数理解析研究所講究録 1420 巻 2005 年 41-62

A Weil Descent Attack against Elliptic Curve Cryptosystems over Quartic Extension Fields

Institute of Information Security
Seigo Arita

(長尾(関東学院大)・松尾(IISEC)・志村(中大)各氏との共同研究)

目次

1. Introduction

離散対数型暗号

G:有限アーベル群
$G \ni g$を固定

指数関数E

$$\begin{aligned} E : Z &\to G \\ n &\mapsto g^n \end{aligned}$$

離散対数問題

$\langle g \rangle \ni h$ に対して $E(n) = h$ となる n を求めよ

離散対数問題が困難ならば,
群Gを用いて公開鍵暗号が構成できる(ElGamal)

超楕円曲線暗号

GF(q)上の種数gの超楕円曲線 H （$g \ll q$）

$$y^2 = f(x) = x^{2g+1} + a_1 x^{2g} + \cdots + a_{2g+1} \quad (a_i \in GF(q))$$

超楕円曲線Hのヤコビ群 J_H

$$J_H = \{ (u(x), v(x)) \mid \deg v < \deg u \leqq g, \; v^2 = f \pmod u \}$$
$$\# J_H \fallingdotseq q^g$$

超楕円曲線H上の離散対数問題(DLP)

$J_H \ni D_1, D_2$ に対して $D_2 = n D_1$ となるn を求めよ

Pollardのrhoアルゴリズム

$J_H \ni D_1, D_2$

random walk によって
D_1, D_2のランダムな線形和R_i を計算していく

$$R_i = \alpha_i D_1 + \beta_i D_2 \quad (i=1,2,3,\ldots)$$

衝突$R_i = R_j$ が起きると

$$\alpha_i D_1 + \beta_i D_2 = \alpha_j D_1 + \beta_j D_2$$

$$\therefore \; D_2 = (\alpha_i - \alpha_j)/(\beta_j - \beta_i) \, D_1$$

↑

$(\#J_H)^{1/2}$ step が必要

Gaudry's 法

$J_H \ni D$ が <u>smooth</u>
D が定義体上の有理点の和

$FB = \{ P_1, P_2, \ldots, P_w \}$: 超楕円曲線H上の全ての有理点を計算しておく ($w \fallingdotseq q$, $O(q)$)

$J_H \ni D_1, D_2$

random walk によって D_1, D_2 のランダムな線形和 R_i を計算:

$$R_i = \alpha_i D_1 + \beta_i D_2 \quad (i=1,2,3,\ldots)$$

smooth な R_i を集める

Gaudry's 法(2)

smooth な R_i がみつかると: (g! 個に一つは smooth)

$R_i = (u(x), v(x))$
$u(x) = \prod (x - x_i)$: GF(q)上1次の既約因子に分解 ($O(q)$)
$y_i = v(x_i) \quad (i=1,\ldots,g)$

$$R_i = (x_1,y_1) + (x_2,y_2) + \ldots + (x_g, y_g)$$

$$= \Sigma_k \ m_{i,k} P_k$$

このようにして

smoothなR_i ←→ $[m_{i,1}, m_{i,2}, \ldots, m_{i,w}]$

Gaudry's 法(3)

smooth な $R_i = \Sigma_k\ m_{i,k} P_k$ が w'(>w) 個あつまると ($O(q^2)$):

$$M := (m_{i,k}) \ : \ w' \times w \text{ 行列, 疎}$$

$(\gamma_i) \in \mathrm{Ker}\ {}^tM$ を求めて ($O(q^2)$)

$$\Sigma_i\ \gamma_i R_i = 0$$

$$\therefore\ \Sigma_i\ \gamma_i(\alpha_i D_1 + \beta_i D_2) = 0$$

$D_2 = \lambda\ D_1$ を 代入すると

$$\lambda = (-\Sigma\ \gamma_i\ \alpha_i)(\Sigma\ \gamma_i\ \beta_i)^{-1}$$

Gaudry法

超楕円曲線上のDLPに対する攻撃法
rho アルゴリズムに因子基底を導入
$O(q^2 \log^c(q))$ (定義体: GF(q), 種数g ≪ q)
→ 種数を大きくしても, q は小さくできない！

C_{ab}曲線や superelliptic 曲線に対しても
Gaudry's 法 は 有効

C_{ab}曲線と superelliptic 曲線

C_{ab}曲線: (a,b) = 1

$$\sum_{0\le i\le b,0\le j\le a,ai+bj\le ab} \alpha_{i,j} x^i y^j = 0$$

superelliptic 曲線: (n, δ) = 1

$$y^n = a_\delta x^\delta + \dots + a_0$$

明らかに,

superelliptic 曲線 $\subset$ C_{ab}曲線

実装実験 ー パラメータ

有限体	GF(84211)
定義方程式	1 + 24740 x^7 + 32427 y^3 = 0
種数	6
ヤコビアンの位数	43・8068970623016239605318986617
自己同型の位数	3・7

