UNIVERSITAT DE BARCELONA

Treball final de grau

GRAU DE MATEMÀTIQUES

GRAU D'ENGINYERIA INFORMÀTICA

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

CRIPTOGRAFIA BASADA EN ISOGÈNIES

Autor: Enric Florit Zacarías

Directors:	Dr. Xavier Guitart
	Dr. Santiago Seguí
	Dr. Ramsès Fernàndez
Realitzat a:	Departament de Matemàtiques i Informàtica i Fundació Eurecat

Barcelona, 19 de gener de 2020

Abstract

One of the central concepts in cryptography is encryption, which can be classified as symmetric or asymmetric depending on whether the used keys are shared by the implicated parts or not. The most used ciphers are symmetric, but they require the parts to agree on the key to be used. To satisfy this need, Diffie and Hellman proposed their key exchange protocol, based on the difficulty of solving the discrete logarithm problem in a cyclic group. With the foreseeable creation of sufficiently powerful quantum computers, this and other problems could become solvable in polynomial time. This creates the need of introducing new key exchange methods that are resistant to quantum cryptanalysis.

In this project we study the SIDH/SIKE protocol, a candidate for the postquantum cryptography standardization process by NIST, which is based on the problem of finding isogenies between two elliptic curves. An elliptic curve is a plane curve defined by a cubic equation. These curves have the property of being both algebraic curves and abelian groups. Nonconstant morphisms between elliptic curves that maintain both structures are called isogenies, and they can be computed in linear time in the size of their kernel. In our case, all curves and morphisms are defined over a finite field $\mathbb{F}_{p^2}$, as we are working with supersingular elliptic curves. We obtain a key exchange system in which a private key is a subgroup of an elliptic curve, and its associated public key is the image curve of the isogeny that has such subgroup as kernel. In addition, the image of two auxiliary points by the secret isogeny is revealed to make an exchange.

To break an SIDH key one needs to find the isogeny connecting the protocol's initial curve with the public key. The best classical attack to do this requires $O(\sqrt[4]{p})$ memory space and $O(\sqrt[4]{p})$ isogeny evaluations, and the best known quantum attack requires $O(\sqrt[6]{p})$ isogeny evaluations. Therefore, the SIDH protocol is considered secure. However, in a key reuse situation, Galbraith et al. have given an attack through which one learns a private key in only $\frac{1}{2}\log_2 p$ steps, by maliciously modifying the auxiliary points. The SIKE protocol is introduced to avoid this kind of attacks.

2010 Mathematics Subject Classification. 94A60, 94A62, 14H52, 14K02

Resum

Un dels conceptes centrals en criptografia és el del xifrat, que es pot classificar en simètric o asimètric segons si les claus emprades són compartides per les parts implicades o no. Els algoritmes de xifrat més utilitzats són simètrics, però requereixen que les parts es posin d'acord en la clau a utilitzar. Per suplir aquesta necessitat, Diffie i Hellman van proposar el seu intercanvi de claus, basant-se en la dificultat de resoldre el problema del logaritme discret en un grup cíclic. Amb la futura creació d'ordinadors quàntics prou potents, aquest i altres problemes es podrien resoldre en temps polinòmic, fent necessària la introducció de nous mètodes d'intercanvi de claus resistents a criptoanàlisi quàntica.

En aquest treball estudiem el protocol SIDH/SIKE, un dels candidats al procés d'estandardització de criptografia postquàntica de l'institut NIST, basat en el problema de trobar isogènies entre dues corbes el·líptiques. Una corba el·líptica és una corba plana definida per una equació cúbica. Aquestes corbes tenen la propietat de ser alhora corbes algebraiques i grups abelians. Els morfismes no constants entre corbes el·líptiques que mantenen les dues estructures s'anomenen isogènies, i es poden calcular en un temps lineal en la mida del seu nucli. En el nostre cas, les corbes i els morfismes es defineixen sobre un cos finit $\mathbb{F}_{p^2}$, ja que treballem amb corbes el·líptiques supersingulars. Ens apareix un sistema d'intercanvi de claus en el qual una clau privada és un subgrup finit d'una corba el·líptica, i la clau pública associada és la corba imatge de la isogènia que té per nucli tal subgrup. Per fer l'intercanvi, a més, es revela la imatge de dos punts auxiliars per la isogènia privada.

Per trencar una clau SIDH cal trobar la isogènia que connecta la corba incial del protocol amb la clau pública. El millor atac clàssic per fer-ho requereix $O(\sqrt[4]{p})$ espai de memòria i $O(\sqrt[4]{p})$ avaluacions d'isogènies, i el millor atac quàntic conegut requereix $O(\sqrt[6]{p})$ avaluacions d'isogènies. Per tant, el protocol SIDH es considera segur. No obstant això, en un context de reutilització de claus, apareix un atac donat per Galbraith et al. que permet esbrinar una clau privada en només $\frac{1}{2}\log_2 p$ passos mitjançant la modificació maliciosa dels punts auxiliars. El protocol SIKE s'introdueix per evitar aquest tipus d'atacs.

Resumen

Uno de los conceptos centrales en criptografía es el del cifrado, que puede clasificarse en simétrico o asimétrico según si las claves utilizadas son compartidas por las partes implicadas o no. Los algoritmos de cifrado más usados son simétricos, pero requieren que las partes se pongan de acuerdo en la clave a utilizar. Para suplir esta necesidad, Diffie y Hellman propusieron su intercambio de claves, basándose en la dificultad de resolver el problema del logaritmo discreto en un grupo cíclico. Con la futura creación de ordenadores cuánticos suficientemente potentes, este y otros problemas se podrían resolver en tiempo polinómico, haciendo necesaria la introducción de nuevos métodos de intercambio de claves resistentes a criptoanálisis cuántico.

En este trabajo estudiamos el protocolo SIDH/SIKE, uno de los candidatos al proceso de estandarización de criptografía postcuántica del instituto NIST, basado en el problema de encontrar isogenias entre dos curvas elípticas. Una curva elíptica es una curva plana definida por una ecuación cúbica. Estas curvas tienen la propiedad de ser a la vez curvas algebraicas y grupos abelianos. Los morfismos no constantes entre curvas elípticas que mantienen ambas estructuras se denominan isogenias, y se pueden calcular en un tiempo lineal en el tamaño de su núcleo. En nuestro caso, las curvas y los morfismos se definen sobre un cuerpo finito $\mathbb{F}_{p^2}$, ya que trabajamos con curvas elípticas supersingulares. Nos aparece un sistema de intercambio de claves en el cual una clave privada es un subgrupo finito de una curva elíptica, y su clave pública asociada es la curva imagen de la isogenia que tiene por núcleo tal subgrupo. Para hacer el intercambio, además, se revela la imagen de dos puntos auxiliares por la isogenia privada.

Para romper una clave SIDH hay que encontrar la isogenia que conecta la curva inicial del protocolo con la clave pública. El mejor ataque clásico para hacerlo requiere $O(\sqrt[4]{p})$ espacio de memoria y $O(\sqrt[4]{p})$ evaluaciones de isogenias, y el mejor ataque cuántico conocido requiere $O(\sqrt[6]{p})$ evaluaciones de isogenias. Por lo tanto, el protocolo SIDH se considera seguro. No obstante, en un contexto de reutilización de claves, aparece un ataque dado por Galbraith et al. que permite descubrir una clave privada en solo $\frac{1}{2}\log_2 p$ pasos mediante la modificación maliciosa de los puntos auxiliares. El protocolo SIKE se introduce para evitar este tipo de ataques.

Agraïments

Vull donar les gràcies al Dr. Xevi Guitart per la proposta del tema d'aquest treball, les indicacions per desenvolupar-ne la part matemàtica i l'ajut durant tot aquest semestre.

També dono les gràcies al Dr. Santi Seguí, per haver escoltat les meves explicacions i validat el treball, i pels suggeriments sobre les visualitzacions dels grafs d'isogènies.

Al Dr. Ramsès Fernàndez li agraeixo l'ajut, els suggeriments i, sobretot, l'acollida a l'equip d'IT Security d'Eurecat. Ha estat un entorn magnífic que m'ha permès desenvolupar aquest treball tant com he volgut.

Gràcies als meus pares, encara que creguin que el mèrit és només meu.

I finalment, et dono les gràcies Ana per donar-me tot el suport que he necessitat, i més.

Índex

Introducció

La criptografia és l'estudi de les tècniques emprades per protegir la informació i garantir la seguretat de les comunicacions. Un dels seus conceptes centrals és el del xifrat: l'acte de transformar la informació per tal que només pugui ser llegida pels seus destinataris. En tots els mètodes de xifrat clàssics, tant l'algoritme de xifrat com el de desxifrat fan ús d'una mateixa clau, rebent l'adjectiu de *simètrics*. Encara avui, els mecanismes més utilitzats (com per exemple AES) són simètrics. Com que les comunicacions es realitzen sovint entre parts que no han tingut necessàriament un contacte previ, sorgeix la necessitat d'estudiar mètodes segurs d'intercanvi de claus.

El concepte de l'intercanvi de claus és un dels primers exemples de criptografia *asimètrica*. Va ser introduït el 1976 per Diffie i Hellman [DH76], basant-se en la dificultat de resoldre el problema del logaritme discret en un grup cíclic. Els millors algoritmes de càlcul de logaritmes discrets són subexponencials, i per tant l'esquema Diffie-Hellman es considera suficientment segur. No obstant això, ara ens trobem enmig d'una cursa per desenvolupar ordinadors quàntics suficientment potents com per resoldre aquest i d'altres problemes en temps polinòmic. L'amenaça d'un adversari capaç de trencar els esquemes actuals és real, per més que la seva aparició sigui encara distant. Seguint la reflexió de Michele Mosca a [Mos15], suposem que la informació xifrada ha de mantenir-se secreta durant x anys, el temps de migració cap a nous protocols és de y anys, i encara queden z anys fins a la posada en marxa d'un sistema capaç de desxifrar la informació. Aleshores, tenim un problema si $z < x + y$, ja que la informació xifrada al final dels pròxims y anys podrà ser desxifrada abans dels x anys previstos.

Així, en les darreres dècades s'ha iniciat el desenvolupament de l'anomenada *criptografia postquàntica*. Aquesta ha de complir els següents requisits: per una banda, els algoritmes de xifrat i desxifrat han de ser eficients amb el maquinari de què disposem actualment; per l'altra, ha de ser resistent a criptoanàlisi, tant clàssica com quàntica.

L'institut NIST va posar en marxa el 2016 un procés en forma de competició per estandarditzar nous protocols amb els requisits esmentats. En els pròxims dos anys s'escolliran els guanyadors a partir de 17 propostes seleccionades (de 82 propostes inicials), podent haver-hi diversos guanyadors –ja que diferents protocols poden ser adequats en diferents situacions. Una de les propostes seleccionades és el protocol SIDH/SIKE, que s'emmarca en l'àmbit de la criptografia basada en isogènies.

Una isogènia és un morfisme entre dues corbes el·líptiques, que té la propietat de ser fàcilment calculable sempre que el seu nucli sigui conegut. La consideració d'aquests morfismes com a eina criptogràfica té tan sols vint anys d'història. L'any 1997, Couveignes [Cou06] proposà un mecanisme d'intercanvi de claus basat en l'acció d'un grup de classes sobre un conjunt de corbes el·líptiques. El seu manuscrit va ser rebutjat, i la idea va ser redescoberta el 2006 per Rostovtsev i Stolbunov [RS06]. El mateix any va ser presentat el primer algoritme de hash basat en isogènies, aquesta vegada emprant corbes el·líptiques *supersingulars*, de la mà de Charles, Goren i Lauter [CGL06]. Emprant principis similars, David Jao i Luca De Feo [FJP11] van publicar el 2011 el seu protocol d'intercanvi de claus basat en isogènies entre corbes supersingulars, anomenat Supersingular Isogeny Diffie-Hellman (SIDH). Aquest és el protocol que es va presentar a la competició del NIST, sota el nom de Supersingular Isogeny Key Encapsulation (SIKE).

L'objectiu principal d'aquest treball és desenvolupar els principis de la criptografia basada en isogènies i fer-ho a través del protocol SIDH/SIKE, el més rellevant actualment i el

més proper a un futur desplegament. Per fer-ho, ens hem de plantejar un altre objectiu: introduir la teoria bàsica de corbes el·líptiques i isogènies, i classificar les corbes el·líptiques sobre cossos finits en ordinàries i supersingulars. Finalment, volem analitzar la seguretat del protocol, mitjançant l'estudi d'alguns atacs proposats en la literatura.

Com a punt de partida d'aquest treball prendrem els continguts de les assignatures d'Aritmètica, Estructures Algebraiques, Equacions Algebraiques, Introducció a l'Àlgebra Commutativa, Geometria Projectiva i Varietats Algebraiques del Grau de Matemàtiques; i les assignatures d'Algorísmica, Algorísmica Avançada i Estructura de Dades del Grau d'Enginyeria Informàtica.

Estructura de la memòria

A la Secció 1 donem la motivació per l'estudi de la criptografia postquàntica, tot explicant l'esquema clàssic de Diffie-Hellman, el problema del logaritme discret, i els millors algoritmes per resoldre'l.

La Secció 2 està dedicada a definir els conceptes bàsics que necessitem relatius a corbes el·líptiques: llei de grup, isogènies, corbes quocient, invariant j, grups de torsió i isogènies duals. Els mètodes emprats es podrien anomenar elementals: amb tècniques de geometria algebraica se simplificarien alguns arguments, però hem optat per una exposició més pràctica sense massa requeriments teòrics.

A la Secció 3 treballem les corbes el·líptiques definides sobre un cos finit. En aquest context, apareixen dues classes de corbes: les ordinàries i les supersingulars. Per una banda, donem criteris per diferenciar entre les dues classes, incloent-hi l'estudi dels anells d'endomorfismes. Per l'altra, i donat que utilitzarem corbes supersingulars per definir el protocol SIDH, calcularem quantes corbes trobem en aquesta classe.

Finalment, la Secció 4 està destinada a introduir l'esquema SIDH. Comencem explicant el seu plantejament i realització. Tot seguit, n'estudiem la tria de paràmetres i les optimitzacions necessàries per fer eficient el càlcul d'isogènies. A continuació veiem dos atacs contra l'esquema, discutim la seva resistència a criptoanàlisi quàntica, i en relacionem la seguretat amb el càlcul d'anells d'endomorfismes de corbes el·líptiques. Per acabar, expliquem SIKE, la modificació necessària per evitar un dels atacs introduïts.

La planificació inicial per realitzar aquest treball es pot trobar a l'Annex A. A l'Annex B es reprodueixen els paràmetres proposats a l'especificació del protocol SIKE, a més d'algunes proves de rendiment. L'Annex C recull les proves fetes per comparar l'eficiència de dues estratègies per al primer atac considerat. Finalment, l'Annex D conté diverses visualitzacions realitzades amb D3.js dels grafs d'isogènies, l'intercanvi SIDH i els atacs estudiats.

1 Diffie-Hellman i logaritmes discrets

Situem-nos en un escenari en el qual dues o més parts volen mantenir comunicacions de forma xifrada en un canal considerat no segur, és a dir, en el qual terceres parts no autoritzades poden veure la informació transmesa pel canal. Per fer-ho, disposen dels següents elements: un conjunt de missatges possibles $\mathcal{M}$, un conjunt de claus $\mathcal{K}$, i per a cada $k \in \mathcal{K}$, dues funcions

$$E_k \colon \mathcal{M} \to \mathcal{M}$$
$$D_k \colon \mathcal{M} \to \mathcal{M}$$

fàcilment computables i tals que $D_k(E_k(m)) = m$, per a qualsevol missatge $m \in \mathcal{M}$. Acabem de definir el paradigma del xifrat simètric. L'estudi i el disseny d'esquemes segurs que segueixen aquest paradigma és una àrea rica i en constant desenvolupament, però com hem esbossat a la introducció, a nosaltres ens interessa un problema anterior: com poden les múltiples parts involucrades en un protocol simètric posar-se d'acord en una mateixa clau?

Definim alguns conceptes per tractar el problema. En primer lloc, un *establiment de claus* és un protocol mitjançant el qual un *secret compartit* esdevé disponible a dues o més parts per a ús criptogràfic posterior. Un protocol de *transport de claus* és un mecanisme d'establiment de claus en què una part crea un valor secret i el transfereix de forma segura a les altres. Finalment, un protocol d'*intercanvi de claus* és un mecanisme d'establiment de claus en què el secret compartit és el producte d'informació contribuïda per cadascuna de les parts.

L'any 1976, Whitfield Diffie i Martin Hellman [DH76] van proposar un protocol senzill d'intercanvi de claus que esdevindria la base del que coneixem de forma corrent com a criptografia de clau pública o asimètrica. Els paràmetres públics del protocol són un nombre primer p, i un generador α del grup $(\mathbb{Z}/p\mathbb{Z})^\times$.[1] Les dues parts de la comunicació (en endavant, Alice i Bob) trien sengles claus privades a i b del conjunt $\{1, \ldots, p-1\}$ de forma aleatòria. Les claus públiques de cadascun són, respectivament, $A \equiv \alpha^a$ i $B \equiv \alpha^b \mod p$. Aquestes claus es transmeten pel canal de comunicació. Al rebre B, Alice calcula $B^a \equiv (\alpha^b)^a \mod p$. Bob fa l'operació simètrica, de forma que els dos obtenen el mateix secret compartit,

$$A^b \equiv B^a \equiv \alpha^{ab} \mod p.$$

L'esquema és pràctic, ja que calcular potències mòdul p es pot fer de forma eficient mitjançant l'algoritme d'exponenciació binària: el càlcul de $\alpha^x \mod p$ té complexitat $O(\log_2 x)$. La seguretat de l'esquema es reflecteix en els problemes computacionals del logaritme discret i de Diffie-Hellman.

Problema 1.1 (Discrete Logarithm Problem (DLP))**.** *Donats un grup cíclic G, un generador α de G, i un element β de G, trobar un enter x tal que $\alpha^x = \beta$.*

Problema 1.2 (Diffie-Hellman Problem (DHP))**.** *Donats un grup cíclic G, un generador α de G, i elements α^a i α^b de G, trobar α^{ab}. Un algoritme capaç de resoldre el problema DLP pot ser usat per resoldre trivialment el problema DHP.*

[1] **Notació:** Si p és un nombre primer, $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ és el conjunt dels enters mòdul p, que és un cos amb les operacions de suma i producte. En denotem el seu grup d'elements invertibles per $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots, p-1\}$. Sovint també escriurem $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ i, si $q = p^r$, $\mathbb{F}_q$ denotarà el cos finit amb q elements.

La relació d'aquests problemes amb el protocol Diffie-Hellman i amb d'altres en camps com l'àlgebra computacional fa que s'hagin donat múltiples algoritmes per resoldre'ls. Per poder comparar-los, recordem primer algunes nocions sobre complexitat.

Definició 1.3 (Notació O gran)**.** *Siguin f i g funcions $\mathbb{N} \to \mathbb{R}$, positives a partir d'un cert nombre natural. Diem que $f(n) = O(g(n))$ si existeixen una constant $c > 0$ i un natural n_0 tals que $0 \leq f(n) < cg(n)$, per a tot $n \geq n_0$.*

Definició 1.4 (Notació o petita)**.** *Siguin f i g funcions $\mathbb{N} \to \mathbb{R}$, positives a partir d'un cert nombre natural. Diem que $f(n) = o(g(n))$ si per a tota constant $c > 0$ existeix un natural n_0 tal que $0 \leq f(n) < cg(n)$, per a tot $n \geq n_0$.*

Intuïtivament, la funció $f(n)$ es fa insignificant en relació a $g(n)$ a mesura que n es fa gran. L'expressió $o(1)$ s'empra sovint per expressar una funció $f(n)$ amb límit igual a 0 quan n tendeix a infinit.

Quan treballem amb algoritmes l'entrada dels quals són nombres enters n, la mida de l'entrada es mesura en els bits necessaris per representar-los, és a dir $1 + \lfloor \log n \rfloor$. Per analitzar de forma compacta aquesta classe d'algoritmes, introduïm la següent notació.

Definició 1.5 (Notació L)**.** *Per a $t, \gamma \in \mathbb{R}$ amb $0 \leq t \leq 1$, la notació $L_n[t, \gamma]$ s'utilitza per a qualsevol funció de n que sigui igual a*

$$e^{(\gamma + o(1))(\log n)^t (\log \log n)^{1-t}}, \text{ quan } n \to \infty.$$

Quan s'utilitza aquesta notació per indicar temps d'execució amb γ fixada, $L_n[t, \gamma]$ abasta des del temps polinòmic fins al temps exponencial:

- *Un temps de $L_n[0, \gamma] = e^{(\gamma + o(1)) \log \log n} = (\log n)^{\gamma + o(1)}$ és polinòmic en $\log n$;*
- *Per a $0 < t < 1$, els temps d'execució $L_n[t, \gamma]$ són exemples de temps subexponencials en $\log n$, és a dir, asimptòticament més grans que temps polinòmic i menys que temps exponencial;*
- *Un temps de $L_n[1, \gamma] = e^{(\gamma + o(1)) \log n} = n^{\gamma + o(1)}$ és exponencial en $\log n$.*

Donem a continuació una relació d'algoritmes per resoldre el problema del logaritme discret.

Algoritme	Complexitat
Cerca exhaustiva	$O(N)$
Baby step–giant step	Temps $O(\sqrt{N})$, memòria $O(\sqrt{N})$
ρ de Pollard	$O(\sqrt{N})$
λ de Pollard	$O(\sqrt{N})$
Pohlig-Hellman	$O(\sum_{i=1}^{r} e_i(\log N + \sqrt{p_i}))$
Index calculus a $\mathbb{F}_{p^n}$	$L_{p^n}[1/2, \sqrt{2}]$
NFS-DLP a $\mathbb{F}_{p^n}$	$L_{p^n}[1/3, c]$

Taula 1: Algoritmes que resolen el problema DLP en un grup d'ordre $N = \prod_{i=1}^{r} p_i^{e_i}$.

Com en el cas de la representació de nombres naturals, al tractar el problema del logaritme discret estem considerant que la mida de l'entrada és $\log N$, i per tant els quatre primers

algoritmes de la taula són exponencials. Els podem classificar com a genèrics, ja que l'única propietat del grup que consideren és l'operació, sense tenir-ne en compte cap altra (com ara l'estructura o l'ordre). S'ha provat [Sho97] que la complexitat de $O(\sqrt{N})$ operacions de grup és òptima per a algoritmes DLP genèrics.

El mètode de Pohlig-Hellman es basa en trobar el logaritme discret mòdul els factors $p_i^{e_i}$ de N, per després combinar la informació obtinguda mitjançant el teorema xinès del residu. Funciona millor quan N és un nombre llis[2]. Tanmateix, si només alguns dels factors són petits, es pot obtenir informació parcial sobre el logaritme mòdul el producte dels primers petits que divideixen N, i emprar posteriorment algun altre algoritme. Si N és primer, l'algoritme és similar al baby step-giant step.

A l'algoritme del garbell de cossos de nombres (NFS-DLP), la constant c pertany al conjunt $\{\sqrt[3]{32/9}, \sqrt[3]{128/9}, \sqrt[3]{64/9}\}$, i depèn de la relació entre $\log p$ i $\log p^n$ (veure [JL11]).

Suposant que només utilitzem el protocol Diffie-Hellman amb grups d'ordre no divisible per primers petits, els millors algoritmes de què disposem per resoldre el problema DLP són exponencials en $\log N$. En cas que estiguem tractant amb el grup multiplicatiu d'un cos finit, però, el millor algoritme esdevé subexponencial amb $t = 1/3$. A més, existeixen mètodes per reduir certs problemes de logaritme discret en certs grups a logaritmes discrets en cossos finits, com és el cas del *MOV Attack* [MVO91]. Aquest atac està enfocat a resoldre logaritmes discrets en corbes el·líptiques, però només és pràctic en el cas de corbes supersingulars (veure [Was08, §5.3]), que s'eviten en ECDH (Elliptic Curve Diffie-Hellman) per aquest motiu.

1.1 Criptografia postquàntica

El 2007, el NIST va publicar la "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography", que ha estat revisada dues vegades fins arribar a la versió de 2018 [Bar+18]. En aquest document s'especifiquen estàndards per a l'intercanvi de claus. Entre d'altres, s'hi recomanen protocols basats en Diffie-Hellman sobre cossos finits i corbes el·líptiques. Donat l'estat actual de la qüestió sobre la resolució del problema DLP, es podria considerar que aquesta especificació proporciona un bon nivell de seguretat a l'hora d'intercanviar claus.

No obstant això, ens falta una part de l'escena, que no tractarem en profunditat però que ens ha de preocupar. El 1994, Peter Shor [Sho94] publicà un mètode per calcular logaritmes discrets en temps polinòmic mitjançant l'ús d'un ordinador quàntic (en aquell moment, teòric). S'han proposat també d'altres algoritmes quàntics per resoldre diversos problemes computacionals rellevants des d'un punt de vista criptogràfic, augmentant la preocupació per la seguretat de qualsevol sistema en cas que un ordinador així es materialitzés.

Com a resposta a l'aparent imminència de la creació d'un ordinador quàntic, el 2016 l'institut d'estàndards NIST va iniciar el seu programa *Post-Quantum Cryptography*. Aquesta competició té com a objectiu determinar els nous estàndards criptogràfics resistents no només a criptoanàlisi clàssica, sinó també a atacs mitjançant algoritmes quàntics. Els protocols proposats han de ser implementables de forma eficient en una gran varietat de dispositius quotidians, i han de permetre realitzar, com a mínim, una de les següents funcions: signatura, xifrat, establiment de claus. Amb l'inici del programa es va publicar un informe [Moo+16] sobre els desenvolupaments de hardware quàntic i les seves implicacions,

[2]Un nombre enter N és llis si tots els seus factors primers són petits (usualment, respecte d'alguna constant).

així com un breu llistat de les línies de recerca que potencialment tindrien una aplicació en forma de criptografia postquàntica. Ja en aquest informe es menciona la criptografia basada en isogènies entre corbes el·líptiques supersingulars.

2 Corbes el·líptiques

Per simplificar l'exposició, K sempre denotarà un cos de característica diferent de 2 i 3.

2.1 Equacions de Weierstrass

Una corba el·líptica E definida sobre K és la corba algebraica definida per l'equació

$$E : y^2 = x^3 + Ax + B, \tag{1}$$

on A, B són elements del cos K. Definim el discriminant de la corba $\Delta := 4A^3 + 27B^2$. L'equació (1) s'anomena una equació de Weierstrass. Donat un cos $L \supseteq K$, denotarem

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

el conjunt de punts amb coordenades en L que satisfan l'equació de E, més un punt a l'infinit que notarem $\mathcal{O}$.

Lema 2.1. *La corba E és regular si, i només si, $\Delta \neq 0$.*[3]

Demostració. Sigui $F(x, y) := y^2 - f(x)$, amb $f(x) = x^3 + Ax + B$. Tenim $\partial F/\partial x = -f'(x)$ i $\partial F/\partial y = 2y$. Si el punt $(x, y) \in E$ és singular, com que la característica és diferent de 2 tindrem $y = 0$. Per tant es compleix $f(x) = f'(x) = 0$, que és equivalent a $\Delta = \Delta_f = 0$. □

També considerarem la clausura projectiva de E, donada pel polinomi homogeni

$$y^2 z = x^3 + Axz^2 + Bz^3. \tag{2}$$

Intersecant E amb la recta de l'infinit $z = 0$, obtenim que l'únic punt d'intersecció (i per tant, punt triple) és $\mathcal{O} = (0 : 1 : 0)$. És un punt no singular: substituint $y = 1$ tenim l'equació $z = x^3 + Ax$. Posant $G(x, z) = z - x^3 - Ax$, observem que $\partial G/\partial z = 1 \neq 0$.

2.2 La llei de grup

Donarem una operació de suma de punts que dotarà $E(K)$ d'estructura de grup abelià. Ho fem seguint una construcció geomètrica, que ens permet també tenir coordenades explícites de la suma de dos punts com a funció racional de les coordenades. La Figura 2.1 exemplifica aquesta operació en una corba el·líptica sobre el cos dels nombres reals.

