Sobre el problema de Diffie-Hellman decisional en gènere 2

Jordi Pujolàs

STNB'07

1 de febrer del 2007

Outline

- El problema de Diffie-Hellman decisional
- Distortion maps
- Exemples

Outline

- El problema de Diffie-Hellman decisional
- Distortion maps
- Exemples

problema de Diffie-Hellman decisional

El problema del Logaritme Discret en un grup cíclic $\langle g \rangle$:

donat $g' \in \langle g \rangle$, trobar e tal que $g' = g^e$

El problema de Diffie-Hellman decisional en un grup G (producte de cíclics $\langle g \rangle$ on pLD és intractable):

donats $g, g^a, g^b \in G$, decidir si $g^{ab} = g^c$ per a qualsevol altre $g^c \in G$

problema de Diffie-Hellman decisional

El problema del Logaritme Discret en un grup cíclic $\langle g \rangle$:

donat $g' \in \langle g \rangle$, trobar e tal que $g' = g^e$

El problema de Diffie-Hellman decisional en un grup G (producte de cíclics $\langle g \rangle$ on pLD és intractable):

donats $g, g^a, g^b \in G$, decidir si $g^{ab} = g^c$ per a qualsevol altre $g^c \in G$

“pDHd té sol·lució eficient” necessari en esquemes d’encriptació basats en la identitat i en esquemes de signatura curta

Per nosaltres, G grup de punts de $Jac(C)$ amb C corba de gènere 2 sobre $\mathbb{F}_q$

G equipat amb un aparellament bilineal, no-degenerat, computable eficientment

$$e_l(\ ,\ ) : G \times G \to \mu_l$$

Per nosaltres, G grup de punts de $Jac(C)$ amb C corba de gènere 2 sobre $\mathbb{F}_q$

G equipat amb un aparellament bilineal, no-degenerat, computable eficientment

$$e_l(\ ,\ ) : G \times G \rightarrow \mu_l$$

que és útil per sol·lucionar pDHd:

si $e_l(g^a, g^b)$ és no trivial, aleshores $e_l(g^a, g^b) = e_l(g, g^c)$ implica $ab = c$

Com que $e_l(g^a, g^b)$ i $e_l(g, g^c)$ son eficientment calculables,

pDHd és sol·lucionable a la pràctica...

Outline

- pDHd
- Distortion maps
- Exemples

Distortion maps

Per assegurar $e_l(\ ,\ ) \neq 1$, Verheul, Schoof (2002) defineixen:

Un **distortion map** respecte de $e_l(\ ,\ )$ i $g^a, g^b \in G$ és un homomorfisme de grups φ tal que $e_l(g^a, \varphi(g^b)) \neq 1$

Distortion maps

Per assegurar $e_l(\ ,\ ) \neq 1$, Verheul, Schoof (2002) defineixen:

Un **distortion map** respecte de $e_l(\ ,\ )$ i $g^a, g^b \in G$ és un homomorfisme de grups φ tal que $e_l(g^a, \varphi(g^b)) \neq 1$

Per a corbes el·líptiques supersingulars, Galbraith & Rotger (2004) donen un algoritme que sol·luciona pDHd.

Sobre $\mathrm{Jac}(C)$

- varietat abeliana de dim 2, $\mathrm{Jac}(C)(\mathbb{F}_q)$ grup abelià finit
- l-torsió $\mathrm{Jac}(C)[l]$ té rang 4, per a primers $l \neq q$ (prou grans com per fer intractable el pLD)
- elements i llei de grup computables eficientment

Sobre $\mathrm{Jac}(C)$

- varietat abeliana de dim 2, $\mathrm{Jac}(C)(\mathbb{F}_q)$ grup abelià finit
- l-torsió $\mathrm{Jac}(C)[l]$ té rang 4, per a primers $l \neq q$ (prou grans com per fer intractable el pLD)
- elements i llei de grup computables eficientment
- àlgebra d'endomorfismes $\mathrm{End}^0(\mathrm{Jac}(C))$ semisimple sobre $\mathbb{Q}$ i de dimensió com a molt $16 = (2g)^2$
- automorfismes de C es poden veure a $\mathrm{End}^0(\mathrm{Jac}(C))$ com a isogènies
- l'algoritme de Miller per calcular l'aparellament de Tate $e_l(\ ,\ )$ es pot adaptar sense problemes

