拡大体上の楕円曲線暗号に対する index calculusについて

情報セキュリティ大学院大学　山外一徳　小崎俊二　松尾和人

2008年 3月8日

対象とする離散対数問題

本研究では、拡大体上の楕円曲線暗号に対する攻撃法 generalized Weil descent **について述べる**

p : **奇素数** , $E/\mathbb{F}_{p^3}$: $Y^2 = f(X)$,

where $f(X) = X^3 + AX + B$, $A \in \mathbb{F}_p$, $B \in \mathbb{F}_{p^3}$

$E(\mathbb{F}_{p^3})$ **の離散対数問題を対象とする**

拡大次数3 : Generalized Weil descent **が効果がある最小の拡大次数**

$E(\mathbb{F}_{p^4})$ **についても少し述べる**

本発表で扱うアルゴリズム

◊ Index calculus

- Plain version
- Double-large-prime version

◊ Relation collection **アルゴリズム**

- Gaudry**のアルゴリズム**
- Nagao**のアルゴリズム**

$E(\mathbb{F}_{p^n})$に対するindex calculus

◊ Index calculus(1991:Adleman-DeMarrais-Huang, 1997:Gaudry)

超楕円曲線上の離散対数問題に対する解法アルゴリズム

◊ Weil descent(1998:Frey)

$E(\mathbb{F}_{p^n})$**の離散対数問題を**$\mathbb{F}_p$**上の超楕円曲線上の離散対数問題に置き換え、**index calculus**を用いる解法アルゴリズム**

⇒

◊ Generalized Weil descent(2004:Gaudry, 2007:Nagao)

$E(\mathbb{F}_{p^n})$**の離散対数問題に対し、直接**index calculus**を用いる解法アルゴリズム**

Generalized Weil descent

Step1 : Relation collection part

Relation を集めるために Gröbner 基底計算を行う

Step2 : Linear algebra part

集めた relation から離散対数問題を解く

Relation collection part

因子基底 $B_0 := \{P_i = (x_i, y_i) \in E(\overline{\mathbb{F}}_{p^3}) \mid x_i \in \mathbb{F}_p\}$, $\#B_0 = O(p)$

For $Q \in E(\mathbb{F}_{p^3})$

$$\text{Relation}: \ Q + P_1 + P_2 + P_3 = 0 \ , \ P_i \in B_0$$

Step1 : **代数方程式の生成**

Step2 : Gröbner**基底計算**

Gröbner**基底計算の計算量評価が困難** $\rightarrow$ **実装実験**

Relation collection アルゴリズム

◊ Gaudryのアルゴリズム

◦ Semaevのsummation polynomials を用いて代数方程式を得る

→ Gröbner基底計算で代数方程式を解く

◊ Nagaoのアルゴリズム

◦ Gaudryと異なる方法で代数方程式を得る

→ Gröbner基底計算で代数方程式を解く

Gaudryのアルゴリズム 1

◦ Semaevのsummation polynomials

For $P_i = (x_i, y_i) \in E(\overline{\mathbb{F}}_{p^3})$

$$f_m(x_1, x_2, x_3, \ldots, x_m) = 0 \ , \ x_1, x_2, x_3, \ldots, x_m \in \overline{\mathbb{F}}_{p^3}$$

$$\Leftrightarrow \quad P_1 + P_2 + P_3 + \cdots + P_m = 0 \in E(\overline{\mathbb{F}}_{p^3})$$

Gaudryのアルゴリズム 2

For $Q = (x, y) \in E(\mathbb{F}_{p^3})$

$$\text{Relation}: \ Q + P_1 + P_2 + P_3 = 0 \ , \ P_i \in B_0$$

Relation**が得られる確率**$\approx \frac{1}{6}$

For $P_i = (X_i, Y_i) \in E(\overline{\mathbb{F}}_{p^3})$, **変数**： X_i, Y_i

Step1： $f_3(X_1, X_2, \tilde{X})$, $\overline{f}_3(X_3, x, \tilde{X})$ **を得る**

Step2： $f_4(X_1, X_2, X_3, x) =$Resultant$(f_3, \overline{f}_3, \tilde{X})$ **を得る**