17ビットの素体上の93ビットC_{37}

自己同型ϕ

$$\phi(x, y) = (\zeta_7 x, \zeta_3 y)$$: 位数21

よって

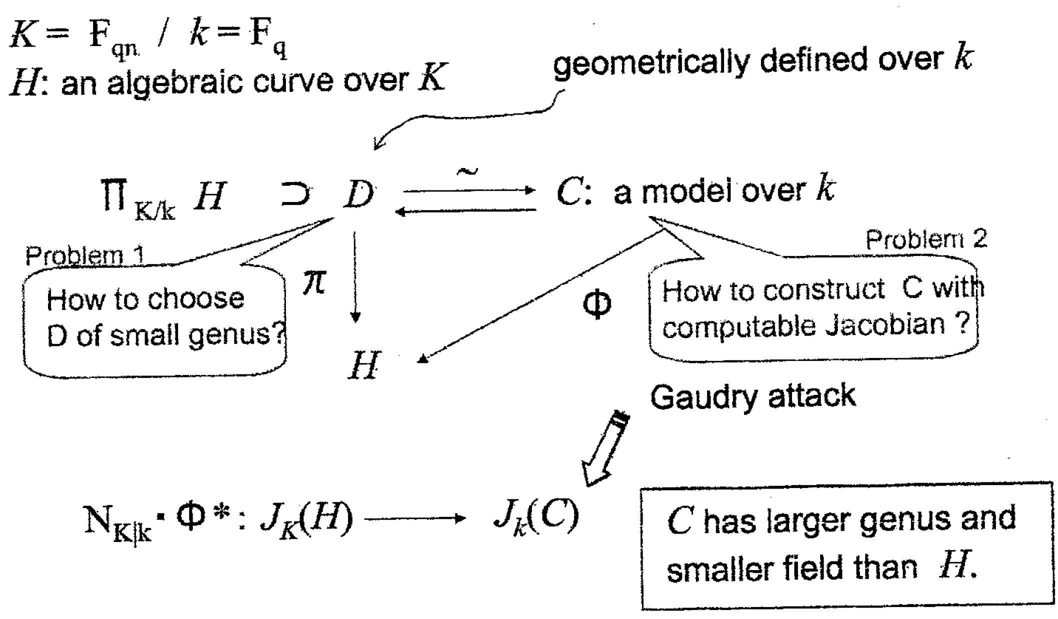
#FB = 84211 / 21 = 4010.・・

実装実験 ー 結果

有理点の収集 (PARI-GP)	5分13秒
スムースな要素の収集 (C)	2時間33分6秒
一次方程式の求解 (C)	32分2秒
合計	3時間11分21秒

17ビットの素体上の93ビットC_{37} 曲線に対するGaudry's variant の適用,
266 MHz Pentium II

Weil descent attack



Weil descent attack
possibly applied against
an algebraic curve cryptosystem over a composition field

The concept: Frey '98
(some of) ECC over char. 2 finite fields: Gaudry,Hess,Smart '00
(some of) HCC over char. 2 finite fields: Galbraith '00
(some of) ECC over char. 3 finite fields : Arita '00
(some of) ECC, HCC over odd char. finite fields : Diem '00

Our contributions

k=GF(q), ch(q)$\neq$2,3
k_2: quadratic ext. of k, k_4: quartic ext. of k
E: elliptic curve over k_4

$$E: v^2 = u^3 + \alpha u + \beta \qquad (\alpha, \beta \in k_4)$$

$$\Pi \uparrow$$

$$H: y^2 = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f \qquad (a,b,c,d,e,f \in k_2)$$

$\Leftarrow$ GHS attack

- In this talk, we show that
  many elliptic curve cryptosystems over quartic degree finite fields
  come under Weil descent attack.

2. Scholten form

Scholten form

k=GF(q) (ch(k) $\neq$ 2,3)
k_4: quartic ext. of k

E_n: Scholten form (of elliptic curve) over k_4

$$v^2 = \alpha u^3 + \beta u^2 + \beta^{q^2} u + \alpha^{q^2}$$
$$(\alpha, \beta \in k_4)$$

Scholten showed

- $\Pi_{k4|k2} E_n \sim J_{k2}(H)$ ($\exists$ H: genus 2 HEC)
- E/k_4 has full 2-torsions $\Rightarrow$ E has Scholten form

We clarify conditions to be Scholten form.

Scholten form is covered by H

$$E_n: v^2 = \alpha u^3 + \beta u^2 + \beta^{q^2} u + \alpha^{q^2} \quad (\alpha, \beta \in k_4)$$

$$\uparrow \quad (u, v) = \prod ((x-c)^2/(x-c^{q^2})^2,\ y/(x-c^{q^2})^3) \quad (c \in k_4 - k_2)$$

$$H: y^2 = \alpha (x-c)^6 + \beta (x-c)^4 (x-c^{q^2})^2 + \beta^{q^2} (x-c)^2 (x-c^{q^2})^4 + \alpha^{q^2} (x-c^{q^2})^6$$

- H: defined over k_2
- DLP on E_n/k_4 → DLP on H/k_2

When E_w can be in Scholten form ?

