種数２の超楕円曲線の位数計算の高速実装

石黒 司
松尾 和人

2010 年度 日本応用数理学会
研究部会連合発表会
JANT セッション
2010 年 3 月 9 日

研究背景

- **安全な代数曲線暗号の構成**
  - **曲線の位数によって安全性が変わる**
    → 曲線の位数計算が必要

- **安全な種数 2 の超楕円曲線の構成**
  - Gaudry-Schost **の** ℓ **進アルゴリズム** (2004)
    - **種数 2 の超楕円曲線一般に適用可能**
    - **素体** $\mathbb{F}_p$ **によって計算量が異なる**

    → 素体上の 160 ビット位数の曲線
    - **特殊な** p **を選ぶことにより高速化**

  - **改良** Gaudry-Schost **の** ℓ **進アルゴリズム** (2008)
    - **全ての曲線に適用できるわけではない**

    → 素体上の 254 ビット位数の特殊な曲線

→ Gaudry-Schost **アルゴリズムを高速化したい**

研究概要

- 位数計算中の ℓ 等分多項式の解析
  $\longrightarrow$ 既約因子の次数が多項式の次数に比べて低いことを示した
- ℓ 等分多項式の因子分解の改良
  $\longrightarrow$ 上記の性質を利用した因子分解アルゴリズム
  $\longrightarrow$ 実装・評価
  [石黒-松尾，SCIS2010]

■ 高速な既約因子分解を利用した位数計算の高速実装

ℓ進アルゴリズム

$\mathcal{J}$: 種数 2 の $\mathbb{F}_p$ 上の超楕円曲線のヤコビアン
$\chi \in \mathbb{Z}[X]$:フロベニウス写像の特性多項式

$$\chi = X^4 - s_1 X^3 + s_2 X^2 - s_1 p X + p^2, s_1, s_2 \in \mathbb{Z}$$

位数 $\#\mathcal{J} = \chi(1)$

ℓ：小さい素数、$\tilde{p},\ \tilde{s}_1,\ \tilde{s}_2 \in \mathbb{F}_\ell$、

$$\tilde{\chi} = X^4 - \tilde{s}_1 X^3 + \tilde{s}_2 X^2 - \tilde{s}_1 \tilde{p} X + \tilde{p}^2 \in \mathbb{F}_\ell[X]$$

$O(\log p)$ 個の $\tilde{\chi} \quad \to \chi \quad \to \chi(1)$ を求める

$\to$ $\boxed{\tilde{s}_1,\ \tilde{s}_2 \text{ を求めたい}}$

ℓ進アルゴリズム

$D \in \mathcal{J}[\ell] = \{\mathcal{D} \in \mathcal{J} | [\ell]\mathcal{D} = 0\}$

$$\phi(D)^4 - \tilde{s}_1\phi(D)^3 + \tilde{s}_2\phi(D)^2 - \tilde{s}_1\tilde{p}\phi(D) + \tilde{p}^2 = 0$$

を満たす $(\tilde{s}_1, \tilde{s}_2)$ **を見つける**

$D \in \mathcal{J}[\ell]$ **の発見**

1. Cantor **の** Division Polynomial(4 **変数、**$O(\ell^2)$ **次多項式** $\times 4$)
2. 1 **変数** $\frac{\ell^4-1}{2}$ **次多項式** (ℓ **等分多項式**)[GS,2004]
   (**楕円曲線の場合、**$\frac{\ell^2-1}{2}$ **次**)
3. $\underbrace{\ell\text{等分多項式の根}}_{\text{計算量大}}$ **から** D **を計算**

ℓ 等分多項式の既約因子分解

ℓ 等分多項式の既約因子分解の計算量が支配的
等分多項式の既約因子分解実験 [GS,2004]
$\ell = 19$
最短時間：約 30 **分**
最大時間：約 100 **時間**
平均時間：約 10 **時間**
$\longrightarrow$ **既約因子分解の最大計算量を削減したい**

ℓ 等分多項式の次数： $\frac{\ell^4-1}{2}$
既約因子の最大次数: $\frac{\ell^3-\ell}{2}$
$\longrightarrow$ **既約因子分解の高速化可能**

