Pairings i les seves aplicacions

Llorenç Huguet Rotger
Josep Rifà Coma
Juan Gabriel Tena Ayuso

PID_00185092

UOC
Universitat Oberta de Catalunya

Índex

Introducció

Una de les eines de la geometria de les corbes el·líptiques que s'han demostrat més fructíferes en criptografia són els denominats *pairings*. Els *pairings* són aplicacions bilineals definides sobre els punts d'una corba el·líptica i amb valors en un grup cíclic d'arrels de la unitat, grup contingut en un cert cos finit.

Hi ha diversos tipus de *pairings*, i els fonamentals són el *pairing* de Weil i el de Tate. Recentment, han estat proposats altres tipus de *pairings*: *eta parings, ate, omega pairings*, etc, els quals tenen un caràcter auxiliar i alguns només són aplicables a tipus particulars de corbes.

El *pairing* de Tate és més general que el de Weil (es pot aplicar a corbes més generals que les el·líptiques) i ofereix certs avantatges computacionals; no obstant això, és més difícil de descriure, i per això, en el que segueix, només considerarem el segon. En qualsevol cas, no estem interessats en la computació explícita d'aquests *pairings*, sinó en el paper que tenen en criptografia, i l'elecció del *pairing* de Weil està motivada exclusivament per la claredat en l'exposició.

Les aplicacions criptogràfiques dels *pairings* són de dos tipus. D'una banda s'han utilitzat amb un propòsit *destructiu*, per a dissenyar atacs al problema del logaritme discret el·líptic, i d'una altra banda, des d'un punt de vista *constructiu*, constitueixen una eina bàsica d'un nou paradigma, el de la criptografia basada en la identitat. L'atac basat en *pairings* té com a conseqüència que certes corbes el·líptiques, les denominades *supersingulars*, no es considerin actualment segures per a implementar criptosistemes i protocols criptogràfics basats en el logaritme discret el·líptic però, curiosament, tals corbes supersingulars són idònies per a la criptografia basada en la identitat.

Descriurem en el que segueix els *pairings* i els dos tipus d'aplicacions criptogràfiques esmentades.

Objectius

En els materials didàctics d'aquest mòdul l'estudiant trobarà els continguts necessaris per a assolir els objectius següents:

1. Conèixer el concepte de "pairing" en corbes el·líptiques, específicament el pairing de Weil.
2. Conèixer les aplicacions criptogràfiques dels pairings, sobretot les enfocades al càlcul del logaritme discret el·líptic i les enfocades a la criptografia basada en l'identitat.
3. Conèixer algun protocol específic de criptografia basada en la identitat (acord de claus, xifratge i signatura).
4. Saber escriure programari per implementar els protocols anteriors.

1. *Pairings* en corbes el·líptiques

En aquest apartat es descriuen els *pairings* definits sobre una corba el·líptica i s'estudien les seves propietats. Es mostra així mateix com el grup d'arribada d'un *pairing* està contingut en un cos finit, extensió del cos base de definició de la corba. Es defineix el grau d'immersió i se'n discuteix el valor.

1.1. Aplicacions bilineals

Els *pairings* són aplicacions bilineals entre certs grups abelians. Comencem considerant les aplicacions bilineals entre espais vectorials, sens dubte més familiars a l'estudiant, i la definició i les propietats es traslladaran immediatament al llenguatge de *pairings*.

Sigui K un cos commutatiu, i V_1, V_2, W, tres espais vectorials sobre K.

Definició 1.1. Una aplicació $f : V_1 \times V_2 \to W$ es diu bilineal si és aplicació lineal d'espais vectorials en cadascuna de les variables, és a dir, si per a tot $a,a' \in V_1$, $b,b' \in V_2$, $\lambda \in K$, es verifiquen les quatre propietats següents:

1) $f(a+a',b) = f(a,b) + f(a',b)$

2) $f(\lambda a,b) = \lambda f(a,b)$

3) $f(a,b+b') = f(a,b) + f(a,b')$

4) $f(a,\lambda b) = \lambda f(a,b)$

Si $W = K$ una aplicació bilineal es diu forma bilineal.

Suposem que $V_1 = V_2 = V$, llavors podem donar la següent definició.

Definició 1.2. Una aplicació bilineal $f : V \times V \to W$ es diu:

1) Simètrica si $\forall a,b \in V$ es verifica: $f(a,b) = f(b,a)$.

2) Antisimètrica si $\forall a,b \in V$ es verifica: $f(a,b) = -f(b,a)$.

3) Alternada si $\forall a \in V$ es verifica: $f(a,a) = 0$.

Lema 1.3.

Tota forma bilineal alternada és antisimètrica.

Si la característica del cos K és diferent de 2 es verifica el recíproc.

Demostració:

1) Suposem f alternada. Per a $a,b \in V$ tindrem:

$$0 = f(a+b,a+b) = f(a,a) + f(a,b) + f(b,a) + f(b,b) = 0 + f(a,b) + f(b,a) + 0 \quad (1)$$

i, per tant, $f(a,b) = -f(b,a)$, és a dir, f és antisimètrica.

2) Suposem f antisimètrica, en particular per a $a = b$; tenim

$$f(a,a) = -f(a,a) \Rightarrow 2f(a,a) = 0. \quad (2)$$

Ja que la característica de K és diferent de 2, ha de ser $f(a,a) = 0$, és a dir, f és alternada.

∎

Exemple 1.1 siguin $K = \mathbb{R}$ i $V = \mathbb{R}^2$. Els elements $a \in V$ seran vectors amb dues coordenades reals, $a = (x,y)$. Siguin les formes bilineals següents $f : V \times V \to \mathbb{R}$:

1) $f((x,i),(x',i')) = axx' + b(xy' + x'i) + cyy',\ a,b,c \in \mathbb{R}$: forma simètrica

2) $f((x,i),(x',i')) = xy' - yx'$: forma antisimètrica i alternada

3) $f((x,i),(x',i')) = axx' + bxy' + b'x'i + cyy',\ a,b,b',c \in \mathbb{R}, b \neq \pm b'$: ni simètrica ni antisimètrica

Definició 1.4. Sigui $f : V_1 \times V_2 \to W$ una forma bilineal. S'anomena *nucli per l'esquerra* de f el conjunt $Ker_{esq} = \{a \in V_1;\ f(a,b) = 0, \forall b \in V_2\}$. De manera semblant, s'anomena *nucli per la dreta* de f el conjunt $Ker_{dre} = \{b \in V_2;\ f(a,b) = 0, \forall a \in V_1\}$.

Lema 1.5. L'element $0 \in V_1$ pertany a Ker_{esq} i l'element $0 \in V_2$ pertany a Ker_{dre}

Demostració: Per a qualsevol $a \in V_1, b \in V_2$ tenim,

$$f(a,b) = f(0+a,b) = f(0,b) + f(a,b) \Rightarrow f(0,b) = 0 \Rightarrow 0 \in Ker_{esq}. \quad (3)$$

El resultat per a $0 \in Ker_{der}$ és semblant. ∎

Formes quadràtiques

Si $f : V \times V \to K$ és una forma bilineal simètrica l'aplicació $q : V \to K, q(a) = f(a,a)$ es diu *forma quadràtica*. La teoria de les formes quadràtiques, estretament relacionada amb la de formes bilineals simètriques, és una branca important de l'àlgebra, i sens dubte és familiar a l'estudiant a propòsit de l'estudi de les còniques i quàdriques.

Observació

La forma quadràtica associada a la forma bilineal simètrica $f((x,y),(x',y')) = axx' + b(xy' + x'y) + cyy'$ és la $q((x,y)) = ax^2 + 2bxy + cy^2$.

Definició 1.6. L'aplicació f es diu *no degenerada per l'esquerra* si $Ker_{esq} = \{0\}$, i *no degenerada per la dreta* si $Ker_{dre} = \{0\}$.

És evident que si f és simètrica o antisimètrica es verifica $Ker_{esq} = Ker_{dre}$.

Definició 1.7. $f : V \times V \to W$ aplicació bilineal simètrica o antisimètrica es diu *no degenerada* si verifica les condicions equivalents següents:

1) f és no degenerada per l'esquerra.

2) f és no degenerada per la dreta.

3) Per a tot $a \in V$ existeix un $b \in V$ tal que $f(a,b) \neq 0$ (i també $f(b,a) \neq 0$).

En cas contrari es diu *degenerada*.

Exemple 1.2 siguin $K = \mathbb{R}$ i $V = \mathbb{R}^2$,

L'aplicació bilineal simètrica, $f : V \times V \to K$, $f((x,y),(x',y')) = xx' + yy'$, és no degenerada.

L'aplicació bilineal simètrica, $f : V \times V \to K$, $f((x,y),(x',y')) = xx'$, és degenerada: tot element $(0,y)$ pertany al nucli per l'esquerra (o per la dreta).

Com s'ha dit abans, la definició d'aplicació bilineal es pot formular per a grups abelians. Per a adaptar-nos a la notació que farem servir més endavant per als *pairings*, suposem dos grups abelians A,B amb notació additiva i C un grup abelià amb notació multiplicativa.

Definició 1.8. Una aplicació $f : A \times B \to C$ es diu bilineal si verifica:

1) $f(a + a',b) = f(a,b) \cdot f(a',b)$

2) $f(a,b + b') = f(a,b) \cdot f(a,b')$

Les definicions i propietats enunciades abans (simètrica, antisimètrica, alternada, no degenerada) continuen essent vàlides en aquest cas, amb els canvis de notació pertinents (en particular l'element neutre de C s'ha d'escriure ara com a 1).

1.2. El *pairing* de Weil

Sigui E una corba el·líptica definida sobre un cos commutatiu K (en el context de les aplicacions criptogràfiques K serà un cos finit). Els *pairings* són aplicacions bilineals que transformen un parell de punts de E en un element d'un grup cíclic finit, els elements del qual es poden identificar amb arrels de la unitat, grup que en el cas $K = \mathbb{F}_q$, cos finit de q elements, veurem que es pot considerar contingut en un cos $\mathbb{F}_{q^k}$ amb q^k elements, per a un cert valor k.

Prendrem com a model el *pairing* de Weil, el primer tipus de *pairing* proposat*. Per a cada enter l, primer amb la característica del cos, es té un *pairing* de Weil e_l, que està definit en els punts del subgrup $E[l]$ de l-torsió de E (subgrup que definim a continuació) i en valors en un grup cíclic μ_l amb l elements, la llei de grup del qual escriurem amb notació multiplicativa. Com que tot element $x \in \mu_l$ verifica que $x^l = 1$, es pot interpretar μ_l com el grup de les arrels l-èsimes de 1. Un generador d'aquest grup cíclic l'anomenarem, en aquest context, arrel primitiva l-èsima de la unitat.

