de corbes.

Coordenades	Doblat	Doblat en M
Jac	1M+8S+1D	7.9M
Jac $a = -3$	3M+5S	7M
Proj	5M+6S+1D	10.3M
Proj $a = -3$	7M+3S	9.3M
Edw	3M+4S	6.2M

Taula 2.2: Comparativa del doblat d'un punt

Finalment, en la taula 2.3, [BL07], s'observa com seria la suma en cas que s'utilitzessin punts ja emprats anteriorment. Aquests càlculs òbviament serien més ràpids que si els punts per sumar fossin la primera vegada que es realitza aquesta operació.

Coordenades	Suma	Suma en M
Jac	10M+4S	13.2M
Proj	12M+2S	13.6M
Edw	10M+1S+1D	11.3M

Taula 2.3: Comparativa de suma de dos punts ja utilitzats

Capítol 3

Targetes intel·ligents i criptografia el·líptica

En aquest capítol ens centrem en les targetes intel·ligents. Aquests dispositius porten un microxip integrat que emmagatzema informació personal del seu usuari. Per aquest motiu, és imprescindible que aquestes dades vagin xifrades. El problema apareix pel fet que aquests dispositius tenen limitacions de còmput i memòria. Així doncs, una bona solució és l'ús de criptografia el·líptica, ja que aquesta garanteix la mateixa seguretat usant mides de claus molt més petites que altres criptosistemes com el RSA.

Primerament, veurem unes nocions bàsiques de les targetes intel·ligents: l'evolució i l'estructura. Després ens centrarem en la criptografia el·líptica i, més concretament, en la que trobem dins de l'entorn de les targetes intel·ligents.

3.1 Targetes intel·ligents

En els setanta, els grans progressos que s'havien aconseguit en la microelectrònica van fer possible la integració, dins d'un xip de silici, d'un microcontrolador amb capacitat d'emmagatzematge: havien nascut les targetes intel·ligents. Des de llavors han estat nombrosos els avenços que s'han anat introduint en aquests dispositius, per convertir-les en un marc immillorable per a la criptografia, ja que poden emmagatzemar claus, certificats digitals, contrasenyes i patrons biomètrics, entre altres, i, alhora, tenen també capacitat d'executar algorismes

criptogràfics que, gràcies als constants avenços, cada cop poden ser més elaborats. No ens podem oblidar que la seva mida és reduïda i que continuen tenint certes limitacions de memòria i còmput, les quals fan que sigui convenient qualsevol disminució de les necessitats computacionals i de memòria dels algorismes criptogràfics que tenen implementats, i, és clar, sense que aquestes disminucions redueixin la seguretat.

3.1.1 Evolució de les targetes intel·ligents

A finals dels seixanta es va desenvolupar la targeta magnètica convencional per satisfer diverses necessitats. Una era permetre que els clients dels bancs i les entitats financeres accedissin i operessin de forma ràpida en els caixers automàtics. Una altra necessitat era proporcionar un medi amb el qual operar en punts de venda específics.

L'objectiu principal d'aquestes targetes era identificar un client per accedir a una base de dades remota i establir-hi una connexió. La informació que posseïa la base de dades permetia acceptar o rebutjar la transacció que es volia realitzar.

Les targetes magnètiques oferien una molt baixa densitat de dades, poca fiabilitat i poca seguretat o cap de la informació que tenia emmagatzemada. Això, juntament amb les noves necessitats del mercat, que no podien satisfer, va fer aparèixer les targetes intel·ligents (Figura 3.1).

Aquestes noves targetes donen més seguretat, ja que poden llegir, i fins i tot manipular, les dades que contenen. Això és gràcies a un xip que tenen integrat i a una sèrie de punts de contacte per poder establir una comunicació entre el terminal i la targeta intel·ligent. El xip integrat té una estructura interna més complexa que la banda magnètica. Aquest xip conté un microprocessador encastat que fa que les possibilitats de manipulació fraudulenta de les dades sigui més reduïda, ja que dota la targeta d'una certa seguretat, i la fa, alhora, més resistent al deteriorament per causes externes de la informació emmagatzemada. A més a més, augmenta la capacitat d'emmagatzemar informació perquè de controla diversos mòduls de memòria.

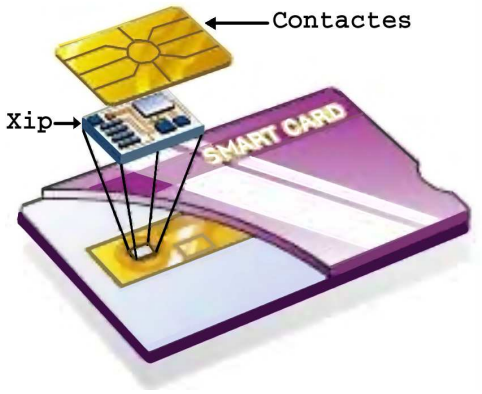


Figura 3.1: Estructura d'una targeta intel·ligent (imatge extreta d'Internet)

3.1.2 Estructura de les targetes intel·ligents

Les targetes intel·ligents treballen sobre un sistema operatiu emmagatzemat en el xip, que és l'encarregat de gestionar totes les operacions que es realitzen i sobre el qual s'executen els diversos programes que conté. Aquest xip inclou, dins, diversos elements, i els més importants són el microprocessador, una memòria ROM emmascarada, un mòdul d'EEPROM, un mòdul de RAM, un port d'entrada/sortida i una CPU.

En la ROM (Read Only Memory) emmascarada hi ha el sistema operatiu de la targeta, que es grava durant el procés de fabricació. El sistema operatiu controla l'accés als arxius del sistema i als programes. Aquesta memòria no pot ser alterada.

L'EEPROM (Electrically Erasable Programmable Read Only Memory) és una memòria no volàtil del microprocessador, en que hi trobem les dades de l'usuari o de l'aplicació , així com el codi de les instruccions que estan sota el control del sistema operatiu. També pot contenir informació, com el nom de l'usuari, el número d'identificació personal (PIN),... Aquesta memòria pot ser de 128 Kbits a 256 Kbits.

La RAM (Random Access Memory) és la memòria de treball del microprocessador. Com que és volàtil es perd tota la informació que conté quan la targeta es desconnecta de la font d'alimentació, per tant, s'utilitza per emmagatzemar registres de forma temporal pel microprocessador.

El port d'entrada/sortida, normalment, consisteix en un registre a través del qual la informació és transferida bit a bit.

En la comunicació entre el xip targeta i el terminal lector hi apareix en els punts de contacte. Les característiques d'aquests contactes, així com la ubicació dins de la targeta i els protocols dels senyals elèctrics i la seva transmissió, estan establertes per la norma ISO 7816.

Figura 3.2: Estructura dels punts de contacte de la targeta intel·ligent

L'assignació de contactes que dóna la norma ISO 7816 és la de la Figura 3.2 i les assignacions són les següents:

Vcc: Entrada de corrent.

RST: (Reset) Reinicia el senyal enviat únicament pel terminal o conjuntament amb un restabliment intern.

CLK: (Clock) Senyal de rellotge.

RFU: Reservat per a usos futurs.

GND: (Ground) Terra (referència de voltatge).

Vpp: Voltatge de programació d'entrada.

I/O: Entrada o sortida de les dades del xip de la targeta intel·ligent.

No totes les targetes intel·ligents contenen aquests punts de contacte per a la comunicació entre aquestes i el terminal. Dins de les targetes intel·ligents hi ha també targetes que es comuniquen amb el terminal mitjançant ones de radiofreqüència. Aquestes targetes són conegudes com targetes de no contacte o *contactless cards*.

3.2 Criptografia amb corbes el·líptiques

La criptografia de clau pública es basa en la intractabilitat de certs problemes matemàtics, dels quals podem destacar per a aquest ús el problema de la factorització entera i el problema del logaritme discret (DLP). Dins del esquemes criptogràfics més usats, basats en factorització, podem destacar el RSA, mentre que en el cas del problema del logaritme discret els més utilitzats són els criptosistemes del tipus ElGamal [EG85]. Aquests criptosistemes basen la seva seguretat en el DLP: donat un grup cíclic G, un generador g de G i un element $g' \in G$, cal trobar un enter n de manera que $g^n = g'$.

En la dècada dels 80, N. Koblitz [Kob87] i V. Miller [Mil86] van proposar introduir el grup de punts d'una corba el·líptica definida sobre un cos finit com a grup on plantejar el DLP. A partir d'això, han estat molts els esquemes criptogràfics que han incorporat corbes el·líptiques per diversos motius. Normalment, en criptografia, es treballa amb corbes definides sobre cossos finits i bàsicament sobre cossos primers, és a dir, sobre $\mathbb{F}_p$, amb p primer, o cossos binaris, és a dir, $\mathbb{F}_{2^n}$.

Els criptosistemes amb corbes el·líptiques que s'utilitzen són el de tipus ElGamal, és a dir, criptosistemes que basen la seva seguretat en la intractabilitat del problema del logaritme discret el·líptic (ECDLP). Els avantatges que ens donen aquests criptosistemes són, entre altres, l'ús de claus amb mida molt inferior als criptosistemes convencionals de clau pública, així com permetre canviar de grup sense haver de canviar de cos, és a dir, amb la mateixa aritmètica modular [BSS99, BSS05, Rio09].

El fet que en aquests criptosistemes emprin claus de mida més petita és deu al fet que hi ha atacs que afecten la criptografia convencional i per als quals no se n'han trobat les variants el·líptiques. De fet, els atacs existents en l'actualitat, que es poden aplicar en qualsevol grup coneguts fins ara són la ρ de Pollard i la λ de Pollard [Pol78]; en el cas de la criptografia el·líptica, aquests atacs necessiten uns $\sqrt{\pi n/4}$ passos per trencar el criptosistema en el cas de la ρ de Pollard, mentre que la λ de Pollard empra uns $2\sqrt{n}$ passos. En el cas del DLP sobre el grup multiplicatiu d'un cos finit i la factorització entera apareixen altres atacs més eficients que els anteriors. Són l'*Index Calculus* [SS98] per al

DLP sobre el grup $\mathbb{F}_p^*$ i el *Number Field Sieve* [LLMP90] que s'utilitza per atacar el RSA [RSA78], que fan que trencar un criptosistema basat en aquests problemes sigui encara més ràpid que amb els anteriors atacs. Així, malgrat que tant la ρ de Pollard com la λ de Pollard poden ser paral·lelitzables, continua sent molt més costós trencar un criptosistema basat en el ECDLP que en el DLP o en el problema de la factorització entera, fet que obliga a treballar amb claus molt més grans quan s'utilitzen criptosistemes basats en el DLP o la factorització entera que quan s'utilitzen basats en el ECDLP.

Un altre factor que s'ha de tenir en compte és la factorització de l'ordre del grup multiplicatiu d'un cos finit, en el cas del DLP, i sobre el grup de punts d'una corba el·líptica, en el cas del ECDLP, atès que existeix l'atac de Pohlig-Hellman [PH78]. En cas que la factorització de l'ordre del grup no tingui cap primer gran com a factor, l'algorisme de Pohlig-Hellman redueix de forma eficient el càlcul del problema de DLP o del ECDLP a logaritmes discrets per als subgrups d'ordre primer que divideixin l'ordre del grup amb el qual es treballa.

Un dels criptosistemes més utilitzat basat en el ECDLP és el conegut com ECIES (*Elliptic Curve Integrated Encryption Scheme*) proposat per M. Bellare i P. Rogaway [BR97], estandarditzat en ANSI X9.63, ISO/IEC 15946-3 i IEEE P1363a. El seu funcionament és el següent:

Algorisme 1 Xifrar amb ECIES

Entrada: Els paràmetres $(q, FR, S, a, b, P, n, h)$, el punt Q i el missatge en clar m

Sortida: El missatge xifrat (R, C, t)

1 Elegir un enter aleatori $k \in [1, n-1]$;
2 Calcular els punts $R = k \cdot P = (\alpha_1, \alpha_2)$ i $Z = h \cdot k \cdot Q = (\beta_1, \beta_2)$;
3 Calcular $(k_1, k_2) \leftarrow KDF(\beta_1, R)$;
4 Calcular $C = ENC(m, k_1)$ i $t = MAC(C, k_2)$;
5 **retorna** (R, C, t);

Els paràmetres k_1 i k_2 són claus de sessió utilitzades per realitzar un xifratge de clau privada i per autenticar el procés de desxifratge, respectivament.

D'altra banda, el procés per desxifrar aniria de la forma següent:

Algorisme 2 Desxifrar amb ECIES

Entrada: El missatge xifrat (R, C, t), els paràmetres $(q, FR, S, a, b, P, n, h)$, la clau privada d

Sortida: El missatge en clar m

1 Calcular el punt $Z = d \cdot h \cdot R = (\beta_1, \beta_2)$;
2 Calcular $(k_1, k_2) \leftarrow KDF(\beta_1, R)$;
3 Calcular $t' = MAC(C, k_2)$;
4 Calcular $m = DEC(C, k_1)$;
5 **retorna** m;

Les funcions utilitzades pel criptosistema ECIES són:

- KDF (*Key Derivation Function*): És una funció de derivació de claus construïda a partir d'una funcio Hash.

- ENC: És un xifratge de clau simètrica, com pot ser el criptosistema AES.

- MAC: Ens dóna un missatge retornat per un algorisme d'autenticació de codi, com pot ser un HMAC.

- DEC: És el procés de desxifratge utilitzant el mateix criptosistema simètric emprat en el procés de xifratge.

3.3 Criptografia el·líptica per a targetes intel·ligents

A part de les components que s'han citat del xip, hi ha targetes intel·ligents que tenen també un mòdul criptogràfic dins del xip. Aquest mòdul afavoreix poder utilitzar de forma més eficient diversos algorismes criptogràfics, donar seguretat a les dades emmagatzemades dins de la targeta permetent i, a més, que la persona o entitat titular d'aquesta targeta pugui autenticar-se. Així, l'ús

de les targetes intel·ligents permet que els serveis que aquestes proporcionen es facin de forma segura.

Ara bé, el fet que la targeta hagi d'emmagatzemar les claus utilitzades pels protocols criptogràfics va en detriment de la mida de les dades que es podran emmagatzemar després.

Les targetes intel·ligents utilitzen majoritàriament el RSA com a protocol criptogràfic. Aquest protocol necessita claus de mida relativament gran, claus de 1.024 o 2.048 bits; ara bé, el xip de la targeta és de mida reduïda, i fa que la seva capacitat d'emmagatzematge sigui molt limitada. No obstant això, la majoria de targetes intel·ligents que hi ha ara al carrer tenen implementats criptosistemes RSA amb claus de 512 bits, una mida de clau que està totalment obsoleta. Sols fa un parell d'anys que es van posar al carrer targetes que tenien implementats criptosistemes RSA amb claus de 1.024 bits, una mida que, actualment, comença a qüestionar-se.

Una solució a aquests problemes d'espai de memòria ha estat incorporar criptosistemes basats en corbes el·líptiques, ja que ofereixen una seguretat com la que dóna el RSA amb claus molt més reduïdes (vegis Taula 3.1 donada pel NIST [NIS03]), deixant, d'aquesta manera, més espai per emmagatzemar dades no relacionades amb el protocol criptogràfic.

RSA	ECC	Ràtio
512	112	1:4,5
1.024	160	1:6
15.360	512	1:30

Taula 3.1: Comparativa de mides de claus del RSA i ECC per una mateixa seguretat

A més a més, existeixen mòduls enfocats específicament a criptosistemes basats sobre corbes el·líptiques, cosa que fa que les operacions que fan aquests protocols vagin més ràpides, ja que estan optimitzats per part d'aquestes. Les operacions que es realitzen en aquests protocols són la suma de dos punts i el doblat d'un punt vistos en el capítol anterior, més concretament, al 2.11 i al 2.12.

Normalment, el criptosistema més implementat del tipus el·líptic és ElGamal [EG85], basat en el problema del logaritme discret el·líptic. El seu esquema de funcionament és el següent:

Algorisme 3 Protocol ElGamal el·líptic

Entrada: Els paràmetres de la corba a, b, el primer p, un punt $P \in E(\mathbb{F}_q)$, el grau de la corba n, la clau pública $Q = d \cdot P$ i el missatge en clar m ;
Sortida: El missatge xifrat $(x_1, y_1, m \cdot x_2)$;

1 Elegir un nombre aleatori $r \in [1..n-1]$;
2 Calcular $r \cdot P = (x_1, y_1]$ i $r \cdot Q = (x_2, y_2)$ en $E(\mathbb{F}_q)$;
3 Calcular $m \cdot x_2$ en $E(\mathbb{F}_q)$;
4 **retorna** $(x_1, y_1, m \cdot x_2)$;

Ara veurem, en pseudocodi, com serien les operacions bàsiques necessàries per realitzar les multiplicacions que hi apareixen d'un punt de la corba per un escalar. Denotem com $ECCADD(P_1, P_2)$ la suma dels punts P_1 i P_2 (2.11) i $ECCDBL(P_1)$ el doblat d'un punt P_1 (2.12). L'algorisme que hauria de fer la targeta intel·ligent seria:

Algorisme 4 Protocol sobre corbes el·líptiques amb suma i doblat

Entrada: $d = (d_{n-1} \cdots d_1 d_0)_2$: nombre enter en binari de manera que $d_{n-1} = 1$;
$P \in E(\mathbb{K})$;
Sortida: dP: d vegades el punt P;

1 $Q \leftarrow P$;
2 **per a** $i \in [n-2..0]$ **fer**
3 $Q \leftarrow ECCDBL(Q)$;
4 **si** $d_i = 1$ **llavors**
5 $Q \leftarrow ECCADD(Q, P)$;
6 **fi**
7 **fi**
8 **retorna** Q;

En aquest algorisme, únicament es fa la suma de dos punts quan el valor del bit que es tracta de d pren el valor d'1; en canvi, independentment del valor del bit tractat, sempre es fa el doblat del punt Q.

En la següent secció veurem que aquest algorisme es pot atacar de forma no gaire complicada. Així mateix, es donarà una versió resistent a aquest atac.

3.4 Atacs *Side-Channel* en targetes intel·ligents

Com ja s'ha dit, les targetes intel·ligents estan formades per un xip de silici, amb unes característiques que el fan susceptible de ser atacat de diverses formes: extraient el xip i manipulant-lo o, simplement, observant-ne el comportament i utilitzant la informació que revela en aquest procés. Aquestes dos formes d'atacar una targeta intel·ligent ens deixen una primera classificació dels atacs [SA03, BJ02]. Així, podem parlar d'*atacs invasius* i *no invasius*.

Els atacs invasius impliquen que hi hagi un accés directe al xip per poder-ne manipular les components. Per aconseguir-ho s'ha d'extreure aquest xip de la targeta físicament. En els atacs no invasius, d'altra banda, solament s'utilitza la informació que ens pot donar la targeta sense haver-la de manipular ni desmuntar. Aquesta informació s'obté de les emissions que la targeta crea quan realitza alguna operació en alguna aplicació que s'estigui executant en aquell moment en la targeta.

La majoria de targetes estan equipades amb mecanismes per evitar els atacs invasius, i deixen de funcin onar si la targeta detecta alguna manipulació del xip. Per contra, les targetes no són capaces d'adonar-se de quan són víctimes d'un atac no invasiu, ja que aquests són completament indetectables per la targeta. Això impossibilita la tasca d'intentar evitar aquests atacs únicament quan es produeixin, com en el cas anterior, i això obliga a utilitzar contramesures en tot cas, sigui fraudulent o verídic.

En [SA03] també apareixen en la classificació els atacs *semi invasius*. Aquests atacs necessiten extreure el xip, però no una manipulació d'aquest.

A part d'aquesta primera classificació, els atacs a targetes intel·ligents poden classificar-se depenent de l'actitud de l'atacant [QS02]; així, tenim *atacs actius* i *atacs passius*. En el primer cas, l'atacant intenta, per exemple, introduir errors en els càlculs que realitza la targeta. Altrament, en els atacs passius

el paper de l'atacant és simplement observar el comportament i utilitzar informació obtinguda dels còmputs de la targeta per obtenir informació sobre el criptosistema, informació que pot arribar a ajudar a trencar el criptosistema. Aquesta informació es coneix com *informació Side-Channel* i els atacs que utilitzen aquestes traces d'informació s'anomenen *atacs Side-Channel*.