Siguin $P, Q \in E$. Traçant la recta L entre els dos punts, sigui R el tercer punt d'intersecció de L amb E (si $P = Q$, L serà la tangent a E en P; si P és un punt triple de E, llavors $R = P$). Sigui M la recta que passa per R i $\mathcal{O}$. Al tercer punt d'intersecció de M i E l'anomenarem $P + Q$.

Si $P = Q = \mathcal{O}$, llavors $L \cap E = \{\mathcal{O}\}$, i $M \cap E = \{\mathcal{O}\}$. Per tant $\mathcal{O} + \mathcal{O} = \mathcal{O}$. Si $P = \mathcal{O}$ i $Q \neq \mathcal{O}$, llavors $M \cap E = \{\mathcal{O}, R, Q\}$ $(L = M)$, per tant $\mathcal{O} + Q = Q$.

[3] Observació: el discriminant Δ de la corba és idèntic al del polinomi $x^3 + Ax + B$, per tant l'afirmació equival a dir que el polinomi no té arrels dobles.

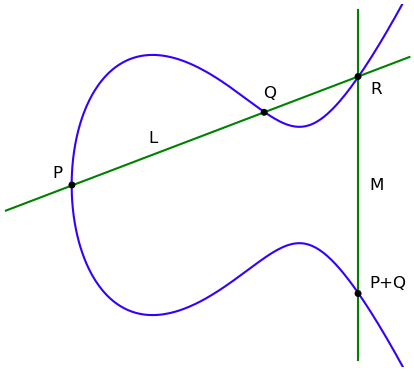


Figura 2.1: Suma de dos punts de la corba $y^2 = x^3 - 3x + 3$ sobre $\mathbb{R}$.

Calculem l'expressió en coordenades de $P + Q$. Posem $P = (x_1, y_1)$, $Q = (x_2, y_2)$, i comencem suposant que $x_1 \neq x_2$. La recta L té pendent $m = \frac{y_2 - y_1}{x_2 - x_1}$, i té equació

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

Substituint a l'equació de E tenim $(m(x-x_1)+y_1)^2 = x^3+Ax+B$, que podem transformar en l'equació

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

Com que x_1 i x_2 són solucions d'aquesta equació, amb la tercera arrel x_3 se satisfà

$$-(x_1 + x_2 + x_3) = -m^2 \implies x_3 = m^2 - x_1 - x_2.$$

El tercer punt d'intersecció és doncs $(x_3, m(x_3 - x_1) + y_1)$. Per a trobar $P + Q = (x_3, y_3)$, hem de traçar M, que té direcció $(0, 1)$, ja que passa pel punt a l'infinit $(0 : 1 : 0)$. Només cal reflectir respecte l'eix d'abscisses, obtenint $y_3 = m(x_1 - x_3) - y_1$.

Si $x_1 = x_2$ però $y_1 \neq y_2$, llavors la recta L és vertical i el tercer punt d'intersecció és $\mathcal{O}$, de manera que $M \cap E = \{\mathcal{O}\}$ i $P + Q = \mathcal{O}$.

Finalment, si $P = Q$ els càlculs són idèntics, però ens fa falta el pendent de la recta tangent. Derivant implícitament

$$2y\frac{dy}{dx} = 3x^2 + A \implies m = \frac{dy}{dx} = \frac{3x^2 + A}{2y}.$$

Per tant $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, sempre que $y \neq 0$. Si $y = 0$, llavors la recta tangent és vertical, i per tant interseca $\mathcal{O}$. Per tant $P + Q = P + P = \mathcal{O}$.

Destaquem que l'operació de suma de punts és tancada en qualsevol cos que contingui K.

Teorema 2.2. *L'operació definida compleix les següents propietats, per a punts $P, Q, R \in E$:*

1. $P + Q = Q + P$ *(commutativa),*
2. *Existeix un punt $\mathcal{O} \in E$ tal que $P + \mathcal{O} = P$ (element neutre),*
3. *Existeix $P' \in E$ tal que $P + P' = \mathcal{O}$, i el denotem $P' = -P$ (existència d'inversos),*
4. $(P + Q) + R = P + (Q + R)$ *(associativa).*

En resum, l'operació + dota E d'estructura de grup abelià amb neutre $\mathcal{O}$.

Demostració.

1. Obvi per construcció.
2. Vist en la discussió anterior.
3. Donat $P = (x, y)$, prenem $P' = -P = (x, -y)$.
4. Es pot veure usant el teorema de Cayley-Bacharach. A [Was08, §2.4] es dona una demostració d'aquest teorema per a un cas particular que implica la propietat associativa.

□

2.3 Isogènies

A continuació volem estudiar els morfismes entre corbes el·líptiques. Com que estem treballant amb objectes que són alhora corbes algebraiques i grups abelians, les aplicacions que considerem hauran de respectar les dues estructures.

Recordem que, donades dues corbes algebraiques C_1 i C_2, un morfisme de corbes $\phi\colon C_1 \to C_2$ és una funció donada per funcions racionals, tal que tot punt P en $C_1(\bar{K})$ té imatge per ϕ.

Definició 2.3. *Siguin E_1, E_2 corbes el·líptiques definides sobre K. Una isogènia $\alpha\colon E_1 \to E_2$ és un morfisme no nul de corbes que indueix un morfisme de grups $E_1(\bar{K}) \to E_2(\bar{K})$. Es diu que E_1 i E_2 són isògenes.*

Diem que E_1 i E_2 són isomorfes si existeixen isogènies $\phi\colon E_1 \to E_2$, $\psi\colon E_2 \to E_1$ tals que $\psi \circ \phi = id_{E_1}$ i $\phi \circ \psi = id_{E_2}$.

Exemple 2.4. *Donat un grup abelià E i un enter n, l'aplicació que envia cada P de E a $n \cdot P$ és un endomorfisme de grups, que sovint denotarem per $[n]$. Si E és una corba el·líptica, l'operació de suma de punts ve donada per funcions racionals, i per tant $[n]$ és una isogènia.*

Proposició 2.5. *Sigui $\alpha\colon E_1 \to E_2$ una isogènia, $E_i : y^2 = x^3 + A_i x + B_i$. Existeixen polinomis $p, q, s, t \in K[x]$ tals que*

$$\alpha(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right)$$

i $(p, q) = 1$, $(s, t) = 1$. Direm que α està en forma estàndard.

Demostració. Suposem que α està definida per la funció racional $(\alpha_x : \alpha_y : \alpha_z)$. Per a un punt afí $(x : y : 1) \in E_1(\bar{K})$, podem escriure

$$\begin{aligned} R_1(x, y) &:= \alpha_x(x, y, 1)/\alpha_z(x, y, 1), \\ R_2(x, y) &:= \alpha_y(x, y, 1)/\alpha_z(x, y, 1), \\ \alpha(x, y) &= (R_1(x, y), R_2(x, y)). \end{aligned}$$

Com que E_1 té per equació $y^2 = x^3 + A_1x + B_1$, donada una funció racional $R(x, y)$ qualsevol, podem substituir potències parelles de y per la potència adequada de $x^3 + A_1x + B_1$. Així, podem suposar que

$$R(x, y) = \frac{q_1(x) + yq_2(x)}{q_3(x) + yq_4(x)}.$$

A més, podem multiplicar numerador i denominador per $q_3(x) - yq_4(x)$ i tornar a substituir y^2, obtenint

$$R(x, y) = \frac{r_1(x) + yr_2(x)}{r_3(x)}.$$

Ara, com que α és morfisme de grups, tenim $\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y)$. Per tant, es compleix

$$R_1(x, -y) = R_1(x, y), \qquad R_2(x, -y) = -R_2(x, y).$$

De la primera equació obtenim $R_1(x, y) = \frac{p(x)}{q(x)}$, i de la segona, $R_2(x, y) = y\frac{s(x)}{t(x)}$. □

Per a un punt $P = (x_0, y_0) \in E_1$ diferent de $\mathcal{O}$, pot passar que $q(x_0) = 0$, i en aquest cas $\alpha(x_0, y_0) = \mathcal{O}$. Si q no s'anul·la, el següent lema ens assegura que la imatge de P està definida.

Lema 2.6. *Siguin $E_i : y^2 = f_i(x)$, $i = 1, 2$ corbes el·líptiques, i sigui*

$$\alpha(x, y) = (p(x)/q(x), ys(x)/t(x))$$

una isogènia de E_1 en E_2 en forma estàndard. Llavors q^3 divideix t^2, i t^2 divideix q^3f_1. En particular, $q(x)$ i $t(x)$ tenen les mateixes arrels en $\bar{K}$.

Demostració. Utilitzant l'equació de E_2,

$$y^2\frac{s(x)^2}{t(x)^2} = \left(\frac{p(x)}{q(x)}\right)^3 + A_2\left(\frac{p(x)}{q(x)}\right) + B_2 \tag{3}$$

$$\implies \frac{(x^3 + A_1x + B_1)s(x)^2}{t(x)^2} = \frac{p(x)^3 + A_2p(x)q(x)^2 + B_2q(x)^3}{q(x)^3}. \tag{4}$$

Posant $u(x) := p(x)^3 + A_2p(x)q(x)^2 + B_2q(x)^3$, observem que els polinomis u i q no tenen arrels en comú. Ara, reescrivim (4) com

$$q(x)^3s(x)^2(x^3 + A_1x + B_1) = q(x)^3s(x)^2f_1(x) = t(x)^2u(x).$$

Com que t i s són coprimers, obtenim el resultat, és a dir $q^3 \mid t^2$ i $t^2 \mid q^3f_1$. □

Lema 2.7. *Sigui $\alpha(x, y) = (p(x)/q(x), ys(x)/t(x))$ una isogènia $E_1 \to E_2$ en forma estàndard, $E_i : y^2 = x^3 + A_ix + B_i$. Els punts afins $(x_0 : y_0 : 1) \in E_1(\bar{K})$ del nucli de α són exactament aquells per als quals $q(x_0) = 0$.*

Demostració. Si $q(x_0) \neq 0$, llavors $t(x_0) \neq 0$, i $\alpha(x_0, y_0)$ és un punt afí, i per tant diferent de $\mathcal{O}$, és a dir $(x_0, y_0) \notin \ker\alpha$.

Homogeneïtzant i posant α en forma projectiva, podem escriure

$$\alpha = (pt : qsy : qt) = (\alpha_x : \alpha_y : \alpha_z),$$

on pt, qsy i qt són polinomis homogenis del mateix grau, amb $p, q, s, t \in K[x, z]$.

Sigui $P = (x_0 : y_0 : 1)$ un punt amb $q(x_0) = 0$. Suposem $y_0 \neq 0$. Pel Lema 2.6, $q(x_0, 1) = 0$ implica $t(x_0, 1) = 0$. La relació $q^3 \mid t^2$ ens diu que la multiplicitat de $(x_0, 1)$ com arrel de t és estrictament més gran que la seva multiplicitat com arrel de v. Per tant (treballant sobre $\bar{K}$) podem normalitzar α dividint per una potència adequada de $(x - x_0 z)$, de manera que α_x i α_z s'anul·lin en P i α_y no. Llavors

$$\alpha(x_0 : y_0 : 1) = (0 : 1 : 0) = \mathcal{O},$$

com volíem veure.

Suposem finalment $y_0 = 0$. Llavors x_0 és una arrel (simple) del polinomi $f_1(x)$ de l'equació $y^2 = f_1(x)$ de E_1. Podem normalitzar α multiplicant per yz i substituint $y^2 z$ pel polinomi homogeni $f_1(x, z) = x^3 + A_1 x z^2 + B_2 z^3$. De nou utilitzant $q^3 \mid t^2$, la multiplicitat de $(x_0, 1)$ com arrel de $q f_1$ és més petita o igual que la multiplicitat com arrel de t. Per tant podem normalitzar de nou dividint per una potència adequada de $(x - x_0 z)$ de manera que α_y no s'anul·li en $(x_0 : y_0 : 1)$ (i α_x, α_z sí, ja que són divisibles per y, i $y_0 = 0$). Novament el punt P és del nucli de α. □

Observació 2.8. *Per a cada arrel x_0 del polinomi $q(x)$, tenim una o dues arrels quadrades (en $\bar{K}$) de $x_0^3 + A_1 x_0 + B_1$. Això ens acota la mida del nucli d'una isogènia per $1 + 2r$, on r és el nombre d'arrels diferents de $q(x)$.*

Definició 2.9. *Definim el grau d'una isogènia α en forma estàndard com*

$$\deg(\alpha) := \max\{\deg p(x), \deg q(x)\}.$$

Per al morfisme trivial $\alpha = 0$, definim $\deg(0) := 0$.

Direm que $\alpha \neq 0$ és separable si $(p/q)' \neq 0$, i inseparable en cas contrari.

Lema 2.10. *Siguin $u, v \in K[x]$ polinomis coprimers. Les afirmacions següents són equivalents:*

1. $\left(\frac{u}{v}\right)' = 0$.
2. $u' = v' = 0$.
3. $u = f(x^p)$, $v = g(x^p)$, *on $f, g \in K[x]$ i p és la característica de K (possiblement zero).*

Demostració. Si $u' = v' = 0$, clarament $(u/v)' = 0$.

Si $(u/v)' = \frac{u'v - uv'}{v^2} = 0$, llavors $u'v = uv'$. Com que u i v són coprimers, la igualtat ens diu que u i u' (resp. v i v') tenen les mateixes arrels, i per tant $u' = v' = 0$.

Per a la segona equivalència, si un polinomi $u(x) = \sum_m a_m x^m$ té derivada nul·la $u'(x) = \sum_m m a_m x^{m-1}$, llavors necessàriament $p \mid m$, o bé $a_m = 0$ (per cada $m > 0$). Per tant $u(x) = f(x^p)$. Recíprocament, si $u(x) = f(x^p)$, llavors $u'(x) = f'(x^p) p x^{p-1} = 0$. □

Proposició 2.11. *Sigui $\alpha\colon E_1 \to E_2$ una isogènia separable. Llavors*

$$\deg(\alpha) = \#\ker(\alpha).$$

Si α és inseparable, llavors $\deg(\alpha) > \#\ker(\alpha)$.

Demostració. Posem $\alpha(x,y) = (r_1(x), yr_2(x))$, $r_1(x) = p(x)/q(x)$. Com que per cada $x \in \bar{K}$ hi ha com a mínim un punt $(x,y) \in E_1(\bar{K})$, $\alpha(E_1(\bar{K}))$ és un conjunt infinit. Per tant, podem triar $(a,b) \in \alpha(E_1(\bar{K}))$ que satisfaci

1. $a \neq 0$, $b \neq 0$, $(a,b) \neq \mathcal{O}$;
2. $\deg(p - aq) = \max\{\deg p, \deg q\} = \deg(\alpha)$;

Trobarem la mida del nucli comptant les antiimatges de (a,b). Per fer-ho, considerem les equacions

$$\frac{p(x_1)}{q(x_1)} = a, \qquad\qquad y_1 r_2(x_1) = b.$$

Com que $(a,b) \neq \mathcal{O}$, $q(x_1) \neq 0$. Pel Lema 2.6, $r_2(x_1)$ estarà definit, així que $y_1 = b/r_2(x_1)$ ($b \neq 0 \implies r_2(x_1) \neq 0$).

Ara –comptant multiplicitats– el polinomi $p - aq$ té $\deg\alpha$ arrels. Suposem que α és separable, és a dir, $r_1'(x) \neq 0$, i $p'q - q'p \neq 0$. Sigui S el conjunt de zeros de $(p'q - q'p)\cdot q$, que és finit. Podem afegir la condició que $a \notin r_1(S)$. Si x_0 fos una arrel múltiple de $p - aq$, tindríem

$$\begin{aligned} p(x_0) - aq(x) &= 0, \\ p'(x_0) - aq'(x_0) &= 0. \end{aligned}$$

Multiplicant les equacions $p = aq$ i $p' = aq'$, obtenim

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Però hem triat $a \neq 0$, implicant que x_0 és una arrel de $pq' - q'p$, i per tant $x_0 \in S$. Això ens diu que $a = r_1(x_0) \in r_1(S)$, contradicció per la tria de a.

Si α no és separable, llavors $p' = q' = 0$, de manera que $p - aq$ té sempre una quantitat d'arrels menor a $\deg(\alpha)$. □

Corol·lari 2.12. *Si* $\mathrm{char}K = 0$*, tota isogènia és separable.*

Demostració. Si $\alpha(x,y) = (p(x)/q(x), ys(x)/t(x))$, el Lema 2.10 ens diu que $(p/q)' = 0$ si, i només si, $p' = q' = 0$. Però en característica zero això és equivalent a que p i q siguin polinomis constants, i per tant α enviaria infinits punts a una mateixa imatge. El teorema anterior ens diu que això no pot passar. □

Proposició 2.13. *Siguin $E_i : y^2 = x^3 + A_i x + B_i$, $i = 1,2$ corbes el·líptiques sobre K. Tota isogènia $\alpha\colon E_1(\bar{K}) \to E_2(\bar{K})$ és exhaustiva.*

Demostració. Posem $\alpha(x,y) = (r_1(x), yr_2(x))$, $r_1(x) = p(x)/q(x)$. Sigui $(a,b) \in E_2(\bar{K})$, diferent de $\mathcal{O}$.

Si $p - aq$ no és constant, sigui x_0 una arrel d'aquest polinomi. Com que p i q són coprimers, $q(x_0) \neq 0$. Triem una de les arrels quadrades de $x_0^3 + A_1x_0 + B_1$, $y_0 \in \bar{K}$. Llavors pel Lema 2.6, $\alpha(x_0, y_0)$ està definit i val (a, b'). Com que $b'^2 = a^3 + A_1a + B_1 = b^2$, tenim $b = \pm b'$. Si $b' = -b$, llavors $\alpha(x_0, -y_0) = (a, -b') = (a, b)$, en cas contrari $\alpha(x_0, y_0) = (a, b)$.

Suposem ara que $p - aq$ és constant. Com que α té nucli finit, p i q no poden ser constants alhora. Per tant, hi ha com a molt un $a \in \bar{K}$ tal que $p - aq$ és constant, i com a màxim dos punts $(a, \pm b) \in E_2(\bar{K})$, que no són a la imatge de α. Sigui (a_1, b_1) un punt de la imatge, amb $\alpha(P_1) = (a_1, b_1)$. Podem triar aquest punt per tal que

$$(a_1, b_1) + (a, b) \neq (a, \pm b),$$

de manera que existeix P_2 amb $\alpha(P_2) = (a_1, b_1) + (a, b)$. D'aquí,

$$\begin{aligned} \alpha(P_2 - P_1) &= (a, b) \\ \alpha(P_1 - P_2) &= (a, -b). \end{aligned}$$

□

Definició 2.14. *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre un cos K de característica $p > 0$. Donat $q = p^r$, $r \geq 1$, definim la corba $E^{(q)}$ per l'equació*

$$E^{(q)} : y^2 = x^3 + A^q x + B^q.$$

Donada una isogènia $\alpha\colon E_1 \to E_2$, la isogènia $\alpha^{(q)}\colon E_1^{(q)} \to E_2^{(q)}$ correspon a elevar cada coeficient de α a q.

Existeix un morfisme de corbes natural entre E i $E^{(q)}$, corresponent a elevar cada coordenada a la q-èsima potència:

$$\begin{aligned} \pi_q\colon E &\to E^{(q)} \\ (x : y : z) &\mapsto (x^q : y^q : z^q), \end{aligned}$$

que anomenem q-Frobenius. Si no hi ha confusió en el valor de q (per exemple, perquè treballem sobre $K = \mathbb{F}_q$, o perquè utilitzem $q = p$), escriurem $\pi_E = \pi_q$.

Observem que per a qualsevol $q = p^r$, $r \geq 1$, el Frobenius π_q té nucli trivial, ja que

$$(x^q : y^q : z^q) = (0 : 1 : 0) \iff x = z = 0,\ y = 1.$$

Lema 2.15. *Sigui $\alpha\colon E_1 \to E_2$ una isogènia inseparable entre les corbes $E_i : y^2 = x^3 + A_ix + B_i$, $i = 1, 2$, definides sobre un cos de característica $p > 0$. Llavors podem escriure α com*

$$\alpha(x, y) = (r_1(x^p), y^p r_2(x^p)),$$

amb $r_1, r_2 \in K(x)$.

Demostració. Posem la isogènia en forma estàndard $\alpha(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right)$. Com que α és inseparable, $(p/q)' = 0$, i directament $p(x)/q(x) = r_1(x^p)$, amb $r_1(x) \in K(x)$. Veiem la segona coordenada. Substituint com al Lema 2.6, tenim la igualtat

$$\frac{fs^2}{t^2} = \frac{w}{q^3},$$

amb $f(x) = y^2 = x^3 + A_1x + B_1$ i $w := p^3 + A_2pq^2 + B_2q^3$. Com que $p' = q' = 0$, $w' = 0$,

$$\left(\frac{w}{q^3}\right)' = \left(\frac{fs^2}{t^2}\right)' = 0.$$

Per tant $s^2f = g(x^p)$ i $t^2 = h(x^p)$, per a certs polinomis $g, h \in K[x]$. Com que les arrels de $g(x^p)$ tenen multiplicitat p, f té tres arrels diferents, i p és senar, $s^2f = s_1^2f^p$, on $s_1 = g_1(x^p)$ per a un cert $g_1 \in K[x]$.

Ara, treballant mòdul l'equació $y^2 = x^3 + A_1x + B_1$,

$$\begin{aligned}(s(x)y)^2 \equiv (s(x))^2f(x) = g_1(x^p)^2f(x)^p \equiv (g_1(x^p)y^p)^2\\ \implies \left(\frac{s(x)}{t(x)}y\right)^2 \equiv \left(\frac{g_1(x^p)}{h(x^p)}y^p\right)^2 = (r(x^p)y^p)^2,\end{aligned}$$

on $r(x) = g_1(x)/h(x)$. Per tant $\frac{s(x)}{t(x)}y \equiv r_2(x^p)y^p$, amb $r_2 = \pm r$. □

Corol·lari 2.16. *Sigui α una isogènia de corbes definides sobre un cos K de característica $p > 0$. Llavors existeix una isogènia separable α_{sep} i un enter $n \geq 0$ tal que*

$$\alpha = \alpha_{\text{sep}} \circ \pi_p^n.$$

A més, $\deg \alpha = p^n \deg \alpha_{\text{sep}}$.

Demostració. Si α és separable, posem $\alpha = \alpha_{\text{sep}}$ i $n = 0$.

Si α és inseparable, el lema anterior ens diu que $\alpha(x, y) = (r_1(x^p), y^p r_2(x^p))$ per a funcions racionals $r_1, r_2 \in K(x)$, i $\alpha = \alpha_1 \circ \pi_p$, on $\alpha_1(x, y) = (r_1(x), yr_2(x))$. Si α_1 és inseparable podem aplicar el mateix procediment per acabar obtenint

$$\alpha = \alpha_n \circ \pi_p^n,$$

amb α_n separable (aquest procediment ha d'acabar, ja que $\deg \alpha$ és finit i a cada pas el dividim per p). Finalment, $\alpha_{\text{sep}} = \alpha_n$. □

Observació 2.17. *El domini de α_{sep} serà la corba $E^{(p^n)}$.*

Definició 2.18. *Amb $\alpha = \alpha_{\text{sep}} \circ \pi_p^n$, definim els graus de separabilitat i inseparabilitat de α com*

$$\begin{aligned}\deg_s \alpha &:= \deg(\alpha_{\text{sep}})\\ \deg_i \alpha &:= p^n.\end{aligned}$$

Pel corol·lari anterior, tenim la igualtat $\deg \alpha = \deg_s \alpha \cdot \deg_i \alpha$. *Les isogènies amb grau de separabilitat 1 es diuen purament inseparables.*

Teorema 2.19. *L'ordre del nucli d'una isogènia és igual al seu grau de separabilitat.*

Demostració. Utilitzant la Proposició 2.11 i el Corol·lari 2.16, tenim

$$\#\ker \alpha = \#\ker \alpha_{\text{sep}} = \deg \alpha_{\text{sep}} = \deg_s \alpha.$$

□

Corol·lari 2.20. *Tota isogènia purament inseparable té nucli trivial.* □

Proposició 2.21. *Donada la composició d'isogènies $\alpha = \beta \circ \gamma$,*

$$\begin{aligned}\deg \alpha &= (\deg \beta)(\deg \gamma),\\ \deg_s \alpha &= (\deg_s \beta)(\deg_s \gamma),\\ \deg_i \alpha &= (\deg_i \beta)(\deg_i \gamma).\end{aligned}$$

Demostració. La primera igualtat és conseqüència de les altres dues. Com que γ és un morfisme de grups exhaustiu, tenim

$$\deg_s \alpha = \#\ker \alpha = \#\ker \beta \cdot \#\ker \gamma = \deg_s \beta \cdot \deg_s \gamma.$$

Factoritzant les isogènies α, β i γ tenim

$$\alpha_{\text{sep}} \circ \pi^a = \beta_{\text{sep}} \circ \pi^b \circ \gamma_{\text{sep}} \circ \pi^c.$$

Les isogènies $\delta = \pi^b \circ \gamma_{\text{sep}}$ i γ_{sep} tenen el mateix nucli (i per tant el mateix grau de separabilitat), i podem escriure

$$\delta = \delta_{\text{sep}} \circ \pi^b.$$

Per tant $\alpha_{\text{sep}} \circ \pi^a = \beta_{\text{sep}} \circ \delta_{\text{sep}} \circ \pi^{bc}$, i $\deg_s \alpha = \deg_s(\beta_{\text{sep}} \circ \delta_{\text{sep}}) = (\deg_s \beta)(\deg_s \delta) = (\deg_s \beta)(\deg_s \gamma)$. Necessàriament $a = bc$, i així $\deg_i \alpha = (\deg_i \beta)(\deg_i \gamma)$, ja que $\beta_{\text{sep}} \circ \gamma_{\text{sep}}$ és separable. □

Definició 2.22. *Donades E_1, E_2 dues corbes el·líptiques sobre K, definim el conjunt*

$$\hom(E_1, E_2) := \{\alpha \colon E_1 \to E_2 \mid \alpha \text{ isogènia definida sobre } K\} \cup \{0 \colon E_1 \to E_2\}.$$

Si L/K és una extensió algebraica, denotem $\hom_L(E_1, E_2)$ el conjunt de morfismes definits sobre L.

El conjunt $\hom(E_1, E_2)$ és un grup abelià, definint la suma com

$$(\alpha + \beta)(P) := \alpha(P) + \beta(P),$$

i amb el morfisme zero com a element neutre. Si $\alpha \in \hom(E_1, E_2)$, tenim $\alpha + \cdots + \alpha = n\alpha = [n] \circ \alpha$, on $[n]$ és la multiplicació per n a E_1. Si α i n són no nuls, els dos són exhaustius, i per tant $n\alpha \neq 0$. Per tant $\hom(E_1, E_2)$ és lliure de torsió.

Definició 2.23. *Sigui E una corba el·líptica sobre K. L'anell d'endomorfismes de E és el grup additiu*

$$\text{End}(E) := \hom(E, E),$$

amb la multiplicació definida per la composició: $\alpha\beta := \alpha \circ \beta$. En efecte, és un anell: la identitat és $1 = [1]$, i per $\alpha, \beta, \gamma \in \text{End}(E)$ i $P \in E(\bar{K})$ qualssevol,

$$\begin{aligned}((\alpha + \beta)\gamma)(P) &= (\alpha + \beta)\gamma(P) = \alpha(\gamma(P)) + \beta(\gamma(P)) = (\alpha\gamma + \beta\gamma)(P),\\ (\alpha(\beta + \gamma))(P) &= \alpha(\beta + \gamma)(P) = \alpha(\beta(P) + \gamma(P)) = (\alpha\beta + \alpha\gamma)(P).\end{aligned}$$

Per cada enter n, el morfisme $[n]$ pertany a $\mathrm{End}(E)$, i l'aplicació $n \mapsto [n]$ defineix un morfisme d'anells $\mathbb{Z} \to \mathrm{End}(E)$, ja que $[0] = 0$, $[1] = 1$, $[m]+[n] = [m+n]$ i $[m][n] = [mn]$. Com que $\hom(E, E)$ és lliure de torsió, el morfisme és injectiu, i podem identificar $\mathbb{Z}$ amb un subanell de $\mathrm{End}(E)$.

