Criptografia, complexitat i geometria

Anna Rio

Departament de Matemàtica Aplicada II • Universitat Politècnica de Catalunya

ÍNDEX

Criptografia del mil.leni?

- Quines capacitats demanarem a la criptografia del futur?

  L'any 1001, un profeta no es podria haver imaginat la criptografia de clau pública (...) Les nostres esperances de predir els requisits criptogràfics d'aquí a mil anys són bastant minses

- L'any 3001, hi haurà algun tipus de criptografia?

  Probablement, millorar les comunicacions porta l'espècie humana cap a una organització molt més unida (...) En un entorn altament integrat encara hi haurà seguretat, però la criptografia pot no ser un mecanisme adient.
  Al cos humà trobem autenticació de tipus criptogràfic en el sistema immunològic, però no xifratge de missatges.

▸ Referència

Criptografia del segle?

Computació quàntica / Criptografia quàntica

- Es pot fer una distribució quàntica de claus que faci pràctic el xifrat de Vernam (*one-time pad*)?

missatge	00011 01111 01101 00101
$\oplus$	
clau	11011 00101 01011 00110
$\downarrow$	
criptograma	11000 01010 00110 00011
$\oplus$	
clau	11011 00101 01011 00110
$\downarrow$	
missatge	00011 01111 01101 00101

- En el disseny de criptosistemes, cal preveure l'aparició d'ordinadors quàntics?

▸ Referència

Criptografia de la dècada?

Cal rebaixar les hipòtesis en què es basa la seguretat

- Hipòtesis d'intractabilitat (de certs problemes matemàtics)
- Hipòtesis de confiança (en certes autoritats)
- Hipòtesis físiques (sobre el canal)

Computació i comunicació són processos físics més que objectes matemàtics idealitzats

Els components crucials de la infraestructura emergent d'informació global hauran d'ésser sistemes que operin de manera fiable i segura en entorns potencialment molt adversos

▸ Referència

Com guanyar un milió de dòlars?

Reptes RSA

Resolt RSA-576	*$10,000*	RSA-896	$75,000
RSA-640	$20,000	RSA-1024	$100,000
RSA-704	$30,000	RSA-1536	$150,000
RSA-768	$50,000	RSA-2048	$200,000

RSA-2048 (617 xifres decimals) $n = pq$

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357

`http://rsasecurity.com/rsalabs/challenges`

Índex

Orígens

1938 El govern britànic instal.la a Bletchey Park la *Foreign Office's Code and Cipher School*

1940 S'incorpora Alan Turing. Durant la 2a Guerra Mundial, deu mil persones hi treballen. El repte per a matemàtics i criptoanalistes és trencar el criptosistema Enigma, que utilitzava l'exèrcit alemany

1944 Es posa en funcionament Colossus, la primera computadora electrònica programable.

D'un art antic a una nova ciència

Fins després de la 2a. Guerra Mundial la criptografia era un art

- Principalment d'ús en àmbits militars
- Concentrat quasi exclusivament en l'encriptació
- Sistemes ad-hoc sense base teòrica de la seva seguretat

Transició cap a la nova ciència

1948 C. E. **Shannon**: A mathematical theory of communication
Bell System Technical Journal

1949 C. E. **Shannon**: Communication theory of secrecy systems
Bell System Technical Journal

1976 W. **Diffie** i M. E. **Hellman**: New directions in cryptography
IEEE Transactions on Information Theory

Informació digitalitzada

$$\begin{array}{rcccc} & \text{ascii} & & \text{base 2} & \\ & \downarrow & & \downarrow & \\ \text{Text} & \longleftrightarrow & (\{0,1,\ldots,255\})^\star & \rightleftarrows & \{0,1\}^{8\star} \\ \text{(cadena de} & & & \uparrow & \text{(cadena de} \\ \text{símbols d'un} & & & \text{base 10} & \text{bytes} \\ \text{alfabet)} & & & & \text{o de bits)} \end{array}$$

