種数２の超楕円曲線の２冪ねじれ点の計算について

小崎 俊二 (情報セキュリティ大学院大学)
松尾 和人 (情報セキュリティ大学院大学)

2006年12月2日

種数２の超楕円曲線の位数計算

超楕円曲線のJacobianの有理点のなす有限アーベル群をもちいて暗号を構成
→群位数が160bit程度の素数となる曲線の探索のために位数計算が必要

- 素体上定義された種数２の超楕円曲線の位数計算
  - P. Gaudry and R. Harley, 2000
    Schoofアルゴリズムを基本とした位数計算
    →２冪ねじれ点の利用
  - P. Gaudry and É. Schost, 2004
    上記の改良により80bit程度の素体上の位数計算
    →２冪ねじれ点計算での16次多項式の根を求めるアルゴリズムの改良

Frobenius写像の特性多項式とJacobianの位数

- p: **奇素数、$\mathbb{F}_p$上定義された種数２の超楕円曲線**:

$$C : Y^2 = F(X),\ \ F \in \mathbb{F}_p[X] :\ \ \text{monic},\ \ \deg F = 5,\ \ \underline{\mathbb{F}_p\text{上既約}}$$

- Jacobian**の**p**乗**Frobenius**写像** $\phi_p : \mathbb{J}_C \to \mathbb{J}_C$ **の特性多項式**:

$$\chi(X) = X^4 - s_1 X^3 + s_2 X^2 - p s_1 X + p^2 \in \mathbb{Z}[X],$$
$$|s_1| \le 4\sqrt{p},\ \ |s_2| \le 6p$$

- Jacobian**の**$\mathbb{F}_p$**-有理点の群位数**:

$$\sharp \mathbb{J}_C(\mathbb{F}_p) = \chi(1)$$

Frobenius写像の特性多項式とねじれ点

自然数$n > 1$に対し、nねじれ点の全体を $\mathbb{J}_C[n]$ とするとき、

$p \nmid n$ならば、ϕ_pの$\mathbb{J}_C[n]$への制限写像の特性多項式は、

$$\widehat{\chi}(X) = \chi(X) \bmod n \in \mathbb{Z}[X]$$

となる。

$\widehat{\chi}(X)$の係数は、$[0, n-1]$の範囲内で、

$$[\chi(\phi_p) \bmod n]\mathcal{D} = 0 \text{ for } {}^{\forall}\mathcal{D} \in \mathbb{J}_C[n]$$

を満足する整数として探索可能

GaudryとHarleyによる位数計算アルゴリズム

1. p と素な小さい素数 ℓ_i または素数冪 $\ell_i^{e_i}$ に対する

$$\chi(X) \bmod \ell_i^{e_i}$$

   の係数を決定

2. 中国人の剰余定理により、$\chi(X) \bmod \prod_i \ell_i^{e_i}$ を決定

3. $\sharp\mathbb{J}_C(\mathbb{F}_p) \equiv \chi(1) \bmod \prod_i \ell_i^{e_i}$ より $\sharp\mathbb{J}_C(\mathbb{F}_p)$ を決定

1.において、特に $\chi(X) \bmod 2^k$ を利用 → <u>２冪ねじれ点の計算が必要</u>

GaudryとHarleyの$\chi(X)$ mod 2^mの計算アルゴリズム

Input: 自然数$m > 1$および、種数２の超楕円曲線C

Output: $\chi(X)$ mod $2^m \in \mathbb{Z}[X]$

Cの定義式のFより２ねじれ点$\mathcal{D}_1$を計算する

$[\chi(\phi_p)$ mod $2]\mathcal{D}_1 = 0$を満足する$\chi_1(X) := \chi(X)$ mod 2を探索

for $k = 1$ to $m - 1$ **do**

　$[2]\mathcal{D}_{k+1} = \mathcal{D}_k$を満足する$\mathcal{D}_{k+1}$を計算する (２等分)