Els morfismes de multiplicació per n commuten doncs amb qualsevol element $\alpha \in \mathrm{End}(E)$: per a tot $P \in E(\bar{K})$,

$$(\alpha \circ [n])(P) = \alpha(P + \cdots + P) = \alpha(P) + \cdots + \alpha(P) = n\alpha(P) = ([n] \circ \alpha)(P).$$

Si $K = \mathbb{F}_q$ és un cos finit, llavors el q-Frobenius π_E també commuta amb qualsevol morfisme α, ja que $(\pi_E \circ \alpha)(x, y) = \alpha(x, y)^q = \alpha(x^q, y^q) = (\alpha \circ \pi_E)(x, y)$. Per tant, el subanell $\mathbb{Z}[\pi_E]$ de $\mathrm{End}(E)$ es troba al centre de $\mathrm{End}(E)$.

Si $\alpha, \beta \in \mathrm{End}(E) \setminus \{0\}$, tots dos són isogènies i per tant exhaustius. D'aquí obtenim que $\alpha\beta = \alpha \circ \beta$ també ho és, i per tant no és nul. Per tant, $\mathrm{End}(E)$ no té divisors de zero.

2.4 Corba quocient i fórmules de Vélu

Fins ara hem vist que qualsevol isogènia és exhaustiva, té nucli finit, i es pot escriure com la composició d'una isogènia purament inseparable amb una de separable (que ens determina el nucli). El següent teorema ens diu que tot subgrup finit d'una corba el·líptica és el nucli d'alguna isogènia.

Teorema 2.24. *Sigui E una corba el·líptica sobre K i sigui G un subgrup finit de $E(\bar{K})$. Existeixen una corba el·líptica E' i una isogènia separable $\phi\colon E \to E'$, definides sobre una extensió finita de K, tals que $\ker \phi = G$. La corba E i la isogènia ϕ són úniques llevat d'isomorfisme.*

Demostració. Veure [Sil09, capítol III, proposició 4.12]. □

Sovint, la corba E' s'anomena el quocient de E per G, i per la unicitat llevat d'isomorfisme, s'escriu $E' \cong E/G$.

Corol·lari 2.25. *Tota isogènia es pot escriure com a composició d'isogènies de grau primer.*

Demostració. Si la isogènia α és inseparable, tenim $\alpha = \alpha_{\mathrm{sep}} \circ \pi^n$, i $\pi^n = \pi \circ \cdots \circ \pi$ és composició d'isogènies de grau p. Si α és separable, podem prendre subgrups d'ordre primer del seu nucli, i emprar el teorema anterior per descompondre la isogènia successivament. □

A més de l'evident importància del Teorema 2.24, el fet més important per a nosaltres és que la isogènia es pot calcular explícitament. A continuació donem les fórmules per calcular la isogènia $E \to E/G$. Suposarem que l'ordre de G és igual a 2 o senar, ja que les expressions són més senzilles i cobreixen tots els casos. Les fórmules generals es poden trobar a [Vél71], i a [Was08, §12.3] se'n dona la comprovació.

Teorema 2.26 (Vélu)**.** *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica sobre K i sigui $x_0 \in \bar{K}$ una arrel del polinomi $x^3 + Ax + B$. Definim $t := 3x_0^2 + A$ i $w := x_0 t$. L'aplicació racional*

$$\phi(x, y) := \left(\frac{x^2 - x_0 x + t}{x - x_0}, \frac{(x - x_0)^2 - t}{(x - x_0)^2} y \right)$$

és una isogènia separable de E en $E' : y^2 = x^3 + A'x + B'$, on $A' := A - 5t$ i $B' := B - 7w$. El nucli de ϕ és el grup d'ordre 2 generat per $(x_0, 0)$.

Teorema 2.27 (Vélu)**.** *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre K i sigui $G \subset E(\bar{K})$ un subgrup finit d'ordre senar. Per cada $Q = (x_Q, y_Q) \neq \mathcal{O}$ en G, definim*

$$t_Q := 3x_Q^2 + A,\ u_Q := 2y_Q^2,\ w_Q := u_Q + t_Q x_Q;$$

i sigui

$$t := \sum_{Q \in G \setminus \{\mathcal{O}\}} t_Q,\ w := \sum_{Q \in G \setminus \{\mathcal{O}\}} w_Q,\ r(x) := x + \sum_{Q \in G \setminus \{\mathcal{O}\}} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right).$$

L'aplicació racional

$$\phi(x, y) := (r(x), r'(x)y)$$

és una isogènia separable de E en $E' : y^2 = x^3 + A'x + B'$, amb $A' := A - 5t$ i $B' := B - 7w$, i $\ker \phi = G$.

2.5 L'invariant j

Definició 2.28. *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica. Definim l'invariant j de E com*

$$j = j(E) := 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

Notem que el denominador és el discriminant de la corba, que és no nul.

Proposició 2.29. *Siguin E_1 i E_2 dues corbes el·líptiques sobre K, amb $E_i : y^2 = x^3 + A_i x + B_i$. Aleshores E_1 i E_2 són isomorfes sobre $\bar{K}$ si, i només si, $j(E_1) = j(E_2)$.*

Demostració. Suposem que $\phi\colon E_1 \to E_2$ és un isomorfisme. Si l'expressem en forma normal, $\phi(x, y) = (r_1(x), y r_2(x))$, resulta que r_1 i r_2 han de ser polinomis de grau com a màxim 1, ja que ϕ té nucli trivial. Posem $r_1(x) = ax + b$. Substituint en l'equació de E_2, tenim

$$\begin{aligned} r_2(x)^2 y^2 &= (ax + b)^3 + A_2(ax + b) + B_2 \\ r_2(x)^2 (x^3 + A_1 x + B_1) &= (ax + b)^3 + A_2(ax + b) + B_2. \end{aligned}$$

Comparant ambdós costats de l'equació, veiem que r_2 ha de ser constant, posem $r_2(x) = c$. Comparant els coeficients de x^2, tenim que b ha de ser zero, i comparant els coeficients de x^3, tenim $a^3 = c^2$. En particular, $a = (c/a)^2$ i $c = (c/a)^3$. Definint $\mu = c/a$, obtenim $\phi(x, y) = (\mu^2 x, \mu^3 y)$. Però llavors

$$\mu^6 (x^3 + A_1 x + B_1) = \mu^6 x^3 + A_2 \mu^2 x + B_2,$$

de manera que $A_2 = \mu^4 A_1$ i $B_2 = \mu^6 B_1$, i

$$j(E_2) = 1728 \frac{4(\mu^4 A_1)^3}{4(\mu^4 A_1)^3 + 27(\mu^6 B_1)^2} = j(E).$$

Recíprocament, siguin j_1 i j_2 els invariants de E_1 i E_2, respectivament. Llavors

$$\frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27B_2^2},$$

d'on obtenim

$$A_1^3 B_2^2 = A_2^3 B_1^2. \tag{5}$$

Suposem primer $A_1 \neq 0$. Llavors $j_1 = j_2 \neq 0$ i $A_2 \neq 0$. Triem μ tal que $A_2 = \mu^4 A_1$. Per (5) tenim $B_2^2 = (\mu^6 B_1)^2$, de manera que $B_2 = \pm\mu^6 B_1$. Si $B_2 = \mu^6 B_1$ ja hem acabat. En cas contrari podem canviar μ per $i\mu$, i així $A_2 = \mu^4 A_1$ i $B_2 = \mu^6 B_1$.

En el cas $A_1 = 0$, $j_1 = j_2 = 0$ i $A_2 = 0$; triem μ tal que $B_2 = \mu^6 B_1$. □

Proposició 2.30. *Donat $j_0 \in \bar{K}$, existeix una corba el·líptica definida sobre el cos $K(j_0)$ amb invariant j igual a j_0.*

Demostració. Si $j_0 \neq 0, 1728$, la corba d'equació

$$y^2 = x^3 + \frac{3j_0}{1728 - j_0}x + \frac{2j_0}{1728 - j_0}$$

té discriminant

$$\Delta = 4\left(\frac{3j_0}{1728 - j_0}\right)^3 + 27\left(\frac{2j_0}{1728 - j_0}\right)^2 \neq 0$$

i invariant j

$$j = 1728\frac{4\left(\frac{3j_0}{1728-j_0}\right)^3}{\Delta} = 1728\frac{1}{1 + \frac{1728-j_0}{j_0}} = \frac{1728 j_0}{j_0 + 1728 - j_0} = j_0.$$

Si $j_0 = 0$ o 1728, tenim les corbes $y^2 = x^3 + 1$ i $y^2 = x^3 + x$, respectivament. □

Definim el grup d'automorfismes d'una corba E com el conjunt d'endomorfismes invertibles, és a dir,

$$\mathrm{Aut}(E) = \{\phi \in \mathrm{End}(E) \mid \exists \phi^{-1} \in \mathrm{End}(E)\}.$$

Proposició 2.31. *Sigui $E\colon y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre K. Llavors el grup* $\mathrm{Aut}(E)$ *és cíclic i té ordre:*

1. *2, si $j(E) \neq 0, 1728$,*
2. *4, si $j(E) = 1728$,*
3. *6, si $j(E) = 0$.*

Demostració. Un automorfisme de E té la forma $\phi(x, y) = (u^2 x, u^3 y)$, amb $u \in \bar{K}^\times$. Substituint, veiem que és necessari que $u^{-4}A = A$ i $u^{-6}B = B$. Si $j(E) \neq 0, 1728$, llavors $AB \neq 0$ i les úniques possibilitats són $u = \pm 1$. Si $j(E) = 1728$, tenim $B = 0$, de manera que $u^4 = 1$ i ϕ té ordre 4 (triant l'arrel de la unitat apropiada). Similarment, si $j(E) = 0$ tenim $A = 0$ i $u^6 = 1$, i per tant ϕ té ordre 6. □

Aquesta proposició ens dona explícitament tots els elements del grup d'automorfismes. Si $j(E) = 1728$, podem prendre $i \in \bar{K}$ una arrel quarta primitiva de la unitat, de manera que $\iota(x, y) = (-x, iy)$ genera $\mathrm{Aut}(E)$. De la mateixa manera, si $j(E) = 0$ agafem $\omega \in \bar{K}$ una arrel sisena primitiva de la unitat, i $\rho(x, y) = (\omega^2 x, -y)$ és un generador del grup.

2.6 Polinomis de divisió i endomorfisme $[n]$

Ja hem comentat que l'endomorfisme $[n]$ és una isogènia per a tot enter $n \neq 0$. En aquesta secció donarem la seva expressió amb funcions racionals, i veurem que és separable si, i només si, la característica de K no divideix n.

Per evitar considerar el cos en què es troben, momentàniament tractarem A i B com a variables. Definim els polinomis de divisió $\psi_m \in \mathbb{Z}[x, y, A, B]$:

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\ m \geq 2 \\
\psi_{2m} &= \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2),\ m \geq 3.
\end{aligned}$$

A continuació donem diversos resultats sense demostració que ens donaran, per una banda, el grau dels polinomis de divisió, i per l'altra, el fet que la multiplicació per n és un morfisme racional. Les demostracions involucren un seguit de càlculs llargs sense més valor que el de la comprovació. Per aquest motiu, hem decidit no incloure-les. Es poden trobar a [Was08, §3.2] i a [Sut17, §6].

Lema 2.32. *Per a n senar, ψ_n és un polinomi en $\mathbb{Z}[x, y^2, A, B]$. Si n és parell, ψ_n és un polinomi en $2y\mathbb{Z}[x, y^2, A, B]$.*

Definim ara $\psi_{-n} := -\psi_n$, i els polinomis

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
\omega_m &= \frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

Lema 2.33. *ϕ_n pertany a $\mathbb{Z}[x, y^2, A, B]$ per a tot n. Si n és senar, llavors ω_n pertany a $y\mathbb{Z}[x, y^2, A, B]$. Si n és parell, ω_n pertany a $\mathbb{Z}[x, y^2, A, B]$. A més, $\phi_{-n} = \phi_n$ i $\omega_{-n} = \omega_n$.*

Utilitzant $y^2 = x^3 + Ax + B$ (A, B continuen sent variables), tractarem els polinomis de $\mathbb{Z}[x, y^2, A, B]$ com polinomis de $\mathbb{Z}[x, A, B]$. Per tant, podem escriure $\phi_n(x)$ i $\psi_n^2(x)$.

Lema 2.34. *Per a tot $n \in \mathbb{Z}$, els polinomis ϕ_n, ψ_n satisfan*

$$\begin{aligned}
\phi_n &= x^{n^2} + \cdots \\
\psi_n &= \begin{cases} nx^{\frac{n^2-1}{2}} + \cdots, & n \text{ senar}, \\ y(nx^{\frac{n^2-4}{2}} + \cdots), & n \text{ parell}. \end{cases}
\end{aligned}$$

Corol·lari 2.35. *Per tot $n \geq 0$, tenim $\psi_n^2(x) = n^2x^{n^2-1} + \cdots$.*

Teorema 2.36. *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre K i n un enter no nul. La funció racional*

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

envia cada punt $P \in E(\bar{K})$ a nP. En particular, és un morfisme de grups.

A continuació calcularem el grau d'aquest endomorfisme i donarem un criteri per determinar la seva separabilitat.

Lema 2.37. *En les hipòtesis del teorema anterior, els polinomis $\phi_n(x)$ i $\psi_n^2(x)$ són coprimers.*

Demostració. Suposem que no ho són. Sigui $x_0 \in \bar{K}$ una arrel comuna, i sigui $P = (x_0, y_0)$ un punt de E diferent de $\mathcal{O}$. Llavors $nP = \mathcal{O}$, ja que $\psi_n^2(x_0) = 0$, i a més

$$\begin{aligned} &\phi_n(x_0) = x_0\psi_n^2(x_0) - \psi_{n+1}(x_0, y_0)\psi_{n-1}(x_0, y_0) \\ \implies\ &0 = 0 - \psi_{n+1}(x_0, y_0)\psi_{n-1}(x_0, y_0), \end{aligned}$$

per tant o bé $\psi_{n+1}(x_0, y_0) = 0$ o bé $\psi_{n-1}(x_0, y_0) = 0$. Però llavors tenim $(n-1)P = \mathcal{O}$ o $(n+1)P = \mathcal{O}$, i restant $nP = \mathcal{O}$ obtenim $-P = \mathcal{O}$ o $P = \mathcal{O}$, contradient la suposició inicial. □

Teorema 2.38. *Sigui E una corba el·líptica definida sobre K. L'endomorfisme de multiplicació per n*

$$[n]\colon E \to E$$

té grau n^2, i és separable si, i només si, n no és divisible per la característica de K.

Demostració. Pel Lema 2.34, tenim $\deg \phi_n = n^2$ i $\deg \psi_n^2 \leq n^2 - 1$, i pel lema anterior, els dos polinomis són coprimers. Per tant $\deg[n] = n^2$.

Si n no és divisible per la característica de K, el seu grau d'inseparabilitat ha de ser 1 i automàticament és separable. Si la característica de K és $p > 0$ i $p \mid n$, llavors el primer terme $n^2 x^{n^2-1}$ de ψ_n^2 s'anul·la. Per tant[4] el Lema 2.7 ens diu que el nucli $\ker[n]$ té estrictament menys de n^2 elements, i $[n]$ és inseparable. □

2.7 El subgrup de n-torsió $E[n]$

Donat $n > 0$, definim el subgrup de n-torsió com

$$E[n] := \{P \in E(\bar{K}) \mid nP = \mathcal{O}\}$$

o, alternativament, com el nucli de l'endomorfisme $[n]$.

En particular, si $p = \operatorname{char} K > 0$ i $p \nmid n$, o K té característica zero, $\#E[n] = n^2$. El següent resultat ens dona l'estructura d'aquests grups.

Teorema 2.39. *Sigui E una corba el·líptica definida sobre K i n un enter positiu. Si la característica de K no divideix n, o és zero, llavors*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Si la característica de K és $p > 0$ i $p \mid n$, posem $n = p^r n'$ amb $p \nmid n'$. Llavors

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \text{ o } E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}.$$

En particular $E[p^e] \cong \{0\}$ o $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.

[4] Per trobar el nombre d'arrels diferents del polinomi ψ_n^2, hem de comptar les arrels simples del factor en x de $\psi_n(x, y)$, i afegir-hi les tres arrels del polinomi $x^3 + Ax + B$ que obtenim al multiplicar per y^2.

Demostració. Pel teorema d'estructura dels grups abelians finitament generats,

$$E[n] \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \mathbb{Z}/n_r\mathbb{Z},$$

amb $n_i \mid n_{i+1}$. Si $p \nmid n$, sigui ℓ un primer dividint n_1. Llavors $\ell \mid n_i$ i $E[\ell] \subset E[n]$ té ordre ℓ^r. Per tant $r = 2$. El morfisme $[n]$ anul·la $E[n] \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, així que $n_2 \mid n$. Com que $n^2 = \#E[n] = n_1 n_2$, tenim $n_1 = n_2 = n$, i per tant

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Per al cas $p \mid n$, mirem primer la p^r-torsió. El nucli de $[p]$ és estrictament més petit que $\deg[p] = p^2$. Com que cada punt de $E[p]$ té ordre 1 o p, l'ordre del grup és una potència de p, i per tant $E[p] \cong \{0\}$ o $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. Si $E[p]$ és trivial, llavors $E[p^e]$ també.

Si $E[p] = \langle P \rangle$, amb $P \in E(\bar{K})$ d'ordre p, podem utilitzar l'exhaustivitat de $[p]\colon E \to E$ per trobar $Q \in E(\bar{K})$ tal que $pQ = P$, que tindrà ordre p^2. Iterant, en $E[p^e]$ tenim punts d'ordre p^e. Posem

$$E[p^e] \cong \langle P_1 \rangle \times \cdots \times \langle P_r \rangle$$

amb cada P_i d'ordre $p^{e_i} > 1$. Llavors

$$E[p] \cong \langle p^{e_1-1}P_1 \rangle \times \cdots \times \langle p^{e_r-1}P_r \rangle \cong (\mathbb{Z}/p\mathbb{Z})^r\,.$$

La conclusió és $r = 1$, i $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.

Ara, si $p \mid n$, posem $n = p^r n'$, $r > 0$ i $p \nmid n'$. Llavors $E[n] \cong E[n'] \times E[p^r]$. Tenim $E[n'] \cong (\mathbb{Z}/n'\mathbb{Z})^2$ i $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ o $\{0\}$. En el primer cas tenim $E[n] \cong (\mathbb{Z}/n'\mathbb{Z})^2$, i en el segon $E[n] \cong \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/p^r\mathbb{Z} \cong \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

Exemple 2.40 (2-torsió)**.** *El subgrup $E[2]$ està format pels punts $P \in E(\bar{K})$ tals que $2P = \mathcal{O}$ o, alternativament, tals que $P = -P$. Suposant que $P = (x_0, y_0) \neq \mathcal{O}$, tenim la igualtat*

$$(x_0, y_0) = -(x_0, y_0) = (x_0, -y_0),$$

de manera que $y_0 = 0$. Com que $y_0^2 = x_0^3 + Ax_0 + B$, obtenim que els punts de 2-torsió són exactament els de la forma $(x_0, 0)$ amb x_0 una arrel de $f(x) = x^3 + Ax + B$. Notem que, al ser E no singular, les tres arrels de f són totes diferents. Per tant $E[2]$ té quatre elements (les tres arrels de f i el punt a l'infinit), i com que tots són de 2-torsió, ha de ser isomorf al grup de Klein,

$$E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

2.8 Isogènies duals

Teorema 2.41. *Donada una isogènia $\alpha\colon E_1 \to E_2$ qualsevol, existeix una única isogènia $\hat{\alpha}\colon E_2 \to E_1$ tal que $\hat{\alpha} \circ \alpha = [n]$, on $n = \deg \alpha$.*

Demostració. La unicitat és immediata, per exhaustivitat: si $\alpha_1 \circ \alpha = \alpha_2 \circ \alpha$, llavors $\alpha_1(P) = \alpha_2(P)$ per a tot $P \in E_2(\bar{K})$, i per tant $\alpha_1 = \alpha_2$.

Per l'existència, procedim per inducció sobre els factors primers de n.

Si $n = 1$, llavors α és un isomorfisme, i podem prendre $\hat{\alpha} = \alpha^{-1}$, i $\hat{\alpha} \circ \alpha = \alpha^{-1} \circ \alpha = [1]$.

Si α té grau primer $\ell \neq p$, llavors és separable, i el grup $E_1[\ell]$ té ℓ^2 elements. Sigui $\alpha'\colon E_2 \to E_3$ la isogènia (separable) amb nucli $\alpha(E_1[\ell])$, que té grau $\#\alpha(E_1[\ell]) = \ell^2/\ell = \ell$.

La composició $\alpha' \circ \alpha$ té nucli $E_1[\ell]$, i per tant existeix un isomorfisme $\iota\colon E_3 \to E_1$ tal que $\iota \circ \alpha' \circ \alpha = [\ell]$, posem $\hat{\alpha} = \iota \circ \alpha'$.

Si α té grau p, distingim dos casos:

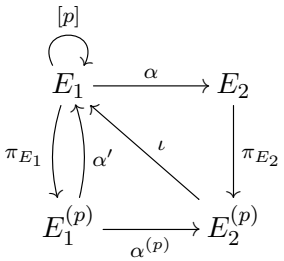
Cas 1: α separable. Posem π_{E_1} i π_{E_2} per representar el p-Frobenius amb domini E_1 i E_2 (amb imatges $E_1^{(p)}$ i $E_2^{(p)}$), respectivament. En aquest cas $\#\ker\alpha = p$, de manera que $E_1[p] \cong \mathbb{Z}/p\mathbb{Z}$, $[p] = \alpha' \circ \pi_{E_1}$, amb α' separable de grau p. Tenim $\pi_{E_2} \circ \alpha = \alpha^{(p)} \circ \pi_{E_1}$:

$$(\pi_{E_2} \circ \alpha)(x, y) = \alpha(x, y)^p = \alpha^{(p)}(x^p, y^p) = (\alpha^{(p)} \circ \pi_{E_1})(x, y).$$

Per tant $\ker(\alpha^{(p)} \circ \pi_{E_1}) = \ker(\pi_{E_2} \circ \alpha) = \ker\alpha = \ker[p] = \ker(\alpha' \circ \pi_{E_1})$, i per tant $\alpha^{(p)}$ i α' són isogènies separables amb el mateix nucli. Si $\iota\colon E_2^{(p)} \to E_1$ és l'isomorfisme donat pel teorema 2.24, tenim $\hat{\alpha} := \iota \circ \pi_{E_2}$, en efecte,

$$\hat{\alpha} \circ \alpha = \iota \circ \pi_{E_2} \circ \alpha = \iota \circ \alpha^{(p)} \circ \pi_{E_1} = \alpha' \circ \pi_{E_1} = [p].$$

La situació es pot resumir amb el següent diagrama commutatiu:



Cas 2: α inseparable. Tenim $\alpha = \iota \circ \pi$, on ι és un isomorfisme. Si $E[p] \cong \{0\}$, $[p]$ és purament inseparable de grau p^2, per tant $[p] = \iota' \circ \pi^2$ (amb ι' un isomorfisme) i podem posar $\hat{\alpha} = \iota' \circ \iota^{-1}$. Si $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ llavors $[p] = \alpha' \circ \pi$, α' separable de grau p, i $\hat{\alpha} := \alpha' \circ \iota^{-1}$.

Si n és compost, podem descompondre α com a producte d'isogènies de grau primer. Això ens permet escriure $\alpha = \alpha_1 \circ \alpha_2$, on α_1, α_2 són isogènies de graus $n_1, n_2 < n$. Sigui $\hat{\alpha} = \hat{\alpha}_2 \circ \hat{\alpha}_1$, on $\hat{\alpha}_1$ i $\hat{\alpha}_2$ existeixen per hipòtesi d'inducció. Llavors

$$\hat{\alpha} \circ \alpha = \hat{\alpha}_2 \circ \hat{\alpha}_1 \circ \alpha_1 \circ \alpha_2 = \hat{\alpha}_2 \circ [n_1] \circ \alpha_2 = \hat{\alpha}_2 \circ \alpha_2 \circ [n_1] = [n_2] \circ [n_1] = [n].$$

□

Definició 2.42. *Diem que $\hat{\alpha}$ és la isogènia dual de α.*

Lema 2.43. *Per tota isogènia α de grau n tenim* $\deg\hat{\alpha} = \deg\alpha = n$, *i* $\alpha \circ \hat{\alpha} = \hat{\alpha} \circ \alpha = [n]$,[5] *de manera que $\hat{\hat{\alpha}} = \alpha$. Per tot enter n, l'endomorfisme $[n]$ és autodual, és a dir, $\widehat{[n]} = [n]$.*

Demostració. Com que $\deg\alpha = n$, i $(\deg\hat{\alpha})(\deg\alpha) = \deg n = n^2$, el grau de $\hat{\alpha}$ és també n. Per la segona igualtat, tenim

$$(\alpha \circ \hat{\alpha}) \circ \alpha = \alpha \circ [n] = [n] \circ \alpha$$

i com que α és exhaustiva, $\alpha \circ \hat{\alpha} = [n]$. Finalment, observem que $[n][n] = [n^2] = [\deg[n]]$, per tant $\widehat{[n]} = [n]$. □

[5] Una de les igualtats té lloc a la corba domini de α, i l'altra, a la corba imatge.

Lema 2.44. *Donats* $\alpha, \beta \in \hom(E_1, E_2)$, $\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}$.

Demostració. La demostració es fa via el grup de divisors de la corba. Veure [Sil09, capítol III, teorema 6.2]. □

Lema 2.45. *Donat un endomorfisme* α *tenim* $\alpha + \hat{\alpha} = 1 + \deg\alpha - \deg(1-\alpha)$, *utilitzant la injecció* $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ *per als enters de la igualtat.*

Demostració.

$$\begin{aligned}\deg(1-\alpha) &= \widehat{(1-\alpha)}(1-\alpha) = (\hat{1}-\hat{\alpha})(1-\alpha)\\ &= (1-\hat{\alpha})(1-\alpha) = 1-(\alpha+\hat{\alpha})+\hat{\alpha}\alpha = 1-(\alpha+\hat{\alpha})+\deg\alpha.\end{aligned}$$

□

Definició 2.46. *La traça d'un endomorfisme* α *és l'enter* $\mathrm{tr}\,\alpha := \alpha + \hat{\alpha}$.

Teorema 2.47. *Sigui* $\alpha \in \mathrm{End}(E)$. *Tant* α *com el dual* $\hat{\alpha}$ *són arrels del polinomi*

$$p(\lambda) = \lambda^2 - (\mathrm{tr}\,\alpha)\lambda + \deg\alpha.$$

Demostració. $p(\alpha) = \alpha^2 - (\alpha+\hat{\alpha})\alpha + \hat{\alpha}\alpha = 0$; $p(\hat{\alpha}) = \hat{\alpha}^2 - (\alpha+\hat{\alpha})\hat{\alpha} + \alpha\hat{\alpha} = 0$. □

3 Corbes el·líptiques sobre cossos finits

En aquesta secció estudiarem les propietats de les corbes el·líptiques definides sobre un cos finit $K = \mathbb{F}_q$, amb $q = p^r$. El nombre de punts de la corba és ara finit, i el Teorema de Hasse ens diu que aquest nombre és aproximadament q. A continuació veurem les estructures possibles de l'anell d'endomorfismes d'una corba. Definirem i caracteritzarem les nocions de corba el·líptica *ordinària* i *supersingular* i, finalment, comptarem el nombre de classes d'isomorfisme de corbes supersingulars per a un primer p.

3.1 Teorema de Hasse

Lema 3.1. *Siguin α, β isogènies de E_1 en E_2 amb α inseparable. Llavors $\alpha + \beta$ és inseparable si, i només si, β és inseparable.*

Demostració. Si β és inseparable, podem escriure $\alpha = \alpha_{\text{sep}} \circ \pi^a$ i $\beta = \beta_{\text{sep}} \circ \pi^b$. Llavors

$$\alpha + \beta = \alpha_{\text{sep}} \circ \pi^a + \beta_{\text{sep}} \circ \pi^b = (\alpha_{\text{sep}} \circ \pi^{a-1} + \beta_{\text{sep}} \circ \pi^{b-1}) \circ \pi,$$

que és inseparable.