* Vegeu, per exemple, A. Menezes (1993). *Elliptic Curves Public Key Cryptography*. Kluwer.

Definició 1.9. Els punts de l-torsió d'una corba el·líptica són els elements del conjunt $E[l] = \{P \in E;\ l \cdot P = 0\}$, en què $l \cdot P$ indica el producte escalar de l pel punt P.

Observació

En les aplicacions criptogràfiques basades en el logaritme discret el·líptic, es treballa en el grup cíclic generat per un punt $P \in E$. Si l és l'ordre de P (usualment primer) llavors el *pairing* que es considera és e_l.

És evident que el conjunt $E[l]$ és un subgrup del grup $E(K)$ de punts de E racionals sobre K. Si $\bar{K}$ és una clausura algebraica de K podem definir anàlogament el grup $E[l](\bar{K})$ de punts de l-torsió racionals sobre $\bar{K}$. El grup $E[l](\bar{K})$ té cardinal l^2 i l'estructura següent (Silverman, 1986).

Referència bibliogràfica

J. H. Silverman (1986). *The Arithmetic of Elliptic Curves*. Springer-Verlag.

Lema 1.10.

$$E[l](\bar{K}) \simeq \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \qquad (4)$$

No obstant això, aquests l^2 punts de $E[l](\bar{K})$ no estan tots necessàriament definits sobre el cos K i, en general, $E[l]$ serà només una part (un subgrup) de $E[l](\bar{K})$. Noteu que aquest subgrup sempre conté almenys l'element neutre $O \in E$.

Exemple 1.3

La corba el·líptica $E : y^2 = x^3 + x + 8$, sobre el cos $\mathbb{F}_{11}$, posseeix només dos punts de 2-torsió amb coeficients en el cos base. Més precisament, $E[2] = \{O,(8,0)\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Exemple 1.4

Per a $l = 3$ la corba el·líptica $E : y^2 = x^3 + 7x$ sobre el cos $\mathbb{F}_{13}$ té 9 punts de 3-torsió racionals, explícitament

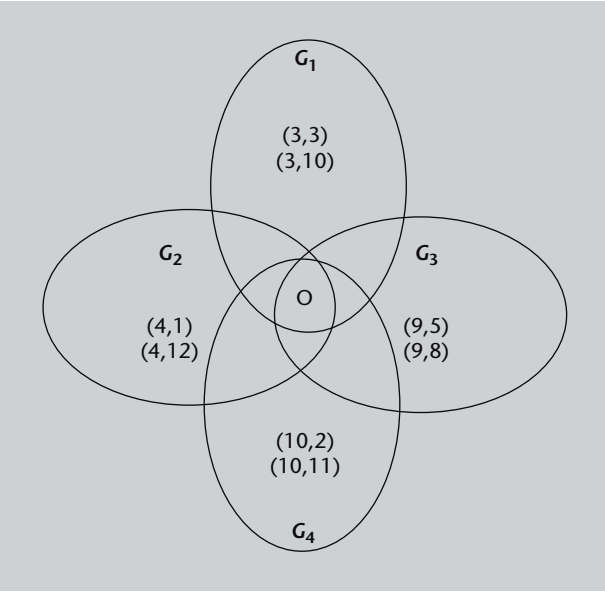
$$E[3] = \{O,(3,3),(3,10),(4,1),(4,12),(9,5),(9,8),(10,2),(10,11)\}$$

Aquests punts constitueixen un subgrup isomorf al grup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, el qual conté quatre subgrups d'ordre tres, que, a la vegada, tenen en comú l'element neutre.

- $G_1 = \{O,(3,3),(3,10)\}$
- $G_2 = \{O,(4,1),(4,12)\}$
- $G_3 = \{O,(9,5),(9,8)\}$
- $G_4 = \{O,(10,2),(10,11)\}$

El diagrama següent mostra aquests quatre subgrups.

Grups de 3-torsió



Definició 1.11. El *pairing* de Weil és una aplicació:

$$e_l : E[l] \times E[l] \longrightarrow \mu_l \tag{5}$$

amb les propietats següents:

1) Bilineal, és a dir, $e_l(P + P',Q) = e_l(P,Q)e_l(P',Q)$, $e_l(P,Q + Q') = e_l(P,Q)e_l(P,Q')$.

2) Alternada, és a dir, $e_l(P,P) = 1$, $\forall P \in I$. Com que és alternada també és antisimètrica, i per tant $e_l(P,Q) = e_l(Q,P)^{-1}$.

3) No degenerada, és a dir, $e_l(P,Q) = 1, \forall Q \Leftrightarrow P = O$, $e_l(P,Q) = 1, \forall P \Leftrightarrow Q = O$.

4) Existeixen punts $P,Q \in E[l]$ tals que $e_l(P,Q)$ és una arrel primitiva l-èsima de la unitat, i per tant e_l és exhaustiva.

Arrels primitives

S'anomena *arrel primitiva d'ordre n de la unitat* aquella l'ordre de la qual és exactament n. Per exemple, en el cos $\mathbb{C}$ dels complexos l'element $e^{2\pi i/5}$ és una arrel d'ordre 15 de la unitat (ja que $(e^{2\pi i/5})^{15} = (e^{2\pi i})^3 = 1^3 = 1$), però no és una arrel primitiva d'ordre 15, ja que el seu ordre és 5 (i, per tant, en realitat és una arrel primitiva d'ordre 5 de la unitat).

Nota

El *pairing* de Tate és més general que el de Weil, ja que exigeix només que el primer punt P estigui en $E[l]$, mentre que Q pot ser qualsevol punt de la corba. No obstant això, com s'ha esmentat, en les aplicacions criptogràfiques els punts considerats estaran en el subgrup $\langle P\rangle$ generat per un punt P d'ordre l, i per tant són tots de l-torsió.

1.3. *Pairing* modificat

La propietat alternada del *pairing* de Weil presenta un inconvenient en les aplicacions criptogràfiques. En aquestes es treballa en el grup generat per un punt $P \in E$. Si fos $e_l(P,P) = 1$, per a tot parell de punts $R,S \in \langle P\rangle$ es tindria també $e_l(R,S) = 1$ (si $R = rP$, $S = sP$ utilitzant la propietat de bilinealitat $e_l(R,S) = e_l(P,P)^{rs} = 1$), és a dir, e_l seria l'aplicació trivial. Una manera de solucionar aquest problema és substituir e_l per un *pairing* modificat $\hat{e}_l$, utilitzant el que s'anomena *aplicació distorsió*.

Definició 1.12. Una aplicació distorsió per al punt P és un endomorfisme ϕ de la corba E tal que $e_l(P,\phi(P)) \neq 1$. A vegades s'exigeix també que $e_l(P,\phi(P))$ sigui una arrel primitiva de la unitat. Si l és un nombre primer, com és habitual, totes dues condicions són equivalents.

Noteu les consideracions següents:

1) En la definició anterior el punt $\phi(P)$ és, igual que P, de l-torsió (ja que $l\phi(P) = \phi(lP) = \phi(O) = O$) i, per tant, té sentit aplicar el *pairing* de Weil al parell $(P,\phi(P))$.

2) En general l'endomorfisme ϕ no està definit sobre el cos $\mathbb{F}_q$ (i, per als nostres propòsits no ho ha d'estar). En particular $\phi(P)$ no tindrà coordenades en $\mathbb{F}_q$, sinó sobre un cos extensió.

3) Es pot provar que en E hi ha una aplicació distorsió si i només si E és supersingular (Blake i altres, 2005). Això fa que les corbes supersingulars siguin especialment útils en la criptografia basada en *pairings*.

Definició 1.13. Sigui ϕ una aplicació distorsió. Es defineix $\hat{e}(R,S) = e(R,\phi(S))$. L'aplicació $\hat{e}$ s'anomena *pairing* modificat.

Fixeu-vos que ara tenim $\hat{e}(P,P) \neq 1$ i, per tant, per a $R,S \in \langle P\rangle$, $R,S \neq O$ també tenim, per bilinealitat, $\hat{e}(R,S) \neq 1$.

La definició 1.11 és òbviament incompleta, ja que enumera les propietats de e_l però no caracteritza qui és l'element $e_l(P,Q)$ corresponent a $P,Q \in E[l]$. La definició d'aquesta imatge comporta conceptes i resultats matemàtics que desenvoluparem en detall. Per altra banda, les aplicacions criptogràfiques posteriors es poden comprendre assumint únicament les propietats de la definició 1.11.

No obstant això, per al possible estudiant interessat, resumirem breument aquí la definició explícita de $e_l(P,Q)$ i donarem un algorisme eficient de càlcul d'aquest valor.

1.3.1. Construcció explícita de e_l

Comencem introduint (sense demostració) els conceptes i resultats necessaris per a la definició de $e_l(P,Q)$.

Lectura recomanada

Vegeu J. H. Silverman (1986). *The Arithmetic of Elliptic Curves*. Springer-Verlag, per a detalls i demostracions

Definició 1.14. Sigui E una corba el·líptica,

1) Un divisor és una suma formal finita de punts de E: $D = \sum_{P\in E} n_P(P)$, amb coeficients n_P nombres enters, positius o negatius (i tots nuls excepte un nombre finit). La notació anterior de suma és un simple símbol formal i no una operació; concretament, no s'ha de confondre amb l'operació d'addició de punts de E. Tampoc no s'ha de confondre el punt $P \in E$ amb el divisor $(E) = 1(E)$.

2) Donats dos divisors $D = \sum_{P\in E} n_P(P)$, $D' = \sum_{P\in E} n'_P(P)$, la suma $D + D' = \sum_{P\in E}(n_P + n'_P)(P)$ dóna al conjunt de divisors una estructura de grup abelià.

3) Es defineix el grau de D : $gr(D) = \sum n_P \in \mathbb{Z}$.

4) Es defineix el suport de D : $sp(D) = \{P;\ \ n_P \neq 0\}$.

Definició 1.15.

1) Funció racional sobre E: funció del tipus $f(x,y) = \frac{F_1(x,i)}{F_2(x,i)}$ amb F_1,F_2 polinomis definits mòdul l'equació de la corba E.

2) Un punt P es diu zero de f si $f(P) = 0$ i pol de f si f no està definit en P (o sigui, $F_2(P) = 0$) i, en aquest cas, s'escriu (per conveni) $f(P) = \infty$.

3) Associat amb una funció f sempre tenim un divisor $div(f) = \sum ord_P(f)(P)$ en què

i) $ord_P(f) = 0$ si $f(P) \neq 0,\infty$

ii) $ord_P(f) = n \geq 1$ si té un zero amb multiplicitat (o ordre) n.

iii) $ord_P(f) = -n\ (n \geq 1)$ si té un pol amb multiplicitat n.