Exemple

Mil.lenni $\longleftrightarrow$ {77, 105, 108, 46, 108, 101, 110, 110, 105}

$\updownarrow$

01001101011010010110110000101110011011000110010101101110011011001101001

$\updownarrow$

0x4d 0x69 0x6c 0x2e 0x6c 0x65 0x6e 0x6e 0x69

Ciència multidisciplinar

W. Diffie: En criptografia, els problemes que entenem i que ens atanyen avui en dia es troben en tres àrees generals

- Matemàtiques
- Complexitat computacional
- Tecnologia informàtica

Matemàtiques

*Els problemes pertanyen principalment al camp de la **geometria aritmètica**, l'àrea de les matemàtiques que tracta de la resolució de sistemes d'equacions algebraiques sobre estructures aritmètiques molt generals. En molts aspectes, la criptografia consisteix a triar o dissenyar sistemes aritmètics pensats per fer les equacions difícils de resoldre*

- Paraula binària de longitud k $\equiv$ element del cos finit $\mathbf{F}_{2^k}$
- Si $k \leq \lfloor \log_2 n \rfloor$

  Paraula binària de longitud k $\equiv$ element de $\{0, 1, \ldots, n-1\}$

  $\equiv$ element de $\mathbf{Z}/n\mathbf{Z}$

Tractament aritmètic de missatges digitalitzats

Complexitat computacional

***La matemàtica**: actitud molt permissiva envers el tema de la resolubilitat d'un problema, tenint molt poc en compte l'eficiència*

***La teoria de la complexitat**: estudia la complexitat intrínseca de les tasques computacionals. Com de difícil és resoldre un problema matemàtic?*

L'objectiu és entendre l'efecte de limitar els recursos computacionals naturals (especialment el temps) en el conjunt dels problemes computacionals que es poden resoldre

$$\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{EXP}$$

Tecnologia informàtica

Llei de Moore

El cost computacional es divideix per la meitat cada 18 mesos

La validesa de la llei de Moore és limitada: com de petites poden arribar a ser les unitats de càlcul? Cordes?
La computació quàntica intenta expandir la computació en paral.lel mitjançant la computació en superposició quàntica

Avui

- possible abordar tasques criptoanalítiques que requereixen aproximadament 2^{64} operacions
- segurs els sistemes, la resolució dels quals requereix 2^{128} operacions

Estàndards actuals

- Xifratge de missatges usant un algoritme de clau secreta
  (FIPS 197: **AES**)
- Xifratge de la clau secreta usant un sistema de clau pública (RSA)
- Càlcul del hash del missatge
  (FIPS 180-2: **SHA-1, SHA-224, SHA-256, SHA-384 i SHA-512**)
- Signatura del hash usant un protocol de signatura digital
  (FIPS 186-2: **DSA, RSA, ECDSA**)

Criptografia de clau secreta

DES (Data Encryption Standard)

- Dissenyat por IBM
- Sistema de xifratge en bloc: blocs de 64 bits, claus de 56 bits.
- El 1998 va ser trencat (DES Cracker)
- Estàndard 1976–2001. Encara vigent TDEA (Triple DES), que dobla la longitud efectiva de la clau (112 bits) al preu de triplicar el nombre d'operacions de xifratge

- **crypt(3)**: Funció de xifratge de passwords en Unix
- **IDEA**: Usat per **PGP**
- **RC5**: Usat per Nestcape per implementar el seu sistema de seguretat en comunicacions **SSL** (Secure Socket Layer)

AES: Advanced Encryption Standard

L'any 2001, l'algoritme RIJNDAEL, dissenyat per Joan Daemen i Vincent Rijmen, de la Universitat Catòlica de Leuven (Bèlgica), es converteix en el nou estàndard

- Algoritme simètric de bloc de 128 bits i clau de 128, 192 o 256 bits
- Les transformacions es fan sobre la matriu d'estat, una matriu 4×4, els coeficients de la qual són bytes
- Realitza operacions al cos finit $\mathbf{F}_{2^8}$ i a l'espai vectorial de dimensió 4 sobre aquest cos

Tots aquests criptosistemes de clau secreta basen la seguretat en la confusió i difusió de la informació

Índex

DIFFIE-HELLMAN (1976)

Intercanvi de claus a través d'un canal insegur

- A i B acorden (públicament) un grup G i un element $x \in G$
- A genera un nombre enter a, envia $x^a \longrightarrow$ B
  B genera un nombre enter b, envia $x^b \longrightarrow$ A
- A calcula $(x^b)^a$, B calcula $(x^a)^b$

CLAU = aquest element comú $x^{ab} \in G$

Eficiència: Bon algoritme d'exponenciació a G?