Si $\alpha + \beta$ és inseparable, llavors $-(\alpha + \beta)$ també, i $\alpha - (\alpha + \beta) = \beta$ és suma d'inseparables, implicant que β és inseparable. □

En particular, si considerem que el morfisme zero és inseparable, el conjunt d'endomorfismes inseparables és un ideal de $\text{End}(E)$.

Teorema 3.2 (Hasse)**.** *Sigui E una corba el·líptica sobre el cos finit $\mathbb{F}_q$. Llavors*

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

on $t := \operatorname{tr} \pi_E$ és la traça de l'endomorfisme de Frobenius, i $|t| \leq 2\sqrt{q}$.

Demostració. L'endomorfisme π_E està definit com

$$(x : y : z) \mapsto (x^q : y^q : z^q),$$

per tant, com que $\mathbb{F}_q$ és el cos fixat pel Frobenius $\alpha \mapsto \alpha^q$,

$$E(\mathbb{F}_q) = \{P \in E(\bar{\mathbb{F}}_q) \mid \pi_E(P) = P\} = \{P \in E(\bar{\mathbb{F}}_q) \mid \pi_E(P) - P = \mathcal{O}\} = \ker(\pi_E - 1).$$

Com que π_E és inseparable i $[1]$ és separable, $\pi_E - 1$ és separable. Per tant

$$\#E(\bar{\mathbb{F}}_q) = \#\ker(\pi_E - 1) = \deg(\pi_E - 1) = \widehat{(\pi_E - 1)}(\pi_E - 1) = \hat{\pi}_E\pi_E - \hat{\pi}_E - \pi_E + 1 = q - t + 1.$$

Només queda comprovar que $|t| \leq 2\sqrt{q}$. Sigui $r, s \in \mathbb{Z}$, aleshores

$$\begin{aligned} 0 \leq \deg(r\pi_E - s) = \widehat{(r\pi_E - s)}(r\pi_E - s) &= \hat{\pi}_E\hat{r}r\pi_E - \hat{\pi}\hat{r}s - \hat{s}r\pi_E + \hat{s}s \\ &= r^2q - rs(\pi_E + \hat{\pi}_E) + s^2 = r^2q - rst + s^2. \end{aligned}$$

Dividint per s^2, tenim que per a tot $r/s \in \mathbb{Q}$

$$q\left(\frac{r}{s}\right)^2 - t\left(\frac{r}{s}\right) + 1 \geq 0.$$

Com que $\mathbb{Q}$ és dens en $\mathbb{R}$, resulta que per a tot $x \in \mathbb{R}$ es compleix $qx^2 - tx + 1 \geq 0$. Per tant, el discriminant d'aquest polinomi no pot ser estrictament positiu, és a dir, $t^2 - 4q \leq 0$. Però això implica $t^2 \leq 4q$, i alhora $|t| \leq 2\sqrt{q}$. □

3.2 Àlgebres d'endomorfismes

Donada una corba el·líptica E/K, sabem que l'anell d'endomorfismes $\mathrm{End}(E)$ és un domini d'integritat que conté $\mathbb{Z}$. Classificarem completament l'estructura d'aquest anell mitjançant l'ús de l'àlgebra d'endomorfismes $\mathrm{End}^0(E)$.

Definició 3.3. *Un antimorfisme d'anells $\phi\colon R \to S$ és un morfisme de grups additius tal que $\phi(\alpha\beta) = \phi(\beta)\phi(\alpha)$ per a tot $\alpha, \beta \in R$. Una (anti) involució és un antimorfisme $\phi\colon R \to R$ que és la seva pròpia aplicació inversa, és a dir $\phi \circ \phi = id_R$. Una involució d'un anell commutatiu és doncs un automorfisme.*

Definició 3.4. *Donat un anell commutatiu R, una R-àlgebra associativa i unitària és un anell A, no necessàriament commutatiu, amb un morfisme d'anells $R \to A$ tal que la imatge de R està continguda al centre de A.*

Si l'anell A té una involució, diem que és una R-involució si la restricció a R és la identitat.

En la nostra situació, l'anell d'endomorfismes $\mathrm{End}(E)$ és una $\mathbb{Z}$-àlgebra, el morfisme $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ és injectiu, i la involució $\alpha \mapsto \hat{\alpha}$ fixa els enters $n \in \mathrm{End}(E)$.

Definició 3.5. *L'àlgebra d'endomorfismes de E és*

$$\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Recordem que donades dues R-àlgebres A i B, podem donar-li estructura d'anell al R-mòdul $A \otimes_R B$ definint el producte com

$$(a \otimes b)(a' \otimes b') = (aa' \otimes bb')$$

i estenent per linealitat (veure [AM69, capítol 2]). El següent lema ens dona una manera còmoda d'escriure els elements de l'àlgebra d'endomorfismes de E.

Lema 3.6. *Sigui R un domini d'integritat amb cos de fraccions B, i sigui A una R-àlgebra. Tot element de $A \otimes_R B$ es pot escriure com $a \otimes b$, amb $a \in A$ i $b \in B$.*

Demostració. Veure [AM69, capítol 3, proposició 3.5]. □

Gràcies al lema, podem escriure cada element de $\mathrm{End}^0(E)$ com $\phi \otimes r$, amb $\phi \in \mathrm{End}(E)$ i $r \in \mathbb{Q}$. Per simplificar, ho escriurem $r\phi$. Els morfismes canònics $\mathrm{End}(E) \to \mathrm{End}^0(E)$, $\phi \mapsto \phi \otimes 1$ i $\mathbb{Q} \to \mathrm{End}(E)$, $r \mapsto 1 \otimes r$ són injectius –ja que $\mathrm{End}(E)$ i $\mathbb{Q}$ són $\mathbb{Z}$-àlgebres lliures de torsió–, i podem identificar $\mathrm{End}(E)$ i $\mathbb{Q}$ amb els corresponents subanells de $\mathrm{End}^0(E)$.

Notem que $\mathrm{End}(E) \cap \mathbb{Q} = \mathbb{Z}$. El subanell $\mathbb{Q}$ està al centre de $\mathrm{End}^0(E)$, per tant $\mathrm{End}^0(E)$ és una $\mathbb{Q}$-àlgebra. Com que tot $\phi \in \mathrm{End}^0(E)$ té un múltiple enter en $\mathrm{End}(E)$, que no té divisors de zero, $\mathrm{End}^0(E)$ no té divisors de zero.

A continuació estendrem la involució de $\mathrm{End}(E)$ donada per l'assignació $\alpha \mapsto \hat{\alpha}$, i veurem que els paral·lelismes amb les seves propietats.

Definició 3.7. *Definim la involució de Rosati per a $r\alpha \in \mathrm{End}^0(E)$ com $\widehat{r\alpha} := r\hat{\alpha}$.*

Per a $r \in \mathbb{Q}$, $\alpha, \beta \in \mathrm{End}^0(E)$, tenim les propietats immediates: $\hat{r} = r$, $\hat{\hat{\alpha}} = \alpha$, $\widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}$, $\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta}$.

Definició 3.8. *Sigui $\alpha \in \mathrm{End}^0(E)$. La norma (reduïda) de α és $N\alpha = \alpha\hat{\alpha}$, i la traça (reduïda) de α és $\operatorname{tr}\alpha := \alpha + \hat{\alpha}$.*

Lema 3.9. *Per a tot $\alpha \in \mathrm{End}^0(E)$, tenim $N\alpha \in \mathbb{Q}_{\geq 0}$, amb $N\alpha = 0$ si, i només si, $\alpha = 0$. A més, $N\hat{\alpha} = N\alpha$ i $N(\alpha\beta) = (N\alpha)(N\beta)$, per a tot $\alpha, \beta \in \mathrm{End}^0(E)$.*

Demostració. Posem $\alpha = r\phi$, amb $r \in \mathbb{Q}$ i $\phi \in \mathrm{End}(E)$. La seva norma compleix $N\alpha = \alpha\hat{\alpha} = r^2 \deg\phi \geq 0$. Si r o ϕ són zero, llavors $\alpha = 0$ i $N\alpha = 0$, en cas contrari $N\alpha > 0$. Si $\alpha \neq 0$, tenim $\alpha N\hat{\alpha} = \alpha\hat{\alpha}\alpha = (N\alpha)\alpha = \alpha N\alpha$, per tant $\alpha(N\hat{\alpha} - N\alpha) = 0$ i $N\hat{\alpha} = N\alpha$. Finalment, si $\alpha, \beta \in \mathrm{End}^0(E)$, $N(\alpha\beta) = \alpha\beta\widehat{\alpha\beta} = \alpha\beta\hat{\beta}\hat{\alpha} = \alpha(N\beta)\hat{\alpha} = \alpha\hat{\alpha}N\beta = N\alpha N\beta$. □

Corol·lari 3.10. *Tot $\alpha \in \mathrm{End}^0(E)$ no nul té invers α^{-1}. Per tant, $\mathrm{End}^0(E)$ és un anell de divisió.*

Demostració. Sigui $\alpha \in \mathrm{End}^0(E) \setminus \{0\}$. Tenim $N\alpha \neq 0$, $\beta = \hat{\alpha}/N\alpha \neq 0$, i $\alpha\beta = \alpha\hat{\alpha}/N\alpha = 1$. Per tant β és una inversa per la dreta de α. Sigui γ una inversa per la dreta de β. Llavors $\beta\gamma = 1$, i $\gamma = \alpha\beta\gamma = \alpha \implies \beta\alpha = \beta\gamma = 1$, i β és una inversa per l'esquerra de α. Per tant $\alpha^{-1} = \beta$. □

Lema 3.11. *Per a tot $\alpha \in \mathrm{End}^0(E)$ tenim $\operatorname{tr}\hat{\alpha} = \operatorname{tr}\alpha \in \mathbb{Q}$. Per a tot $r \in \mathbb{Q}$, $\alpha, \beta \in \mathrm{End}^0(E)$ tenim $\operatorname{tr}(\alpha + \beta) = \operatorname{tr}\alpha + \operatorname{tr}\beta$, $\operatorname{tr}(r\alpha) = r\operatorname{tr}\alpha$.*

Demostració. En primer lloc, $\operatorname{tr}\hat{\alpha} = \hat{\alpha} + \hat{\hat{\alpha}} = \hat{\alpha} + \alpha = \operatorname{tr}\alpha$. A més,

$$\operatorname{tr}\alpha = \alpha + \hat{\alpha} = 1 + \alpha\hat{\alpha} - (1-\alpha)(1-\hat{\alpha}) = 1 + N\alpha - N(1-\alpha) \in \mathbb{Q}.$$

També tenim $\operatorname{tr}(\alpha+\beta) = \alpha + \beta + \widehat{\alpha+\beta} = \alpha + \beta + \hat{\alpha} + \hat{\beta} = (\alpha+\hat{\alpha}) + (\beta+\hat{\beta}) = \operatorname{tr}\alpha + \operatorname{tr}\beta$. Finalment $\operatorname{tr}(r\alpha) = r\alpha + \widehat{r\alpha} = r\alpha + \hat{\alpha}\hat{r} = r\alpha + \hat{\alpha}r = r\alpha + r\hat{\alpha} = r(\alpha + \hat{\alpha}) = r\operatorname{tr}\alpha$. □

Lema 3.12. *Sigui $\alpha \in \mathrm{End}^0(E)$. Llavors α i $\hat{\alpha}$ són arrels del polinomi característic*

$$p(x) = x^2 - (\operatorname{tr}\alpha)x + N\alpha \in \mathbb{Q}[x].$$

Demostració. $p(\alpha) = \alpha^2 - (\operatorname{tr}\alpha)\alpha + N\alpha = \alpha^2 - (\alpha+\hat{\alpha})\alpha + \hat{\alpha}\alpha = 0$; $p(\hat{\alpha}) = \hat{\alpha}^2 - (\operatorname{tr}\hat{\alpha})\hat{\alpha} + N\hat{\alpha} = \hat{\alpha}^2 - (\hat{\alpha}+\alpha)\hat{\alpha} + \alpha\hat{\alpha} = 0$. □

Corol·lari 3.13. *Per tot $\alpha \in \mathrm{End}^0(E)$ no nul tal que $\operatorname{tr}\alpha = 0$, $\alpha^2 = -N\alpha < 0$. Un element $\alpha \in \mathrm{End}^0(E)$ és fix per la involució de Rosati si, i només si, $\alpha \in \mathbb{Q}$.*

Demostració. La primera igualtat se segueix de l'equació $\alpha^2 - (\operatorname{tr}\alpha)\alpha + N\alpha = 0$. Per veure la segona afirmació, donat $r \in \mathbb{Q}$ tenim $\hat{r} = r$. Si $\hat{\alpha} = \alpha$ llavors el discriminant de $p(x)$, $(\operatorname{tr}\alpha)^2 - 4N\alpha$ ha de ser zero, i per tant $\alpha = (\operatorname{tr}\alpha)/2$. □

Un dels tipus d'àlgebres d'endomorfismes que ens apareixeran són les àlgebres de quaternions, que introduïm a continuació.

Definició 3.14. *Una àlgebra de quaternions sobre un cos K és una K-àlgebra amb una base de la forma $\{1, \alpha, \beta, \alpha\beta\}$, on $\alpha^2, \beta^2 \in K^\times$ i $\alpha\beta = -\beta\alpha$.*

Si H és una àlgebra de quaternions sobre un cos K, H és un espai vectorial quatridimensional amb base $\{1, \alpha, \beta, \alpha\beta\}$. Posem $H = K \oplus H_0$, on $K = \langle 1 \rangle$ i $H_0 = \langle \alpha, \beta, \alpha\beta \rangle$. Anomenem H_0 l'espai dels quaternions purs. Tot $\gamma \in H$ té una descomposició única de la forma $a + \gamma_0$, amb $a \in K$ i $\gamma_0 \in H_0$. L'únic $\hat{\gamma} = a - \gamma_0$ tal que $\gamma + \hat{\gamma} = 2a$ s'anomena el *conjugat* de γ.

L'aplicació $\gamma \mapsto \hat{\gamma}$ és una involució de la K-àlgebra H, i definim la traça $\operatorname{tr}\gamma := \gamma + \hat{\gamma}$ i la norma $N\gamma := \gamma\hat{\gamma}$. Les dues aplicacions donen valors en K: en el cas de la traça és clar per la definició del conjugat, i en el cas de la norma, posant $\gamma = a + \gamma_0$ i $\gamma_0 = b\alpha + c\beta + d\alpha\beta$,

$$N\gamma = (a + \gamma_0)(a - \gamma_0) = a^2 - (b\alpha + c\beta + d\alpha\beta)^2 = a^2 - (b^2\alpha^2 + c^2\beta^2 - d^2\alpha^2\beta^2) \in K.$$

Tenim $\operatorname{tr}\gamma = \operatorname{tr}\hat{\gamma}$, $N\gamma = N\hat{\gamma}$, la traça és additiva, i la norma és multiplicativa.

Teorema 3.15. *Sigui E una corba el·líptica sobre el cos K. Llavors l'àlgebra d'endomorfismes $\operatorname{End}^0(E)$ és isomorfa a una $\mathbb{Q}$-àlgebra de les següents:*

1. *El cos dels nombres racionals $\mathbb{Q}$,*
2. *Un cos quadràtic imaginari $\mathbb{Q}(\alpha)$, amb $\alpha^2 < 0$,*
3. *Una àlgebra de quaternions $\mathbb{Q}(\alpha, \beta)$, amb $\alpha^2, \beta^2 < 0$.*

Demostració. Si $\operatorname{End}^0(E) = \mathbb{Q}$, estem al primer cas. Si no hi ha igualtat, sigui α un element de $\operatorname{End}^0(E) \setminus \mathbb{Q}$. Substituint α per $\alpha - \frac{1}{2}\operatorname{tr}\alpha$, podem suposar $\operatorname{tr}\alpha = 0$, ja que

$$\operatorname{tr}(\alpha - \frac{1}{2}\operatorname{tr}\alpha) = \operatorname{tr}\alpha - \frac{1}{2}\operatorname{tr}(\operatorname{tr}\alpha) = \operatorname{tr}\alpha - \frac{1}{2}(\widehat{\operatorname{tr}\alpha} + \operatorname{tr}\alpha) = 0.$$

Tenim doncs $\alpha^2 < 0$, i $\mathbb{Q}(\alpha) \subseteq \operatorname{End}^0(E)$ és un cos quadràtic imaginari. Si hi ha igualtat, ens trobem al segon cas. Si no hi ha igualtat, sigui $\beta \in \operatorname{End}^0(E) \setminus \mathbb{Q}(\alpha)$. De nou podem suposar que $\operatorname{tr}\beta = 0$ i $\beta^2 < 0$. Substituint β per $\beta - \frac{\operatorname{tr}(\alpha\beta)}{2\alpha^2}\alpha$, podem suposar també que $\operatorname{tr}(\alpha\beta) = 0$. Per tant $\operatorname{tr}\alpha = \operatorname{tr}\beta = \operatorname{tr}(\alpha\beta) = 0$.

Això implica $\alpha = -\hat{\alpha}$, $\beta = -\hat{\beta}$, i $\alpha\beta = -\widehat{\alpha\beta} = -\hat{\beta}\hat{\alpha}$. D'aquí obtenim $\alpha\beta = -\beta\alpha$. Juntament amb el fet que $\alpha^2, \beta^2 < 0$ estan en $\mathbb{Q}$, resulta que $\{1, \alpha, \beta, \alpha\beta\}$ generen $\mathbb{Q}(\alpha, \beta)$ com a $\mathbb{Q}$-espai vectorial. Ens falta veure que són linealment independents. Suposem que

$$\alpha\beta = a + b\alpha + c\beta, \ \ a, b, c \in \mathbb{Q}.$$

Necessàriament $c \neq 0$, en cas contrari $\alpha\beta \in \mathbb{Q}(\alpha)$, que implica $\beta \in \mathbb{Q}(\alpha)$. Elevant al quadrat,

$$(\alpha\beta)^2 = (a + b\alpha + c\beta)^2 = (a^2 + b^2\alpha^2 + c^2\beta^2) + 2a(b\alpha + c\beta) + bc(\alpha\beta + \beta\alpha).$$

Ara $\operatorname{tr}\alpha\beta = 0$ implica $(\alpha\beta)^2 \in \mathbb{Q}$. Com que $\alpha\beta = -\beta\alpha$, el darrer terme de la suma és zero. El primer pertany a $\mathbb{Q}$, i per tant $d = b\alpha + c\beta \in \mathbb{Q}$. Però llavors $\beta \in (d - b\alpha)/c \in \mathbb{Q}(\alpha)$, contradicció. Per tant $\mathbb{Q}(\alpha, \beta) \subseteq \operatorname{End}^0(E)$ és una àlgebra de quaternions amb $\alpha^2, \beta^2 < 0$. Si hi ha igualtat, obtenim el tercer cas.

Si no hi hagués igualtat, podríem triar $\gamma \in \operatorname{End}^0(E) \setminus \mathbb{Q}(\alpha, \beta)$. De nou, podem suposar $\operatorname{tr}\gamma = \operatorname{tr}(\alpha\gamma) = 0$, que implica $\alpha\gamma = -\gamma\alpha$. Llavors $\alpha\beta\gamma = -\beta\alpha\gamma = \beta\gamma\alpha$, és a dir, α i $\beta\gamma$ commuten. Pel següent lema, $\beta\gamma \in \mathbb{Q}(\alpha)$, i al seu torn $\gamma \in \mathbb{Q}(\alpha, \beta)$, contradient la no igualtat. □

Lema 3.16. *Si $\alpha, \delta \in \mathrm{End}^0(E)$ commuten i $\alpha \notin \mathbb{Q}$, llavors $\delta \in \mathbb{Q}(\alpha)$.*

Demostració. Com a la demostració anterior, podem suposar que $\operatorname{tr}\alpha = \operatorname{tr}\delta = \operatorname{tr}(\alpha\delta) = 0$, i per tant $\alpha\delta = -\delta\alpha$. Com que els canvis necessaris són $\mathbb{Q}$-lineals, α i δ segueixen commutant. Però llavors $2\alpha\delta = 0$, implicant que $\alpha = 0$ o $\delta = 0$, com que $\alpha \notin \mathbb{Q}$, tenim $\delta = 0 \in \mathbb{Q}(\alpha)$. □

Finalment, podem donar l'estructura de l'anell d'endomorfismes $\mathrm{End}(E)$.

Corol·lari 3.17. *Sigui E una corba el·líptica sobre K. L'anell d'endomorfismes $\mathrm{End}(E)$ és un $\mathbb{Z}$-mòdul lliure de rang r, on $r = 1, 2, 4$ és la dimensió de $\mathrm{End}^0(E)$ com a $\mathbb{Q}$-espai vectorial.*

Demostració. Veure [Sut17, corol·lari 13.20] □

Definició 3.18 (Ordre)**.** *Sigui H una $\mathbb{Q}$-àlgebra amb $\dim_{\mathbb{Q}} H = r < \infty$. Un ordre O en H és un subanell de H que és un $\mathbb{Z}$-mòdul lliure de rang r.*

Pel Corol·lari 3.17, l'anell d'endomorfismes $\mathrm{End}(E)$ és un ordre en la $\mathbb{Q}$-àlgebra $\mathrm{End}^0(E)$.

3.3 Corbes supersingulars

Definició 3.19. *Sigui E una corba el·líptica definida sobre un cos K de característica $p > 0$. Diem que E és ordinària si $E[p] \cong \mathbb{Z}/p\mathbb{Z}$, i supersingular si $E[p] \cong \{0\}$.*

Direm que $j_0 \in \bar{K}$ és un invariant j supersingular si les corbes de la classe d'isomorfisme amb invariant j igual a j_0 són supersingulars.

Notem que E és supersingular si, i només si, $[p]$ és una isogènia purament inseparable, és a dir $\deg_s[p] = 1$ i $\deg_i[p] = p^2$.

Podem justificar el nom "supersingular" amb el següent lema, que ens diu que hi ha –com a màxim– p^2 invariants j supersingulars (recordem que cada $j_0 \in \bar{K}$ ens dona una classe d'isomorfisme de corbes el·líptiques).

Teorema 3.20. *Sigui $E\colon y^2 = x^3 + Ax + B$ una corba el·líptica supersingular definida sobre un cos K de característica $p > 0$. Llavors $j(E) \in \mathbb{F}_{p^2}$.*

Demostració. Sigui π el p-Frobenius entre E i $E^{(p)}$. L'endomorfisme $[p] = \hat{\pi}\pi$ té nucli trivial, per tant la isogènia $\hat{\pi}\colon E^{(p)} \to E$ té nucli trivial i ha de tenir grau d'inseparabilitat p. Per tant $\hat{\pi} = \hat{\pi}_{\mathrm{sep}} \circ \pi$, amb $\hat{\pi}_{\mathrm{sep}}$ un isomorfisme. Llavors podem expressar $[p] = \hat{\pi}_{\mathrm{sep}} \circ \pi^2$, i per tant $\hat{\pi}_{\mathrm{sep}}$ és un isomorfisme de $E^{(p^2)}$ en E. Però llavors $j(E) = j(E^{(p^2)}) = j(A^{p^2}, B^{p^2}) = j(A, B)^{p^2} = j(E)^{p^2}$. Obtenim que $j(E)$ és fix per l'automorfisme $\sigma\colon x \mapsto x^{p^2}$, i per tant $j(E) \in \mathbb{F}_{p^2}$. □

Els següents resultats ens permetran caracteritzar les corbes supersingulars, en particular, el nostre objectiu és estudiar-ne els anells d'endomorfismes.

Proposició 3.21. *Sigui $\phi\colon E_1 \to E_2$ una isogènia. Llavors E_1 és supersingular si, i només si, E_2 és supersingular.*

Demostració. Siguin $p_1 \in \mathrm{End}(E_1)$, $p_2 \in \mathrm{End}(E_2)$ els morfismes de multiplicació per p respectius de cada corba. Llavors $\phi \circ p_1 = p_2 \circ \phi$. Per tant $\deg_s \phi \deg_s p_1 = \deg_s p_2 \deg_s \phi$, i per tant $\deg_s p_1 = \deg_s p_2$. El resultat se segueix del fet que E_i és supersingular si i només si $\deg_s p_i = 1$. □

Proposició 3.22. *Una corba el·líptica $E/\mathbb{F}_q$ és supersingular si, i només si,* $\operatorname{tr} \pi_E \equiv 0 \mod p$.

Demostració. Posem $q = p^r$. Si E és supersingular, $E[p] = \ker[p] = \ker \pi\hat{\pi}$ és trivial, per tant $\hat{\pi}$ té nucli trivial i és inseparable. La isogènia $\hat{\pi}^r = \widehat{\pi^r} = \hat{\pi}_E$ és doncs inseparable, com també ho és π_E, i per tant $\operatorname{tr} \pi_E = \pi_E + \hat{\pi}_E$ és inseparable. Però $\operatorname{tr} \pi_E$ és un enter, implicant que $\operatorname{tr} \pi_E \equiv 0 \mod p$.

Recíprocament, si $\operatorname{tr} \pi_E \equiv 0 \mod p$ llavors $[\operatorname{tr} \pi_E]$ és inseparable, i per tant $\hat{\pi}_E = \operatorname{tr} \pi_E - \pi_E$ també ho és. Obtenim que $\hat{\pi}^n$ i $\hat{\pi}$ són inseparables, i el nucli de $\hat{\pi}$ és trivial, ja que $\deg \hat{\pi} = p$. El nucli de π també és trivial, de manera que $E[p] = \ker \hat{\pi}\pi$ és trivial i E és supersingular. □

Corol·lari 3.23. *Sigui E una corba el·líptica sobre $\mathbb{F}_p$, amb p un primer més gran que 3. Llavors E és supersingular si, i només si, $\#E(\mathbb{F}_p) = p + 1$.*

Demostració. Pel Teorema de Hasse, $|\operatorname{tr} \pi_E| \leq 2\sqrt{p}$, i per a $p > 3$, $2\sqrt{p} < p$. □

Lema 3.24. *Sigui $E/\mathbb{F}_q$ una corba el·líptica ordinària. Llavors $\pi_E^m = a\pi_E + b$ per a $m \geq 1$, amb $a \not\equiv 0 \mod p$ i $b \equiv 0 \mod p$.*

Demostració. Fem inducció sobre m. Si $m = 1$, podem prendre $a = 1$, $b = 0$. Aplicant la hipòtesi d'inducció,

$$\begin{aligned} \pi_E^{m+1} &= \pi_E \pi_E^m = \pi_E(a\pi_E + b) \\ &= a((\operatorname{tr} \pi_E)\pi_E - q) + b\pi_E \\ &= (a(\operatorname{tr} \pi_E) + b)\pi_E - aq \\ &= c\pi_E + d, \end{aligned}$$

on $c = a(\operatorname{tr} \pi_E) + b \not\equiv 0 \mod p$ (ja que $a \operatorname{tr} \pi_E \not\equiv 0$), i $d = -aq \equiv 0 \mod p$. □

Teorema 3.25. *Si $E/\mathbb{F}_q$ és una corba el·líptica ordinària,* $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$ *és un cos quadràtic imaginari.*

Demostració. Posem $q = p^r$. Si π_E fos un enter n, llavors $q = \deg \pi_E = \deg[n] = n^2$, que implicaria $n = \pm p^{r/2}$. Però llavors $\operatorname{tr} \pi_E = 2n \equiv 0 \mod p$, i E seria supersingular.

Per tant $\pi_E \notin \mathbb{Z}$, i $\pi_E \notin \mathbb{Q}$, ja que π_E és arrel d'un polinomi mònic amb coeficients enters. Pel lema anterior, $\pi_E^m \notin \mathbb{Q}$ per a $m \geq 1$, ja que $\pi_E^m = a\pi_E + b$ amb $a \neq 0$.