Step3： **代数方程式を得る**

$\rightarrow$ **代数方程式を解き、**X_1, X_2, X_3 **を得る**

Gaudryのアルゴリズム 3

For $Q \in E(\mathbb{F}_{p^3})$, $P_1, P_2, P_3 \in E(\overline{\mathbb{F}}_{p^3})$, $f(X) = X^3 + AX + B$

Step1:

Summation polynomial

$$\begin{aligned} f_3(X_1, X_2, \tilde{X}) &= (X_1 - X_2)^2 \tilde{X}^2 - 2((X_1 + X_2)(X_1 X_2 + A) + 2B) \\ &\quad + ((X_1 X_2 - A)^2 - 4B(X_1 + X_2)) \\ \overline{f}_3(X_3, x, \tilde{X}) &= (X_3 - x)^2 \tilde{X}^2 - 2((X_3 + x)(X_3 x + A) + 2B) \\ &\quad + ((X_3 x - A)^2 - 4B(X_3 + x)) \end{aligned}$$

Gaudryのアルゴリズム 4

Step2:

$f_4(X_1, X_2, X_3, x) = \mathrm{Resultant}(f_3, \overline{f}_3, \tilde{X})$ を計算

Step3:

$\mathbb{F}_{p^3}/\mathbb{F}_p$ の基底を $1, t, t^2$ とする

$$f_4 = \phi_0(X_1, X_2, X_3) + \phi_1(X_1, X_2, X_3)t + \phi_2(X_1, X_2, X_3)t^2$$

where $\phi_i(X_1, X_2, X_3) \in \mathbb{F}_p[X_1, X_2, X_3]$

$f_4(X_1, X_2, X_3, x) = 0 \Leftrightarrow Q + P_1 + P_2 + P_3 = 0$

$\Rightarrow \phi_0 = 0, \phi_1 = 0, \phi_2 = 0$

$\Rightarrow \phi_0 = 0, \phi_1 = 0, \phi_2 = 0$ を解き、X_1, X_2, X_3 を得る

Gaudryのアルゴリズム まとめ

Relationを求める

Step1： 代数方程式$\phi_0 = 0, \phi_1 = 0, \phi_2 = 0$ を得る

Step2： 代数方程式をGröbner基底計算で解く

Step3： $X_1, X_2, X_3 \in \mathbb{F}_p$が得られる
$\Rightarrow P_i = (X_i, Y_i) \in B_0$

基本対称式を用いる

Gaudryのアルゴリズムで得た代数方程式： 次数, 項数が大

→ 基本対称式で整理： 次数, 項数を削減

Step1： $\phi_0 = 0, \phi_1 = 0, \phi_2 = 0$ を基本対称式で整理

$$\begin{aligned} T_1 &= X_1 + X_2 + X_3 \\ T_2 &= X_1X_2 + X_2X_3 + X_1X_3 \\ T_3 &= X_1X_2X_3 \end{aligned}$$

Step2： $\phi_0(T_1, T_2, T_3) = 0, \phi_1(T_1, T_2, T_3) = 0, \phi_2(T_1, T_2, T_3) = 0$
を Gröbner 基底計算で解く

Step3： $X^3 + T_1X^2 + T_2X + T_3$ ，変数： X
→ X_1, X_2, X_3 を得る

Nagaoのアルゴリズム 1

For $Q = (x, y) \in E(\mathbb{F}_{p^3})$

$$\text{Relation}: Q + P_1 + P_2 + P_3 = 0, P_i \in B_0$$

Q, P_1, P_2, P_3 **で** E **と交わる多項式** $h(X, Y) = 0$

$$h(X, Y) = (X - x)(X + u) + (Y - y)v \text{ , 変数}: u, v$$

と書ける

Nagaoのアルゴリズム 2

$h(X,Y)=0$ と $Y^2=f(X)$ から Y を消去

$$
\begin{aligned}
S(X) &:= -v^2 f(X) + ((X-x)(u+X)-yv)^2 \\
&= X^4 + (-v^2+2u-2x)X^3 \\
&\quad +(-2yv+u^2-4xu+x^2)X^2 \\
&\quad +(-Av^2-2yuv+2xyv-2xu^2+2x^2u)X \\
&\quad -Bv^2+y^2v^2+2xyuv+x^2u^2 \\
&= 0
\end{aligned}
$$

