**SCIS 2004** The 2004 Symposium on Cryptography and Information Security
Sendai, Japan, Jan.27-30, 2004
The Institute of Electronics, Information and Communication Engineers

# 4 次拡大体上の楕円曲線暗号に対する Weil descent attack について I
# A Weil Descent Attack against Elliptic Curve Cryptosystems over Quartic Fields I

長尾孝一* 有田正剛† 松尾和人† 志村真帆呂‡
Koh-ichi Nagao Seigo Arita Kazuto Matsuo Mahoro Shimura

**あらまし** 4 次拡大体上定義された楕円曲線に対し、Jacobian がこの楕円曲線とそれを $q^2$ 乗フロベニウス写像で移した楕円曲線の直和となっている genus 2 の超楕円曲線を考える。本論文では、この genus 2 の超楕円曲線が、多くの場合 2 次拡大体上定義されることを示す。従って、4 次拡大体上の楕円曲線上定義された DLP の多くは、2 次拡大体上の genus 2 の超楕円曲線の Jacobian 群上の DLP に帰着される。

**キーワード** 回文形式, 楕円曲線暗号, Weil descent 攻撃, reducible Jacobian, Gaudry's variant

## 1 はじめに

Frey [6] によってアイデアが示された Weil descent 攻撃は、拡大体上の (超) 楕円曲線上で定義された DLP を部分体上の genus のより大きい代数曲線の Jacobi 群上の DLP に帰着し、これを解く攻撃法である。しかし、一般には DLP が帰着される部分体上の曲線の genus が非常に大きくなり、この攻撃法は効果を持たない。その後、GHS 切断と呼ばれる手法により、部分体上の曲線の genus が小く抑えられ、攻撃が成立する場合があることが Gaudry, Hess, Smart [9] によって示され、この GHS 切断を用いた Weil descent 攻撃に関し、多くの研究がなされてきた [7, 5, 2, 3]。

本論文では、4 次拡大体 $\mathbb{F}_{q^4}$ 上の楕円曲線暗号に対する、reducible Jacobian を用いたある種の Weil descent 攻撃を与える。本攻撃法においては GHS 切断は利用されない。

本論文で与えられる Weil descent 攻撃では、まず $\mathbb{F}_{q^4}$ 上定義された楕円曲線 $E$ を "回文形式" と呼ばれるモデル $E_N$ に $\mathbb{F}_{q^4}$-同型変換する。次に $\mathbf{Jac}_C \simeq E_N \times E_N^{q^2}$ となる genus 2 の曲線 $C$ を構成する。本論文で示されるように、$C$ は多くの場合 $\mathbb{F}_{q^2}$ 上定義されており、従って $E(\mathbb{F}_{q^4})$ 上の DLP は $\mathbf{Jac}_C(\mathbb{F}_{q^2})$ 上の DLP に帰着される。また、本論文に続く "4 次拡大体上の楕円曲線暗号に対する Weil descent attack について II" [4] において、$\mathbf{Jac}_C(\mathbb{F}_{q^2})$ 上の DLP が $\mathbb{F}_q$ 上定義された genus 9 の $C_{ab}$ 曲線の Jacobian 群上の DLP に帰着される。この DLP は、Gaudry's variant の Thériault [12] による改良により解くことが可能であり。その計算量、即ち $E(\mathbb{F}_{q^4})$ 上の DLP を解くために必要な計算量は $O(q^{34/19})$ となる。一方、$E(\mathbb{F}_{q^4})$ 上の DLP を square-root 法を用いて解いた場合、その計算量は $O(q^2)$ である。従って、本論文で示す Weil descent 攻撃は、理論上 4 次拡大体 $\mathbb{F}_{q^4}$ 上の多くの楕円曲線暗号に対し効果を持つ。

以下では、$k = \mathbb{F}_q$ を標数が 2 でない有限体、$k_n := \mathbb{F}_{q^n}$ をその $n$ 次拡大体とする。また、Weil descent 攻撃の対象とする、楕円曲線 $E$ は 3 次式 $f(x) \in k_4[x]$ を用いて

$$E/k_4 : y^2 = f(x)$$

と定義されているものとする。

## 2 回文形式

3 次多項式

$$F(x) := \alpha x^3 + \beta x^2 + \beta^{q^2} x + \alpha^{q^2} \quad (\alpha(\neq 0), \beta \in k_4)$$

を用いて、楕円曲線 $E/k_4$ が $E : y^2 = F(x)$ と書かれているとき、$E$ を回文形式と呼び、$E$ を特に $E_N$ と書く。任意の $\lambda \in k_4 \backslash k_2$ を用いて、$E_N/k_4$ に対し $C$ を

$$\begin{aligned} C : y^2 &= \alpha(x-\lambda)^6 + \beta(x-\lambda)^4(x-\lambda^{q^2})^2 \\ &\quad +\beta^{q^2}(x-\lambda)^2(x-\lambda^{q^2})^4 \\ &\quad +\alpha^{q^2}(x-\lambda^{q^2})^6 \end{aligned} \tag{1}$$

で定義する。尚、$C$ は $\lambda$ のとり方によらず、$k_2$-同型である。すると、[13, Ch. 14] の議論から、直ちに $\mathbf{Jac}_C \simeq E_N \times E_N^{q^2}$ を得る。また、$C$ から $E_N$ への写像が

$$\psi(x,y) := \left( \left( \frac{x-\lambda}{x-\lambda^{q^2}} \right)^2, \frac{y}{(x-\lambda^{q^2})^3} \right)$$

で定義される。さらに、その構成法から、明かに $C$ は体 $k_2$ 上定義される。

$E_N$ 上の点 $P$ に対し、$\psi$ の逆写像 $\psi^{-1}$ の $C$ 上の像は 2 点存在する。簡単の為にこれらを $\{\psi^{-1}(P), \psi^{-1}(P)'\}$ と書く。特に $E_N$ 上の無限遠点 $\infty_{E_N}$ の逆像は $C$ 上の 2

