Criptografia FIB

Criptografia basada en logaritme discret. Sigantura digital DSA i ECDSA

Anna Rio

Departament de Matemàtica Aplicada II • Universitat Politècnica de Catalunya

Taher ElGamal

A public key cryptosystem and a signature schema based on discrete logarithms (1985), IEEE Transactions on Information Theory

Cossos finits

En criptografia s'usen dos tipus de cossos finits:

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\} \quad \text{on } p \text{ és un primer}$$

$$\mathbb{F}_{2^m} = GF(2^m) = \{\text{vectors binaris de dimensió } m\}$$

Estructura de cos

Tenim dues operacions (suma i producte) amb les propietats habituals (associatives, commutatives, existència de neutres, existència d'oposats per a la suma, distributiva del producte respecte la suma) de manera que tot element$\neq 0$ té invers respecte el producte (és a dir, podem *dividir*)

Cossos finits

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\} \quad \text{on } p \text{ és un primer}$$

Suma Suma d'enters amb reducció mòdul p

Producte Producte d'enters amb reducció mòdul p

$$\mathbb{F}_{2^m} = GF(2^m) = \{\text{vectors binaris de dimensió } m\}$$

Suma Suma de vectors binaris (XOR bit a bit)

Producte Cal fixar un polinomi binari $p(x)$ irreductible de grau m, interpretar els vectors com a polinomis de grau $< m$, multiplicar-los i reduir mòdul $p(x)$

Cossos finits

- $GF(2^m)$ és un espai vectorial de dimensió m sobre el cos $\mathbb{F}_2 = \{0, 1\}$.
- Fixada una base, per calcular el producte de dos elements qualssevol només cal conèixer els productes dels elements de la base (matriu del producte)
- Es treballa amb valors de m per als quals existeixen bases normals òptimes: bases de la forma $\alpha, \ \alpha^2, \alpha^4, \ldots, \alpha^{2^{m-1}}$ tals que la matriu del producte *té molts zeros*

El grup multiplicatiu és cíclic

Tant en el cas $\mathbb{F}_p$ com en el cas $GF(2^m)$, si treiem el zero, podem escriure tots els elements com a potències d'un element g (generador)

$$\mathbb{F}^* = \langle g \rangle = \{1, g, g^2, g^3, \ldots g^{|\mathbb{F}|-2}\}$$

Exemple: $GF(2^8)^*$ és el conjunt de les potències de $g = \texttt{0x03} = (0, 0, 0, 0, 0, 0, 1, 1)$

En el cas $\mathbb{F}_p$, com sabem si un element és generador?

$$g^{p-1} = 1\,, \qquad g^{\frac{p-1}{2}} = -1, \qquad g^{\frac{p-1}{q}} \neq 1 \quad \text{per a tot } q \text{ divisor de } p-1$$

Cossos finits

$p = 23$

$\mathbf{Z}/p\mathbf{Z} = \{0, 1, 2, 3, \ldots, 22\} = \mathbf{F}_p = GF(p)$ Cos finit de p elements

$\mathbf{F}_p^* = \{1, 2, 3, \ldots, 22\}$ Grup de $p - 1$ elements

Grup una operació (neutre, inversos, associativa)

Grup cíclic

$\langle 5 \rangle = \{5, 5^2, 5^3, 5^4, 5^5, 5^6, 5^7, 5^8, 5^9, 5^{10}, 5^{11}, 5^{12}, 5^{13}, 5^{14}, \ldots, 5^{22}\} =$

$\{5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14, 1\}$

$$\mathbf{F}_p^* = \langle 5 \rangle$$

Subgrups

$\langle 2 \rangle = \{2, 2^2, 2^3, 2^4, \ldots\} = \{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1\}$
té cardinal 11, divisor de $p - 1$

$\langle 22 \rangle = \{22, 1\}$ té cardinal 2

Logaritme discret

Problema

$17 \in \langle 5 \rangle$ Quina potència de 5 mòdul 23 dóna 17?

$18 \in \langle 2 \rangle$ Quina potència de 2 mòdul 23 dóna 18?