　$\chi_k(X) \equiv \chi_{k+1}(X)$ mod 2^k, $\chi_{k+1}(\phi_p)(\mathcal{D}_{k+1}) = 0$を満足する$\chi_{k+1}(X)$を探索

return $\chi_m(X)$

$\chi(X)$ mod 2^m **の計算においては２等分計算の時間が支配的**

GaudryとHarleyの２冪ねじれ点の計算アルゴリズム

$\mathcal{D}_k \in \mathbb{J}_C[2^k]$、$\mathbb{F}_q/\mathbb{F}_p$: $\mathcal{D}_k$の定義される拡大体

$$\mathcal{D}_k = (X^2 + u_1 X + u_0, v_1 X + v_0),\ u_1, u_0, v_1, v_0 \in \mathbb{F}_q$$

$[2]\mathcal{D} = \mathcal{D}_k$を満足する$\mathcal{D}$のweightは２と仮定

$$\mathcal{D} := (X^2 + U_1 X + U_0, V_1 X + V_0),\ U_1, U_0, V_1, V_0 : \text{変数}$$

$$((V_1 X + V_0)^2 - F) \bmod (X^2 + U_1 X + U_0) \equiv \underline{G_1} X + \underline{G_2} = 0,$$
$$G_1, G_2 \in \mathbb{F}_q[U_1, U_0, V_1, V_0]$$

$$[2]\mathcal{D} = (X^2 + \underline{H_1} X + \underline{H_2}, \underline{H_3} X + \underline{H_4}) = \mathcal{D}_k,$$
$$H_i \in \mathbb{F}_q(U_1, U_0, V_1, V_0),\ 1 \le i \le 4$$

GaudryとHarleyの２冪ねじれ点の計算アルゴリズム

$[2]\mathcal{D} = \mathcal{D}_k$ の係数を比較

$$\begin{cases} G_1(U_1, U_0, V_1, V_0) = 0, & G_2(U_1, U_0, V_1, V_0) = 0, \\ H_1(U_1, U_0, V_1, V_0) = u_1, & H_3(U_1, U_0, V_1, V_0) = v_1, \\ H_2(U_1, U_0, V_1, V_0) = u_0, & H_4(U_1, U_0, V_1, V_0) = v_0 \end{cases}$$

$V_0 \succ V_1 \succ U_0 \succ U_1$ の辞書順Gröbner基底計算

$$\begin{cases} V_0 - L_0(U_1) = 0, \\ V_1 - L_1(U_1) = 0, \\ U_0 - M_0(U_1) = 0, \\ \underline{M_1(U_1)} = 0 \end{cases}$$

$$L_0, L_1, M_0, M_1 \in \mathbb{F}_q[U_1],\ \deg M_0, \deg L_1, \deg L_0 < \deg M_1 = 16$$

$\mathcal{D}_k \in \mathbb{J}_C[2^k]$, $\underline{k\text{ の増加}}$ にともない $\mathcal{D}_k$ の定義される体 $\underline{\mathbb{F}_q\text{ の拡大次数の増加}}$

→ M_1 の係数体 $\mathbb{F}_q$ が $\mathbb{F}_p$ の高次の拡大体となることが問題

GaudryとSchostのM_1の根の計算アルゴリズム

M_1の根への$g \in \mathbb{J}_C[2]$の作用

$$\begin{aligned}\mathbf{D}_0 :=& (X^2 + U_1 X + M_0(U_1), L_1(U_1)X + L_0(U_1)) \in \mathbb{J}_C(\mathbb{F}_q[U_1]/(M_1))\\ \mathbf{D}_g :=& \mathbf{D}_0 + g\\ =& (X^2 + \underline{U_1^{(g)}} X + U_0^{(g)}, V_1^{(g)} X + V_0^{(g)}) \in \mathbb{J}_C(\mathbb{F}_q[U_1]/(M_1))\\ & U_1^{(g)}, U_0^{(g)}, V_1^{(g)}, V_0^{(g)} \in \mathbb{F}_q[U_1]/(M_1)\end{aligned}$$