E_w : $y^2 = f(x)$: Weierstrass form / k_4, f(x): irreducible / k_4

$$\xrightarrow[\substack{x \to A x + B \\ y \to C y}]{} \quad E_n: y^2 = F(x): \text{Scholten form} / k_4 \qquad (A,B,C \in k_4)$$

δ : a root of $F(x) = a x^3 + b x^2 + b^{q^2} x + a^{q^2}$

$$\delta^{-q^2} \in \{ \delta, \delta^{q^4}, \delta^{q^8} \}$$

$$\delta^{-q^2} = \delta \Rightarrow \delta^{q^4-1} = 1 \Rightarrow \delta \in k_4$$

$$\delta^{-q^2} = \delta^{q^4} \Rightarrow \delta^{q^2} = \delta^{-1} \Rightarrow \delta \in k_4$$

$$\therefore \quad \delta^{1+q^6} = 1$$

Proposition 2

$E_w : y^2 = f(x)$: Weierstrass form / k_4, $f(x)$: irreducible / k_4

E_w is isomorphic to Scholten form E_n over k_4

$\Leftrightarrow$

(*) $\exists A(\neq 0) \in k_4,\ B \in k_4$
$\gamma = A\delta + B,\ \ \delta^{1+q^6} = 1 \quad (\gamma$: a root of $f(x)$)

Then,

$a := -A^{2-q^2}\delta^{1+q^4-q^2},\ \ b := -A(\delta + \delta^{q^4} + \delta^{q-2})$

$E_w \to E_n : y^2 = a\,x^3 + b\,x^2 + b^{q^2}\,x + a^{q^2}$
$(\, y \to a\,y,\ x \to a\,x + B\,)$

$f(x)$: irreducible / k_4, γ : a root of $f(x)$

$$d(\gamma) := (\gamma^{q^2+q^4} - \gamma^{q^2+1}) + (\gamma^{q^6+q^8} - \gamma^{q^6+q^4}) + (\gamma^{q^{10}+1} - \gamma^{q^{10}+q^8})$$

$d(\gamma) \neq 0$ $\Leftrightarrow$ (*) $\exists A(\neq 0) \in k_4,\ B \in k_4$ $\gamma = A\delta + B,\ \ \delta^{1+q^6} = 1 \quad (\gamma$: a root of $f(x)$)

$\because$ $(\gamma - B)^{1+q^6} \in k_2$

$\Leftrightarrow (\gamma - B)^{q^2} (\gamma^{q^6} - B^{q^6})^{q^2} = (\gamma - B)(\gamma^{q^6} - B^{q^6})$

$\Leftrightarrow \begin{cases} g(B) = 0 \\ g^{q^2}(B^{q^2}) = 0 \end{cases}$ Bの連立1次方程式

E_w: $y^2 = f(x)$ with $f(x)$: irreducible / k_4, γ : a root of $f(x)$

$$d(\gamma) = (\gamma^{q2+q4} - \gamma^{q2+1}) + (\gamma^{q6+q8} - \gamma^{q6+q4}) + (\gamma^{q10+1} - \gamma^{q10+q8})$$

$$d(\gamma) = 0 \Leftrightarrow j(E_w) \in k_2$$

∵

$$j(E_w) \in k_2 \Leftrightarrow \gamma = A\alpha + B \quad (A, B \in k_4, \ \alpha \in k_6)$$
$$\Leftrightarrow d(\gamma - B) = 0$$
$$\Leftrightarrow d(\gamma) = 0$$

When E_w can be in Scholten form

E_w : $y^2 = f(x)$: Weierstrass form / k_4

- $f(x)$: 既約 / k_4
  $j(E_w) \in k_4 - k_2$ ならば、
  E_wはScholten formに k_4上で変換される。

- $f(x)$ = 1次式 x 既約2次式 / k_4
  E_wはScholten formで表されない。

- $f(x)$: 完全分解 / k_4
  E_wは常にScholten formに k_4上で変換される。

3. GHS attack for genus 2 HEC

GHS attack in our case

$k_2 = F_{q^2} \mid k = F_q$ (of char. $\neq 2$), σ : Frob. Automorphism of k_2/k

$H: y^2 = x^6 + a\,x^5 + b\,x^4 + c\,x^3 + d\,x^2 + e\,x + f \quad (a,b,c,d,e,f \in k_2)$

$\sigma : x_1 \rightarrow x_2,\ y_1 \rightarrow y_2$

$$\Pi_{k2/k}\, H : \begin{cases} y_1^2 = x_1^6 + a\,x_1^5 + b\,x_1^4 + c\,x_1^3 + d\,x_1^2 + e\,x_1 + f \\ y_2^2 = x_2^6 + a^q x_2^5 + b^q x_2^4 + c^q x_2^3 + d^q x_2^2 + e^q x_2 + f^q \end{cases}$$

$\cup \qquad x := x_1 = x_2$

GHS-section D:

$$\begin{cases} y_1^2 = x^6 + a\,x^5 + b\,x^4 + c\,x^3 + d\,x^2 + e\,x + f \\ y_2^2 = x^6 + a^q x^5 + b^q x^4 + c^q x^3 + d^q x^2 + e^q x + f^q \end{cases}$$

Assumption for non-singularity

$H: y^2 = x^6 + a\,x^5 + b\,x^4 + c\,x^3 + d\,x^2 + e\,x + f$ on $k_2 = F_{q^2} / k = F_q$

Assumption

$x^6 + a\,x^5 + b\,x^4 + c\,x^3 + d\,x^2 + e\,x + f$ contains no non-trivial factor defined over k.