La informació *Side-Channel* és conseqüència del fet que una targeta intel·ligent no té cap bateria ni pila interna que la proveeixi de la potència necessària per realitzar les operacions que té implementades. Per tant, necessita un lector que els doni l'energia que requereixen per efectuar les tasques pertinents. Aquest ús del lector implica que un atacant pot obtenir dades que desprèn la targeta quan aquesta s'utilitza de forma relativament fàcil [Kel02]. A més a més, els atacs de *Side-Channel* poden utilitzar diversos tipus d'informació (potència consumida, temps transcorregut,...), extrets d'execucions de la targeta sense que aquests siguin excloents entre si. Així, depenent de la informació que utilitzin, podem classificar els atacs *Side-Channel* com:

Atacs de potència de consum: Aquests atacs [CJRR03, MOP06] estan basats a analitzar la potència de consum de la targeta mentre aquesta està treballant. Ja sigui mitjançant una anàlisi de poques o moltes traces d'informació, un atacant pot saber quins processos estan passant dins del dispositiu i obtenir una informació que, combinada amb la que es pot obtenir d'altres tècniques de criptoanàlisi, pot ajudar a recuperar la clau secreta. Aquests atacs, alhora, es poden dividir en dos grans grups, depenent del nombre de traces que tenen en compte i dels mètodes usats per tractar-les:

Simple Power Analysis: Es basa a interpretar la informació visual d'una o poques traces obtingudes mentre la targeta realitzava un procés criptogràfic. Aquest atac ajuda a obtenir informació sobre les seqüències de les instruccions executades.

Differential Power Analysis: En aquest atac [KJJ99, BMM00] s'observen un conjunt de traces de consum de potència i, a partir de mètodes estadístics, i mirant les variacions de consum que hi ha, s'intenta obtenir informació de la clau i, fins i tot, obtenir la clau

utilitzada trencant, així, el criptosistema.

Atacs de temps: En aquests atacs [Sch00, Koc96], el que fa l'atacant és mesurar els temps que la targeta necessita per realitzar les instruccions. A partir d'aquestes mesures, i coneixent quan temps de mitjana necessita la targeta per executar diferents instruccions, l'atacant pot extreure informació sobre la naturalesa d'aquestes operacions i de la clau privada. L'atacant coneix aquesta mitjana, ja que, al principi, haurà enviat a la targeta una sèrie de missatges per poder fer una estimació del temps de cada operació que realitza, i així sap el que tarda a executar cada operació.

Atacs electromagnètics: Aquest tipus d'atac va ser introduït per J. J. Quisquater i D. Samyde [QS01] el 2001. Utilitza el fet que el xip que té incorporat una targeta intel·ligent és de silici, un semiconductor; quan a aquest xip se li introdueix una¡ corrent elèctric, aleshores genera un camp elèctric al seu voltant; radiacions electromagnètiques que tenen diferents característiques depenent del treball que s'estigui realitzant en cada moment. Aquestes ones electromagnètiques poden ser les que genera el mateix xip o també es poden induir posant un corrent extern a la targeta. Mirant aquestes radiacions, es pot obtenir també informació sensible que pot portar a trencar l'algorisme criptogràfic de la targeta. La forma d'analitzar aquestes radiacions és igual que en els atacs de potència de consum i, per tant, també podem parlar de *Simple* i *Differential Electromagnetic Attacks* (SEMA i DEMA)[AARR03].

Aquests atacs poden donar-se en qualsevol tipus d'algorismes criptogràfics, ja siguin simètrics o asimètrics, així com també en els criptosistemes basats en corbes el·líptiques.

3.4.1 Contramesures als atacs *Side-Channel*

Els atacs *Side-Channel* s'intenten evitar o pal·liar introduint a la implementació dels criptosistemes i a la targeta en si mecanismes de protecció o contramesures que facin que no es pugui utilitzar la informació *Side-Channel* o que

sigui errònia i inservible, eliminant així la relació existent entre la clau i l'algorisme. Les formes més emprades d'aconseguir aquesta tasca són *emmascarar* la informació o *ocultar-la* [Mes01, Mer78].

El primer tipus introdueix valors aleatoris en les operacions, que després revertiran, perquè la clau quedi emmascarada sense que el resultat final canviï, mentre que el segon tipus introdueix retards aleatoris o operacions innecessàries perquè l'atacant no pugui tenir un patró per saber què està fent i quan ho fa la targeta. Aquestes contramesures normalment estan implementades via software, encara que n'hi ha algunes que es poden implementar via hardware.

En el cas de contramesures via software, les més utilitzades intenten obligar que el flux d'execució sigui tan constant com es pugui. En altres paraules, que la potència consumida no vagi estrictament lligada a la clau o a l'algorisme que s'usa. També és molt comú afegir-hi aleatorietat introduint soroll executant operacions aleatòries que no tindrien per que fer-se.

D'altra banda, les contramesures via hardware intenten desincronitzar els tics del rellotge intern perquè no es pugui fer un patró de l'algorisme criptogràfic ni tenir una idea de la mida de la clau, o fins i tot introdueixen un altre conjunt de components per balancejar la feina que ha de fer el microprocessador.

Pel que fa als criptosistemes basats en corbes el·líptiques, les contramesures més comuns són les proposades per J. S. Coron [Cor99] i les proposades per Joye-Tymen [JT01]. El que proposen és aleatoritzar el punt de la corba multiplicant el punt inicial per un escalar i treballar amb aquest, canviar a una corba isomorfa i passar-hi el punt al seu equivalent o, fins i tot, canviar el cos on està definida la corba.

3.4.2 Atacs *Side-Channel* en criptosistemes basats en corbes el·líptiques i contramesures

Els criptosistemes amb corbes el·líptiques tampoc s'escapen de ser atacats mitjançant l'obtenció d'informació *Side-Channel*. En aquest cas particular de criptosistemes, el que es vol atacar de la targeta intel·ligent és el valor de l'escalar d pel qual multipliquem el punt P de la corba el·líptica, de manera

com podem veure en l'Algorisme 4. Per obtenir aquest valor, l'atacant utilitza el fet que costa molt més, computacionalment parlant, fer una suma de dos punts que el doblat d'un punt. Per tant, si s'observa el consum de la targeta, un atacant pot saber en quina posició, el paràmetre d, pren valor 0 o 1, això fa que es pugui obtenir el valor de d sense gaire dificultat.

La solució més senzilla a aquest atac, que ja s'implementa en les targetes intel·ligents, és intentar que no es noti aquesta diferència. Per aconseguir ocultar aquesta diferència de consum el que s'ha de fer és que la targeta calculi en tot cas el doblat i la suma, encara que el bit que es tracti sigui un 0, així la potència serà similar en tots els casos sense donar informació dels bits de d. L'Algorisme 4 amb aquesta contramesura quedaria:

Algorisme 5 Protocol sobre corbes el·líptiques amb suma i doblat (sempre)

Entrada: $d = (d_{n-1} \cdots d_1 d_0)_2$: nombre enter en binari de manera que $d_{n-1} = 1$;
$P \in E(\mathbb{K})$;
Sortida: dP: d vegades el punt P;

```
1 Q[0] ← P;
2 per a i ∈ [n − 2..0] fer
3     Q[0] ← ECCDNL(Q[0]);
4     Q[1 − d_i] ← ECCADD(Q[0], P);
5 fi
6 retorna Q[0];
```

Es pot observar que en el cas que $d_i = 0$, cas en què en 4 no es feia la suma, el resultat d'aquesta s'emmagatzemarà en $Q[1]$, un punt auxiliar que no s'utilitza en cap lloc de l'algorisme, amb el qual tindrem que la suma no es tindrà en compte. Això no passa en el cas contrari, quan $d_i = 0$. En aquest cas la suma s'emmagatzemarà en $Q[0]$ retornant, després de l'execució, al mateix punt que ens retornaria l'algorisme anterior.

Emprant aquest algorisme, també apareix un atac específic per a criptosistemes sobre corbes el·líptiques conegut com atac de punt amb valor zero (*Zero-Value Point Attack*). Aquest atac s'explota el fet que si alguns paràmetres emprats en la suma i el doblat d'un punt són zero, el consum baixa considerablement, fins al punt que un atacant pot obtenir informació útil per

trencar el criptosistema usat. S'aprofundirà més en aquest atac en el Capítol 6, en què es donarà un algorisme que busqui corbes que compleixin una sèrie de condicions perquè els paràmetres intermedis dels quals s'ha parlat no puguin ser zero.

Capítol 4

Volcans d'isogènies de corbes el·líptiques

D. Kohel i M. Fouquet, en les seves respectives tesis [Koh96, Fou01], van ser els primers que van estudiar l'estructura dels volcans d'isogènies de corbes el·líptiques. En aquest capítol, es parteix de l'estudi iniciat en la tesi de D. Sadornil [Sad04], on trobem un extensiu estudi dels volcans d'isogènies de grau 2 amb les seves característiques. Seguint aquests resultats, en aquesta tesi, es caracteritza l'altura d'un volcà de ℓ-isogènies de corbes el·líptiques a partir de la valoració ℓ-àdica del cardinal de la corba, per un primer ℓ qualsevol, i es tracta detalladament el cas de volcans d'isogènies de grau 3.

4.1 Estructura d'un volcà

Abans d'entrar a definir què s'entén per *volcà d'isogènies de corbes el·líptiques*, donarem la noció de direcció d'una isogènia que es necessitarà per construir-lo. Així doncs, donada una isogènia $\mathcal{I}$ de grau ℓ entre dos corbes el·líptiques E i E' sobre un cos finit, és a dir, una ℓ-isogènia, Kohel [Koh96] va demostrar que l'índex dels seus anells d'endomorfismes $[\mathcal{O} : \mathcal{O}']$ = 1, ℓ, o $\frac{1}{\ell}$. Així, es pot dir que la isogènia $\mathcal{I}$ és *horitzontal*, *descendent* o *ascendent*, segons que l'índex sigui 1, ℓ o $\frac{1}{\ell}$, respectivament.

A partir d'aquesta noció de direcció de les isogènies, començant per una corba $E/\mathbb{F}_q$ i considerant totes les seves ℓ^k-isogènies, obtenim un graf on els no-

des representen classes d'isomorfia de corbes el·líptiques, mentre que les arestes representen ℓ-isogènies entre classes d'isomorfia. A aquest graf se l'anomena *volcà de ℓ-isogènies*, o bé *ℓ-volcà*, per la seva peculiar forma.

Aquests grafs contenen un únic cicle anomenat *cràter*. De cadascun dels nodes que forma el cràter hi pengen $\ell - 1$ arbres ℓ-aris, tots amb la mateix altura. Les fulles de tots aquests arbres es troben al mateix nivell i se les anomena *terra* del ℓ-volcà. Els altres nodes dels arbres es diu que estan al *vessant* del volcà. Tots els nodes, excepte els que formen el terra, tenen $\ell + 1$ arestes.

Es pot observar l'estructura d'un ℓ-volcà en un cas particular amb $\ell = 3$ en la figura següent:

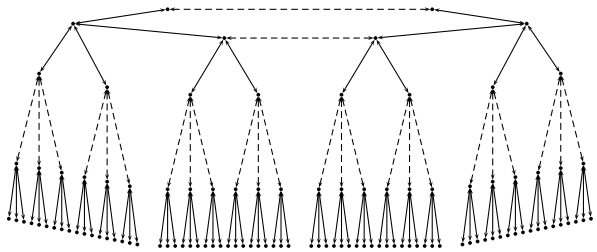


Figura 4.1: Estructura d'un 3-volcà

En la Secció 2.7 del Capítol 2 es dóna el nombre de ℓ-isogènies que pot tenir una corba, concretament, 0, 1, 2 o $\ell + 1$. Així les corbes del terra són les que únicament tenen una isogènia, mentre que les del vessant i les del cràter en tenen $\ell + 1$. Ara bé, hi ha un cas particular de volcans en què els nodes únicament tenen 2 arestes. A aquests volcans se'ls anomena *volcans plans*, i passa quan el cràter està situat al terra, en altres paraules, el volcà sols té cràter.

D. Kohel va especificar en la seva tesi el nombre de ℓ-isogènies que hi ha de cada tipus d'una corba d'un volcà segons el seu anell d'endomorfismes.

Sigui doncs E una corba el·líptica ordinària definida sobre $\mathbb{F}_q$ d'ordre m i sigui $\mathcal{O}$ el seu anell d'endormorfismes. Aleshores, $\mathcal{O}$ és un ordre del cos quadràtic imaginari de $\mathbb{K} = \mathbb{Q}(\sqrt{t^2 - 4q})$ [Hus04], en que t és la traça de l'endomorfisme de Frobenius π de E, que satisfà:

$$\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{K}},$$

on $O_{\mathbb{K}}$ és l'anell d'enters de $\mathbb{K}$. Si D és el discriminant de l'ordre $\mathcal{O}$, aleshores D. Kohel en [Koh96] dóna el següent resultat sobre el nombre de ℓ-isogènies de cada tipus:

Cas		Tipus	Nombre total
$\ell \nmid [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D}{\ell}\right) \quad \rightarrow$	$1 + \left(\frac{D}{\ell}\right)$
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 + \left(\frac{D}{\ell}\right) & \rightarrow \\ \ell - \left(\frac{D}{\ell}\right) & \downarrow \end{cases}$	$\ell + 1$
$\ell \mid [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 \quad \uparrow$	1
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 & \uparrow \\ \ell & \downarrow \end{cases}$	$\ell + 1$

Taula 4.1: Tipus d'isogènies de grau ℓ

denota que amb ($\uparrow$) si la isogènia $\mathcal{I}$ de la corba E a E' és ascendent, ($\downarrow$) si la isogènia és descendent i, finalment, ($\rightarrow$) si la isogènia entre aquestes dos corbes és horitzontal.

4.1.1 Altura d'un ℓ-volcà

Sigui E una corba el·líptica ordinària definida sobre $\mathbb{F}_q$ d'ordre m. Es pot observar que si d és la part lliure de quadrats del discriminant de l'endomorfisme de Frobenius

$$d_\pi = t^2 - 4q = f_0^2 d,$$

aleshores [Koh96] el conductor f de l'ordre $\mathbb{Z}[\pi]$ ve donat per:

$$f = \begin{cases} f_0, & d \equiv 1 \pmod 4, \\ \frac{f_0}{2}, & d \equiv 2, 3 \pmod 4. \end{cases}$$

Si denotem $V_\ell(E/\mathbb{F}_q)$ el ℓ-volcà associat a la corba $E/\mathbb{F}_q$ construït mitjançant el càlcul de ℓ-isogènies, aleshores tenim que totes les corbes el·líptiques que pertanyen a aquest ℓ-volcà tenen el mateix conductor f de l'ordre $\mathbb{Z}[\pi]$. Per tant, l'altura del ℓ-volcà, $h(V_\ell(E/\mathbb{F}_q))$, depèn d'aquests elements. Precisament, es pot deduir de [FM02, Wit01] que:

$$h(V_\ell(E/\mathbb{F}_q)) = v_\ell(f).$$

Així doncs, per analitzar l'altura d'un ℓ-volcà és útil estudiar les característiques de f. Per tant, l'estudi de la valoració ℓ-àdica de d_π proporcionarà informació sobre $v_\ell(f)$. En aquesta secció se suposarà que les corbes el·líptiques sempre tenen algun punt racional d'ordre ℓ. Atesa aquesta condició, sempre tindrem que $v_\ell(m) \geq 1$.

Cal dir que es pot obtenir la valoració ℓ-àdica $v_\ell(m)$ del cardinal de la corba sense conèixer el cardinal m, calculant el subgrup de ℓ-Sylow de la corba. A la tesi de R. Moreno [Mor05], així com als treballs [MMRV05, MMRV08] es donen algorismes que, a partir dels punts de ℓ-torsió de la corba, determinen l'estructura del subgrup de ℓ-Sylow i, en particular, $v_\ell(m)$.

Abans d'entrar en el cas més general de $\ell > 2$, es donaran els resultats vistos en [Sad04, MMS$^+$06] per al cas particular de $\ell = 2$. En aquest cas, els resultats es donen, segons $q \equiv 1 \pmod 4$ o bé $q \equiv 3 \pmod 4$:

Proposició 4.1. *Sigui E una corba el·líptica ordinària definida sobre $\mathbb{F}_q$ d'ordre m amb $v_2(m) > 2$. Si $q \equiv 1 \pmod 4$ se satisfà:*

i) Si $v_2(m) \geq 2v_2(q-1)$, aleshores $h(V_2(E/\mathbb{F}_q)) = v_2(q-1)$.

ii) Si $v_2(m) = 2v_2(q-1) - 1$, aleshores $h(V_2(E/\mathbb{F}_q)) = v_2(q-1) - 1$.

iii) Si $v_2(m) = 2v_2(q-1) - 2$, aleshores $h(V_2(E/\mathbb{F}_q)) \geq v_2(q-1) - 1$.

iv) Si $v_2(m) \leq 2v_2(q-1) - 3$, aleshores $h(V_2(E/\mathbb{F}_q)) = (v_2(m) - 1)/2$ si

$v_2(m)$ és senar o bé $h(V_2(E/\mathbb{F}_q))$ és igual a $v_2(m)/2$ o a $(v_2(m)+2)/2$ si $v_2(m)$ és parell.

Si $v_2(m) > 2$ i $q \equiv 3 \pmod 4$ el 2-volcà té $h(V_2(E/\mathbb{F}_q)) = 1$.

La Proposició 4.1 únicament dóna informació per als casos en que $v_2(m) > 2$. En el cas $v_2(m) = 2$ es pot obtenir estudiant l'altura del volcà corresponent a la corba *twisted* de $E/\mathbb{F}_q$, $E^t/\mathbb{F}_q$ [Hus04, Sil86]. De fet, resulta fàcil veure que el volcà $V_2(E/\mathbb{F}_q)$ és isomorf a $V_2(E'/\mathbb{F}_q)$; per tant:

$$h(V_2(E/\mathbb{F}_q)) = h(V_2(E'/\mathbb{F}_q)).$$

En cas que $q \equiv 1 \pmod 4$, si $v_2(|E(\mathbb{F}_q)|) = 2$ aleshores $v_2(|E^t(\mathbb{F}_q)|) > 2$ (això es deu al fet que $v_2(|E(\mathbb{F}_q)| + |E^t(\mathbb{F}_q)|) = v_2(2(q+1)) = 2$). Per tant, la Proposició 4.1 és pot utilitzar per estudiar $h(V_2(E^t/\mathbb{F}_q))$, per obtenir el resultat en aquest cas particular.

També cal dir que en la Proposició 4.1 no es tracta el cas $v_2(m) = 1$. Això es deu al fet que en aquest cas totes les corbes que formen el 2-volcà satisfan que $\chi(\rho) = -1$, i, per tant, $h(V_2(E/\mathbb{F}_q)) = 0$. Més concretament, en aquest cas, el 2-volcà està format per dos nodes units per un parell d'isogènies duals.

Ara generalitzarem aquests resultats quan $\ell \geq 3$:

Teorema 4.2. *Sigui E una corba el·líptica definida sobre un cos $\mathbb{F}_q$ d'ordre m amb $v_\ell(m) \geq 1$. Si $v_\ell(q-1) \geq 1$ i $\ell \geq 3$ se satisfà:*

i) Si $v_\ell(m) > 2v_\ell(q-1)$, aleshores $h(V_\ell(E/\mathbb{F}_q)) = v_\ell(q-1)$.

ii) Si $v_\ell(m) = 2v_\ell(q-1)$, aleshores $h(V_\ell(E/\mathbb{F}_q)) \geq v_\ell(q-1)$.

iii) Si $v_\ell(m) < 2v_\ell(q-1)$, aleshores $h(V_\ell(E/\mathbb{F}_q)) = (v_\ell(m)-1)/2$ quan $v_\ell(m)$ és senar o $h(V_\ell(E/\mathbb{F}_q)) = v_\ell(m)/2$ quan $v_\ell(m)$ és parell.

Altrament, si $v_\ell(q-1) = 0$ aleshores $h(V_\ell(E/\mathbb{F}_q)) = 0$.

Demostració. El fet que $t^2 - 4q = (q-1)^2 - m[m - 2(q-1) - 4]$ comporta que $v_\ell(t^2-4q) \geq \min\{2v_\ell(q-1), v_\ell(m)\}$. El valor de $v_\ell(t^2-4q)$ està determinat, sempre i que no ens trobem en el cas $2v_\ell(q-1) = v_\ell(m)$. Per a aquest segon

cas, aquesta situació propicia que únicament es pugui donar la cota inferior de l'altura del volcà. Si ens trobéssim en el tercer cas, l'altura només pot ser dos possibles valors depenent de la paritat de $v_\ell(m)$.