Trobar r tal que $2^r \bmod 23 = 18$? $r = \log_2 18$ a $\mathbf{F}_p^*$

Problema del logaritme discret

Fixem un grup G i un element $g \in G$.
Donat un element $b \in \langle g \rangle$, trobar el nombre r tal que $g^r = b$

Logaritme discret

Conjectures

- El problema del logaritme discret es conjectura intractable
  Cal tenir present que el problema depèn del grup G triat
- El problema de Diffie-Hellman es conjectura equivalent al del logaritme discret

Criptosistema de ElGamal

Paràmetres del sistema

- Un primer p
- Un element $g \mod p$ generador de $\mathbb{F}_p^*$

Claus

- Cada usuari tria una clau privada r, un enter mòdul $p-1$,
- Fa pública la clau $u = g^r \mod p$

Criptosistema de ElGamal

Xifratge

- Les unitats de missatge són enters m mòdul $p-1$
- Per a cada m es tria aleatòriament un enter k mòdul $p-1$ i s'envia el criptograma

$$c = (c_1, c_2) = (g^k, mu^k) \mod p$$

Observacions

El criptograma dobla la longitud del missatge

Xifrar dues vegades el mateix missatge dóna criptogrames diferents

Desxifratge

$$c_2\, c_1^{-r} = m\, g^{rk}\, g^{-rk} = m$$

Trobar la clau

Trobar la clau privada r a partir de la clau pública

$$u = g^r \mod p$$

és un problema de logaritme discret en $\mathbb{F}_p^*$ (base g)

El problema del logaritme discret es conjectura intractable.

A dia d'avui no es coneix cap algoritme polinòmic per resoldre'l

Trobar el missatge

Trobar el missatge a partir del criptograma c (sense conèixer la clau secreta r) és un problema de Diffie-Hellman en $\mathbb{F}_p^*$:

Coneguts

$$\begin{aligned} c_1 &= g^k \mod p \\ u &= g^r \mod p \end{aligned}$$

trobar

$$x = g^{kr} \mod p$$

Invertint aquest element i multiplicant-lo per c_2 recuperem m

$$x^{-1} c_2 = g^{-kr} m u^k = g^{-kr} m g^{kr} = m$$

El problema de Diffie-Hellman es conjectura equivalent al del logaritme discret (i, per tant, intractable), tot i que podria ser més fàcil.

Trobar el missatge

Trobar el missatge a partir del criptograma c (sense conèixer la clau secreta r) és un problema de Diffie-Hellman en $\mathbb{F}_p^*$:
Coneguts

$$\begin{aligned} c_1 &= g^k \mod p \\ u &= g^r \mod p \end{aligned}$$

trobar

$$x = g^{kr} \mod p$$

Invertint aquest element i multiplicant-lo per c_2 recuperem m

$$x^{-1}c_2 = g^{-kr}mu^k = g^{-kr}mg^{kr} = m$$

El problema de Diffie-Hellman es conjectura equivalent al del logaritme discret (i, per tant, intractable), tot i que podria ser més fàcil.

SEGURETAT

Trobar el missatge

Trobar el missatge a partir del criptograma c (sense conèixer la clau secreta r) és un problema de Diffie-Hellman en $\mathbb{F}_p^*$:

Coneguts

$$c_1 = g^k \mod p$$
$$u = g^r \mod p$$

trobar

$$x = g^{kr} \mod p$$

Invertint aquest element i multiplicant-lo per c_2 recuperem m

$$x^{-1} c_2 = g^{-kr} m u^k = g^{-kr} m g^{kr} = m$$

El problema de Diffie-Hellman es conjectura equivalent al del logaritme discret (i, per tant, intractable), tot i que podria ser més fàcil.

Trobar el missatge

Trobar el missatge a partir del criptograma c (sense conèixer la clau secreta r) és un problema de Diffie-Hellman en $\mathbb{F}_p^*$:

Coneguts

$$c_1 = g^k \mod p$$
$$u = g^r \mod p$$

trobar

$$x = g^{kr} \mod p$$

Invertint aquest element i multiplicant-lo per c_2 recuperem m

$$x^{-1}c_2 = g^{-kr}mu^k = g^{-kr}mg^{kr} = m$$

El problema de Diffie-Hellman es conjectura equivalent al del logaritme discret (i, per tant, intractable), tot i que podria ser més fàcil.