↓ then

GHS-section D is non-singular as affine curve.

Genus of GHS-section *D*

GHS-section D:

$$\begin{cases} y_1^2 = x^6 + a\,x^5 + b\,x^4 + c\,x^3 + d\,x^2 + e\,x + f \\ y_2^2 = x^6 + a^q\,x^5 + b^q\,x^4 + c^q\,x^3 + d^q\,x^2 + e^q\,x + f^q \end{cases}$$

↓ 12 ramification points (points with $y_1=0$)

$$H: y^2 = x^6 + a\,x^5 + b\,x^4 + c\,x^3 + d\,x^2 + e\,x + f$$

Hurwitz formula

$$2g(D)-2 = [K(D):K(H)]\cdot(2g(H)-2) + \Sigma\,(e(P'|P)-1)\cdot \deg P'$$

∴ genus of GHS-section D = 9; small ⟹ Problem 1

What we need to do is to construct C_{ab} model over k of GHS-section D. ⟹ Problem 2

Points at infinity of GHS-section D

$\Pi_{k2|k} H \supset D$: $x=x_1=x_2$; GHS-section

$$\begin{array}{ccc} D & P_1 \quad P_2 & P_3 \quad P_4 \\ {\scriptstyle 2}\downarrow & \diagdown\ \diagup & \diagdown\ \diagup \\ H & Q_1 & Q_2 \end{array}$$

: two points at infinity of H $\qquad v_{Q_i}(x)=-1,\ v_{Q_i}(y)=-3$

$t = x^2/y_1$: local parameter at Q_1 and Q_2

$$\begin{cases} x = t^{-1} + \alpha_0^{(i)} + \alpha_2^{(i)} t + \ldots . \\ y_1 = t^{-3} + \beta_{-2}^{(i)} t^{-2} + \beta_{-1}^{(i)} t^{-1} + \ldots . \end{cases} \quad \text{at } Q_i \ (i=1,2)$$

Substituting the above x for the second equation $y_2^2 = x^6 + a^q x^5 + b^q x^4 + c^q x^3 + d^q x^2 + e^q x + f^q$ of GHS-section D,

$$y_2 = -t^{-3} + \gamma_{-2}^{(2i-1)} t^{-2} + \ldots \quad \text{at } P_{2i-1} \ (i=1,2)$$

or $$y_2 = t^{-3} + \gamma_{-2}^{(2i)} t^{-2} + \ldots \quad \text{at } P_{2i} \ (i=1,2)$$

Points at infinity of GHS-section

$\Pi_{k2|k} H \supset D$: $x=x_1=x_2$ $\quad t = x^2/y$

$$P_1 \begin{cases} x = -t^{-1} + \alpha_0^{(1)} + \alpha_1^{(1)} t + \cdots \\ y_1 = t^{-3} + \beta_{-2}^{(1)} t^{-2} + \beta_{-1}^{(1)} t^{-1} + \cdots \\ y_2 = -t^{-3} + \gamma_{-2}^{(1)} t^{-2} + \gamma_{-1}^{(1)} t^{-1} + \cdots \end{cases}$$

$$P_2 \begin{cases} x = -t^{-1} + \alpha_0^{(1)} + \alpha_1^{(1)} t + \cdots \\ y_1 = t^{-3} + \beta_{-2}^{(1)} t^{-2} + \beta_{-1}^{(1)} t^{-1} + \cdots \\ y_2 = t^{-3} + \gamma_{-2}^{(2)} t^{-2} + \gamma_{-1}^{(2)} t^{-1} + \cdots \end{cases}$$

$$P_3 \begin{cases} x = t^{-1} + \alpha_0^{(2)} + \alpha_1^{(2)} t + \cdots \\ y_1 = t^{-3} + \beta_{-2}^{(2)} t^{-2} + \beta_{-1}^{(2)} t^{-1} + \cdots \\ y_2 = -t^{-3} + \gamma_{-2}^{(3)} t^{-2} + \gamma_{-1}^{(3)} t^{-1} + \cdots \end{cases}$$

$$P_4 \begin{cases} x = t^{-1} + \alpha_0^{(2)} + \alpha_1^{(2)} t + \cdots \\ y_1 = t^{-3} + \beta_{-2}^{(2)} t^{-2} + \beta_{-1}^{(2)} t^{-1} + \cdots \\ y_2 = t^{-3} + \gamma_{-2}^{(4)} t^{-2} + \gamma_{-1}^{(4)} t^{-1} + \cdots \end{cases}$$

$\longrightarrow$ 'value' of any polynomial $f(x, y_1, y_2)$ at P_i, $\sigma(P_4) = P_4$

C_{ab} model of GHS-section D

- We construct C_{ab} model of D with the point P_4 at infinity as a base point.