* 関東学院大学 工学部, Dept. of Engineering, Kanto-Gakuin Univ.
† 中央大学 研究開発機構, The Research and Development Initiative of Chuo University
‡ 中央大学 21 世紀 COE プログラム, Chuo University 21st Century Center Of Excellence Program
本研究の一部は、通信・放送機構「情報セキュリティ高度化のための第 3 世代暗号技術の研究開発」プロジェクトの一環として行われた。

つの無限遠点 $\{\infty_C, \infty_C'\}$ である。$\psi^{-1}(P), \psi^{-1}(P)'$ の $x$ 座標、$y$ 座標は

$$\left(\frac{x-\lambda}{x-\lambda^{q^2}}\right)^2 = x(P), \quad \frac{y}{(x-\lambda^{q^2})^3} = y(P)$$

の解として得られる。

$h$ を以下で定義する:

$$\begin{aligned} h : E_N(k_4) &\to \mathbf{Jac}_C(k_4) \qquad (2)\\ P &\mapsto \psi^{-1}(P) + \psi^{-1}(P)' - \infty_C - \infty_C' \end{aligned}$$

明らかに $h$ は群準同型写像である。ここで、

$$\nu(x) := \mathrm{monic}((x-\lambda)^2 - x(P)(x-\lambda^{q^2})^2)$$

$$w(x) := y(P)(x-\lambda^{q^2})^3 \bmod \nu(x)$$

と置くと、$h(P)$ は Mumford 表現を用いて $(\nu(x), w(x))$ と書ける [10, 11]。$\mathbf{Jac}_C(k_4)$ から $\mathbf{Jac}_C(k_2)$ へのトレース写像

$$\mathrm{T}\left(\sum_i n_i P_i\right) := \sum_i n_i \left(P_i + P_i^{q^2}\right) \qquad (3)$$

は明らかに準同型写像である。

**補題 2.1.** $G \subseteq E_N(k_4)$ を素位数かつ位数が $2q^2+2$ 以上である部分群とする。$P \in G \backslash 0$ に対して、$\mathrm{T} \circ h(P) \neq 0$.

証明. $\mathrm{T} \circ h(P) \neq 0$ を満たす $P \in E_N(k_4)$ が高々 $2q^2+1$ 個であることをいえば十分である。$P$ を $x(P) \neq 1, \infty$ である点とする。この仮定の下で、$\mathrm{T} \circ h(P) \neq 0$ を満たす $P$ が高々 $2q^2-2$ 個であることをいえばよい。$b := (-1+x(P))/2$, $A(x) := (x-\lambda)^2 + (x-\lambda^{q^2})^2$, $B(x) := (x-\lambda)^2 - (x-\lambda^{q^2})^2$ と置く。$\nu(x) = \frac{1}{2}(A(x) + \frac{b+1}{b}B(x))$ と書けている。$A(x)$,$B(x)$ は $q^2$ 乗フロベニウス写像によって、それぞれ $A(x)$, $-B(x)$ に移る。$\mathrm{T} \circ h(P) = 0$ としたとき、$\nu(x)$ は $q^2$ 乗フロベニウス写像によって不変であるので、$(\frac{b+1}{b})^{q^2} = -\frac{b+1}{b}$ を得る。この式を満たす $b$ は高々 $q^2-1$ 個であるので、このような $P$ は高々 $2q^2-2$ 個しかないことがわかる。 □

この補題から、暗号に利用される位数が almost prime の $E_N(k_4)$ については、写像 $T \circ h$ による $\mathbf{Jac}_C(k_2)$ への像が潰れないことがわかる。以下では、どのような楕円曲線が回文形式と同型であるかを調べる。

## 3 回文形式の性質

定数項が 0 でない 3 次式 $F(x) \in k_4[x]$ に対して、その根の集合を

$$S_F := \{\delta \in \bar{k_4} | F(\delta) = 0\}$$

と書く。また、

$$S_F^{-q^2} := \{\delta^{-q^2} \in \bar{k_4} | F(\delta) = 0\}$$

とする。

**補題 3.1.** $F(x)$ が $r, \alpha, \beta \in k_4$ を用いて、$r(\alpha x^3 + \beta x^2 + \beta^{q^2} x + \alpha^{q^2})$ と書かれる $\iff S_F = S_F^{-q^2}$.

証明. $(\Rightarrow)$ $(r(\alpha\delta^3 + \beta\delta^2 + \beta^{q^2}\delta + \alpha^{q^2}))^{q^2} = r^{q^2}\delta^{3q^2}(\alpha^{q^2} + \beta^{q^2}(\frac{1}{\delta^{q^2}}) + \beta(\frac{1}{\delta^{q^2}})^2 + \alpha(\frac{1}{\delta^{q^2}})^3)$ より明らか。

$(\Leftarrow)$ $S_F = \{\delta_1, \delta_2, \delta_3\}$ とする。$\mathrm{N}_{k_4/k_2}(-\delta_1\delta_2\delta_3) = (-\delta_1\delta_2\delta_3)^{q^2+1} = 1$ より、Hilbert の定理 90 から、$\frac{r^{q^2}}{r} = -\delta_1\delta_2\delta_3$ を満足する $r \in k_4$ が存在する。$F(x) = r(x-\delta_1)(x-\delta_2)(x-\delta_3)$ と置くと、$F(x) = r(x - (\frac{1}{\delta_1})^{q^2})(x - (\frac{1}{\delta_2})^{q^2})(x - (\frac{1}{\delta_3})^{q^2}) = x^3 r^{q^2}(\frac{1}{x} - \delta_1^{q^2})(\frac{1}{x} - \delta_2^{q^2})(\frac{1}{x} - \delta_3^{q^2}) = x^3 F^{(q^2)}(\frac{1}{x})$ を得る。 □