→$U_1^{(g)}(U_1)$として、M_1の根へのgの作用をえる

部分群$G \subset \mathbb{J}_C[2]$に対して、

$$s_G(U_1) := \sum_{g \in G} U_1^{(g)}(U_1) \in \mathbb{F}_q[U_1]/(M_1)$$

の$\mathbb{F}_q$上の最小多項式の次数は、$[\mathbb{J}_C[2] : G]$

GaudryとSchostのM_1の根の計算アルゴリズム

$$\mathbb{J}_C[2] \simeq (\mathbb{Z}/2\mathbb{Z})^4 \supsetneq G_3 \simeq (\mathbb{Z}/2\mathbb{Z})^3 \supsetneq G_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$$
$$\supsetneq G_1 \simeq (\mathbb{Z}/2\mathbb{Z}) \supsetneq G_0 \simeq \{0\}$$

$$s_{G_3}(U_1),\ s_{G_2}(U_1),\ s_{G_1}(U_1),\ s_{G_0}(U_1) = U_1 \in \mathbb{F}_q[U_1]/(M_1)$$

$$s_{G_3}(U_1) \to T_3(X_3) \in \mathbb{F}_q[X_3]$$
$$s_{G_2}(U_1) \to T_2(X_3, X_2) \in \mathbb{F}_q[X_3, X_2]$$
$$s_{G_1}(U_1) \to T_1(X_3, X_2, X_1) \in \mathbb{F}_q[X_3, X_2, X_1]$$
$$s_{G_0}(U_1) \to T_0(X_3, X_2, X_1, U_1) \in \mathbb{F}_q[X_3, X_2, X_1, U_1]$$
$$\deg_{X_3} T_3 = \deg_{X_2} T_2 = \deg_{X_1} T_1 = \deg_{U_1} T_0 = 2$$

GaudryとSchostのM_1の根の計算アルゴリズム

$s_{G_3}(U_1)$の$\underline{\mathbb{F}_q\text{上の最小多項式}T_3(X_3)}$の根$\alpha_3$
→$s_{G_2}(U_1)$の$\underline{\mathbb{F}_q(\alpha_3)\text{上の最小多項式}T_2(\alpha_3, X_2)}$の根$\alpha_2$
→$s_{G_1}(U_1)$の$\underline{\mathbb{F}_q(\alpha_3, \alpha_2)\text{上の最小多項式}T_1(\alpha_3, \alpha_2, X_1)}$の根$\alpha_1$
→$s_{G_0}(U_1)$の$\underline{\mathbb{F}_q(\alpha_3, \alpha_2, \alpha_1)\text{上の最小多項式}T_0(\alpha_3, \alpha_2, \alpha_1, U_1)}$→$M_1$の根

16次多項式M_1の根を４つの２次多項式を順次解き求める

各２次多項式は、その直前の多項式の根を添加した体上の多項式

→T_2, T_1, T_0は、$\underline{\mathbb{F}_q\text{の拡大体上の多項式}}$となり係数体の拡大が問題

M_1 の因子分解パターン実験

2冪ねじれ点計算にあらわれる16次多項式 M_1 の特徴を調べる

- 曲線の定義体の位数: $11 \leq p \leq 61$
- 各 p に対し、100本のランダムな曲線 $C/\mathbb{F}_p$ を選ぶ
- 各 C の2冪ねじれ点 $\mathcal{D}_k$, $3 \leq k \leq 8$ に対する $M_1^{(k)}$ を求める

→ $M_1^{(k)}$ の因子分解パターンをみる

M_1 の因子分解パターン実験結果

２次の因子が８個 または、１次の因子が16個 のパターンのみ

１次の因子に分解したものの数

$k\backslash p$	11	13	17	19	23	29	31	37	41	43	47	53	59	61
3	0	33	28	0	0	23	0	25	31	0	0	32	0	23
4	0	0	7	0	0	0	0	0	6	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0