$$EXP_G \in \mathbf{P} \ ?$$

Secret: Coneguts $x^a, x^b \in G$, es pot calcular fàcilment $x^{ab} \in G$?

$$DHP_G \notin \mathbf{P} \ ?$$

Sistemes de clau pública

- **La regla d'encriptació es pot fer pública sense comprometre la seguretat del sistema**
- Es pot establir comunicació xifrada sense intercanvi previ de claus
- Permeten la signatura de documents i l'autenticació de signatures.
- La seguretat depèn del secret de la clau privada. Ha d'ésser impossible obtenir-la a partir de la pública

Impossible $\approx$ Computacionalment intractable

Sabem quina és la fórmula matemàtica per obtenir-la però no existeix (o no es coneix?) un bon algoritme per calcular-la ràpidament.

El problema **P** vs. **NP** a la nostra vida quotidiana?

Ara

- Usem caixers automàtics?
- Usem telèfons mòbils?
- Comprem entrades usant internet?
- Fem la presentació telemàtica de la declaració de renda?

Aviat

- Farem votacions electròniques?
- Tindrem un DNI digital?

Índex

El criptosistema RSA (Rivest-Shamir-Adleman, 1978)

Generació de claus

Cada usuari

1. tria dos nombres primers p i q
2. calcula $n = pq$
3. calcula $\varphi(n) = (p-1)(q-1)$
4. tria e tal que $\gcd(e, \varphi(n)) = 1$
5. calcula $d = e^{-1} \bmod \varphi(n)$
6. dóna a conèixer la clau pública $\{n, e\}$
7. guarda la clau privada d (o bé $\{d, p, q\}$)

Claus RSA

Mòdul n de 1024 bits (309 xifres decimals)

p 84997172489332578490384442745470933566648021786255802843114129
106338875770084181315383045268895951414271920538102125284234191
35275391648150563020216378773

q 12498707513769968201013034478471988740117176620918442925481400
72671578056682003180611331386571634174065507550509272324872789
84454650243654196318594606447 67

n 10623547984416231311262362237670606283574838895956233591624382
11426385162644599890062869006179036928029108937300098743285623
57789700487670277809790099753313862825239708084105047965267520
60747600512765302119035357533637842950893724249852886076997137
38635598015442404762112284450806251799198351285190964723308 91

e 65537

d 17594334471039836222659212311774533561487602633124640951445907
42149012703563557563932187953837872776725811304233138165650179
97679083432743823389453551844338427178964159288543712996418572
64697286846478411297010522536915508500419178724741886020587392
57329691571217940699653246780450866451583806390361244939905 7

Xifratge RSA

Missatge per a l'usuari **(n,e)**

1. Bloc de missatge $\rightsquigarrow m \in \mathbf{Z}/n\mathbf{Z}$
2. Criptograma $c = m^e \bmod n$

Criptograma rebut per l'usuari (n,e,**d**)

1. Missatge $m = c^d \bmod n$ (Teorema d'Euler)
2. $m \in \mathbf{Z}/n\mathbf{Z} \rightsquigarrow$ Bloc de missatge

Signatura RSA

L'usuari A **signa** un missatge m destinat a l'usuari B

1. Rúbrica $r = h(m)^{d_A} \bmod n_A$

   $h(m)$ és un hash del missatge. Per exemple, SHA-256 és un algoritme de hash de 256 bits
2. Signatura digital $s = r^{e_B} \bmod n_B$

L'usuari B **autentica** la signatura del missatge m per part de A

1. $s^{d_B} \bmod n_B = r$
2. $r^{e_A} \bmod n_A = h(m)$

`http://www.catcert.net` `http://www.fnmt.es`

Eficiència RSA

- MCD i inversos modulars d'enters $< n$

Algoritme d'Euclides (estès) $\mathcal{O}(\ell(n)^2)$

- Exponenciació modular d'enters $< n$

Algoritme de quadrats successius $\mathcal{O}(\ell(n)^3)$

$$\begin{aligned} 23 = 10111 \quad &= \quad 2 \cdot 11 + 1 = 2(2 \cdot 5 + 1) + 1 = \cdots = \\ &= \quad 2(2(2(2(0 + 1) + 0) + 1) + 1) + 1 \\ a^{23} \quad &= \quad ((((1 * a)^2 * 1)^2 * a)^2 * a)^2 * a \qquad \text{(8 productes)} \end{aligned}$$

$$65537 = 2^{16} + 1 = 1000000000000001$$

$$a^{65537} = ((((((((((((((((1 * a)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2 * a$$