Sigui $\alpha \in \mathrm{End}^0(E)$. Podem escriure $\alpha = s\phi$ amb $s \in \mathbb{Q}$ i $\phi \in \mathrm{End}(E)$. L'endomorfisme ϕ està definit sobre $\mathbb{F}_{q^m}$, per algun m. Posant $\phi(x, y) = (r_1(x), r_2(x)y)$, tenim

$$(\phi\pi_E^m)(x, y) = (r_1(x^{q^m}), r_2(x^{q^m})y^{q^m}) = (r_1(x)^{q^m}, r_2(x)^{q^m} y^{q^m}) = (\pi_E^m \phi)(x, y),$$

i per tant α commuta amb π_E^m. Pel Lema 3.16, $\alpha \in \mathbb{Q}(\pi_E^m) \subseteq \mathbb{Q}(\pi_E)$. Per tant $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$. □

Corol·lari 3.26. *Si $E/\mathbb{F}_q$ és una corba el·líptica ordinària, llavors* $\mathrm{End}^0(E) \cong \mathbb{Q}(\sqrt{D})$, *on $D = t^2 - 4q < 0$, amb $t = tr\pi_E$.*

Demostració. Pel teorema anterior, tenim $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$, i $D = t^2 - 4q$ és el discriminant del polinomi característic de π_E, $X^2 - \operatorname{tr}\pi_E X + q$. L'enter D és negatiu perquè $\mathrm{End}^0(E)$ és un cos quadràtic imaginari. □

Lema 3.27. *Sigui D un enter lliure de quadrats. Aleshores existeixen infinits primers ℓ_i tals que* $\left(\frac{D}{\ell_i}\right) = -1$.

El lema es pot demostrar imposant equacions a ℓ_i mòdul els diferents primers que divideixen D, emprant la llei de reciprocitat quadràtica, i aplicant el Teorema de Dirichlet sobre primers en progressions aritmètiques.

Teorema 3.28. *Sigui E/K una corba el·líptica supersingular. Llavors* $\mathrm{End}^0(E)$ *és una àlgebra de quaternions.*

Demostració. Suposem que no és així. Llavors $\mathrm{End}(E)$ és isomorf a $\mathbb{Z}$ o a un ordre en un cos quadràtic imaginari $\mathbb{Q}(\sqrt{D})$, amb $D < 0$ lliure de quadrats. En el primer cas, tot endomorfisme té per grau un quadrat, per tant per a qualsevol primer ℓ, no hi ha cap endomorfisme ϕ de E amb grau ℓ.

En el segon cas, per a tot $\phi \in \mathrm{End}(E)$ el discriminant del polinomi característic $X^2 - (\operatorname{tr}\phi)X + \deg\phi$ és un enter que ha de ser un quadrat a $\mathrm{End}(E)$, ja que ϕ n'és una arrel. Si $\deg\phi$ és un primer ℓ, llavors

$$(\operatorname{tr}\phi)^2 - 4\ell = v^2 D,\ v \in \mathbb{Z},$$

implicant que D és un quadrat mòdul ℓ. Recíprocament, pel lema anterior existeixen infinits primers ℓ_i tals que $(D/\ell_i) = -1$, i per tant infinits primers ℓ_i tals que no existeix cap endomorfisme de grau ℓ_i.

Siguin doncs $\ell_1, \ell_2, \ldots$ una successió infinita de primers per als quals $\mathrm{End}(E)$ no conté elements de grau ℓ_i. Per cada ℓ_i, podem prendre $P_i \in E[\ell_i]$ d'ordre ℓ_i, i construir la isogènia separable $\phi_i \colon E \to E/\langle P_i\rangle =: E_i$. Les corbes E_i són totes supersingulars, i com que només en tenim un nombre finit de classes d'isomorfisme, existirà un isomorfisme $\alpha \colon E_i \xrightarrow{\sim} E_j$ amb $i \neq j$.

Considerem l'endomorfisme $\phi := \hat{\phi}_j \circ \alpha \circ \phi_i \in \mathrm{End}(E)$, de grau $\ell_i\ell_j$. El grau no és un quadrat, per tant $\mathrm{End}(E) \ncong \mathbb{Z}$, i $\mathrm{End}^0(E) \cong \mathbb{Q}(\sqrt{D})$. Però llavors el discriminant $(\operatorname{tr}\phi)^2 - 4\ell_i\ell_j$ és un quadrat, implicant que D és un quadrat mòdul ℓ_i. Hem trobat doncs una contradicció, i així $\mathrm{End}^0(E)$ és una àlgebra de quaternions. □

Corol·lari 3.29. *Sigui E una corba el·líptica sobre un cos finit $\mathbb{F}_q$.*

1. *E és ordinària si, i només si,* $\mathrm{End}^0(E) \cong \mathbb{Q}(\sqrt{D}),\ D < 0$.
2. *E és supersingular si, i només si,* $\mathrm{End}^0(E) \cong \mathbb{Q}(\alpha, \beta),\ \alpha^2, \beta^2 < 0,\ \alpha\beta = -\beta\alpha$.

3.4 El número d'invariants j supersingulars

El Teorema 3.20 ens diu que tot invariant j supersingular sobre un cos de característica $p > 0$ es troba en $\mathbb{F}_{p^2}$. Així, sabem que hi ha –com a molt– p^2 classes d'isomorfisme de corbes el·líptiques supersingulars. Però encara no hem vist cap exemple d'una tal corba, ni sabem quants elements de $\mathbb{F}_{p^2}$ són invariants j supersingulars.

En aquesta secció donarem una resposta a aquestes qüestions. El resultat principal es pot resumir dient que, en un cos K de característica $p > 0$, hi ha aproximadament $p/12$ invariants j supersingulars.

Definició 3.30. *Sigui $\lambda \in \bar{K} \setminus \{0, 1\}$. Definim l'equació de Legendre amb paràmetre λ com*

$$y^2 = x(x-1)(x-\lambda).$$

Lema 3.31. *Sigui E una corba el·líptica en forma de Weierstrass $y^2 = x^3 + Ax + B = (x-e_1)(x-e_2)(x-e_3)$, amb $e_i \in \bar{K}$. Siguin*

$$x_1 = (e_2 - e_1)^{-1}(x - e_1),\ y_1 = (e_2 - e_1)^{-3/2} y,\ \lambda = \frac{e_3 - e_1}{e_2 - e_1}.$$

Llavors $\lambda \neq 0, 1$, i $y_1^2 = x_1(x_1 - 1)(x_1 - \lambda)$.

Demostració. Sabem que $\lambda \neq 0, 1$ ja que E és no singular i $e_i \neq e_j$ per a $i \neq j$. L'equació es pot obtenir per càlcul directe, utilitzant $y = (e_2 - e_1)^{3/2} y_1$ i $x = x_1(e_2 - e_1) + e_1$:

$$\begin{aligned} &\Big((e_2 - e_1)^{3/2} y_1\Big) = (x_1(e_2 - e_1))(x_1(e_2 - e_1) + e_1 - e_2)(x_1(e_2 - e_1) + e_1 - e_3) \\ \implies &(e_2 - e_1)^3 y_1^2 = (e_2 - e_1)^3 x_1(x_1 - 1)(x_1 - \lambda). \end{aligned}$$

□

Recíprocament, en una equació de Legendre podem prendre el polinomi $x^3 - (\lambda+1)x^2 + \lambda x$, fer-li el canvi de variable $x \mapsto x + \frac{\lambda+1}{3}$, i obtenir una equació de Weierstrass. Per tant tenim una bijecció entre equacions de Weierstrass i equacions de Legendre (com sempre, demanem que siguin no singulars).

Es pot calcular que l'invariant j de la corba $y^2 = x(x-1)(x-\lambda)$ és

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (1-\lambda)^2}.$$

Notem que aquesta expressió roman invariant per les transformacions $\lambda \mapsto 1/\lambda$, $\lambda \mapsto 1 - \lambda$. Per tant, cada paràmetre del conjunt

$$\left\{\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}\right\} \tag{6}$$

defineix una equació de Legendre amb el mateix invariant j. Considerem el polinomi $p_j(\lambda) = 2^8(\lambda^2 - \lambda + 1)^3 - j\lambda^2(1-\lambda)^2$. En el cas $j = 0$, els paràmetres λ corresponents són les dues arrels de $\lambda^2 - \lambda + 1$. El cas $j = 1728$ correspon a $\lambda = -1, 2, 1/2$.

Si $j \neq 0, 1728$, podem igualar dos a dos els elements de (6) per veure que tots són diferents. Com que p_j té grau 6, el conjunt conté tots els paràmetres amb aquest invariant j.

A continuació estudiarem per a quins valors de λ tenim una corba supersingular.

Lema 3.32. *Sigui $i > 0$ un enter. Llavors*

$$\sum_{x\in\mathbb{F}_q} x^i = \begin{cases} 0, & \text{si } q-1 \nmid i \\ -1, & \text{si } q-1 \mid i. \end{cases}$$

Demostració. Si $q-1 \mid i$ llavors $x^i = 1$ per a tot $x \in \mathbb{F}_q^\times$, i la suma val $q-1 = -1$ (en $\mathbb{F}_q$). Si $q-1 \nmid i$, sigui g un generador del grup cíclic $\mathbb{F}_q^\times$. Llavors

$$\sum_{x\in\mathbb{F}_q} x^i = 0 + \sum_{j=0}^{g-2} (g^j)^i = \sum_{j=0}^{g-2} (g^i)^j = \frac{(g^i)^{q-1}-1}{g^i-1} = 0.$$

□

Lema 3.33. *Sigui $f(x) = x^3 + c_2x^2 + c_1x + c_0$ un polinomi amb coeficients en un cos de característica $p > 0$. Per cada $r \geq 1$, sigui A_{p^r} el coeficient de x^{p^r-1} en $f(x)^{\frac{p^r-1}{2}}$. Llavors*

$$A_{p^r} = A_p^{1+p+p^2+\cdots+p^{r-1}}.$$

Demostració. Fem inducció sobre r. Si $r = 1$ el resultat és immediat. Per fer el pas inductiu, observem la igualtat $\frac{p^{r+1}-1}{2} = \frac{p^r-1}{2} + \frac{p^{r+1}-p^r}{2}$. Tenim

$$\begin{aligned} \left(f(x)^{\frac{p-1}{2}}\right)^{p^r} &= \left(x^{3\frac{p-1}{2}} + \cdots + A_p x^{p-1} + \cdots\right)^{p^r} \\ &= \left(x^{3\frac{(p-1)p^r}{2}} + \cdots + A_p^{p^r} x^{(p-1)p^r} + \cdots\right). \end{aligned}$$

Per tant

$$f(x)^{\frac{p^{r+1}-1}{2}} = f(x)^{\frac{p^r-1}{2}} \left(f(x)^{\frac{p-1}{2}}\right)^{p^r} \tag{7}$$

$$= \left(x^{3\frac{p-1}{2}} + \cdots + A_p x^{p-1} + \cdots\right) \cdot \left(x^{3\frac{(p-1)p^r}{2}} + \cdots + A_p^{p^r} x^{(p-1)p^r} + \cdots\right). \tag{8}$$

Per obtenir el coeficient de $x^{p^{r+1}-1}$, prenem índexos i, j tals que $i + j = p^{r+1} - 1$, multipliquem els coeficients corresponents del primer i el segon polinomi, i en fem la suma. Com que $0 \geq i \geq 3\frac{p^r-1}{2}$, llavors ens cal

$$p^{r+1} - 1 \geq j \geq (p^{r+1}-1) - \frac{3}{2}(p^r-1) \geq (p-2)p^r.$$

Com que tots els exponents del segon factor de (7) són múltiples de p^r, l'única j possible en el rang $[p^r(p-1), p^{r+1}-1]$ és $j = p^r(p-1)$, corresponent a $i = p^r - 1$. Per tant tenim

$$A_{p^{r+1}} = A_{p^r} A_p^{p^r}.$$

□

Lema 3.34. *Definim el símbol de Legendre en $\mathbb{F}_q$, $\left(\frac{\cdot}{F_q}\right) : \mathbb{F}_q^\times \to \{\pm 1\}$, de manera que $(x/\mathbb{F}_q) = 1$ si, i només si, x és un quadrat a $\mathbb{F}_q^\times$. A més, definim $(0/\mathbb{F}_q) = 0$.*

Sigui $E\colon y^2 = f(x)$ una corba el·líptica definida sobre el cos finit $\mathbb{F}_q$, amb f un polinomi de grau 3. Llavors

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{f(x)}{\mathbb{F}_q}\right) = q + 1 + \sum_{x\in\mathbb{F}_q} f(x)^{\frac{q-1}{2}}.$$

Demostració. Com que $1 + (f(x_0)/\mathbb{F}_q)$ ens diu el nombre d'arrels quadrades de $f(x_0)$ en F_q, i per tant el nombre de punts afins amb coordenada x_0, tenim

$$\#E(\mathbb{F}_q) = 1 + \sum_{x\in\mathbb{F}_q} \left(1 + \left(\frac{f(x)}{\mathbb{F}_q}\right)\right) = q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{f(x)}{\mathbb{F}_q}\right).$$

La segona igualtat és anàloga al criteri d'Euler. Observem que si $x \in \mathbb{F}_q^\times$, tenim $x^{q-1} = 1$, i $x^{\frac{q-1}{2}} = \pm 1$. Si $(x/\mathbb{F}_q) = 1$, llavors $x = a^2$, d'on $x^{\frac{q-1}{2}} = (a^2)^{\frac{q-1}{2}} = a^{q-1} = 1$. Ara, tenim $(q-1)/2$ quadrats en $\mathbb{F}_q^\times$ (ja que $a^2 = (-a)^2$ i $a \neq -a$ si $a \neq 0$). Tots els quadrats són arrels del polinomi $x^{\frac{q-1}{2}} - 1$, i per tant els no quadrats no poden ser-ho. Concloem doncs que si $(x/\mathbb{F}_q) = -1$, llavors $x^{\frac{q-1}{2}} = -1$. □

Teorema 3.35. *Sigui p un primer senar. Definim el polinomi*

$$H_p(T) = \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 T^i \in \mathbb{F}_p[T].$$

Donat $\lambda \in \bar{\mathbb{F}}_p$, la corba el·líptica E donada per $y^2 = x(x-1)(x-\lambda)$ és supersingular si i només si $H_p(\lambda) = 0$.

Demostració. Sigui $n \geq 1$ tal que $\lambda \in \mathbb{F}_{p^n}$ i E estigui definida sobre $\mathbb{F}_q$, $q = p^n$. Per determinar si E és supersingular, és suficient comptar-ne els punts sobre $E(\mathbb{F}_q)$. Tenim

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x\in\mathbb{F}_q} (x(x-1)(x-\lambda))^{(q-1)/2},$$

on els enters de la fórmula corresponen a elements de $\mathbb{F}_p \subseteq \mathbb{F}_q$. Expandint $(x(x-1)(x-\lambda))^{(q-1)/2}$, obtenim un polinomi de grau $3(q-1)/2$ sense terme independent. Per tant l'únic terme x^i amb $q-1 \mid i$ és x^{q-1}. Si A_q és el coeficient de x^{q-1}, aplicant el lema anterior

$$\sum_{x\in\mathbb{F}_q} (x(x-1)(x-\lambda))^{(q-1)/2} = -A_q.$$

Per tant, en $\mathbb{F}_q$, $\#E(\mathbb{F}_q) = 1 - A_q$. Per tant E és supersingular si, i només si, $A_q = 0$ en $\mathbb{F}_q$ (i per tant mòdul p). Pel Lema 3.33, E és supersingular si, i només si, $A_p = 0$. Ens queda doncs expressar A_p com a polinomi en λ.

El coeficient A_p de x^{p-1} en $(x(x-1)(x-\lambda))^{(p-1)/2}$ és el coeficient de $x^{(p-1)/2}$ en $((x-1)(x-\lambda))^{(p-1)/2}$. Desenvolupant les expressions,

$$(x-1)^{(p-1)/2} = \sum_i \binom{(p-1)/2}{i} x^i (-1)^{(p-1)/2-i},$$
$$(x-\lambda)^{(p-1)/2} = \sum_j \binom{(p-1)/2}{j} x^{(p-1)/2} (-\lambda)^j.$$

Per tant, el coeficient A_p buscat és

$$(-1)^{(p-1)/2} \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 \lambda^k = (-1)^{(p-1)/2} H_p(\lambda),$$

i E és supersingular si, i només si, $H_p(\lambda) = 0$. □

Hem acotat el nombre d'invariants j supersingulars per $(p-1)/2$, tot i que sabem que alguns paràmetres λ correspondran al mateix invariant. Abans de donar el resultat final, utilitzarem la tècnica de la demostració anterior per veure quan les corbes amb $j = 0, 1728$ són supersingulars.

Proposició 3.36. *Sigui $p \geq 5$ un primer. La corba el·líptica $y^2 = x^3 + 1$ sobre $\mathbb{F}_p$ és supersingular si, i només si, $p \equiv 2 \mod 3$, i la corba el·líptica $y^2 = x^3 + x$ sobre $\mathbb{F}_p$ és supersingular si, i només si, $p \equiv 3 \mod 4$.*

Demostració. Com que tots els exponents de $(x^3+1)^{(p-1)/2}$ són múltiples de 3, si $p \equiv 2 \mod 3$ el coeficient de x^{p-1} serà zero. En canvi, si $p \equiv 1 \mod 3$, el coeficient serà $\binom{(p-1)/2}{(p-1)/3} \not\equiv 0 \mod p$.

Veiem la segona corba. Com que $(x^3+x)^{(p-1)/2} = x^{(p-1)/2}(x^2+1)^{(p-1)/2}$, el coeficient de x^{p-1} en $(x^3+x)^{(p-1)/2}$ és el coeficient de $x^{(p-1)/2}$ en $(x^2+1)^{(p-1)/2}$. Tots els exponents en aquest darrer polinomi són parells, de manera que $x^{(p-1)/2}$ no apareix si $p \equiv 3 \mod 4$. Si $p \equiv 1 \mod 4$, el coeficient és $\binom{(p-1)/2}{(p-1)/4} \not\equiv 0 \mod p$. □

Lema 3.37. *$H_p(T)$ té $(p-1)/2$ arrels diferents en $\bar{\mathbb{F}}_p$.*

Demostració. Veure [Was08, proposició 4.38] □

Teorema 3.38. *Sigui $p \geq 5$ un nombre primer. El nombre de $j_0 \in \bar{\mathbb{F}}_p$ que són invariants j supersingulars és*

$$\left[\frac{p}{12}\right] + \varepsilon_p,$$

on $\varepsilon_p = 0, 1, 1, 2$ si $p \equiv 1, 5, 7, 11 \mod 12$, respectivament.

Demostració. Donat un invariant j, posem $\varepsilon_p(j)$ igual a 1 o 0 segons si j és supersingular o no. Llavors el nombre d'invariants supersingulars és

$$\frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728)\right) + \varepsilon_p(0) + \varepsilon_p(1728) = \frac{p-1}{12} + \frac{2}{3}\varepsilon_p(0) + \frac{1}{2}\varepsilon_p(1728).$$

Combinant les quatre possibilitats per a p mòdul 12 amb la Proposició 3.36 obtenim el resultat. □

4 Supersingular Isogeny Diffie-Hellman

En aquesta secció estudiem el sistema d'intercanvi de claus Supersingular Isogeny Diffie-Hellman (SIDH), presentat per David Jao i Luca De Feo a [FJP11].

Al llarg de tota la secció, hem de tenir present el concepte de *graf d'isogènies supersingulars*. Donat un primer p i un conjunt $L \subset \mathbb{Z}$ finit, definim el graf $\mathcal{G}(p, L) = \{V, E\}$, on el conjunt de vèrtexs $V \subset \mathbb{F}_{p^2}$ està format pels invariants j supersingulars en $\bar{\mathbb{F}}_p$, i el conjunt d'arestes E està format per les isogènies amb grau $d \in L$ entre corbes supersingulars mòdul isomorfisme. Notem que aquest graf és no dirigit, ja que per tota isogènia $\phi\colon E_1 \to E_2$ de grau $d \in L$, la seva dual $\hat{\phi}\colon E_2 \to E_1$ també té grau d. A l'Annex D es poden trobar algunes visualitzacions de tals grafs.

4.1 Intercanvi de claus

Siguin ℓ_A i ℓ_B dos primers (petits, per exemple 2 i 3), i sigui p un primer de la forma $\ell_A^{e_A}\ell_B^{e_B} f \pm 1$, on e_A, e_B i f són enters positius. Suposarem que tenim una corba E_0 definida sobre $\mathbb{F}_q = \mathbb{F}_{p^2}$ d'ordre $(\ell_A^{e_A}\ell_B^{e_B} f)^2$. Notem que E_0 és supersingular. En efecte, pel Teorema de Hasse l'ordre de $E_0(\mathbb{F}_q)$ és $q + 1 - t$, amb $t = \operatorname{tr} \pi_E$, i tenim

$$t = (\ell_A^{e_A}\ell_B^{e_B} f \pm 1)^2 + 1 - (\ell_A^{e_A}\ell_B^{e_B} f)^2 = \pm 2\ell_A^{e_A}\ell_B^{e_B} f + 2 = \pm 2p \equiv 0 \mod p.$$

Lema 4.1. *Sigui E una corba el·líptica sobre $\mathbb{F}_q$. Suposem que π_E pertany a $\mathbb{Z}$, i sigui $n \geq 1$ tal que $n^2 \mid \#E(\mathbb{F}_q) = q + 1 - t$. Llavors $E[n] \subset E(\mathbb{F}_q)$.*

Demostració. Com que π_E és un enter, tenim $\hat{\pi}_E = \pi_E$, de manera que $t = \operatorname{tr} \pi_E = 2\pi_E$, i $\hat{\pi}_E \pi_E = \pi_E^2 = q$. D'aquí, $(\pi_E - 1)^2 = q - 2\pi_E + 1 = q - t + 1$. Per tant $n \mid \pi_E - 1$ i $\frac{\pi_E - 1}{n} \in \mathbb{Z}$. Ara, si P és un punt d'n-torsió, llavors $nP = \mathcal{O}$. Però llavors

$$\mathcal{O} = \left(\frac{\pi_E - 1}{n}\right)(nP) = (\pi_E - 1)(P),$$

implicant que $P \in E(\mathbb{F}_q)$. □

Ara, π_{E_0} és una arrel del polinomi $x^2 \mp 2px + p^2 = (x \mp p)^2$, és a dir $\pi_{E_0} = \pm p$. Com que $\ell_A^{2e_A}$ i $\ell_B^{2e_B}$ divideixen $\#E_0(\mathbb{F}_q)$, el lema ens diu que $E_0[\ell_A^{e_A}]$ i $E_0[\ell_B^{e_B}]$ estan definits sobre $\mathbb{F}_q$.

Lema 4.2. *Sigui ℓ un primer i n un enter positiu. El grup $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ té $\ell^{n-1}(\ell + 1)$ subgrups cíclics d'ordre ℓ^n.*

Demostració. Sigui $(a, b) \in \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$. Aquest element té ordre ℓ^n si, i només si, el mínim comú múltiple dels ordres de a i b és ℓ^n. Això és equivalent a que el mínim comú múltiple de $\operatorname{mcd}(\ell^n, a)$ i $\operatorname{mcd}(\ell^n, b)$ sigui ℓ^n, i alhora al fet que a o b sigui coprimer amb ℓ. El nombre de parells d'ordre ℓ^n és doncs

$$\varphi(\ell^n)\ell^n + (\ell^n - \varphi(\ell^n))\varphi(\ell^n) = \varphi(\ell^n)(2\ell^n - \varphi(\ell^n)).$$

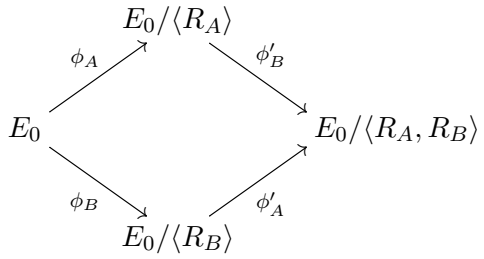
A cada subgrup $\langle (a, b) \rangle$ d'ordre ℓ^n, hi ha $\varphi(\ell^n)$ elements que el generen. Per tant el nombre de subgrups és

$$\frac{1}{\varphi(\ell^n)}\varphi(\ell^n)(2\ell^n - \varphi(\ell^n)) = 2\ell^n - \ell^{n-1}(\ell - 1) = \ell^{n-1}(\ell + 1).$$

□

En resum, a la corba $E_0(\mathbb{F}_q)$ hi tenim els subgrups $E_0[\ell_A^{e_A}]$ i $E_0[\ell_B^{e_B}]$, que contenen ${\ell_A^{e_A}}^{-1}(\ell_A+1)$ (resp. ${\ell_B^{e_B}}^{-1}(\ell_B+1)$) subgrups d'ordre $\ell_A^{e_A}$ (resp. $\ell_B^{e_B}$). Pel Teorema 2.24, cadascun d'aquests subgrups ens dona una isogènia separable amb domini E_0.

Per fer l'intercanvi de claus, farem que les dues parts puguin computar el següent diagrama d'isogènies, tenint només coneixement d'un dels dos camins.



Fixem com a paràmetres públics de l'esquema d'intercanvi de claus la corba E_0 definida sobre $\mathbb{F}_{p^2}$, i sengles bases $\{P_A, Q_A\}$, $\{P_B, Q_B\}$ de $E_0[\ell_A^{e_A}]$ i $E_0[\ell_A^{e_B}]$ (com a $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ i $\mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ mòduls, respectivament).

Per construir el seu parell de claus, Alice tria dos elements aleatoris m_A, n_A de $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, amb un dels dos coprimer amb ℓ_A, i calcula una isogènia $\phi_A\colon E_0 \to E_A$ amb nucli $\langle m_A P_A + n_A Q_A\rangle$. A més, calcula la imatge $\{\phi_A(P_B), \phi_A(Q_B)\} \subset E_A$ de la base de $E_0[\ell_B^{e_B}]$, i envia aquests punts a Bob juntament amb E_A.

Similarment, Bob selecciona m_B, n_B de $\mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ aleatoris i calcula una isogènia $\phi_B\colon E_0 \to E_B$ amb nucli $\langle m_B P_B + n_B Q_B\rangle$, juntament amb els punts $\{\phi_B(P_A), \phi_B(Q_A)\} \subset E_B$.

Havent rebut E_B, $\phi_B(P_A)$ i $\phi_B(Q_A)$, Alice calcula una isogènia $\phi'_A\colon E_B \to E_{AB}$ amb nucli $\langle m_A\phi_B(P_A) + n_A\phi_B(Q_A)\rangle$. Bob fa el procés simètric, tot calculant $\phi'_B\colon E_A \to E_{AB}$.

Aleshores, Alice i Bob poden utilitzar l'invariant j de la corba

$$E_{AB} \cong \phi'_B(\phi_A(E_0)) \cong \phi'_A(\phi_B(E_0)) \cong E_0/\langle m_A P_A + n_A Q_A, m_B P_B + n_B Q_B\rangle$$

per formar una clau secreta compartida.

A l'Annex D.1 es pot trobar una visualització del protocol SIDH sobre el graf d'isogènies amb $p = 863$.

4.2 Consideracions pràctiques i implementació

La primera qüestió que ens apareix per posar en pràctica el protocol que hem especificat és la generació de paràmetres. És a dir, triar (si és possible) ℓ_A, ℓ_B, e_A, e_B, f, p i E_0 de manera que es compleixin totes les hipòtesis, especialment el fet que $\#E_0(\mathbb{F}_{p^2}) = (\ell_A^{e_A}\ell_B^{e_B} f)^2$.

Seguint les implementacions de referència del protocol, prendrem $\ell_A = 2$, $\ell_B = 3$ i $f = 1$. A més, farem que el primer p sigui de la forma $2^{e_A}3^{e_B} - 1$, amb $2^{e_A} \approx 3^{e_B}$. Un tal primer existeix, pel Teorema de Dirichlet sobre primers en progressions aritmètiques. D'aquesta manera aconseguim $p \equiv 11 \mod 12$. Per la Proposició 3.36, sabem que les corbes $y^2 = x^3 + 1$ i $y^2 = x^3 + x$ seran supersingulars, de manera que tenim candidats per intentar cercar una corba amb l'ordre que necessitem.

Lema 4.3. *Sigui E una corba el·líptica sobre $\mathbb{F}_q$, amb ordre $\#E(\mathbb{F}_q) = q + 1 - t$, on $t = \operatorname{tr}\pi_E$. Posem $X^2 - tX + q = (X - \alpha)(X - \beta)$. Llavors*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),$$

per a tot $n \geq 1$.

Demostració. Notem que $\alpha^n + \beta^n$ és enter, ja que α i β són enters algebraics (arrels d'un polinomi mònic amb coeficients enters) i $\alpha^n + \beta^n$ és racional (ja que és fix pel grup de Galois de $\mathbb{Q}(\alpha)/\mathbb{Q}$).

