Criptografia basada en isogènies

Enric Florit Zacarías
efz1005@gmail.com

Departament de Matemàtiques i Informàtica
Universitat de Barcelona

Una de les grans àrees d'estudi dintre de la criptografia és l'anomenada criptografia de clau pública, que treballa amb criptosistemes que permeten la comunicació xifrada o protegida entre parts que no necessàriament han tingut un contacte previ. Ja des dels inicis del concepte de clau pública, als anys setanta, tenim exemples basats en grups cíclics i enters mòdul n: l'intercanvi de claus de Diffie i Hellman (1976), i el xifrat RSA (1977).

L'intercanvi de claus de **Diffie i Hellman** soluciona el problema d'acordar una clau entre dues parts per al seu posterior ús en protocols simètrics (essent l'estàndard actual el xifrat AES, emprat, per exemple, en el protocol HTTPS dels navegadors d'Internet). Es proposà inicialment sobre grups finits $\mathbb{Z}/p\mathbb{Z}$ amb p primer. Havent fixat un generador g públic, una clau privada és un enter $0 < a < p$, i la corresponent clau pública és $A = g^a$. Així, si (a, g^a) és el parell de claus corresponent a Alice i (b, g^b) és el parell de claus corresponent a Bob, l'intercanvi entre els dos es representa pel diagrama següent:

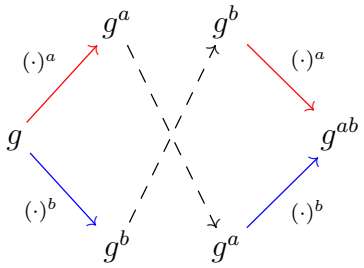


Figura 1: Intercanvi de claus Diffie-Hellman. A la part superior, les operacions que realitza **Alice**, a la inferior, les operacions que realitza **Bob**. Les fletxes discontínues indiquen l'intercanvi de les claus públiques (a través de la xarxa).

Cal destacar que si algú hagués obtingut A o B, i a més pogués resoldre l'equació $g^a \equiv A \mod p$ o $g^b \equiv B \mod p$, aleshores podria fer el mateix càlcul que Alice i Bob i obtindria el mateix secret. La resolució d'aquest tipus d'equacions rep el nom de *logaritme discret*, i és on rau la seguretat del protocol de Diffie i Hellman.

Aquest protocol es considera segur, ja que el millor algoritme per resoldre logaritmes discrets opera en temps subexponencial –és a dir, augmentant suficientment la mida dels paràmetres (en aquest cas el primer p) no es poden resoldre instàncies de logaritme discret en un temps raonable.

Tot i això, la creixent atenció en el camp de la computació quàntica pot fer inservible aquest i altres sistemes de clau pública. El 1994 Peter Shor publicà el seu algoritme

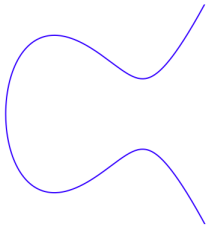
quàntic de factorització d'enters i resolució de logaritmes discrets, en aquell moment encara teòric. Però segons diverses prediccions, aquests algoritmes podrien ser implementats en les dècades següents, motivant la recerca de nous criptosistemes resistents a ser analitzats tant amb tècniques clàssiques com quàntiques. És el que anomenem criptografia postquàntica.

Un dels sistemes proposats és conegut com a **Supersingular Isogeny Diffie-Hellman** (SIDH), que explicarem a continuació. Aquest protocol va ser introduït per De Feo, Jao i Plût el 2011 [FJP11], i es va presentar al concurs d'estandardització de criptografia postquàntica creat per l'Institut NIST el 2016 [Moo+16]. Actualment, SIDH és un dels sistemes que han superat les dues primeres fases de selecció d'aquest concurs, i és un dels denominats "protocols alternatius": criptosistemes segurs i efectius, però que no es troben entre les propostes més ràpides.

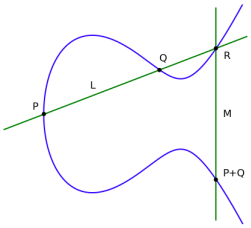
El criptosistema que estudiem en aquest treball requereix parlar de corbes el·líptiques i isogènies. Una **corba el·líptica** ve donada per una equació de Weierstrass

$$E\colon y^2 = x^3 + Ax + B,$$

on A i B són elements d'un cert cos K que satisfan $4A^3 + 27B^2 \neq 0$. A la Figura 2a trobem un exemple de corba el·líptica sobre els reals.