4) Els divisors de funcions racionals s'anomenen *divisors principals*.

5) Dos divisors D,D' es diuen *equivalents* si es diferencien en un divisor principal, és a dir: $D = D' + div(f)$.

6) Sigui f una funció i $D = \sum_{P\in E} n_P(P)$ un divisor. Es defineix $f(D) = \prod f(P)^{n_P}$.

Observació

Encara que la grafia és semblant convé no confondre el punt neutre de la corba el·líptica, O (l'únic punt de l'infinit de la corba) amb 0, element neutre del cos K sobre el qual està definida la corba, ni amb l'element neutre (O) del grup de divisors.

Proposició 1.16.

1) Un divisor principal té grau zero. Com a conseqüència, dos divisors equivalents tenen igual grau.

2) Un divisor amb grau zero no és necessàriament principal, però admet una expressió en *forma canònica*: $D = (P) - (O) + div(f)$, amb P únic.

3) Donats $D_i = (P_i) - (O) + div(f_i)$, $i = 1,2$, divisors de grau 0, però no principals (per tant, $P_i \neq O$), la forma canònica de la seva suma és

$$D = D_1 + D_2 = (P_3) - (O) + div(f_1 f_2 f_3) \qquad (6)$$

en què $P_3 = P_1 + P_2$ i $f_3 = s/v$ amb s equació de la recta secant que uneix P_1, P_2 (tangent a la corba si $P_1 = P_2$) i v equació de la recta vertical que uneix P_3 amb el punt de l'infinit O (si $P_3 = O$ llavors $v = 1$).

4) Un divisor $D = \sum n_P(P)$ és principal si i només si $\sum n_P = 0$ i $\sum n_P P = 0$ (en l'última expressió la suma indica la suma de punts en la corba el·líptica).

Exemple 1.5

Sigui la corba el·líptica $E : y^2 = x^3 + x + 4$ definida sobre el cos finit $\mathbb{F}_7$.

1) Sigui la recta $r : y = 2x + 2$. Determineu el divisor principal $div(r)$:

El divisor de r és la combinació lineal formal dels zeros i pols de la recta en els punts de la corba el·líptica, contats amb les seves multiplicitats.

Per a calcular els zeros fem la intersecció de E i r: substituint $y = 2x + 2$ en l'equació de E s'obté l'equació $x^3 - 4x^2 = 0$. Aquesta equació té l'arrel doble $x = 0$ i l'arrel simple $x = 4$. Els zeros són, doncs, els punts $(0,2)$, amb multiplicitat 2 (es pot comprovar que la recta és tangent a la corba en aquest punt) i $(4,3)$ amb multiplicitat 1.

En virtut de la proposició 1.16 $div(r)$ ha de tenir grau 0. Com que hi ha 3 zeros (comptats amb les seves multiplicitats), han d'existir tres pols. Veiem que en els punts afins de E, la recta r no té pols, i per tant aquests han d'estar en el punt de l'infinit $O = (0 : 1 : 0)$ de la corba, punt que serà, doncs, un pol d'ordre 3.

Noteu que si s'escriu l'equació de E en coordenades projectives, $y^2 z = x^3 + xz^2 + 4z^3$, fent $z = 0$, tenim $x^3 = 0$, que és de grau 3. Per tant,

$$div(r) = 2(0,2) + 1(4,3) - 3(O).$$

2) Sigui el divisor $D = 1(0,2) + 1(0,5) + (-2)(6,3)$. Aquest divisor té grau $1 + 1 - 2 = 0$. No obstant això, no és un divisor principal: en efecte, d'acord amb la proposició 1.16, si ho fos hauria de tenir grau 0, condició que verifica; però, a més a més, la suma en E dels punts del divisor hauria de donar el punt de l'infinit O. Nogensmenys, utilitzant les fórmules d'addició,

$$(0,2) + (0,5) - 2(6,3) = O - 2(6,3) = 2(6,4) = (4,4).$$

Vegeu també

Les fórmules d'addició s'estudien al mòdul "Criptografia amb corbes el·líptiques" d'aquesta assignatura.

Estem ja en disposició de definir l'element $e_l(P,Q)$.

Definició 1.17. Donats $P,Q \in E[l]$ triem A,B divisors de grau zero amb suports disjunts i tals que:

$$A \sim (P) - (0), \quad B \sim (Q) - (O)$$

Siguin f_A,f_B funcions sobre E tals que,

$$div(f_A) = lA, \qquad div(f_B) = lB.$$

Llavors definim:

$$e_l(P,Q) = f_A(B)/f_B(A) \tag{7}$$

A partir d'aquesta definició es dedueixen les propietats del *pairing* enunciades en 1.11*.

* Per a la demostració, vegeu J. H. Silverman (1986). *The Arithmetic of Elliptic Curves.* Springer-Verlag.

Observeu que els divisors A,B han de ser disjunts perquè $f_A(B),f_B(A)$ estiguin ben definits. Una manera d'obtenir-los és prendre un punt $S \in E$ amb $S \neq O,P,-Q,P-Q$ i $A = (P+S) - (S)$; $B = (Q-S) - (-S)$. Llavors

$$e_l(P,Q) = f_A((Q-S) - (-S))/f_B((P+S) - (S)) = \frac{f_A(Q-S)f_B(S)}{f_A(-S)f_B(P+S)} \tag{8}$$

El càlcul del *pairing* es redueix, doncs, a avaluar certes funcions en certs divisors. El problema és el còmput de tals funcions f_A,f_B. Aquesta computació es pot fer eficientment utilitzant l'algorisme següent*. Aquest algorisme també permet la computació del *pairing* de Tate.

* Vegeu A. Menezes (1993). *Elliptic Curves Public Key Cryptography.* Kluwer

1.3.2. L'algorisme de Miller

Algorisme 1.18 (Algorisme de Miller)

input: $D = \sum_{i=1}^{r} n_i(P_i)$ un divisor principal.

output: una funció f tal que $D = div(f)$

1) Com que D té grau 0 es pot escriure: $D = \sum_{i=1}^{r} n_i((P_i) - (O))$

2) Per a cada i obtenim la forma canònica $(P_i') - (O) + div(f_i)$, del divisor $n_i((P_i) - (O))$ de la manera següent:

i) Sigui $b_{d-1}b_{d-2}\cdots b_1b_0$ l'expressió binària de n_i (en què b_0 són les unitats i $b_{d-1} = 1$), $R := P_i$; $f_i := 1$.

ii) El mètode per a sumar divisors canònics especificat en l'equació 6 proporciona per a $i = b_{d-2}, \ldots, 0$:

a) $f_i := f_i^2 g_{RR}$; $R := 2R$

b) Si $b_i = 1$, $f_i := f_i g_{RP_i}$, $R := R + P_i$

c) *output* f_i.

en què, donats els dos punts R,S, g_{RS} és la funció tal que $div(g_{RS}) = (R) + (S) - (R + S) - (O)$.

3) Sumant els divisors canònics anteriors s'obté la funció buscada f.

Exemple 1.6

Agafem la corba el·líptica de l'exemple 1.4, $E : y^2 = x^3 + 7x$, definida sobre el cos $\mathbb{F}_{13}$, i els punts de E: $P = (3,3)$, $Q = (4,1)$ tots dos punts de 3-torsió. L'algorisme de Miller permet obtenir

L'exemple 1.6 es deu a A. Menezes (1993). *Elliptic Curves Public Key Cryptography*. Kluwer

$$f_A = \frac{(8x + y)(x + y + 1)(x + 4)}{(x + 3)(11x + y)(8x + y + 11)}, \tag{9}$$

$$f_B = \frac{(3x + y)(x + y + 10)}{(10x + y)(12x + y + 3)} \tag{10}$$

i, finalment, $e_3(P,Q) = 9$.

1.4. Grau d'immersió

Suposem $K = \mathbb{F}_q$, un cos finit amb q elements. Vegem que el grup d'arribada μ_l del *pairing* e_l es pot considerar contingut en una extensió $\mathbb{F}_{q^k}$ per a algun valor (mínim) k.

Lema 1.19. Existeix un nombre natural k (de fet, es pot agafar $1 \leq k \leq l-1$), tal que el grup multiplicatiu $(\mathbb{F}_{q^k})^*$ conté un subgrup isomorf a μ_l.

Demostració: El grup $(\mathbb{F}_{q^k})^*$ és cíclic, amb cardinal $q^k - 1$. Aquest grup conté un subgrup de cardinal l si i només si $l|(q^k - 1)$, és a dir, $q^k \equiv 1 \pmod{l}$. Ara bé, per hipòtesis, $mcd(q,l) = 1$ i, per tant, $q \in (\mathbb{Z}/l\mathbb{Z})^*$, subgrup d'elements invertibles de $\mathbb{Z}/l\mathbb{Z}$. L'ordre k de q en aquest grup serà una solució del problema. ∎

Definició 1.20. El mínim valor k que verifica el lema 1.19 es diu *grau d'immersió*.

El valor del grau d'immersió serà crucial per als atacs al logaritme discret el·líptic, objecte de l'apartat següent. Recordeu que, en virtut del teorema de Hasse el cardinal d'una corba el·líptica E està determinat per $\#E = q+1-t$, amb $|t| \leq 2\sqrt{q}$. En les aplicacions criptogràfiques basades en el logaritme discret el·líptic s'utilitza un subgrup cíclic, del major ordre possible (i amb preferència primer), $\langle P \rangle \subseteq E$, l'ordre l del qual, serà, doncs, un divisor de $\#E$.

Per a les corbes el·líptiques ordinàries el grau d'immersió és, en general, molt gran (exponencial en $\log(q)$, segons varen demostrar Koblitz i Balasubramanian, 1998). Nogensmenys, Menezes, Okamoto i Vanstone varen mostrar que per a les corbes supersingulars aquest grau és petit; de fet, $k \leq 6$*.

Recordeu, tal com s'ha vist al mòdul "Criptografia amb corbes el·líptiques", que una corba el·líptica amb cardinal $q + 1 - t$ es diu *supersingular* si la característica p del cos divideix t. En altre cas la corba s'anomena *ordinària*.

Per a demostrar aquest resultat Menezes, Okamoto i Vanstone es basen en la proposició següent.

Proposició 1.21. Les corbes el·líptiques supersingulars definides sobre el cos finit $\mathbb{F}_q$, $q = p^m$ i amb cardinal $q + 1 - t$ es classifiquen en els sis tipus següents:

Tipus I) $t = 0$ i $E(\mathbb{F}_q) \simeq \mathbb{Z}/(q+1)\mathbb{Z}$.