Nagaoのアルゴリズム 3

$(X - x) \mid S(X)$ から $g(X) := \frac{S(X)}{X-x}$

$$g(X) := X^3 + C_2X^2 + C_1X + C_0 = 0, \text{ where } C_i \in \mathbb{F}_{p^3}[u, v]$$

◦ $g(X) = 0$ の根は P_1, P_2, P_3 の X 座標

$\mathbb{F}_{p^3}/\mathbb{F}_p$ の基底を $1, t, t^2$ とする

$$u = u_0 + u_1t + u_2t^2$$

$$v = v_0 + v_1t + v_2t^2$$

変数： u_i, v_i

Nagaoのアルゴリズム 4

$g(X) := X^3 + C_2X^2 + C_1X + C_0$

$C_{i,j} \in \mathbb{F}_p[u_0, \ldots, v_2]$ **とする**, i.e.

$$\begin{aligned} C_0 &= C_{0,0} + C_{0,1}t + C_{0,2}t^2 \\ C_1 &= C_{1,0} + C_{1,1}t + C_{1,2}t^2 \\ C_2 &= C_{2,0} + C_{2,1}t + C_{2,2}t^2 \end{aligned}$$

$P_1, P_2, P_3 \in B_0 \Rightarrow g(X) \in \mathbb{F}_p[X]$

$$g(X) = X^3 + C_{2,0}X^2 + C_{1,0}X + C_{0,0}$$

すなわち $C_{0,1} = 0, \ldots, C_{2,2} = 0$

Nagaoのアルゴリズム まとめ

Relation を求める

Step1： 代数方程式 $C_{0,1} = 0, C_{0,2} = 0, C_{1,1} = 0, C_{1,2} = 0,$
$C_{2,1} = 0, C_{2,2} = 0$ を得る

Step2： 代数方程式を Gröbner 基底計算で解く
$\Rightarrow u_0, \ldots, v_2 \in \mathbb{F}_p$
$\Rightarrow C_{0,0}, C_{1,0}, C_{2,0} \in \mathbb{F}_p$

Step3： $g(X) = X^3 + C_{2,0}X^2 + C_{1,0}X + C_{0,0}$

- $g(X) = (X - x_1)(X - x_2)(X - x_3) = 0$ s.t. $x_i \in \mathbb{F}_p$
  $\Rightarrow P_i = (x_i, y_i) \in B_0$

代数方程式の比較

代数方程式	Gaudry	Gaudry＋基本対称式	Nagao
変数の数	3	3	6
代数方程式の数	3	3	6
最高次数	12	4	2
項数	125,124,124	35,33,33	21,21,15,15,5,5

Gröbner基底計算の時間が異なることが考えられる

Relation collection アルゴリズム 実装実験

□ 目的

Relation collection **アルゴリズムの計算量評価**

□ 環境

OS:Linux version 2.6.13
CPU:AMD Athlon 64 X2 , 2.4GHz
メモリ：4GB**搭載**
代数計算システム：MAGMA V2.14-5

□ 内容

Gaudry**のアルゴリズム＋基本対称式**，Nagao**のアルゴリズム**

p^3**のサイズ**42-160bit**それぞれに対し、**relation**を**1000**個集める時間を測定**

実験結果

Relationを1個得るために要する計算時間

Gaudry＋基本対称式

$\log p^3$	代数方程式生成	Gröbner基底計算	合計
64 (bit)	0.751 (sec)	0.101 (sec)	0.856 (sec)
96 (bit)	1.339 (sec)	0.355 (sec)	1.714 (sec)
128 (bit)	1.299 (sec)	0.365 (sec)	1.690 (sec)
160 (bit)	1.279 (sec)	0.407 (sec)	1.703 (sec)