(a) La corba $E\colon y^2 = x^3 - 3x + 3$.



(b) Llei de grup en una corba el·líptica sobre $\mathbb{R}$.

Figura 2: Corba el·líptica sobre els reals i exemple de la llei de grup corresponent.

La propietat que fa interessants les corbes el·líptiques és que, a més de corbes algebraiques, tenen estructura de grup abelià, de manera que podem sumar punts amb una certa regla geomètrica, representada a la Figura 2b.

Dels morfismes algebraics no constants entre corbes el·líptiques que són també morfismes de grups en diem isogènies. Més concretament, una *isogènia* $\phi\colon E \to E'$ ve donada per polinomis p, q, r, s tals que

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

i de manera que $\phi(P + Q) = \phi(P) + \phi(Q)$. Clarament, la composició d'isogènies és una isogènia. El *grau* de ϕ es defineix com el màxim entre els graus de p i q.

Totes les isogènies són morfismes exhaustius i tenen nucli finit. Si l'ordre del nucli de ϕ no és divisible per la característica del cos K, diem que ϕ és una isogènia separable i el seu grau és l'ordre del nucli. Quan $p = \operatorname{car} K \neq 0$ divideix $\#\ker\phi$, la isogènia podria ser inseparable (no necessitarem aquesta noció). Donades aquestes propietats, podem pensar en una isogènia com un "quasi-isomorfisme", on ens falta "dividir" pel grau.

Exemple: multiplicació per un enter. Donat un enter no nul m, l'aplicació que multiplica cada punt d'una corba E per m, és a dir,

$$\begin{aligned}[m]\colon E &\to E\\ P &\mapsto P + \overset{m}{\cdots} + P,\end{aligned}$$

és una isogènia. Té grau m^2, i el seu nucli és el subgrup de m-torsió, denotat $E[m]$.

El següent resultat ens permet utilitzar les isogènies per fer criptografia, associant corbes el·líptiques a claus públiques, i subgrups finits a claus privades.

Teorema (de la corba quocient). Donada una corba el·líptica E i un subgrup finit G de E, existeixen una corba E' i una isogènia separable $\phi\colon E \to E'$ tals que $\ker\phi = G$. A més, la corba E' és única mòdul isomorfisme, cosa que ens permet escriure $E' = E/G$.

La versió efectiva d'aquest teorema són les anomenades fórmules de Vélu, i ens permeten calcular la corba E' i l'expressió de ϕ en temps lineal en la mida de G.

Si considerem una corba el·líptica E definida sobre un cos finit $\mathbb{F}_q$, on $q = p^r$ per algun $r \geq 1$, el grup $E(\mathbb{F}_q)$ és finit. El teorema de Hasse ens dona una estimació sobre el nombre de punts d'aquest grup: si posem $\#E(\mathbb{F}_q) = q + 1 - t$, aleshores se satisfà

$$|t| \leq 2\sqrt{q}.$$

Diem que la corba E és **supersingular** (en contraposició a ordinària) quan $t \equiv 0 \mod p$. Es pot demostrar que, en aquest cas, el grup de punts de p-torsió de E és trivial. A més, la corba E té com a anell d'endomorfismes $\mathrm{End}(E)$ un ordre en una $\mathbb{Q}$-àlgebra de quaternions. Cal destacar que dues corbes supersingulars sempre són isògenes sobre $\bar{\mathbb{F}}_q$.

Si tenim un conjunt V de (classes d'isomorfisme de) corbes el·líptiques i ℓ un primer, podem definir un graf de ℓ-isogènies entre les corbes de V: dues corbes E, E' de V estan connectades per una aresta si i només si hi ha una isogènia $E \to E'$ de grau ℓ.