既約因子分解の高速化

$\frac{\ell^4-1}{2}$ 次の ℓ 等分多項式の因子の次数: $O(\ell^3)$

一般的な既約因子分解アルゴリズム：

$$x, x^p, \cdots, x^{p^{O(\ell^4)}}$$

もしくは、BabyStep-GiantStep **アルゴリズム：**

$$x, x^p, \cdots, x^{p^{\ell^2}},$$
$$x^{p^{\ell^2}}, x^{p^{2\ell^2}}, \cdots, x^{p^{\ell^4}}$$

因子の最大次数が $O(\ell^3)$ **の場合**
$\longrightarrow$ $x^{p^{O(\ell^3)}}$ **まで必要**

$\longrightarrow$ **既約因子分解アルゴリズムの計算量を削減できる**

既約因子分解の計算量

- Cantor-Zassenhaus
  p **乗計算** $\times O(\ell^3) \to O(\ell^3 M(\ell^4)\log p) = O(\ell^{8+o(1)})$

- Gathen-Shoup ：BabyStep-GiantStep
  multipoint evaluation **を利用**
  $\to O(\ell^4 M(\ell^4)\log \ell) = O(\ell^{8+o(1)})$

- Kaltofen-Shoup ：BabyStep-GiantStep
  modular composition **による** p **乗計算**
  $\to O(\ell^{7.797+o(1)})$

- Shoup (NTL) ：BabyStep-GiantStep
  行列を用いない modular composition **による** p **乗**
  $\to O(\ell^{1.5}(\ell^4)^2) = O(\ell^{9.5})$

計算量の比較

Algorithm	$s \in O(\ell^4)$	$s \in O(\ell^3)$
Cantor-Zassenhaus	$O(\ell^{9+o(1)})$	$O(\ell^{8+o(1)})$
Gathen-Shoup	$O(\ell^{8+o(1)})$	$O(\ell^{8+o(1)})$
Shoup (NTL)	$O(\ell^{10})$	$O(\ell^{9.5})$
KS ($\omega = 3$)	$O(\ell^{8.5+o(1)})$	$O(\ell^{8+o(1)})$
KS ($\omega = \log_2 7$)	$O(\ell^{8.272+o(1)})$	$O(\ell^{7.797+o(1)})$
KS ($\omega = 2.375477$)	$O(\ell^{7.667+o(1)})$	$O(\ell^{7.260+o(1)})$