En el cas que $v_\ell(q-1)=0$, podem obtenir $v_\ell(t^2-4q)=0$. A més a més, tenim que t^2-4q és un residu quadràtic mòdul ℓ. Aleshores, el polinomi modular $\phi_\ell(x,j)$, sent j el j-invariant d'$E/\mathbb{F}_q$, té exactament dos arrels quadrades [BSS99], és a dir, la corba $E/\mathbb{F}_q$ tindrà exactament dos ℓ-isogènies. Com a conseqüència, la corba $E/\mathbb{F}_q$ ha d'estar al cràter del ℓ-volcà i, com que aquesta situació és la mateixa amb la qual es trobaran totes les corbes pertanyents a aquest ℓ-volcà, tenim que l'altura $h(V_\ell(E/\mathbb{F}_q))=0$.

□

4.1.2 Localització de les corbes el·líptiques en $V_\ell(E/\mathbb{F}_q)$ depenent del seu subgrup de ℓ-Sylow

En aquesta secció es veuran més detalls sobre l'estructura d'un volcà de ℓ-isogènies depenent dels subgrups de ℓ-Sylow de les corbes que el formen.

Primer de tot, es pot observar que les corbes que componen el terra del volcà són, precisament, aquelles que el seu subgrup de ℓ-Sylow és cíclic. Això es deu al fet que aquestes corbes són les úniques que tenen una o dos ℓ-isogènies.

Sigui E una corba definida sobre un cos $\mathbb{F}_q$ d'ordre m, i sigui $\mathcal{O}$ l'anell d'endomorfismes de $E/\mathbb{F}_q$, tenim que, l'anell d'enters de $\mathbb{K}$ és $\mathcal{O}_\mathbb{K}=\mathbb{Z}\oplus\mathbb{Z}\omega$, en què:

$$\omega=\begin{cases}\dfrac{1+\sqrt{d}}{2}, & d\equiv 1 \pmod 4,\\ \sqrt{d}, & d\equiv 2,3 \pmod 4.\end{cases}$$

on d és la part lliure de quadrats del discriminant de l'endomorfisme de Frobenius π de $E/\mathbb{F}_q$ i $\mathcal{O}_\mathbb{K}$ és l'anell d'enters de $\mathbb{K}$.

L'endomorfisme de Frobenius π com a element de l'anell $\mathcal{O}_\mathbb{K}=\mathbb{Z}\oplus\mathbb{Z}\omega$ es pot escriure com:

$$\pi=a+f\omega,$$

on l'enter a satisfà [Koh96]:

$$a = \begin{cases} \frac{t-f}{2}, & d \equiv 1 \pmod 4, \\ \frac{t}{2}, & d \equiv 2,3 \pmod 4. \end{cases}$$

Dels treballs de H. Lenstra [Len96] i de C. Wittman [Wit01] es pot veure que $E(\mathbb{F}_q) \cong \mathcal{O}/(\pi - 1)$ com $\mathcal{O}$-mòduls, d'on es pot deduir que

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}, \quad n_2 = \gcd(a-1, f/g), \ n_2|n_1, \quad n_2|(q-1)$$

i g és el conductor de $\mathcal{O}$. Aleshores, també es pot deduir el següent resultat:

Proposició 4.3. *Sigui E una corba el·líptica definida sobre el cos $\mathbb{F}_q$ amb ordre m, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} \oplus \mathbb{Z}[\omega]$ i $\pi = a + f\omega$. Aleshores $v_\ell(a-1) \geq \min\{v_\ell(f), v_\ell(m)/2\}$.*

Demostració. Si $d \equiv 2,3 \pmod 4$, amb $a = t/2$, tenim que $(a-1)^2 = f^2 d + m$. D'altra banda, $a = \frac{t-f}{2}$ i, atès que $(t-2)^2 = f^2 d + 4m$, aleshores $4(a-1)^2 = 4m + f^2(d-1) - 4f(a-1)$. Considerant la valoració ℓ-àdica d'aquestes expressions, tenim l'anterior proposició. □

D'aquesta manera podem tenir alguna idea sobre la ubicació de la corba donada $E/\mathbb{F}_q$ en el volcà segons el subgrup de ℓ-Sylow $S_\ell(E(\mathbb{F}_q))$.

Atès que aquest és un subgrup de $E(\mathbb{F}_q)$, la seva estructura és $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, amb $s \leq \min\{r, v_\ell(q-1)\}$.

Cal adonar-se que del resultat anterior es pot assegurar que el nodes que es troben en el mateix nivell dins del volcà tenen el mateix grup de ℓ-Sylow. A més a més, si es va ascendint pels nodes del volcà, el valor del paràmetre s augmenta o es manté igual. Aleshores, tenint en compte la Proposició 4.3 i el fet que $s \leq v_\ell(q-1)$, obtenim el següent resultat, que generalitza qualsevol $\ell \geq 2$ en [MMS+06]:

Teorema 4.4. *Sigui E una corba el·líptica definida en $\mathbb{F}_q$ d'ordre m amb $\nu = v_\ell(m) \geq 1$. Aleshores el volcà $V_\ell(E/\mathbb{F}_q)$ satisfà:*

i) El subgrup de ℓ-Sylow de les corbes que formen el terra d'aquest volcà és $\mathbb{Z}/\ell^\nu\mathbb{Z}$.

ii) Si ν és senar, el subgrup de ℓ-Sylow de les corbes en el i-èssim nivell és $\mathbb{Z}/\ell^{\nu-i}\mathbb{Z} \times \mathbb{Z}/\ell^i\mathbb{Z}$.

iii) Si ν és parell, el subgrup de ℓ-Sylow de les corbes que formen el nivell i-èssim és $\mathbb{Z}/\ell^{\nu-i}\mathbb{Z} \times \mathbb{Z}/\ell^{i}\mathbb{Z}$ per a tot i, $1 \leq i \leq \nu/2$. A més a més, la resta de nivells fins a arribar al cràter, en cas que n'hi hagi, tenen la mateixa estructura $\mathbb{Z}/\ell^{\nu/2}\mathbb{Z} \times \mathbb{Z}/\ell^{\nu/2}\mathbb{Z}$.

Es pot observar amb aquest resultat que en cas que ν sigui parell i l'altura del volcà sigui major que $\nu/2$, del nivell $\nu/2$ fins a arribar al cràter del ℓ-volcà, l'estructura del grup de ℓ-Sylow romandrà inalterable, isomorfa a $\mathbb{Z}/\ell^{\nu/2}\mathbb{Z} \times \mathbb{Z}/\ell^{\nu/2}\mathbb{Z}$. Aquesta situació no pot passar en cas que el valor de ν sigui senar, ja que l'altura és menor que $\nu/2$.

Definició 4.5. *S'anomena nivell d'estabilització el nivell en el qual l'estructura del subgrup de ℓ-Sylow estabilitza, que és el nivell $\nu/2$. Els ℓ-volcans que tenen altura menor o igual que el nivell d'estabilitat s'anomenaran volcans regulars.*

4.2 Procediment per construir un ℓ-volcà

En aquesta secció donem un algorisme per trobar l'altura d'un ℓ-volcà, així com la mida del seu cràter. L'algorisme que presentem és una generalització del donat en [MMS+02] per al cas $\ell = 2$.

Al final de la secció mostrem alguns exemples de volcans amb l'altura i la longitud del cràter per al cas $\ell = 3$.

4.2.1 Algorisme

En aquesta secció donem un algorisme, que, donada un corba el·líptica E definida sobre $\mathbb{F}_q$ i un primer ℓ, retorna l'altura h i la mida del cràter c del ℓ-volcà $V_\ell(E/\mathbb{F}_q)$, així com el nivell k on es troba la corba inicial.

Aquest algorisme dóna l'altura en els casos no regulars, ja que en els casos regulars, aquesta s'obté directament de la Proposició 4.1 i del Teorema 4.2. Per obtenir aquests paràmetres, la idea bàsica d'aquest algorisme consisteix a trobar un camí ascendent des del nivell on es troba $E/\mathbb{F}_q$ fins al cràter del ℓ-volcà al qual pertany. Aleshores, la mida del cràter s'obté recorrent els nodes que el formen. Vegem el pseudocodi d'aquest algorisme en Algorisme 6:

Algorisme 6 Algorisme ℓ-volcans

Entrada: una corba el·líptica E sobre un cos finit $\mathbb{F}_q$ i un primer ℓ.
Sortida: (k, h, c), on k és el nivell on es troba $E/\mathbb{F}_q$ dins el ℓ-volcà, h és l'altura del ℓ-volcà i c la mida del cràter.

```
1  Determinant el nivell de E/F_q dins del ℓ-volcà
2     si ℓ = 2 i  v_2(m) = 2 i  v_2(q − 1) ≥ 2 llavors
3        E :=Twisted(E) ;
4     fi
5     (n, r) :=ℓ-Sylow(E);
6     ν := v_ℓ(q − 1);
7     si r < n o (r = n i r ≠ ν) llavors
8        k := r;
9     sinó
10       s :=Passos_Fins_Nivell_Estabilitat(E);
11       k := r + s;
12    fi
13
14 Buscant el cràter del ℓ-volcà
15    h := k;
16    mentre No És_Corba_Cràter(E) fer
17       E :=Obtenir_Corba_Isògena_Ascendent(E);
18       h := h + 1;
19    fi
20
21 Recorrent el cràter del ℓ-volcà
22    c := 1;
23    E_seg :=Elegir_Corba_Isògena_Horitzontal(E);
24    E_ant := E;
25    mentre E_seg ≠ E fer
26       c := c + 1;
27       E_aux := E_seg;
28       E_seg :=Corba_Isògena_Horitzontal(E_seg, E_ant);
29       E_ant := E_aux;
30    fi
31
32 retorna (k, h, c);
```

Les funcions utilitzades en aquest algorisme són les següents:

- Twisted: En el cas particular que $\ell = 2$, $v_2(m) = 2$ i $v_2(q-1) \geq 2$, ens dóna més informació útil la corba *twisted* que la corba inicial i, per tant, en aquest cas agafem la *twisted* per obtenir la informació que retorna aquest algorisme. Així aquesta funció únicament ens dóna la corba *twisted* de la que se li ha entrat com a paràmetre.

- ℓ-Sylow: Retorna un parell d'enters (n, r), $r \leq n$, de manera que el subgrup de ℓ-Sylow de la corba $E/\mathbb{F}_q$ és isomorf a $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}$. Aquesta funció ve donada en l'algorisme de temps polinòmic descrit en [Mor05].

- Passos_Fins_Nivell_Estabilitat: Obté com a paràmetre d'entrada la corba el·líptica $E/\mathbb{F}_q$ i calcula $\ell + 1$ camins d'isògenes de $E/\mathbb{F}_q$ fins que arribi al nivell d'estabilitat. Es pot observar que almenys $\ell - 2$ d'aquests $\ell + 1$ camins seran descendents. Aleshores, la funció retorna el nombre de passos d'un d'aquests camins descendents, que és el mateix que dir la distància entre la corba $E/\mathbb{F}_q$ i el nivell d'estabilitat.

- És_Corba_Cràter: Retorna Cert si $E/\mathbb{F}_q$ pertany al cràter del ℓ-volcà i Fals, altrament. Per saber si una corba pertany o no al cràter, es calcula el nivell on es troba en el ℓ-volcà. En el cas de volcans regulars, el nivell on es troba la corba ve donat pels paràmetres del seu subgrup de ℓ-Sylow, i, com s'ha vist en el Teorema 4.2, ens proporcionen també l'altura del volcà. D'altra banda, el nivell de les corbes pot obtenir-se utilitzant la funció anterior. En aquest cas, es troba el cràter quan el nivell de totes les corbes isògenes de $E/\mathbb{F}_q$ és igual o menor que el nivell on es troba $E/\mathbb{F}_q$ (igual en les isogènies horitzontals i menor en les descendents).

- Obtenir_Corba_Isògena_Ascendent: Calcula les corbes isògenes d'$E/\mathbb{F}_q$ mitjançant les fórmules de Vélu, en els casos $\ell = 2$ i $\ell = 3$, i mitjançant polinomis modulars en els casos $\ell > 3$, i elegeix la corba isògena ascendent mitjançant l'obtenció del seu nivell en el ℓ-volcà.

- Elegir_Corba_Isògena_Horitzontal: Calcula les corbes isògenes d'$E/\mathbb{F}_q$ i retorna una de les seves isògenes horitzontals. Això es realitza mitjançant l'obtenció del seu nivell dins del volcà.

- Corba_Isògena_Horitzontal: Donades dos corbes $E/\mathbb{F}_q$ i $E'/\mathbb{F}_q$ en què existeix una isogènia horitzontal $\mathcal{I}' : E'/\mathbb{F}_q \longrightarrow E/\mathbb{F}_q$, aquesta funció retorna la corba $E''/\mathbb{F}_q$ de manera que existeix la isogènia horitzontal $\mathcal{I} : E/\mathbb{F}_q \longrightarrow E''/\mathbb{F}_q$ no dual a la isogènia $\mathcal{I}'$.

Es pot observar que el nivell de la corba es pot obtenir mitjançant el càlcul de camins descendents cap al nivell inferior de forma similar al procediment utilitzat per [FM02]. Tanmateix, aquest algorisme proposa una millora utilitzant l'algorisme donat en [Mor05]. Per això, es pot evitar calcular els camins descendents en cas de volcans regulars, mentre que en cas de volcans no regulars, sols és necessari calcular fins al nivell d'estabilitat.

4.2.2 Alguns exemples per a $\ell = 3$

Considerem, en primer lloc, un model d'equació de la corba que ens assegura tenir punts d'ordre 3. Així, agafant un d'aquests punts com l'origen, l'equació de la corba es pot expressar de la següent manera:

$$E_{a,b} : \qquad y^2 + axy + by = x^3, \quad a, b \in \mathbb{F}_q.$$

Utilitzant aquest model, els punts $(0, 0)$ i $(0 - b)$ són punts d'ordre 3. A més a més, tenint en compte el seu polinomi de 3-divisió:

$$\Psi_3(x) = x(x^3 + a^2/3x^2 + 3abx + b^2),$$

l'estructura del subgrup de 3-torsió s'obté fàcilment mitjançant:

- Si $v_3(q - 1) = 0$, el tipus de factorització de $\Psi_3(x)$ és $[1, 1, 2]$, però únicament l'abscissa $x = 0$ dóna dos punts racionals de $E_{a,b}/\mathbb{F}_q$, i així, $E_{a,b}(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z}$.

- Si $v_3(q - 1) > 0$, el tipus de factorització de $\Psi_3(x)$ pot ser o bé $[1, 3]$,

o bé $[1,1,1,1]$. En el primer cas, $E_{a,b}(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z}$, mentre que en el segon cas tenim que $E_{a,b}(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Segons les classes d'isomorfia de les corbes $E_{a,b}/\mathbb{F}_q$, un representant de cadascuna d'aquestes classes es pot obtenir de la següent manera:

- Si $v_3(q-1) = 0$, cada classe d'isomorfia pot ser representada de forma unívoca per la corba $E_{1,\lambda}/\mathbb{F}_q$ (sent $\lambda = \frac{b}{a^3}$), llevat que $a = 0$; en aquest cas una corba representant és $E_{0,1}/\mathbb{F}_q$.

- Si $v_3(q-1) > 0$, es poden distingir dos casos, depenent del tipus de factorització de $\Psi_3(x)$, o bé $[1,3]$ o bé $[1,1,1,1]$.

  - La primera situació, és a dir, quan la factorització de $\Psi_3(x)$ és $[1,3]$, és similar a l'anterior, quan $a \neq 0$. Per tant, una corba representant d'aquesta classe d'isomorfia també és $E_{1,\lambda}/\mathbb{F}_q$. D'altra banda, les corbes amb $a = 0$ pertanyen a dos classes d'isomorfia diferents: $E_{0,\delta_1}/\mathbb{F}_q$ i $E_{0,\delta_2}/\mathbb{F}_q$, sent $\delta_1^{3^{v-1}}$ i $\delta_2^{3^{v-1}}$ les arrels cúbiques primitives d'1, on $v = v_3(q-1)$.

  - En la segona situació, $a \neq 0$, existeixen quatre representants diferents del tipus $E_{1,\lambda}$ en cada classe d'isomorfia. Això es deu al fet que l'origen, en aquests casos, es pot canviar a altres punts d'ordre 3. L'algorisme agafa el representant que té el valor de λ més petit. En cas que $a = 0$, el representant de la classe d'isomorfia torna a ser $E_{0,1}/\mathbb{F}_q$.

La corba isògena de la corba $E_{a,b}/\mathbb{F}_p$ amb nucli $\{\mathcal{O}, (0,0), (0,-b)\}$, d'acord amb la fórmula de Vélu, té equació:

$$E'/\mathbb{F}_p : y^2 + axy + by = x^3 - 5abx - b(a^3 + 7b),$$

amb polinomi de 3-divisió: $\Psi_3'(x) = (x + a^2/3)(x^3 - 9abx - b(a^3 + 27b))$.

Aleshores, considerant les arrels d'aquest polinomi, la corba $E'/\mathbb{F}_q$ pot ser expressada en el model $E_{a,b}/\mathbb{F}_q$. La Taula 4.2 recull les corbes isògenes obtingudes. De fet, per al cas $v_3(q-1)=0$, es pot observar que solament es dóna la isogènia corresponent al punt racional.