Digital Signature Standard

L'any 1991 el NIST va proposar un estàndard de signatura digital publicat al FIPS 186

> *Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory. This is known as nonrepudiation since the signatory cannot, at a later time, repudiate the signature.*

> *A ds algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication.*

SIGNATURA DIGITAL

Els criptosistemes de clau pública (RSA, ElGamal) permeten signar digitalment: la signatura es un afegit al missatge que indica autoria, conformitat amb el contingut del missatge, responsabilitat d'haver-ho enviat...

Aquests sistemes proporcionen, doncs, serveis de

- identificació
- integritat
- no repudi

DUES DIFERÈNCIES AMB LA SIGNATURA MANUSCRITA

1. La signatura digital no pot dependre només de qui firma, ha de dependre també del què es firma, del missatge que l'acompanya. Per tant, la verificació d'una signatura digital no es pot fer comparant-la amb la d'un document anterior.

2. La signatura digital no permet distingir un document original d'una còpia.

FIPS-186 DSS:Digital Signature Standard

FIPS 186 (1991)

- DSA

FIPS 186-2 Publicat el 27 de gener de 2000. Obligatori des de 27 de juliol de 2001.
Especifica els tres algoritmes que es poden usar en les aplicacions que requereixen una signatura digital.

- DSA (Digital Signature Algorithm)
- RSA (DNI Espanya)
- ECDSA(Elliptic Curve Digital Signature Algorithm) (Passaports Alemanya)

La signatura digital DSA (Digital Signature Algorithm)

Paràmetres

- Públics i comuns per a un grup d'usuaris
  - Un primer p de 2048 bits
  - Un primer q de 256 bits, divisor de $p-1$
    Per obtenir p i q, es genera primer q i després $p = 2\lambda q + 1$
  - g, generador d'un subgrup d'ordre q a $\mathbf{F}_p^*$
    $g = x^{(p-1)/q} \bmod p$, on x és qualsevol enter amb $1 < x < p-1$ tal que $x^{(p-1)/q} \bmod p \neq 1$
- Claus privada i pública d'un usuari
  - r un enter mòdul $q-1$ aleatori o pseudoaleatori
  - $u = g^r \bmod p$
- Paràmetre (secret) que cal generar per a cada signatura
  - k un enter mòdul q aleatori o pseudoaleatori

La signatura digital DSA (Digital Signature Algorithm)

Paràmetres

- Públics i comuns per a un grup d'usuaris
  - Un primer p de 2048 bits
  - Un primer q de 256 bits, divisor de $p-1$
    Per obtenir p i q, es genera primer q i després $p = 2\lambda q + 1$
  - g, generador d'un subgrup d'ordre q a $\mathbf{F}_p^*$
    $g = x^{(p-1)/q} \bmod p$, on x és qualsevol enter amb $1 < x < p-1$ tal que $x^{(p-1)/q} \bmod p \neq 1$
- Claus privada i pública d'un usuari
  - r un enter mòdul $q-1$ aleatori o pseudoaleatori
  - $u = g^r \bmod p$
- Paràmetre (secret) que cal generar per a cada signatura
  - k un enter mòdul q aleatori o pseudoaleatori

La signatura digital DSA (Digital Signature Algorithm)

Paràmetres

- Públics i comuns per a un grup d'usuaris
  - Un primer p de 2048 bits
  - Un primer q de 256 bits, divisor de $p-1$
    Per obtenir p i q, es genera primer q i després $p = 2\lambda q + 1$
  - g, generador d'un subgrup d'ordre q a $\mathbf{F}_p^*$
    $g = x^{(p-1)/q} \bmod p$, on x és qualsevol enter amb $1 < x < p-1$ tal que $x^{(p-1)/q} \bmod p \neq 1$
- Claus privada i pública d'un usuari
  - r un enter mòdul $q-1$ aleatori o pseudoaleatori
  - $u = g^r \bmod p$
- Paràmetre (secret) que cal generar per a cada signatura
  - k un enter mòdul q aleatori o pseudoaleatori