Tipus II) $q \equiv 3 \pmod{4}$, $t = 0$ i $E(\mathbb{F}_q) \simeq \mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Tipus III) m parell, $t^2 = q$, i $E(\mathbb{F}_q)$ cíclic.

Tipus IV) $p = 2$, m imparell, $t^2 = 2q$ i $E(\mathbb{F}_q)$ cíclic.

Tipus V) $p = 3$, m imparell, $t^2 = 3q$ i $E(\mathbb{F}_q)$ cíclic.

Tipus VI) m parell, $t^2 = 4q$ i $E(\mathbb{F}_q) \simeq \mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z}$.

Observació

El cardinal del grup $(\mathbb{Z}/l\mathbb{Z})^*$, igual al nombre d'elements no nuls en $\mathbb{Z}/l\mathbb{Z}$ coprimers amb l, s'anomena *funció d'Euler* $\varphi(l)$. En particular, si l és primer tenim $\varphi(l) = l - 1$. L'ordre multiplicatiu k del cardinal q del cos $\mathbb{F}_q$ és sempre un divisor de $\varphi(l)$.

Vegeu també

La funció d'Euler s'estudia al mòdul "Cossos finits" d'aquesta assignatura.

Vegeu també

El teorema de Hasse s'estudia al mòdul "Criptografia amb corbes el·líptiques".

*** Vegeu A. Menezes (1993). *Elliptic Curves Public Key Cryptography*. Kluwer.**

A partir de la classificació de la proposició 1.21 és un simple exercici obtenir els graus d'immersió k per a cadascun dels tipus, si (com és habitual) es pren $l = n_1$ cardinal del subgrup cíclic maximal de E. Així, per exemple, per a les corbes del tipus I, amb $q+1$ elements, és obvi que q^2-1 és múltiple de $q+1$ i per tant, el grau d'immersió d'aquestes corbes és $k = 2$. Els resultats es recullen en la taula següent.

Tipus	t	n_1	k
I	0	$q+1$	2
II	0	$(q+1)/2$	2
III	$\pm\sqrt{q}$	$q+1\mp\sqrt{q}$	3
IV	$\pm\sqrt{2q}$	$q+1\mp\sqrt{2q}$	4
V	$\pm\sqrt{3q}$	$q+1\mp\sqrt{3q}$	6
VI	$\pm 2\sqrt{q}$	$\sqrt{q}\mp 1$	1

2. Atacs basats en *pairings*

Els *pairings* permeten un tipus d'atac al logaritme discret el·líptic, els anomenats *algorismes de reducció*. Així, Menezes, Okamoto i Vanstone (1993), mostren com traslladar, utilitzant el *pairing* de Weil, aquest logaritme definit sobre una corba el·líptica sobre el cos finit $\mathbb{F}_q$ al logaritme discret sobre $\mathbb{F}_{q^k}$, amb k el grau d'immersió.

Referència bibliogràfica

Menezes, Okamoto i Vanstone (1993). "Reducing elliptic curves logarithms to a finite field". *IEEE Trans. Info. Theory* (vol. 39, pàg. 1639-1646).

Agafem $\langle P\rangle \subseteq E(\mathbb{F}q)$ el grup subjacent al logaritme discret el·líptic, subgrup d'ordre l primer amb la característica p i denotem $\mu_l \subset \mathbb{F}_{q^k}$. L'atac de Menezes, Okamoto i Vanstone (MOV) està determinat per l'algorisme següent.

Algorisme 2.1 (Atac MOV).

Input: $P, R \in \langle P\rangle$, $R \neq 0$.

Output: m, $0 < m < l$, $mP = R$.

1) Trobar el menor k tal que $\mu_l \subset \mathbb{F}_{q^k}$.

2) Trobar Q tal que $\alpha = e_l(P,Q)$ tingui ordre l.

3) Calcular $\beta = e_l(R,Q)$.

4) Calcular m, el logaritme de β en la base α, en $\mathbb{F}_{q^k}$.

5) Retornar m.

Exemple 2.1

Per a la corba de l'exemple 1.6 sobre $\mathbb{F}_q = 13$ sigui el punt $R = (3,10) \in \langle P\rangle$. Com que $l = 3$ i $\mu_3 \subset \mathbb{F}_{13}$ el grau d'immersió és 1.

El punt $Q = (4,1)$ verifica que $\alpha = e_3(P,Q) = 9$ i té ordre 3 (mod 13). Obtenim $\beta = e_3(R,Q) = 3$. Com que $9^2 \equiv 3 \pmod{13}$ tenim que $\log_P(R) = 2$, és a dir, $R = 2P$.

Lectura recomanada

Vegeu-ne els detalls de l'exemple 2.1 a A. Menezes (1993). *Elliptic Curves Public Key Cryptography*. Kluwer, i també un dels exercicis al final del mòdul.

La utilitat de l'algorisme MOV depèn fortament del valor de k: recordem que el logaritme discret clàssic sobre el grup multiplicatiu $(\mathbb{F}_{q^k})^*$ es sensible a l'anomenat *index calculus*, mentre que el logaritme discret el·líptic és immune a aquest, fet que possibilita emprar claus molt menors. Així, claus de 163 bits en el cas el·líptic ofereixen la mateixa seguretat que claus de 1.024 bits en el cas clàssic.

Vegeu també

El logaritme discret clàssic sobre el grup multiplicatiu s'estudia al mòdul "Elements de criptografia".

Ara bé, el que fa l'algorisme MOV és traslladar el problema en una corba el·líptica sobre el cos $\mathbb{F}_q$ a un problema similar en $\mathbb{F}_{q^k}$. La longitud binària

de q^k és k vegades la longitud binària de q, i per tant per a k gran la mida del cos $\mathbb{F}_{q^k}$ fa ineficaç els atacs basats en l'*index calculus*. No obstant això, com ja hem vist abans, per a corbes supersingulars el valor de k és, a tot, estirar, 6. En aquest cas, corresponent a corbes del tipus V en la proposició 1.21, per a cossos de longitud $q = 163$ bits, tenim que q^6 té longitud 978, per la qual cosa la seguretat és equiparable al cas clàssic amb longitud de clau 1.024. I per descomptat, per a corbes del tipus VI en la proposició 1.21, la seguretat és la mateixa que en el cas clàssic sobre el cos base, cas que, per a longitud 163, es considera actualment molt vulnerable a l'*index calculus*.

Com a conseqüència, les corbes supersingulars no són adequades per a criptosistemes i protocols basats en el logaritme discret el·líptic.

Dues observacions abans d'acabar:

- Frey i Ruck (1994) van proposar un atac similar al de MOV utilitzant el *pairing* de Weil. Kanayama, Kobayashi, Saito i Uchiyama (2000) van provar que si l no és un divisor de $q-1$, els algorismes MOV i Frey-Ruck són equivalents; no obstant això, per a corbes amb cardinal $q-1$, l'algorisme de Frey-Ruck és més eficient.

- Per a les anomenades *corbes anòmales*, corbes definides sobre un cos primer $\mathbb{F}_p$ i amb cardinal p, hi ha un altre algorisme de reducció degut a Semaev, Smart, Satoh i Araki (vegeu l'obra de Blake i altres (2000)).

Lectura recomanada

Frey i Ruck (1994). "A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves". *Mathematics of Computation* (vol. 62, pàg. 865-874) .

3. Criptografia basada en la identitat

Una de les motivacions de Diffie i Hellman per a la seva introducció de la criptografia de clau pública va ser el problema de la distribució de claus (la signatura digital n'és una altra motivació). L'augment del nombre d'usuaris dels sistemes criptogràfics,en afegir-se nous actors als clàssics (governamentals i militars), va fer que potencialment cada dos de tals usuaris A,B necessitessin en algun moment comunicar-se de manera segura, cosa que, utilitzant un sistema de clau privada, exigia una clau compartida K_{AB}. La manera de fer arribar aquesta clau a tots dos usuaris plantejava un problema de *gestió i distribució de claus*.

Vegeu també

La criptografia de clau pública s'estudia al mòdul "Elements de criptografia" d'aquesta assignatura.

La criptografia de clau pública va proporcionar un sistema eficient de resoldre tal distribució de claus, ja que l'enviament de K_{AB} es pot fer de manera segura, per mitjà d'un canal insegur, utilitzant les claus públiques de A i B. De fet, actualment, els sistemes de clau pública s'utilitzen principalment per a la distribució de claus de comunicacions d'un sistema privat.

No obstant això, aviat es va fer palès un nou problema: una clau pública que ens fan arribar com a pertanyent a A pot en realitat pertànyer a un atacant C. Això obliga a garantir l'autenticitat de les claus públiques mitjançant un sistema de certificats i d'autoritats de certificació, cosa que genera una enutjosa infraestructura de clau pública (PKI).

Vegeu també

La infraestructura de clau pública (PKI) s'estudia al mòdul "Elements de criptografia" d'aquesta assignatura.

Un paradigma alternatiu va ser proposat el 1984 per A. Shamir (1994). La idea era poder utilitzar, de manera segura, claus públiques derivades de la identitat mateixa de l'usuari (d'això ve el nom de *criptografia basada en la identitat*). Shamir mateix va construir un esquema de distribució de claus basat en aquesta idea, però no obstant això, una solució satisfactòria a la idea dels criptosistemes basats en la identitat només es va aconseguir amb la utilització de *pairings*. Aquest mètode es coneix també com a *criptografia basada en pairings*.

Referència bibliogràfica

A. Shamir (1994). "Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology. Proceedings of Crypto'84". *Lecture Notes in Computer Science*, núm. 7, pàgs. 47-53.

La criptografia basada en la identitat implica l'existència d'una certa *autoritat de confiança* (AC), que selecciona els paràmetres comuns a tots els participants i els proporciona unes certes claus privades (claus que poden ser generades només quan l'usuari les necessita, cosa que evita l'emmagatzematge i redueix el risc d'escletxes de seguretat). En el que segueix, suposarem que la AC ha seleccionat i fet públics almenys una corba el·líptica E sobre un cos finit $\mathbb{F}_q$, un punt $P \in E$ d'ordre primer l, una aplicació distorsió ϕ i el corresponent *pairing* modificat $\hat{e}_l$. Així mateix l'AC ha triat una certa clau secreta pròpia $s, 1 < s < l$, que li servirà tant per a generar la seva clau pública, com les claus privades dels participants.

En el que segueix exposarem alguns dels mètodes bàsics d'aquesta criptografia per a l'intercanvi de claus, criptosistemes i signatura digital.

Lectura recomanada

Per a més detalls sobre la criptografia basada en la identitat, vegeu l'obra de Blake i altres (2005) i la de Luther (2008).