Corba	Arrels de $\psi_3'(x)$	Corba isògena: cas $v_3(q-1)=0$
$(1,\lambda)$	$-1/3, \beta$	$\left(1, \dfrac{(\beta+9\lambda)^4}{(6\beta^2+\beta-9\lambda)^3}\right)$ si $6\beta^2+\beta-9\lambda\neq 0$ $(0,1)$ si $6\beta^2+\beta-9\lambda=0$
$(0,1)$	$-1/3, 3$	$\left(1, \dfrac{1}{24}\right)$
Corba	**Arrels de $\psi_3'(x)$**	**Corba isògena: cas $v_3(q-1)>0$**
$(1,\lambda)$	0	$\left(1, \dfrac{1}{27}-\lambda\right)$
$(1,\lambda)$	$0, \beta_1, \beta_2, \beta_3$ $(\beta_i,\gamma_i)\in E_{1,\lambda}(\mathbb{F}_q)$	$\left(1, \dfrac{1}{27}-\lambda\right)$ $\left(1, \dfrac{1}{27}-\dfrac{(\beta_i+2\gamma_i+\lambda)^4}{(6\beta_i^2+\beta_i+\lambda)^3}\right)$ si $6\beta_i^2+\beta_i+\lambda\neq 0$ $(0,1)$ si $6\beta_i^2+\beta_i+\lambda=0$
$(0,1)$	$0, -1, \rho_1, \rho_2$	$(0,1),\ \left(1,-\dfrac{1}{216}\right),\ \left(1,-\dfrac{1}{216}\right),\ \left(1,-\dfrac{1}{216}\right)$
$(0,\delta_i)$	0	$(0,\delta_i)$

Taula 4.2: Coeficients de les corbes isògenes

La Taula 4.3 recull alguns exemples de volcans corresponents a corbes $E_{1,\lambda}/\mathbb{F}_p$. Els resultats obtinguts mostren, d'una banda, que la mitjana de les altures és molt petita i, de l'altra, que la mida dels cràters pot arribar a ser enorme. Més concretament, els resultats empírics indiquen que c pot assolir el valor de $\sqrt{p}$.

p	$v_3(p-1)$	λ	$v_3(\lvert E_{1,\lambda}\rvert)$	(h,c)
10007	0	130	3	(0, 132)
131221	8	118403	8	(4, 4)
4738294793	0	483209742	1	(0, 5255)
5764865399	0	845734783	2	(0, 28193)
6473810533	1	978203893	3	(1, 2337)
$10^{14}+99$	2	4	2	(1, 810556)
$10^{20}+441$	3	1	5	(2, 2)
$10^{40}+921$	1	345789102	2	(1, 1)
$10^{80}+129$	1	500	2	(1, 2)

Taula 4.3: Estructura d'alguns 3-volcans $V_3(E_{1,\lambda})/\mathbb{F}_p$

A més a més, aquest algorisme s'ha utilitzat per estudiar la distribució dels 3-volcans sobre un cos finit $\mathbb{F}_p$. Les Taules 4.4 i 4.5 proporcionen l'estructura de tots els volcans obtinguts per als primers $p = 227$ i $p = 229$, respectivament. El paràmetre m denota l'ordre de les corbes de manera que $v_3(m) \geq 1$. Més precisament, cada estructura de volcà possible ve determinada pel parell (h, c), i aquestes taules cataloguen els volcans corresponents als donats pels paràmetres d'una corba del seu cràter. Finalment, l'última columna de la Taula 4.5 mostra la regularitat del volcà (es pot observar que els volcans no regulars són bastant difícils de trobar en el cas $v_3(p-1) \geq 1$ i no se n'han trobat en el cas $v_3(p-1) = 0$).

h	c	Paràmetres corba	m	$v_3(m)$
0	1	(1,199)	198	2
0	1	(1,213)	258	1
0	3	(1,10)	204	1
0	3	(1,146)	252	2
0	4	(1,33)	228	1
0	5	(1,103)	201	1
0	5	(1,25)	213	1
0	5	(1,7), (1,14)	222	1
0	5	(1,1), (1,5), (1,8)	228	1
0	5	(1,52), (1,72)	234	2
0	5	(1,6)	243	5
0	5	(1,16)	255	1
0	7	(1,26)	207	2
0	7	(1,31)	219	1
0	7	(1,53)	237	1
0	7	(1,32)	249	1
0	8	(1,13), (1,57)	210	1
0	8	(1,21), (1,27)	246	1
0	9	(1,11)	204	1
0	9	(1,40)	252	2
0	13	(1,24), (1,58)	216	3
0	13	(1,2), (1,18)	240	1
0	14	(1,4)	225	2
0	14	(1,50)	231	1

Taula 4.4: Estructura de 3-volcans sobre $\mathbb{F}_p$, $p = 227$, $v_3(p-1) = 0$

h	c	Paràmetres corba	m	$v_3(m)$	Reg.
0	1	(0,134)	201	1	sí
		(0,94)	237	1	sí
0	2	(1,111)	201	1	sí
		(1,20), (1,92), (1,96), (1,116)	204	1	sí
		(1,50), (1,55), (1,63), (1,72), (1,79), (1,83)	210	1	sí
		(1,24), (1,40)	213	1	sí
		(1,90), (1,99)	219	1	sí
		(1,56), (1,80), (1,87), (1,112)	222	1	sí
		(1,7), (1,46), (1,67), (1,82), (1,94), (1,98)	228	1	sí
		(1,5), (1,75), (1,89), (1,119)	231	1	sí
		(1,23), (1,95), (1,113)	237	1	sí
		(1,3), (1,35), (1,41), (1,48), (1,58), (1,62)	240	1	sí
		(1,65), (1,73), (1,91), (1,117)	240	1	sí
		(1,29), (1,31), (1,66), (1,76)	246	1	sí
		(1,37), (1,97)	249	1	sí
		(1,36), (1,100)	255	1	sí
		(1,45), (1,102)	258	1	sí
1	1	(1,38)	207	2	sí
		(1,6), (1,18), (1,49)	234	2	sí
		(1,33), (1,105)≅(0,1)	252	2	sí
1	2	(1,4)	252	2	sí
1	3	(1,1)	243	5	sí
1	4	(1,2), (1,44)	216	3	sí
2	1	(1,60)	225	2	no

Taula 4.5: Estructura de 3-volcans sobre $\mathbb{F}_p$, $p = 229$, $v_3(p-1) = 1$

4.3 Volcans d'isogènies racionals

En aquesta secció mostrem com estendre el càlcul de l'altura d'un volcà a volcans d'isogènies racionals.

4.3.1 Procediment per calcular l'altura d'un volcà

Donada E és una corba definida sobre un cos $\mathbb{K}$ i G és un subgrup de $E(\mathbb{K})$ Galois-invariant, és a dir, si G és $\mathbb{K}$-racional, aleshores la corba isògena E' determinada per G i la isogènia $\mathcal{I}_G$ també estan definides sobre $\mathbb{K}$.

Amb aquest fi donem dos resultats del treball [MMS+08] sobre el grau de les extensions del cos $\mathbb{F}_q$ per al qual podem garantir que la corba E té punts de ℓ-torsió racionals.

Proposició 4.6. *Sigui $E/\mathbb{F}_q$ una corba el·líptica sobre $\mathbb{F}_q$. Si $E/\mathbb{F}_q$ té 1 o $\ell+1$ isogènies racionals de grau ℓ, aleshores $\#E(\mathbb{F}_{q^{ord_\ell(q)}})$ o $\#E^t(\mathbb{F}_{q^{ord_\ell(q)}})$ és un múltiple de ℓ, on $ord_\ell(q)$ és l'ordre de q en el grup $\mathbb{F}_\ell^*$.*

D'altra banda, la relació que hi ha entre l'altura d'un volcà sobre $\mathbb{F}_q$ i la del volcà sobre una extensió $\mathbb{F}_{q^n}$ ve donada pel següent resultat:

Proposició 4.7. *Sigui $E/\mathbb{F}_q$ una corba el·líptica de manera que $h(V_\ell(E/\mathbb{F}_q)) = 0$. Aleshores se satisfà:*

$$h(V_\ell(E/\mathbb{F}_{q^n})) = h(V_\ell(E/\mathbb{F}_q)) + v_\ell(n).$$

Donem ara el següent procediment explicat a [MMS+08] per al càlcul de l'altura d'un ℓ-volcà $V_\ell(E/\mathbb{F}_q)$:

(1) Calculem $v_\ell(q-1)$.

(2) Calculem $v_\ell(m)$ a partir de l'estructura del subgrup de ℓ-Sylow de $E/\mathbb{F}_q$.

(3) Si $v_\ell(q-1) \geq 1$ i $v_\ell(m) \geq 1$, es calcula l'altura de $V_\ell(E/\mathbb{F}_q)$ aplicant la Proposició 4.1 i el Teorema 4.2.

(4) Si $v_\ell(q-1) = 0$ i $v_\ell(m) \geq 1$, llavors $h(V_\ell(E/\mathbb{F}_q)) = 0$.

(5) Si $v_\ell(m) = 0$, calculem $v_\ell(m')$, sent m' l'ordre del grup de la corba *twisted* $E^t/\mathbb{F}_q$.

(6) Si $v_\ell(m') \geq 1$, obtenim $h(V_\ell(E^t/\mathbb{F}_q))$ usant els passos (3) i (4). Llavors, $h(V_\ell(E/\mathbb{F}_q)) = h(V_\ell(E^t/\mathbb{F}_q))$.

(7) Si $v_\ell(q-1) = 0$, $v_\ell(m) = 0$ $v_\ell(m') = 0$, calculem $E(\mathbb{F}_q^{ord_\ell q})[\ell]$ i $E'(\mathbb{F}_q^{ord_\ell q})[\ell]$.

- Si $E(\mathbb{F}_q^{ord_\ell q})[\ell] \neq \{0\}$, aleshores $h(V_\ell(E/\mathbb{F}_q)) = h(V_\ell(E'/\mathbb{F}_{q^{ord_\ell(q)}}))$.
- Si $E'(\mathbb{F}_q^{ord_\ell q})[\ell] \neq \{0\}$, aleshores $h(V_\ell(E/\mathbb{F}_q)) = h(V_\ell(E'/\mathbb{F}_{q^{ord_\ell(q)}}))$.
- Altrament, $h(V_\ell(E/\mathbb{F}_{q^{ord_\ell(q)}})) = 0$.

4.3.2 Alguns exemples per a $\ell \geq 5$

Les corbes el·líptiques amb subgrups d'ordre ℓ es poden parametritzar mitjançant les corbes modulars $X_0(\ell)$ i $X_1(\ell)$. Així, la corba modular $X_0(\ell)$ parametritza les classes d'equivalència de parells $(E/\mathbb{K}, G)$, on $E/\mathbb{K}$ és una corba el·líptica i G, un subgrup racional d'ordre ℓ d'$E/\mathbb{K}$, de manera que el parell $(E'/\mathbb{K}, G')$ pertany a la classe $(E/\mathbb{K}, G)$, si, i només si, existeix un isomorfisme entre E i E' que transforma el grup G en el grup G'. Per tant, $X_0(\ell)$ parametritza, també, les classes d'equivalència dels parells $(E/\mathbb{K}, \mathcal{I}_G)$, on $\mathcal{I}_G$ és una isogènia d'$E/\mathbb{K}$ amb $\ker \mathcal{I}_G = G$ i $|G| = \ell$.

Així mateix, $X_1(\ell)$ parametritza les classes d'equivalència $(E/\mathbb{K}, P)$, on P és un punt racional de ℓ-torsió de $E/\mathbb{K}$ i, per tant, les classes d'equivalència $(E/\mathbb{K}, \mathcal{I}_{\langle P \rangle})$.

Com a exemple de paràmetres establerts, considerarem la corba modular $X_0(5)$, amb equació $xy = 5^3$. El morfisme d'*oblit* que fa correspondre cada parell $(E/\mathbb{K}, G)$ en $X_0(5)$ a la corba $(E/\mathbb{K})$ en $X_0(1)$, de manera que identificant $X_0(1)$ amb la forma projectiva $P^1(\mathbb{K})$, aquest morfisme ve donat per:

$$\begin{array}{rcl} X_0(5) & \longrightarrow & \mathbb{P}^1(\mathbb{K}), \\ (u, v) & \longmapsto & j_u, \end{array}$$

sent $j_u = \dfrac{(u^2 + 10u + 5)^3}{u}$ el j-invariant de E. Per tant, utilitzant el model

$$E/\mathbb{K}: \; y^2 = x^3 + \frac{x^2}{4} - \frac{36}{j - 1728}x - \frac{1}{j - 1728},$$

quan la característica de $\mathbb{K}$ és diferent de 2 i $j = j(E) \neq 0, 1728$, obtenim les corbes el·líptiques següents:

$$E_5(u)/\mathbb{K}: \quad y^2 = x^3 + \frac{x^2}{4} - 36R_5(u)x - R_5(u),$$

$$\text{amb} \quad R_5(u) = \frac{u}{(u^2+4u-1)^2(u^2+22u+125)},$$

$$\text{i} \quad u \in \mathbb{K} \setminus \{-5 \pm 2\sqrt{5}, -2 \pm 2\sqrt{5}, -11 \pm 2\sqrt{-1}, 0\},$$

que tenen un subgrup $\mathbb{K}$-racional $G \subseteq E(\mathbb{K})$ d'ordre 5.

Per a $\ell \in \{2, 3, 5, 7, 13\}$, la corba modular $X_0(\ell)$ té gènere 0: en la Taula 4.6 podem veure l'expressió $R_\ell(u)$ de l'equació de la corba el·líptica,

$$E_\ell(u)/\mathbb{K}: \; y^2 = x^3 + \frac{x^2}{4} - 36R_\ell(u)x - R_\ell(u),$$

amb $u \in \mathbb{K} \setminus \mathcal{U}_\ell$ per a cadascun d'aquests valors, on $\mathcal{U}_\ell$ és el conjunt dels zeros del denominador de l'expressió racional que defineix $R_\ell(u)$.

ℓ	$R_\ell(u)$
2	$\dfrac{u}{(u+64)(u-8)^2}$
3	$\dfrac{u}{(u^2+18u-27)^2}$
5	$\dfrac{u}{(u^2+4u-1)^2(u^2+22u+125)}$
7	$\dfrac{u}{(u^4+14u^3+63u^2+70u-7)^2}$
13	$\dfrac{u}{(u^6+10u^5+46u^4+108u^3+122u^2+38u-1)^2(u^2+6u+13)}$

Taula 4.6: Expressions de $R_\ell(u)$

Llavors, utilitzant aquestes parametritzacions, hem obtingut diversos exemples de corbes el·líptiques que tenen un grup racional d'ordre ℓ. La Taula 4.7 recull l'altura de diversos volcans corresponents a corbes el·líptiques $E/\mathbb{F}_p$ donades mitjançant els diferents valors de $R_\ell(u)$ i de manera que la valoració ℓ-àdica del seu cardinal és zero. En aquesta taula, r denota l'ordre de q en $\mathbb{F}_\ell^*$.

ℓ	q	r	$v_\ell(q^r-1)$	u	$R_\ell(u)$	$v_\ell(m_r)$	$v_\ell(m'_r)$	h
5	751	1	3	26	724	0	3	1
	15559	2	1	4280	8627	0	2	2
	733	4	1	257	625	2	0	0
7	701	1	1	29	95	0	3	1
	1049	2	1	487	379	2	0	0
	1439	3	2	1392	1349	0	2	1
	733	6	1	228	27	3	0	0
13	677	1	2	68	158	0	2	1
	2027	2	2	265	914	0	2	1
	1049	3	1	1019	368	2	0	0
	733	4	1	40	524	2	0	0
	3137	6	1	176	66	0	2	1
	661	12	1	374	286	2	0	0

Taula 4.7: Altura d'alguns ℓ-volcans

Podem veure que en el cas $\ell = 2$ no hi ha cap corba $E/\mathbb{F}_q$ que compleixi aquesta condició, ja que els subgrups racionals de $E/\mathbb{F}_q$ estan generats per un punt racional. El cas $\ell = 3$ pot ser classificat segons el valor de $v_\ell(q-1)$. Quan aquest valor és 0, la corba $E/\mathbb{F}_q$ té isogènies racionals, si, i només si, $E/\mathbb{F}_q$ o $E^t/\mathbb{F}_q$ tenen punts racionals d'ordre 3. Així, si n'existeixen, hi ha dos isogènies racionals. Per tant, de la Proposició 4.1 es dedueix $h(V_\ell(E/\mathbb{F}_q)) = 0$. Quan $v_\ell(q-1) \geq 1$ hi ha dos possibilitats. Si $E/\mathbb{F}_q$ o $E^t/\mathbb{F}_q$ tenen punts racionals d'ordre 3, de la Proposició 4.1 s'obté que $h(V_\ell(E/\mathbb{F}_q)) \neq 0$. D'altra banda, pel Teorema 4.2 obtenim $h(V_\ell(E/\mathbb{F}_q)) = 0$.

Per als casos $\ell = 5, 7, 13$ observem que del Teorema 4.2, assumint que ni $E/\mathbb{F}_q$ ni $E^t/\mathbb{F}_q$ tenen punts racionals d'ordre ℓ si $ord_\ell(q) = 1$ o $v_2(ord_\ell(q)) = v_2(\ell-1)$, es dedueix $h(V_\ell(E/\mathbb{F}_q)) = 0$. Per tant, l'altura del volcà pot ser diferent de zero quan $ord_5(q) = 2$, $ord_7(q) = 3$ o $ord_{13}(q) = 2, 3, 6$. A més,

per a aquests ordres de q, quan $v_\ell(m_{ord_\ell(q)}) > 1$ o $v_\ell(m'_{ord_\ell(q)}) > 1$ tenim $h(V_\ell(E/\mathbb{F}_q)) = h(V_\ell(E/\mathbb{F}_{q^2}))$ si $\ell = 5$ i $h(V_\ell(E/\mathbb{F}_q)) = h(V_\ell(E/\mathbb{F}_{q^3}))$ si $\ell = 7$.

Aquest algorisme també ha estat implementat en MAGMA [BCP97] per estudiar la distribució dels volcans de 5-isogènies sobre un cos finit $\mathbb{F}_q$. La Taula 4.8 proporciona l'estructura de tots els volcans obtinguts amb el primer $p = 79$. Per a cada estructura possible determinada pel parell (h, c), la taula cataloga els volcans corresponents amb el paràmetre $R_5(u)$ d'una de les corbes situada en el cràter d'aquest volcà, mentre que el paràmetre m és l'ordre del grup de les corbes del volcà.

h	c	$R_5(u)$	m	$v_5(m)$	$v_5(m')$	$v_5(m_2)$	$v_5(m'_2)$
1	1	3	76	0	0	0	2
0	6	6	70	1	1	2	0
		37	90	1	1	2	0
0	5	19, 41	80	1	1	2	0
0	4	25	75	2	1	3	0
		26	85	2	1	3	0
0	2	44	65	1	1	2	0
		7	66	0	0	0	1
		50, 64	69	0	0	0	1
		28	70	1	1	2	0
		56	74	0	0	0	1
		5, 45, 49	79	0	0	0	1
		40	81	0	0	0	1
		39	86	0	0	0	1
		18	89	0	0	0	1
		47	90	1	1	2	0
		67, 72	91	0	0	0	1
		12, 61	94	0	0	0	1
		20, 27	96	0	0	0	1

Taula 4.8: Estructura dels volcans de 5-isogènies sobre $\mathbb{F}_p$, $p = 79$

Capítol 5

Cordilleres de volcans d'isogènies

En el capítol anterior hem vist com, a partir d'una corba el·líptica, podem generar un llistat de corbes diferents mitjançant la construcció del seu ℓ-volcà, i totes amb el mateix cardinal. Ara bé, pot ser que puguem trobar altres ℓ-volcans, disjunts a l'inicial, formats per corbes que comparteixen també el mateix cardinal que la corba donada, és a dir, que el graf de ℓ-isogènies no sigui connex. Tots els possibles volcans diferents, per un valor ℓ fixat formen el que anomenarem *ℓ-cordillera*. Així, en una ℓ-cordillera hi trobarem totes les corbes definides sobre un mateix cos amb un mateix cardinal.

En aquest capítol donem un mètode per generar corbes amb el mateix cardinal mitjançant isogènies i utilitzant propietats de cordilleres de volcans [MST+08].

5.1 Concepte de cordillera de volcans

Els volcans són grafs formats per corbes isògenes entre si. Això implica que un node representa una classe d'isomorfia de corbes el·líptiques definides sobre un mateix cos i que alhora tenen el mateix cardinal, però no totes les corbes amb un mateix cardinal estan distribuïdes en un únic volcà.

Definició 5.1. *Donat un cos finit $\mathbb{F}_q$ i un primer ℓ, anomenem ℓ-cordillera al conjunt de tots els ℓ-volcans de corbes el·líptiques definides sobre $\mathbb{F}_q$ que tenen un mateix cardinal.*

Donada una corba el·líptica $E/\mathbb{F}_q$, denotarem la seva ℓ-cordillera com

$C_\ell(E/\mathbb{F}_q)$. Totes les corbes contingudes en una mateixa ℓ-cordillera comparteixen el mateix cardinal. És a dir, si tenim una corba E i una altra E' de manera que $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$, aleshores $E/\mathbb{F}_q$ i $E'/\mathbb{F}_q \in C_\ell(E/\mathbb{F}_q)$ encara que $V_\ell(E/\mathbb{F}_q) \neq V_\ell(E'/\mathbb{F}_q)$.

Proposició 5.2. *Siguin ℓ i ℓ' dos nombres primers. Aleshores se satisfà:*

i) Tots els ℓ-volcans que formen una ℓ-cordillera tenen la mateixa altura.

ii) Si $\ell \neq \ell'$, corbes el·líptiques que estan a diferents nivells en un ℓ-volcà, es troben en components connexes diferents de la ℓ'-cordillera.

Demostració. Totes les corbes amb el mateix cardinal tenen el mateix conductor dels ordres generats pel seus endomorfismes de Frobenius. Per aquest motiu, l'altura de tots els volcans formats per aquestes corbes és la mateixa.

Quant a l'apartat *ii)*, si tenim dos corbes $E/\mathbb{F}_q$ i $E'/\mathbb{F}_q$ que pertanyen a dos volcans de ℓ i ℓ'-isogènies de manera que $V_\ell(E/\mathbb{F}_q) = V_\ell(E'/\mathbb{F}_q)$ i $V_{\ell'}(E/\mathbb{F}_q) = V_{\ell'}(E'/\mathbb{F}_q)$, aleshores els anells d'endomorfismes satisfan que

$$[\mathcal{O} : \mathcal{O}'] = \ell^n \text{ i } [\mathcal{O} : \mathcal{O}'] = (\ell')^{n'}.$$

Per tant, les dos relacions solament es poden donar quan $n = n' = 0$. Així doncs, les corbes E i E' han d'estar ubicades en el mateix nivell en el volcà $V_\ell(E/\mathbb{F}_q)$, així com en el volcà $V_{\ell'}(E/\mathbb{F}_q)$.