En el nostre cas

- $G \cong \mathrm{Jac}(C)[l] \cong Cl^0(\mathcal{O}_C)[l]$
- $\mathrm{Jac}(C)$ superfície abeliana simple, per tant l'endomorfisme de frobenius π "elevar a q" genera una extensió de grau 4

En el nostre cas

- $G \cong \mathsf{Jac}(C)[l] \cong Cl^0(\mathcal{O}_C)[l]$
- $\mathsf{Jac}(C)$ superfície abeliana simple, per tant l'endomorfisme de frobenius π "elevar a q" genera una extensió de grau 4
- $\mathsf{Jac}(C)$ supersingular (isògena sobre $\bar{\mathbb{F}}_q$ a un producte de corbes el·líptiques supersingulars)
- π satisfà un polinomi ciclotòmic reescalat
- π es torna un enter $\in \mathbb{Z}$ després d'extendre el cos base a $\mathbb{F}_q^k$ per certa k ($\sim$ "embedding degree") i de fet $G = \mathsf{Jac}(C)(\mathbb{F}_q^k)[l]$

Distortion maps: existència

Siguin D_1, D_2 elements no trivials de $\mathsf{Jac}(C)$ d'ordre l. Aleshores hi ha un element $\phi \in \mathsf{End}(\mathsf{Jac}(C))$ tal que $e_l(D_1, \phi(D_2)) \neq 1$

Distortion maps: existència

Siguin D_1, D_2 elements no trivials de $\mathrm{Jac}(C)$ d'ordre l. Aleshores hi ha un element $\phi \in \mathrm{End}(\mathrm{Jac}(C))$ tal que $e_l(D_1, \phi(D_2)) \neq 1$

$K := \mathbb{F}_{q^k}$, $H := \mathrm{Gal}(\overline{K}/K)$

$\mathrm{Jac}(C)$ supersingular $\Rightarrow$ $\mathrm{End}(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ té rang 16

Pel teorema de Tate $\mathrm{End}_K(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ és isomorf a $\mathrm{End}_H(T_l(\mathrm{Jac}(C)))$, homomorfismes que commuten amb el frobenius "elevar a q^k", per tant tots

Distortion maps: existència

Siguin D_1, D_2 elements no trivials de $\mathrm{Jac}(C)$ d'ordre l. Aleshores hi ha un element $\phi \in \mathrm{End}(\mathrm{Jac}(C))$ tal que $e_l(D_1, \phi(D_2)) \neq 1$

$K := \mathbb{F}_{q^k}$, $H := \mathrm{Gal}(\overline{K}/K)$
$\mathrm{Jac}(C)$ supersingular $\Rightarrow$ $\mathrm{End}(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ té rang 16

Pel teorema de Tate $\mathrm{End}_K(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ és isomorf a $\mathrm{End}_H(T_l(\mathrm{Jac}(C)))$, homomorfismes que commuten amb el frobenius "elevar a q^k", per tant tots

Com que $T_l(\mathrm{Jac}(C)) \cong \mathbb{Z}_l^4$, aleshores
$\mathrm{End}_H(T_l(\mathrm{Jac}(C))) \cong M_4(\mathbb{Z}_l)$

Distortion maps exist

Per tant $\mathrm{End}_K(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong M_4(\mathbb{Z}_l)$

i per tant $\mathrm{End}_K(\mathrm{Jac}(C)) \cong \mathrm{End}(\mathrm{Jac}(C))$ també té rang 16

$\mathrm{End}_K(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}/l\mathbb{Z} \cong M_4(\mathbb{Z}/l\mathbb{Z})$

Prenem $D_3 \in \mathrm{Jac}(C)[l]$ tal que $e_l(D_1, D_3) \neq 1$

Prenem una matriu $\Phi \in M_4(\mathbb{Z}/l\mathbb{Z})$ que correspongui a una aplicació de $\langle D_2 \rangle$ en $\langle D_3 \rangle$