Volem emprar grafs d'isogènies entre corbes el·líptiques supersingulars per tres raons. En primer lloc, totes les corbes supersingulars estan definides sobre el cos finit $\mathbb{F}_{p^2}$, fet que ens acota la complexitat de les operacions elementals i ens permet treballar amb coeficients de la forma $(a, b) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

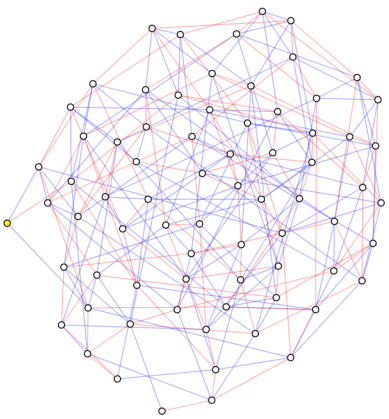


Figura 3: Graf d'isogènies supersingulars amb $p = 863$. Les arestes vermelles corresponen a isogènies de grau 2, les blaves corresponen a isogènies de grau 3.

En segon lloc, aquests grafs tenen les millors propietats d'*expansió*: efectuant camins aleatoris de longitud $O(\log p)$, podem estar segurs d'haver arribat a una corba aleatòria uniformement distribuïda en el conjunt de nodes.

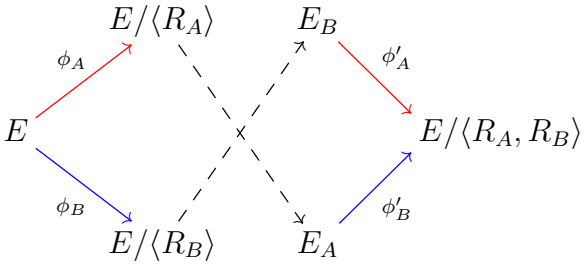
Finalment, trobar camins (és a dir, isogènies) entre dues corbes donades té una complexitat exponencial en el cas supersingular, mentre que per corbes ordinàries hi ha un algoritme quàntic per trobar-ne en temps subexponencial.

Per definir el nostre criptosistema, considerarem corbes sobre cossos finits $\mathbb{F}_{p^2}$, on p és un primer de la forma $2^e3^f - 1$ amb e i f enters positius. Emprant primers d'aquesta forma, la corba $E\colon y^2 = x^3 + x$ sempre serà supersingular, i a més tindrà $(2^e3^f)^2$ punts. Amb la corba fixada $E\colon y^2 = x^3 + x$ sobre $\mathbb{F}_{p^2}$, procedim a definir l'intercanvi SIDH.

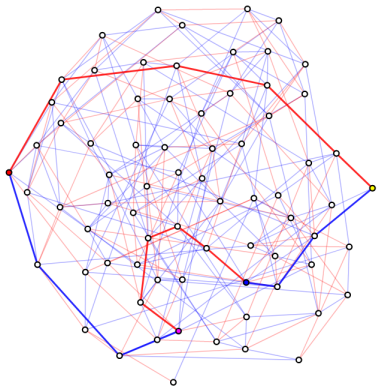
Alice tria com a clau privada un punt R_A d'ordre 2^e, i Bob tria com a clau privada un punt R_B d'ordre 3^f. Les claus públiques són les corbes

$$\phi_A\colon E \to E_A = E/\langle R_A\rangle,$$
$$\phi_B\colon E \to E_B = E/\langle R_B\rangle.$$

La informació revelada és $(E_A, \phi_A(P_B), \phi_A(Q_B))$ i $(E_B, \phi_B(P_A), \phi_B(Q_A))$, on $\{P_A, Q_A\}$ (resp. $\{P_B, Q_B\}$) és una $\mathbb{Z}/2^e\mathbb{Z}$-base de $E[2^e]$ (resp. $\mathbb{Z}/3^f\mathbb{Z}$-base de $E[3^f]$) en la qual podem expressar R_A (resp. R_B). Els punts auxiliars són necessaris per a poder completar l'intercanvi, de manera que els dos participants arriben a una corba el·líptica compartida E_{AB}. El diagrama d'isogènies resultant ens recorda el de Diffie-Hellman:



(a) Diagrama del SIDH.



(b) Intercanvi SIDH representat sobre el graf amb $p = 863$.

Figura 4: Representacions del protocol SIDH com a diagrama commutatiu i com a camins sobre un graf. En **vermell**, les operacions realitzades per Alice. En **blau**, les operacions realitzades per Bob. Les fletxes discontínues indiquen l'intercanvi de les claus públiques.

