種数の大きな超楕円曲線上の指数計算法の計算機実験

古林靖規　　　　高木剛

公立はこだて未来大学大学院 システム情報科学研究科
041-8655 北海道函館市亀田中野町 116-2

あらまし 近年, 超楕円曲線上のペアリング暗号が注目を集めている. 超楕円曲線上のペアリングの安全性は, 入力のヤコビアンに対する離散対数問題と出力の有限体上の離散対数問題に依存している. しかし, 種数の大きな超楕円曲線上のヤコビアンに対する離散対数問題 (HCDLP) の計算機実験の報告は数件しかなく, 実験データに基づく困難性の評価を行うにはデータが不十分である. 本稿では, 素体 $\mathbb{F}_3$ 上定義される超楕円曲線 $H : y^2 = x^{2g+1} + 1$ 上に対し, 種数の大きな超楕円曲線上の HCDLP に対し漸近的に最も高速である指数計算法を実装し, 計算機実験を行った. その結果, 種数 $g = 74$ である $J_H(\mathbb{F}_3)$ の HCDLP($\sharp J_H(\mathbb{F}_3) \approx 2^{120}$) を解くことが出来た.

Implementation of Index Calculus Attack for Hyperelliptic Curves of High Genera

Yasunori Kobayashi　　　　Tsuyoshi Takagi

Graduate School of Systems Information Science, Future University Hakodate,
116-2, Kamedanakano-cho, Hakodate, Hokkaido, 041-0806, Japan.

Abstract Recently, pairngs over hyperelliptic curves have been getting more attentions due to novel protocols and their rich algebraic structures. The security of these pairings depends on both the discrete logarithm problem over hyperelliptic curves (HCDLP) and that over finite fields. However, there are a few previous works which evaluate the security of the HCDLP with high genus by implementing them on computers. In this paper, we implement an efficient algorithm called index calculus method for solving the HCDLP of high genus hyperelliptic curve $H : y^2 = x^{2g+1} + 1$ over $\mathbb{F}_3$. Then we solved the HCDLP over $J_H(\mathbb{F}_3)$ of g = 74, $\sharp J_H(\mathbb{F}_3) \approx 2^{120}$, in 2.3 days using Core 2 Quad(2.66GHz), Core 2 Quad(2.40GHz), and Core 2 Duo(3.00GHz).

1 はじめに

ID ベース暗号 [6], 暗号文キーワード検索 [5] など, 従来の公開鍵方式では実現が困難であった応用プロトコルを実現可能であるペアリング暗号が, 次世代公開鍵暗号方式として注目を集めている. 近年では, 楕円曲線上のペアリングでは実現困難な新たな応用プロトコル [19] が提案されるなど, 超楕円曲線上のペアリング暗号に関する研究が行われている.

超楕円曲線上のペアリングは, 超楕円曲線上のヤコビアンを入力として, 有限体を出力する関数である. 従って, その安全性は入力のヤコビアンに対する離散対数問題 (HCDLP), 及び出力の有限体上の離散対数問題 (DLP) の困難性に依存する. 有限体 $\mathbb{F}_{p^n}$ に対する DLP の効率的な計算手法として数体篩法 [12, 14], 関数体篩法 [1, 3] などが知られている. HCLDP の効率的な計算手法として指数計算法などが知られている. しかし, 種数の大きな超楕円曲線上のヤコビアンに対する HCDLP の計算機実験の報告は数件しかなく, 実験データに基づく困難性の評価を行うにはデータが不十分である.

本稿では, 種数の大きな超楕円曲線上の HCDLP の計算に有効な指数計算法を扱う. 以下, p を超楕円曲線の定義体の標数, q を定義体の位数, g を種数とする. 超楕円曲線上の指数計算法は, 1994 年, Adleman 等によって提案された [2]. Adleman 等による提案アルゴリズムはヒューリスティックなアルゴリズムであり, 計算量は $L_{p^{2g+1}}[1/2, c], c \leq 2.181$ と分析されている. 但し,

$$L_N(\alpha, c) = \exp\left(c(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right)$$

とする. Flassenberg 等は 1997 年, 指数計算法に篩処理を適用し, 初めて指数計算法の実機実験を行った [8]. 但し, Flassenberg 等による実装は, 群位数が高々 40 ビットの実験であった. Enge は 2002 年, ヒューリスティック性を除いた指数計算法を提案し, 計算量を $L_{q^g}(1/2, 6/\sqrt{5})$ と見積もっている [9]. また 2002 年, Enge と Gaudry は計算量評価 $L_{q^g}(1/2, \sqrt{2})$ を持つ指数計算法を提案した [10].