3.1. Intercanvi de claus en criptografia basada en la identitat

Com s'ha dit, una de les motivacions per a la introducció de la clau pública va ser el problema de la distribució de claus. De fet, Diffie i Hellman proposen un sistema bipartit per a acordar una clau comuna entre dos participants A,B: fixat un grup cíclic convenient $\langle g\rangle$ (per exemple, $\mathbb{F}_q^*$, el grup cíclic multiplicatiu d'un cos finit), A i B trien separadament nombres aleatoris n_A,n_B; $1 < n_A,n_B < l$, calculen els elements del grup g^{n_A}, g^{n_B} i s'intercanvien aquests valors.

Tant A com B poden llavors calcular la clau comuna $K_{AB} = g^{n_A n_B}$. La seguretat del mètode consisteix que un atacant, interceptant g^{n_A},g^{n_B}, per a poder conèixer la clau es veuria enfrontat al problema següent.

Definició 3.1 (Problema computacional de Diffie-Hellman).

Coneguts g^{n_A},g^{n_B} calcular $g^{n_A n_B}$.

La dificultat del problema computacional de Diffie-Hellman es considera equivalent a la del logaritme discret en el mateix grup. Per descomptat, si un adversari pogués resoldre el problema del logaritme discret podria obtenir n_A,n_B i calcular $g^{n_A n_B}$.

Un esquema semblant es pot formular en la criptografia basada en la identitat, utilitzant *pairings* i la identitat Id_A de cada usuari A (el nom o qualsevol altra informació personal, com l'adreça electrònica, una foto digital, o qualsevol seqüència binària seleccionada per A). A més a més, en aquest tipus de criptografia, hi ha la possibilitat d'un protocol d'acord tripartit de claus. Vegem aquests dos algorismes.

3.1.1. Acord bipartit de claus

En aquest esquema se suposa que l'AC ha triat i fet públic, a més a més de les dades referides a la corba el·líptica i el *pairing*, una funció resum h que transforma qualsevol seqüència binària en un punt de $\langle P\rangle$. L'esquema d'acord bipartit de claus ve donat per l'algorisme següent.

Vegeu també

La funció resum s'estudia al mòdul "Elements de criptografia" d'aquesta assignatura.

Algorisme 3.2.

- **Claus privades de *A* i *B***: sol·licitud prèvia de A, i B, a l'AC, aquesta

1) calcula i envia a A el punt $S_A = sP_A \in \langle P \rangle$, en què $P_A = h(Id_A)$,
2) calcula i envia a B el punt $S_B = sP_B \in \langle P \rangle$, en què $P_B = h(Id_B)$.

- **Acord de clau**: els participants A i B calculen,

1) A, utilitzant la seva clau privada S_A i P_B (que pot calcular, ja que tant la identitat Id_B com la funció resum h són públiques), obté

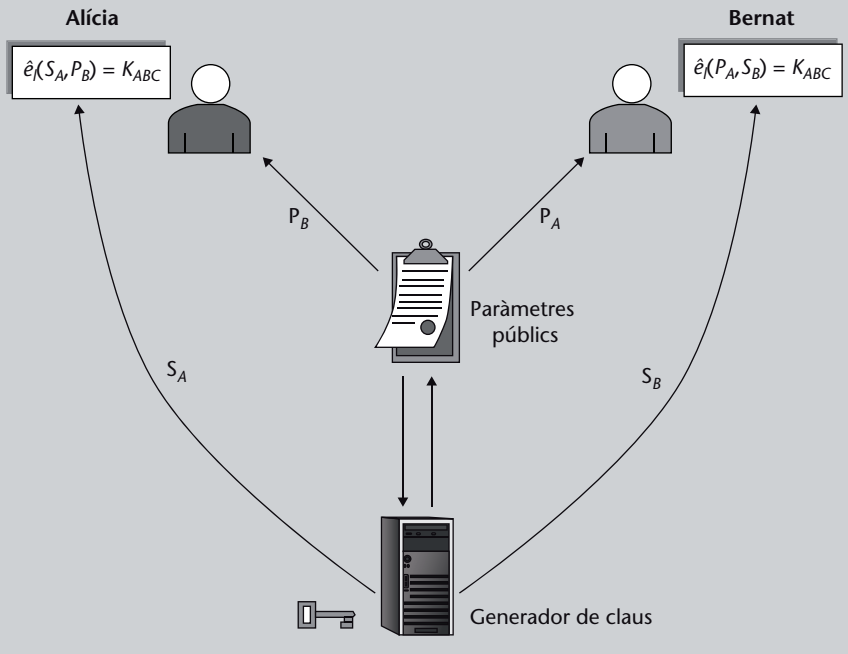
$$\hat{e}_l(S_A,P_B) = \hat{e}_l(sP_A,P_B) = \hat{e}_l(P_A,P_B)^s \in \mu_l. \quad (11)$$

2) B, utilitzant la seva la seva clau privada S_B i P_A obté

$$\hat{e}_l(P_A,S_B) = \hat{e}_l(P_A,sP_B) = \hat{e}_l(P_A,P_B)^s \in \mu_l. \quad (12)$$

3) La clau comuna és $K_{AB} = \hat{e}_l(S_A,P_B) = \hat{e}_l(P_A,S_B)$.

Acord bipartit de claus



3.1.2. Acord tripartit de claus

El protocol següent, proposat per A. Joux (2000), permet l'acord d'una clau comuna entre tres entitats A,B,C. Aquest acord que, a diferència de l'ante-

Lectura recomanada

A. Joux (2000). "A one round protocol for tripartite Diffie-Hellmann". *LNCS* (vol. 1838, pàg. 385-394).

rior, no necessita claus secretes dels participants, ve donat per l'algorisme següent.

Algorisme 3.3.

- **Intercanvi de missatges**: Els participants A,B,C

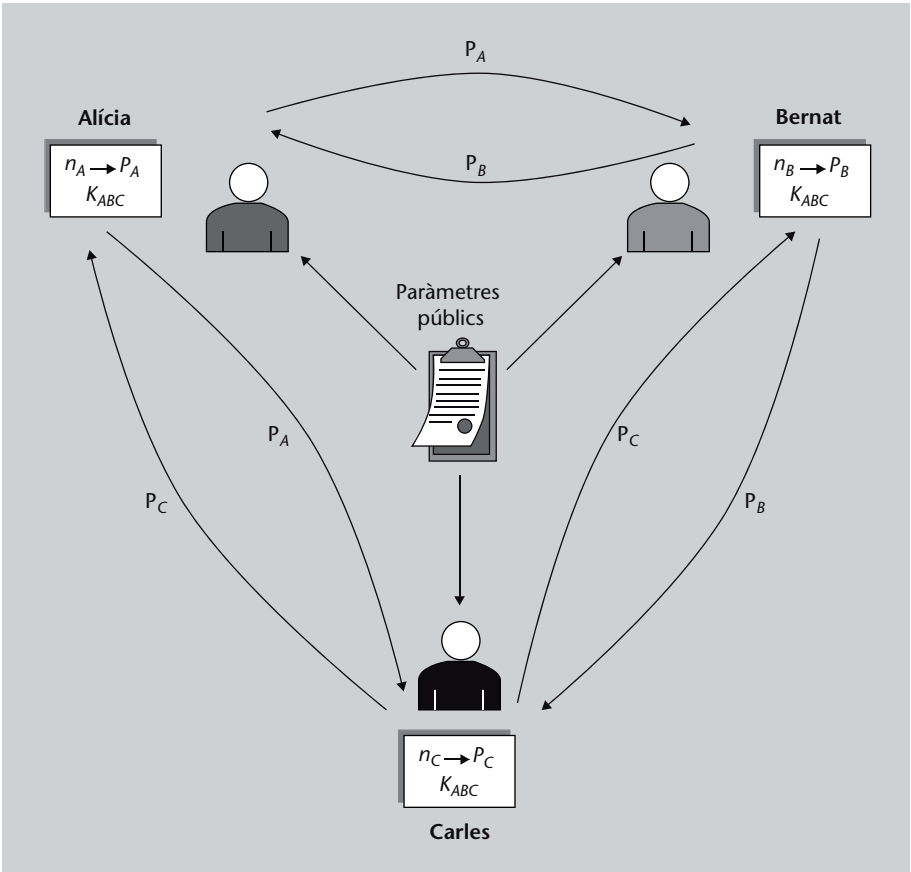
1) A pren un nombre aleatori n_A; $1 < n_A < l$ i calcula $P_A = n_A P$
2) B pren un nombre aleatori n_B; $1 < n_B < l$ i calcula $P_B = n_B P$
3) C pren un nombre aleatori n_C; $1 < n_C < l$ i calcula $P_C = n_C P$
4) A,B,C intercanvien els valors de P_A,P_B,P_C

- **Acord de claus**: els participants calculen la clau comuna,

1) $\hat{e}_l(P_B,P_C)^{n_A} = \hat{e}_l(P,P)^{n_A n_B n_C} = K_{ABC}$
2) $\hat{e}_l(P_A,P_C)^{n_B} = \hat{e}_l(P,P)^{n_A n_B n_C} = K_{ABC}$
3) $\hat{e}_l(P_A,P_B)^{n_C} = \hat{e}_l(P,P)^{n_A n_B n_C} = K_{ABC}$

Resumim el protocol de Joux en el diagrama següent.

Acord tripartit de Joux



Si la seguretat de l'esquema clàssic de Diffie-Hellman es basa en el problema computacional de Diffie-Hellman, l'acord tripartit descansa en la suposada intractabilitat de la variant següent.

Definició 3.4 (Problema bilineal de Diffie-Hellman).

Coneguts n_AP, n_BP, n_CP, calcular $\hat{e}_l(P,P)^{n_An_Bn_C}$.

Exemple 3.1

Sigui $q = 1303$ i la corba el·líptica $E : y^2 = x^3 + x$ sobre $\mathbb{F}_q$. El punt $P = (334,920) \in E$ té ordre primer $l = 163$. L'aplicació distorsió $\phi : (x,y) \to (-x,iy)$ en què $i \in \mathbb{F}_{q^2}$ és tal que $i^2 = -1$ proporciona el *pairing* modificat $\hat{e}_{163}$.*

Siguin les eleccions de A,B,C:

1) $n_A = 71$. A calcula i fa públic $P_A = (1279,1171)$.