Primalitat

Generació de primers de longitud ℓ (probabilitat d'error $< 4^{-s}$)

- N enter senar aleatori de ℓ dígits
- N divisible per primers "petits"? (taula $\leftarrow$ Garbell d'Eratòstenes)
- Test de Miller-Rabin amb s bases $\mathcal{O}(\ell^3)$
- $N := N + 2$

Test de Miller-Rabin

- Algoritme probabilístic de Monte-Carlo
- Basat en
  - **Petit teorema de Fermat**: p primer i $(p, b) = 1 \Rightarrow b^{p-1} \equiv 1 \bmod p$
  - p primer $\Rightarrow X^2 = 1 \bmod p$ té exactament dues solucions: 1 i $p - 1$

$$N - 1 = 2^t N_0 \qquad x_0 = b^{N_0} \bmod N \qquad x_{i+1} = x_i^2 \bmod N$$

Primalitat $\in$ **P**

Problema decisional

Donat N enter senar positiu, és N primer?

Miller-Rabin

Primalitat $\in$ **PP**

AKS (Agrawal, Kayal, Saxena)

Primalitat $\in$ **P**

Seguretat RSA

Obtenir el missatge a partir del criptograma?

$$c = m^e \bmod n$$

Extracció d'arrels $e-$èsimes mòdul n?

Es conjectura equivalent a la factorització, podria ser més fàcil

Obtenir la clau privada a partir de la pública?

$$d = e^{-1} \bmod \varphi(n)$$

El càlcul de $\varphi(n) = (p-1)(q-1) = n - p - q + 1$ és equivalent a la factorització de n:

$$\left.\begin{array}{rcl} p+q & = & n - \varphi(n) + 1 \\ (p-q)^2 & = & (p+q)^2 - 4n \end{array}\right\} \quad 2q = (p+q) - (p-q)$$

Factorització

Problema

Donat n enter senar positiu compost, trobar un divisor no trivial de n

- Factorització $\in$ **NP**
- Conjectura: Factorització $\notin$ **P**

Millor algoritme conegut: Number Field Sieve
Usar bases de factors i garbellar per buscar $x^2 \equiv y^2 \bmod n$
Complexitat subexponencial $O(e^{c(\log n)^{1/3}(\log\log n)^{2/3}})$

Rècord (Desembre 2003)

NFS $\longrightarrow$ 576 bits (174 xifres decimals)

RSA-576 = 188198812920607963838697239461650439807
163563379417382700763356422988859715234
665485319060606504743045317388011303396
716199692321205734031879550656996221305
16875930765025705 9

p = 398075086424064937397125500550386491199
064362342526708406385189575946388957261
768583317

q = 472772146107435302536223071973048224632
914695302097116459852171130520711256363
590397527

Índex

La signatura digital DSA (Digital Signature Algorithm)

Paràmetres

- Públics i comuns per a un grup d'usuaris
  - Un primer p de 1024 bits
  - Un primer q de 160 bits, divisor de $p-1$
  - $g = x^{(p-1)/q} \bmod p$, generador d'un subgrup d'ordre q a $\mathbf{F}_p^*$
- 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

$$f_1 = (g^k \bmod p) \bmod q$$
$$f_2 = k^{-1}(SHA1(m) + f_1 r) \bmod q$$

La signatura que acompanya el missatge és (f_1, f_2) (320 bits)

Verificació d'una signatura (f_1, f_2)

1. Calcular
$$w = (f_2)^{-1} \bmod q$$
$$w_1 = SHA1(m)\, w \bmod q$$
$$w_2 = f_1\, w \bmod q$$
$$v = (g^{w_1} u^{w_2} \bmod p) \bmod q$$
2. Acceptar si $v = f_1$

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**

Logaritme discret

$G = \langle g \rangle$ grup cíclic d'ordre n

$$\begin{array}{rcl} \exp_g : \mathbf{Z}/n\mathbf{Z} & \longrightarrow & G \\ a & \mapsto & g^a \end{array}$$

és un isomorfisme de grups

Problema

Fer explícit l'isomorfisme invers

$$\log_g : G \longrightarrow \mathbf{Z}/n\mathbf{Z}$$

Donats $G = \langle g \rangle$ d'ordre n i $b \in G$, trobar $a \in \mathbf{Z}/n\mathbf{Z}$ tal que $b = g^a$

Conjectura

DLOG$\notin \mathbf{P}$

Factorització vs. Logaritme discret

El temps d'execució del millor algoritme per al logaritme discret és aproximadament igual al del millor algoritme de factorització.