本稿では, 素体 $\mathbb{F}_3$ 上定義される超楕円曲線 H :

$y^2 = x^{2g+1} + 1$ に特化して Enge と Gaudry による指数計算法 [10] の初期実装を行い, 計算機実験を行う. 実装は C 言語を用いて行い, コンパイラは gcc を利用した. 多倍長演算には多倍長演算ライブラリ gnu mp(http://gmplib.org/) を用いた. この指数計算法は $D_1, D_2 \in J_H(\mathbb{F}_p)$, $\sharp J_H(\mathbb{F}_p) = p^g + 1$, smooth bound $B \in \mathbb{N}$ を入力とし, $D_2 = nD_1$ を満たす $n \in [0, \sharp J_H(\mathbb{F}_p) - 1] \subset \mathbb{Z}$ を出力するアルゴリズムであり, 因子基底構成ステップ, 関係探索ステップ, 線形代数ステップの 3 ステップから構成される.

本稿では, 関係探索ステップにおける smooth テスト, 及び既約多項式分解に Cantor-Zassenhaus 法を用いた. 線形代数ステップは Lanczos 法 [16] を実装した. 実験の結果, 因子基底 $F(B)$ の個数 $\sharp F(B) = O(3^B)$ となることを確認した. これは見積もりに近い結果であった. smooth テストに成功する確率は, 見積もり $\exp\left(-\frac{g \log\log(q^g)}{2B}\right)$ に近い結果であった. また, Core 2 Quad (2.40GHz) を搭載した計算機 1 台, Core 2 Quad (2.66GHz) を搭載した計算機 1 台, Core 2 Duo (3.00GHz) を搭載した計算機 1 台, 合計 3 台の計算機 (10 コア) を用いてパラメータ $g = 74, B = 13$ に対し, 約 1.3 日で $\sharp F(B) = 96,124$ 個の関係を探索することが出来た. また, 線形代数ステップでは, Core 2 Quad (2.66GHz) を搭載した計算機 1 台を用いて約 1 日を要して行列を解くことが出来た. 合わせて約 2.3 日を要して約 120 ビット ($\sharp J_H(\mathbb{F}_3) \approx 2^{120}$) の HCDLP を解くことが出来た.

本稿では以下, 2 章で超楕円曲線のヤコビアンについて説明し, 3 章では指数計算法 [10] について説明する. 4 章では指数計算法の実装を行い, 計算機実験の結果を報告する. 5 章では本稿の纏めを行い, 付録として HCDLP の解読データを示す.

2 超楕円曲線

本章では, 超楕円曲線上のヤコビアンについて説明する. p を奇素数とし, $q = p^m, m \in \mathbb{N}$ とする. このとき, 次で与えられる代数曲線 C を有限体 $\mathbb{F}_q$ 上定義される種数 $g \in \mathbb{N}$ の超楕円曲線という.

$$C : y^2 = f(x), \tag{1}$$

ここで, $f(x) \in \mathbb{F}_q[x]$ は $\bar{\mathbb{F}}_q$ において重根を持たず, $\deg(f) = 2g + 1$ を満たすモニック多項式である.

リーマンロッホの定理より, C 上の任意のヤコビアンに対し, 同値類の代表元として次で与えられるヤコビアンが唯一つ存在する.

$$\sum_{P_i \in C} m_i P - \sum_{P_i \in C} m_i \mathcal{O}, m_i \in \mathbb{N}, \sum_{P_i \in C} m_i \leq g \tag{2}$$

ここで, $\mathcal{O}$ は無限遠点である. 本稿では, 式 (2) の形で表現されるヤコビアンを既約因子と呼ぶ. $\mathbb{F}_q$ 上定義される C の既約因子は加法群をなし, この加法群を $J_C(\mathbb{F}_q)$ と表記する. Hasse の定理より, $J_C(\mathbb{F}_q)$ の群位数に関し

$$(\sqrt{q} - 1)^{2g} \leq \sharp J_C(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g} \tag{3}$$

となることが知られている.

2.1 Mumford 表現

本節では, Mumford 表現 [18] について説明する. いま, 式 (2) で与えられる既約因子 $D \in J_C(\mathbb{F}_q)$ に対し, $P_i = (\alpha_i, \beta_i) \in \bar{\mathbb{F}}_q$ として, 次の条件を満たす多項式の組 $U(x), V(x) \in \mathbb{F}_q[x]$ を考える.

$$\begin{cases} U(\alpha_i) = 0, V(\alpha_i) = \beta_i, \\ U(x) \mid f(x) - V(x)^2, \\ \deg(V) \leq \deg(U) \leq g, \\ U(x) : monic \end{cases} \tag{4}$$

D は条件 (4) を満たす多項式の組 $[U(x), V(x)] \in \mathbb{F}_q[x]^2$ を用いて一意的に表現されることが知られており, この既約因子の多項式表現を Mumford 表現という.