**補題 3.2.** $E/k_4$ が $r, \alpha, \beta \in k_4$ を用いて、

$$E : y^2 = r(\alpha' x^3 + \beta' x^2 + \beta'^{q^2} x + \alpha'^{q^2})$$

で定義されているとする。このとき、$E$ と $k_4$-同型な回文形式 $E_N$ が存在する。また、この $E_N$ は $\alpha := \alpha' r^{2q^2}/r$, $\beta := \beta' r^{q^2}$ により、

$$E_N : y^2 = \alpha x^3 + \beta x^2 + \beta^{q^2} x + \alpha^{q^2}$$

と採ることができる。

証明. $u := r^{(-q^2+1)/2}$ とする。このとき $u^2 = r/r^{q^2}$ である。この $r$, $u$ と $\alpha$, $\beta$ を用いて、$u^2 r(\alpha' x^3 + \beta' x^2 + \beta'^{q^2} x + \alpha'^{q^2}) = \alpha(u^2 x)^3 + \beta(u^2 x)^2 + \beta^{q^2}(u^2 x) + \alpha^{q^2})$ を得る。従って、$y' := yu$, $x' := u^2 x$ により、$E$ は $E_N : y'^2 = \alpha x'^3 + \beta x'^2 + \beta^{q^2} x' + \alpha^{q^2}$ と $k_4$-同型である。 □

補題 3.1, 3.2 から次の命題とその系を得る。

**命題 3.3.** 3 次式 $F(x) \in k_4[x]$ が $S_F = S_F^{-q^2}$ を満足するとき、楕円曲線 $E/k_4 : y^2 = F(x)$ と $k_4$-同型な回文形式 $E_N$ が存在する。

**系 3.4.** 楕円曲線 $E/k_4 : y^2 = f(x)$ に対して、$S_{f(Ax+B)} = S_{f(Ax+B)}^{-q^2}$ を満足する $A(\neq 0), B \in k_4$ が存在するとき、$E$ と $k_4$-同型な回文形式 $E_N$ が存在する。

証明. 楕円曲線 $y^2 = f(Ax+B)$ は $E$ と $k_4$-同型である。従って、命題 3.3 から明らか。 □

## 4 回文形式であらわされる楕円曲線

### 4.1 $f(x)$ が既約の場合

ここでは、$f(x)$ が既約の場合に、楕円曲線 $E : y^2 = f(x)$ と $k_4$-同型な回文形式が存在する条件について調べる。

$f(x) \in k_4[x]$ を既約な 3 次式で、$S_f = S_f^{-q^2}$ が成り立つものとする。$\delta$ を $f(x) = 0$ の一つの解とする。$f(x)$ は既約であるので、$S_f = \{\delta, \delta^{q^4}, \delta^{q^8}\}$ である。

**補題 4.1.** $\mathrm{N}_{k_{12}/k_6}(\delta) = \delta^6 + 1 = 1$

証明. $\{\delta, \delta^{q^4}, \delta^{q^8}\} = S_f = S_f^{-q^2} = \{\delta^{-q^2}, \delta^{-q^4}, \delta^{-q^8}\}$ より、$\delta^{-q^2}$ は $\delta, \delta^{q^4}, \delta^{q^8}$ のいずれかである。$\delta^{-q^2} = \delta$ とすると、$\delta^{q^2+1} = 1$ より、$\delta \in k_4$ を得る。これは $f(x)$ の既約性に反する。$\delta^{-q^2} = \delta^{q^4}$ とすると、$(\delta^{q^2+1})^{q^2} = 1$ より両辺を $q^{10}$ 乗することによって、やはり、$\delta^{q^2+1} = (\delta^{q^2+1})^{q^{12}} = 1$, $\delta \in k_4$ を得る。これもまた、$f(x)$ の既約性に反する。従って、$\delta^{-q^2} = \delta^{q^8}$ を得る。この式を、$(\delta^{q^6+1})^{q^2} = 1$ と変形し、更に両辺を $q^{10}$ 乗して、

$$1 = (\delta^{q^6+1})^{q^{12}} = \delta^{q^6+1} = \mathrm{N}_{k_{12}/k_6}(\delta)$$

を得る。 □

今の補題の逆を考える。$\delta$ を $\mathrm{N}_{k_{12}/k_6}(\delta)=\delta^6+1=1$ を満たす $k_{12}\backslash k_4$ の元とする。

$$f(x):=(x-\delta)(x-\delta^{q^4})(x-\delta^{q^8})$$

と置く。

**補題 4.2.** $S_f=S_f^{-q^2}$.

証明. $S_f^{-q^2}=\{\delta^{-q^2},\delta^{-q^6},\delta^{-q^{10}}\}$ である。$1=(\delta^{q^6+1})^{q^2}=\delta^{q^8+q^2}$ より $\delta^{-q^2}=\delta^{q^8}$、$1=\delta^{q^6+1}$ より $\delta^{-q^6}=\delta$、$1=(\delta^{q^6+1})^{q^4}=\delta^{q^{10}+q^4}$ より $\delta^{-q^{10}}=\delta^{q^4}$ を得る。よって、$S_f^{-q^2}=S_f$ を得る。 □

先の 2 つの補題より直ちに次の補題を得る。

**補題 4.3.** $f(x)\in k_4[x]$ を 3 次既約多項式とする。また、$\delta\in k_{12}$ を $f(x)$ の根とする。このとき、

$$\mathrm{N}_{k_{12}/k_6}(\delta)=\delta^{q^6+1}=1\Leftrightarrow S_f=S_f^{-q^2}$$

以下、$\delta\in k_{12}\backslash k_4$ に対して、$\mathrm{N}_{k_{12}/k_6}(\delta-B)\in k_2$ となる $B\in k_4$ の存在する条件を考える。以下では、

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

と置く。

**補題 4.4.** $\mathrm{N}_{k_{12}/k_6}(\delta-B)\in k_2$ となる $B\in k_4$ が存在する必要十分条件は $d(\delta)\neq 0$ である。また、$d(\delta)\neq 0$ のとき、この $B$ は、

$$B=-\frac{1}{d(\delta)}\big(\delta^{q^8}(\delta^{q^2+1}-\delta^{q^2+q^4})+\delta(\delta^{q^4+q^6}-\delta^{q^6+q^8})+\delta^{q^4}(\delta^{q^8+q^{10}}-\delta^{1+q^{10}})\big)\in k_4$$