DSA: signatura

Signatura d'un missatge m

El que signem és un hash del missatge m.
Es calculen:

$$\begin{aligned} f_1 &= (g^k \bmod p) \bmod q \\ f_2 &= k^{-1}(SHA(m) + f_1\, r) \bmod q \end{aligned}$$

Si $f_1 = 0$ o $f_2 = 0$, s'ha de generar un nou valor de k i s'ha de recalcular la signatura.
La signatura que acompanya el missatge és

$$s = (f_1, f_2) \qquad (512 bits)$$

Verificació de la signatura

Verificació d'una signatura (f_1, f_2)

Cal disposar de p, q, g i la clau pública de l'emissor de manera fiable. S'han rebut m', f_1', f_2'

1. Comprovar que $0 < f_1' < q$ i $0 < f_2' < q$
2. Calcular

$$
\begin{aligned}
w &= (f_2')^{-1} \bmod q \\
w_1 &= SHA(m')\, w \bmod q \\
w_2 &= f_1'\, w \bmod q \\
v &= (g^{w_1} u^{w_2} \bmod p) \bmod q
\end{aligned}
$$

3. Acceptar si $v = f_1'$

ja que $\quad g^{w_1} u^{w_2} = g^{f_2^{-1}(SHA(m)+f_1 r)} = g^k = f_1$

Eficiència/Seguretat DSA

Algoritmes eficients

Inversos modulars i exponenciació modular

Obtenir la clau privada a partir de la pública

$$u = g^r \bmod q$$

Problema de **logaritme discret**

Grups d'utilitat criptogràfica

Operació eficient i cardinal divisible per algun primer gran

Exemple

En el DSA $\mathbf{F}_p^*$ té

- operació: producte mòdul p
- cardinal $p-1$, que es divideix per un primer gran: q de 256 bits

Criptografia amb corbes el.líptiques

Substituir el grup $\mathbf{F}_p^*$ (nombres enters mòdul p) per un grup de *punts* que satisfan l'equació d'una corba i usar la dificultat del logaritme discret en aquest grup *geomètric* per basar la seguretat

CORBES EL.LÍPTIQUES

Una corba el.líptica definida sobre un cos K és una corba no singular donada per una equació

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

amb els $a_i \in K$, més un punt de l'infinit **O**.

No singular significa que les derivades parcials no s'anul.len simultàniament en cap punt de la corba. És a dir, en tots els punts existeix la recta tangent.

$Y^2 = X^3 + aX + b$

$$F(X,Y) = X^3 + aX + b - Y^2$$

$$\left(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}\right) = (3X^2 + a, -2Y)$$

Punt singular:

$$\left\{ \begin{array}{l} x^3 + ax + b - y^2 = 0 \\ 3x^2 + a = 0 \\ -2y = 0 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x = -\frac{3b}{2a} \\ x^2 = -\frac{a}{3} \\ y = 0 \end{array} \right.$$

És corba el.líptica $\Leftrightarrow 4a^3 + 27b^2 \neq 0$

$K = \mathbb{F}_{2^m} = \{$vectors binaris de m components$\}$

$K = \mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ (suma, producte, inversos)

Equacions

$K = \mathbb{F}_{2^m}$

$$\begin{aligned} Y^2 + XY &= X^3 + aX^2 + b \\ Y^2 + cY &= X^3 + aX + b \end{aligned}$$

$K = \mathbb{F}_p$ $(p > 3)$

$$Y^2 = X^3 + AX + B \qquad (4A^3 + 27B^2 \neq 0)$$

Corba K-163 del FIPS 186-2

$$E/\mathbb{F}_{2^{163}} \quad Y^2 + XY = X^3 + X^2 + 1$$

Corba P-192 del FIPS 186-2

$$E/\mathbb{F}_p \quad Y^2 = X^3 - 3X^2 + B$$

$$\begin{aligned} p &= 2^{192} - 2^{64} - 1 \\ &= 627710173538668076383578942320766641608390\backslash \\ &\quad 870039032496 1279 \\ B &= 64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1 \end{aligned}$$

GRUP DE PUNTS

Corba el.líptica definida sobre un cos K

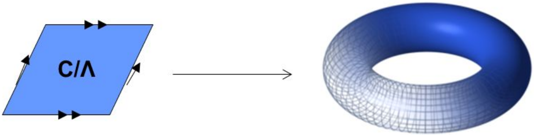
$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

Grup

$$E(K) = \{(x, y) \mid x, y \in K \text{ que satisfan l'equació}\} \cup \{\mathbf{O}\}$$

GRUP DE PUNTS... sobre quin cos?