Sigui $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n$. Llavors $X^2 - tX + q = (X - \alpha)(X - \beta)$ divideix $f(X)$, de manera que existeix un polinomi $Q(x)$ amb coeficients enters tal que $f(X) = Q(X)(X^2 - tX + q)$. Avaluant en π_q,

$$(\pi_q^n)^2 - (\alpha^n + \beta^n)\pi_q^n + q^n = f(\pi_q) = Q(\pi_q)(\pi_q^2 - t\pi_q + q) = 0.$$

Com que $\pi_q^n = \pi_{q^n}$, el polinomi $X^2 - (\alpha^n + \beta^n)X + q^n$ té per arrel π_{q^n}, de manera que $\alpha^n + \beta^n = \operatorname{tr} \pi_{q^n}$, i obtenim el resultat. □

Si prenem com a corba inicial la corba $E_0 \colon y^2 = x^3 + x$, la Proposició 3.22 ens diu que E_0 té exactament $p + 1$ punts sobre $\mathbb{F}_p$, i el Frobenius π_p és arrel del polinomi $X^2 + p$. Amb la notació del lema, tenim $\alpha, \beta = \pm\sqrt{-p}$. Per tant el Frobenius π_{p^2} tindrà traça $-2p$, i per tant la corba E_0 tindrà cardinal sobre $\mathbb{F}_{p^2}$

$$\#E_0(\mathbb{F}_{p^2}) = p^2 + 1 - (-2p) = p^2 + 1 + 2p = (p + 1)^2.$$

Observació 4.4. *El raonament que acabem de fer és vàlid per a qualsevol invariant j supersingular que estigui en $\mathbb{F}_p$. Això ens justifica la tria de p: si fos de la forma $2^{e_A}3^{e_B}+1$, les corbes amb invariants j pertanyents a $\mathbb{F}_p$ tindrien $(p + 1)^2 \neq (2^{e_A}3^{e_B})^2$ punts sobre $\mathbb{F}_{p^2}$, i hauríem de cercar invariants j supersingulars per a E_0 en $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Si volem emprar primers ℓ_A i ℓ_B diferents de 2 i 3, la corba E_0 serà supersingular amb $(p + 1)^2$ punts si posem f igual a un múltiple de 12.*

El següent que hem de considerar és la manera de fer l'intercanvi de claus de forma eficient. Els dos passos crítics són el producte d'un punt per un enter, i el càlcul d'*isogènies cícliques* (és a dir, amb nucli generat per un únic punt).

El producte d'un punt P de E_0 per un enter es pot calcular amb un algoritme anàleg al d'exponenciació binària en aritmètica modular. Si volem calcular $[n]P$, llavors necessitarem $O(\log_2 n)$ sumes de punts, i alhora podem considerar que aquestes tenen un cost constant.

Per al càlcul d'una isogènia separable amb nucli $H \subset E$ utilitzarem les fórmules de Vélu, que hem enunciat als Teoremes 2.26 i 2.27. A la vista de les fórmules, podem afirmar que una avaluació d'un punt per la isogènia $\phi \colon E \to E/H$ té un cost $O(|H|) = O(\deg \phi)$ (tant en operacions en $\mathbb{F}_{p^2}$ com en espai: necessitem disposar del grup sencer). En el nostre cas volem calcular una isogènia $\phi \colon E \to E/\langle R \rangle$ de grau ℓ^e, així que no podem aplicar directament les fórmules per la complexitat exponencial en e que això suposaria.

L'aproximació que utilitzarem per evitar aquesta complexitat es basa en la descomposició de la isogènia ϕ, de grau ℓ^e, en e isogènies de grau ℓ. En efecte, sigui $E_0 = E$, $R_0 = R$, i per a $0 \leq i < e$ sigui

$$E_{i+1} = E_i/\langle \ell^{e-i-1} R_i \rangle, \quad \phi_i \colon E_i \to E_{i+1}, \quad R_{i+1} = \phi_i(R_i).$$

Llavors $E/\langle R \rangle = E_e$ i $\phi = \phi_{e-1} \circ \cdots \circ \phi_0$. A la primera versió de [FJP11] es donen dos algoritmes que fan aquest càlcul amb complexitat quadràtica respecte de e. En presentem

un, que a l'article citat se li ha donat l'adjectiu d'*isogeny-based*. L'algoritme té dues parts: en primer lloc es genera la llista $(\ell^i P)_{1\leq i\leq e-1}$, i després es calculen successivament les isogènies ϕ_i, fent servir la imatge del punt $\ell^{e-i-1}P$ per totes les isogènies ja calculades.

Algoritme 1: Càlcul de la isogènia cíclica $E \to E/\langle P\rangle$

Data: E, P, ℓ, e
Result: $\phi\colon E \to E/\langle P\rangle$
$P_0 \leftarrow P$
for $1 \leq i \leq e-1$ **do**
  $P_i \leftarrow [\ell]P_{i-1}$
end
$\phi \leftarrow id_E$
for $0 \leq i \leq e-1$ **do**
  $\phi_i\colon E_i \to E_i/\langle\phi(P_{e-1-i})\rangle$
  $\phi \leftarrow \phi_i \circ \phi$
end

El pas més costós és el càlcul de la isogènia ϕ_i, amb $O(i\ell)$ operacions. Com que aquest es fa e vegades, es realitzen $e(e+1)/2$ avaluacions d'isogènies de grau ℓ. Per tant, l'algoritme té un cost de $O(\ell e^2)$, quadràtic en l'exponent e. A la segona versió de [FJP11] es donen estratègies computacionals que milloren aquesta complexitat fins a $O(e\log e)$ operacions.

A l'Annex B es pot trobar una taula amb els conjunts de paràmetres proposats a l'especificació del protocol SIDH/SIKE [Jao+19], juntament amb els *benchmarks* oficials i propis realitzats per a cada conjunt de paràmetres.

4.3 Problemes computacionals

Per avaluar la seguretat del protocol definim, com és habitual, els problemes computacionals sobre els quals es basa. Els atacs que provarem per trencar-lo aniran enfocats a resoldre algun d'aquests problemes.

Com abans, ℓ_A i ℓ_B seran dos primers petits, p serà un primer de la forma $\ell_A^{e_A}\ell_B^{e_B} - 1$, E_0 una corba el·líptica supersingular sobre $\mathbb{F}_{p^2}$, i $E_0[\ell_A^{e_A}]$ (respectivament $E_0[\ell_B^{e_B}]$) estan generats per $\{P_A, Q_A\}$ (respectivament $\{P_B, Q_B\}$).

Donem els noms dels problemes en anglès, ja que és útil conèixer-ne les sigles: DSSI, CSSI, SSCDH i SSDDH.

Problema 4.5 (Decisional Supersingular Isogeny (DSSI) problem)**.** *Donada E_A una corba supersingular definida sobre $\mathbb{F}_{p^2}$, decidir si E_A és $\ell_A^{e_A}$-isògena a E_0.*

Problema 4.6 (Computational Supersingular Isogeny (CSSI) problem)**.** *Sigui $\phi_A\colon E_0 \to E_A$ una isogènia amb nucli $\langle m_A P_A + n_A Q_A\rangle$, on m_A, n_A s'escullen aleatòriament en $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ i no són alhora divisibles per ℓ_A. Donades les corbes E_0, E_A i els valors $\phi_A(P_B)$ i $\phi_A(Q_B)$, trobar un generador R_A de $\langle m_A P_A + n_A Q_A\rangle$.*

A [Tes99] es dona un algoritme (anomenat EDL, logaritme discret *estès*) que ens permet trobar (m_A, n_A) a partir del generador R_A.

Problema 4.7 (Supersingular Computational Diffie-Hellman (SSCDH) problem)**.** *Sigui $\phi_A\colon E_0 \to E_A$ una isogènia amb nucli $\langle m_A P_A + n_A Q_A\rangle$, i sigui $\phi_B\colon E_0 \to E_B$ una isogènia*

amb nucli $\langle m_B P_B + n_B Q_B \rangle$*, on* $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$*,* $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ *es trien amb la restricció de divisibilitat habitual. Donades les corbes* E_A, E_B *i els punts* $\phi_A(P_B)$*,* $\phi_A(Q_B)$*,* $\phi_B(P_A)$*,* $\phi_B(Q_A)$*, trobar l'invariant* j *de la corba* $E_0/\langle m_A P_A + n_A Q_A, m_B P_B + n_B Q_B \rangle$*.*

Problema 4.8 (Supersingular Decision Diffie-Hellman (SSDDH) problem)**.** *Donada una tupla triada amb probabilitat* $1/2$ *d'entre les següents distribucions:*

- $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E_{AB})$*, on* E_A*,* E_B*,* $\phi_A(P_B)$*,* $\phi_A(Q_B)$*,* $\phi_B(P_A)$*,* $\phi_B(Q_A)$ *són com al problema SSCDH i*

$$E_{AB} \cong \langle m_A P_A + n_A Q_A, m_B P_B + n_B Q_B \rangle,$$

- $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E_C)$*, on* E_A*,* E_B*,* $\phi_A(P_B)$*,* $\phi_A(Q_B)$*,* $\phi_B(P_A)$*,* $\phi_B(Q_A)$ *són com al problema SSCDH i*

$$E_C \cong \langle m'_A P_A + n'_A Q_A, m'_B P_B + n'_B Q_B \rangle,$$

  on m'_A, n'_A *(resp.* m'_B, n'_B*) estan triats aleatòriament de* $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ *(resp.* $\mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$*) i no són tots dos múltiples de* ℓ_A *(resp.* ℓ_B*),*

determinar de quina distribució s'ha triat la tupla.

Donat un algoritme que resolgui el problema CSSI (resp. SSCDH), és trivial resoldre el problema SSCDH (resp. SSDDH). Donat un algoritme per resoldre el problema DSSI, podem resoldre també el problema SSDDH.

4.4 Criptoanàlisi del SIDH

Veiem a continuació diverses maneres d'analitzar la seguretat del protocol SIDH. La primera és una situació *passiva*: com a atacants, disposem de la clau pública i els punts auxiliars d'un usuari del protocol, però no podem interactuar amb l'usuari. El nostre objectiu és trobar la clau secreta, és a dir, resoldre el problema CSSI.

La segona situació és *activa*, ja que permetem la interacció amb l'usuari per intentar deduir la seva clau. En aquesta situació, suposarem que l'usuari atacat reutilitza la clau cada vegada (en cas contrari, encara que obtinguem informació parcial sobre una clau secreta, aquesta haurà canviat a la propera execució del protocol), però com a analistes no tenim per què utilitzar sempre la mateixa.

Finalment, veurem la seguretat quàntica del protocol i comentarem breument la relació del protocol amb el càlcul d'anells d'endomorfismes de corbes el·líptiques.

4.4.1 Atacs passius

Podem suposar que estem atacant la clau d'Alice i fixar $\ell = \ell_A$ i $e = e_A$. Recordem que les claus privades de l'esquema SIDH són parells $(m, n) \in \mathbb{Z}/\ell^e\mathbb{Z} \times \mathbb{Z}/\ell^e\mathbb{Z}$, amb m o n coprimers amb ℓ. Donada una base $\{P, Q\}$ de $E_0[\ell^e]$, podem identificar (m, n) amb un subgrup d'ordre ℓ^e, $\langle mP + nQ \rangle$. Com que només necessitem tenir-ne un generador, podem fer el següent: si $\ell \nmid m$, podem multiplicar el generador per m^{-1} i obtenir la clau $(1, m^{-1}n)$. Similarment, si $\ell \nmid n$ la clau serà $(n^{-1}m, 1)$. Així doncs, un conjunt de representants de les $\ell^{e-1}(\ell + 1) = \ell^e + \ell^{e-1}$ claus possibles és

$$\mathcal{K}_{\ell^e} = \{(1, n) \mid 0 \leq n < \ell^e\} \cup \{(\ell m', 1) \mid 0 \leq m' < \ell^{e-1}\}.$$

El nostre objectiu és trobar una isogènia cíclica de grau ℓ^e entre E_0 i E_A, de manera que podem provar les $\ell^{e-1}(\ell+1)$ possibilitats de forma aleatòria fins a trobar la clau privada. Això ens dona un atac de força bruta per al qual necessitem $O(\ell^e) = O(\sqrt{p})$ avaluacions d'isogènies cícliques, que podem realitzar amb els algoritmes comentats.

Problema 4.9. *Donades dues funcions $f\colon A \to C$ i $g\colon B \to C$, trobar un parell (a, b) tal que $f(a) = g(b)$ es coneix com el problema de la col·lisió (o també claw problem). Podem resoldre el problema en $O(|A| + |B|)$ avaluacions de f i g i espai $O(|A|)$, construint una taula hash amb $f(a)$ per a tot $a \in A$, i després cercant coincidències de $g(b)$ per a tot $b \in B$.*

Podem aprofitar aquest model per millorar l'atac de força bruta. En primer lloc, construïm totes les isogènies de grau $\ell^{\lceil e/2 \rceil}$ des de la corba E_0, i guardem l'invariant j de cada corba imatge. Després fem una exploració des de la corba E_A. Comprovant col·lisions amb la taula hash construïda, arribarem a trobar una corba $\tilde{E}$ intermèdia, juntament amb isogènies $\psi_1\colon E_0 \to \tilde{E}$ i $\hat{\psi}_2\colon E_A \to \tilde{E}$.[6] Si la isogènia $\psi_2 \circ \psi_1$ fos cíclica, el seu nucli ens donaria la clau privada, obtenint un atac en $O(\ell^{e/2}) = O(\sqrt[4]{p})$ avaluacions d'isogènies. A l'Annex D.2 hi trobem una visualització d'aquest l'algoritme.

Fixem la següent notació: donat l'exponent e, f i c seran enters positius tals que $e = f + c$ i $f \leq c$. Per exemple, podem prendre $f = \lfloor \frac{e}{2} \rfloor$ i $c = \lceil \frac{e}{2} \rceil$.

Algoritme 2: Esquema de l'algoritme *claw-finding*.

```
j-invariants ← dict()
for j ∈ {j(E') | ψ1: E0 → E' ℓ^f-isogènia cíclica} do
    Guardar j a j-invariants.
end
for j ∈ {j(E') | ψ̂2: EA → E' ℓ^c-isogènia cíclica} do
    if j = j(Ẽ) ∈ j-invariants then
        Trobar el nucli de E0 → Ẽ → EA.
    end
end
```

Sabem que la isogènia secreta ϕ_A és cíclica. La podem escriure com a 4.2, $\phi_A = \phi_{e-1} \circ \cdots \circ \phi_0$ amb cada ϕ_i una isogènia de grau ℓ. Posem $\psi_1 = \phi_{f-1} \circ \cdots \circ \phi_0$ i $\psi_2 = \phi_{e-1} \circ \cdots \circ \phi_f$, de manera que estem en la situació de l'atac. El següent lema ens diu que $\hat{\psi}_2$ és cíclica, cosa que ens facilitarà els càlculs.

Lema 4.10. *Sigui $\psi\colon E \to E/\langle R \rangle$ una ℓ^c-isogènia cíclica, amb $R \in E[\ell^c]$. Aleshores, la isogènia dual $\hat{\psi}$ també és cíclica. Més concretament, si $E[\ell^c] = \langle P, Q \rangle$ i $R = P + \alpha Q$, aleshores* $\ker \hat{\psi} = \langle \psi(Q) \rangle$.

Demostració. Tenim $\hat{\psi} \circ \psi = [\ell^c]$. Així doncs, el nucli de $\hat{\psi}$ està generat per $\psi(P)$ i $\psi(Q)$. Però $\psi(P) = \psi(P - R) = \psi(-\alpha Q) = -\alpha\psi(Q)$, de manera que $\ker \hat{\psi} = \langle \psi(P), \psi(Q) \rangle = \langle \psi(Q) \rangle$. □

[6] La corba imatge de ψ_1 i la corba domini de ψ_2 són isomorfes, però no són necessàriament iguals. Tot i així, podem suposar que ho són, composant ψ_1 amb un isomorfisme adequat.

Amb aquesta informació podem donar mètodes per explorar isogènies des de E_0 i E_A i per calcular el nucli de $\psi_2 \circ \psi_1$. Els dos bucles de l'Algoritme 2 tenen la mateixa estructura, ja que es basen en generar isogènies de grau una potència de ℓ des de les corbes E_0 i E_A. Per simplificar la discussió de la generació de les isogènies, fixarem la corba inicial E_0 i grau ℓ^f. Els mètodes funcionen de la mateixa manera per al cas de la corba inicial E_A i grau ℓ^c.

El primer mètode l'anomenarem exploració per parells o exploració MN. Consisteix en fixar una base $\{P, Q\}$ de $E_0[\ell^f]$, generar tots els parells $(m, n) \in \mathcal{K}_{\ell^f}$, i calcular successivament les isogènies $E_0 \to E_0/\langle mP + nQ\rangle$. Aquest mètode ens facilitarà també el càlcul del nucli: si prenem dos parells $(1, n), (1, n') \in \mathcal{K}_{\ell^e}$ (el cas $(m, 1)$ és simètric), tindrem $\ell^c(1, n) \equiv \ell^c(1, n') \mod \ell^e$ si, i només si, $\ell^c(n - n') \equiv 0 \mod \ell^e$. Això és equivalent a que $\ell^f \mid n - n'$, és a dir, $n \equiv n' \mod \ell^f$. Per tant, un cop trobades la corba intermèdia i les isogènies ψ_1 i ψ_2, podem emprar el parell (m, n) associat a ψ_1 per buscar el nucli.

Algoritme 3: Exploració MN. La funció `explorar` correspon a guardar els objectes generats en un diccionari o comprovar si es troben en el diccionari ja generat.

Data: E_0, $\{P, Q\}$, ℓ, f
for $(m, n) \in \mathcal{K}_{\ell^f}$ **do**
  $R \leftarrow mP + nQ$
  Calcular $\phi\colon E_0 \to E_0/\langle R\rangle$
  $j \leftarrow j(E_0/\langle R\rangle)$
  `explorar`(ϕ, j, (m, n))
end

Amb aquesta estratègia, el càlcul més costós és el de la isogènia ϕ, que ja hem vist que es pot realitzar amb $O(\ell f \log f)$ operacions en el cos finit. Aquest càlcul es fa $\ell^{f-1}(\ell + 1)$ vegades: és raonable suposar que hi ha una certa quantitat d'ℓ-isogènies intermèdies que es calculen més d'una vegada. Per tant, una exploració del graf d'ℓ-isogènies "aresta a aresta" ens pot estalviar alguns càlculs.

Farem una exploració de tipus *depth-first search* (DFS) amb profunditat limitada d. Aquesta exploració ens convé més que una de tipus *breadth-first search*, per exemple, ja que l'estructura necessària per efectuar-la (una pila en comptes d'una cua) emmagatzemarà molts menys nodes intermedis.

Hem de trobar una manera d'associar un parell $(m, n) \in \mathcal{K}_{\ell^f}$ a cada camí en el graf d'isogènies de longitud f. El següent resultat ens diu com fer-ho.

Proposició 4.11. *Sigui $\{P, Q\}$ una base de $E_0[\ell^f]$, i considerem dos parells (m, n), $(m', n') \in \mathcal{K}_{\ell^f}$. Siguin $\phi\colon E_0 \to E$, $\psi\colon E_0 \to E'$ les isogènies obtingudes quocientant E_0 pels subgrups $\langle mP + nQ\rangle$ i $\langle m'P + n'Q\rangle$, respectivament. Descomponem $\phi = \phi_{f-1} \circ \cdots \circ \phi_0$ i $\psi = \psi_{f-1} \circ \cdots \circ \psi_0$ en ℓ-isogènies com a l'Algoritme 1. Si existeix un exponent d amb $1 \leq d \leq f$, tal que $(m, n) \equiv (m', n') \mod \ell^d$, aleshores $\phi_{i-1} \circ \cdots \circ \phi_0 = \psi_{i-1} \circ \cdots \circ \psi_0$ (llevat d'isomorfisme) per a cada $1 \leq i \leq d$.*

Demostració. Sigui i amb $1 \leq i \leq d$, i denotem $\phi' = \phi_{i-1} \circ \cdots \circ \phi_0$ i $\psi' = \psi_{i-1} \circ \cdots \circ \psi_0$. Com s'explica en la discussió de l'esmentat algoritme, els nuclis de ϕ' i ψ' són, respectivament, $\langle \ell^{e-i}(mP_A + nQ_A)\rangle$ i $\langle \ell^{e-i}(m'P_A + n'Q_A)\rangle$. Però per hipòtesi, $(m, n) \equiv (m', n') \mod \ell^i$, que ens implica $\ell^{e-i}(m, n) \equiv \ell^{e-i}(m', n') \mod \ell^e$, de manera que els generadors dels nuclis són iguals. El Teorema 2.24 ens diu que ϕ' i ψ' són iguals llevat d'isomorfisme. □

Fixem una base $\{P, Q\}$ de $E_0[\ell^f]$. Per a cada $(m, n) \in \mathcal{K}_\ell$, calculem la isogènia $\phi\colon E_0 \to E_1 = E_0/\langle \ell^{f-1}(mP + nQ)\rangle$. La inicialització de la pila del recorregut DFS serà una llista de tuples

$$(\phi, (m, n), 1, \phi(P), \phi(Q)),$$

amb un total de $\ell + 1$ tuples. El número 1 indica la profunditat de l'exploració, que s'incrementarà cada cop que afegim nodes a la pila. Els punts $\phi(P)$ i $\phi(Q)$ són elements de $E_1[\ell^f]$, que tot i no ser-ne una base necessàriament, són suficients per calcular les següents ℓ-isogènies.

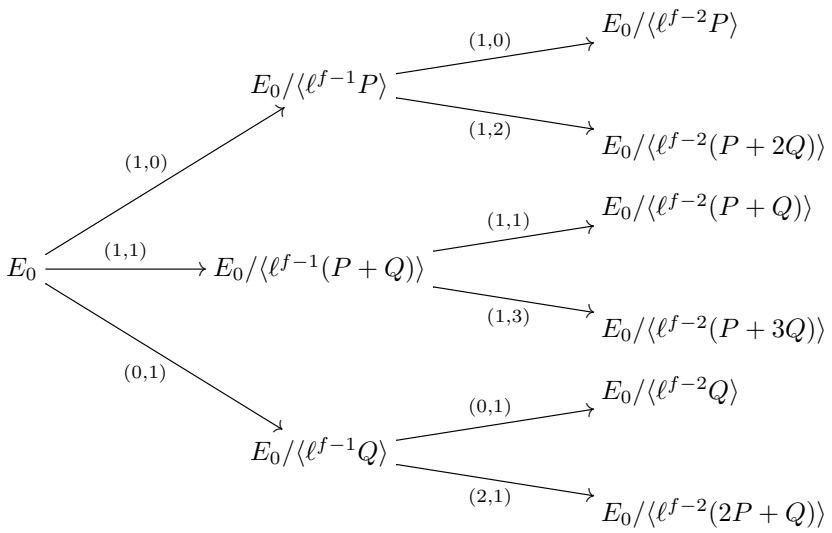


Figura 4.1: Diagrama amb els primers 2 nivells de l'exploració DFS, en el cas $\ell = 2$.

A l'efectuar l'exploració, traurem una tupla $(\phi\colon E_0 \to E_d, (m, n), d, \tilde{P}, \tilde{Q})$ de la pila. Si $d = f$, la isogènia ϕ té grau ℓ^f. En cas contrari, seguirem l'exploració, tot afegint nodes a la pila tal com descrivim a continuació.

El parell (m, n) ens indica que la corba E_d és isomorfa a la corba $E_0/\langle \ell^{f-d}(mP + nQ)\rangle$. Sabem que o bé $m = 1$ o bé $n = 1$, suposem que $m = 1$. Per a cada x en el conjunt $\{0, \ldots, \ell - 1\}$, calcularem $(1, n + \ell^d \cdot x)$, i amb aquest parell, trobarem la isogènia $\psi\colon E_d \to E_{d+1} = E_d/\langle \ell^{f-d-1}(\tilde{P} + (n + \ell^d \cdot x)\tilde{Q})\rangle$. Finalment, afegim a la pila la tupla

$$(\psi \circ \phi\colon E_0 \to E_{d+1}, (1, n + \ell^d \cdot x), d + 1, \psi(\tilde{P}), \psi(\tilde{Q}))$$

En termes de la Proposició 4.11, hem afegit un dígit a l'expansió en base ℓ del parell de $\mathcal{K}_{\ell f}$ que identifica la isogènia. L'exploració realitzada s'il·lustra amb el diagrama de la Figura 4.1.

Amb l'exploració DFS, calculem $(\ell+1)+(\ell+1)\ell+\cdots+(\ell+1)\ell^{f-1} = (\ell+1)\frac{\ell^f-1}{\ell-1} = O(\ell^f)$ isogènies de grau ℓ, de manera que efectuem $O(\ell^{f+1})$ operacions en el cos finit. La complexitat de l'exploració MN era de $O(\ell^{f+1} f \log f)$ operacions, de manera que millorem la complexitat de l'exploració de totes les claus de $\mathcal{K}_{\ell f}$ en un factor de $O(f \log f)$ operacions. Així, hem arribat al mateix resultat (de manera teòrica) que al descrit a [Adj+19]. A l'Annex C es pot trobar una mesura del rendiment de l'atac utilitzant l'exploració MN i DFS, validant aquest resultat teòric.

Algoritme 4: Exploració DFS amb construcció de parells (m, n).

Data: E, $\{P, Q\}$, ℓ, f
stack $\leftarrow$ [ ]
for $(m, n) \in \mathcal{K}_{\ell^f}$ **do**
  Calcular $\phi\colon E \to E/\langle \ell^{f-1}(mP + nQ)\rangle$
  stack.push($(\phi, (m, n), 1, \phi(P), \phi(Q))$)
end
while *not stack.empty()* **do**
  $(\phi\colon E_0 \to E_d, (m, n), d, \tilde{P}, \tilde{Q}) \leftarrow$ stack.pop()
  if $d < f$ **then**
    for $x \in \{0, \ldots, \ell - 1\}$ **do**
      if $m = 1$ **then**
        $n = n + \ell^d \cdot x$
      else
        $m = m + \ell^d \cdot x$
      end
      Calcular $\psi\colon E_d \to E_d/\langle \ell^{f-d-1}(m\tilde{P} + n\tilde{Q})\rangle$
      stack.push($(\psi \circ \phi, (m, n), d + 1, \psi(\tilde{P}), \psi(\tilde{Q}))$)
    end
  else
    `explorar`$(j(E_d), \phi, (m, n))$
  end
end

Un cop trobada la isogènia $\hat{\psi}_2\colon E_A \to \tilde{E}$ associada al parell $(u, v) \in \mathcal{K}_{\ell^c}$, podem calcular ψ_2 mitjançant el Lema 4.10. Podem descartar la col·lisió en cas que les imatges per $\psi_2 \circ \psi_1$ de P_B o Q_B no siguin iguals a $\phi_A(P_B)$ i $\phi_A(Q_B)$.

Només resta el problema de calcular el nucli de $\psi_2 \circ \psi_1$, coneixent el parell $(r, s) \in \mathcal{K}_{\ell^f}$ que determina ψ_1 (suposarem que $r = 1$, el cas $s = 1$ és simètric) i la descomposició de ψ_2 en ℓ-isogènies, $\psi_2 = \phi_{e-1} \circ \cdots \circ \phi_f$. El resoldrem amb un algoritme lineal en c, basat en el fet que el nucli de ϕ_i estarà generat per $\ell^{e-i-1}(\phi_{i-1} \circ \cdots \circ \phi_f \circ \psi_1)(r \cdot P_A + (s + \ell^i x) \cdot Q_A)$ per a un cert $x \in \{0, \cdots, \ell - 1\}$. Així, iterarem sobre x fins a trobar un punt d'aquesta forma tal que la seva imatge per ϕ_i sigui $\mathcal{O}$. Per tant, l'Algoritme 5 té complexitat $O(c\ell)$.

Amb les diferents consideracions, obtenim un algoritme amb complexitat $O(\ell^f + \ell^c) = O(\sqrt[4]{p})$ avaluacions d'isogènies que requereix $O(\ell^f) = O(\sqrt[4]{p})$ unitats de memòria, tal com havíem previst.