Odlyzko(1991)

Factorització d'enters de 110 dígits equival al càlcul de logaritmes discrets mòdul primers de 100 dígits

Històricament

Avenços algorítmics simultanis

Quin és el lligam entre les complexitats d'aquests dos problemes?

Algoritme Index-Calculus

- Base de factors: $B = \{p_1, p_2, \ldots, p_m\}$
- Primera etapa: Garbell + Àlgebra Lineal per obtenir els logaritmes dels elements de B
- Segona etapa:

$$b\, g^n = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m} \Rightarrow \log b + n = \sum e_i \log p_i$$

És el millor algoritme conegut: complexitat subexponencial

$$O(e^{c(\log p)^{1/2}(\log\log p)^{1/2}})$$

(del logaritme discret a $\mathbf{F}_p^*$)

Rècord de Joux i Lercier (2001)

119 xifres decimals

$$
\begin{aligned}
p &= \lfloor 10^{119}\pi \rfloor + 207819 \\
&= 31415926535897932384626433832795028841971693993751058209749445923078164062862089\\
&\quad 98628034825342117067982148086513284384 83 \\
g &= 2 \\
b &= \lfloor 10^{119} e \rfloor \\
&= 27182818284590452353602874713526624977572470936999595749669676277240766303535475\\
&\quad 94571382178525166427427466391932003059 92
\end{aligned}
$$

$$
\begin{aligned}
b &= g\hat{}26211228068581138763600862203819182737039076852065697424303538038219347876743601\\
&\quad 86814498049408403737416414528647307650 82
\end{aligned}
$$

Algoritme de Pohlig-Hellman

- $G =< g >$ d'ordre p^v
- $\zeta = g^{p^{v-1}}$ és una arrel $p-$èsima de la unitat
- El logaritme en base g es redueix al logaritme en base ζ

$$b^{p^{v-1}} = g^{p^{v-1}a} = \zeta^{a_0}$$

on a_0 és el primer $p-$dígit de a

Amb una taula de potències de ζ, $\mathcal{O}(v^2)$ operacions de grup

$DLOG \in \mathbf{P}$!!!

només si $|G|$ és producte de primers petits !