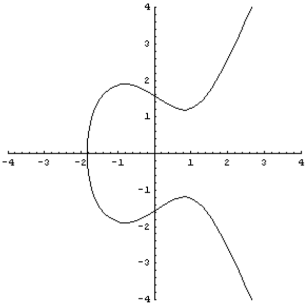
Elliptic Curves over Complex Numbers

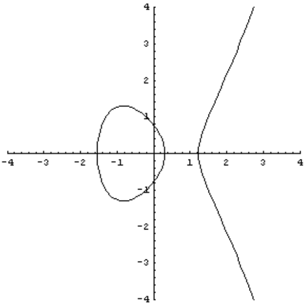


$$\mathbb{C}/\Lambda \longrightarrow E : y^2 = x^3 + Ax + B$$
$$z \longmapsto (\wp(z), -\wp'(z)/2)$$

GRUP DE PUNTS... sobre quin cos?

$$Y^2 = X^3 - 2X + b \quad \textcolor{red}{\text{sobre } \mathbb{R}}$$



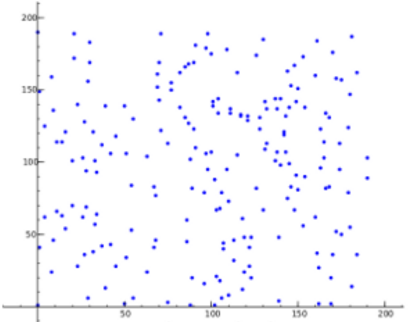


$b = 2$ $\qquad\qquad$ $b = 1/2$

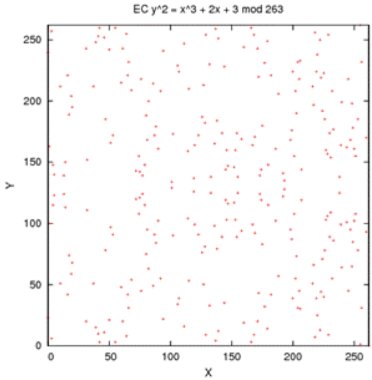
-1.77 $\qquad\qquad$ $-1.52, 0.26, 1.27$

GRUP DE PUNTS... sobre quin cos?

Les de la Criptografia són sobre un cos finit $\mathbb{F}_p$



Elliptic Curve $y^2 + xy = x^3 + x^2 + 1$ over $GF(191)$



$$E/\mathbb{F}_{131} \ : \ Y^2 = X^3 + X + 2$$

$\mathbf{P} = (\mathbf{5}, \mathbf{1})$ $\quad 5^3 + 5 + 2 = 125 + 5 + 2 = 132 \equiv 1$
$(5, 130)$ també és punt de la corba

$\mathbf{Q} = (\mathbf{60}, \mathbf{49})$ $\quad$ i també $(60, 82)$
$60^3 + 60 + 2 = 216000 + 60 + 2 = 216062 = 131 \cdot 1649 + 43 \equiv 43$
$49^2 = 2401 = 18 \cdot 131 + 43 \equiv 43$

Com trobar punts?

$$Y^2 = X^3 + aX + b$$

Punt aleatori

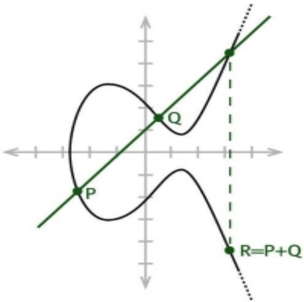
- Donem x aleatori. Calculem $z = x^3 + ax + b \bmod p$.
- Si $z = 0$, aleshores obtenim el punt $(x, 0)$
- Si $z \neq 0$, És un quadrat a $\mathbb{F}_p^*$?
- Símbol de Legendre: z és quadrat si i només si