Suppose P_4 is not a Weierstrass point:

Pole numbers at $P_4 = < 10, 11, \ldots, 19 >$.

Construct
a polynomial f_i with a unique pole of order i at P_4
for $i = 10, 11, \ldots, 19$.

> Note: t-expansion of P_i gives the value at P_i

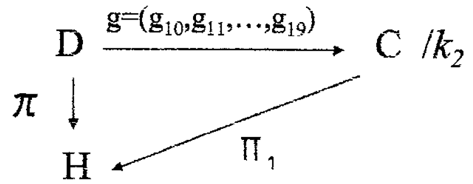
$$f_{10}, f_{11}, \ldots, f_{19} \longrightarrow \quad C_{10,11,\ldots,19} \text{ model over } k_2 \text{ of } D$$

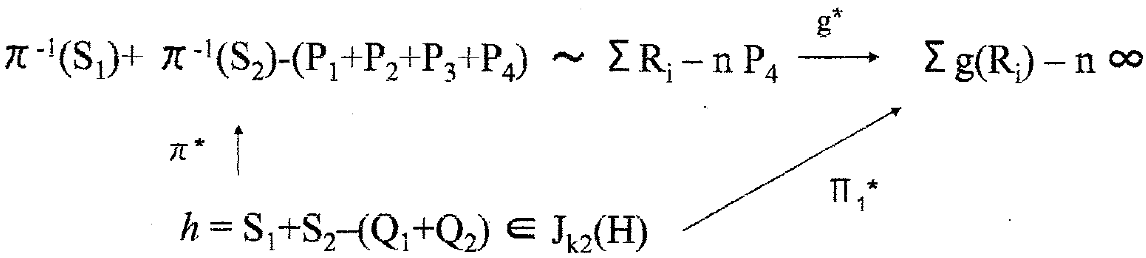
$$g_i := \mathrm{Tr}_{k2|k}(f_i) \qquad (\mathrm{Tr}_{k2|k}(f) = f + \sigma(f))$$

$$g_{10}, g_{11}, \ldots, g_{19} \longrightarrow \quad C_{10,11,\ldots,19} \text{ model } C \text{ over } k \text{ of } D$$

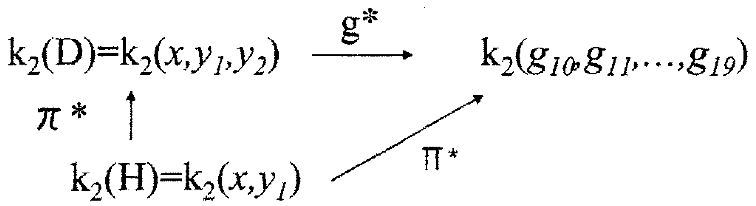
> Note: P_4 is fixed by σ.

Reduction : H → C





Reduction: H → C with ideals



$w := h \cdot g \subset k_2[x,y_1,y_2]$ ⟶ an ideal $v \subset k_2[g_{10},g_{11},\ldots,g_{19}]$ of relations among $g_{10}(x,y_1,y_2), g_{11}(x,y_1,y_2), \ldots, g_{19}(x,y_1,y_2) \bmod w$

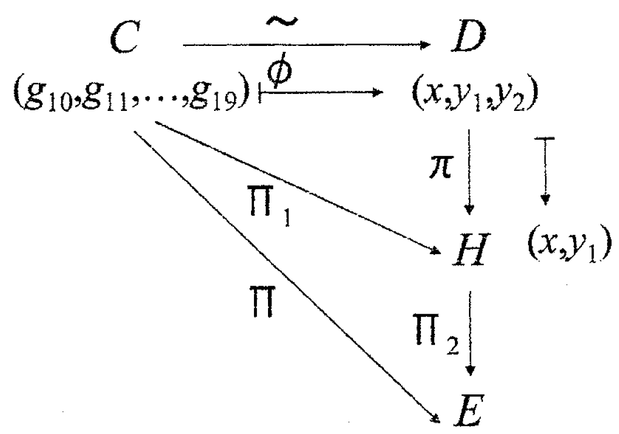
↑ ($v_{P_i}(g) \geqq 1$, $i = 1,2,3$)

an ideal $h \subset k_2[x,y_1]$

$v = g^*(w) = \Pi^*(h)$

Reduction: E → C

C: C_{ab} model over k of GHS-section D



$$\Psi : E(k_4) \xrightarrow{\Pi^*} \mathrm{Jac}_C(k_4) \xrightarrow{N_{k_4/k}} \mathrm{Jac}_C(k)$$

Ψ reduces DLP on E/k_4 to DLP on C/k.