□

5.2 Procediment per obtenir corbes isògenes d'una cordillera

En el capítol anterior hem donat un algorisme per obtenir les corbes d'un volcà d'ℓ-isogènies. El problema és quan busquem una corba amb una sèrie de característiques específiques i no la trobem en aquest ℓ-volcà. É-s aquí quan apareix el concepte de ℓ-cordillera, ja que, per definició, en una ℓ-cordillera apareixeran totes les corbes d'un cos que tenen un mateix cardinal, no únicament les que apareixen en un ℓ-volcà, ampliant així aquest registre de corbes que ens oferia el volcà.

Com ja s'ha dit, una ℓ-cordillera està formada per tots els ℓ-volcans de corbes el·líptiques definides en un mateix cos i que tenen un mateix cardinal, però aquests ℓ-volcans diferents són grafs no connexos i, malauradament, no hi ha cap manera immediata de passar d'un d'aquests volcans que formen la ℓ-cordillera a un altre. La manera que proposem per construir tota la cordillera és anar canviant de ℓ alhora de construir els ℓ-volcans.

D'altra banda, una corba no té isogènies de grau un primer qualsevol. Així, donada una corba el·líptica $E/\mathbb{F}_q$, considerarem una sèrie de nombres primers ℓ_1, ℓ_2,...,ℓ_{final} per als quals sabem que $E/\mathbb{F}_q$ té isogènies d'aquests graus.

Una vegada fixada la llista, per intentar obtenir totes les corbes que tenen al mateix cardinal $E/\mathbb{F}_q$ inicial, la idea que proposem és fer primer el ℓ_1-volcà d'aquesta corba, emmagatzemar totes les corbes d'aquest ℓ_1-volcà inicial i fer el ℓ_2-volcà de la corba . Normalment, en aquest nou ℓ_2-volcà apareixeran corbes que no teníem encara emmagatzemades, i això vol dir que no eren en el ℓ_1-volcà. Per tant, en la ℓ_1-cordillera estaven en una altra component que encara no s'havia calculat. Construint el ℓ_1-volcà d'aquestes noves corbes apareixeran noves components de la ℓ_1-cordillera. Així mateix, podem també construir els ℓ_2-volcans de corbes que no han sortit en el ℓ_2-volcà, i obtenir noves corbes. Fent aquest procés reiteradament i augmentant el primer ℓ_i quan sigui necessari, anirem trobant totes les components no connexes que formen la ℓ_1-cordillera.

Resumint, la idea per obtenir totes les corbes pertanyents a una ℓ-cordillera és construir tots els ℓ-volcans que la formen. Així, necessitem almenys emmagatzemar una corba de cada ℓ-volcà. Per obtenir aquestes corbes, l'estratègia que seguirem serà aconseguir corbes a partir de la construcció de ℓ'-volcans, ℓ' diferent de ℓ, i guardar les corbes que van apareixent en una llista de corbes no tractades. Després, es construeixen els seus respectius ℓ-volcans, i es trobaran així noves corbes pertanyents a la ℓ-cordillera.

Ara veurem com quedaria plasmada aquesta idea en el següent algorisme [MST$^+$08]:

Algorisme 7 Corbes_Isògenes

Entrada: E: Corba el·líptica sobre un cos $\mathbb{F}_q$;
ℓ_{lim}: Nombre primer ;
L_E: Llista creixent de primers $\{\ell_1, \ell_2, ..., \ell_{lim}\}$ per als quals E té almenys una ℓ_i-isogènia;
Sortida: Llista de corbes el·líptiques amb el mateix cardinal que E ;

```
1  cordillera := E ;
2  per a ℓ nombre primer de manera que ℓ ∈ L_E fer
3      Pendents[ℓ] := ∅ ;
4  fi
5  ℓ_act := Obtenir_ℓ_act(L_E) ;
6  Pendents[ℓ_act] := Afegir(E) ;
7  noves := Fals;
8  mentre No Buida(Pendents[ℓ_act]) fer
9      E' := Primera(Pendents[ℓ_act]) ;
10     V := ℓ_act-volcà(E') ;
11     per a corba el·líptica E'' en V fer
12         si E'' ∈ cordillera llavors
13             Pendents[ℓ_act] := Eliminar(E'');
14         sinó
15             cordillera := Afegir(E'') ;
16             noves := Cert ;
17             per a  ℓ ∈ L_E fer
18                 si  ℓ ≠ ℓ_act llavors
19                     Pendents[ℓ] := Afegir(E'') ;
20                 fi
21             fi
22         fi
23     fi
24 fi
25 si noves, llavors
26     ℓ_act := Obtenir_ℓ_act(L_E) ;
27     noves := Fals;
28 fi
```

Variables utilitzades:

ℓ, ℓ_{act}: Nombres primers;
E', E'': Corbes el·líptiques;
V: Llista de nodes del volcà;
noves: Booleà;
Per a ℓ nombre primer **de manera que** $\ell \in L_E$
  Pendents[ℓ]: Llista de corbes el·líptiques que encara no s'han tractat;

Aquest algorisme té com a paràmetres d'entrada una corba el·líptica $E/\mathbb{F}_q$ que serveix de punt de partida per a l'algorisme, ja que serà a partir d'aquesta que s'aniran omplint la llista de corbes que formen la cordillera. D'altra banda, també tenim com a paràmetre que s'introdueix el nombre primer ℓ_{lim} que correspon al valor màxim del primer per al qual es construirà el seu volcà, és a dir, la llista de primers L_E, que també forma part dels paràmetres d'entrada de l'algorisme, arribarà com a molt al valor ℓ_{lim}, per tant, no hi haurà cap valor $\ell_i \in L_E$ com ara $\ell_i > \ell_{lim}$. A més a més, els primers, ℓ_i que pertanyin a aquesta llista L_E seran els que almenys tinguin una ℓ_i-isogènia de E en el cos $\mathbb{F}_q$. Com a sortida, ens retornarà un llistat de corbes isògenes a $E/\mathbb{F}_q$ obtingudes fent isogènies de grau $\ell \in L_E$.

En l'algorisme, la variable Pendents[ℓ_i] s'usa per emmagatzemar la llista de corbes de les quals no s'ha construït el seu ℓ_i-volcà. D'altra banda, la funció Primera(L) ens retorna el primer valor de la llista L. També tenim la funció ℓ_{act}-volcà(E), que, per la seva part, ens retorna una llista amb tots els nodes del ℓ_{act}-volcà de la corba E. Aquesta funció, primer de tot, trobarà un camí de la corba inicial fins al cràter del volcà i aleshores anirà passant per tots els nodes del vessant [FM02, MMS$^+$06, MST$^+$07], sent aquesta forma d'abordar el volcà paral·lelitzable, com es pot veure en [MTR$^+$06].

Aquest algorisme s'ha implementat utilitzant el programa Magma [BCP97]. El cost depèn del nombre d'isogènies que es volen obtenir, així com dels graus ℓ_i de les isogènies que es calculen.

5.3 Resultats i exemples

Vegem com procediria aquest algorisme en un cas hipotètic. Siguin {A, B, C, D, E, F, G, H, I, J} corbes amb el mateix cardinal, suposem que es reparteixen en les següents cordilleres de ℓ-volcans:

2-cordillera: {{A, B, C, D}, {E, F, G, H},{I, J} }
3-cordillera: {{A, E}, {B, F}, {C, G}, {D, H},{I, J} }
5-cordillera: {{A, E, I, J}, {B, C, D, F, G, H}}
⋮ ⋮

En la iteració 0, inicialitzem $\ell_{act} = 2$ i $\ell_{lim} = 5$ de manera que recorrem els volcans de 2, 3 i 5 isogènies. A partir d'aquests valors, en les següents iteracions obtindrem:

	Isògenes	ℓ_{act}	Pendents[2]	Pendents[3]	Pendents[5]
0	*A*	2	**A**	*A*	*A*
1	A*BCD*	3	∅	**A***BCD*	A*BCD*
2	ABCD*E*	2	**E**	BCD	ABCD*E*
3	ABCDE*FGH*	3	∅	**B**CD*FGH*	ABCDE*FGH*
4	ABCDEFGH	3	∅	**C**DGH	ABCDEFGH
5	ABCDEFGH	3	∅	**D**H	ABCDEFGH
6	ABCDEFGH	5	∅	∅	**A**BCDEFGH
7	ABCDEFGH*IJ*	2	***I****J*	*IJ*	BCDFGH
8	ABCDEFGHIJ	3	∅	**I**J	BCDFGH
9	ABCDEFGHIJ	5	∅	∅	**B**CDFGH
10	ABCDEFGHIJ	7	∅	∅	∅

Podem veure que en el pas 0 s'ha inicialitzat la llista d'isògenes amb la corba A. Llavors l'algorisme genera el 2-volcà per obtenir les següents corbes isògenes. En la llista d'Isògenes s'afegiran en cada pas les corbes noves que s'han obtingut en calcular en el pas previ els seus ℓ_i-volcans. En les columnes denotades com Pendents[ℓ_i] es van afegint les corbes no tractades que apareixen en cada iteració, aquelles que el seu ℓ_i-volcà encara no ha estat calculat. Així, en la

iteració 1 es calcula el 2-volcà que conté la corba A, i s'afegiran en les llistes de pendents de $\ell = 3$ i de $\ell = 5$ les corbes pertanyents al 2-volcà construït.

Així mateix, es van eliminant les corbes que apareixen en cadascuna de les columnes Pendents[ℓ_i] a mesura que es vagin calculant els seus ℓ_i-volcans. En la iteració 1 s'utilitzarà la primera corba que tingui Pendents[3], ja que en la llista de Pendents[2] no hi ha cap altra corba per tractar en aquest moment, de manera que es construirà el 3-volcà de A.

D'aquesta manera es considerarà en cada iteració la primera corba de la llista de Pendents[ℓ_i] no buida amb ℓ_i menor, fins que totes les llistes estiguin buides. Això es pot observar en l'última iteració, on tenim $\ell_{act} = 7$, però en haver inicialitzat $\ell_{lim} = 5$ no recorrerem els 7-volcans. Notem que ℓ_{act} ha arribat a 7 pel fet que en les llistes de pendents de 2, 3 i 5 ja no hi ha cap corba que no hagi estat tractada.

Més en concret, mostrem aquí un primer exemple sobre el cos $\mathbb{F}_{317}$ i corbes amb cardinal

$$m = 312 = 2^3 \cdot 3 \cdot 13.$$

Així, $t^2 - 4p = -2^4 \cdot 77$ i, per tant,

$$\mathbb{K} = \mathbb{Q}(\sqrt{-77}), \quad \mathcal{O}_{\mathbb{K}} = \langle 1, \sqrt{-77} \rangle, \quad D_{\mathbb{K}} = -4 \cdot 77$$

$$Disc(\mathbb{Z}[\pi] = -2^4 \cdot 77 = 2^2 D_{\mathbb{K}},$$

d'on resulta que el conductor de $\mathbb{Z}[\pi]$ en $\mathcal{O}_{\mathbb{K}}$ és $f = 2$. Com que aquestes corbes tenen cardinal múltiple de 3, admeten un model del següent tipus:

$$E_{a,b}/\mathbb{F}_p : y^2 + axy + by = x^3,$$

amb discriminant $\Delta = b^3(a^3 - 27b) \neq 0$. Cada classe d'isomorfia està unívocament representada per una corba $E_{1,\lambda}/\mathbb{F}_p$ (sent $\lambda = \frac{b}{a^3}$), excepte quan $a = 0$. En aquest cas, considerarem com a representant de la classe la corba $E_{0,1}/\mathbb{F}_p$. Per simplificar, denotarem aquestes corbes com E_λ, i E_0 la corba $E_{0,1}$.

Per això hem inicialitzat els paràmetres de l'algorisme amb la corba E_{316} sobre el cos $\mathbb{F}_{317}$. S'ha escollit 3 com a valor de ℓ_{lim}, per tant, la llista L_E={2,3}.

A partir d'aquesta corba obtenim el primer 2-volcà de la 2-cordillera. Tant la corba inicial com les corbes trobades en aquest 2-volcà s'afegeixen a Pendents[3]. En aquest cas, com que Pendents[2] es troba buida, es calcula el 3-volcà associat a E_{316}. Els nous nodes trobats en aquest còmput no havien estat tractats abans i donen lloc a l'obtenció de la resta de volcans de la 2-cordillera. Vegem els 2 i 3-volcans obtinguts:

2-Cord.: $\{\{E_{316},E_{259},E_{246},E_{205},E_{255},E_{284}\}, \{E_{137},E_{206},E_{36},E_{46},E_{119},E_{290}\}$
$\{E_{287},E_{87},E_{187},E_{250},E_{196},E_{70}\},\{E_{149},E_{116},E_{51},E_{42},E_{200},E_{148}\}\}$

3-Cord.: $\{\{E_{316},E_{137},E_{287},E_{149}\},\{E_{259},E_{206},E_{87},E_{116},E_{246},E_{36},E_{187},E_{51}\},$
$\{E_{205},E_{46},E_{250},E_{42}\},\{E_{255},E_{290},E_{196},E_{148},E_{284},E_{119},E_{70},E_{200}\}\}$

Quant a l'estructura dels volcans trobats en aquest exemple, podem veure que corresponen a dos tipologies. D'una banda, tots els 2-volcans tenen altura 1 i cràters formats per 2 nodes, mentre que els 3-volcans són plans (vegis Figura 5.1).

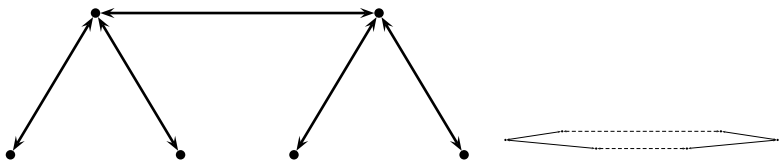


Figura 5.1: Estructura dels 2 i 3-volcans de l'exemple

Com es pot veure, en cadascuna de les ℓ-cordilleres ($\ell = 2$ o 3) apareixen totes les classes d'isomorfia amb cardinal $p + 1 - t = 312$ sobre el cos $\mathbb{F}_{317}$, en total (Teorema 4.6 de [Sch87]):

$$H(t^2 - 4p) = 24.$$

A més, aquestes classes d'isomorfia s'han distribuït en la 2-cordillera i en la 3-cordillera mantenint un determinat comportament: cada 3-volcà conté corbes de cadascun dels quatre 2-volcans (Figures 5.2 i 5.3). És a dir, si considerem un graf les arestes del qual fossin 2-isogènies i 3-isogènies, aquest seria connex.

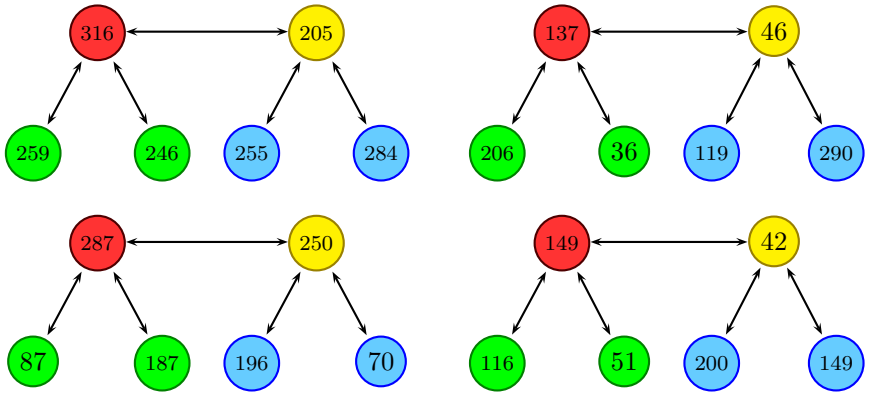


Figura 5.2: Cordilleres de 2-volcans sobre $\mathbb{F}_{317}$

Així mateix, considerant per cada parell de corbes E_λ, $E_{\lambda'}$ del graf de la forma quadràtica que assigna a cada isogènia $\mathcal{I} : E_\lambda \longrightarrow E_{\lambda'}$ el seu grau, podríem obtenir, segons [FMS$^+$08], més informació sobre els graus de les isogènies entre E_λ i $E_{\lambda'}$.

Considerem ara un altre exemple sobre el cos $\mathbb{F}_{691}$ i corbes amb cardinal

$$m = 700 = 2^2 \cdot 5^2 \cdot 7.$$

Aleshores $t^2 - 4p = -2700 = -2^2 \cdot 3^3 \cdot 5^2$ i, per tant,

$$\mathbb{K} = \mathbb{Q}(\sqrt{-3}), \quad \mathcal{O}_\mathbb{K} = \langle 1, \sqrt{-3} \rangle, \quad D_\mathbb{K} = -3$$

$$Disc(\mathbb{Z}[\pi]) = -2^2 \cdot 3^3 \cdot 5^2 = 2^2 \cdot 3^2 \cdot 5^2 \cdot D_\mathbb{K},$$

així doncs, el conductor de $\mathbb{Z}[\pi]$ en $\mathcal{O}_\mathbb{K}$ és $f = 2 \cdot 3 \cdot 5 = 30$.

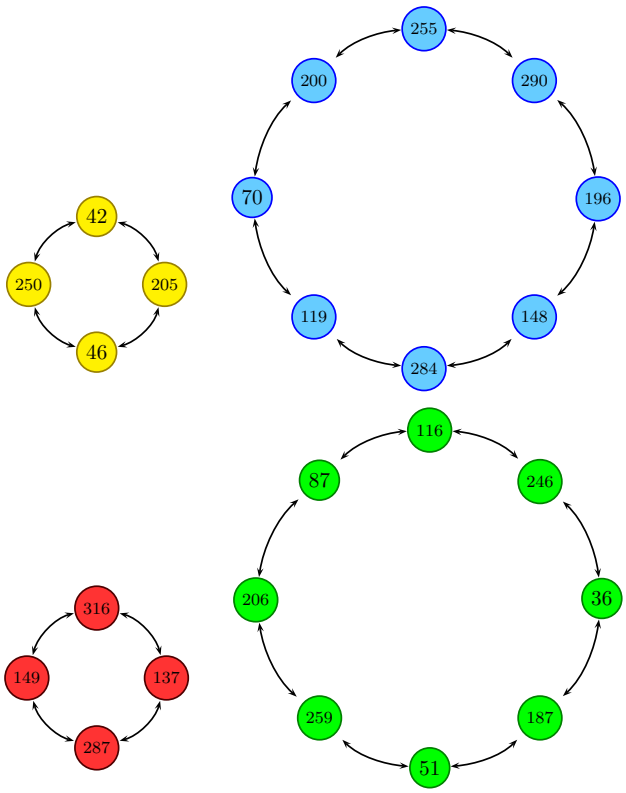


Figura 5.3: Cordilleres de 3-volcans sobre $\mathbb{F}_{317}$

En aquest exemple, cada classe d'isomorfia es denotarà com E_j, sent j el j-invariant de les corbes que formen aquesta classe. Els coeficients d'una corba de cada classe es poden calcular usant les expressions donades en 2.8.