Nagao

$\log p^3$	代数方程式生成	Gröbner基底計算	合計
64 (bit)	0.011 (sec)	0.188 (sec)	0.201 (sec)
96 (bit)	0.015 (sec)	0.972 (sec)	0.994 (sec)
128 (bit)	0.014 (sec)	1.036 (sec)	1.058 (sec)
160 (bit)	0.013 (sec)	1.106 (sec)	1.128 (sec)

推定

Index calculus(plain version)
Relation collection part : p**個程度の** relation **を集める**

◊ Gaudry**のアルゴリズム＋基本対称式** , Nagao**のアルゴリズム**

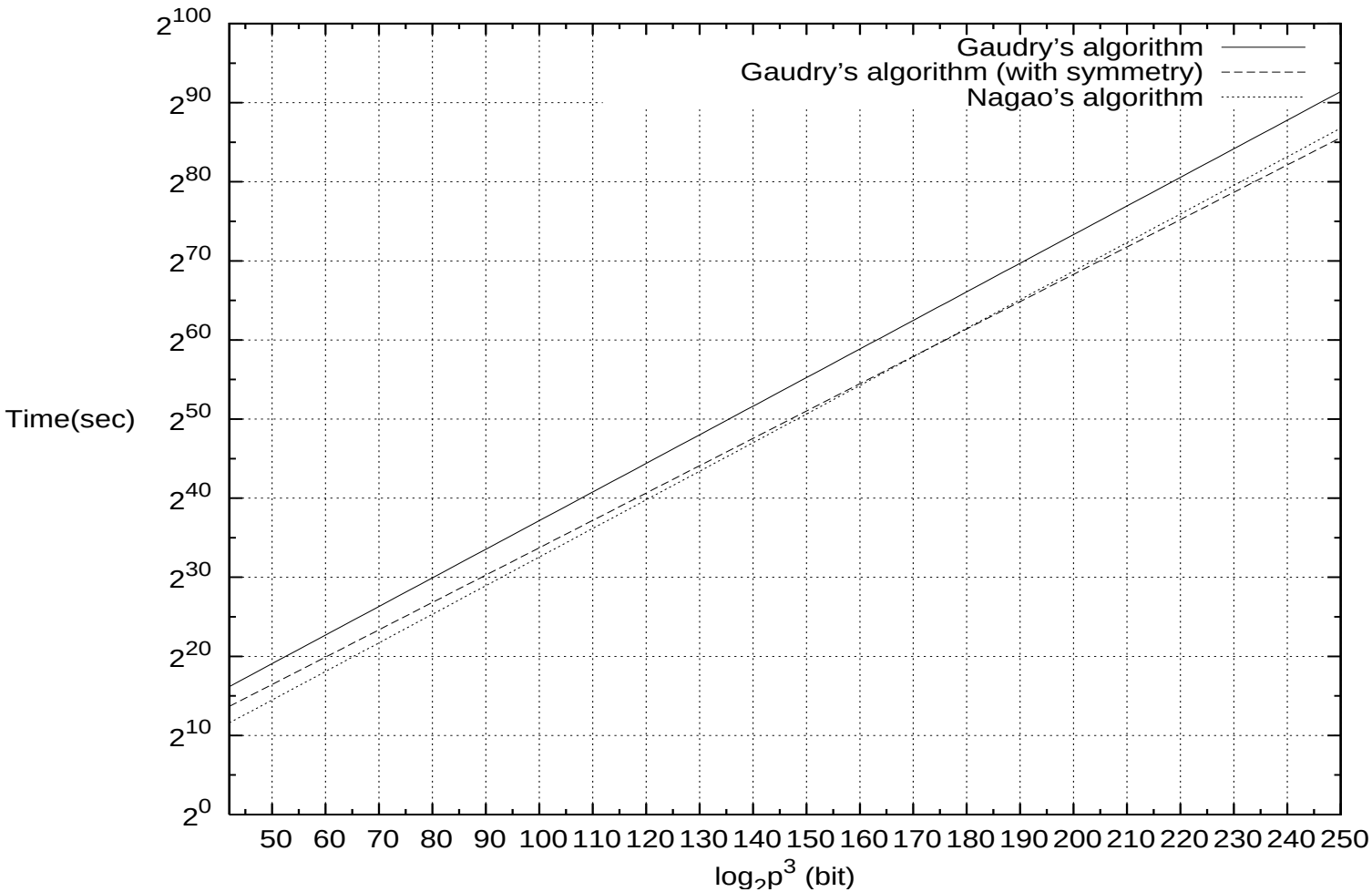
- **実験データから** relation **を** p**個集める計算時間を推定**