本稿では $D = [U(x), V(x)]$ に対し $wt(D) = \deg(U)$ と定義し, $U(x)$ が $\mathbb{F}_q$ 上既約であるとき D を素因子 ($prime$) と呼ぶ. Mumford 表現において $D = [U(x), V(x)]$ の逆元は $-D = [U(x), -V(x)]$ として与えられる. Mumford 表現された既約因子の加算アルゴリズムは, Cantor アルゴリズム [7] などが知られている.

2.2 ペアリング

本節では, 超楕円曲線上のペアリングについて説明する. r を $r \mid \sharp J_C(\mathbb{F}_q)$ を満たす大きな素数とし, k を $r \mid q^k - 1$ を満たす最小の自然数とする. k を埋め込み次数 k と呼ぶ. 加法群 $\mathbb{G}_1 = J_C(\mathbb{F}_q)[r], \mathbb{G}_2 = J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k})$, 乗法群 $\mathbb{G}_3 = \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r$ として, C 上の Tate ペアリングは以下で定義される双線形性を満たす 2 入力 1 出力関数である.

$$\langle\ ,\ \rangle : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3$$

Tate ペアリングを効率的に計算するアルゴリズムとして η_T ペアリング [4], Ate ペアリング [13] などが知られている.

2.3 超楕円曲線上の離散対数問題

$D_1 \in J_C(\mathbb{F}_q)$, $D_2 \in \langle D_1 \rangle$ とする. このとき, $D_2 = \alpha D_1$ を満たす $\alpha \in \{0, 1, 2, \cdots, \sharp\langle D_1 \rangle - 1\}$ を求める問題を, 超楕円曲線上の離散対数問題 (Hyperelliptic Curves Discrete Logarithm Problem, HCDLP) という. 本稿では, 上記 α を $\alpha = \log_{D_1}(D_2)$ と表記する.

3 指数計算法

本章では Enge と Gaudry による指数計算法 [10] について説明する. C を有限体 $\mathbb{F}_q$ 上定義される種数 g の超楕円曲線とする.

この指数計算法は $D_1 \in J_C(\mathbb{F}_q)$, $D_2 \in \langle D_1 \rangle$, $\sharp\langle D_1 \rangle$, 及び smooth-bound と呼ばれる自然数 $B \in \mathbb{N}$ を入力とし, $\log_{D_1}(D_2)$ を出力するアルゴリズムである. 指数計算法は (1) 因子基底構成ステップ, (2) 関係探索ステップ, (3) 線形代数ステップの 3 ステップにより構成される.

3.1 因子基底

本節では因子基底, 及び因子基底の個数の見積もりについて説明する. 因子基底構成ステップでは, smooth-bound $B \in \mathbb{N}$ に対し素因子の部分集合として

$$F(B) = \{D \in J_C(\mathbb{F}_q) \mid D : prime, wt(D) \le B\} \quad (5)$$

を求める.

以下, $\sharp F(B)$ の見積もりについて説明する. $\mathbb{F}_q[x]$ 上の n 次既約多項式の個数 $\nu(n)$ は, メビウス関数を用いて

$$\nu(n) = n^{-1} \sum_{k|n} \mu(k) q^{n/k}$$

で与えられることが知られている [17]. ここで, $\mu(k)$ はメビウス関数である. $\deg(U) < g$ を満たす既約多項式 $U(x) \in \mathbb{F}_q[x]$ に対し, 条件 (4) を満たす対 $V(x) \in \mathbb{F}_q[x]$ の有無を考える. 即ち, $X^2 \equiv f(x) \pmod{U(x)}, \deg(X) < \deg(U)$ を満たす $X \in \mathbb{F}_q[x]$ 存在の有無を決定したいとする. これは, $U(x)$ が既約多項式であることから, 有限体 $\mathbb{F}_{q^{\deg(U)}}$ 上で平方剰余 $X^2 = f(x) \pmod{U(x)}$ の有無を決定する問題と同値である.

以下, $\mathbb{F}_q$ の部分集合 $\{a \in \mathbb{F}_q \mid \deg(a) < \deg(U)\}$ において, 有限体上の平方剰余が偏りなくランダム分布していると仮定する. このとき, 平方剰余が存在する確率は約 1/2 であるため,

$$\sharp F(B) \approx \frac{1}{2} \sum_{n=1}^{B} \nu(n)$$

となる. ここで, $k \ge 2$ において $q^{n/k} \le q^{n/2}$ となることから, $q^n \to \infty$ において

$$\begin{aligned} \sum_{k|n} \mu(k) q^{n/k} &= q^n + \sum_{k|n, k\ge 2} \mu(k) q^{n/k} \\ &\approx q^n \end{aligned}$$

が成り立ため, $\sharp F(B) \approx \sum_{n=1}^{B} \frac{q^n}{2n}$ となる. 従って,

$$\sharp F(B) = O(q^B) \quad (6)$$

となる.