L'algorisme ha treballat amb les 2, 3, 5 i 7-cordilleres. Tot seguit, es pot veure l'estructura dels volcans que les formen:

$$\begin{aligned}
\text{2-Cord.:}\quad & \{\{E_0, E_{102}\}, \{E_{53}, E_{52}, E_{440}, E_{460}\}, \{E_{674}, E_{61}, E_{91}, E_{172}\},\\
& \{E_{651}, E_{83}, E_{540}, E_{686}\}, \{E_{428}, E_{87}, E_{181}, E_{345}\},\\
& \{E_{170}, E_{98}, E_{317}, E_{406}\}, \{E_{647}, E_{101}, E_{118}, E_{468}\},\\
& \{E_{635}, E_{143}, E_{289}, E_{654}\}, \{E_{497}, E_{161}, E_{316}, E_{676}\},\\
& \{E_{619}, E_{192}, E_{573}, E_{610}\}\}
\end{aligned}$$

3-Cord.: $\{\{E_0, E_{53}\}, \{E_{102}, E_{52}, E_{440}, E_{460}\},$
$\{E_{540}, E_{345}, E_{61}, E_{101}, E_{317}, E_{676}, E_{610}, E_{654}\},$
$\{E_{83}, E_{87}, E_{406}, E_{172}, E_{118}, E_{573}, E_{316}, E_{289}\},$
$\{E_{686}, E_{181}, E_{91}, E_{98}, E_{468}, E_{192}, E_{161}, E_{143}\},$
$\{E_{651}, E_{428}, E_{170}, E_{647}, E_{674}, E_{635}, E_{619}, E_{497}\}\}$

5-Cord.: $\{\{E_0, E_{428}, E_{651}\}, \{E_{52}, E_{192}, E_{406}, E_{91}, E_{676}, E_{101}, E_{289}\},$
$\{E_{53}, E_{497}, E_{674}, E_{635}, E_{619}, E_{647}, E_{170}\},$
$\{E_{440}, E_{61}, E_{118}, E_{98}, E_{143}, E_{610}, E_{316}\},$
$\{E_{102}, E_{83}, E_{686}, E_{540}, E_{345}, E_{87}, E_{181}\},$
$\{E_{460}, E_{161}, E_{654}, E_{172}, E_{317}, E_{468}, E_{573}\}\}$

7-Cord.: $\{\{E_0\}, \{E_{53}\}, \{E_{102}\}, \{E_{428}, E_{651}\}, \{E_{52}, E_{440}, E_{460}\}$
$\{E_{61}, E_{161}, E_{406}, E_{610}, E_{468}, E_{289}\},$
$\{E_{83}, E_{345}, E_{686}, E_{87}, E_{540}, E_{181}\},$
$\{E_{91}, E_{316}, E_{317}, E_{192}, E_{118}, E_{654}\},$
$\{E_{98}, E_{573}, E_{101}, E_{143}, E_{172}, E_{676}\},$
$\{E_{170}, E_{619}, E_{647}, E_{635}, E_{674}, E_{497}\}\}$

De la valoració ℓ-àdica del conductor de $\mathbb{Z}[\pi]$ resulta que les altures dels 2, 3 i 5-volcans que formen les respectives cordilleres és 1, mentre que la dels 7-volcans és 0, és a dir, són volcans plans formats únicament per un cràter, i les corbes que els formen tenen solament 2 corbes isògenes diferents.

Agafant $E_{53} : y^2 = x^3 + 2x + 114$ com a corba inicial, com que el polinomi modular $\Phi_2(x, j)$ amb $j = 53$ té tres arrels, resulta que la corba E_{53} és al cràter del 2-volcà. En el cas del 3-volcà, el polinomi $\Phi_3(x, 53)$ té una única arrel $\tilde{j} = 0$ i, per tant, E_{53} és al terra. L'algorisme ens proporciona dos components connexes de la 2 i de la 3-cordillera, com podem veure en la Figura 5.4:

Aquestes dos components ens donen 6 classes d'isomorfia de les 38 que hi ha en total. Ara bé, per obtenir noves classes d'isomorfia el que fa l'algorisme és augmentar el valor de ℓ a 5 i calcular el 5-volcà de la nostra corba inicial

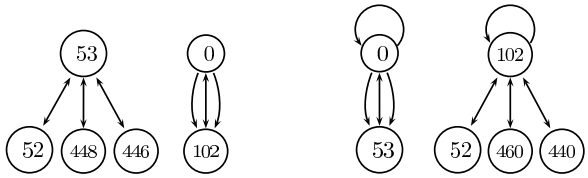


Figura 5.4: Volcans de 2 i 3-isogènies sobre $\mathbb{F}_{691}$

donant sis noves classes d'isomorfia que encara no s'havien tractat, com es pot veure en la Figura 5.5:

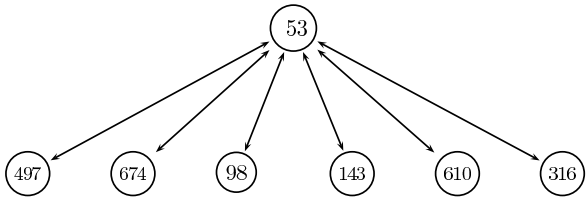


Figura 5.5: Volcà de 5-isogènies sobre $\mathbb{F}_{691}$

Amb les noves classes d'isomorfia que ens han aparegut en aquest 5-volcà, l'algorisme construeix els seus 2-volcans, i ens dóna 6 noves components de la 2-cordillera (vegis Figura 5.6) i accés a altres classes d'isomorfia encara no tractades.

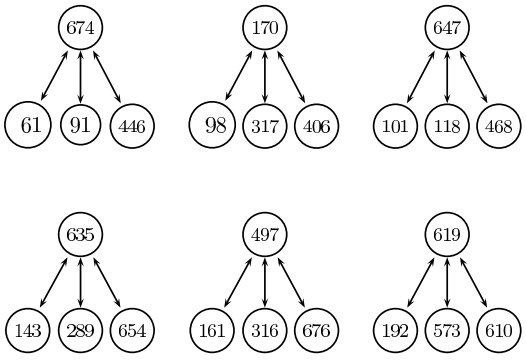


Figura 5.6: Volcans de 2-isogènies sobre $\mathbb{F}_{691}$

Un cop aquí, l'algorisme procedeix a construir els 3-volcans de les noves classes d'isomorfia de les quals encara no s'han tractat per al cas $\ell = 3$. En la Figura 5.7 es pot observar la construcció d'una d'aquestes components, més precisament el 3-volcà de la corba E_{497}:

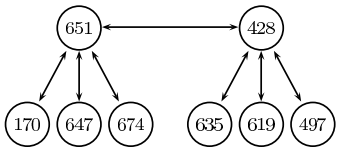


Figura 5.7: Volcà de 3-isogènies sobre $\mathbb{F}_{691}$

Finalment, construint els 2-volcans de les noves classes que ens han aparegut ja ens han sortit les 38 classes d'isomorfia sobre el cos $\mathbb{F}_q$ amb cardinal 700. Notem que no ha estat necessari construir cap component de la 7-cordillera. Si aquest no hagués estat el cas, l'algorisme hauria construït els 7-volcans corresponents i la 7-cordillera hauria quedat com es mostra en la Figura 5.8:

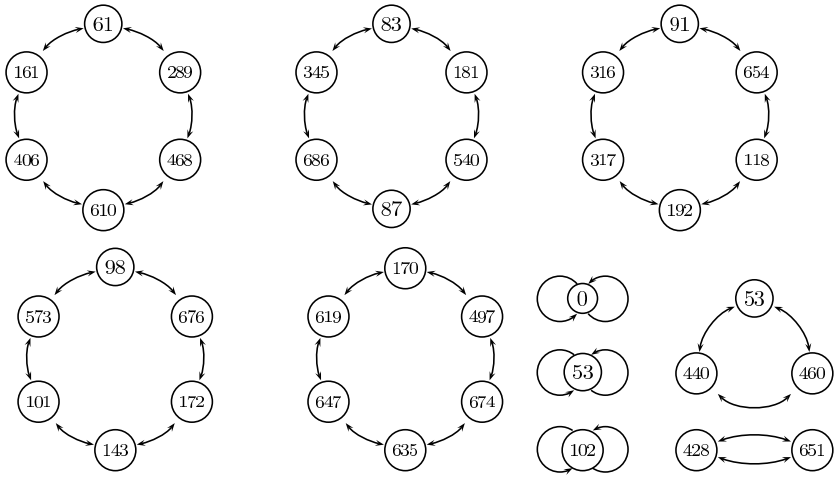


Figura 5.8: Cordillera de 7-volcans sobre $\mathbb{F}_{691}$

Capítol 6

Corbes resistents als atacs ZVP

Amb l'ús de la criptografia en dispositius com les targetes intel·ligents apareixen nous atacs, com els *Side-Channel Attacks* [Joy03], presentats en el Capítol 3. A causa d'aquests atacs i a les limitacions de còmput i memòria, la criptografia el·líptica esdevé una de les més apropiades en aquest tipus de dispositius.

La criptografia amb corbes el·líptiques és, també, vulnerable a aquests atacs, però la mida de la clau en aquest cas deixa més marge per ampliar el nombre de bits sense que l'eficiència se'n ressenti gaire. En aquest tipus de criptografia, apareix un altre atac del grup dels *Side-Channel Attacks*, conegut com *Zero-Value Point Attack* i proposat per L. Goubin [Gou03]. En aquest capítol es comenten les contramesures proposades per N. Smart i Akishita-Takagi [Sma90, AT03, AT04] i es dóna una proposta per millorar-les [MST+09].

Finalment, en aquest capítol, també proposem una nova contramesura a aquests atacs, més eficient que les proposades anteriorment, basada en l'ús de corbes d'Edwards [Edw07], que tenen la propietat de no ser vulnerables als atacs ZVP [MST+10].

6.1 Atacs *Zero-Value Point* i contramesures

La idea plantejada d'utilitzar criptografia el·líptica en les targetes intel·ligents per millorar els temes d'espai de memòria i capacitat de còmput no queda exempta d'atacs Side-Channel.

Un atac pertanyent a aquest tipus va ser trobat per L. Goubin [Gou03] en

adonar-se'n que si la targeta treballava amb un punt amb abscissa o ordenada amb valor 0, aleshores el consum de la targeta intel·ligent tenia un decrement considerable. Aquesta diferència de consum és fàcilment identificable en les traces de consum que s'obtenen enal fer operacions amb aquests punts, anomenats *punts especials*.

Per demostrar-ho, L. Goubin va mostrar el funcionament d'aquest atac mitjançant la construcció d'un punt de forma recursiva, que va donant el bit i-èssim en aquesta iteració, coneixent els $i-1$ bits anteriors de la clau. Dit d'una altra manera, l'atacant suposaria que el bit i-èssim de la clau tindria un dels dos possibles valors. A partir d'aquesta suposició, construiria, coneixent també tots els bits anteriors a aquest, el punt que fes, en la iteració i-èssima, aparegués un punt especial si la suposició ha estat correcta. Aleshores, l'atacant únicament hauria d'observar la potència de consum en aquesta iteració i veure si hi ha la davallada que produiria un punt especial o no.

Així, si aparegués el punt especial voldria dir que l'atacant tenia raó i el valor del bit i-èssim era el predit amb anterioritat, mentre que si no s'obtingués aquesta davallada en el consum, el bit i-èssim seria el negat del que havia suposat. Per tant, ja sigui per encertar-lo o per no encertar-lo, l'atacant sabria el valor exacte del bit i-èssim de la clau. Aleshores podria passar a construir un altre cop un punt com en el cas anterior, però ara deduint quin seria el bit $(i+1)$-èssim coneixent els valors dels i bits anteriors. Aquest procés començaria pel primer bit de la clau secreta i conclouria amb l'últim bit. Per tant, en n passos, sent n la mida de la clau, l'atacant obtindria la clau.

Les contramesures proposades per J. S. Coron [Cor99] i Joye-Timen [JT01] utilitzades en els atacs *Side-Channel* anteriors en corbes el·líptiques, no pal·liaven aquest atac, ja que fetes les modificacions, canvis d'una corba a les seves isomorfes, els punts amb coordenades amb valor 0 es mantenien, és a dir, si bé no eren el mateix punt, el punt resultant continuava sent especial.

Tot i així, L. Goubin va proposar utilitzar corbes en les quals no apareguessin punts amb alguna coordenada amb valor 0 i va donar unes condicions que havia de tenir la corba perquè això no passés. Aquestes condicions són que el paràmetre b de l'equació de Weierstraß:

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b$$

no sigui un residu quadràtic, per tant, la corba no tindria punts d'ordre 2 que són de la forma $P = (0, y)$. Pel que fa a l'ordenada, únicament existeixen punts de la forma $(x, 0)$ en cas que la corba tingui cardinal 2 i, com que les corbes el·líptiques donades per l'Standards for Efficient Cryptography Group (SECG) [SEC] tenen cardinal primer, no pot passar que en el grup de punts de la corba el·líptica utilitzada ens trobem un punt que compleixi que la seva ordenada sigui zero.

6.1.1 Condicions d'existència de *Zero-Value Points*

T. Akishita i T. Takagi [AT03, AT04], continuant amb l'atac que va enunciar L. Goubin, van demostrar que no solament donaven informació punts amb alguna coordenada amb valor 0, sinó que hi havia alguns paràmetres intermedis que s'usaven en la suma i el doblat de punts que, si tenien valor 0, també hi havia una davallada en el consum de potència, i es donava informació a l'atacant. Així, i englobant també les condicions trobades per L. Goubin, van donar un llista de condicions que, si se'n complia alguna, la corba era vulnerable.

Si $P = (x, y)$ és un punt de la corba $E/\mathbb{F}_p : y^2 = x^3 + ax + b$, les condicions que no s'han de complir en el cas del doblat són:

ED1: $3x^2 + a = 0$;

ED2: $5x^4 + 2ax^2 - 4bx + a^2 = 0$;

ED3: L'ordre de P sigui igual a 3;

ED4: $x(P) = 0$ o $x(2P) = 0$, és a dir, b sigui un residu quadràtic;

ED5: $y(P) = 0$ o $y(2P) = 0$, és a dir, l'ordre de P sigui igual a 2,

mentre que les obtingudes de la suma de dos punts P i cP, $c \in \mathbb{F}_p$, són:

EA1: L'ordenada del punt P sigui d'autocol·lisió;

EA2: $x(cP) + x(P) = 0$;

EA3: $x(P) - x(cP) = \lambda(P, cP)^2$;

EA4: $2x(cP) = \lambda(P, cP)^2$, $x(cP) = \lambda(P, cP)^2$ o $x((c+1)P) = \lambda(P, cP)^2$;

EA5: L'ordre de P sigui $2c + 1$;

EA6: $x(cP) = 0$, $x(P) = 0$ o $x((c + 1)P) = 0$;

EA7: $y(cP) = 0$, $y(P) = 0$ o $y((c + 1)P) = 0$,

on $\lambda(P, cP) = \frac{y(cP)-y(P)}{x(P)-x(cP)}$.

Per la complexitat de les noves condicions donades, T. Akishita i T. Takagi únicament van introduir una nova condició que no era tractada per N. Smart, i aquesta va ser la condició ED1. Així, ells buscaven corbes en què el paràmetre b de la corba no fos un residu quadràtic i que no existís cap punt pertanyent a la corba en què $3x^2 + a = 0$.

Estudiem ara, de forma no exhaustiva, la probabilitat que una corba el·líptica definida sobre un cos finit compleixi alguna de les condicions enunciades. Les probabilitats que hem obtingut, suposant que totes les condicions són independents les unes de les altres, han estat les següents.

- En el cas de la condició ED4, és a dir, que el paràmetre b de la corba el·líptica sigui residu quadràtic, la probabilitat és d'$1/2$, ja que es redueix a mirar si un nombre dins d'un cos finit és o no un quadrat i, en un cos finit, la meitat dels nombres són residus quadràtics.

- D'altra banda, la probabilitat que una corba no satisfaci la condició ED1, $3x^2 + a = 0$ és al voltant d'$1/4$, ja que la probabilitat que $a/3$ sigui residu quadràtic, com que en el cas anterior és $1/2$, la probabilitat que x sigui l'abscissa d'un punt que pertanyi a la corba que és també, aproximadament, $1/2$.

- Veient aquestes probabilitats, i mirant cada cas en concret, tenim que N. Smart tracta la condició que s'ha anomenat ED4, que té una probabilitat d'$1/2$. D'altra banda, en el cas de T. Akishita i T. Takagi, busquen corbes que no compleixin les condicions ED1 i ED4. Utilitzant els càlculs de

l'apartat anterior tenim que la probabilitat de trobar una corba que no satisfaci ambdues condicions és de l'ordre d'1/8.

- Finalment, la probabilitat de trobar una corba que no sucumbeixi a les condicions ED1, ED2 i ED4 és d'aproximadament 3/40. Aquesta probabilitat ve del fet que la corba no compleixi les condicions ED1 i ED4, és a dir, 1/8, i que la corba no satisfaci ED2. La probabilitat que aquesta condició no es compleixi és d'aproximadament 3/5, i s'obté de mirar que el polinomi $5x^4 + 2ax^2 - 4bx + a^2$ no tingui cap arrel i, en cas que en tingui alguna, que cap de les seves arrels sigui abscissa d'algun punt de la corba.

6.1.2 Corbes isògenes per evitar atacs ZVP

N. Smart [Sma90], estudiant l'atac ZVP, va trobar una solució factible sense haver de canviar les dades de partida sobre el cardinal de la corba el·líptica. Aquesta solució consistia a buscar una corba isògena a l'emmagatzemada de manera que el seu paràmetre b no sigui un residu quadràtic. Així, l'ús d'una corba isògena a l'inicial ens dóna, presumiblement, la mateixa seguretat que tenia l'original [JMV05], però sense que aquesta sigui vulnerable a aquest atac. T. Akishita i T. Takagi, en els seus treballs [AT03, AT04], també proposaven el càlcul d'isogènies com a contramesura a aquest atac.

La tècnica proposada era, a partir de la corba inicial, que no complia les condicions que ells tractaven calculant les seves ℓ_1-isògenes adjacents, essent ℓ_1 el menor nombre primer de manera que existeix almenys una isògena de la corba inicial. Si aquestes noves corbes trobades tampoc complien totes les condicions, aleshores calculaven les ℓ_2-isogènies, essent ℓ_2 el següent primer pel qual existeixen isogènies; i així s'anava augmentant el valor dels primers ℓ_i fins a trobar una isogènia que satisfés totes les condicions desitjades.

D'altra banda, les corbes que es donen com a estàndard en SECG [SEC], compleixen totes que el paràmetre a pren el valor -3. Aquesta condició no és cap condició que faci la corba més resistent enfront els atacs ZVP, únicament es tracta d'una condició d'eficiència a l'hora de fer doblats de punts.

Hem de pensar que en alguns casos és impossible trobar una corba que

compleixi les condicions ED1, ED2 i que el seu paràmetre $a = -3$, com es dedueix dels resultats següents:

Proposició 6.1. *Sigui E una corba el·líptica definida sobre un cos finit $\mathbb{F}_p$ d'equació $y^2 = x^3 + ax + b$. Si $a = -3$, $\#E(\mathbb{F}_p)$ és senar i $\left(\frac{-3}{p}\right) = 1$, aleshores existeix almenys un punt $P = (x, y) \in E(\mathbb{F}_p)$, que satisfà $3x^2 + a = 0$.*

Demostració. En cas que $E/\mathbb{F}_p$ tingui cardinal senar, cap punt $P \in E(\mathbb{F}_p)$ serà de la forma $P = (x, 0)$, per tant, l'equació $x^3 + ax + b = 0$ no tindrà solució. D'altra banda, en cas que $a = -3$, la condició $\left(\frac{-3}{p}\right) = -1$ implica que $\left(\frac{(b+2)(b-2)}{p}\right) = -1$ perquè

$$\Delta = -16(4(-3)^3 + 27b^2) = -3(12)^2(b+2)(b-2).$$

Com que sabem que $\left(\frac{\Delta}{p}\right) = 1$, aleshores

$$\left(\frac{b+2}{p}\right) = -1 \text{ o } \left(\frac{b-2}{p}\right) = -1.$$

Per tant, l'equació de la corba amb $a = -3$ i $x = \pm 1$ té solució en y. Conseqüentment, la corba el·líptica $E/\mathbb{F}_p$ té un punt que compleix que $3x^2 + a = 0$. □

Corol·lari 6.2. *Sigui E una corba el·líptica definida sobre un cos $\mathbb{F}_p$. Si $\#E(\mathbb{F}_p)$ és senar i $\left(\frac{-3}{p}\right) = -1$, aleshores E no pot tenir cap corba isògena E' amb paràmetre $a = -3$ i resistent contra els atacs ZVP.*

Utilitzant les probabilitats donades en la subsecció 6.1.1 i el cost computacional de calcular una ℓ-isogènia podem dir que trobar una corba resistent o, en altres paraules, que satisfaci una sèrie de condicions, utilitzant el mètode anterior, pot fer que el cost computacional incrementi bastant, atès que en cada pas s'anirà augmentant el valor de ℓ. En canvi, si utilitzem l'algorisme *Isogeny-route* descrit en la secció següent, el valor de ℓ es mantindrà més estable, cosa que comportarà que el cost no augmenti en cada pas. Per aquesta raó, s'ha pogut tractar també la condició ED2 sense un increment temporal i computacional molt elevat.

6.2 Ruta d'isogènies en una cordillera

En aquesta secció, es descriu un algorisme [MST+09] per obtenir corbes resistents a l'atac ZVP de forma més ràpida i eficient que les propostes anteriors. Per aconseguir-ho, s'utilitzen les estructures de volcans d'isogènies vistos en la secció 4.1 i, més concretament, cordilleres de volcans per trobar un camí entre aquestes més ràpid per obtenir una corba "bona".