で与えられる。

証明. $\mathrm{N}_{k_{12}/k_6}(\delta-B)\in k_2$ を

$$\Big((\delta-B)(\delta-B)^{q^6}\Big)^{q^2}=(\delta-B)(\delta-B)^{q^6}$$

と書き、$B\in k_4$ より、$B^{q^4}=B^{q^8}=B$ に注意すると、線形方程式系

$$\begin{bmatrix}\delta^{q^2}-\delta^{q^6} & \delta^{q^8}-\delta\\ \delta^{q^{10}}-\delta^{q^2} & \delta^{q^4}-\delta^{q^8}\end{bmatrix}\begin{bmatrix}B\\ B^{q^2}\end{bmatrix}=\begin{bmatrix}\delta^{1+q^6}-\delta^{q^2+q^8}\\ \delta^{q^2+q^8}-\delta^{q^4+q^{10}}\end{bmatrix}$$

を得る。上式の左辺の行列の行列式 $=d(\delta)$ である。これを解いて、与えられた $B$ を得る。

逆に、$d(\delta)=0$ かつ 上の行列で書かれた線形方程式系が解 $B\in k_4$ をもつと仮定する。このとき、

$$(\delta^{q^8}-\delta)(\delta^{q^2+q^8}-\delta^{q^4+q^{10}})-(\delta^{q^4}-\delta^{q^8})(\delta^{1+q^6}-\delta^{q^2+q^8})=0$$

である。左辺の式を $M(\delta)$ と置くと、

$$0=M(\delta)+\delta^{q^2}d(\delta)=(\delta^{q^6}-\delta^{q^2})(\delta^{q^4}-\delta)(\delta^{q^8}-\delta^{q^4})$$

を得て、$\delta\in k_4$ となり最初の仮定に矛盾する。 □

$\delta\in k_{12}\backslash k_4$ に対して、

$$f_\delta(x):=(x-\delta)(x-\delta^{q^4})(x-\delta^{q^8})\in k_4[x],$$

$$E_\delta/k_4:y^2=f_\delta(x)$$

と置く。$d(\delta)=0$ としたとき、補題 4.4 より $\mathrm{N}_{k_{12}/k_6}(A\delta+B)=1$ となる $A,B\in k_4$ が存在しないことがわかる。このため、補題 4.1,4.2, 及び系 3.4 より、$E_\delta$ と $k_4$-同型な回文形式が存在しないことがわかる。

逆に、$d(\delta)\neq 0$ とし、$B\in k_4$ を上の補題 4.4 から得られる値とする。ノルム写像 $\mathrm{N}_{k_4/k_2}$ は surjective であるので、$\mathrm{N}_{k_4/k_2}(A)=A^{q^2+1}=\mathrm{N}_{k_4/k_2}(\delta-B)$ を満たす $A\in k_4$ が存在する。実際、

$$A=\begin{cases}\sqrt{\mathrm{N}_{k_4/k_2}(\delta-B)} & \mathrm{N}_{k_4/k_2}(\delta-B)\in k_2^{\times 2}\\ \sqrt{-\mathrm{N}_{k_4/k_2}(\delta-B)} & \mathrm{N}_{k_4/k_2}(\delta-B)\notin k_2^{\times 2}\end{cases}$$

と採れば十分である。また、$A\in k_4$ より、$\mathrm{N}_{k_{12}/k_6}(A)=A^{q^6+1}=A^{q^2+1}=\mathrm{N}_{k_4/k_2}(\delta-B)$ である。

$$F(x):=f_\delta(Ax+B)\tag{4}$$

と置く。$F(\frac{\delta-B}{A})=f_\delta(\delta)=0$, $F(\frac{\delta^{q^4}-B}{A})=f_\delta(\delta^{q^4})=0$, $F(\frac{\delta^{q^8}-B}{A})=f_\delta(\delta^{q^8})=0$ より、

$$S_F=\left\{\frac{\delta-B}{A},\frac{\delta^{q^4}-B}{A},\frac{\delta^{q^8}-B}{A}\right\}$$

を得る。また、$\mathrm{N}_{k_{12}/k_6}(\frac{\delta-B}{A})=\frac{\mathrm{N}_{k_4/k_2}(\delta-B)}{\mathrm{N}_{k_4/k_2}(\delta-B)}=1$ であるので、補題 4.3 より、$S_F=S_F^{-q^2}$ を得る。以上と系 3.4 より、次の命題を得る。

**命題 4.5.** $E_\delta$ と $k_4$-同型な回文形式 $E_N$ が存在する必要十分条件は $d(\delta)\neq 0$ である。

さらに、$d(\delta)=0$ となる $E_\delta$ の特徴づけを考える。$j(E_\delta)\in k_2$ とする。このとき、$\delta=\eta\theta$, $(\eta\in k_4,\theta\in k_6)$ と書かれている。このため、$\eta^{q^4}=\eta$, $\theta^{q^6}=\theta$ に注意すると、$d(\delta)=d(\eta\theta)=\eta^{1+q^2}(\theta^{q^2+q^6}-\theta^{q^2+1}+\theta^{q^4+1}-\theta^{q^4+1}+\theta^{q^2+1}+\theta^{q^2+1})=0$ を得る。以下では、体 $k$ の標数が 3 でない場合について、次の命題を示す。

**命題 4.6.** $j(E_\delta)\in k_4\backslash k_2$ のとき、$d(\delta)\neq 0$ である。また、$E_\delta$ と $k_4$-同型な回文形式 $E_N$ が存在する。

上で述べた議論と併せると、$d(\delta)=0$ となる $E_\delta$ は $j(E_\delta)\in k_2$ と特徴付けられる。

$$t:=-\frac{1}{3}\mathrm{Tr}_{k_{12}/k_4}(\delta),\ \Delta:=\delta+t$$

と置く。

**補題 4.7.**

$$\mathrm{Tr}_{k_{12}/k_4}(\Delta)=\Delta+\Delta^{q^4}+\Delta^{q^8}=0.$$

証明. $\Delta$ の定義より直ちに従う。 □

**補題 4.8.**

$$d(\delta)=d(\Delta).$$

証明. 補題 4.4 より直ちに従う。 □

**補題 4.9.**

$$\begin{aligned} d(\Delta) &= 3(\Delta^{1+q^{10}} - \Delta^{q^4+q^6}) \\ &= 3(\Delta^{q^4+q^2} - \Delta^{q^8+q^{10}}) \\ &= 3(\Delta^{q^8+q^6} - \Delta^{1+q^2}) \\ &= -3(\Delta^{1+q^2} + \Delta^{1+q^6} + \Delta^{q^4+q^6}) \end{aligned}$$