3.2 B-smooth な因子

本節では B-smooth の概念について説明した後, $J_C(\mathbb{F}_q)$ からランダムに選択した既約因子 D が B-smooth となる確率の見積もりを行う.

既約因子 $D = [U(x), V(x)]$ において, $U(x)$ が既約多項式の積として $U(x) = \Pi U_i(x)^{c_i}$ と既約多項式分解されるとき, 条件 (4) から D は

$$D[U(x), V(x)] = \sum c_i P_i, P_i = [U_i(x), V_i(x)] \quad (7)$$

と素因子の和として表現できる. このとき式 (7) において, 全ての素因子 P_i が smooth bound B に対し $wt(P_i) \le B$ を満たすとき, D は B-smooth であるという.

以下, $J_C(\mathbb{F}_q)$ からランダムに選択した D が B-smooth となる確率の見積もりについて説明する. 但し, $J_C(\mathbb{F}_q)$ において B-smooth な既約因子が偏りなくランダムに分布していると仮定する. $S(B)$ を $J_C(\mathbb{F}_q)$ に含まれる B-smooth な既約因子の集合とする. Enge と Stein により $\rho > 0$ に対し, smooth bound B を

$$B = \lceil \log_q L_{q^g}(1/2, \rho) \rceil \quad (8)$$

と取ったとき,

$$\sharp S(B) \ge q^g \cdot L_{q^g}\left(1/2, -\frac{1}{2\rho} + o(1)\right) \quad (9)$$

が成り立つことが示された [11]. ここで $L_N(c, \alpha)$ は, $N > 0, c \in [0,1], \alpha > 0$ に対し

$$L_N(c, \alpha) = \exp(c(\log N)^{\alpha} (\log\log N)^{1-\alpha})$$

で定義される関数である. また, 式 (9) において $o(1)$ は, $N \to \infty$ に対して $o(1) \to 0$ を満たす関数である. 従って, 式 (8) により smooth bound B を与えた場合, $J_C(\mathbb{F}_q)$ からランダムに選択した D が B-smooth となる確率は, 式 (3), (9) より

$$\sharp S(B) / \sharp J_C(\mathbb{F}_q) \approx L_{q^g}\left(1/2, -\frac{1}{2\rho}\right) \quad (10)$$

となる. また式 (8) より, 式 (10) は B を用いて

$$\exp\left(-\frac{g \log\log(q^g)}{2B}\right) \quad (11)$$

と評価できる.

3.3 関係探索ステップ

本章では, 関係探索ステップについて説明した後, 関係探索ステップの計算量見積もりについて説明する. 因子基底 $F(B)$ 上の素因子が $P_1, P_2, \cdots, P_{\sharp F(B)}$ とラベル付けされているとする. 即ち, 因子基底 $F(B) = \{P_1, P_2, \cdots, P_{\sharp F(B)}\}$ と仮定する. このとき, B-smooth な既約因子 $D = \sum c_i P_i \in S(B)$ に対し, 関係 v を以下で定義する.

$$v = (c_1, c_2, \cdots, c_{\sharp F(B)})^T$$

関係探索ステップでは, 異なる $(\sharp F(B) + 1)$ 個の関係を探索する. 探索は以下の手順で行う.

1. ランダムに選択した $\alpha, \beta \in [0, \sharp J_C(\mathbb{F}_q) - 1] \subset \mathbb{Z}$ に対し, $D = \alpha D_1 + \beta D_2$ を計算する.

2. D が B-smooth であるかをテストする. このテストを smooth テストと呼ぶ.

3. D が B-smooth である場合, (α,β,v) の組を保存する.

smooth テストは, $D=[U(x),V(x)]$ に対し $U(x)$ を既約多項式分解し, B 次より大きな既約多項式を因子に持つかを見ればよい.

以下, 関係探索ステップの計算量見積もりについて説明する. 式 (10) より, $(\sharp F(B)+1)$ 個の関係を見つけるのに必要な既約因子の加算, 及び smooth テストの試行回数の見積もりは $(\sharp F(B)+1)/L_{q^g}(1/2,\frac{1}{2\rho}))$ である. 1 回あたりの既約因子の加算, 及び既約多項式分解は多項式時間で可能である. 従って, 関係探索ステップの漸近的計算量は

$$L_{q^g}\left(1/2,\rho+\frac{1}{2\rho}+o(1)\right) \tag{12}$$

となる.