Example1 : Transformation to palindrome form

k: prime field of char. $q=p=71$
k_2: quadratic ext. by o^2-2o+7 of k
k_4: quartic ext. by r^2-or+1

$\#E(k_4)=n=25404727$:prime
$j(E_w)=o^{1854}\,r+o^{2692} \notin k_2$

$$E_w/k_4:\ v_1^2+70\,u_1^3+(o^{2058}\,r+o^{4231})\,u_1+o^{3375}\,r+o^{2069}=0$$

$$\wr\uparrow\ \Pi_2^{(1)}:\begin{cases} u=a^{-1}(u_1+\beta_2) \\ v=a^{-1}v_1 \end{cases}$$

$a=o^{2258}\,r+o^{214}$
$b=o^{3519}\,r+o^{2654}$
$\beta_2=o^{4167}\,r+o^{3302}$

$$\begin{aligned} E_n/k_4:\ v^2 &= a\,u^3+b\,u^2+b^{q2}\,u+a^{q2} \\ &= (o^{2258}r+o^{214})\,u^3+(o^{3519}\,r+o^{2654})\,u^2+ \\ &\quad (o^{999}r+o^{3103})\,u+\ o^{4778}r+o^{355} \end{aligned}$$

Example1 : Covering by hyperelliptic curve

$$\begin{aligned} E_n/k_4:\ v^2 &= a\,u^3+b\,u^2+b^{q2}\,u+a^{q2} \\ &= (o^{2258}r+o^{214})\,u^3+(o^{3519}\,r+o^{2654})\,u^2+(o^{999}r+o^{3103})\,u+o^{4778}r+o^{355} \end{aligned}$$

$$\uparrow\ \Pi_2^{(2)}:\begin{cases} u=(x_0-c)/(x_0-c^{q2})^2 \\ v=y_0/(x_0-c^{q2})^3 \end{cases}$$

$$\begin{aligned} H_0/k_2:\ y_0^2 &= a(x_0-c)^6+b(x_0-c)^4(x_0-c^{q2})^2+b^{q2}\,(x_0-c)^2\,(x_0-c^{q2})^4+a^{q2}\,(x_0-c^{q2})^6 \\ &= o^{1463}x_0^6+o^{666}x_0^5+o^{2070}x_0^4+o^{1093}x_0^3+o^{794}x_0^2+o^{315}x_0+o^{1939} \end{aligned}$$

$$\wr\uparrow\ \Pi_2^{(3)}:\begin{cases} y_1=F(\beta)^{-(1/2)}(x_0-\beta)^{-3}y_0 \\ x=1/(x_0-\beta) \end{cases}$$

$c=r$
H_0: $y_0^2=F(x)$
$\beta=3$

$$H/k_2:\ y_1^2=x^6+o^{2177}x^5+o^{4311}x^4+o^{2447}x^3+o^{566}x^2+o^{3664}x+o^{3747}$$

$$\Pi_2:=\Pi_2^{(1)}\,\Pi_2^{(2)}\,\Pi_2^{(3)}:H\longrightarrow E_w$$

Example1 : Points at infinity of GHS-section *D*

$\Pi_{k2|k} H \supset D$: $x = x_1 = x_2 \quad t = x^2/y$

$$P_1 \begin{cases} x = 70\, t^{-1} + o^{4265} + o^{261}\, t + o^{4535}\, t^2 + o^{2836}\, t^3 + \cdots \\ y_1 = t^{-3} + o^{2177}\, t^{-2} + o^{4111}\, t^{-1} + o^{3867} + o^{3086}\, t + \cdots \\ y_2 = 70\, t^{-3} + o^{2713}\, t^{-2} + o^{4163}\, t^{-1} + o^{3058} + o^{4299}\, t + \cdots \end{cases}$$

$$P_2 \begin{cases} x = 70\, t^{-1} + o^{4265} + o^{261}\, t + o^{4535}\, t^2 + o^{2836}\, t^3 + \cdots \\ y_1 = t^{-3} + o^{2177}\, t^{-2} + o^{4111}\, t^{-1} + o^{3867} + o^{3086}\, t + \cdots \\ y_2 = t^{-3} + o^{193}\, t^{-2} + o^{1643}\, t^{-1} + o^{538} + o^{1779}\, t + \cdots \end{cases}$$

$$P_3 \begin{cases} x = t^{-1} + o^{4265} + o^{2781}\, t + o^{4535}\, t^2 + o^{316}\, t^3 + \cdots \\ y_1 = t^{-3} + o^{4697}\, t^{-2} + o^{4111}\, t^{-1} + o^{1347} + o^{3086}\, t + \cdots \\ y_2 = 70\, t^{-3} + o^{193}\, t^{-2} + o^{4163}\, t^{-1} + o^{538} + o^{4299}\, t + \cdots \end{cases}$$

$$P_4 \begin{cases} x = t^{-1} + o^{4265} + o^{2781}\, t + o^{4535}\, t^2 + o^{316}\, t^3 + \cdots \\ y_1 = t^{-3} + o^{4697}\, t^{-2} + o^{4111}\, t^{-1} + o^{1347} + o^{3086}\, t + \cdots \\ y_2 = t^{-3} + o^{2713}\, t^{-2} + o^{1643}\, t^{-1} + o^{3058} + o^{1779}\, t + \cdots \end{cases}$$