証明. $d(\delta)$ は $(\Delta^{1+q^{10}} - \Delta^{q^4+q^6})$, $(\Delta^{q^4+q^2} - \Delta^{q^8+q^{10}})$, $(\Delta^{q^8+q^6} - \Delta^{1+q^2})$ の 3 項の和で書かれている。補題 4.7 から得られる $\Delta^{q^8} = -\Delta^{q^4} - \Delta$, $\Delta^{q^{10}} = -\Delta^{q^6} - \Delta^{q^2}$ を用いて、これらの項から $\Delta^{q^8}$, $\Delta^{q^{10}}$ を消去すると、これらが $-(\Delta^{1+q^2} + \Delta^{1+q^6} + \Delta^{q^4+q^6})$ に等しいことがわかる。 □

**補題 4.10.** $d(\delta) = 0$ のとき、

$$\frac{\Delta}{\Delta + \Delta^{q^6}} = \frac{\Delta^{q^4}}{\Delta^{q^4} + \Delta^{q^{10}}} = \frac{\Delta^{q^8}}{\Delta^{q^8} + \Delta^{q^2}} \in k_4$$

証明. $\Delta^{q^6-1} \in k_4$ をいえば十分である。補題 4.8 4.9 より、

$$\begin{aligned} \Delta^{q^6-1} - (\Delta^{q^6-1})^{q^4} &= \frac{\Delta^{q^6+q^4} + \Delta(\Delta^{q^2} + \Delta^{q^6})}{\Delta^{q^4+1}} \\ &= -\frac{d(\Delta)}{3\Delta^{q^4+1}} = -\frac{d(\delta)}{3\Delta^{q^4+1}} = 0 \end{aligned}$$

である。 □

命題 4.6 の証明. $d(\delta) = 0$ と仮定する。ここで、

$$\delta + t = \Delta = (\Delta + \Delta^{q^6})\frac{\Delta}{\Delta + \Delta^{q^6}}$$

と書けば、$\Delta + \Delta^{q^6} \in k_6$ であり、また、 補題 4.10 より $\frac{\Delta}{\Delta+\Delta^{q^6}} = \frac{\Delta^{q^4}}{\Delta^{q^4}+\Delta^{q^{10}}} = \frac{\Delta^{q^8}}{\Delta^{q^8}+\Delta^{q^2}} \in k_4$ である。

$$F(x) := f_\delta(\frac{\Delta}{\Delta + \Delta^{q^6}}x - t) \in k_4[x]$$

と置く。$F(\Delta + \Delta^{q^6}) = f_\delta(\Delta - t) = f_\delta(\delta) = 0$, $F(\Delta^{q^4} + \Delta^{q^{10}}) = f_\delta(\Delta^{q^4} - t) = f_\delta(\delta^{q^4}) = 0$, $F(\Delta^{q^8} + \Delta^{q^2}) = f_\delta(\Delta^{q^8} - t) = f_\delta(\delta^{q^8}) = 0$ より $F$ の全ての根は $k_6$ に入る。従って、$F$ は $k_4 \cap k_6 = k_2$ 上の monic 多項式と $k_4$ の元の積で書かれる。明らかに $E' : y^2 = F(x)$ は $E_\delta$ と $k_4$-同型であり、また、$j(E') \in k_2$ である。よって、$j(E_\delta) \in k_2$ である。以上で、$j(E_\delta) \notin k_2$ のとき $d(\delta) \neq 0$ であることが示された。よって、これと命題 4.5 より、命題 4.6 を得る。 □

以上の議論から明らかなように、標数が 2, 3 でない体 $k_4$ 上定義され、$f$ が既約 (即ち $2 \nmid \#E(k_4)$) であり、且つ $j(E) \in k_4 \backslash k_2$ である $E$ を用いた楕円曲線暗号の全てに Weil descent 攻撃が適用可能である。また、$k_4$ の標数が 3 の場合についても、多くの場合に Weil descent 攻撃が成立することを実験により確認した。更に、$j(E) \in k_2$ の場合にも、適当な $k_4$-isogeny によって $E$ を $j(E') \in k_4 \backslash k_2$ である $E'$ に写像することで、Weil descent 攻撃を適用可能であると考えられる。

以下に、$E$ と $k_4$-同型な回文形式 $E_N$ を求めるアルゴリズムを示す。

**Algorithm 1** Finding a palindrome form

**Input:** $E/k_4 : y^2 = f(x)$ s.t. $f$ is irreducible$/k_4$
**Output:** A palindrome form $E_N/k_4$ s.t. $E_N \cong E$

1: Find a root $\delta \in k_{12}$ of $f$
2: Compute $B = -\frac{1}{d(\delta)}\big(\delta^{q^8}(\delta^{q^2+1} - \delta^{q^2+q^4}) + \delta(\delta^{q^4+q^6} - \delta^{q^6+q^8}) + \delta^{q^4}(\delta^{q^8+q^{10}} - \delta^{1+q^{10}})\big) \in k_4$
3: Find $A$ s.t. $\mathrm{N}_{k_4/k_2}A = \mathrm{N}_{k_{12}/k_6}(\delta - B)$
4: $F(x) = f(Ax + B)$
5: Find $r, \alpha', \beta' \in k_4$ s.t. $F(x) = r(\alpha' x^3 + \beta' x^2 + \beta'^{q^2} x + \alpha'^{q^2})$
6: $\alpha = \alpha' r^{2q^2}/r$, $\beta = \beta' r^{q^2}$
7: $E_N : y^2 = \alpha x^3 + \beta x^2 + \beta^{q^2} x + \alpha^{q^2}$

### 4.2 $f(x)$ が可約の場合

この節では、3 次式 $f(x)$ が可約のとき、楕円曲線 $E/k_4 : y^2 = f(x)$ と $k_4$ 同型な回文形式が存在するか否かの問題を考える。