3.4 線形代数ステップ

線形代数ステップでは, 関係探索ステップで集めた関係に対し連立一次方程式を立て, 行列計算によりその解を求める. 以下, 関係探索ステップでは $\sharp F(B)+1$ 個の関係 $v_1,v_2,\cdots,v_{\sharp F(B)+1}$ を集めたと仮定し, $v_i=(c_{i,1},c_{i,2},\cdots,c_{i,\sharp F(B)})^T$ と表記する. このとき, $(\sharp F(B))\times(\sharp F(B)+1)$ 行列 A を以下で定義する.

$$\begin{aligned} A &= (v_1,\cdots,v_{\sharp F(B)+1}) \\ &= \begin{pmatrix} c_{1,1} & \cdots & c_{\sharp F(B)+1,1} \\ c_{1,2} & \cdots & c_{\sharp F(B)+1,2} \\ \vdots & \ddots & \vdots \\ c_{1,\sharp F(B)} & \cdots & c_{\sharp F(B)+1,\sharp F(B)} \end{pmatrix} \end{aligned}$$

各関係 v_i に含まれる非零成分は高々g 個であるため A は疎行列であり, 全ての非零成分は高々g 以下の自然数である. 線形代数ステップでは,

$$AX=0 \bmod \sharp J_C(\mathbb{F}_q) \tag{13}$$

を満たす $(\sharp F(B)+1)$ 次ベクトル X を行列計算を用いて解く. このとき,

$$rank(A)\le F(B)<(X \text{ の未知数の個数})$$

より, 方程式 (13) は非自明な解を持つことが保証される. 行列計算は $\mathbb{Z}/J_C(\mathbb{F}_q)$ 上で行うため, 式 (13) の非自明な解 $X\in(\mathbb{Z}/J_C(\mathbb{F}_q)\mathbb{Z})^{\sharp F(B)+1}$ の成分は, 最大 $(\sharp J_C(\mathbb{F}_q)-1)$ の大きな整数を取り得る.

A が疎行列であることから, 方程式 (13) の効率的な解法として Lanczos 法 [16], Wiedemann 法 [21] などが挙げられる. Lanczos 法を用いたとき, 線形代数ステップの計算量は

$$O(\sharp F(B)^2)=O\left(L_{q^g}\left(\frac{1}{2},2\rho\right)\right) \tag{14}$$

で与えられる.

式 (13) の非自明な解 $X=(x_1,x_2,\cdots,x_{\sharp F(B)+1})$ に対し, $\sum_{i=0}^{\sharp F(B)+1}x_i(\alpha_iD_1+\beta D_2)=0$ が成り立つ. 従って, $(\sum x_i\beta_i)D_2=-(\sum x_i\alpha_i)D_1$ となるため, 離散対数 $\log_{D_1}(D_2)$ は

$$\log_{D_1}(D_2)=-\frac{\sum_{i=0}^{\sharp F(B)+1}x_i\alpha_i}{\sum_{i=0}^{\sharp F(B)+1}x_i\beta_i} \bmod \sharp J_C(\mathbb{F}_q)$$

となる.

3.5 指数計算法の計算量

smooth-bound B を式 (8) で与えたとき, 式 (12), (14) より, 指数計算法に必要な計算量は

$$\begin{aligned} & L_{q^g}\left(\frac{1}{2},\rho+\frac{1}{2\rho}\right)+L_{q^g}\left(\frac{1}{2},2\rho\right) \\ & \approx L_{q^g}\left(\frac{1}{2},\max\left\{\rho+\frac{1}{2\rho},2\rho\right\}\right) \end{aligned}$$

で与えられる. $\max\left\{\rho+\frac{1}{2\rho},2\rho\right\}$ は $\rho=1/\sqrt{2}$ で最小値 $\sqrt{2}$ を持つので, 本指数計算法の計算量は

$$L_{q^g}(1/2,\sqrt{2}) \tag{15}$$

となる.

4 実装結果

本章では, 指数計算法 [10] の計算機実験による結果を報告する. 本稿では次の 2 つの理由により, 素体 $\mathbb{F}_p$ 上定義される種数 g の超楕円曲線 $H: y^2=x^{2g+1}+1$ に対し指数計算法の実装を行う.

1. $2g+1$ が素数となり, 且つ $p \bmod 2g+1$ が $\mathbb{F}_{2g+1}$ の生成元となる p,g の組に対し, 高島により与えられた distortion 写像 [20] を用いることで, 種数の大きな超楕円曲線上のペアリングを構成可能である.

2. 上記条件を満たす p,g の組に対し, $\sharp J_H(\mathbb{F}_p)=p^g+1$ が成り立つため, 群位数の計算が容易である.

本稿では, 以下の 2 つの理由により, 標数 $p=3$ に固定して実装を行う. (1) $\mathbb{F}_p[x]$ 上の演算に, 著者等が CSS2008 で $J_H(\mathbb{F}_3)$ 上の Tate ペアリング [22] の実装に用いたライブラリを利用する. (2) 他の奇標数を選択した場合と比較して, 大きな g に対しても短時間でデータを取ることが可能である.