Prenem ϕ una antiimatge de Φ en $\mathrm{End}(\mathrm{Jac}(C))$

Aleshores $e_l(D_1, \phi(D_2)) \neq 1$

Outline

- pDHd
- Distortion maps
- Exemples

Exemples

a) $y^2 = x^5 + 1$ sobre $\mathbb{F}_p$

amb $p \equiv 2, 3 \bmod 5$

b) $y^2 + y = x^5 + x^3 + 1$ sobre $\mathbb{F}_{2^m}$

amb $m \equiv 1, 5 \bmod 6$

Exemples

a) $y^2 = x^5 + 1$ sobre $\mathbb{F}_p$

amb $p \equiv 2, 3$ mod 5

b) $y^2 + y = x^5 + x^3 + 1$ sobre $\mathbb{F}_{2^m}$

amb $m \equiv 1, 5$ mod 6

Automorfismes

a) $\xi_5 : (x, y) \longmapsto (\xi_5 x, y)$

amb ξ_5 una arrel $5ena$ de la unitat

b) $\sigma_\omega : (x, y) \longmapsto (x + \omega, y + s_2 x^2 + s_1 x + s_0)$

amb ω una arrel qualsevol de $x^{16} + x^8 + x^2 + x$,
$s_2 = \omega^8 + \omega^4 + \omega$, $s_1 = \omega^4 + \omega^2$, $s_0^2 + s_0 = \omega^5 + \omega^3$

Exemple a

$C : y^2 = x^5 + 1$ sobre $\mathbb{F}_p$, $p \equiv 2, 3$ mod 5

Polinomi car de π: $X^4 + q^2 \Rightarrow \mathrm{Jac}(C)$ simple, supersingular, embedding degree $k = 4$

Cossos $X^4 + X^3 + X^2 + X + 1$, $X^4 + q^2$ ficats en $\mathrm{End}^0(\mathrm{Jac}(C))$

Idea: sumes de productes de π, ξ_5 son distortion maps respecte de qualsevol parella de divisors de $\mathrm{Jac}(C)[l]$:

Exemple a

$C : y^2 = x^5 + 1$ sobre $\mathbb{F}_p$, $p \equiv 2, 3$ mod 5

Polinomi car de π: $X^4 + q^2 \Rightarrow \mathrm{Jac}(C)$ simple, supersingular, embedding degree $k = 4$

Cossos $X^4 + X^3 + X^2 + X + 1$, $X^4 + q^2$ ficats en $\mathrm{End}^0(\mathrm{Jac}(C))$

Idea: sumes de productes de π, ξ_5 son distortion maps respecte de qualsevol parella de divisors de $\mathrm{Jac}(C)[l]$:

com que $\pi^j \xi_5 \pi^{-j} = \xi_5^{p^j}$ i $p \equiv 2, 3$ mod 5, conjugació té ordre 4 i correspon a un generador σ del grup cíclic $\mathrm{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$

Exemple a

$C : y^2 = x^5 + 1$ sobre $\mathbb{F}_p$, $p \equiv 2, 3$ mod 5

Polinomi car de π: $X^4 + q^2 \Rightarrow \mathrm{Jac}(C)$ simple, supersingular, embedding degree $k = 4$

Cossos $X^4 + X^3 + X^2 + X + 1$, $X^4 + q^2$ ficats en $\mathrm{End}^0(\mathrm{Jac}(C))$

Idea: sumes de productes de π, ξ_5 son distortion maps respecte de qualsevol parella de divisors de $\mathrm{Jac}(C)[l]$:

com que $\pi^j \xi_5 \pi^{-j} = \xi_5^{p^j}$ i $p \equiv 2, 3$ mod 5, conjugació té ordre 4 i correspon a un generador σ del grup cíclic $\mathrm{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$

En conseqüència,

$\mathrm{End}^0(\mathrm{Jac}(C)) \cong \mathbb{Q}(\xi_5) \oplus \pi\mathbb{Q}(\xi_5) \oplus \pi^2\mathbb{Q}(\xi_5) \oplus \pi^3\mathbb{Q}(\xi_5)$

Exemple a

$\mathrm{End}^0(\mathrm{Jac}(C))$ 16-dimensional, central, simple $\mathbb{Q}$-àlgebra que conté un cos de nombres cíclic de grau 4 (generat per ξ_5)

"crossed-product algebra" sobre $\mathbb{Q}$ (Albert, 1930's,40's)

Exemple a

$\mathrm{End}^0(\mathrm{Jac}(C))$ 16-dimensional, central, simple $\mathbb{Q}$-àlgebra que conté un cos de nombres cíclic de grau 4 (generat per ξ_5)

"crossed-product algebra" sobre $\mathbb{Q}$ (Albert, 1930's,40's)