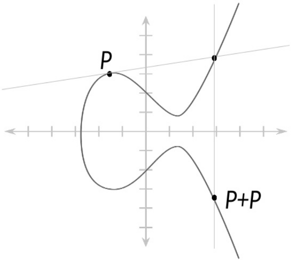
$$z^{\frac{p-1}{2}} \equiv 1 \bmod p$$

- Si z no és quadrat, nova x. Si és quadrat, cal calcular una arrel quadrada mòdul p
- Si $p \equiv 3 \bmod 4$, una arrel quadrada és $y = z^{\frac{p+1}{4}} \bmod p$
- **Obtenim dos punts**: (x, y) i $(x, p - y)$

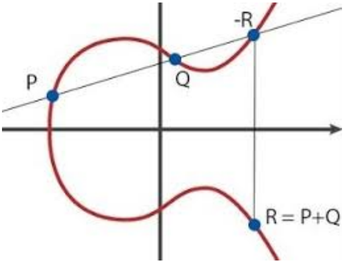
Suma de punts

Llei d'addició Tres punts sumen **O** si i només si estan alineats





Llei de grup. Cas criptogràfic $Y^2 = X^3 + aX + b$



$P = (x_1, y_1) \quad Q = (x_2, y_2) \quad R = P + Q$

Pendent de la secant o la tangent

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \\ \dfrac{3x_1^2 + a}{2y_1} & \textbf{duplicació} \end{cases}$$

$\nu = y_1 - \lambda x_1$
Recta per P i Q és $Y = \lambda X + \nu$
Tall recta-corba: $(\lambda X + \nu)^2 = X^3 + aX + b$
té solucions x_1, x_2 i $x(R)$

$$x(R) = \lambda^2 - x_1 - x_2$$
$$y(R) = \lambda(x_1 - x(R)) - y_1$$

Llei de grup

- El punt de l'infinit és el neutre: $P + \mathbf{O} = P$
- L'oposat de $P = (x_1, y_1)$ és $-P = (x_1, p - y_1)$
- Els punts d'ordre 2, és a dir, els que compleixen $2P = \mathbf{O}$ són els que tenen $y = 0$. Pot haver-ne un o tres.

La suma de punts és commutativa i associativa

Llei de grup

$E(\mathbf{F}_p)$ grup commutatiu finit, amb operació eficient

$$E/\mathbf{F}_{131} \;:\; Y^2 = X^3 + X + 2$$

$$P = (5,1) \quad Q = (60,49) \Longrightarrow \begin{cases} -P & = & (5,130) \\ P+Q & = & (127,14) \\ 2P & = & (124,62) \\ 2Q & = & (32,24) \end{cases}$$

"Exponenciació": amb l'algoritme de "quadrats successius"

$$13 = 1101_2 \quad \Rightarrow \quad 13P = 2\,(2\,(2\,P \,+\, P\,)\,) + \,P$$

$$\Rightarrow \quad 13\,P = (77, 83)$$

$$k = b_r \cdot 2^r + \cdots + b_1 \cdot 2 + b_0 \qquad b_i \in \{0, 1\}$$

$R \leftarrow \mathbf{O},\ i \leftarrow r$
mentre $i \geq 0$ **fer**
  $R \leftarrow R + R$
  si $b_i = 1$ **fer** $R \leftarrow R + P$
  $i \leftarrow i - 1$
sortida R

ECDH: Diffie-Hellman amb corbes el.líptiques

- Paràmetres públics i comuns:
  un primer p
  una corba el.líptica $Y^2 = X^3 + aX + b$
  un punt $P = (x_p, y_P)$ de la corba

- Clau privada de A: r_A Clau pública de A: $Q_A = r_A P$
- Clau privada de B: r_B Clau pública de B: $Q_B = r_B P$