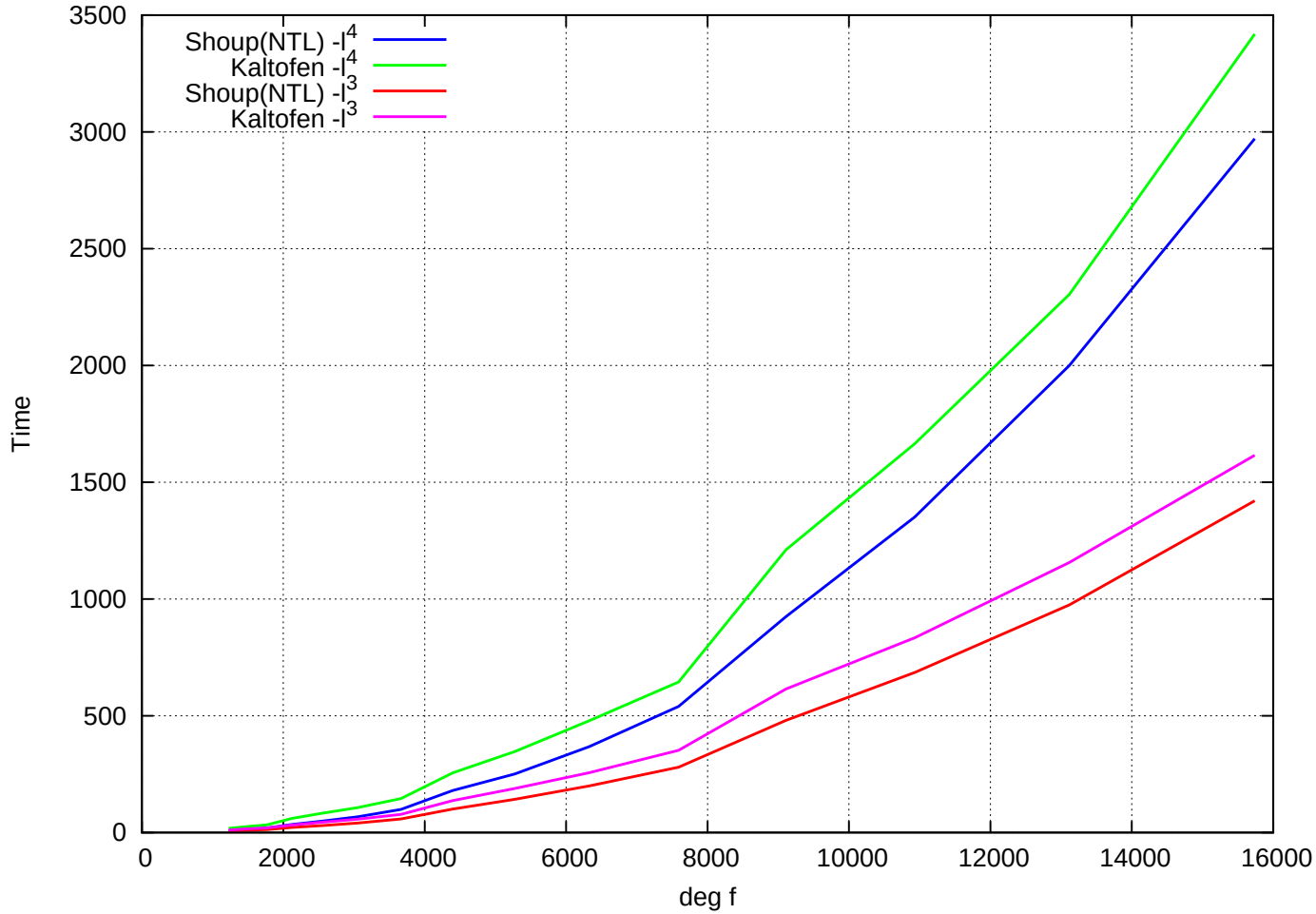
$\longrightarrow$ **漸近的には** Kaltofen-Shoup **が高速**

行列の乗算の計算量： $O(n^\omega)$

KS : Kaltofen-Shoup

既約因子分解の実装結果

$f \in \mathbb{F}_p[X]$ の既約因子分解 ($O(l^3)$ 次の因子)



p:80 ビット

CPU : Opteron 2384 2.7GHz

ℓ 等分多項式の既約因子分解

- 位数計算では根が全部必要なわけではない
  $\longrightarrow$ 小さい次数の根から一つずつ求める
- ワーストケース：$O(\ell^3)$ の次数の根
- 160 ビットの位数計算
  $\longrightarrow$ ℓ は 19 まで必要
- 80 ビット素体 $\mathbb{F}_p, \ell = 19$
  $\longrightarrow$ $\frac{\ell^4-1}{2} = 65160$ 次の $\mathbb{F}_p$ 上の多項式の既約因子分解

ℓ 等分多項式の既約因子分解：実装結果

p:80 ビット (固定)、

次数：$\frac{\ell^4-1}{2} = 65160$ 次

ランダム曲線 40 本

	平均時間 [s]	最大計算時間 [s]
Cantor-Zassenhaus	28647.5	158965.2
Shoup	35144.2	40102
Kaltofen-Shoup	19934.8	36873

1. 最大、平均時間ともに Kaltofen-Shoup が最も高速
2. ℓ を大きくすると、更に Kaltofen-Shoup が効率的

CPU : Opteron 2384 2.7GHz
Memory : 16GB
OS : SUSE Linux
gcc4.3.2, gmp4.2.3, NTL 5.5.2