4.1 実装環境

実装は C 言語により行い, コンパイラは gcc を用いる. 線形代数ステップで行う多倍長演算には, 多倍長演算ライブラリ gnu mp(http://gmplib.org/) を用いる.

本実験はCore 2 Quad Q6600(2.40GHz), 3.25 GB RAM, Windows XP を搭載した計算機 1 台を主計算機として実験を行う．但し, 一部の計算に Core 2 Quad(2.66 GHz), 4.00 GB RAM, Windows Vista を搭載した計算機 1 台, 及び Core 2 Duo(3.00 GHz), 4.00 GB RAM, Windows XP を搭載した計算機 1 台の計 2 台を並列分散処理に用いる．

4.2 パラメータの選択

本稿では, 標数 p を 3 に固定して指数計算法の実装を行うため, 計算時間などに影響を与えるパラメータは種数 g, 及び smooth-bound B の 2 つである．

種数 g に関しては, $g = 74$ のとき $\sharp J_H(\mathbb{F}_3) \approx 2^{120}$ となること, 及び g の変動に伴う計算時間の変動を見るため, $g = 26, 56, 74$ とした．このとき, $\sharp J_H(\mathbb{F}_3) = 3^g + 1$ のビット長はそれぞれ 40 ビット, 80 ビット, 120 ビット程度である．

smooth-bound B に関しては, 式 (8), (15) において理論的に最適となる $B = L_{p^g}(1/2, 1/\sqrt{2})$ を基準として考慮した．この際, $g = 26, 56, 74$ における B の値はそれぞれ 7,11,13 であった．この値を基に, B の変化に伴い, 関係探索ステップにおいて smooth テストに成功する確率, 及び関係探索ステップに必要な計算時間の変動を見るために $B = 10, 11, 12, 13, 14, 15, 16, 17$ とした．

4.3 実装方法の詳細

因子基底

$[U(x), -V(x)] = -[U(x), V(x)]$ より, $[U(x), V(x)]$ が $F(B)$ に保存されているとき, $[U(x), -V(x)]$ は $F(B)$ の元として保存しない．こうすることで, $F(B)$ に保存する因子基底の個数を約半分に削減することが出来る．表 1 に, 各 B に対し, 上記削減を行った際の $\sharp F(B)$ を示す．表 1 より $\sharp F(B) = O(3^B)$ であるが, これは見積もり (6) と一致する．

表 1：実装で必要であった因子基底の個数

B	$\sharp F(B)$
10	4,672
11	12,724
12	34,804
13	96,124
14	266,787
15	745,075
16	2,090,080
17	5,888,320

各因子基底 $[U(x), V(x)]$ に対し, 条件 (4) より $V(x)$ は $U(x)$ を用いて計算可能である．従って, $F(B)$ は各因子基底 $[U(x), V(x)]$ を構成する多項式 $U(x)$ からなるテーブルとして実装を行う．これにより, $F(B)$ に要するメモリ量を約半分に削減できる．

関係探索ステップ

関係探索ステップは以下のように実装を行う． 幅 $l \in \mathbb{N}$ を指定し, 入力された $D_1, D_2 \in J_H(\mathbb{F}_3)$ に対しテーブル $\{D_1, 2D_1 \cdots, lD_1, D_2, 2D_2 \cdots, lD_2\}$ を作成する．本稿では $l = 1000$ とした．

$S_i, T_i \in J_H(\mathbb{F}_3), (i = 0, 1, 2, \cdots)$ を次のように与える． まず, 入力された D_1, D_2 とランダムに選択した $s, t \in [0, \sharp J_H(\mathbb{F}_3) - 1] \subset \mathbb{Z}$ に対し, 初期値を $S_0 = sD_1$, $T_0 = tD_2$ として与える．上記テーブルを用いて, ランダムに選択した $\alpha_i, \beta_i \in \{1, 2, \cdots, l\}$ に対し, $S_{i+1} = S_i + \alpha_i D_1$, $T_{i+1} = T_i + \beta_i D_2$ として S_i, T_i の更新を行う．このとき, 各 S_i, T_i に対し $D = S_i + T_i$ を計算し, smooth テストにより D が B-smooth であるか調べる．$D = [U(x), V(x)]$ に対し, smooth テストは Cantor-Zassenhaus 法を用いて $U(x)$ の既約多項式分解を行うことで実装する．但し, distinct degree factorization(DDF) において次数 B より大きな多項式が検出された時点で smooth テストは終了とする．$U(x) = \Pi U_i(x)^{m_i}, U_i \in F(B)$ と既約多項式分解されたとき, $m_i \neq 0$ を満たす m_i の個数は $\sharp F(B)$ 個の成分中, 高々g 個であり高い確率で $m_i = 0$ となる．また実験の結果, 非零 m_i に対してはほぼ全て $m_i = 1$ であった。