$\longrightarrow$ 'value' of any polynomial $f(x, y_1, y_2)$ at P_i

---

Example1 : C_{ab} model of GHS-section *D*

a polynomial with a unique pole of order i at P_4 : $g_i = \mathrm{Tr}_{k2|k}(f_i)$

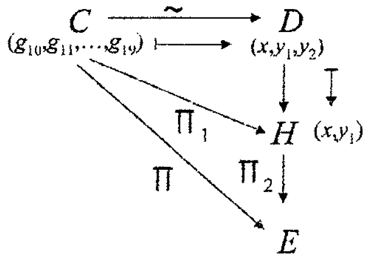
$$\begin{cases} g_{10} = o^{1264}\, x^3 y_1^2 + 3\, x^3 y_1 y_2 + o^{271}\, x^3 y_1 + \cdots + o^{1754}\, y_2 \\ g_{11} = o^{1386}\, x^3 y_1^2 + x^3 y_1 y_2 + o^{2108}\, x^3 y_1 + \cdots + o^{630}\, y_2 \\ \cdots \\ g_{19} = o^{3534}\, x^3 y_1^2 + 41\, x^3 y_1 y_2 + o^{3210}\, x_3 y_1 + \cdots + o^{1622}\, y_2 \end{cases}$$

Relations among $g_{10}, g_{11}, \cdots, g_{19}$:

$$\begin{cases} g_{11}^2 - (5g_{10}g_{12} + 42g_{10}g_{11} + 18g_{10}^2 + \cdots + 25) = 0 \\ g_{11}g_{12} - (26g_{10}g_{13} + 38g_{10}g_{12} + \cdots + 58) = 0 \\ \cdots \\ g_{12}g_{19} - (9g_{10}^2 g_{11} + 62g_{10}^3 + 10g_{10}g_{19} + \cdots + 28) = 0 \end{cases}$$

$\uparrow$ $C_{10,11,\ldots,19}$ curve over k in g_{10}-g_{11}-…-g_{19} space

Example1 : Reduction(1)



$E_w \ni G=(o^{387}\, r + o^{397},\ o^{166}\, r + o^{1205})$

From the definition of $Π_2$

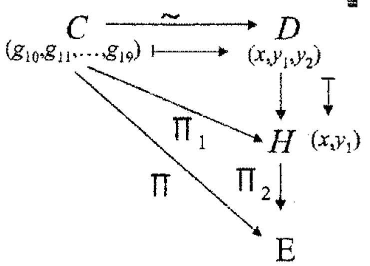
$$J_1 = Π_2^*(G)$$
$$= \{a\,((\beta - c)\, x+1)^2 - (G_x + \beta_2)\,((\beta - c^{q2})\, x+1)^2,\ a\,\alpha^{1/2} y_1 - G_y\,((\beta - c^{q2})\, x+1)^3 \}$$

$$= \{(o^{353}r+o^{4196})x^2+(o^{1900}r+o^{1805})x+o^{1922}r+o^{2318},\ (o^{3720}r+o^{1533})x^3+ (o^{1693}r+o^{4323})x^2+(o^{3636}r+o^{1592})y_1+ (o^{1256}r+o^{3701})x+o^{2686}r+o^{3725}\}$$

To compute $Π_1^*(J)$, we use elimination ideal:

$$J_2 \leftarrow \mathrm{Eliminate}(J_1+(g_{10}-g_{10}(x,y_1,y_2), g_{11}-g_{11}(x,y_1,y_2), \dots, g_{19}-g_{19}(x,y_1,y_2),\ \{x,y_1,y_2\})$$

Example1 : Reduction(2)



Finally we compute the norm:

$$J = \Psi(G) = J_2 + J_2^{q} + J_2^{q2} + J_2^{q3}$$
$$= \{ g_{17}^2+37g_{17}+21g_{16}+49g_{15}+33g_{14}+\cdots+59,$$
$$g_{16}g_{17}+45g_{17}+15g_{16}+45g_{15}+21g_{14}+\cdots+ 63,$$
$$\cdots$$
$$g_{18}+24g_{17}+27g_{16}+31g_{15}+64g_{14}+\cdots+64 \}$$

Similarly, m=25415194-times point $G_m=(o^{637}r+o^{224},\ o^{1671}r+o^{3481})$ of G is transferred to

$$J_m= \{ g_{17}^2+6g_{17}+70g_{16}+66g_{15}+15g_{14}+\cdots+68,$$
$$g_{16}g_{17}+5g_{17}+20g_{16}+56g_{15}+16g_{14}+\cdots+11,$$
$$\cdots$$
$$g_{18}+23g_{17}+34g_{16}+65g_{15}+18g_{14}+\cdots+4 \}$$

We verified $J_m = m \cdot J$ on C.