$\{1, \pi, \pi^2, \pi^3\}$ $\mathbb{Q}(\xi_5)$-base cíclica de $\mathrm{End}^0(\mathrm{Jac}(C))$

$$\{1, \underbrace{2\xi_5 + 2\xi_5^{-1} + 1}_{\Delta}, \underbrace{\xi_5 - p\xi_5^2\pi^2 + p\xi_5^3\pi^2}_{\rho}, \Delta\rho\}$$

$\mathbb{Q}(\pi)$-base no cíclica de $\mathrm{End}^0\mathrm{Jac}(C)$

Exemple **a**

En conseqüència

$$\phi = \sum_{i,j} \lambda_{i,j} \pi^i \xi_5^j$$

amb $\lambda_{i,j} \in \mathbb{Q}$

Detall: necessitem suposar que l i $mcm(\lambda_{i,j})$ siguin coprimers

cota de l' índex de $\mathrm{End}(\mathrm{Jac}(C))$ en l'ordre maximal

Altres exemples CM

Van Wamelen (1999) llista totes les corbes de gènere 2 sobre $\mathbb{Q}$ amb CM per un cos quàrtic i descriu la CM-isogènia α, per exemple

$$C : y^2 = x^5 - 3x^4 - 2x^3 + 6x^2 + 3x - 1$$

CM amb $\alpha^4 + 4\alpha^2 + 2 = 0$, α arrel del char poly de la isogènia (de grau > 1) amb segones coordenades

Altres exemples CM

Van Wamelen (1999) llista totes les corbes de gènere 2 sobre $\mathbb{Q}$ amb CM per un cos quàrtic i descriu la CM-isogènia α, per exemple

$$C : y^2 = x^5 - 3x^4 - 2x^3 + 6x^2 + 3x - 1$$

CM amb $\alpha^4 + 4\alpha^2 + 2 = 0$, α arrel del char poly de la isogènia (de grau > 1) amb segones coordenades

$$y_1(x,y) = \frac{(-\alpha^3 - 4\alpha)yx_1}{2(x+1)} + \frac{1/2(-\alpha^3 - 4\alpha)xy + (\alpha^3 + 3\alpha)y}{(x+1)}$$

$$y_2(x,y) = \frac{(-\alpha^3 - 4\alpha)yx_1}{2(x+1)} + \frac{1/2(-\alpha^3 - 2\alpha)xy + (\alpha^3 + 4\alpha)y}{(x+1)}$$

Altres exemples CM

Les mateixes idees de l'exemple a) valen

- si p primer inert en $\mathbb{Q}(\alpha)$ aleshores les corbes de VW tenen reducció supersingular
- conjugació proporciona un generador del grup cíclic $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$
- π satisfà el mateix polinomi $X^4 + p^2$
- per tant π, α proporcionen distortion maps per a qualsevol parella de divisors

Exemple b

$C : y^2 + y = x^5 + x + 1$ over $\mathbb{F}_{2^m}$, $m \equiv 1, 5$ mod 6
$\sigma_\omega : (x, y) \longmapsto (x + \omega, y + s_2 x^2 + s_1 x + s_0)$

π satisfà $X^4 \pm 2^{(m+1)/2} X^3 + 2^m X^2 \pm 2^{(3m+1)/2} X + 2^{2m}$
“quasi simètric” $\Rightarrow$ Jac(C) simple, supersingular, embedding degree $k = 12$

Com que $m \equiv 1, 5$ mod 6 el “polinomi dels automorfismes” $x^{16} + x^8 + x^2 + x$ factoritza com

$$(x^6+x^5+x^3+x^2+1)(x^3+x^2+1)(x^3+x+1)(x^2+x+1)(x+1)x$$

Exemple b

$\sigma_1 \notin \mathbb{Q}$ està al centre
$\mathrm{End}^0(\mathrm{Jac}(C))$ no central, conté un cos de nombres de grau 4 no cíclic, i altres subcossos quadràtics

τ arrel de $x^6 + x^5 + x^3 + x^2 + x + 1$
θ arrel de $x^2 + x + 1$
ξ arrel de $x^3 + x^2 + 1$

σ_ω's satisfan $X^2 + 1$ com a molt
sumes de productes de $\pi, \sigma_\tau, \sigma_\theta, \sigma_\xi$ proporcionen distortion maps per a tota parella de $\mathrm{Jac}(C)(\mathbb{F}_{2^{12m}})[l]$