B-smooth である $D = [U(x), V(x)]$ に対し, 関係 $v = (c_1, c_2, \cdots, c_{\sharp F(B)})^T$ の作成は次の手順で行う．上記既約多項式分解において, $m_i = 0$ である全ての i に対し, $c_i = 0$ とする．$m_i \neq 0$ である i に対しては $a(x) = V(x) \mod U_i(x)$ を計算し, $a(x)$ の最高次数の係数が 1 又は 0 であれば $c_i = m_i$ とし, $a(x)$ の最高次数の係数が -1 であれば $c_i = -m_i$ とする．

線形代数ステップ

線形探索ステップでは Lanczos 法を用い実装を行う．尚, Structured Gaussian Elimination(SGE)[15] を用いることで式 (13) における行列 X のサイズを小さくすることができるが, 本稿では SGE の実装は行っていない．

4.4 線形探索ステップの実装データ

本節では, 4.2 節で述べた g, B に対し, 主計算機 1 台を用いて 10,000 個の関係探索を行った結果を示す．表 2 に種数 $g = 26$ の結果を, 表 3 に $g = 56$ の結果を, 表 3 に $g = 74$ の結果をそれぞれ示す．尚, 表中の $Pr(B)$ は smooth テストに成功した平均確率, 即ち, $Pr(B) =$ 10,000/(10,000 個の関係を見つけるのに行った smooth テストの回数) である．ave は 1 つの関係を見つけるのに要した平均時間, 即ち, ave = (10,000 個の関係を見つけるのに要した時間)/10,000 を指す．total は関係探索ステップの計算時間の見積もり, 即ち, total = $(\sharp F(B) + 1)$ave である．

smooth テストに成功した平均確率は, 見積もり (11) に近い結果であった．一方, 関係探索ステップに要する計算時間の見積もりは, 式 (12) とは異なる結果であった．その理由として, DDF において B 次より大きな多項式が検出された時点でテストを終了するよう smooth テストの実装を行ったことが影響していると考えられる．

表 2：$g = 26$ case ($\sharp J_H(\mathbb{F}_3) \approx 2^{40}$)

B	$Pr(B)$	ave(μsec)	total(sec)
10	0.14	367	1.7
11	0.20	244	3.1
12	0.27	205	7.2
13	0.34	165	15.9
14	0.42	142	37.9
15	0.48	131	97.6

表 3：$g = 56$ case ($\sharp J_H(\mathbb{F}_3) \approx 2^{80}$)

B	$Pr(B)$	ave(sec)	total(hour)
10	9.4×10^{-5}	3.32	4.3
11	3.6×10^{-4}	0.85	3.0
12	1.1×10^{-3}	0.29	2.8
13	2.7×10^{-3}	0.12	3.2
14	5.5×10^{-3}	0.06	4.7
15	1.0×10^{-2}	0.03	6.6

表 4：$g = 74$ case ($\sharp J_H(\mathbb{F}_3) \approx 2^{120}$)

B	$Pr(B)$	ave(sec)	total(day)
12	1.7×10^{-5}	14.89	5.9
13	6.5×10^{-5}	3.73	4.1
14	2.2×10^{-4}	1.14	3.5
15	5.3×10^{-4}	0.49	4.2
16	1.2×10^{-3}	0.22	5.3
17	2.2×10^{-3}	0.12	7.9

4.5 $g = 74, B = 13$ の場合

本節では, 種数 $g = 74$ における smooth bound B の理論的最適値 $B = \lceil L_{3^{74}}(1/2, 1/\sqrt{2}) \rceil = 13$ に対する指数計算法の実装結果を示す. 関係探索ステップで要した時間は, 4.1 節で述べた計 3 台の計算機 (10 コア) を用いて約 1.3 日であった. 線形探索ステップは, 主計算機 1 台を用いて約 1 日で方程式 (13) を解くことができた. 指数計算法全体で約 2.3 日を要してパラメータ $g = 74, B = 13$ における $J_H(\mathbb{F}_3)$ 上の HCDLP を解くことが出来た. 解読結果は付録に示した.

5 まとめ

本稿では, 素体 $\mathbb{F}_3$ 上定義される超楕円曲線 $H : y^2 = x^{2g+1} + 1$ に特化した指数計算法の実装を行い, 計算機実験を行った. 関係探索ステップは smooth テスト, 及び既約多項式分解に Cantor-Zassenhaus 法を利用した. 線形代数ステップは Lanczos 法を用いた. その結果, smooth bound B に対し smooth テストを成功する確率は, 見積もり $\exp\left(-\frac{g \log \log(q^g)}{2B}\right)$ に近い結果を得た. また, パラメータ $g = 7, B = 13$ に対し, 約 120 ビットの HCDLP を解くことが出来た.