6.2.1 Algorisme

Hem vist que tant N. Smart [Sma90] com T. Akishita i T. Takagi [AT03, AT04], a partir d'una corba vulnerable, buscaven una corba isògena resistent.

El problema ve quan no es troben corbes bones amb valors ℓ petits, donat que el càlcul d'una isogènia és de l'ordre de $\mathcal{O}(\ell^2(\ln p))$. Per tant, si augmentem el valor de ℓ el cost incrementa de forma considerable.

La idea principal de la proposta que presentem, l'algorisme *Isogeny-route* [MST+09], es basa en el fet que és més simple i eficient fer una ℓ-isògena com més petit és aquest valor de ℓ. L'algorisme *Isogeny-route*, per trobar una corba resistent, va generant primer el seu ℓ_1-volcà, no només les ℓ_1 isogènies, com feien N. Smart i T. Akishita i T. Takagi. Si dins d'aquest volcà no en troba cap, calcula les ℓ_2-isogènies de la corba inicial, i mira si compleixen o no les condicions. En cas que cap sigui resistent, continua generant els ℓ_1-volcans. D'aquesta manera, i donat que les probabilitats són independents, es troben corbes resistents millorant els temps que s'han necessitat amb el mètode anterior.

Ara es mostrarà la proposta en pseudocodi:

Les funcions utilitzades per l'algorisme són:

- Pendent[i]: És un vector de llistes de corbes el·líptiques que han aparegut en els còmputs i a les quals no se'ls han calculat les ℓ_i-isogènies.

- GrausIsogenia[i]: Conté una llista de primers ℓ_1, ℓ_2, ..., ℓ_n pels quals E té almenys una isogènia.

- Tractada[i]: És també un vector de llistes de corbes que ja han comprovat

Algorisme 8 Isogeny-route

Entrada: Una corba el·líptica E sobre un cos finit $\mathbb{F}_p$, una llista de n primers on E té almenys una isogènia
Sortida: Una corba el·líptica E', isògena a E, resistent a l'atac ZVP

si *E és resistent a ZVP* **llavors**
  retorna *E;*
fi
mentre $\exists j,\ j = 0$ **fins** $n-1$ **de manera que** *Pendent[j]*$\neq \emptyset$ **fer**
  ℓ = GrausIsogenia[j];
  E_{actual} =PrimerElement(Pendent[j]);
  Tractada[j]$\leftarrow E_{actual}$;
  Borrar(E_{act}, Pendent[j]);
  $E_{segent} = \ell$-isogeny(E_{actual});
  si *ZVP-Resistent*(E_{segent}) **llavors**
    retorna E_{segent};
  fi
  per a $i = 0$ **fins** $n-1$ **de manera que** $i \neq j$ **fer**
    Pendent[i]$\leftarrow E_{segent}$;
  fi
fi

que no compleixen totes les condicions i que ja s'han emmagatzemat totes les seves ℓ_i-isogènies.

- ZVP-Resistent(E): Comprova si la corba E compleix o no totes les condicions proposades.

Pel que fa al funcionament, cal dir que aquest algorisme s'haurà executat prèviament; d'aquesta manera, a la targeta intel·ligent ja se li haurà inserit la corba resistent i el millor camí per arribar-hi des de la corba inicial. Per tant, el cost computacional que haurà de fer la targeta intel·ligent és passar els punts de la corba inicial als de la isogènia, fer els còmputs necessaris en aquesta isogènia i, finalment, passar el punt obtingut a la corba inicial.

6.2.2 Implementació i complexitat

En aquesta secció, mostrarem els resultats obtinguts després d'haver fet la implementació dels dos mètodes. Les proves s'han realitzat utilitzant les corbes

que apareixen a la llista del SECG [SEC], que són considerades un estàndard en la criptografia de corbes el·líptiques. Aquestes implementacions han estat fetes utilitzant el programa MAGMA [BCP97] i les isogènies s'han calculat emprant polinomis de divisió.

Tant el mètode utilitzat per N. Smart [Sma90] com per T. Akishita i T. Takagi [AT03, AT04] consisteix a anar incrementant el valor del primer ℓ fins a trobar una corba ℓ-isogènia resistent o, millor dit, una corba que satisfaci totes les condicions demanades en cada moment.

El mètode que proposem en [MST+09] (*Isogeny-route*) utilitza la concatenació de ℓ-isogènies. Això implica que no cal incrementar el valor de ℓ en cada pas. Únicament es canviarà el valor de ℓ quan s'hagi recorregut tot el ℓ-volcà actual. El valor del paràmetre ℓ utilitzant aquest nou algorisme no sols s'incrementa en cas que no hagi trobat cap corba resistent en el ℓ-volcà actual, sinó que també pot decrementar-se en cas que hagin aparegut corbes que no s'hagin tractat amb valors anteriors del paràmetre ℓ.

Finalment, quan l'algorisme trobi una corba resistent o, millor dit, que compleixi les condicions demanades, ens retornarà el camí d'isogènies més ràpid que ens porti de la corba inicial a aquesta corba resistent, sent aquest camí, també, el que utilitza valors de ℓ més petits.

Aquest nou mètode utilitza menys temps per obtenir una corba resistent, sense oblidar-nos que el cost computacional de calcular una ℓ-isogènia augmenta considerablement alhora que va augmentant el valor de ℓ.

En aquest mètode s'assumeix que el comportament de les corbes és independent del grau de la isogènia que es tracta, és a dir, que hi ha la mateixa probabilitat de trobar una corba que compleixi les condicions demanades en cada cas calculant isogènies de graus petits que calculant isogènies de graus grans. Considerant que el cost de calcular una ℓ-isogènia en $\mathbb{F}_p$ és $\mathcal{O}(\ell^2(\ln p))$, podem afirmar que és preferible que el grau de la isogènia sigui el més petit possible. En aquest sentit, l'algorisme isogeny-route afavoreix que apareguin resultats millors.

6.3 Resultats i exemples

En aquesta secció mostren les taules obtingudes pel que fa al temps i al camí d'isogènies recorregut en els diferents casos que s'han tractat, tant en el nostre com per a N. Smart i per a T. Akishita i T. Takagi. També hi hem afegit una taula on es mostra la cerca d'una corba que no satisfaci les condicions ED1, ED2 i ED4, un cas que no s'ha tractat amb l'altre mètode. Per obtenir aquestes taules s'ha utilitzat la llista de corbes que apareixen en el SECG. Aquesta llista està formada per nou corbes definides sobre un cos $\mathbb{F}_p$ denotades per:

secp112r1, secp128r1, secp160r1, secp160r2, secp192r1, secp224r1, secp256r1, secp384r1 i secp521r1,

on els dígits que segueixen secp són la mida en bits del primer p del cos $\mathbb{F}_p$ on està definida cada corba. Així, secp192r1 ve definida pels següents paràmetres:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF= $2^{192} - 2^{64} - 1$

a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFC

b = 64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1

En la Taula 6.1 podem observar els resultats obtinguts per N. Smart amb el seu mètode comparant-los amb elss obtinguts utilitzant el mètode proposat. En aquesta taula apareixen dos notacions noves:

- ℓ_{std}: El grau mínim de la isogènia que no satisfà la condició ED4;
- ℓ_{prf}: El grau mínim de la isogènia que no satisfà la condició ED4 i en què $a = -3$;

Les notacions de ℓ_{std}-route i ℓ_{prf}-route fan referència al camí d'isogènies trobat per l'algorisme des de la corba inicial fins a una corba resistent a les condicions demanades. En el cas de ℓ_{std}-route, hi veurem el camí d'isogènies

fins a trobar una corba resistent, mentre que en ℓ_{prf}-route, a més a més de satisfer les condicions de seguretat, la corba trobada també complirà que el seu paràmetre $a = -3$.

ED4	ℓ_{std}	ℓ_{std}-route	ℓ_{prf}	ℓ_{prf}-route
secp112r1	1	1	1	1
secp128r1	7	7	7	7
secp160r1	13	13	13	13
secp160r2	19	19	*41*	*19-19*
secp192r1	*23*	*5-13*	*73*	*5-13-23*
secp224r1	1	1	1	1
secp256r1	3	3	*11*	*3-5*
secp384r1	19	19	19	19
secp521r1	5	5	5	5

Taula 6.1: Graus més petits trobats de les isogènies resistents a ED4

A les dos primeres columnes de la Taula 6.1 tenim calculat amb els dos mètodes, en cas que sigui necessari, el camí d'isogènies per obtenir una corba resistent a la condició ED4. En les dos últimes columnes, mirem si es compleix que el paràmetre a de la corba és -3. Veiem que les diferències que hem obtingut sobre el grau de les isogènies estan en itàlica.

En la Taula 6.2 veiem com aquestes diferències en els graus de les isogènies es plasmen en el cost temporal i conseqüentment en millores de temps de la proposta que presentem respecte a les existents.

T. Còmput/T. Cerca.	Mètode anterior (seg.)	Isogeny-route (seg.)
secp160r2 (ℓ_{prf})	267.63 / 547.01	41.8 /46.78
secp192r1 (ℓ_{std})	44.30 / 51.24	6.01 / 6.99
secp192r1 (ℓ_{prf})	3474.7 / 4788.15	50.31 / 59.22
secp256r1 (ℓ_{prf})	5.93 / 6.43	0.035 / 0.043

Taula 6.2: Temps de càlcul de corbes isògenes resistents a ED4

En aquesta Taula 6.2 podem observar dos valors de temps:

- Temps de Còmput: És el temps necessari per calcular, a partir d'una corba inicial, la corba isògena resistent.

- Temps de Cerca: És el temps que es perd fent proves fins a obtenir una isogènia resistent.

Així, el temps de cerca d'una isògena resistent per la corba secp192r1 en el cas del grau ℓ_{std} utilitzant el mètode anterior es donaria per:

- Primer calcular les 5-isogènies, després les 11-isogènies, les 13-isogènies i, finalment, la trobaríem fent el càlcul de les 23-isogènies,

mentre que el temps de còmput seria únicament calcular a partir de la corba inicial la seva 23-isogènia resistent. En aquesta corba no existeixen corbes isògenes de graus 2, 3, 7, 17 ni 19, i és per això que no es calculen.

En aquesta taula es pot observar que per la corba secp192r1 en el cas del grau ℓ_{prf} el temps utilitzant el mètode anterior és més de 80 vegades el que ens dóna utilitzant l'*Isogeny-route*.

Ara veurem els resultats obtinguts utilitzant les condicions tractades per T. Akishita i T. Takagi, és a dir, ED1 i ED4. En la Taula 6.3 es pot veure la comparació dels resultats obtinguts mitjançant ambdós mètodes amb aquestes dos condicions:

ED1+ED4	ℓ_{std}	ℓ_{std}-route	ℓ_{prf}	ℓ_{prf}-route
secp112r1	7	7	-	-
secp128r1	7	7	7	7
secp160r1	13	13	13	13
secp160r2	19	19	*41*	*19-23-23*
secp192r1	*23*	*13-13*	-	-
secp224r1	1	1	1	1
secp256r1	3	3	*23*	*5-11*
secp384r1	31	31	-	-
secp521r1	5	5	5	5

Taula 6.3: Graus més petits trobats de les isogènies resistents a ED1 i ED4

En aquesta Taula 6.3 es pot observar que hi ha corbes per a les quals no hi ha cap isògena que no satisfaci ED1 ni ED2 i, a més, el paràmetre de la corba sigui $a = -3$. Ara veurem la comparativa de temps en la Taula 6.4, en què es mostrem únicament els casos on l'algorisme *Isogeny-route* ha trobat una camí d'isogènies. Els temps tornen a ser més eficients utilitzant el nou mètode.

T. Còmput/T. Cerca	Mètode anterior (seg.)	Isogeny-route (seg.)
secp160r2 (ℓ_{prf})	267.63 / 547.01	91.8 / 146.78
secp192r1 (ℓ_{std})	44.30 / 51.24	11.92 / 16.35
secp256r1 (ℓ_{prf})	97.11 / 145.87	6.07 / 6.45

Taula 6.4: Temps de càlcul de corbes isògenes resistents a ED1 i ED4

Com s'ha vist en les taules anteriors, els temps obtinguts amb l'algorisme *Isogeny-route* han estat millors que els obtinguts amb el mètode anterior; a més a més, un altre avantatge que ens ofereix aquest algorisme és que obtenim moltes més corbes en menys temps que amb els altres mètodes. Això ens permet poder fer cerques més restrictives sense augmentar molt els temps de càlcul. D'aquesta manera, utilitzant aquest algorisme, s'ha introduït en la cerca una altra condició, concretament la condició ED2, sense que això produís un augment considerable dels graus de les isogènies que s'han calculat. El fet que els valors de ℓ s'hagin mantingut relativament petits ha fet possible que es pogués tractar aquesta nova condició sense que els valors de ℓ augmentessin excessivament.

En la Taula 6.5 es poden observar els resultats tant sobre el camí d'isogènies com sobre el cost temporal obtinguts a l'hora de tractar les condicions ED1, ED2 i ED4 a la llista de corbes del SECG. De fet, només en tres d'aquestes nou corbes s'obté una corba isògena diferent que si tractessin únicament les condicions ED1 i ED2.

ED1+ED2+ED4	ℓ_{std}-route	temps-route
secp112r1	7	0.22
secp128r1	7	0.332
secp160r1	13	4.93
secp160r2	19	16.58
secp192r1	13-13	13.44
secp224r1	3-3	0.06
secp256r1	3	0.02
secp384r1	19-19-19-19	327.93
secp521r1	7-7	8.38

Taula 6.5: Grau i temps de còmput d'una isògena resistent a ED1, ED2 i ED4

Les equacions de les corbes isògenes d'aquests resultats han estat calculades utilitzant polinomis de ℓ-divisió. També s'haurien pogut calcular utilitzant polinomis modulars $\Phi_\ell(x, y)$, però en MAGMA [BCP97] únicament estan emmagatzemats fins a un cert valor de ℓ. Utilitzant aquests altres polinomis els temps continuen essent més baixos utilitzant l'algorisme *Isogeny-route* que el mètode utilitzat per N. Smart i Akishita-Takagi.

6.4 Corbes d'Edwards com a contramesura dels atacs ZVP

En aquesta secció es planteja una alternativa a l'ús d'isogènies de corbes el·líptiques per evitar atacs ZVP, l'ús de corbes d'Edwards.

D. Bernstein i T. Lange han mostrat recentment en [BL07] que les corbes d'Edwards són també compatibles amb mesures de prevenció davant atacs SCA, com ara l'aleatorització d'escalars, de coordenades, de punts o de corbes. Aquí ens plantegem si les corbes d'Edwards també poden emprar-se per evitar atacs ZVP [MST$^+$10]. Per aquest motiu, estudiem quan els paràmetres intermedis poden anul·lar-se durant els procediments de suma i doblat. Concloem que això només succeeix per a punts que no són criptogràficament interessants, per la qual cosa usar corbes d'Edwards en targetes intel·ligents resulta segur contra aquest tipus d'atacs.

Noti's que prendre corbes d'Edwards (quan això sigui possible) serà una contramesura més eficient que buscar corbes isògenes. Malauradament, l'inconvenient és que no totes les corbes el·líptiques tenen una corba equivalent en la forma d'Edwards.

6.4.1 Possibles *Zero-Value Points* del doblat

A partir de les fórmules donades en la secció 2.11 per al doblat d'un punt en una corba d'Edwards, el resultat següent determina les condicions perquè un punt sigui un ZVP.

Teorema 6.3. *Sigui $x^2 + y^2 = c^2(1 + dx^2y^2)$ una corba d'Edwards sobre un cos finit amb d un no residu quadràtic. Un punt P és un ZVP per al doblat si, i només si, P és l'element neutre de la suma, o és un punt d'ordre 2, 4 o 8.*

Demostració. Usant coordenades projectives, sigui $P = (X_1 : Y_1 : Z_1)$ el punt a doblar. Els paràmetres intermedis poden ser zero si, i només si, algun dels següents valors (de les expressions del doblat) s'anul·len:.

$$(X_1 + Y_1)^2, X_1^2, Y_1^2, X_1^2 + Y_1^2, cZ_1, E - 2H,\ B - E,\ C - D$$

Noti's que $Z_1 \neq 0$ lloc que estem tractant amb punts afins. Si $X_1 = 0$, el punt P seria o bé l'element neutre $(0, c)$ o el punt d'ordre 2 $(0, -c)$. En cas que $Y_1 = 0$, el punt és un dels dos punts d'ordre 4 de la corba: $(c, 0)$ o el seu oposat $(-c, 0)$.

La condició $B - E = 0$ és equivalent a $0 = (X_1 + Y_2)^2 - X_1^2 - Y_1^2 = 2X_1^2Y_1^2$, la qual cosa es redueix als casos anteriors.

Si es compleix $E - 2H = 0$, prenent coordenades afins, s'ha de $x_1^2 + y_1^2 = 2c^2$; llavors, com que el punt pertany a la corba, es conclou que $1 = dx_1^2y_1^2$, la qual cosa contradiu el fet que d és un no quadrat. Similarment, s'aconseguiria la mateixa contradicció si es considerés $X_1^2 + Y_1^2 = 0$.

El cas més interessant ocorre quan $(X_1 + Y_1)^2$ o $C - D = X_1^2 - Y_1^2$ són zero. En aquesta situació, el punt afí és o bé $(x_1, -x_1)$ o (x_1, x_1). Com que $2(x_1, -x_1) = (-c, 0)$ i $2(x_1, x_1) = (c, 0)$, aquests són punts d'ordre 8.

Noti's que existeixen punts d'ordre 8 en la corba si, i només si, $1 - c^4d$ és un residu quadràtic (aquesta condició es dedueix fàcilment en verificar l'existència de punts $(x_1, -x_1)$ o (x_1, x_1) en la corba). □

6.4.2 Possibles *Zero-Value Points* de la suma

De manera similar al cas del doblat, el resultat següent determina les condicions necessàries i suficients perquè un punt P sigui un punt de valor zero en calcular la suma $P + kP$.

Teorema 6.4. *Sigui $x^2 + y^2 = c^2(1 + dx^2y^2)$ una corba d'Edwards sobre un cos finit, amb d un no residu quadràtic. Un punt P és un ZVP per a la suma de P i $kP = (x_2, y_2)$ si, i només si, P és l'element neutre per a la suma, o és un punt d'ordre 2, 4 o 8 o el seu ordre és un divisor d'algun dels nombres enters $\{k, k+1, 2k, 2(k+1), 4k, 4(k+1), 8k\}$.*

Demostració. Utilitzant coordenades projectives, sigui $P = (X_1 : Y_1 : Z_1)$ el punt sumat a $kP = (X_2 : Y_2 : Z_2)$. Els paràmetres intermedis poden ser zero si, i només si, algun dels valors següents (de les expressions de la suma) s'anul·la:

$$Z_1Z_2, X_1X_2, Y_1Y_2, B - E, B + E, (X_1 + Y_1)(X_2 + Y_2), Y_3, X_3,$$

on $(k+1)P = (X_3 : Y_3 : Z_3)$.

Donat que estem sumant punts afins, Z_1Z_2 necessàriament serà no nul. Si $X_1X_2 = 0$, llavors X_1 o X_2 són zero. En el primer cas, P és element neutre de la suma, o és el punt d'ordre 2 de la corba. En el segon cas, o bé $kP = (0, c)$ o bé $2kP = 2(0, -c) = (0, c)$. Llavors l'ordre de P divideix a k o a $2k$. El cas $Y_1Y_2 = 0$ es pot tractar de forma similar, i s'obté que P és d'ordre 4 o la seva ordre és un divisor de $4k$.

Noti's que $B - E$ i $B + E$ mai poden ser 0; en cas contrari, prenent coordenades afins, hauria d'haver-se de $dx_1x_2y_1y_2 \in \{-1, 1\}$, la qual cosa contradiu la propietat de completesa de la suma sobre la corba d'Edwards (Teorema 3.3 en [BL07]).

Si $(X_1+Y_1)(X_2+Y_2) = 0$, procedint de forma similar que en la demostració del teorema anterior, s'obté que P o kP tenen ordre 8. En l'últim cas, l'ordre de P és un divisor de $8k$.

Si $I_3 = 0$, o bé ens trobem en un dels casos anteriors o bé $D - C = 0$. En aquesta situació, s'obté que l'ordre de P és un divisor de $4(k+1)$, ja que $(k+1)P$ té ordre 4.