⇦ Gaudry method

Example2 (160 bits length)

k: prime field of char. $p = 2^{40}-2^{35}-1$
k_2: quadratic ext. of k by $o^2 + 352619714346$
k_4: quartic ext. of k by $r^2 + 702753204573\, o + 465976829831$

E_w: elliptic curve over k_4

$$v_1^2 = u_1^3+((773569929047o+698785454132)r+892468792697o+773390597884)u_1+ (245022657483o+657619174138)r+721187940068o+865450731541$$

($\#E(k_4)$=1287200406650928609777376029597716043015507861907: 160 bits prime)

⇩

C: $C_{10,11,\ldots,19}$ curve over k

$$\begin{cases} g_{11}^2 - (671010913434\, g_{10} g_{12} + 306446345201\, g_{10} g_{11} + 205461673669\, g_{10}^2 + \cdots + 675147796101) = 0 \\ g_{11} g_{12} - (752537421825\, g_{10} g_{13} + 1016531429604\, g_{10} g_{12} + 897328181722\, g_{10} g_{11} + \cdots + 1053682994222) = 0 \\ \cdots \\ g_{12} g_{19} - (128634052382\, g_{10}^2 g_{11} + 950367786029\, g_{10}^3 + 457707828730\, g_{10} g_{19} + \cdots + 665817232135) = 0. \end{cases}$$

⇦ Gaudry method

Estimate of computational amounts

- Computational amounts of Gaudry method against C_{ab} curve of genus g over GF(q) is

$$O(q^{2g/(g+1)+\varepsilon}) \quad (q \to \infty)$$

- So, computational amounts of our Weil descent attack(g=9):

$$q^{18/10} = q^{9/5} \;(< q^2) \quad (q \to \infty)$$

↑

Computational amounts of Pollard's rho method against elliptic curves on GF(q^4):

More precise estimate

•Computational amounts of Gaudry method against C_{ab} curves of genus g defined on GF(q): ($l \geqq 1$: parameter)

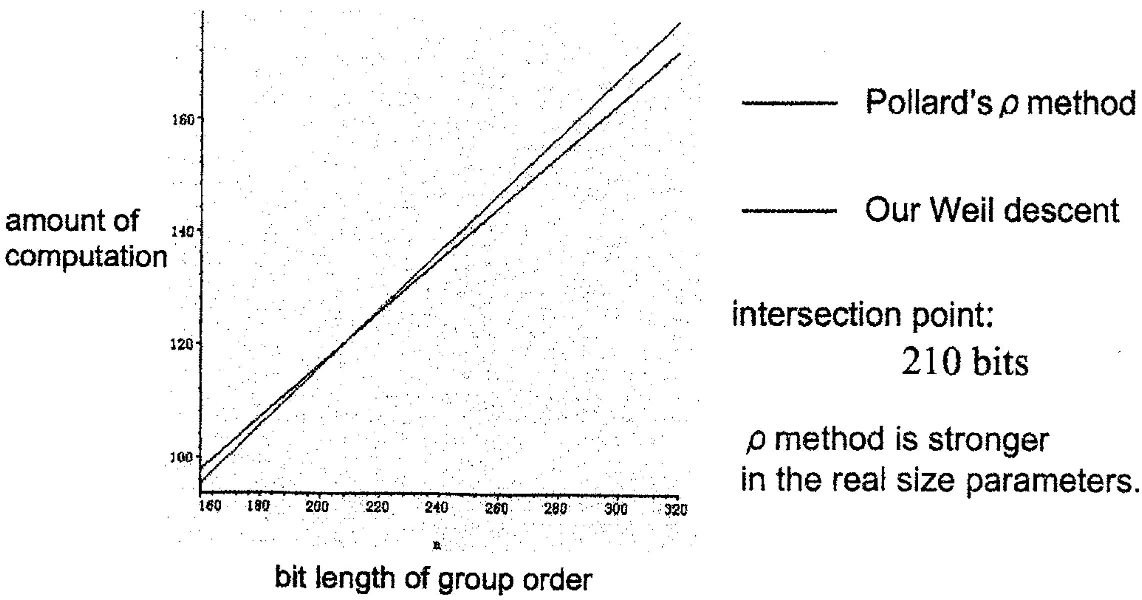
Minimum w.r.t. l of

$$l^{g-1} \cdot g^3 \cdot g! \cdot q \cdot (\log_2(q))^3 + l^{-2} \cdot g^3 \cdot q^2 \cdot (\log_2(q))^2$$

•Computational amounts of Pollard's rho method against elliptic curves on GF(q^4):

$$1.5 \cdot q^2 \cdot (\log_2(q^4))^2$$

Pollard v.s. Our Weil descent



intersection point:
210 bits

ρ method is stronger in the real size parameters.