#### 4.2.1 $f(x)$ が 1 次式と既約 2 次式の積に分解する場合

**補題 4.11.** $f(x)$ が 1 次式と 2 次式の積でかけているとき、$E/k_4$ と $k_4$-同型な回文形式は存在しない。

証明. $E$ と $k_4$-同型な回文形式 $E'/k_4 : y^2 = F(x)$, $F(x) := \alpha x^3 + \beta x^2 + \beta^{q^2} x + \alpha^{q^2}$ があったと仮定し、矛盾を導く。$E$ の定義式が 1 次式と 2 次式の積で書けるので、$E(k_4) \simeq \mathbb{Z}/2\mathbb{Z} \simeq E'(k_4)$ である。従って多項式 $F(x)$ も $k_4$ 内で 1 次式と 2 次式の積で書ける。従って $c \in k_4$, $\alpha, \delta \in k_8, \notin k_4$ を用いて $F(x) = \alpha(x - c)(x - \delta)(x - \delta^{q^4})$ と書かれる。補題3.1 で示した回文形式の特性から $\delta^{-q^2} = \delta^{q^4}$ または $\delta^{-q^2} = \delta$ が導き出される。$\delta^{-q^2} = \delta^{q^4}$ とすると $\delta^{q^2+q^4} = 1$ であり、その両辺を $q^6(q^2 - 1)$ 乗すると $\delta^{q^4-1} = \delta^{q^8(q^4-1)} = 1$ を得る。よって $\delta \in k_4$ となり矛盾である。一方、$\delta^{-q^2} = \delta$ とすると $\delta^{q^2+1} = 1$ であり、その両辺を $q^2 - 1$ 乗すると $\delta^{q^4-1} = 1$ を得る。よって $\delta \in k_4$ となりこちらも矛盾である。従って、補題が証明された。 □

**注意**： Genus 2 の曲線 $C/k_2$ の Jacobian $\mathbf{Jac}_C$ が $k_4$ 上定義された楕円曲線 $E$ と $E^{q^2}$ の直積と同型であるとき、$E$ は回文形式で書かれることを、中央大学の百瀬文之教授に御指摘頂いた。このため、$f(x)$ が 1 次式と既約 2 次式の積でかけているとき、genus 2 の曲線 $C/k_2$ で、$\mathbf{Jac}_C \simeq E \times E^{q^2}$ を満たすものが存在しないことがわかる。

#### 4.2.2 $f(x)$ が 1 次式の積に分解する場合

**命題 4.12.** $f(x)$ が一次式の積に分解するとき、楕円曲線 $E/k_4$ と $k_4$-同型な回文形式 $E_N$ が存在する。

このような楕円曲線は Legendre form またはその 2 次 twist と $k_4$-同型なので、定義式が

$$y^2 = rx(x - 1)(x - c), \quad c \in k_4 \backslash \{0, 1\},\ r \in k_4^\times$$

の形で書かれるとして一般性を失わない。$f(x) = rx(x - 1)(x - c)$ と置く。以下では、2 つの場合に場合分けすることによって、それぞれの場合に

$$S_{f(Ax+B)} = S_{f(Ax+B)}^{-q^2}$$

となる $A(\neq 0), B \in k_4$ があることを示す。これによって、系 3.4 より、命題 4.12 の証明が完成する。

**補題 4.13.** 方程式系 $\mathrm{N}_{k_4/k_2}(B) = \mathrm{N}_{k_4/k_2}(1+B) = \mathrm{N}_{k_4/k_2}(c+B)$ は解

$$B = \frac{1}{c - c^{q^2}}(c + c^{q^2+1})$$

を持つ。

証明. 与えられた方程式系を

$$B^{1+q^2} = (1+B)(1+B^{q^2}) = (c+B)(c^{q^2} + B^{q^2})$$

と書くと、ここから直ちに線型方程式系

$$\begin{bmatrix} 1 & 1 \\ c^{q^2} & c \end{bmatrix} \begin{bmatrix} B \\ B^{q^2} \end{bmatrix} = \begin{bmatrix} -1 \\ c^{q^2+1} \end{bmatrix}$$

を得る。ここで、$c \notin k_2$ なので、$c - c^{q^2} \neq 0$ であり、この方程式系は与えられた解 $B$ を持つ。 □

命題 4.12 の証明.
($c \in k_4 \backslash k_2$ の場合) 補題 4.13 で与えられた $B$ を用いて、

$$F(x) := f(Bx - B)$$

と置く。すると、$F(1) = f(0) = 0$, $F(\frac{1+B}{B}) = f(1) = 0$, $F(\frac{c+B}{B}) = f(c) = 0$ から、$S_F = \{1, \frac{1+B}{B}, \frac{c+B}{B}\}$ を得る。また、補題 4.13 より、

$$\mathrm{N}_{k_4/k_2}(1) = \mathrm{N}_{k_4/k_2}\left(\frac{1+B}{B}\right) = \mathrm{N}_{k_4/k_2}\left(\frac{c+B}{B}\right) = 1$$

である。$\mathrm{N}_{k_4/k_2}(x) = x^{q^2+1}$ に注意すると、$S_F = S_F^{-q^2}$ がわかる。
($c \in k_2 \backslash \{0,1\}$ の場合) $c \neq -1$ とし、

$$F(x) := f(-\frac{c}{1+c}x + \frac{c}{1+c})$$

と置くと、$F(1) = f(0) = 1$, $F(-\frac{1}{c}) = f(1) = 0$, $F(-c) = f(c) = 0$ より、$S_F = \{1, -\frac{1}{c}, -c\}$ を得る。また、$c^{q^2} = c$ より $(-\frac{1}{c})^{-q^2} = -c$, $S_F = S_F^{-q^2}$ がわかる。
次に、$c = -1$ とし、

$$F(x) := f(-\frac{2}{3}x - \frac{1}{3})$$

と置くと、$F(-\frac{1}{2}) = f(0) = 1$, $F(-2) = f(1) = 0$, $F(1) = f(-1) = 0$ より、$S_F = \{1, -\frac{1}{2}, -2\}, S_F = S_F^{-q^2}$ がわかる。 □