◊ Gaudry**のアルゴリズム**

- p^3**のサイズ** 20-50bit **それぞれに対し、** relation **を** 100 **個集める時間を測定**
- **実験データから** relation **を** p**個集める計算時間を推定**

最小二乗法を用いて推定

Relation collection アルゴリズム 推定計算時間



Index calculus

◊ Gaudry**法** (Gaudry) : Plain version　　**計算量**$O(p^2)$

Plain version**の改良アルゴリズム**

→ ◊ Gaudry-Harley**法** (Gaudry-Harley)　　**計算量**$O(p^{\frac{3}{2}})$

→ ◊ Single-large-prime version (Thériault)

→ ◊ Double-large-prime version
(Nagao,Gaudry-Thomé-Thériault-Diem)
計算量$O(p^{\frac{4}{3}}) <$ Rho**法** $O(p^{\frac{3}{2}})$

Index calculus (plain version)

因子基底 B_0 s.t. $\#B_0 \approx p$

□ Relation collection part $\rightarrow$ **計算量**$O(p)$

□ Linear algebra part $\rightarrow$ **計算量**$O(p^2)$

$\Rightarrow$ **因子基底のサイズ程度の素行列演算**

全体の計算量$O(p^2)$: Rho**法より漸近計算量 大**

Index calculus (plain version) 実装実験

□ 目的

Index calculusの計算量評価

□ 内容

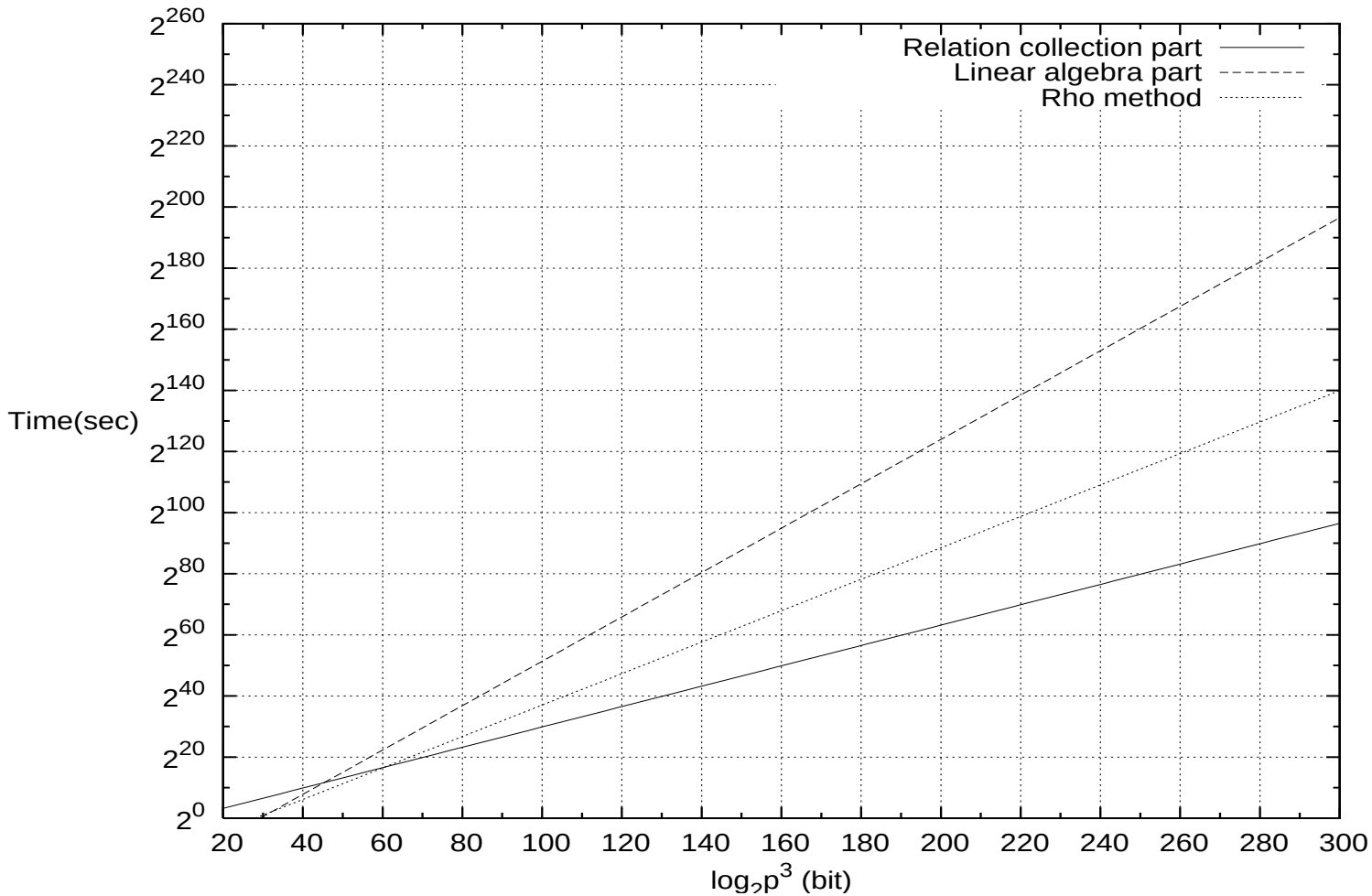
p^3のサイズ20-53bitに対し離散対数問題を解く
(Relation collection by Nagaoのアルゴリズム)

□ 計算時間を推定

測定結果から53bit以降の計算時間を推定

最小二乗法を用いて推定

Index calculus (plain version) 推定計算時間



Index calculus (double-large-prime version)