Per què és segur el protocol SIDH? Suposem que disposem d'una clau pública

$$(E_A, \phi_A(P_B), \phi_A(Q_B))$$

de SIDH. L'objectiu de l'anàlisi d'aquest sistema és recuperar la clau privada (R_A, ϕ_A) que la genera. Si no tenim possibilitat de comunicar-nos amb l'usuari d'aquesta clau, la millor aproximació és la força bruta sobre el graf d'isogènies. Sobre qualsevol graf, la manera de trobar un camí entre dos nodes (si no tenim cap heurística disponible) és

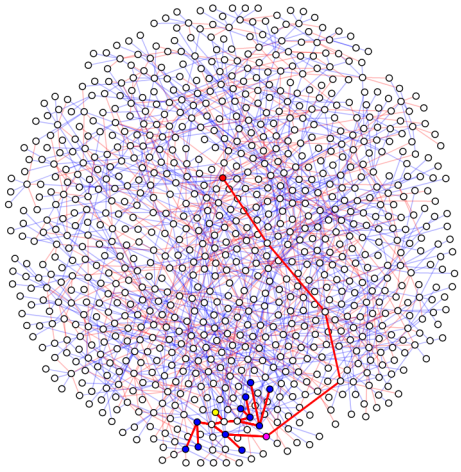


Figura 5: Il·lustració de l'atac *claw*. El node **groc** correspon a la corba E inicial. El node **vermell** correspon a la clau pública analitzada. Els nodes de color **blau** són les corbes guardades en la taula *hash*. El node de color **magenta** és la col·lisió trobada per l'algoritme.

efectuar recorreguts aleatoris amb profunditat limitada des d'un dels dos fins a arribar a l'altre.

Podem invertir una mica d'espai de memòria per estalviar alguns càlculs. Les isogènies $E \to E_A$ són de grau 2^e, de manera que venen donades per un camí de longitud e en el graf. Així, podem fixar una quantitat $d \leq \frac{e}{2}$, i guardar en un diccionari tots els camins possibles des de E de longitud d. Després, explorarem des de E_A amb profunditat $e-d$, fins que arribem a trobar una col·lisió amb el diccionari guardat. Aquesta tècnica s'anomena **atac *claw*** (Figura 5), i té una complexitat de $O(2^{e/2}) = O(\sqrt[4]{p})$ en temps i memòria quan $d = \frac{e}{2}$. Si transformem aquesta idea a un algoritme quàntic, obtenim un atac de complexitat $O(\sqrt[6]{p})$ en temps i memòria.

Les dues complexitats són exponencials en $\log p$. Aquests són els millors atacs coneguts, de manera que SIDH es considera resistent a criptoanàlisi tant clàssica com quàntica. Hem de remarcar que aquests no imposen restriccions de memòria: si la quantitat de memòria està acotada (diguem, de manera lineal en $\log p$), el millor atac té una complexitat exponencial amb constants més elevades.

El protocol SIDH té una diferència clarament marcada amb l'esquema de Diffie i Hellman: les claus intercanviades inclouen una informació extra: els punts auxiliars

$$\{\phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)\},$$

que, aparentment, podrien estar revelant una part de la clau pública. Amb només una execució del protocol, no s'ha aconseguit extreure cap dada que permeti trencar la clau. No obstant això, si la part atacada no canvia mai la seva clau privada, podem recuperar-la bit a bit efectuant només $O(\log p)$ intercanvis maliciosos.

Aquest atac va ser proposat per Galbraith *et al.* el 2016 [Gal+16]. Es pot evitar canviant la clau a cada intercanvi (utilitzant el que es coneix com a clau efímera), o bé aplicant una transformació que impedeix utilitzar claus malicioses a canvi d'augmentar el temps de càlcul. El protocol SIDH transformat es coneix com a Supersingular Isogeny Key Encapsulation (SIKE).

Com a conclusió, SIDH és un sistema d'intercanvi de claus considerat resistent a criptoanàlisi clàssica i quàntica. Destaquem que els principis utilitzats per definir-lo es poden aplicar a altres sistemes criptogràfics, com ara funcions de *hash*, signatures digitals i compartició de secrets.

Referències

[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.

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

[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.