2) $n_B = 3$. B calcula i fa públic $P_B = (872,515)$

3) $n_C = 126$. C calcula i fa públic $P_C = (196,815)$

Els tres participants poden calcular ara la clau comuna (per als càlculs tingueu en compte que $i^2 = -1$ i reduïu totes les operacions mòdul 1303):

1) $\hat{e}_l(P_B,P_C)^{71} = (172 + 256i)^{71} = 768 + 662i$

2) $\hat{e}_l(P_A,P_C)^3 = (1227 + 206i)^3 = 768 + 662i$

3) $\hat{e}_l(P_A,P_B)^{126} = (282 + 173i)^{126} = 768 + 662i$

Lectura recomanada

L'exemple 3.1 es pot trobar a J. Hoffstein; J. Pipher; J. Silverman (2008). *An Introduction to Mathematical Cryptography*. Springer.

*** Vegeu els exercicis del final del mòdul**

3.2. Xifratge basat en la identitat

Un sistema criptogràfic efectiu, basat en la idea de Shamir d'emprar la identitat d'un usuari com la seva clau pública, va ser proposat per Boneh i Franklin (2001). En realitat aquests autors proposen dues versions. Vegem en primer lloc la versió que anomenen *bàsica*.

Lectura recomanada

Boneh i Franklin (2001). "Identity based encryption from the Weil pairing". *LNCS* (vol. 2139, pàg. 213-229).

Algorisme 3.5. **(Esquema bàsic de Boneh i Franklin)**

- **Paràmetres**: els missatges en clar M seran elements del conjunt $\mathcal{M}$ de seqüències binàries d'una longitud prefixada n, és a dir, $\mathcal{M} = \{0,1\}^n$. A més a més, dels paràmetres abans esmentats amb caràcter general, l'autoritat de confiança (AC),

1) crea i envia als participants la seu clau pública pròpia $P_{AC} = sP$,

2) tria una funció resum h_1 que permet assignar a la identitat de cada usuari A una clau pública $P_A = h_1(Id_A) \in \langle P \rangle$,

3) tria una funció resum $h_2 : \mu_l \to \mathcal{M}$,

4) calcula la clau privada de cada participant $S_A = sP_A$.

- **Xifratge**: si B vol enviar a A un missatge $M \in \mathcal{M}$,

1) calcula $P_A = h_1(Id_A)$ (tant h_1 com Id_A són coneguts),

2) pren, aleatòriament, r, $1 < r < l$ i calcula:

$$C_1 = rP, \qquad C_2 = M \oplus h_2(\hat{e}_l(P_A, P_{AC})^r) \tag{13}$$

(on $\bigoplus$ indica la summa bit per bit (o sigui, XOR) de totes dues seqüències binàries).

3) B envia a A la parella $C = (C_1, C_2)$.

- **Desxifratge**: quan A rep el missatge xifrat $C = (C_1, C_2)$,

1) calcula

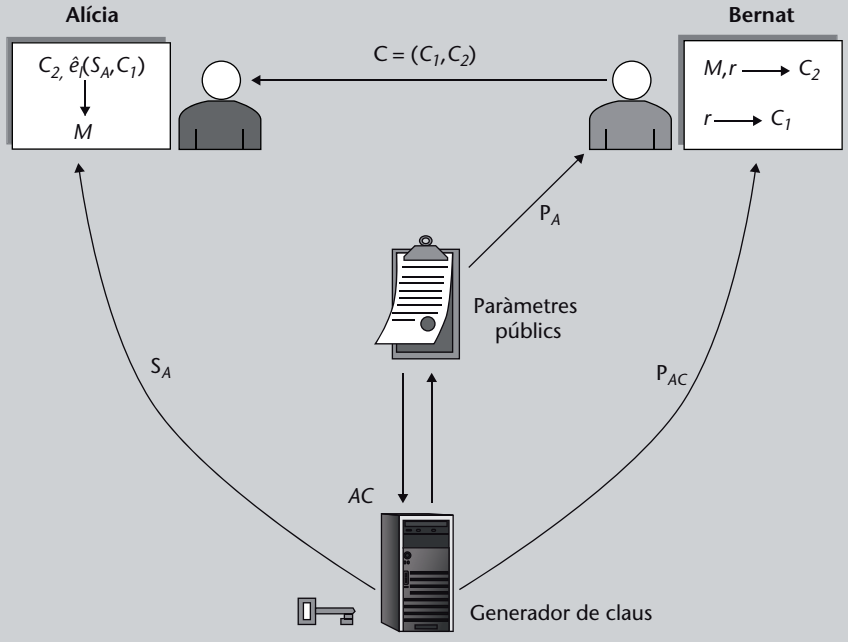
$$\hat{e}_l(S_A, C_1) = \hat{e}_l(sP_A, rP) = \hat{e}_l(P_A, P)^{rs} = \hat{e}_l(P_A, sP)^r = \hat{e}_l(P_A, P_{AC})^r, \tag{14}$$

2) calcula

$$C_2 \oplus h_2(\hat{e}_l(S_A, C_1)) = M \oplus h_2(\hat{e}_l(P_A, P_{AC}))^r \oplus h_2(\hat{e}_l(P_A, P_{AC}))^r = M. \tag{15}$$

L'esquema següent il·lustra l'esquema bàsic de Boneh i Franklin.

Xifratge bàsic de Boneh-Franklin



Observació

S'ha d'assenyalar la similitud formal entre la versió bàsica del criptosistema de Boneh-Franklin i el criptosistema ElGamal: en tots dos el xifratge és per una parella, un component de la qual és el producte o potència del generador i un nombre aleatori, mentre que l'altre component inclou el missatge en clar com a sumand o factor.

Boneh i Franklin consideren que el seu esquema bàsic no reuneix les garanties suficients de seguretat, i proposen un altre esquema *complet*.

Algorisme 3.6.

- **Paràmetres**: a més a més dels paràmetres de l'esquema bàsic anterior, es consideren dues funcions resum addicionals:

1) $h_3 : \{0,1\}^{2n} \to \{r;\ \ 1 < r < l\}$
2) $h_4 : \{0,1\}^n \to \{0,1\}^n$

- **Xifratge**: si B vol enviar a A un missatge $M \in \mathcal{M}$,

1) calcula $P_A = h_1(Id_A)$,
2) pren $S \in \{0,1\}^n$ aleatòriament,
3) calcula $r = h_3(S,M)$,
4) calcula $C = (C_1,C_2,C_3)$ en què,

$$C_1 = rP, \qquad C_2 = S \oplus h_2(\hat{e}_l(P_A,P_{AC})^r), \qquad C_3 = M \oplus h_4(S). \tag{16}$$

- **Desxifratge**: quan A rep el missatge xifrat $C = (C_1,C_2,C_3)$,

1) calcula $S' = C_2 \oplus h_2(\hat{e}_l(S_A,C_1))$,
2) calcula $M' = C_3 \oplus h_4(S')$,
3) calcula $r' = h_3(S',M')$.
4) Si $C_1 = r'P$, A accepta com a vàlid M' (= M). En cas contrari rebutja el missatge rebut.

La seguretat del model complet de Boneh i Franklin es considera equiparable a la del problema bilineal de Diffie-Hellman.

Lectura recomanada

Per a una anàlisi de la seguretat del model complet de Boneh i Franklin, vegeu l'obra de Blake i altres (2005) i la de Luther (2008).

3.3. Esquemes de signatura basats en la identitat

La infraestructura basada en la identitat de l'esquema de xifratge de Boneh-Franklin es pot adaptar també al procés de signatura digital. Recordem que la signatura digital d'un missatge M és l'anàleg electrònic de la signatura ordinària (amb la diferència que la signatura electrònica depèn del missatge concret M), ja que permet demostrar, fins i tot amb valor legal, la identitat de qui ha produït la signatura de M, i l'intent de falsificar aquesta signatura per part d'un adversari és computacionalment difícil.

Vegeu també

La signatura digital d'un missatge s'estudia al mòdul "Elements de criptografia" d'aquesta assignatura.

Un esquema de signatura digital comporta sempre dos algorismes.

Definició 3.7.

1) **Algorisme de signatura**: implica un còmput en el qual intervé el missatge M i la clau privada del signant (la qual, en el cas de la criptografia de clau pública clàssica haurà estat triada per ell mateix i, en el cas de la criptografia basada en la identitat, li ha de ser proporcionada per l'AC) i una certa funció resum. Aquest còmput produeix un resultat $F(M)$.

2) **Algorisme de verificació**: rebut com a *input* el missatge M i la seva signatura $F(M)$, té com a *output* un dels dos valors següents: *signatura vàlida* o *signatura no vàlida*

Observem les següents característiques importants:

1) Certs tipus de signatures, *signatures amb recuperació del missatge*, recuperen M durant el procés de verificació. No obstant això, l'usual és que les signatures requereixin el missatge original (potser prèviament xifrat si en volem preservar el secret) per a la verificació: *signatures amb apèndix*.

2) En les signatures amb apèndix, l'ús d'una funció resum permet que el text per signar sigui petit. A més a més, la funció resum té un paper crucial en la seguretat de la signatura. (*hash-and-sign paradigm*).

3) Dues signatures del mateix missatge poden produir el mateix resultat, *signatures deterministes*, o bé,

4) La signatura pot dependre d'un valor aleatori, *signatures aleatòries* (per exemple, la signatura basada en ElGamal, la *digital signature standard* (DSA), etc.).

Vegeu també

Els diferents tipus de signatures s'estudien al mòdul "Elements de criptografia" d'aquesta assignatura.

L'algorisme següent esquematitza un exemple de signatura digital (aleatòria, amb apèndix, similar a la signatura d'ElGamal.

Algorisme 3.8.

- **Paràmetres**: els missatges $M \in \mathcal{M}$ seran seqüències binàries de longitud arbitrària. Com sempre, l'AC haurà seleccionat una corba el·líptica E, el punt base $P \in E$, d'ordre primer l, una aplicació distorsió ϕ i el corresponent *pairing* modificat $\hat{e}_l$, i també la seva clau secreta pròpia s, $1 < s < l$. A més a més, l'AC,

1) crea i envia als participants la seu clau pública pròpia $P_{AC} = sP$,

2) tria una funció resum h_1 que permet assignar a la identitat de cada usuari A una clau pública $P_A = h_1(Id_A) \in \langle P \rangle$,

3) tria una funció resum $h_2 : \mathcal{M} \times \langle P \rangle \to \{r;\ 1 < r < l\}$,

4) calcula la clau privada de cada participant $S_A = sP_A$.

- **Algorisme de signatura**: si A vol signar el missatge M, llavors

1) tria aleatòriament r; $1 < r < l$ i

2) calcula:

$$F_1 = rP_A; \quad h = h_2(M,F_1); \quad F_2 = (r+h)S_A. \tag{17}$$

3) La parella $F = (F_1,F_2)$ és la signatura de M.