Algoritme 5: Càlcul del nucli de $\psi \circ \phi$, suposant que $r = 1$.

Data: $\psi_1 \colon E_0 \to \tilde{E}$, $\psi_2 \colon \tilde{E} \to E_A$, $\phi_{e-1} \circ \cdots \circ \phi_f = \psi_2$, $(r, s) \in \mathcal{K}_{\ell f}$
if $(\psi_2 \circ \psi_1)(P_B) \neq \phi_A(P_B) \parallel (\psi_2 \circ \psi_1)(Q_B) \neq \phi_A(Q_B)$ **then**
  return *None*
end
$P, Q \leftarrow \psi_1(P_A), \psi_1(Q_A)$
$R \leftarrow r \cdot P + s \cdot Q$
for $i \in \{f, \ldots, e-1\}$ **do**
  $R \leftarrow \phi_i(R)$
  $Q \leftarrow \phi_i(Q)$
  $found \leftarrow false$
  $x \leftarrow 0$
  while *not* $found$ **do**
    if $\ell^{e-i-1}(R + \ell^i x \cdot Q) == \mathcal{O}$ **then**
      $found \leftarrow true$
    else
      $x \leftarrow x + 1$
    end
  end
  $s \leftarrow s + \ell^i x$
  $R \leftarrow R + \ell^i x \cdot Q$
end
return $(r, s), r \cdot P_A + s \cdot Q_A$

4.4.2 Atac actiu

En aquesta secció estudiarem l'atac actiu[7] de Galbraith, Petit, Shani i Ti [Gal+16]. Un atac actiu és un tipus estàndard d'atac contra criptosistemes de clau asimètrica en què s'utilitzen claus estàtiques. En el nostre context, suposarem que Alice té una clau fixa (m_A, n_A), i actuarem com a Bob de forma *no honesta* per intentar obtenir informació sobre la clau d'Alice. Necessitarem disposar d'una funció anomenada oracle, que pren com a paràmetres dues corbes E i E' i dos punts R i S de E. Es defineix com

$$O_{(m_A,n_A)}(E, R, S, E') = \begin{cases} 1, \text{ si } j(E') = j(E/\langle m_A R + n_A S \rangle), \\ 0, \text{ altrament.} \end{cases}$$

Aquesta informació serà proporcionada per Alice, quan ens doni un missatge d'error en adonar-se que el seu secret compartit no coincideix amb el de Bob (degut a una verificació com ara un codi MAC, veure [MVO96, §9.5]).

Per simplicitat, suposarem que $\ell_A = 2$, i després ho generalitzarem al cas de primer senar. La clau privada d'Alice és doncs $(m_A, n_A) \in \mathcal{K}_{2^e}$, amb $0 \leq m_A, n_A < 2^e$ i no tots dos divisibles per 2. El primer pas de l'atac consisteix en esbrinar quina paritat tenen m_A i n_A.

Lema 4.12. *Siguin R i S dos punts linealment independents de $E[2^e]$ d'ordre 2^e, i siguin m_A i n_A enters. Llavors n_A és parell si, i només si,*

$$\langle m_A R + n_A(S + 2^{e-1} R) \rangle = \langle m_A R + n_A S \rangle.$$

[7] La denominació en anglès d'aquest atac és *active* i, de vegades, *adaptive*. Aquest segon nom es justifica pel fet que adaptem les interaccions amb l'usuari atac en funció de la informació que ja hem aconseguit.

Demostració. Si n_A és parell, llavors $m_AR+n_A(S+2^{e-1}R) = m_AR+n_AS$. Recíprocament, suposem que els dos grups són iguals. Aleshores existeix $\lambda \in (\mathbb{Z}/2^e\mathbb{Z})^\times$ tal que

$$m_AR + n_A(S + 2^{e-1}R) = \lambda(m_AR + n_AS).$$

Per la independència lineal de R i S podem igualar coeficients, de manera que tenim $m_A + n_A 2^{e-1} \equiv \lambda m_A$ i $n_A \equiv \lambda n_A \mod 2^e$. De la segona igualtat obtenim $\lambda \equiv 1$, i de la primera $n_A 2^{e-1} \equiv 0 \mod 2^e$. Per tant, $2 \mid n_A$. □

Procedim de la següent manera: actuem com a Bob seguint el protocol, tot generant una clau pública vàlida $(E_B, R = \phi_B(P_A), S = \phi_B(Q_A))$ i un secret compartit $j(E_{AB})$. No obstant això, enviem $(E_B, R, S + 2^{e-1}R)$, així que l'oracle ens retornarà

$$n_A \equiv O_{(m_A,n_A)}(E_B, R, S + 2^{e-1}R, E_{AB}) \mod 2.$$

Igualment esbrinarem la paritat de m_A.

Per continuar l'atac, suposarem que la clau privada d'Alice és de la forma $(1, \alpha)$, amb $0 \leq \alpha < \ell^e$ (el cas simètric $(\alpha, 1)$ amb α parell és idèntic). L'expressió binària de α és

$$\alpha = \alpha_0 + 2^1\alpha_1 + \cdots + 2^{e-1}\alpha_{e-1}.$$

A cada consulta de l'oracle, coneixerem un bit més de α. Suposem que ja hem recuperat els primers i bits de α, de manera que $\alpha = K_i + 2^i\alpha_i + 2^{i+1}\alpha'$, on K_i és conegut però $\alpha_i \in \{0, 1\}$ i $\alpha' \in \mathbb{Z}$ són desconeguts.

De nou, generem una clau pública vàlida $(E_B, R = \phi_B(P_A), S = \phi_B(Q_A))$ i un secret compartit $j(E_{AB})$. Per recuperar α_i, triarem enters a_i, b_i, c_i, d_i apropiats i consultarem

$$O_{(m_A,n_A)}(E_B, a_iR + b_iS, c_iR + d_iS, E_{AB}).$$

Els coeficients han de satisfer:

1. Si $\alpha_i = 0$, llavors $\langle (a_i + \alpha c_i)R + (b_i + \alpha d_i)S\rangle = \langle R + \alpha S\rangle$.
2. Si $\alpha_i = 1$, llavors $\langle (a_i + \alpha c_i)R + (b_i + \alpha d_i)S\rangle \neq \langle R + \alpha S\rangle$.
3. $a_iR + b_iS$ i $c_iR + d_iS$ han de tenir ordre 2^e.

És directe comprovar que els coeficients $a_i = 1$, $b_i = -2^{e-i-1}K_i$, $c_i = 0$, $d_i = 1 + 2^{e-i-1}$ satisfan la tercera condició. Per a les altres dues condicions, notem que $\langle a_iR + b_iS + \alpha(c_iR + d_iS)\rangle$ és igual a

$$\begin{aligned}
&\langle R - (2^{e-i-1}K_i)S + \alpha(1 + 2^{e-i-1})S\rangle \\
=&\langle R + \alpha S + (-2^{e-i-1}K_i + 2^{e-i-1}(K_i + 2^i\alpha_i + 2^{i+1}\alpha'))S\rangle \\
=&\langle R + \alpha S + (\alpha_i 2^{e-1})S\rangle \\
=&\begin{cases} \langle R + \alpha S\rangle & \text{si } \alpha_i = 0, \\ \langle R + \alpha S + 2^{e-1}S\rangle & \text{si } \alpha_i = 1. \end{cases}
\end{aligned}$$

Lema 4.13. *Siguin R i S dos punts linealment independents de $E[2^e]$ d'ordre 2^e. Llavors els grups*

$$\langle R + \alpha S + 2^{e-1}S\rangle \text{ i } \langle R + \alpha S\rangle$$

són diferents.

Demostració. Els dos grups tenen ordre 2^e. Si fossin iguals, existiria un $\lambda \in (\mathbb{Z}/2^e\mathbb{Z})^\times$ tal que

$$\lambda R + \lambda\alpha S = R + \alpha S + 2^{e-1}S.$$

Per independència lineal, obtenim que $\lambda = 1$, de manera que $2^{e-1}S = \mathcal{O}$. Però això implicaria que S té ordre un divisor de 2^{e-1}, la qual cosa és una contradicció. Per tant, els dos grups són diferents. □

A [Gal+16] es comenta la possibilitat de detectar l'atac mitjançant el pairing de Weil (veure [Sil09, §III.8]). Tanmateix, aquesta detecció és impossible si multipliquem els coeficients per una certa constant θ, i a més evitem fer les darreres dues consultes a l'oracle. Els dos últims bits es poden trobar provant les quatre possibilitats.

Per fer la generalització al cas que ℓ és un primer senar, escrivim $\alpha = K_i + \ell^i\alpha_i + \ell^{i+1}\alpha'$, amb K_i conegut, i $\alpha_i \in \{0, \ldots, \ell-1\}$ i $\alpha' \in \mathbb{Z}$ desconeguts. Per esbrinar si α_i és igual a un $x \in \{0, \ldots, \ell-1\}$ fixat, emprem els coeficients $a = 1$, $b = -(K_i + \ell^i x)\ell^{e-i-1}$, $c = 0$, $d = 1 + \ell^{e-i-1}$. Llavors el grup $\langle R - (K_i + \ell^i x)\ell^{e-i-1}S + \alpha(1 + \ell^{e-i-1})S\rangle$ és igual a

$$\begin{aligned}&\langle R + \alpha S + (-\ell^{e-i-1}(K_i + \ell^i x) + \ell^{e-i-1}(K_i + \ell^i\alpha_i + \ell^{i+1}\alpha'))S\rangle\\ =&\langle R + \alpha S + \ell^{e-1}(\alpha_i - x)S\rangle.\end{aligned}$$

El següent lema ens dona la informació que volem.

Lema 4.14. *Siguin R i S dos punts linealment independents de $E[\ell^e]$ d'ordre ℓ^e. Amb la notació que acabem de definir, $\alpha_i \equiv x \mod \ell$ si, i només si,*

$$\langle R + \alpha S\rangle = \langle R + \alpha S + \ell^{e-1}(\alpha_i - x)S\rangle.$$

Demostració. Si $\alpha_i \equiv x \mod \ell$, tenim $\ell^{e-1}(\alpha_i - x)S = \mathcal{O}$ i els grups són iguals. Recíprocament, si els grups són iguals existirà $\lambda \in (\mathbb{Z}/\ell^e\mathbb{Z})^\times$ tal que

$$\lambda(R + \alpha S) = R + \alpha S + \ell^{e-1}(\alpha_i - x)S.$$

Per la independència lineal de R i S, obtenim que $\lambda \equiv 1$ i $\ell^{e-1}(\alpha_i - x)S = \mathcal{O}$. Per tant, $\alpha_i \equiv x \mod \ell$. □

Així doncs, en $\ell - 1$ consultes a l'oracle (per a $x \in \{0, \ldots, \ell-2\}$) descobrim l'$i$-èsim coeficient de l'expressió en base ℓ de α. Per al primer coeficient, $i = 0$, emprem els mateixos coeficients que al Lema 4.12, canviant el primer 2 per ℓ.

Si visualitzem les isogènies obtingudes utilitzant el coneixement parcial de la clau K_i, obtenim la visualització de l'Annex D.3. La Proposició 4.11 ens formalitza el que veiem al graf: si $\phi_A = \phi_{e-1} \circ \cdots \circ \phi_0$, el d-èsim bit de la clau ens determina la isogènia ϕ_d, per a $0 \leq d \leq e-1$.

4.4.3 Seguretat quàntica

L'algoritme *claw-finding* que hem emprat és el millor algoritme clàssic de què disposem per trencar una clau en el context passiu (és a dir, sense intervenir cap comunicació). Aquest mètode té una versió per a ordinadors quàntics, introduïda per Tani a [Tan09]. Donades les funcions $f\colon A \to C$, $g\colon B \to C$ com a l'enunciat del Problema 4.9, aquesta versió requereix $O(\sqrt[3]{|A||B|})$ consultes de f i g, essent òptima aquesta complexitat si f i g

són funcions *black-box* (és a dir, no utilitzem cap propietat sobre el càlcul de f i g fora de les seves implementacions). Aplicat al nostre cas, arribaríem a un atac requerint $O(\sqrt[6]{p})$ avaluacions d'isogènies.

No obstant això, semblaria que l'algoritme (també clàssic) per trobar col·lisions de van Oorschot-Wiener (estudiat a [Adj+19] i [Cos+19]) podria ser millor que l'algoritme quàntic de Tani. Aquest mètode es basa en idees similars a les que hem fet servir per al nostre algoritme *claw*, però amb dues particularitats: utilitza menys memòria[8] a canvi d'una complexitat temporal més gran, i es pot paral·lelitzar fàcilment.

4.4.4 Ús de l'anell d'endomorfismes

Sigui E una corba el·líptica definida sobre un cos finit $\mathbb{F}_q$, que de moment no fixarem que sigui ordinària o supersingular. Fixem la notació $O = \mathrm{End}(E)$ i $B = O \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}^0(E)$.

Donat un ideal per l'esquerra[9] no nul $I \subset O$, volem assignar-li una corba E_I i una isogènia $\phi_I \colon E \to E_I$. Si I conté una isogènia separable $\alpha \colon E \to E$, llavors podem definir $E[I] = \{P \in E \mid \beta(P) = \mathcal{O}\ \forall \beta \in I\}$, i assignem la isogènia $\phi_I \colon E \to E_I = E/E[I]$. Si totes les isogènies de I són inseparables, podem escriure $I = P^r I'$, on $P = (\pi_p)$ és l'ideal generat pel p-Frobenius descrit al Lema 3.1, i I' conté una isogènia separable. Aleshores tindrem la isogènia $\phi_I \colon E \to E^{(p^r)} \to E_I$, on $E_I = E^{(p^r)}/E^{(p^r)}[I']$. El següent lema ens diu que la classe d'isomorfisme de E_I no varia si multipliquem l'ideal I per la dreta.

Lema 4.15. *Si $J = I\beta \subset O$ per a un cert $\beta \in B^\times$, llavors $E_I \cong E_J$.*

Demostració. Suposem primer que $\beta \in O$. Llavors $E[I\beta] = \{P \in E \mid \alpha\beta(P) = \mathcal{O}\ \forall \alpha \in I\}$. Afirmem que $\beta E[I\beta] = E[I]$. La inclusió ($\subseteq$) és immediata. Per la inclusió ($\supseteq$), sigui $Q \in E[I]$. Com que la isogènia β és exhaustiva, existeix un punt $P \in E$ tal que $\beta(P) = Q$. Per tant, per a tot $\alpha \in I$, tenim $(\alpha\beta)(P) = \alpha(Q) = \mathcal{O}$ i $P \in E[I\beta]$. Per l'afirmació, podem concloure que $\phi_{I\beta} = \phi_I\beta$ i que $E_{I\beta} \cong E_I$.

En general, existeix un enter m no nul tal que $m\beta$ pertany a O. Pel raonament que acabem de fer, $E_I \cong E_{I(m\beta)} = E_{(I\beta)m} \cong E_{I\beta}$. □

Notem que, en B, l'invers de ϕ_I és $\hat{\phi}_I/N\phi_I$. A l'ideal per l'esquerra I se li pot associar un ordre de B, que anomenem el mòdul per la dreta de I: $O_R(I) := \{r \in B \mid Ir \subseteq I\}$. Aquest mòdul resulta ser isomorf a l'anell d'endomorfismes de la corba E_I.

Lema 4.16. *El morfisme d'anells*

$$\begin{aligned} \iota \colon \mathrm{End}(E_I) &\hookrightarrow B \\ \beta &\mapsto \phi_I^{-1}\beta\phi_I = \frac{1}{\deg \phi_I}(\hat{\phi}_I\beta\phi_I) \end{aligned}$$

és injectiu, i $\iota(End(E_I)) = O_R(I)$.

Demostració. Veure [Voi19, lema 42.2.9]. □

[8] L'ús reduït de memòria s'assoleix fent servir funcions de hash de la mateixa manera que es farien servir en un filtre de Bloom.

[9] Diem que un subgrup I d'un anell O és un ideal per l'esquerra si $la \in I$, per a tot $l \in O$ i $a \in I$.

Hem vist que a cada classe d'ideals per l'esquerra de O li podem assignar una isogènia. La correspondència també funciona en el sentit oposat, com expliquem a continuació. Donat un subgrup finit $H \subset E$, definim $I(H) := \{\alpha \in O \mid \alpha(P) = \mathcal{O}\ \forall P \in H\} \subseteq O$, que és un ideal per l'esquerra de O, no nul ja que l'endomorfisme $[\#H]$ hi pertany. Si $H_1 \subseteq H_2 \subseteq E$ són subgrups finits, aleshores $I(H_1) \supseteq I(H_2)$. Si, a més, $I(H_1) = I(H_2)$, es pot demostrar que $H_1 = H_2$. Similarment, es pot veure que per a tot ideal no nul $I \subset O$, $I(E[I]) = I$. Com a conseqüència, obtenim el següent resultat.

Proposició 4.17. *Donada una isogènia $\phi\colon E \to E'$, existeix un ideal per l'esquerra I de O i un isomorfisme $\rho\colon E_I \to E'$ tal que $\phi = \rho\phi_I$.*

Demostració. Sigui H el nucli de ϕ, i posem $I = I(H)$. Aleshores $H \subseteq E[I(H)]$, i a més, $I(H) = I(E[I(H)])$. Se segueix que $H = E[I]$. Per tant existeix un isomorfisme $\rho\colon E' \to E/E[I] = E_I$, com volíem demostrar. □

Veiem doncs que hi ha una bijecció natural entre isogènies amb domini E_0 (llevat d'isomorfisme), i ideals per l'esquerra en l'anell d'endomorfismes de E_0. En el cas que E_0 sigui ordinària, podem anar més enllà, i demostrar que el grup de classes $\mathrm{Cl}(O)$ (que és finit i abelià) actua de manera fidel i transitiva sobre el conjunt de corbes el·líptiques amb anell d'endomorfismes O. Les propietats d'aquest grup són utilitzades a [CJS14] per resoldre l'anàleg ordinari del problema CSSI en temps subexponencial amb un algoritme quàntic. L'estratègia de l'algoritme depèn fortament de les propietats dels grups abelians, de manera que no és adaptable al cas supersingular, en el qual els ideals de l'anell d'endomorfismes no formen un grup.

El Lema 4.16 ens dona encara una estratègia addicional per trobar isogènies entre dues corbes E_0 i E_A. Si coneixem els anells d'endomorfismes de cada corba, sabem que $\mathrm{End}(\mathrm{E_A})$ és isomorf a un ordre O_A de l'àlgebra d'endomorfismes $\mathrm{End}^0(E_0)$, i que l'ideal I tal que $O_A = O_R(I)$ ens dona una isogènia $E_0 \to E_A$. Per trobar la isogènia de grau ℓ^e apropiada, només caldria escalar I per un element $\beta \in \mathrm{End}^0(E_0)^\times$. Malauradament, aquesta estratègia no és pràctica: els algoritmes coneguts per calcular l'anell d'endomorfismes d'una corba requereixen trobar-ne una isogènia que la connecti amb una corba amb anell conegut, o amb ella mateixa. Ambdós problemes, actualment, es consideren intractables.

4.5 SIKE

No disposem d'un mecanisme que permeti comprovar si una clau pública $(E_B, \phi_B(P_A), \phi_B(Q_A))$ s'ha format correctament. Tal mecanisme podria prevenir l'atac actiu descrit a 4.4.2. Una possibilitat per evitar l'atac és l'ús de claus efímeres, és a dir, imposar que tant Alice com Bob hagin de generar noves claus aleatòries a cada execució del protocol.

Si volem permetre que una de les parts pugui reutilitzar la seva clau, podem aplicar una transformació al protocol SIDH per convertir-lo en el protocol SIKE (Supersingular Isogeny Key Encapsulation). Per descriure-la, utilitzem la següent notació: H i H' són funcions de hash apropiades, $||$ és l'operació de concatenació de bits, i $\oplus$ és l'operació XOR bit a bit ($b_1 \oplus b_2 = 1 \iff b_1 \neq b_2$). Recordem que, donades dues cadenes de bits a i b de la mateixa longitud, es compleix la propietat $a \oplus (a \oplus b) = b$.

Es permet que Alice utilitzi una clau estàtica, de manera que en genera una i publica $PK_A = (E_A, \phi_A(P_B), \phi_A(Q_B))$. Bob genera una clau privada k_B a partir del hash

$H(PK_A||m)$, on m és un valor aleatori.[10] A partir de la seva clau privada i la clau pública d'Alice, Bob calcula el secret compartit j. A continuació, envia la clau pública $PK_B = (E_B, \phi_B(P_A), \phi_B(Q_A))$ a Alice. Addicionalment, li enviarà $H'(j) \oplus m$.

Al rebre $(PK_B, H'(j) \oplus m)$, Alice efectua el protocol SIDH a la seva banda, obtenint un secret compartit j'. Després efectua l'operació $m' = H'(j') \oplus (H'(j) \oplus m)$. Si $j = j'$, aleshores es complirà $m = m'$. A partir del valor m', Alice pot reproduir l'execució del protocol actuant com a Bob i comprovar si aquest ha executat el protocol de forma honesta i enviat els valors correctes de PK_B. Si detectés un ús incorrecte del protocol, Alice pot retornar un error (i Bob no aprendrà res de la clau estàtica).

Notem que, amb aquest esquema, Bob no pot reutilitzar la seva clau, ja que l'està revelant a Alice.

[10] El valor del hash es pot utilitzar per inicialitzar un generador de nombres pseudoaleatoris amb el qual obtenir k_B.

Conclusions

El protocol SIDH/SIKE es presenta com una alternativa postquàntica eficient als sistemes d'intercanvi de claus actuals basats en Diffie-Hellman. Si s'evita la reutilització de claus, SIDH és per ara un criptosistema segur, i els millors atacs per trencar-lo –tant clàssics com quàntics– són exponencials. A més, la modificació introduïda amb SIKE permet que una part reutilitzi la seva clau al llarg del temps, característica desitjable, per exemple, per a l'ús en servidors.

Amb aquest protocol hem introduït els aspectes bàsics de la criptografia basada en isogènies: entre d'altres, el càlcul de corbes quocient mitjançant les fórmules de Vélu, la classificació dels anells d'endomorfismes, i l'assignació de diferents subgrups de torsió d'una corba a elements criptogràfics com ara claus privades. Les eines vistes no només són útils per definir protocols criptogràfics; també són essencials per analitzar-ne la seguretat.

L'anàlisi s'ha concretat en dos atacs: un de passiu, en el qual s'intenta recuperar una clau privada a partir d'una clau pública; i un d'actiu, en què s'executen múltiples interaccions amb la part atacada per recuperar la clau privada progressivament. El primer s'ha desenvolupat a partir d'una observació feta a l'article original de Jao i De Feo [FJP11], en què s'argumentava que el millor atac clàssic requeriria $O(\sqrt[4]{p})$ avaluacions d'isogènies. L'algoritme final, a més de trobar una col·lisió en el graf d'isogènies, aconsegueix la clau privada original en la forma d'un parell d'enters. Hem arribat a un mètode similar al proposat a [Adj+19], i el càlcul final dels coeficients del nucli guarda relació amb el procediment indicat a l'Annex F de [Cos+19]. El segon atac és el descrit per Galbraith, Petit, Shani i Ti a [Gal+16], que hem generalitzat al cas de primers senars seguint la indicació feta pels autors. Amb aquest atac es crea la necessitat d'introduir SIKE.

Algunes construccions criptogràfiques basades en isogènies són molt similars al protocol SIDH. La funció de hash de Charles, Goren i Lauter n'és un exemple, i va ser, de fet, part de la inspiració que va portar al desenvolupament d'aquest sistema d'intercanvi de claus. En la línia de SIDH també trobem esquemes de *zero-knowledge proofs* i de xifrat de clau pública, presentats per Jao i De Feo. Altres construccions tenen un enfocament lleugerament diferent del que hem vist, basat en la teoria de la multiplicació complexa. Així naixia la idea, donada independentment per Couveignes i Rostovtsev-Stolbunov, d'emprar isogènies per fer criptografia, tot i que la seva proposta era totalment ineficient. Amb certes millores, Castryck et al. han introduït l'intercanvi de claus CSIDH, que tot i ser susceptible a un atac quàntic subexponencial, té un avantatge sobre SIDH al no haver de transmetre punts auxiliars i, a més, treballa amb claus de només 64 bytes (sis vegades més petites).

Per acabar, proposem dues possibles continuacions d'aquest treball. La primera consisteix en l'estudi de les corbes el·líptiques amb multiplicació complexa i el seu ús per realitzar protocols com el CSIDH. El principal objectiu relatiu a aquest sistema és l'optimització, ja que actualment és un ordre de magnitud més lent que SIDH. La segona continuació és la generalització dels esquemes basats en isogènies a altres objectes, com ara a varietats jacobianes de corbes hiperel·líptiques. En aquest cas, es presenten grafs d'isogènies més grans, fet que es tradueix en un major espai de claus.

Referències

[Adj+19] Gora Adj et al. "On the Cost of Computing Isogenies Between Supersingular Elliptic Curves". A: *Selected Areas in Cryptography – SAC 2018*. Ed. de Carlos Cid i Michael J. Jacobson Jr. Cham: Springer International Publishing, 2019, pàg. 322 - 343. ISBN: 978-3-030-10970-7.

[AM69] Michael Francis Atiyah i I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969, pàg. I - IX, 1 - 128. ISBN: 978-0-201-40751-8.

[Bar+18] Elaine B. Barker et al. *SP 800-56A Rev. 3. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. Inf. tèc. Gaithersburg, MD, United States, 2018.

[CGL06] Denis Charles, Eyal Goren i Kristin Lauter. *Cryptographic hash functions from expander graphs*. Cryptology ePrint Archive, Report 2006/021. `https://eprint.iacr.org/2006/021`. 2006.

[CJS14] Andrew Childs, David Jao i Vladimir Soukharev. "Constructing elliptic curve isogenies in quantum subexponential time". A: *Journal of Mathematical Cryptology* 8.1 (gen. de 2014), pàg. 1 - 29. ISSN: 1862-2984.

[Cos+19] Craig Costello et al. *Improved Classical Cryptanalysis of the Computational Supersingular Isogeny Problem*. Cryptology ePrint Archive, Report 2019/298. `https://eprint.iacr.org/2019/298`. 2019.

[Cos19] Craig Costello. *Supersingular isogeny key exchange for beginners*. Cryptology ePrint Archive, Report 2019/1321. `https://eprint.iacr.org/2019/1321`. 2019.

[Cou06] Jean-Marc Couveignes. *Hard Homogeneous Spaces*. Cryptology ePrint Archive, Report 2006/291. `https://eprint.iacr.org/2006/291`. 2006.

[DH76] W. Diffie i M. Hellman. "New Directions in Cryptography". A: *IEEE Trans. Inf. Theor.* 22.6 (set. de 1976), pàg. 644 - 654. ISSN: 0018-9448.

[FJP11] Luca De Feo, David Jao i Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. Cryptology ePrint Archive, Report 2011/506. `https://eprint.iacr.org/2011/506`. 2011.

[Gal+16] Steven D. Galbraith et al. *On the Security of Supersingular Isogeny Cryptosystems*. Cryptology ePrint Archive, Report 2016/859. `https://eprint.iacr.org/2016/859`. 2016.

[Gor11] Dan Gordon. "Discrete Logarithm Problem". A: *Encyclopedia of Cryptography and Security*. Ed. de Henk C. A. van Tilborg i Sushil Jajodia. Boston, MA: Springer US, 2011, pàg. 352 - 353. ISBN: 978-1-4419-5906-5.

[Jao+19] David Jao et al. *SIKE. Submission to NIST's Post-Quantum Cryptography Standardization*. Últim accés: 30 de desembre de 2019. Abr. de 2019. URL: `https://sike.org/files/SIDH-spec.pdf`.

[JL11] Antoine Joux i Reynald Lercier. "Number Field Sieve for the DLP". A: *Encyclopedia of Cryptography and Security*. Ed. de Henk C. A. van Tilborg i Sushil Jajodia. Boston, MA: Springer US, 2011, pàg. 867 - 873. ISBN: 978-1-4419-5906-5.

[Len11] Arjen K. Lenstra. "L Notation". A: *Encyclopedia of Cryptography and Security*. Ed. de Henk C. A. van Tilborg i Sushil Jajodia. Boston, MA: Springer US, 2011, pàg. 709 - 710. ISBN: 978-1-4419-5906-5.