この場合にも既約の場合と同様に $E$ と $k_4$-同型な回文形式 $E_N$ を求めるアルゴリズムが上の議論より得られる。

**注意:** 楕円曲線 $E/k_4 : y^2 = f(x)$ を定義する 3 次式 $f(x) \in k_4[x]$ が既約多項式で与えられたとき、式 1 で与えられる genus 2 の曲線 $C/k_2 : y^2 = g(x)$ を定義する 6 次式 $g(x) \in k_2[x]$ は一次因子を持たないことが証明できる。一方、楕円曲線 $E/k_4$ の定義式 $f(x)$ が 3 つの 1 次式の積で与えられたとき、半数以上の $E$ に対し $C/k_2$ を定義する 6 次式 $g(x) \in k_2[x]$ が一次因子を持つことを、数値実験により確認した。$g(x)$ が一次因子を持つとき、$C$ と $k_2$-同型で $C' : y^2 =$ monic 5 次多項式 型の曲線が存在する。従って、$E(k_4)$ 上の DLP を $\mathbf{Jac}_{C'}(k_2)$ 上の DLP に帰着可能である。この DLP は genus 8 の $C_{ab}$ 曲線の Jacobian 群の DLP に帰着され、Weil descent 攻撃が成立することが既に知られている [3]。また、[12] によって、これを $O(q^{30/17})$ の計算量で解くことが可能である。

**Algorithm 2** A Weil descent attack against ECDLP over the quartic extension of a finite field

**Input:** $E/k_4 : y^2 = f(x)$, $P, Q \in E(k_4)$
**Output:** $m \in \mathbb{Z}$ s.t. $Q = [m]P$
1: **if** $f$ has only one linear factor **then**
2: Compute $m$ by a square-root method and terminate
3: Compute $E_N$ from $E$ according to §4
4: Compute $P_N, Q_N \in E_N(k_4)$ w.r.t $P, Q$ according to §2
5: Compute $C$ from $E_N$ according to §2
6: Compute $P_J, Q_J \in \mathbf{Jac}_C(k_2)$ w.r.t $P_N, Q_N$ according to §2
7: Compute a $C_{ab}$ curve $C_S$ over $k$ from $C$ according to [3] or [4]
8: Compute $P_S, Q_S \in \mathbf{Jac}_{C_S}(k_2)$ w.r.t $P_J, Q_J$ according to [3] or [4]
9: Compute $m$ s.t. $Q_S = [r]P_S$ by Gaudry's variant and terminate

## 5 アルゴリズムと例

以上をまとめ、以下のアルゴリズムと例を得る。

**例** 標数 $p = 2^{40} - 2^{35} - 1$ の素体 $k = \mathbb{F}_p$ 上、既約式 $w_2^2 + 352619714346 = 0$ で定義された 2 次拡大体を $k_2 = \mathbb{F}_p(w_2)$、さらに $k_2$ 上既約式 $w_4^2 + 702753204573w_2 + 465976829831 = 0$ で定義された 2 次拡大体を $k_4 = k_2(w_4)$ と書く。ここでは、160-bit 素位数

$$\#E(k_4) = 1287200406650928609777376029597716043015507861907$$

を持つ楕円曲線

$$\begin{aligned} E/k_4 : y^2 &= f(x) \\ &= x^3 + ((773569929047w_2 + 698785454132)w_4 \\ &\quad +892468792697w_2 + 773390597884)x \\ &\quad +(245022657483w_2 + 657619174138)w_4 \\ &\quad +721187940068w_2 + 865450731541 \end{aligned}$$

から、論文に従い $C/k_2$ を求め、また、$E(k_4)$ 上の

$$\begin{aligned} P &= (1, P_y) \in E(k_4) \\ Q &= [m]P = (Q_x, Q_y) \\ P_y &= (448960196430w_2 + 540742096931)w_4 \\ &\quad +521019129313w_2 + 684726004416 \\ Q_x &= (554052113845w_2 + 305126934156)w_4 \\ &\quad +227302711986w_2 + 315595177192 \\ Q_y &= (636988126233w_2 + 293526808818)w_4 \\ &\quad +683215412630w_2 + 342318641365 \end{aligned}$$

に関する離散対数

$$m = 113621283281226371392249533867737215949797543810 2$$

が $\mathbf{Jac}_C(k_2)$ で保存されることを見る。

以降では、$\mathbf{Jac}_C$ の元は Mumford 表現を用いて表現されていることに注意されたい。

$\delta \in k_{12}$ を $f$ の根とする。このとき、補題 4.4 から $\mathrm{N}_{k_{12}/k_6}(\delta - B) \in k_2$ を満足する $B$ が

$$\begin{aligned} B &= (101648944861w_2 + 120556554953)w_4 \\ &\quad +583174529096w_2 + 817810031436 \end{aligned}$$

と求まる。ここで、

$$\mathrm{N}_{k_{12}/k_6}(\delta - B) = 253347179597w_2 + 921896027794$$

である。また、$\mathrm{N}_{k_4/k_2}A = \mathrm{N}_{k_{12}/k_6}(\delta - B)$ を満足する $A$ が

$$A = (45957271749w_2 + 782860143746)w_4$$

と計算される。以上から式 (4) で定義された $F$ が以下で得られる。

$$\begin{aligned}
F(x) &= f(Ax+B) = f_3x^3+f_2x^2+f_1x+f_0\\
f_0 &= (421959795543w_2+963459810790)w_4\\
&\quad +160664071863w_2+584860541020\\
f_1 &= (362452213480w_2+267260686737)w_4\\
&\quad +236832125718w_2+195395175747\\
f_2 &= (485197838509w_2+311648591036)w_4\\
&\quad +189134940001w_2+22525966308\\
f_3 &= (199493764869w_2+334874746536)w_4
\end{aligned}$$

この $F$ は $S_F = S_F^{-p^2}$ を満足する。$f_0/f_3 = \eta+\theta w_4,\quad (\eta,\theta\in k_2)$ と置く。$S_F = S_F^{-p^2}$ より $\mathrm{N}_{k_4/k_2}(\eta+\theta w_4) = \eta^2-\theta^2w_4^2 = 1$ が成り立つ。また、

$$\begin{aligned}
\alpha_1 &= -\theta w_4^2+(\eta-1)w_4\\
&= (129199088229w_2+591281372544)w_4\\
&\quad +361658692699w_2+870974870617
\end{aligned}$$