$M_1 \in \mathbb{F}_q[U_1]$ の根は、$\mathbb{F}_q$ の高々２次の拡大体上に存在

$\Rightarrow$ ４つの２次多項式 $T_3,\ T_2,\ T_1,\ T_0$ のうち高々１つが既約

２ねじれ点部分群G_1, G_2, G_3の選択の影響

$M_1 \in \mathbb{F}_q[U_1]$の根が$\mathbb{F}_q$の２次拡大体に存在
$\Rightarrow$ T_3, T_2, T_1: $\mathbb{F}_q$上可約, T_0: $\mathbb{F}_q$上既約 ならば効率的

２ねじれ点の部分群$G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \mathbb{J}_C[2] \simeq (\mathbb{Z}/2\mathbb{Z})^4$は、

$$\begin{aligned} G_0 = \{0\} \subsetneq G_1 = \langle g_1 \rangle \subsetneq G_2 = \langle g_1, g_2 \rangle \\ \subsetneq G_3 = \langle g_1, g_2, g_3 \rangle \subsetneq \mathbb{J}_C[2] = \langle g_1, g_2, g_3, g_4 \rangle \end{aligned}$$

の生成系(g_1, g_2, g_3, g_4)の選び方に依存

→T_3, T_2, T_1, T_0のうち既約なものを制御

２ねじれ点群$\mathbb{J}_C[2]$の生成系の選択

$T_0 \in \mathbb{F}_q[U_1] \Rightarrow T_1$ の根 $\alpha_1 \in \mathbb{F}_q$

T_1 は、$s_{G_1}(U_1) = U_1 + U_1^{(g_1)}(U_1)$ の最小多項式

U_1 と $U_1^{(g_1)}(U_1)$ が M_1 の根のうち共役

$$\underline{U_1^{(g)}(U_1) = U_1^q \bmod M_1}$$

を満足する $g \in \mathbb{J}_C[2] \backslash \{0\}$ に対して、

$$\begin{aligned} G_0 = \{0\} &\subsetneq G_1 = \langle \underline{g} \rangle \subsetneq G_2 = \langle \underline{g}, g_2 \rangle \\ &\subsetneq G_3 = \langle \underline{g}, g_2, g_3 \rangle \subsetneq \mathbb{J}_C[2] = \langle \underline{g}, g_2, g_3, g_4 \rangle \end{aligned}$$

$\Rightarrow T_3$, T_2, T_1: $\mathbb{F}_q$ 上可約, T_0: $\mathbb{F}_q$ 上既約

$U_1^{(g)}(U_1) = U_1^q \bmod M_1$を満足する２ねじれ点$g$の探索実験

- 曲線の定義体の位数: $11 \le p \le 61$

- 各pに対し、100本のランダムな曲線$C/\mathbb{F}_p$を選ぶ

- $\mathbb{J}_C[2]$の生成系(g_1, g_2, g_3, g_4)を$(g_1, \phi_p(g_1), \phi_p^2(g_1), \phi_p^3(g_1))$と固定

- ２ねじれ点$g_1 \in \mathbb{J}_C[2]$を初期値とし、

$$[2^{k-1}]\mathcal{D}_k = g_1,\ 3 \le k \le 8$$

となる２冪ねじれ点$\mathcal{D}_k$それぞれ対し、

$$U_1^{(g)}(U_1) = U_1^q \bmod M_1,\ M_1 \in \mathbb{F}_q[U_1]$$

を満足する２ねじれ点$g \in \mathbb{J}_C[2]$を探索

$U_1^{(g)}(U_1) = U_1^q \bmod M_1$ を満足する g の探索実験結果

$p \backslash k$	3	4	5	6	7	8	出現回数
11	g_4+g_3	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	44
11	$g_4+g_3+g_1$	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	56
13	g_1	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	45
13	$0/g_3+g_2$	g_3+g_2	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	12
13	$0/g_3+g_2+g_1$	$g_3+g_2+g_1$	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	16
13	$0/g_4+g_2$	g_4+g_2	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	9
13	$0/g_4+g_2+g_1$	$g_4+g_2+g_1$	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	18
17	$0/g_1$	g_1	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	69
17	0	0	0	g_3+g_2	$\leftarrow$	$\leftarrow$	1
17	0	0	$0/g_4+g_2$	g_4+g_2	$\leftarrow$	$\leftarrow$	3
17	$0/g_4+g_3$	$0/g_4+g_3$	g_4+g_3	$\leftarrow$	$\leftarrow$	$\leftarrow$	20
17	$0/g_4+g_3+g_1$	$g_4+g_3+g_1$	$\leftarrow$	$\leftarrow$	$\leftarrow$	$\leftarrow$	7