Grups d'utilitat criptogràfica

Operació eficient i cardinal divisible per algun primer gran

Índex

Equacions de Weierstraß

Cúbica no singular

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

Punt de l'infinit $O = (0 : 1 : 0)$

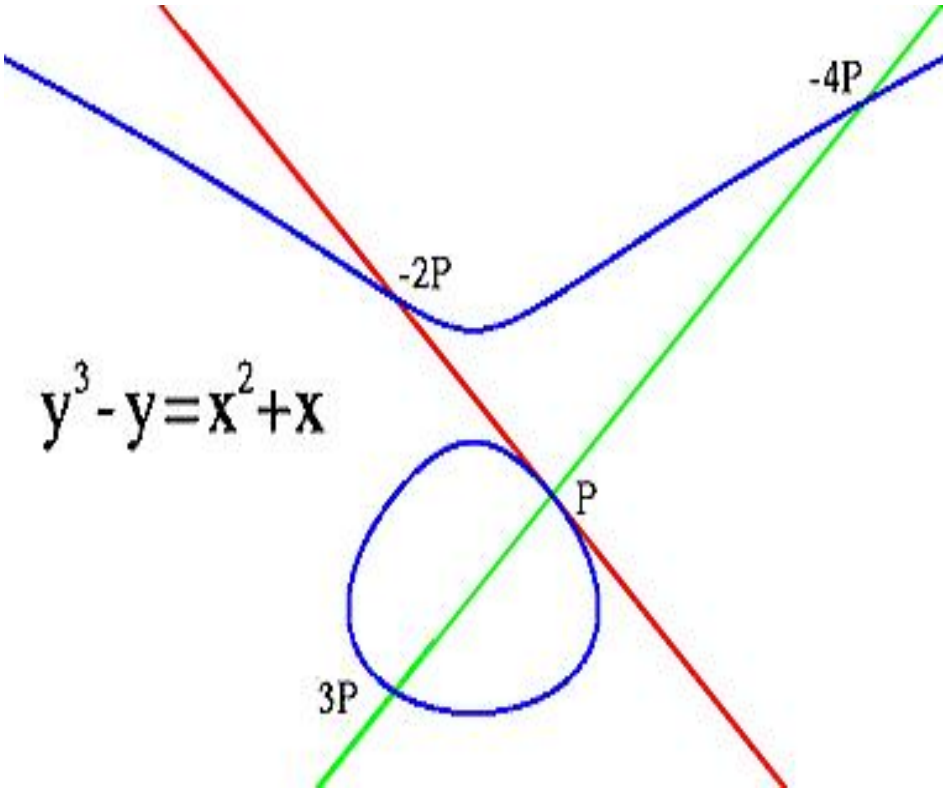
$\mathrm{car}(K) > 3$	$Y^2 = X^3 + aX + b$
$\mathrm{car}(K) = 3$	$Y^2 = X^3 + aX^2 + bX + c$
$\mathrm{car}(K) = 2$	$Y^2 + XY = X^3 + aX^2 + b$

Corbes el.líptiques en criptografia

$K = \mathbf{F}_{2^n}$ o bé $K = \mathbf{F}_p$

Corda-tangent

Tres punts sumen O si, i només si, estan alineats



Llei de grup

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

$$\mu = y_1 - \lambda x_1$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} & x_1 = x_2 \end{cases}$$

$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2$$

$$y_3 = -(\lambda + a_1) x_3 - \mu - a_3$$

$E(\mathbf{F}_q)$ grup abelià finit, amb operació eficient

Cardinal del grup $E(\mathbf{F}_q)$

Interval de Hasse

$$|E(\mathbf{F}_q)| \in [\, q+1-2\sqrt{q}\,,\ q+1+2\sqrt{q}\,]$$

Teorema de Weil

E definida sobre $\mathbf{F}_p$

$$a_p = p+1-|E(\mathbf{F}_p)|$$

$$T^2 - a_p T + p = (T-\alpha)(T-\bar{\alpha})$$

Aleshores

$$|E(\mathbf{F}_{p^m})| = 1 + p^m - \alpha^m - \bar{\alpha}^m$$

Corba K-163 del FIPS 186-2

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

$$E(\mathbf{F}_2) = \{O, (0,1)\} \quad \Rightarrow \quad a_2 = 2 + 1 - 2 = 1$$

$$T^2 - T + 2 = (T - \alpha)(T - \bar{\alpha}) \quad \Rightarrow \quad \alpha = \frac{1 + i\sqrt{7}}{2}$$

$$t = \alpha^{163} + \bar{\alpha}^{163} = -4835703278458516698824704$$

$$|E(\mathbf{F}_{2^{163}})| = 2^{163} + 1 - t$$

$$= 2 \cdot 5846006549323611672814741753598448348329118574063$$

Corba P-192 del FIPS 186-2

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

$$
\begin{aligned}
p &= 2^{192} - 2^{64} - 1 \\
&= 6277101735386680763835789423 \\
&\quad 207666416083908700390324961279 \\
B &= 64210519e59c80e70fa7e9ab72243049 \\
&\quad feb8deecc146b9b1 \\
|E(\mathbf{F}_p)| &= 6277101735386680763835789423 \\
&\quad 176059013767194773182842284081 = q
\end{aligned}
$$

Comptar punts de manera eficient

Algoritme de Schoof

$T^2 - a_p T + p$ és el polinomi característic de l'endomorfisme de Frobenius operant a $E[\ell]$

Complexitat: $\mathcal{O}((\log p)^8)$

Algoritme SEA

Atkin-Elkies: Introdueixen la corba modular $X_0(\ell)$ per treballar amb isogènies de grau ℓ. Complexitat: $\mathcal{O}((\log p)^6)$

- Construcció de corbes el.líptiques amb cardinal prefixat usant la teoria de multiplicació complexa
- Mètodes $p-$àdics (Satoh, AGM) en característica 2 i 3