Finalment, si $X_3 = 0$, llavors o $(k+1)P = (0, c)$ o $(k+1)P = (0, -c)$ i, per tant, l'ordre de P és un divisor de $k+1$ o de $2(k+1)$. □

Noti's que l'última condició en el Teorema 6.4 és equivalent al següent lema, on r és l'ordre del punt P.

Lema 6.5. *Sigui r un primer > 2 i k un enter no negatiu menor que r. Llavors r és un divisor d'algun dels enters $\{k, k+1, 2k, 2(k+1), 4k, 4(k+1), 8k\}$ si, i només si, $k = 0$ o $k = r - 1$.*

Finalment, a partir dels Teoremes 6.3 i 6.4, podem concloure que:

Corol·lari 6.6. *Les corbes d'Edwards són adequades per ser implementades en targetes intel·ligents que usin criptografia de corbes el·líptiques, perquè són resistents als atacs ZVP.*

Demostració. En criptografia amb corbes el·líptiques, es necessita calcular múltiples d'un punt (mP), on m és un paràmetre gran. Quan s'implementa en targetes intel·ligents, cal garantir que no apareixeran punts ZVP durant el còmput de mP (la qual cosa es realitza per mitjà de l'algorisme de suma i doblat).

Per motius de seguretat (per garantir que el logaritme discret sigui difícil), el punt P té ordre primer r (de fet, r es pren com el primer més gran que divideix el cardinal de la corba). D'aquí que l'ordre de P mai serà divisor de 8. A més, pel que fa a les condicions indicades en el lema anterior, noti's que el cas $k = 0$ no apareixerà durant el còmput de mP. El mateix passa per a la segona condició, perquè, en la pràctica, m serà més petit que r.

Així, durant el càlcul de mP, el procediment mai es trobarà amb un punt ZVP, ni en la suma ni en el doblat. □

Bibliografia

[AARR03] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side-Channel(s). In *CHES '02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, pages 29–45, London, UK, 2003.

[ASM98] Kiyomichi Araki, Takakazu Satoh, and Shinji Miura. Overview of Elliptic Curve Cryptography. In *PKC '98: Proceedings of the First International Workshop on Practice and Theory in Public Key Cryptography*, pages 29–49. Springer-Verlag, 1998.

[AT03] Toru Akishita and Tsuyoshi Takagi. Zero-value point attacks on elliptic curve cryptosystem. In *ISC 2003: 6th Information Security Conference*, volume 2851 of *LNCS*, pages 218–233. Springer-Verlag, 2003.

[AT04] Toru Akishita and Tsuyoshi Takagi. On the Optimal Parameter Choice for Elliptic Curve Cryptosystems Using Isogeny. In *Public Key Cryptography*, volume 2947 of *LNCS*, pages 346–359. Springer-Verlag, 2004.

[Atk92] Arthur Oliver L. Atkin. The number of points on an elliptic curve modulo a prime (II). Disponible en la pàgina web http://listserv.nodak.edu/archives/nmbrthry.html, 1992.

[BB08] Shi Bai and Richard Peirce Brent. On the efficiency of pollard's rho method for discrete logarithms. In *CATS '08: Proceedings of the Fourteenth Symposium on Computing: the Australasian Theory*,

pages 125–131, Darlinghurst, Australia, 2008. Australian Computer Society, Inc.

[BBLP08] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters. Ecm using edwards curves. Cryptology ePrint Archive, Report 2008/016, 2008.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3–4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BJ02] Eric Brier and Marc Joye. Weierstraß Elliptic Curves and Side-Channel Attacks. In *PKC '02: Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems*, volume 2274 of *LNCS*, pages 335–345. Springer-Verlag, 2002.

[BL07] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *ASIACRYPT '07: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*, pages 29–50, 2007.

[BL09] Daniel J. Bernstein and Tanja Lange. A complete set of addition laws for incomplete edwards curves. Cryptology ePrint Archive, Report 2009/580, 2009.

[BMB+09] Brian Baldwin, Richard Moloney, Andrew Byrne, Gary Mcguire, and William P. Marnane. A hardware analysis of twisted edwards curves for an elliptic curve cryptosystem. In *ARC '09: Proceedings of the 5th International Workshop on Reconfigurable Computing: Architectures, Tools and Applications*, pages 355–361, 2009.

[BMM00] Ingrid Biehl, Bernd Meyer, and Volker Müller. Differential Fault Attacks on Elliptic Curve Cryptosystems. In *CRYPTO '00: Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, volume 1880 of *LNCS*, pages 131–146. Springer-Verlag, 2000.

[BR97] Mihir Bellare and Phillip Rogaway. Minimizing the use of random oracles in authenticated encryption schemes. In *ICICS '97: Proceedings of the First International Conference on Information and Communication Security*, volume 1334 of *LNCS*, pages 1–16. Springer-Verlag, 1997.

[BS10] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 2010. preprint arXiv{0902.4670}.

[BSS99] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography*, volume 265. Cambridge University Press, 1999.

[BSS05] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Advances in Elliptic Curve Cryptography*, volume 317. Cambridge University Press, 2005.

[Cas66] John William S. Cassels. Diophantine Equations with Special Reference To Elliptic Curves. *Journal of London Mathematical Society*, s1-41(1):193–291, 1966.

[CF05] Henri Cohen and Gerhard Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC Press, 2005.

[CJRR03] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Power analysis: attacks and countermeasures,. pages 415–439, 2003.

[CL05] Denis Charles and Kristin Lauter. Computing Modular Polynomials. volume 8 of *Journal of Computational Mathematics*, pages 195–204. London Mathematical Society, 2005.

[CMO98] Henri Cohen, Atsuko Miyaji, and Takatoshi Ono. Efficient elliptic curve exponentiation using mixed coordinates. In *ASIACRYPT '98: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*, volume 1514 of *LNCS*, pages 51–65. Springer-Verlag, 1998.

[Cor99] Jean-Sébastien Coron. Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. In *CHES '99: Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems*, volume 1717 of *LNCS*, pages 292–302. Springer-Verlag, 1999.

[DH76] Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[DS08] M. Prem Das and Palash Sarkar. Pairing Computation on Twisted Edwards Form Elliptic Curves. In *Proceedings of the 2nd International Conference on Pairing-Based Cryptography*, Pairing '08, pages 192–210. Springer-Verlag, 2008.

[Edw07] Harold M. Edwards. A normal form for elliptic curves. In *Bulletin of the American Mathematical Society*, volume 44, pages 393–422, 2007.

[EG85] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *CRYPTO '84: Proceedings of the 4th Annual International Cryptology Conference on Advances in Cryptology*, volume 196 of *LNCS*, pages 10–18. Springer-Verlag, 1985.

[Elk98] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.

[FM02] Mireille Fouquet and François Morain. Isogeny volcanoes and the SEA algorithm. In *ANTS-V – Algorithmic Number Theory*, volume 2369 of *LNCS*, pages 276–291. Springer-Verlag, 2002.

[FMS+08] Mireille Fouquet, Josep M. Miret, Daniel Sadornil, Juan G. Tena, and Magda Valls. Isogenies between elliptic curves over finite fields and binary quadratic forms. In *Proceedings of the "Segundas Jornadas de Teoría de Números"*, Bibl. Rev. Mat. Iberoamericana, pages 153–164. Rev. Mat. Iberoamericana, 2008.

[Fou01] Mireille Fouquet. *Anneau d'endomorphismes et cardinalité de courbes elliptiques: aspects algorithmiques*. Thèse, École Polytechnique, Paris, 2001.

[Gal99] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *Journal of Computational Mathematics*, 2:118–138, 1999.

[Geb04] Catherine H. Gebotys. Design of secure cryptography against the threat of power-attacks in DSP-embedded processors. *ACM Transactions on Embedded Computing Systems*, 3(1):92–113, 2004.

[GG03] Catherine H. Gebotys and Robert J. Gebotys. Secure Elliptic Curve Implementations: An Analysis of Resistance to Power-Attacks in a DSP Processor. In *CHES '02: Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, volume 2523 of *LNCS*, pages 114–128. Springer-Verlag, 2003.

[Gou03] Louis Goubin. A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems. In *PKC '03: Proceedings of the 6th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2567 of *LNCS*, pages 199–210. Springer-Verlag, 2003.

[Ham44] William Rowan Hamilton. On a new Species of Imaginary Quantities connected with a theory of Quaternions. In *Proceedings of the Royal Irish Academy*, number 2, pages 424–434, 1844.

[Has33] Helmut Hasse. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzeta-

funktionen in gewissen elliptischen Fällen. Vorläufie Mitteilung. 42(3):253–262, 1933.

[Has01] M. Anwarul Hasan. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems. *IEEE Transactions on Computers*, 50(10):1071–1083, 2001.

[Hen01] Mike Hendry. *Smart Card Security and Applications*. Artech House Inc., second edition, 2001.

[HM02] Yvonne Hitchcock and Paul Montague. A New Elliptic Curve Scalar Multiplication Algorithm to Resist Simple Power Analysis. In *ACISP 2002: 7th Australasian Conference Information Security and Privacy*, volume 2384 of *LNCS*, pages 214–225. Springer-Verlag, 2002.

[HMV03] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc., 2003.

[Hus04] Dale Husemöller. *Elliptic Curves*. Springer-Verlag New York, Inc., 2004. 2nd Edition.

[IIT04] Kouichi Itoh, Tetsuya Izu, and Masahiko Takenaka. Efficient Countermeasures against Power Analysis for Elliptic Curve Cryptosystems. In *CARDIS VI – Smart Card Research and Advanced Application Conference*, pages 99–114, 2004.

[IJ10] Sorina Ionica and Antoine Joux. Pairing the volcano. In *ANTS IX – Algorithmic Number Theory Symposium*, volume 6197 of *LNCS*, pages 201–218. Springer-Verlag, 2010.

[IMT02] Tetsuya Izu, Bodo Möller, and Tsuyoshi Takagi. Improved Elliptic Curve Multiplication Methods Resistant Against Side Channel Attacks. In *Proceedings of Indocrypt 2002*, volume 2551 of *LNCS*, pages 296–313. Springer-Verlag, 2002.

[IT02] Tetsuya Izu and Tsuyoshi Takagi. A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks. In *PKC '02: Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems*, volume 2274 of *LNCS*, pages 280–296. Springer-Verlag, 2002.

[JMV05] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log? In *ASIACRYPT '05: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*, volume 3788 of *LNCS*, pages 21–40, 2005.

[Joy03] Marc Joye. Elliptic curves and side-channel analysis. volume 4 of *ST Journal of System Research*, pages 283–306, 2003.

[JT01] Marc Joye and Christophe Tymen. Protections against Differential Analysis for Elliptic Curve Cryptography. In *CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, volume 2162 of *LNCS*, pages 377–390. Springer-Verlag, 2001.

[Kel02] John Kelsey. Compression and Information Leakage of Plaintext. volume 2365 of *LNCS*, pages 263–276. Springer-Verlag, 2002.

[KJJ99] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48 (177):203–209, 1987.

[Koc96] Paul C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *CRYPTO '96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, volume 1109 of *LNCS*, pages 104–113. Springer-Verlag, 1996.

[Koh96] David R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Thesis, University of California at Berkeley, 1996.

[Len96] Hendrik W. Lenstra. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 2(56):227–241, 1996.

[Ler97] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. Thèse, École Polytechnique, Paris, 1997.

[LLMP90] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., Mark S. Manasse, and John M. Pollard. The number field sieve. In *STOC '90: Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, pages 564–572, 1990.

[LS01] Pierre-Yvan Liardet and Nigel P. Smart. Preventing SPA/DPA in ECC Systems Using the Jacobi Form. In *CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, pages 391–401. Springer-Verlag, 2001.

[Mer78] Ralph C. Merkle. Secure communications over insecure channels. *Commun. ACM*, 21(4):294–299, 1978.

[Mes01] Thomas S. Messerges. Securing the aes finalists against power analysis attacks. In *FSE '00: Proceedings of the 7th International Workshop on Fast Software Encryption*, volume 1978 of *LNCS*, pages 293–301. Springer-Verlag, 2001.

[Mil86] Victor S. Miller. Use of Elliptic Curves in Cryptography. In *CRYPTO '85: Proceedings of the 5th Annual International Cryptology Conference on Advances in Cryptology*, volume 218 of *LNCS*, pages 417–426. Springer-Verlag New York, Inc., 1986.

[MMM06] Hideyo Mamiya, Atsuko Miyaji, and Hiroaki Morimoto. Secure Elliptic Curve Exponentiation against RPA, ZRA, DPA, and SPA. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E89-A(8):2207–2215, 2006.

[MMRV05] Josep M. Miret, Ramiro Moreno, Anna Rio, and Magda Valls. Determining the 2–Sylow subgroup of an elliptic curve over a finite field. *Mathematics of Computation*, 74(249):411–427, 2005.

[MMRV08] Josep M. Miret, Ramiro Moreno, Anna Rio, and Magda Valls. Computing the ℓ–power torsion of an elliptic curve over a finite field. *Mathematics of Computation*, 78(267):1767–1786, 2008.

[MMRV09] J. Miret, R. Moreno, A. Rio, and M. Valls. Computing the ll-power torsion of an elliptic curve over a finite field. *Mathematics of Computation*, 78(267):1767–1786, 2009.

[MMS+02] Josep M. Miret, Ramiro Moreno, Daniel Sadornil, Juan Tena, and Magda Valls. Isomorphism classes of elliptic curves with even order over a finite field. *Int. Math. Journal*, 2(9):931–942, 2002.

[MMS+06] Josep M. Miret, Ramiro Moreno, Daniel Sadornil, Juan Tena, and Magda Valls. An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 176(2):739–750, 2006.

[MMS+08] Josep M. Miret, Ramiro Moreno, Daniel Sadornil, Juan Tena, and Magda Valls. Computing the height of volcanoes of ℓ–isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 196(1):67–76, 2008.

[MOC97] Atsuko Miyaji, Takatoshi Ono, and Henri Cohen. Efficient elliptic curve exponentiation. In *ICICS '97: Proceedings of the First International Conference on Information and Communication Security*, volume 1334 of *LNCS*, pages 282–291. Springer-Verlag, 1997.

[MOP06] Stephan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks and Countermeasures for Cryptographic Smart Cards*, volume 450. Springer-Verlag, 2006.

[Mor05] Ramiro Moreno. *Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos.* Tesis, Universitat Politècnica de Catalunya, 2005.

[Mor09] François Morain. Edwards curves and CM curves. Technical report, 2009.

[MST+07] Josep M. Miret, Daniel Sadornil, Juan Tena, Rosana Tomàs, and Magda Valls. Volcanoes of ℓ–isogenies of elliptic curves over finite fields: the case $\ell = 3$. *Publicacions Matemàtiques*, (1):165–180, 2007.

[MST+08] Josep M. Miret, Daniel Sadornil, Juan Tena, Rosana Tomàs, and Magda Valls. Exploiting Isogeny Cordillera Structure to Obtain Cryptographically Good Elliptic Curves. In *Journal of Research and Practice in Information Technology*, volume 40, pages 255–265. Australian Computer Society Inc., 2008.

[MST+09] Josep M. Miret, Daniel Sadornil, Juan Tena, Rosana Tomàs, and Magda Valls. On Avoiding ZVP–Attacks Using Isogeny Volcanoes. In *WISA '08: Workshop on Information Security Applications*, volume 5379 of *LNCS*, pages 266–277. Springer-Verlag, 2009.

[MST+10] Santi Martínez, Daniel Sadornil, Juan Tena, Rosana Tomàs, and Magda Valls. Curvas de Edwards y ataques basados en puntos de valor cero (ZVP). In *XI RECSI: Reunión Española sobre Criptología y Seguridad de la Información*, pages 49–53, 2010.

[MTR+06] Santi Martínez, Rosana Tomàs, Concepció Roig, Magda Valls, and Ramiro Moreno. Parallel Calculation of Volcanoes for Cryptographic Uses. In *IPDPS: 20th IEEE International Parallel & Distributed Processing Symposium, PDSEC: Workshop on Parallel and Distributed Scientific and Engineering Computing*, page 307. IEEE Computer Society Press, 2006.

[MVOV96] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Inc., 1996.

[NIS03] Special Publication 800-57: Recommendation for Key Management. Part 1: General Guideline. Technical report, http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf, 2003.

[OS00] Katsuyuki Okeya and Kouichi Sakurai. Power analysis breaks elliptic curve cryptosystems even secure against the timing attack. In *INDOCRYPT 2000: Progress in Cryptology*, volume 1977 of *LNCS*, pages 178–190. Springer-Verlag, 2000.

[Osw05] Maria Elisabeth Oswald. *Side-Channel Analysis book title: Advances in Elliptic Curve Cryptography*, volume 317, pages 69–86. Cambridge University Press, 2005.

[PH78] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24:106–110, 1978.

[Pol78] John M. Pollard. Monte Carlo methods for index computation mod p. *Mathematics of Computation*, 32:918–924, 1978.

[QS01] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and Couter-Measures for Smard Cards. In *E-smart 2001: Smart Card Programming and Security*, volume 2140 of *LNCS*, pages 200–210. Springer-Verlag, 2001.

[QS02] Jean-Jacques Quisquater and David Samyde. Side Channel Cryptanalysis. In *SECI 02: Invited talk in SEcurité de la Communication sur Internet*, 2002.

[Rab79] Michael O. Rabin. Digital signatures and public-key functions as intractable as factorization. Technical report, MIT Laboratory for Computer Science, 1979.

[RC07] Wolfgang Rankl and Kenneth Cox. *Smart Card Applications: Design Models for Using and Programming Smart Cards*. John Wiley & Sons, Inc., 2007.

[RE00] Wolfgang Rankl and Wolfgang Effing. *Smart card handbook*. John Wiley and Sons, Inc., second edition, 2000.

[Rio09] Anna Rio. Criptografía con curvas elípticas. In *RSME 2009: Nuevos avances en criptografía y codificación de la información*, pages 107–119. Edicions UdL, 2009.

[RSA78] Ron L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Rüc87] Hans-Georg Rück. A Note on Elliptic Curves Over Finite Fields. *Mathematics of Computation*, 49(179):301–304, 1987.

[SA03] Sergei P. Skorobogatov and Ross J. Anderson. Optical fault induction attacks. In *CHES '02: Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, volume 2523 of *LNCS*, pages 2–12. Springer-Verlag, 2003.

[Sad04] Daniel Sadornil. *Curvas elípticas de cardinal par sobre cuerpos finitos y volcanes de 2-isogenias. Algoritmos y Aplicaciones*. Tesis, Universidad de Valladolid, 2004.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44:483–494, 1985.

[Sch87] René Schoof. Nonsingular Plane Cubic Curves over Finite Fields. *J. Comb. Theory Ser. A*, 46(2):183–211, 1987.

[Sch00] Werner Schindler. A Timing Attack against RSA with the Chinese Remainder Theorem. In *CHES '00: Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded*

Systems, volume 1965 of *LNCS*, pages 109–124. Springer-Verlag, 2000.

[SEC] Certicom Corp. SECG. SEC 2: Recommended elliptic curve domain parameters.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer-Verlag, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151. Springer-Verlag, 1994.

[Sma90] Nigel P. Smart. An Analysis of Goubin's Refined Power Analysis Attack. In *CHES '03: Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*, volume 2779 of *LNCS*. Springer-Verlag, 281–290.

[SS98] Joseph H. Silverman and Joe Suzuki. Elliptic Curve Discrete Logarithms and the Index Calculus. In *ASIACRYPT '98: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*, volume 1514 of *LNCS*, pages 110–125. Springer-Verlag, 1998.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones Mathematicae*, 2:134–144, 1966.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Série I*, 273:238–241, 1971.

[Wat69] William C. Waterhouse. Abelian varieties over Finite Fields. *Annales scientifiques de l'École Normale Supérieure*, 4(2):521–560, 1969.

[Wei49] André Weil. Number of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55:397–508, 1949.

[Wil80] Hugh C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, 26:726–729, 1980.

[Wit01] Christian Wittmann. Group Structure of Elliptic Curves over Finite Fields. *Journal of Number Theory*, 88(2):335–344, 2001.

[WS05] Colin Walter and David Samyde. Data Dependent Power Use in Multipliers. Computer Arithmetic, IEEE Symposium on, pages 4–12. IEEE Computer Society, 2005.