$\mathbb{J}_C[2] = \langle g_1, g_2, g_3, g_4 \rangle$, $[2^{k-1}]\mathcal{D}_k = g_1$

$U_1^{(g)}(U_1) = U_1^q \bmod M_1$ を満足する g と k の関係

- $19 \leq p \leq 61$ に対しても同様の結果
  →各曲線の2ねじれ点 g_1 を初期値とし、$[2^{k-1}]\mathcal{D}_k = g_1$ を満足する 2^k ねじれ点 $\mathcal{D}_k$ に対し、$U_1^{(g)}(U_1) = U_1^q \bmod M_1$ を満足する2ねじれ点 $g \neq 0$ は、$k > 2$ によらず一定

→$U_1^q \bmod M_1$ の計算は、拡大次数 $[\mathbb{F}_q : \mathbb{F}_p]$ の小さいときに1度おこなえばよい
k の増加にともなう $U_1^q \bmod M_1$ の計算時間は増加の問題はない

２ねじれ点の生成系の変更をおこなうアルゴリズム

Input: $m \in \mathbb{N}_{\geq 2}$, C:HEC, $g_1 \in \mathbb{J}_C[2]$, $\mathcal{D}_2 \in \mathbb{J}_C[2^2]$s.t.$[2]\mathcal{D}_2 = g_1$

Output: $\mathcal{D}_m \in \mathbb{J}_C[2^m]$

```
(g_1, φ_p(g_1), φ_p^2(g_1), φ_p^3(g_1))生成系として、G_iを構成
flag ← false
for k = 3 to m do
    D_{k-1}より M_1^{(k)} ∈ F_q[U_1], D̂_k ∈ J_C(F_q[U_1]/(M_1^{(k)}))を計算
    D̂_k, G_iをもちいて、2^kねじれ点D_kを計算
    if flag=falseかつ、D_k ∉ J_C(F_q) then
        flag ← ture
        U_1^{(g)}(U_1)=U_1^q mod M_1^{(k)}を満足するgを探索
        (g, g'_2, g'_3, g'_4)を生成系として、G_iを再構成
return D_m
```

実装による計算時間の比較

$p = 5 \times 10^{24} + 8503491$

$$\begin{aligned} C : Y^2 = X^5 &+ 2682810822839355644900736X^3 \\ &+ 226591355295993102902116X^2 \\ &+ 2547674715952929717899918X \\ &+ 4797309959708489673059350 \end{aligned}$$

- Magma V2.12-22
- CPU: Athlon64 2.4GHz

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$
G_i**の再構成なし**	39	93	354	684	4062	17716	65665	360224
G_i**の再構成あり**	45	55	288	326	921	4950	21648	83718

単位(秒)

まとめ

- 2冪ねじれ点$\mathcal{D}_k$に対しその2等分点$\mathcal{D}_{k+1}$は、高々2次の拡大体上定義される

- $U_1^{(g)}(U_1) = U_1^q \bmod M_1$を満足する$g$に対して、

  $$G_1 = \langle \underline{g} \rangle \subsetneq G_2 = \langle \underline{g}, g_2 \rangle \subsetneq G_3 = \langle \underline{g}, g_2, g_3 \rangle \Rightarrow T_0 : \mathbb{F}_q \text{上既約}$$

  とし、より効率的にM_1の根を求めることが可能

- $U_1^{(g)}(U_1)=U_1^q \bmod M_1$を満足する2ねじれ点$g$は、初期値が同一の2ねじれ点よりえられる$2^k$ねじれ点$\mathcal{D}_k$に対しては、冪指数$k$によらず一定