Clau comuna $Q = r_B Q_A = r_A Q_B$

Log discret a $E/\mathbf{F}_{131}$: $Y^2 = X^3 + X + 2$

$$
\begin{aligned}
E(\mathbf{F}_{131}) \; = \; & \{O, (1, \pm 2), (2, \pm 55), (5, \pm 1), (8, \pm 28), (11, \pm 54), (12, \pm 63), \\
& (14, \pm 3), \ldots, (126, \pm 38), (127, \pm 14), (129, \pm 56), (-1, 0)\}
\end{aligned}
$$

té $124 = 4 \cdot 31$ elements

El punt $P = (14, 3)$ genera un subgrup de cardinal $q = 31$

$$
\begin{array}{rcl}
2P & = & (93, 80) \\
3P & = & (40, 101) \\
4P & = & (54, 78) \\
 & \ldots & \\
30P & = & (14, 128) = -P \\
31P & = & \mathbf{O}
\end{array}
$$

Problema del logaritme discret

Donat un punt Q, del qual sabem que és $Q = r\,P$, trobar r

Cardinal del grup

Interval de Hasse

$$|E(\mathbf{F}_p)| \in [\, p+1-2\sqrt{p}\,,\; p+1+2\sqrt{p}\,]$$

El cardinal del grup és del mateix ordre que el primer p

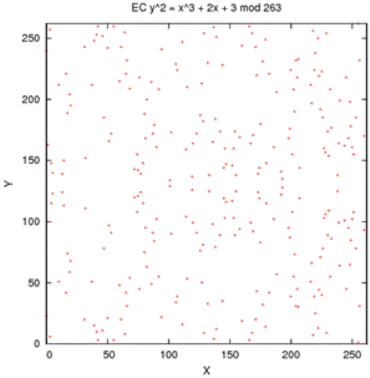
Càlcul del valor exacte

- Algoritme SEA: Complexitat $\mathcal{O}((\log p)^6)$
- Construcció de corbes el.líptiques amb cardinal prefixat

És el càlcul més difícil dels que es fan a la criptografia amb corbes el.líptiques

Cal buscar cardinals primers o quasi primers

Corba $Y^2 = x^3 + 2x + 3 \bmod 263$



té $270 = 2 \cdot 3^3 \cdot 5$ punts

“Cardinal producte de primers petits no és criptogràficament útil"

Corba P-192 del FIPS 186-2

$$E/\mathbf{F}_p \quad Y^2 = X^3 - 3X^2 + B$$

$$\begin{aligned} p &= 2^{192} - 2^{64} - 1 \\ &= 6277101735386680763835789423 \\ &\ 2076664160839087003903249612 79 \\ B &= 64210519e59c80e70fa7e9ab72243049 \\ &\ feb8deecc146b9b1 \end{aligned}$$

Cardinal

$$\begin{aligned} |E(\mathbf{F}_p)| &= 6277101735386680763835789423 \\ &\ 176059013767194773182842284081 = q \text{ (primer)} \end{aligned}$$

Cardinal del grup

Si el cardinal del grup $E(\mathbb{F}_p)$ és primer
aleshores qualsevol punt $P \neq \mathbf{O}$ n'és un generador.

L'espai de claus

$$\langle P \rangle = \{P, 2P, 3P, \ldots, rP, \ldots\}$$

és el grup sencer.

Tenim $\mathcal{O}(p)$ claus diferents.

Si p té 256 bits, tenim de l'ordre de 2^{256} claus diferents.

ECDSA:Elliptic Curve Digital Signature Algorithm

- Paràmetres
  $P \in E(\mathbf{F}_p) \quad |\langle P \rangle| = q$ primer
- Clau pública $Q = rP$
- Clau privada r enter $\bmod q$
- Signatura (f_1, f_2)
  - $kP = (x_1, y_1)$ amb $1 < k < q - 1$ aleatori
  - $f_1 = x_1 \mod q$
  - $f_2 = k^{-1}\,(\,SHA(m) + f_1 r) \mod q$
- Verificació
  - $w_1 = SHA(m) f_2^{-1} \mod q$
  - $w_2 = f_1 f_2^{-1} \mod q$
  - $w_1 P + w_2 Q = (x_0, y_0)$
  - Acceptar si $x_0 \mod q = f_1$