[Moo+16] Dustin Moody et al. "NIST Report on Post-Quantum Cryptography". A: (abr. de 2016). DOI: 10.6028/NIST.IR.8105.

[Mos15] Michele Mosca. *Cybersecurity in an era with quantum computers: will we be ready?* Cryptology ePrint Archive, Report 2015/1075. https://eprint.iacr.org/2015/1075. 2015.

[MP19] Chloe Martindale i Lorenz Panny. *How to not break SIDH*. Cryptology ePrint Archive, Report 2019/558. https://eprint.iacr.org/2019/558. 2019.

[MVO91] Alfred Menezes, Scott Vanstone i Tatsuaki Okamoto. "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field". A: *Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing*. STOC '91. New Orleans, Louisiana, USA: ACM, 1991, pàg. 80 - 89. ISBN: 0-89791-397-3.

[MVO96] Alfred J. Menezes, Scott A. Vanstone i Paul C. Van Oorschot. *Handbook of Applied Cryptography*. 1a ed. CRC Press, Inc., 1996. ISBN: 0849385237.

[Ngu11] Kim Nguyen. "Index Calculus Method". A: *Encyclopedia of Cryptography and Security*. Ed. de Henk C. A. van Tilborg i Sushil Jajodia. Boston, MA: Springer US, 2011, pàg. 597 - 600. ISBN: 978-1-4419-5906-5.

[RS06] Alexander Rostovtsev i Anton Stolbunov. *PUBLIC-KEY CRYPTOSYSTEM BASED ON ISOGENIES*. Cryptology ePrint Archive, Report 2006/145. https://eprint.iacr.org/2006/145. 2006.

[Sch87] René Schoof. "Nonsingular plane cubic curves over finite fields". A: *Journal of Combinatorial Theory, Series A* 46.2 (1987), pàg. 183 - 211. ISSN: 0097-3165.

[Sag19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*. https://www.sagemath.org. 2019.

[Sho94] Peter W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". A: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. SFCS '94. Washington, DC, USA: IEEE Computer Society, 1994, pàg. 124 - 134. ISBN: 0-8186-6580-7.

[Sho97] Victor Shoup. "Lower Bounds for Discrete Logarithms and Related Problems". A: *Advances in Cryptology — EUROCRYPT '97*. Ed. de Walter Fumy. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pàg. 256 - 266. ISBN: 978-3-540-69053-5.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946.

[Sut17] Andrew Sutherland. *18.783 Elliptic Curves*. Massachusetts Institute of Technology: MIT OpenCourseWare. 2017. URL: https://ocw.mit.edu. License: Creative Commons BY-NC-SA.

[Tan09] Seiichiro Tani. "Claw finding algorithms using quantum walk". A: *Theoretical Computer Science* 410.50 (nov. de 2009), pàg. 5285 - 5297. ISSN: 0304-3975.

[Tes99] Edlyn Teske. "The Pohlig–Hellman Method Generalized for Group Structure Computation". A: *Journal of Symbolic Computation* 27.6 (1999), pàg. 521 - 534. ISSN: 0747-7171.

[Vél71] Jacques Vélu. "Isogénies entre courbes elliptiques." A: *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences. Séries A et B* 273 (jul. de 1971), pàg. 238 - 241. ISSN: 01510509.

[Voi19] John Voight. *Quaternion algebras*. v.0.9.15. Maig de 2019. URL: `https://math.dartmouth.edu/~jvoight/quat-book.pdf`.

[Was08] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. 2a ed. Chapman & Hall/CRC, 2008. ISBN: 9781420071467.

Annexos

A Planificació temporal

Aquest treball es va plantejar de la següent manera:

Quinzena	Tasca
1 - 15 set.	Equacions de Weierstrass, llei de grup, isogènies
16 - 30 set.	Isogènies, polinomis de divisió, grups de torsió, morfisme de Frobenius, T. de Hasse
1 - 15 oct.	Corbes supersingulars, anells d'endomorfismes i quaternions
16 - 31 oct.	SIDH, implementació inicial en Sage
1 - 15 nov.	Atac claw i atac actiu
16 - 30 nov.	Introducció criptogràfica, Diffie-Hellman, Logaritmes discrets i motivació criptografia postquàntica
1 - 15 des.	Problemes computacionals, altres atacs
16 - 31 des.	Introducció i conclusions del treball
1 - 15 gen.	Documentació final del codi Sage

Taula 2: Planificació inicial per quinzenes.

La redacció de cada secció estava prevista per al període de temps respectiu. La realització de la Secció 4 inclou la implementació en Sage del protocol i els atacs claw i actiu. La realització del treball s'ha efectuat tal com estava previst fins la primera setmana d'octubre. Al novembre va sorgir la possibilitat de donar una xerrada al Seminari Informal de Matemàtiques de Barcelona (SIMBa) a finals de mes, que va obligar a avançar una quinzena la recerca de la Secció 1.

A banda, la realització de les seccions dels atacs *claw* i l'actiu de Galbraith et al. va durar des d'aproximadament el 20 de novembre al 15 de desembre. Conseqüentment, els problemes computacionals, els atacs quàntics i la relació amb l'anell d'endomorfismes s'han desenvolupat la segona quinzena de desembre, alhora que la redacció de la introducció i les conclusions. El calendari final, així com la seva visualització en forma de diagrama de Gantt, es troben detallats a la Taula 3 i la Figura A.1.

Quinzena	Tasca
1 - 15 set.	Equacions de Weierstrass, llei de grup, isogènies
16 - 30 set.	Isogènies, polinomis de divisió, grups de torsió, morfisme de Frobenius, T. de Hasse
1 - 15 oct.	Corbes supersingulars, anells d'endomorfismes i quaternions
16 - 31 oct.	SIDH, implementació inicial en Sage
1 - 20 nov.	Introducció criptogràfica, Diffie-Hellman, Logaritmes discrets i motivació criptografia postquàntica
20 nov. - 15 des.	Atac claw i atac actiu
15 des. - 30 des.	Problemes computacionals, altres atacs
25 des. - 5 gen.	Introducció i conclusions del treball
1 - 15 gen.	Documentació final del codi Sage

Taula 3: Calendari final aproximat.

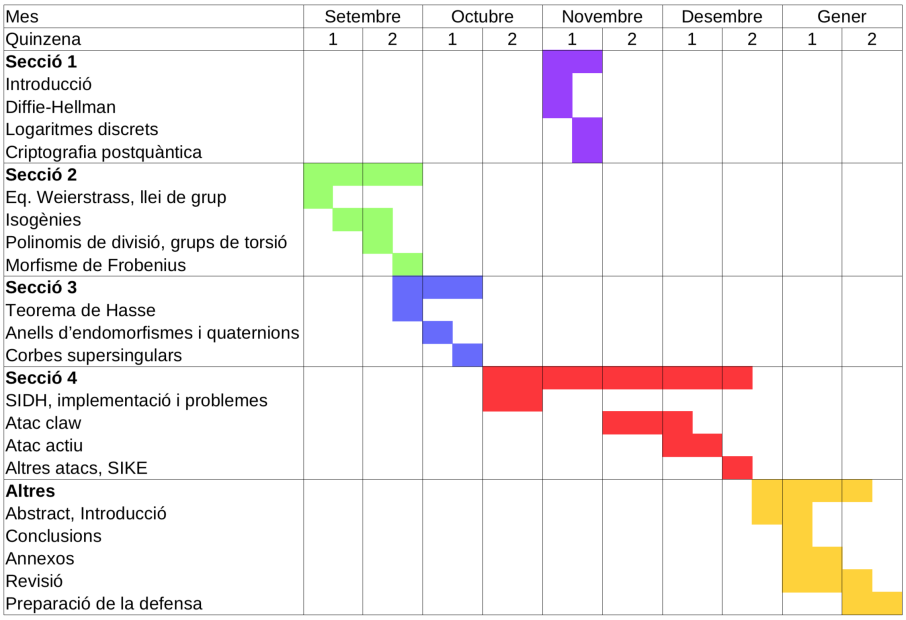


Figura A.1: Diagrama de Gantt representant l'execució del treball.

B Paràmetres proposats

L'especificació del protocol SIKE (en la versió publicada el 17 d'abril de 2019) dona quatre conjunts de paràmetres possibles per efectuar el protocol, etiquetats segons la mida del nombre primer p utilitzat (en bits). A continuació donem la relació dels primers utilitzats, juntament amb el temps per generar una clau i fer un intercanvi amb la implementació oficial (segons els *benchmarks* donats a [Jao+19], fets en un Intel Core i7-6700 Skylake a 3,4GHz).

Incloem també el temps amb la nostra implementació en Sage actuant com a Bob (*benchmarks* fets en un Intel Core i7-8650U a 1,90GHz i mesurats amb la funció de Python `time.process_time()`). Veiem que la implementació oficial és aproximadament entre 1500 i 2000 vegades més ràpida, fet que s'explica per diversos motius: l'ús d'un processador més ràpid, la implementació a baix nivell, el càlcul de ℓ^e-isogènies amb un algoritme amb complexitat $O(e \log e)$ (el nostre té complexitat $O(e^2)$), i les diferents optimitzacions realitzades a l'estàndard.

Etiqueta	p	Mida clau (bytes)	B. oficial (ms)	B. propi (ms)
`SIKEp434`	$2^{216}3^{137} - 1$	330	6,3	12277
`SIKEp503`	$2^{250}3^{159} - 1$	378	9,0	17336
`SIKEp610`	$2^{305}3^{192} - 1$	462	16,8	25529
`SIKEp751`	$2^{372}3^{239} - 1$	564	25,8	42740

Taula 4: Paràmetres especificats juntament amb el protocol SIKE, mida de les claus obtingudes i *benchmarks*.

C Rendiment de l'atac actiu

Hem realitzat una sèrie de proves amb l'atac *claw* utilitzant els algoritmes MN i DFS per a l'exploració. Les proves s'han realitzat amb els primers que apareixen a la taula, atacant sempre una clau pública d'Alice amb $\ell_A = 2$. A la taula es mostra el temps total d'execució de l'atac, el temps de generació del diccionari d'invariants j, i el temps mitjà de càlcul d'una isogènia (és a dir, el temps de generació del diccionari entre el total de parelles $(m, n) \in \mathcal{K}_{\ell^f}$ explorades). Mesurem el temps de generació del diccionari perquè és la part de l'atac que tarda una quantitat fixa de temps: l'exploració per trobar una isogènia $\hat{\psi}_2 \colon E_A \to \tilde{E}$ troba una col·lisió després d'una quantitat aleatòria de passos, depenent de la clau privada.

	MN				DFS			
p	t_{total} (s)	t_j (s)	t_i (ms)	RAM	t_{total} (s)	t_j (s)	t_i (ms)	RAM
$2^8 3^5 - 1$	1,7	0,2	11,6	3,4	1,7	0,2	9,0	3,9
$2^{13} 3^7 - 1$	4,7	1,3	19,0	11,1	2,7	0,6	9,0	11,7
$2^{15} 3^8 - 1$	10,6	2,9	22,2	19,4	3,2	1,1	8,6	16,6
$2^{18} 3^{13} - 1$	28,0	16,5	32,2	72,8	9,7	4,6	9,0	60,0
$2^{20} 3^{11} - 1$	61,0	39,1	38,1	145,1	15,4	9,1	8,9	110,2
$2^{22} 3^{15} - 1$	144,0	88,0	42,9	294,5	28,6	18,5	9,0	202,8

Taula 5: Taula de rendiment de l'algoritme *claw* amb exploració MN i DFS. El temps total d'execució t_{total} està en segons. El temps de càlcul del diccionari d'invariants j t_j està en segons. El temps mitjà per isogènia calculada t_i està en milisegons. Finalment, RAM representa els MB de memòria *per sobre de 200* que ha arribat a ocupar el procés.

Totes les proves han estat realitzades amb un processador Intel Core i7-8650U a 1,90GHz. Les mesures de t_{total} i RAM s'han efectuat amb el mode `verbose` de `time`, i les mesures de t_j i t_i, amb la comanda de Python `time.process_time_ns()`. S'han realitzat tres mesures per algoritme i primer p, les dades de la taula corresponen a la mitjana de les mesures. A la Figura C.1 es poden veure representades les dades de la taula, amb barres d'error representant les desviacions estàndard.

És remarcable el fet que l'exploració DFS mantingui un temps constant per isogènia, mentre que amb l'exploració MN el temps vagi augmentant. L'exploració DFS efectua $O(\ell^{f+1})$ operacions en el cos finit, i es calculen $\ell^f + \ell^{f-1}$ isogènies de grau ℓ^f. Per contra, l'exploració MN efectua $O(\ell^{f+1} f \log f)$ operacions en el cos finit. La diferència entre els dos algoritmes és el factor $O(f \log f)$, que augmenta amb el primer p.

La diferència en l'ús de memòria dels dos algoritmes es deu a la gestió que fa Python dels objectes. Com que cada isogènia és una composició d'objectes isogènia, i a l'algoritme DFS s'evita al màxim el càlcul repetit d'una mateixa ℓ-isogènia, cadascuna es guarda un únic cop, aprofitant l'espai de memòria.

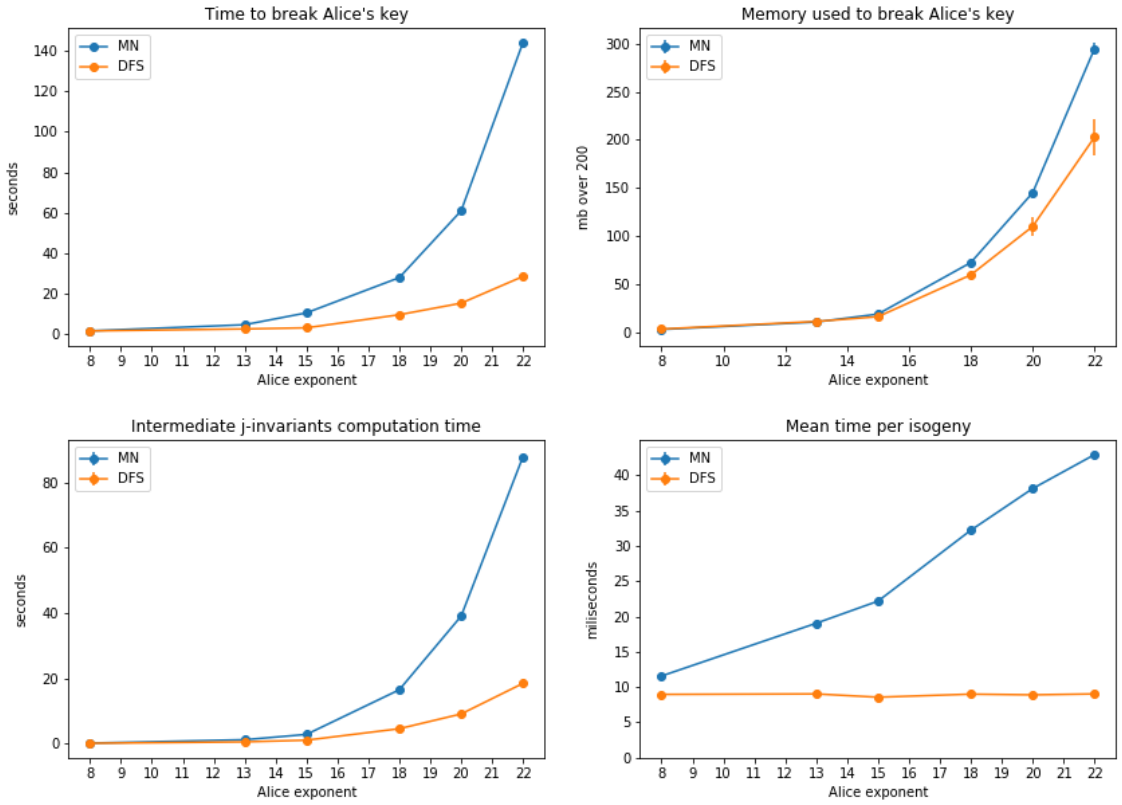


Figura C.1: Temps total (s), memòria utilitzada per sobre de 200 MB, temps de càlcul del diccionari d'invariants j (s) i temps mitjà per isogènia (ms), en funció de l'exponent e_A utilitzat per Alice.

D Visualitzacions dels grafs d'isogènies

Hem generat diverses visualitzacions emprant D3.js de grafs d'isogènies. Aquestes visualitzacions ens permeten explicar i comprendre millor els aspectes tractats: l'intercanvi de claus SIDH, l'atac *claw* i l'atac actiu de Galbraith, Petit, Shani i Ti.

D.1 Intercanvi SIDH

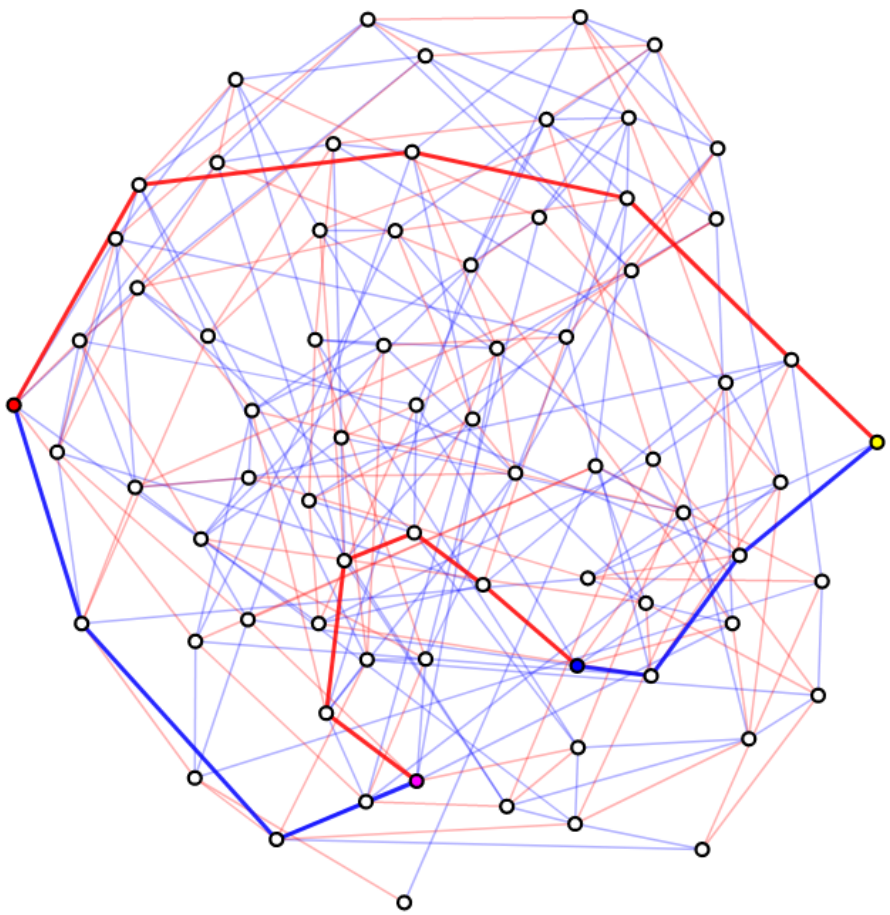


Figura D.1: Graf d'invariants j supersingulars per a $p = 2^5 3^3 - 1 = 863$, amb 73 invariants supersingulars. Les 2-isogènies estan representades de color vermell, i les 3-isogènies, de color blau. Les isogènies calculades per fer un intercanvi SIDH són les arestes **gruixudes**. El node **groc** correspon a la corba E_0 amb $j(E_0) = 1728$. Els nodes **vermell** i **blau** corresponen a les claus públiques d'Alice i Bob, respectivament. El node de color **magenta** és el secret compartit obtingut al fer l'intercanvi.

D.2 Atac *claw*

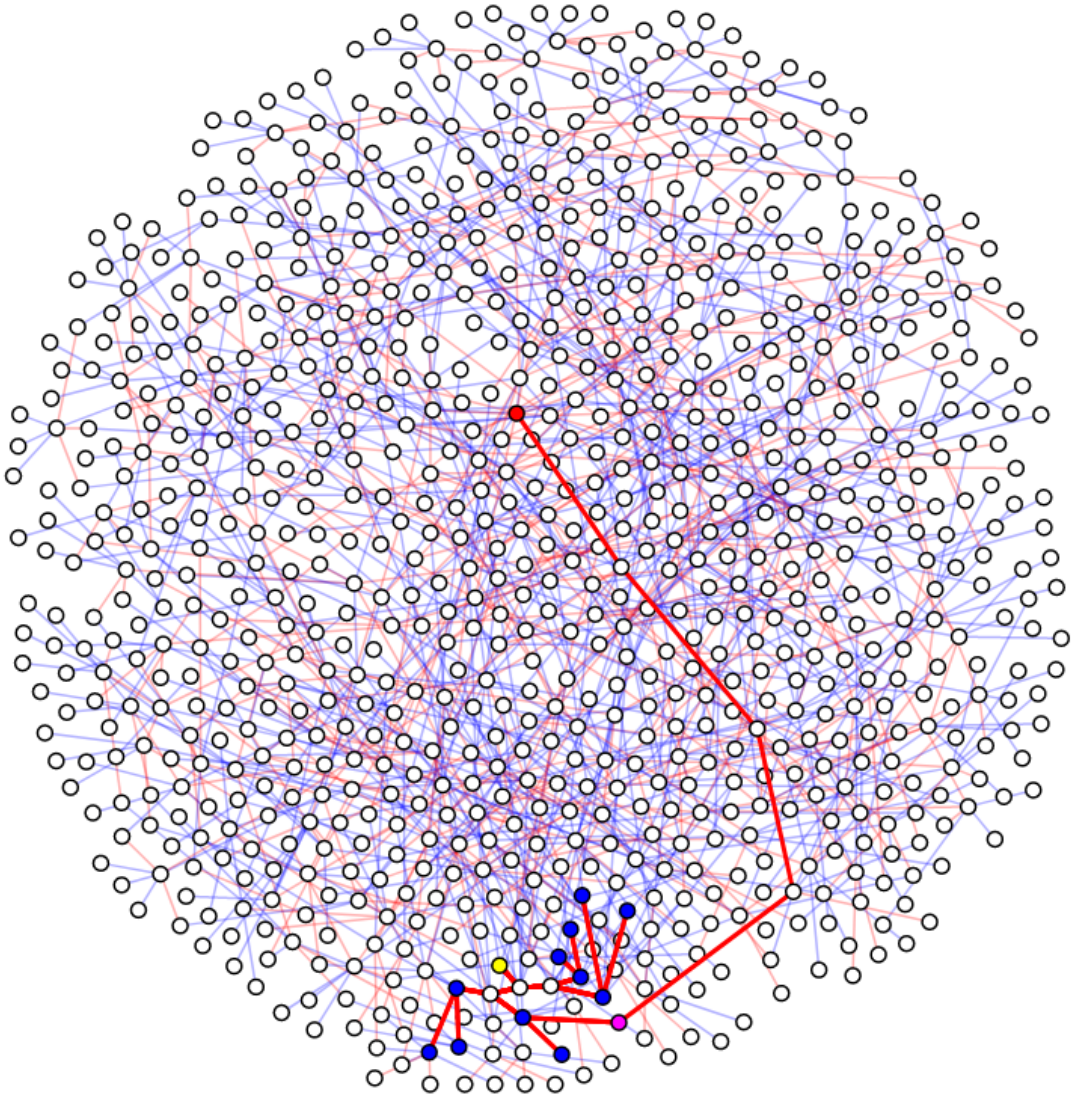


Figura D.2: Graf d'invariants j supersingulars per a $p = 2^8 3^5 - 1 = 62207$. Per a aquest primer, hi ha 5185 invariants supersingulars, dels quals només se'n mostren 907. Les 2-isogènies estan representades de color vermell, i les 3-isogènies, de color blau. El node **groc** correspon a la corba E_0 amb $j(E_0) = 1728$. El node **vermell** correspon a la clau pública d'Alice. Els nodes de color **blau** són els invariants j guardats en la taula hash. El node de color **magenta** és la col·lisió trobada per l'algoritme.

D.3 Atac actiu

La visualització d'aquest atac va portar a l'enunciat de la Proposició 4.11. Aquest resultat ens diu informalment que el coneixement de d bits d'una clau privada ens permet conèixer les d primeres ℓ-isogènies de la descomposició $\psi = \psi_{e-1} \circ \cdots \circ \psi_0$ d'una ℓ^e-isogènia.

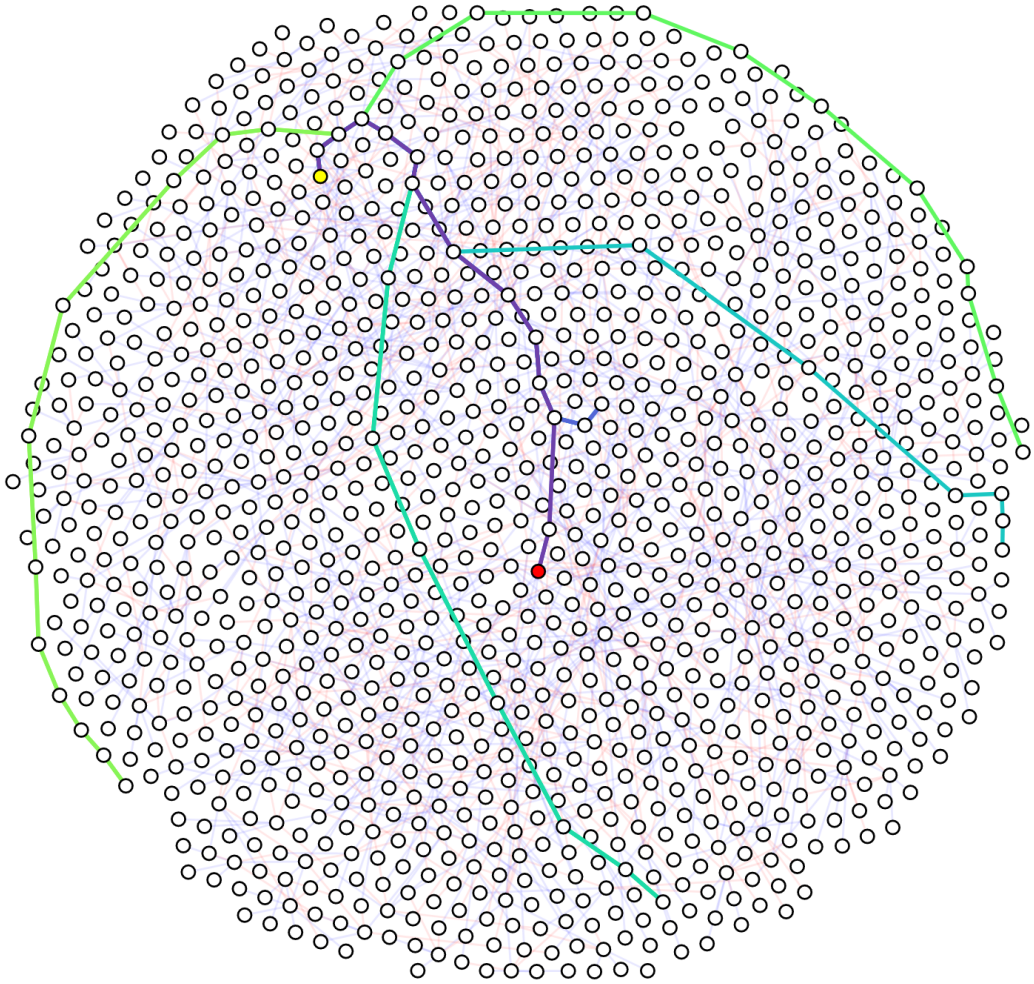


Figura D.3: Graf d'invariants j supersingulars per a $p = 2^{13}3^7 - 1 = 17915903$. Per a aquest primer, hi ha 1492993 invariants supersingulars, dels quals només se'n mostren 1240. Les 2-isogènies estan representades de color vermell, i les 3-isogènies, de color blau. El node **groc** correspon a la corba E_0 amb $j(E_0) = 1728$. El node **vermell** correspon a la clau pública d'Alice. L'escala de color de les isogènies ressaltades va del **verd clar** ($i = 1$) al **lila** ($i = 13$). Cada isogènia és la resultant de fer el quocient només coneixent els primers i bits de la clau.