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
- Signatura (f_1, f_2)
  - $kP = (x_1, y_1)$ amb $1 < k < q - 1$ aleatori
  - $f_1 = x_1 \bmod q$
  - $f_2 = k^{-1}\,(\,SHA1(m) + f_1 r\,) \in \mathbf{Z}/q\mathbf{Z}$
- Verificació
  - $w_1 = SHA1(m) f_2^{-1} \bmod q$
  - $w_2 = f_1 f_2^{-1} \bmod q$
  - $w_1 P + w_2 Q = (x_0, y_0)$
  - Acceptar si $x_0 \bmod q = f_1$

Per què corbes el.líptiques?

Si treballem a $E(\mathbf{F}_q)$, com es trien punts P_i tals que molts punts de la corba es puguin escriure fàcilment com

$$P = \sum n_i P_i \qquad \textbf{?}$$

(bases de factors). No hi ha una noció de punt irreductible.
No es pot usar INDEX-CALCULUS, l' únic algoritme subexponencial conegut $\Rightarrow$ **mateixa seguretat amb claus més petites**

ECC challenges

100.000 dòlars si resoleu ECC2K-358, logaritme discret a un $E(\mathbf{F}_p)$ amb p de 359 bits `http://www.certicom.com`

Índex

Substituir corbes el.líptiques per varietats abelianes?

Jacobianes de corbes hiperel.líptiques

$\mathcal{C}: \ Y^2 + h(X)Y = f(X)$ sobre $\mathbf{F}_q$ $\quad (\deg f = 2g+1, \ \deg h \leq g)$

Jacobiana: $\mathrm{Jac}(\mathcal{C}) = \mathrm{Div}_0(\mathcal{C})/\mathrm{Pr}(\mathcal{C})$ varietat abeliana de dimensió g

Representació polinomial de divisors

- Operació eficient (Algoritme de Cantor)
- Cardinal: algoritmes anàlegs al cas el.líptic
- Noció d'irreductibilitat i base de factors: es pot usar un algoritme index-calculus (Adleman-DeMarrais-Huang, Enge-Gaudry)
- Algoritme de Gaudry ($4 \leq g \leq 10$). Si $g = 2$ o $g = 3$, el millor algoritme és exponencial

Estratègia

Traslladar el problema de logaritme discret des de E a Jac($\mathcal{C}$)

corba el.líptica	E	$\rightsquigarrow$	A	varietat abeliana
corba hiperel.líptica	$\mathcal{C}$	$\hookrightarrow$	A	

Ús criptogràfic de la restricció de Weil

Tendències

- Criptografia amb corbes de gènere 3 no hiperel.líptiques
- Criptografia basada en aparellaments $G \times G \to H$

- Weil: $E(\mathbf{F}_q)[\ell] \times E(\mathbf{F}_q)[\ell] \longrightarrow \mu_\ell$
- Tate: $E(K)[\ell] \times E(K)/\ell E(K) \longrightarrow K^*/K^{*\ell}$
- Tate-Lichtenbaum: $\mathrm{Jac}(\mathcal{C})(\mathbf{F}_q)[\ell] \times \mathrm{Jac}(\mathcal{C})(\mathbf{F}_q)[\ell] \longrightarrow \mu_\ell$

- Criptografia usant grups de Brauer

Prof. G. Frey ens ho explicarà la setmana vinent !

Referències


Whitfield Diffie.
Ultimate Cryptography.
Comunications of the ACM, 44(3): 84–87, 2001.

Torna

Referències

Fausto Montoya
La criptografía cuántica, ¿realidad o ficción?
http://www.iec.csic.es/ fausto/publica/Montoya04.pdf

SECOQC - Development of a Global Network for Secure Communication based on Quantum Cryptography
Projecte de la Unió Europea endegat a Austria l'abril de 2004 i finançat amb 11,4 milions d'Euros
http://www.secoqc.net/index.html

Susan Landau
Communications Security for the Twenty-first Century: The Advanced Encryption Standard
AMS Notices, Abril 2000

◂ Torna

Referències


Üli Maurer
Cryptography 2000 $\pm$ 10
Informatics: 10 Years Back, 10 Years Ahead. Lecture Notes in Computer Science, 2000: 63–85, 2001
◂ Torna