ECDSA:Elliptic Curve Digital Signature Algorithm

- Paràmetres
  $P \in E(\mathbf{F}_p) \quad |\langle P\rangle| = q$ primer
- Clau pública $Q = rP$
- Clau privada r enter mod q
- Signatura (f_1, f_2)
  - $kP = (x_1, y_1)$ amb $1 < k < q-1$ aleatori
  - $f_1 = x_1 \bmod q$
  - $f_2 = k^{-1}\,(SHA(m) + f_1 r) \bmod q$
- Verificació
  - $w_1 = SHA(m) f_2^{-1} \bmod q$
  - $w_2 = f_1 f_2^{-1} \bmod q$
  - $w_1 P + w_2 Q = (x_0, y_0)$
  - Acceptar si $x_0 \bmod q = f_1$

ECDSA:Elliptic Curve Digital Signature Algorithm

- Paràmetres
  $P \in E(\mathbf{F}_p) \quad |\langle P \rangle| = q$ primer
- Clau pública $Q = rP$
- Clau privada r enter $\bmod q$
- Signatura (f_1, f_2)
  - $kP = (x_1, y_1)$ amb $1 < k < q - 1$ aleatori
  - $f_1 = x_1 \mod q$
  - $f_2 = k^{-1} \, (SHA(m) + f_1 r) \mod q$
- Verificació
  - $w_1 = SHA(m) f_2^{-1} \mod q$
  - $w_2 = f_1 f_2^{-1} \mod q$
  - $w_1 P + w_2 Q = (x_0, y_0)$
  - Acceptar si $x_0 \mod q = f_1$

ECDSA:Elliptic Curve Digital Signature Algorithm

- Paràmetres
  $P \in E(\mathbf{F}_p) \quad |\langle P \rangle| = q$ primer
- Clau pública $Q = rP$
- Clau privada r enter mod q
- Signatura (f_1, f_2)
  - $kP = (x_1, y_1)$ amb $1 < k < q - 1$ aleatori
  - $f_1 = x_1 \bmod q$
  - $f_2 = k^{-1}\,(SHA(m) + f_1 r) \bmod q$
- Verificació
  - $w_1 = SHA(m) f_2^{-1} \bmod q$
  - $w_2 = f_1 f_2^{-1} \bmod q$
  - $w_1 P + w_2 Q = (x_0, y_0)$
  - Acceptar si $x_0 \bmod q = f_1$

ECDSA:Elliptic Curve Digital Signature Algorithm

- Paràmetres
  $P \in E(\mathbf{F}_p) \quad |\langle P \rangle| = q$ primer
- Clau pública $Q = rP$
- Clau privada r enter mod q
- Signatura (f_1, f_2)
  - $kP = (x_1, y_1)$ amb $1 < k < q - 1$ aleatori
  - $f_1 = x_1 \bmod q$
  - $f_2 = k^{-1}\,(SHA(m) + f_1 r) \bmod q$
- Verificació
  - $w_1 = SHA(m) f_2^{-1} \bmod q$
  - $w_2 = f_1 f_2^{-1} \bmod q$
  - $w_1 P + w_2 Q = (x_0, y_0)$
  - Acceptar si $x_0 \bmod q = f_1$

ECDSA:Elliptic Curve Digital Signature Algorithm

- Paràmetres
  $P \in E(\mathbf{F}_p) \quad |\langle P \rangle| = q$ primer
- Clau pública $Q = rP$
- Clau privada r enter $\bmod q$
- Signatura (f_1, f_2)
  - $kP = (x_1, y_1)$ amb $1 < k < q - 1$ aleatori
  - $f_1 = x_1 \bmod q$
  - $f_2 = k^{-1}\,(SHA(m) + f_1 r) \bmod q$
- Verificació
  - $w_1 = SHA(m) f_2^{-1} \bmod q$
  - $w_2 = f_1 f_2^{-1} \bmod q$
  - $w_1 P + w_2 Q = (x_0, y_0)$
  - Acceptar si $x_0 \bmod q = f_1$

NEXT: ECDSA vs DSA

Avantatges?