- **Algorisme de verificació**: quan el verificador rep la parella (M,F),

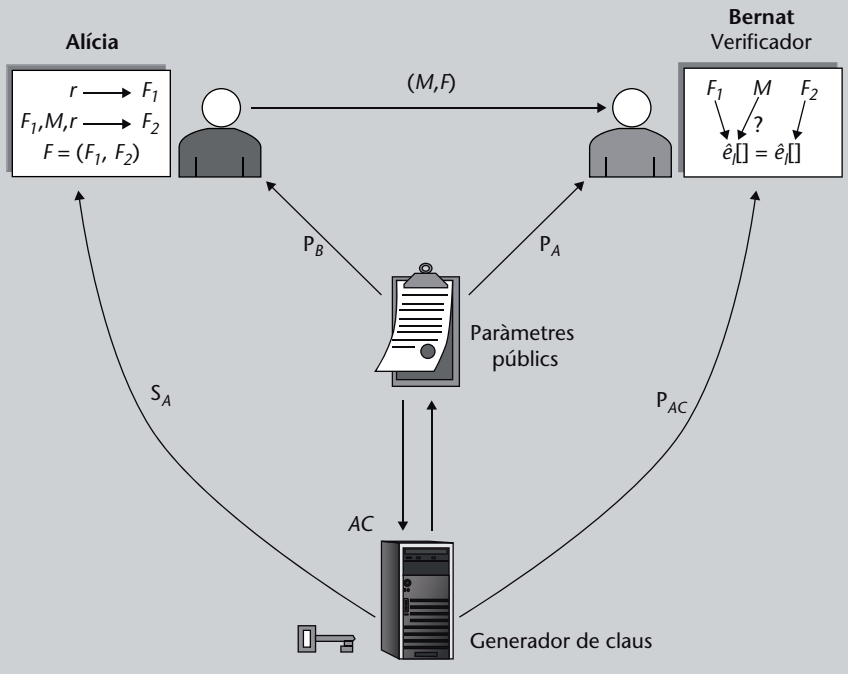
1) calcula si es verifica la igualtat següent

$$\hat{e}_l(P_{AC},F_1 + hP_A) = \hat{e}_l(P,F_2). \tag{18}$$

2) En cas afirmatiu accepta la signatura com a vàlida (un simple càlcul mostra que, si el procés s'ha fet correctament, s'ha de verificar tal igualtat).

Resumim l'esquema de signatura en el diagrama següent.

Signatura basada en la identitat



Igual que en la signatura basada en ElGamal es pot provar la seguretat existencial (un atacant no és capaç de crear una signatura que sigui acceptable com a vàlida per cap missatge) de la signatura descrita, també es pot provar en el model de seguretat denominat *random oracle model*.

L'esquema següent de signatura, degut a Boneh, Lynn i Shacham (2001), és especialment eficient i permet claus molt curtes.

Algorisme 3.9 (Signatura curta de BLS).

- **Paràmetres**: els missatges $M \in \mathcal{M}$ són seqüències binàries de longitud arbitrària. Com sempre, l'AC haurà seleccionat una corba el·líptica E, el punt base $P \in E$, d'ordre primer l, una aplicació distorsió ϕ i el corresponent *pairing* modificat $\hat{e}_l$. A més a més, haurà calculat

1) una funció resum $h : \mathcal{M} \to \langle P \rangle$,

2) una clau privada de cada participant n_A; $1 < n_A < l$ i pública $P_A = n_A P$.

- **Algorisme de signatura**: si A vol signar el missatge M calcula $F(M) = n_A h(M)$.

- **Algorisme de verificació**: quan el verificador rep el parell (M,F), accepta la signatura si i només si,

$$\hat{e}_l(F(M),P) = \hat{e}_l(h(M),P_A).$$

En aquest esquema el procés de signatura només requereix una funció resum i una multiplicació escalar, mentre que la verificació només necessita calcular dos *pairings*. Per altra banda, és possible l'ús de claus de longitud petita. Així, M. Barreto i altres (2002) han fet una implementació sobre el cos $\mathbb{F}_{3^{97}}$ amb longitud binària $\log_2(3^{97}) = 97 \log_2 3 \approx 154$ bits, que permet el mateix nivell de seguretat que el *digital signature algorithm* (DSA), el qual utilitza claus de 320 bits.

Models de seguretat

La seguretat d'un esquema criptogràfic es demostra en el context d'un *model de seguretat*. En el model estàndard es tracta de provar que trencar el sistema implica resoldre un problema matemàtic computacionalment intractable. El model *random oracle* demostra la seguretat assumint que les funcions resum utilitzades són realment funcions aleatòries.

Lectura recomanada

Boneh, Lynn i Shacham (2001). "Short signatures from the Weil pairings". *Asiacrypt 2001. LNCS* (vol. 2248, pàg. 514-532)

Lectura recomanada

M. Barreto i altres (2002). "Efficient algorithms for pairing-based cryptosystems". CRYPTO 2002. *LNCS* (vol. 2442, pàg. 354-368)

Exercicis d'autoavaluació

1. Sigui $\mathbb{F}_q$ el cos finit amb $q = p^n$ elements i sigui $Tr : \mathbb{F}_q \to \mathbb{F}_p$ l'aplicació traça. Sigui l'aplicació de dues variables, $T : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_p$, definida per $T(x,y) = Tr(xy)$. Demostreu:
a) T és una forma bilineal no degenerada (en l'espai vectorial $\mathbb{F}_q$, de dimensió n sobre el cos $\mathbb{F}_p$).
b) Suposem que n no és múltiple de la característica p. Llavors, T és no degenerada.

2. Sigui V un espai vectorial de dimensió n sobre un cos commutatiu K i $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ una base de V. Si $f : V \times V \to K$ és una forma bilineal simètrica s'anomena $Dis_{\mathcal{B}}(f)$, discriminant de f en la base $\mathcal{B}$, el determinant de la matriu $n \times n$: $(f(v_i, v_j))$. Demostreu:
a) Si el discriminant de f és nul (respectivament, no nul) en la base $\mathcal{B}$, llavors és nul (respectivament, no nul) en qualsevol altra base $\mathcal{B}'$.
b) L'aplicació f és no degenerada si i només si el discriminant, en qualsevol base, és no nul.

Traça

En els exercicis del mòdul "Cossos finits" d'aquesta assignatura es va introduir la noció d'aplicació traça, la qual assigna a un element $x \in \mathbb{F}_q$ l'element de $\mathbb{F}_p$ traça de la multiplicació per x en l'espai vectorial $\mathbb{F}_q$ sobre $\mathbb{F}_p$.

3. Sigui la corba el·líptica $E : y^2 = x^3 + x$ definida sobre el cos finit $\mathbb{F}_7$.
a) Sigui la recta $r : y = x$. Determineu el divisor principal $div(r)$.
b) Siguin els dos divisors: $D_1 = 2(1,4) + (-1)(5,5)$; $D_2 = 1(1,3) + 2(5,5)$. Utilitzant l'apartat anterior, trobeu divisors D_1', D_2' equivalents a D_1 i D_2 i que tinguin suports disjunts.

4. Sigui la corba el·líptica $E : y^2 = x^3 + 1$ definida sobre el cos finit $\mathbb{F}_{11}$ i sigui la recta $r : x = 0$. Determineu el divisor $div(r)$.

5. Sigui ϕ un endomorfisme de la corba el·líptica E, $P \in E$ un punt d'ordre primer l i e_l el *pairing* de Weil. Proveu que $e_l(P, \phi(P)) \neq 1$ si i només si tots dos punts són linealment independents.

6. Sigui la corba el·líptica $E : y^2 = x^3 + 7x$ definida sobre el cos $\mathbb{F}_{13}$ i els punts de 3-torsió de E: $P = (3,3)$, $R = (3,10)$. En l'exemple 2.1 s'ha vist que $R = 2P$. Proveu aquest resultat sense utilitzar l'algorisme de Miller.

7. Sigui $p = 101$ i la corba el·líptica sobre $\mathbb{F}_{101}$, $E : y^2 = x^3 + 1$, amb cardinal 102. El punt $P = (87,61)$ pertany a la corba i té ordre 17 (això es pot comprovar utilitzant les fórmules d'addició de punts d'una corba el·líptica).
a) Calculeu el grau d'immersió de e_{17}.
b) Sigui l'aplicació $\phi : E \to E$; $\phi(x,y) = (x, \zeta y)$ en què $\zeta^3 = 1$. L'element ζ no és en el cos $\mathbb{F}_{101}$, sinó en la seva extensió de grau 2, $\mathbb{F}_{101^2}$, (en efecte, ζ és arrel del polinomi $X^2 + X + 1$, irreductible sobre $\mathbb{F}_{101}$). Proveu que ϕ és una aplicació distorsió per a P.

Vegeu també

Les corbes el·líptiques s'estudien al mòdul "Criptografia amb corbes el·líptiques" d'aquesta assignatura.

8. Sigui $p = 547$ i la corba el·líptica sobre $\mathbb{F}_{547}$, $E : y^2 = x^3 + x$, amb cardinal 548. El punt $P = (67,481) \in E$ té ordre $l = 137$.
a) Calculeu el grau d'immersió de e_{137}.
b) Sigui l'aplicació $\phi : E \to E$; $\phi(x,y) = (-x, iy)$ en què $i^2 = -1$, element en $\mathbb{F}_{547^2}$ (arrel del polinomi $X^2 + 1$, irreductible sobre $\mathbb{F}_{547}$). Proveu que ϕ és una aplicació distorsió per a P.

9. Siguin les mateixes dades de l'exercici anterior i sigui $\hat{e}_{137}$ el *pairing* modificat corresponent a P i ϕ. Tres participants A,B,C volen acordar una clau comuna K_{ABC} mitjançant el protocol d'acord tripartit de Joux.
a) Els participants trien i desen com a secrets els valors: $n_A = 4$, $n_B = 10$, $n_C = 5$. Calculeu els punts $P_A = 4P$, $P_B = 10P$, $P_C = 5P$
b) Coneguts els punts calculats en l'apartat anterior, i suposant que ens donen com a dades els valors,

i) $\hat{e}_{137}(P_B, P_C) = 151 + 135i$.

ii) $\hat{e}_{137}(P_A, P_C) = 74 + 514i$.

iii) $\hat{e}_{137}(P_A, P_B) = 11 + 39i$.

Calculeu la clau comuna del protocol donat en l'algorisme 3.3.

10. Escriviu un *script* en SAGE que permeti calcular la clau comuna K_{ABC} de l'algorisme de Joux, coneixent la clau privada n_A de A i les claus públiques P_B i P_C de B i C, respectivament. Les dades públiques, o sigui, el cos finit, la corba el·líptica, el punt P i la distorsió que permet definir el *pairing* de Weil modificat són les mateixes de l'exercici 8.
Calculeu la clau acordada entre els tres participants en el cas que $n_A = 7$, $P_B = (97,151)$ i $P_C = (497,498)$.