◊ **因子基底** : $B \subsetneq B_0$ s.t. $\#B \approx p^{\frac{2}{3}}$

□ Relation collection part $\rightarrow$ **計算量**$O(p^{\frac{4}{3}})$

□ Linear algebra part $\rightarrow$ **計算量**$O(p^{\frac{4}{3}})$

全体の計算量$O(p^{\frac{4}{3}}) <$ Rho**法 計算量**$O(p^{\frac{3}{2}})$

Double-large-prime version 実装実験

□ 目的

Double-large-prime versionの現実的な計算量評価

□ 内容

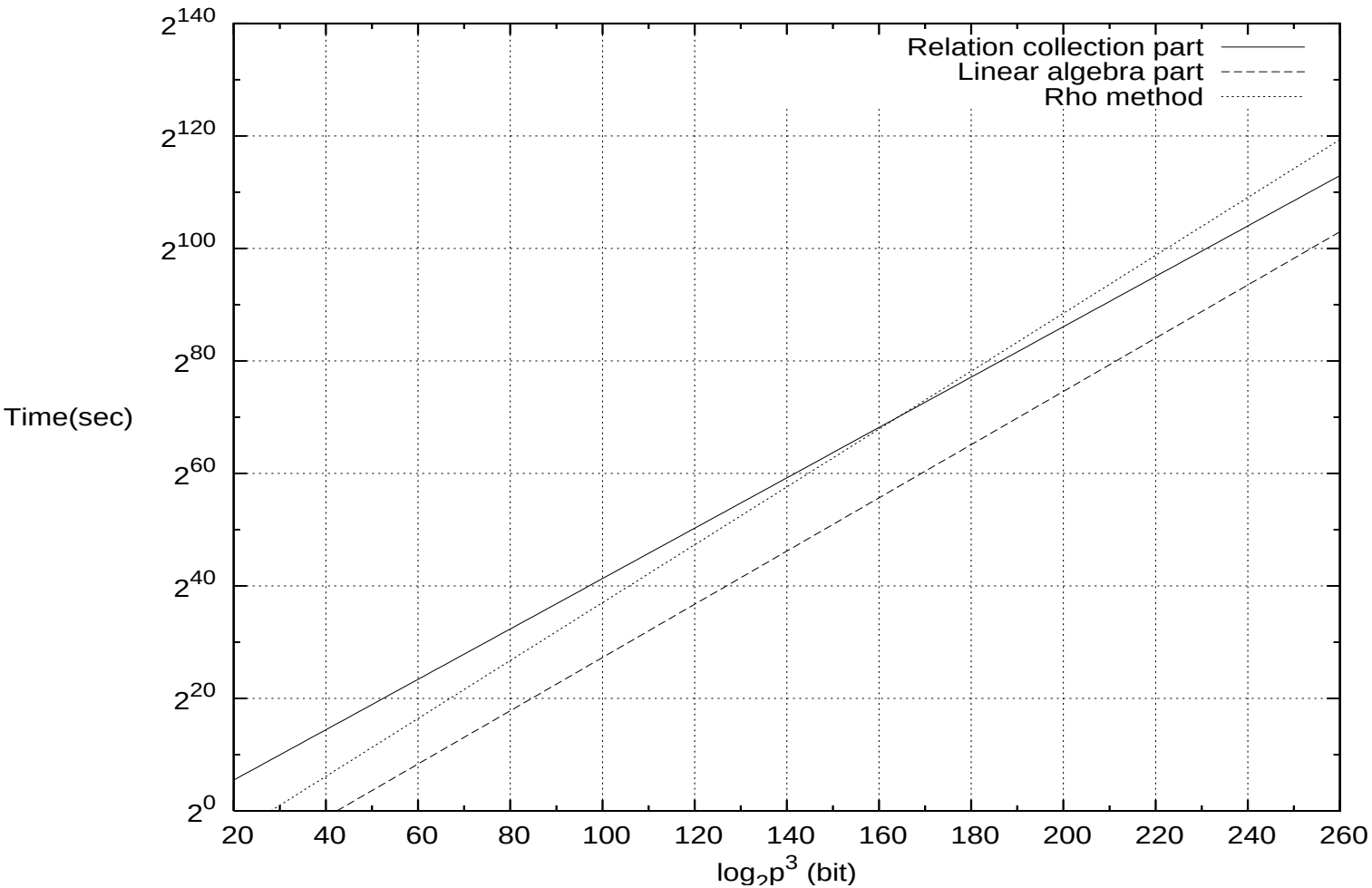
p^3のサイズ20-35bitに対する離散対数問題を解く
(Relation collection by Nagaoのアルゴリズム)