参考文献

[1] L. M. Adleman, "The Function Field Sieve", ANTS-I, LNCS 877, pp.108-121, 1994.

[2] L. M. Adleman, J. DeMarrais and M. D. A. Huang, "A Subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields", ANTS-I, LNCS 877, pp.28-40, 1994.

[3] L. M. Adleman and M. D. A. Huang. "Function Field Sieve Method for Discrete Logarithms over Finite Fields", Inform. and Comput., 151, 12, pp.5-16, 1999.

[4] P. S. L. M. Barreto, S. Galbraith, C. hEigeartaigh and M. Scott, "Efficient Pairing Computation on Supersingular Abelian Varieties", Designs, Codes and Cryptography, 42, 3, pp.239-271, 2007.

[5] D. Boneh, G.D. Crescenzo, R. Ostrovsky and G. Persiano, "Public Key Encryption with Keyword Search", EUROCRYPT 2004, LNCS 3027, pp.506-522, 2004.

[6] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing", CRYPTO 2001, LNCS 2139, pp.213-229, 2001.

[7] D.G. Cantor, "Computing in the Jacobian of a Hyperelliptic Curve", Math. Comp., 48, 177, pp.95-101, 1987.

[8] R. Flassenberg and S. Paulus, "Sieving in Function Fields", Experiment. Math., 8, pp.339-349, 1999. (Preliminary Version: Technical Report, TI-97-13, Darmstadt University of Technology, 1997.)

[9] A. Enge, "Computing Discrete Logarithm in High-Genus Hyperelliptic Jacobians in Provably Subexponential Time", Math. Comp., 71, pp.729-742, 2002.

[10] A. Enge and P. Gaudry, "A General Framework for Subexponential Discrete Logarithm Algorithm", Acta Arith, 102, pp.83-103, 2002.

[11] A. Enge and A. Stein, "Smooth Ideals in Hyperelliptic Function Fields", Math. Comp., 71, pp.1219-1230, 2002.

[12] D. M. Gordon, "Discrete Logarithms in GF(p) Using the Number Field Sieve", SIAM Journal on Discrete Mathmatics 6, 1, pp.124-138, 1993.

[13] R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren, "Ate Pairing on Hyperelliptic Curves", EUROCRYPT 2007, LNCS 4515, pp.430-447, 2007.

[14] A. Joux, R. Lercier, N. Smart and F. Vercauteren, "The Number Field Sieve in the Medium Prime Case", CRYPTO 2006, LNCS 4117, pp.326-344, 2006.

[15] B. A. LaMacchia and A. M. Odlyzko, "Solving Large Sparse Linear Systems over Finite Fields", CRYPTO 90, LNCS 537, pp.109-133, 1991.

[16] C. Lanczos, "Solution of Systems of Linear Equations by Minimized Iterations", J. Res. Nat. Bur. Stand, 49, pp.33-53, 1952.

[17] R. Lidl and H. Niederreiter, *Introduction to Finite Field and Their Applications*, Cambridge University Press, pp.85-86, 1986.

[18] D. Mumford, *Tata Lectures on Theta II*, Birkhaeuser, 1984.

[19] T. Okamoto and K. Takashima "Homomorphic Encryption and Signatures from Vector Decomposition", Pairing 2008, LNCS 5209, pp.57-74, 2008.

[20] K. Takashima, "Efficiently Computable Distortion Maps for Supersingular Curves", ANTS VIII, LNCS 5011, pp.88-101, 2008.

[21] D. H. Wiedemann, "Solving Sparse Linear Equations over Finite Fields", IEEE Trans. Information Theory, IT-32, pp.54-62, 1986.

[22] 古林靖規, 高木剛, "種数の大きな超楕円曲線を利用した Tate ペアリングの実装", CSS 2008, 論文集 第一冊分, pp.187-192, 2008.

付録 解読データ

4.5 節における HCDLP の解読に使用した入力 $D_1 = [U_1(x), V_1(x)]$, $D_2 = [U_2(x), V_2(x)]$, 及び離散対数 $\alpha = \log_{D_1}(D_2)$ を示す. 以下, 次数 n の多項式 $a(x) = \sum_{i=0}^{n} c_i x^i$ を, $a = c_n c_{n-1} \cdots c_1 c_0$ と表記する.

$U_1 =$ 10 01202100 01010200 12022012 01022222
22200111 20000220 10000022 01001002 22121021

$V_1 =$ 11222100 10002121 10012111 11212021
02002122 10021202 02212212 10201120 02102112

$U_2 =$ 12 20120102 22122100 00011110 01001221
00122122 21121121 22210210 00202011 02212012

$V_2 =$ 1 20122100 21202221 01110222 00020102
12110120 02200121 21201211 11100102 12111012

$\alpha =$ 19 82417165 79069728 64909939