位数計算実装

- Gaudry の NTLJac2 を修正
- **多項式の既約因子分解：**Kaltofen-Shoup
  - **行列乗算：**Adaptive Winograd **アルゴリズム** $(w = \log_2 7 = 2.8)$[D'Alberto,Nicolau,2009]
  - Brent-Kung **アルゴリズムによる** p **乗計算** [Brent,Kung,1978]
  - **位数計算とインタラクティブ**
- 2^{10} **ねじれ点計算** [**小崎，松尾，**2007]
- MCT **アルゴリズム** [**松尾，趙，辻井，**2004]

$(\tilde{s}_1, \tilde{s}_2)$ の決定

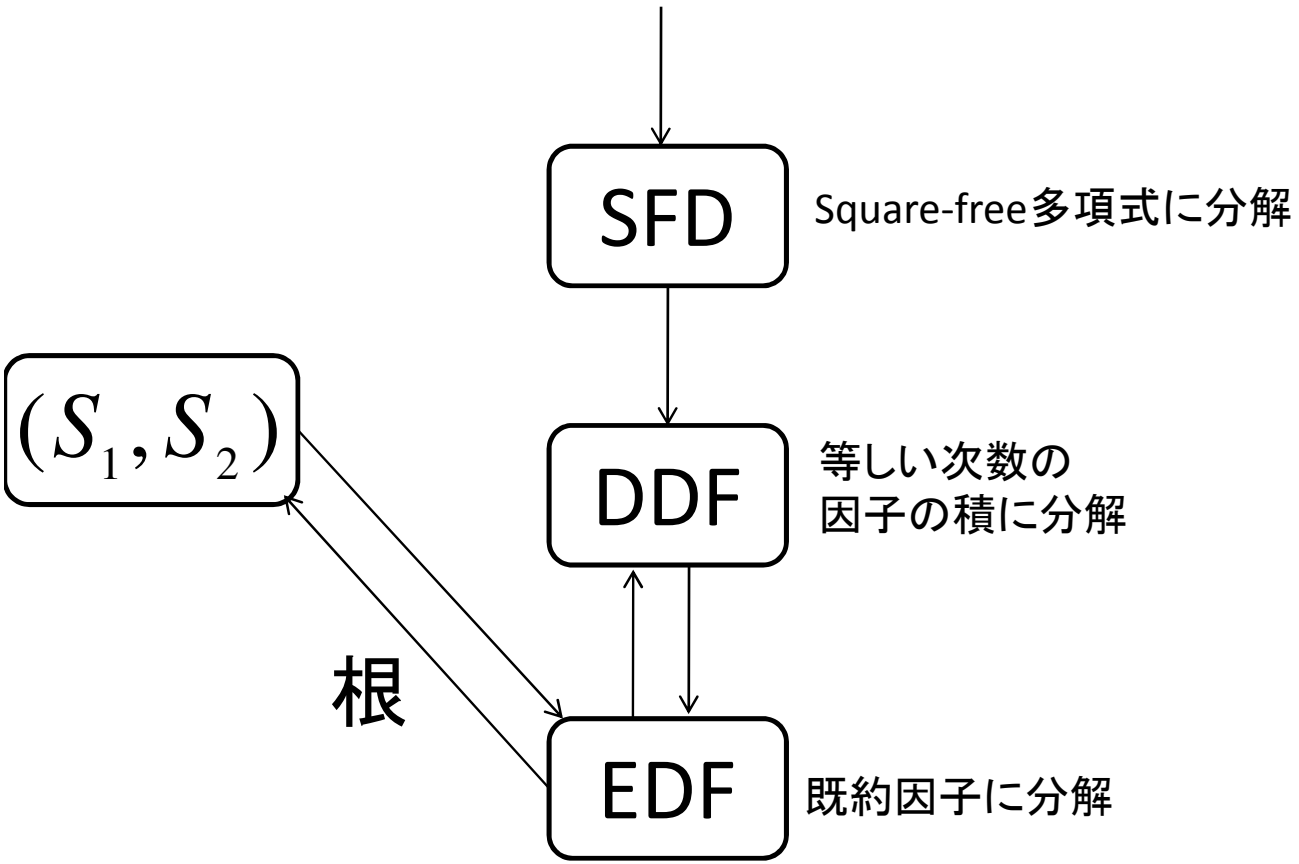
1. Cantor の Division Polynomial を計算
2. 2 変数,$O(l^2)$ 次連立方程式 $E_1(x_1, x_2) = E_2(x_1, x_2) = E_3(x_1, x_2) = 0$ を得る
3. Resultant 計算によって ℓ 等分多項式を生成
4. ℓ 等分多項式の根を一つ求める
5. 根を用いて $\mathbb{F}_p$ を拡大し、拡大体上の根 X_1 を得る
6. X_1 を E_1, E_2 に代入し、X_2 を得る
7. X_1, X_2 から Y_1, Y_2 を得る
8. $P_1 = (X_1, Y_1), P_2 = (X_2, Y_2)$
9. $D = P_1 + P_2 - 2P_\infty$ とし、