Solucions

1) **a)** T és bilineal, ja que és lineal a cada variable. La simetria se dedueix de la propietat commutativa del producte en $\mathbb{F}_q$.

b) Sigui $x \neq 0$ un element de $\mathbb{F}_q$. Veiem que existeix un y tal que $T(x,y) \neq 0$. N'hi ha prou a prendre $y = x^{-1}$. En efecte, $T(x,x^{-1}) = Tr(xx^{-1}) = Tr(1) = n \neq 0$ (ja que n no és múltiple de p).

2) **a)** Suposem que les equacions del canvi de base són $v'_i = \sum_j c_{ij} v_j$ o, matricialment, $\mathcal{B}' = C\mathcal{B}$ en què C és una matriu invertible i, per tant, amb determinant no nul. Substituint aquestes equacions en $Dis_{\mathcal{B}'}(f)$ i utilitzant la propietat de bilinealitat s'obté $Dis_{\mathcal{B}'}(f) = |C|^2 Dis_{\mathcal{B}}(f)$, d'on obtenim el resultat.

b) Suposem nul el discriminant (en qualsevol base $\mathcal{B}$). Existirà, doncs, una combinació lineal no trivial $\lambda_1 F_1 + \cdots + \lambda_n F_n = 0$ entre les files F_i de la matriu $(f(v_i,v_j))$ i, per tant, per a tot j es té una relació: $\lambda_1 f(v_1,v_j) + \cdots + \lambda_n f(v_n,v_j) = 0$. Denotant $w = \lambda_1 v_1 + \cdots + \lambda_n v_n$ ($w \neq 0$, ja que els λ_i no són tots nuls) i utilitzant les propietats de bilinealitat de f s'obté $f(w,v_j) = 0$. Com que això és cert per a tots els vectors v_j de la base també $f(w,v) = 0$, $\forall v \in V$. Per tant, w és un element del nucli de f (per la dreta i per l'esquerra), i f és degenerada.

El recíproc és anàleg. Si f és degenerada existirà un vector no nul $w \in V$ tal que $f(w,v) = 0$, $\forall v \in V$. Si $w = \lambda_1 v_1 + \cdots \lambda_n v_n$, es dedueix llavors una relació de dependència entre les files F_i amb coeficients λ_i.

3) **a)** Per a determinar el divisor de r cal trobar els zeros i pols de la recta en els punts de la corba el·líptica, comptats amb les seves multiplicitats.

Per a determinar els zeros fem la intersecció de E i r. Substituint $y = x$ en l'equació de E s'obté l'equació $x^3 - x^2 + x = 0$. Una arrel d'aquesta equació de tercer grau és $x = 0$. Resolent (en el cos $\mathbb{F}_7$) l'equació $x^2 - x + 1$ s'obtenen les altres dues arrels: $x = 5$; $x = 3$. Els zeros són, doncs, els punts (0,0), (3,3), (5,5) els quals tenen multiplicitat 1 (ja que són diferents).

Com en l'exemple 1.5, es veu que existeix un pol d'ordre 3 en el punt de l'infinit $O = (0 : 1 : 0)$.

Per tant,

$$div(r) = 1(0,0) + 1(3,3) + 1(5,5) - 3(O)$$

b) Els divisors D_1, D_2 tenen suports amb un punt comú (5,5). Si s'observa que aquest punt apareix també en el suport de $div(r)$ resulta raonable prendre,

$$D'_1 = D_1 + div(r) = 1(0,0) + 2(1,4) + 1(3,3) - 3(O).$$

D'_1 ja té suport disjunt amb D_2, i per tant n'hi ha prou d'agafar $D'_2 = D_2$.

4) Per a trobar els zeros determinem els punts de tall de la corba el·líptica i de la recta. Fent $x = 0$ s'obtenen els dos punts (0,1) i (0,10) amb multiplicitat 1. El tercer punt de tall de r (l'eix y) amb la corba el·líptica és el punt de l'infinit. Però en aquest punt la corba no té un zero sinó un pol. Ja que tenim dos zeros aquest pol hauria de ser d'ordre 2. No obstant això, tant en l'exemple 1.5 com en l'exercici anterior aquest ordre era 3. A què obeeix la diferència?

Escrivim l'equació de E en coordenades projectives: $y^2z = x^3 + z^3$. Ara el tall amb $x = 0$ dóna $y^2z = z^3$ i, simplificant, $y^2 = z^3$. Fent $z = 0$, es té la funció quadràtica y^2, d'on tenim la multiplicitat 2.

Per tant: $div(r) = 1(0,1) + 1(0,10) - (2)O$.

5) Si els punts fossin dependents, és a dir, si $\phi(P) \in \langle P \rangle$, es tindria $\phi(P) = mP$, per a algun m, o sigui, que $e_l(P,\phi(P)) = e_l(P,P)^m = 1$.

Suposem que tots dos punts són linealment independents; en particular ha de ser $\phi(P) \neq O$. En virtut del lema 1.10 el grup de l-torsió $E[l](\bar{K})$ és producte de dos grups cíclics d'ordre l.

Per hipòtesi un d'aquests és $\langle P\rangle$, i per tant $\phi(P)$, per a ser independent de P ha d'estar en el segon grup cíclic i, com que aquest és d'ordre primer, $\phi(P)$ n'és un generador.

En definitiva, la parella $\{P, \phi(P)\}$ és una base de $E[l](\bar{K})$. Per tant, s'ha de complir que $e_l(P,\phi(P)) \neq 1$, ja que en cas contrari e_l seria trivial en tot $E[l](\bar{K})$, en contra de la no-degeneració de e_l; vegeu la definició 1.11.

6) Atès que sabem que $R \in \langle P\rangle$ i que $\langle P\rangle$ té cardinal 3, tindrem que $\langle P\rangle = \{P, 2P, 3P = O\}$. Com que $R \neq P, O$ ha de ser $R = 2P$, cosa que també es pot comprovar utilitzant les fórmules d'addició de punts en E.

Vegeu també

Les fórmules d'addició de punts en E s'han donat en el mòdul "Criptografia amb corbes el·líptiques".

No obstant això, en les aplicacions criptogràfiques, l és molt gran i el raonament anterior no és aplicable.

7) **a)** El grau d'immersió és el menor k tal que 17 divideix $101^k - 1$. Fàcilment es comprova que $k = 2$, cosa que també s'hauria pogut deduir del fet de ser E una corba supersingular de tipus I (vegeu la proposició 1.21).

b) En primer lloc és necessari veure que ϕ és realment una aplicació de E en E, és a dir, que si (x,y) és un punt de la corba també ho és $(x,\zeta y)$. Tenint en compte l'equació de la corba i que $\zeta^3 = 1$, la comprovació és trivial. És també immediata la linealitat de ϕ. Per tant, ϕ és un endomorfisme de la corba.

Com que $\phi(P)$ no té coeficients en $\mathbb{F}_{103}$, no pot ser un múltiple de P és a dir P i $\phi(P)$ són linealment independents i per tant (vegeu un problema anterior) $e_{17}(P,\phi(P) \neq 1$, és a dir, ϕ és una aplicació distorsió.

8) De manera anàloga al problema anterior s'obté,

a) El grau d'immersió és 2 (E és una corba supersingular de tipus II, vegeu la proposició 1.21).

b) Si $(x,y) \in E$ es comprova que també $(-x,iy) \in E$. Així mateix es comprova la linealitat de ϕ, i per tant ϕ és un endomorfisme de la corba.

El mateix raonament del problema anterior és aplicable per a comprovar que ϕ és una aplicació distorsió.

9) **a)** Utilitzant les fórmules d'addició i de càlcul del doble dels punts en una corba el·líptica, s'obté:

i) $P_A = 4(67,481) = (391,472)$

ii) $P_B = 10(67,481) = (157,5)$

iii) $P_C = 5(67,481) = (395,379)$

b) Aplicant l'algorisme 3.3 i fent les operacions corresponents en el cos $\mathbb{F}_{547^2}$ (és a dir, reduint els càlculs mòdul 547 i tenint en compte que $i^2 = -1$), s'obté:

i) A calcula $(151 + 135i)^4 = 137 + 289i$.

ii) B calcula $(74 + 514i)^{10} = 137 + 289i$.

iii) C calcula $(11 + 39i)^5 = 137 + 289i$.

10) La descripció de l'*script* la farem directament sobre cada una de les instruccions que fem servir.

```
sage: F=GF(547); E=EllipticCurve(F,[0,0,0,1,0]);E.order()
# Construim la corba elliptica que ens donen i en comprovem l'ordre

sage: FX.<x>=F[]
#Construim l'anell de polinomis a coeficients en F

sage: F2.<alpha> = GF(547^2, name='alpha', modulus=x^2+1 )
#Construim el cos extensio quadratica de F i anomenem alpha el seu generador

sage: Ex=E.change_ring(F2)
# Construim la corba elliptica sobre el nou cos finit
```

En aquest punt, definim el *pairing* de Weil modificat. La definició la donem en funció del *pairing* de Weil que ja està inclòs en SAGE.

```
sage: def weil_pairing_modificat(P,Q,l):
        return P.weil_pairing(Ex(-Q[0],alpha*Q[1]),l)
```

Ara només ens queda entrar les dades del problema concret que volem resoldre i trobar el resultat:

```
sage: P=E(67,481); order(P)
# Construim el punt P i en comprovem l'ordre
137

sage: Px=Ex(P)
#El punt P sobre la corba elliptica calculada en el nou cos estes.

sage: PB = Ex(97,151), PC = Ex(497,498)
# Els punts que ens dona l'enunciat

sage: nA = 47;
# la clau privada de A

sage: W = weil_pairing_modificat(PB,PC,137); KABC = W**nA; KABC
54 + 198 alpha
```

Bibliografia

Blake, I.; Seroussi, G.; Smart, N. (2000). "Elliptic Curves in Cryptography". *London Mathematical Society Lecture Note Series* (núm. 265). Cambridge: Cambridge U. Press.

Blake, I.; Seroussi, G.; Smart, N. (2005). "Advances in Elliptic Curves in Cryptography". *London Mathematical Society Lecture Note Series* (núm. 317). Cambridge: Cambridge U. Press.

Hoffstein, J.; Pipher, J.; Silverman, J. (2008). "An Introduction to Mathematical Cryptography." *Undergraduate Texts in Mathematics*. Nova York: Springer.

Martin, L. (2008). "Introduction to Identity-based Encryption". *Artech House Inc*. Massachusetts: Norwood.