□ 計算時間を推定

測定結果からdouble-large-prime versionの計算時間を推定

最小二乗法を用いて推定

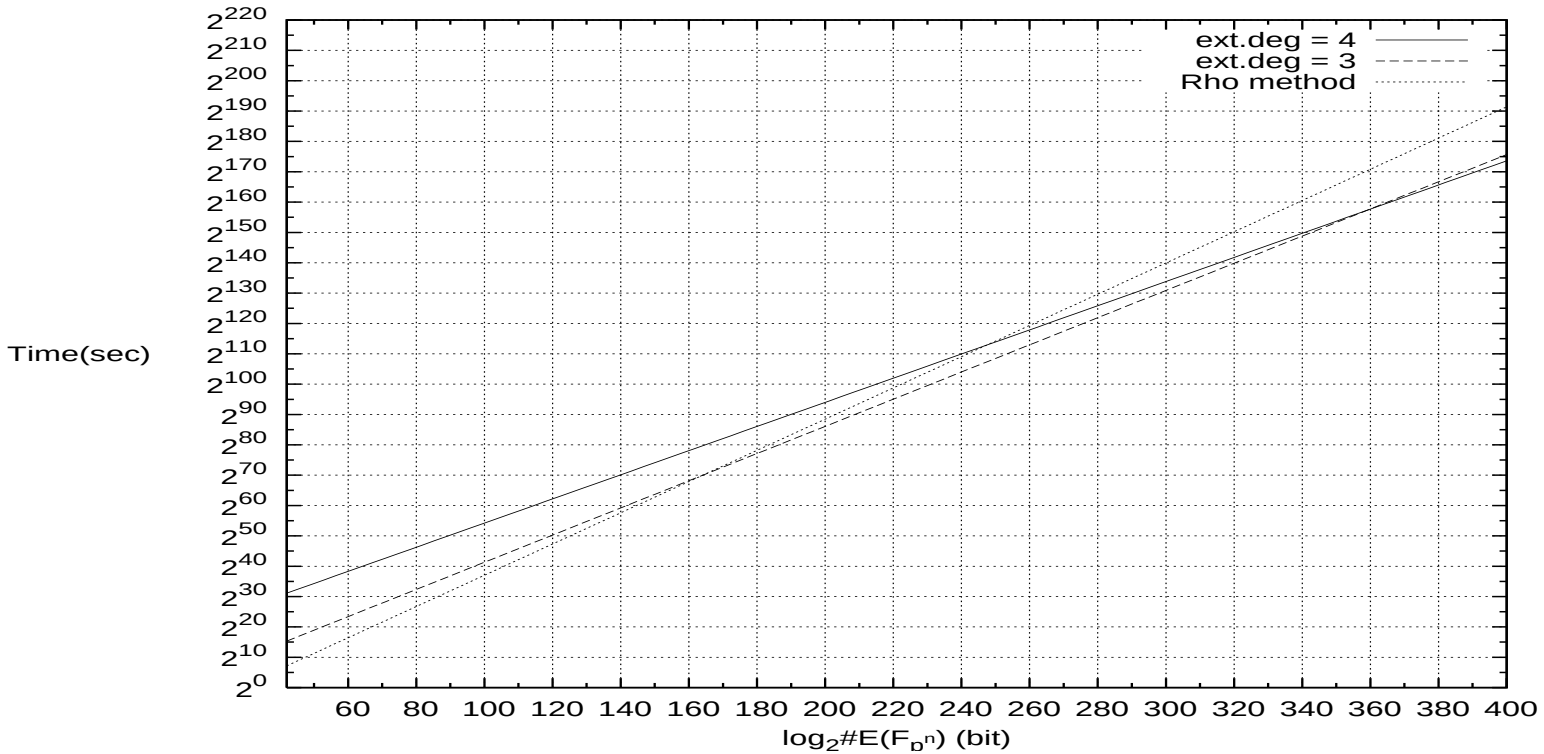
Double-large-prime-version 推定計算時間



拡大次数4に対するRelation collection アルゴリズム

Relationを1個得るために要する計算時間

64(bit)： 59808 (sec)　　96(bit)： 194352 (sec)



$p^3 : p^{\frac{4}{3}}$, $p^4 : p^{\frac{3}{2}}$ 個のrelationを集めるのに必要な時間

まとめ

次の実装を行った

◊ Relation collection **アルゴリズム**

- Gaudry**のアルゴリズム**
- Nagao**のアルゴリズム**

◊ Index calculus

- Plain version
- Double-large-prime version

◊ Generalized Weil descent

3次拡大に対し攻撃法として効果を持ち得る