$$\phi(D)^4 - \tilde{s}_1\phi(D)^3 + \tilde{s}_2\phi(D)^2 - \tilde{s}_1\tilde{p}\phi(D) + \tilde{p}^2 = 0$$

を満たす $(\tilde{s}_1, \tilde{s}_2)$ を求める

10. $(\tilde{s}_1, \tilde{s}_2)$ が一意に決まるまで 4〜9 まで繰り返す

因子分解


SFD
Square-free多項式に分解
(S_1, S_2)
DDF
等しい次数の
因子の積に分解
根
EDF
既約因子に分解

位数計算実験 1: $\ell = 19$ worst

$p = 71790712076413756478322 7$: 80 ビット

$$
\begin{aligned}
F(X) &= 320683748210147980892362 \\
&+ 560320003960304168676108X \\
&+ 337553632677137575675137X^2 \\
&+ 462700990939751235538893X^3 + X^5
\end{aligned}
$$

$\longrightarrow$

$$
\begin{aligned}
\#\mathcal{J}(\mathbb{F}_p) &= 515390634044594811904759575893203445672304630267 \\
&= 3^3 \cdot 11 \cdot 31 \cdot 10447747 \cdot 15517088599248073 \\
&\quad \cdot 3452911853436666600551
\end{aligned}
$$

:160 ビット

位数計算実験 1

$\ell : 3 \sim 13$ ℓ 等分多項式	3372
$\ell : 3 \sim 13$ Factoring	1896
$\ell = 17$ ℓ 等分多項式	15191
$\ell = 17$ Factoring	12092
$\ell = 19$ ℓ 等分多項式	26054
$\ell = 19$ Factoring	34476
Total $\ell : 3 \sim 19$	94081 = 約 25h
2^{10} torsion	7622
MCT	30134
Total	134934 = 約 36h

CPU : Opteron 2.7GHz
Memory : 16GB
OS : SUSE Linux
gcc4.3.2, gmp4.2.3, NTL 5.5.2

位数計算実験２

$p = 106581482163237588163311 7$: 80 ビット

$$
\begin{aligned}
F(X) &= 50460573473923507010426 3 \\
&+ 33473343260281577513564 0X \\
&+ 75095568300707430304059 4X^2 \\
&+ 10352505379391890696156 00X^3 + X^5
\end{aligned}
$$

$\rightarrow$

$$
\begin{aligned}
\#\mathcal{J}(\mathbb{F}_p) &= 1135961234010851883416337124656122155 \\
&\quad 693413001971 \\
&= 3 \cdot 37865374467028396113877904155204071 \\
&\quad 8564471000657
\end{aligned}
$$

:160 ビット

位数計算実験 1

$\ell : 3 \sim 13$ ℓ 等分多項式	3276
$\ell : 3 \sim 13$ Factoring	2018
$\ell = 17$ ℓ 等分多項式	13974
$\ell = 17$ Factoring	13128
$\ell = 19$ ℓ 等分多項式	27338
$\ell = 19$ Factoring	16264
Total $\ell : 3 \sim 19$	75998 = 約 21h
2^{10} torsion	8358
MCT	22338
Total	106694 = 約 30h

まとめ

- ℓ 等分多項式の因子次数が $O(l^3)$ であることを利用した既約因子分解アルゴリズムを位数計算に適用した
- 位数計算のワースト計算時間が短縮されることを示した
- 特殊性のない安全な超楕円曲線が構成可能となった