と置くと、$\alpha_1^{p^2}/\alpha_1 = \eta+\theta w_4$ が成り立ち、従って、

$$\begin{aligned}
r &= f_3/\alpha_1\\
&= (65304165587w_2+784860577952)w_4\\
&\quad +432829062269w_2+897714516139\\
\beta_1 &= f_2/r\\
&= (936494890610w_2+111201003029)w_4\\
&\quad +972810577860w_2+408884372077
\end{aligned}$$

と順に置くと、$F(x) = r(\alpha_1x^3+\beta_1x^2+\beta_1^{q^2}x+\alpha_1^{q^2})$ を得る。この $F$ から補題 3.2 を用いて回文形式

$$\begin{aligned}
E_N : y^2 &= \alpha x^3+\beta x^2+\beta^{q^2}x+\alpha^{q^2}\\
\alpha &= (466343339604w_2+161750065456)w_4\\
&\quad +4183637413w_2+140045024888\\
\beta &= (702699675927w_2+797891202670)w_4\\
&\quad +236832125718w_2+195395175747
\end{aligned}$$

を得る。また、$P$, $Q$ は $E$ から $E_N$ への写像 $[x,y]\to[u^2(x-B)/A, -uy]$, $(u = r^{(-p^2+1)/2})$ でそれぞれ

$$\begin{aligned}
P_N &= ((1026198339885w_2+622054511877)w_4\\
&\quad +965716986883w_2+175034817821,\\
&\quad (1054404722659w_2+808531732609)w_4\\
&\quad +177343228221w_2+689845800924)\\
Q_N &= ((1013457255238w_2+635696622283)w_4\\
&\quad +43128785303w_2+975234248539,\\
&\quad (659699726602w_2+989595947969)w_4\\
&\quad +734878177854w_2+518709355081)
\end{aligned}$$

に写される。この $P_N$, $Q_N$ が $Q_N = [m]P_N$ を満足することは、簡単に確認される。

上記 $\alpha$, $\beta$ を用いて、式 (1) で定義された genus 2 の超楕円曲線 $C$ が下式で直ちに与えられる。

$$\begin{aligned}
C : y^2 &= \alpha(x-w_4)^6+\beta(x-w_4)^4(x-w_4^{q^2})^2\\
&\quad +\beta^{q^2}(x-w_4)^2(x-w_4^{q^2})^4\\
&\quad +\alpha^{q^2}(x-w_4^{q^2})^6 \in k_2[x]
\end{aligned}$$

また、$P_N$, $Q_N$ は式 (2) で与えられた $h$ を用いて以下のように $\mathbf{Jac}_C(k_4)$ に写される。

$$\begin{aligned}
h(P_N) &= (\nu_P(x),\omega_P(x)) \in \mathbf{Jac}_C(k_4),\\
h(Q_N) &= (\nu_Q(x),\omega_Q(x)) \in \mathbf{Jac}_C(k_4)
\end{aligned}$$

ここで、

$$\begin{aligned}
\nu_P &= x^2+((765281714270w_2+155009478785)w_4\\
&\quad +107776055490w_2+120797279935)x\\
&\quad +362398684834w_2+599175059576,\\
\omega_P &= ((528286298588w_2+1012295684893)w_4\\
&\quad +467771408273w_2+361856605123)x\\
&\quad +(635420074360w_2+932405568036)w_4\\
&\quad +61690796195w_2+987490679453,\\
\nu_Q &= x^2+((320197624936w_2+423097463820)w_4\\
&\quad +188194602926w_2+708719777488)x\\
&\quad +362398684834w_2+599175059576,\\
\omega_Q &= ((906341208601w_2+506741645177)w_4\\
&\quad +706483696179w_2+1021648490723)x\\
&\quad +(622451845238w_2+498339241990)w_4\\
&\quad +786508327564w_2+19689717291
\end{aligned}$$

である。これらを式 (3) で与えられた T によって $\mathbf{Jac}_C(k_2)$ に写像し、

$$\begin{aligned}
P_J = \mathrm{T}\circ h(P_N) &= (\nu_{P_J}(x),\omega_{P_J}(x)) \in \mathbf{Jac}_C(k_2),\\
Q_J = \mathrm{T}\circ h(Q_N) &= (\nu_{Q_J}(x),\omega_{Q_J}(x)) \in \mathbf{Jac}_C(k_2)
\end{aligned}$$

を得る。ここで、

$$\begin{aligned}
\nu_{P_J} &= x^2+(530325203389w_2+52918280646)x\\
&\quad +799424110003w_2+985712352828,\\
\omega_{P_J} &= (687709924521w_2+726803053772)x\\
&\quad +207266484953w_2+557513628060,\\
\nu_{Q_J} &= x^2+(202922060979w_2+200883060101)x\\
&\quad +674539377451w_2+936808994813,\\
\omega_{Q_J} &= (979403069297w_2+315201256271)x\\
&\quad +613304483883w_2+70549896070
\end{aligned}$$

である。この $P_J$, $Q_J$ に対し、$Q_J = [m]P_J$ の成立を確認した。更に、これらの $P_J$, $Q_J$ は $k$ 上の genus 9 の $C_{ab}$ 曲線の Jacobian 群に埋め込まれる。これについては、[4, 例 2] を参照されたい。尚、本例の作成には Magma を使用した。

## 参考文献


[1] S. Arita, Gaudry's variant against $C_{ab}$ curves, IEICE Trans. Found., E83-A (2000), 1809-1814.

[2] S. Arita, Weil descent of elliptic curves over finite fields of characteristic three, ASIACRYPT 2000, LNCS 1976, pp.248-258, Kyoto, 2000.

[3] 有田正剛、偶数次拡大体上の種数 2 超楕円曲線に対する Weil descent attack について, Technical Report of IEICE, Vol.102, No.323, pp.39–46, 2002/9.

[4] 有田正剛、4 次拡大体上の楕円曲線暗号に対する Weil descent attack について II, Proc. of SCIS2004, IEICE Japan, 2004.

[5] C. Diem, The GHS-attack in odd characteristic, preprint, 2001. Available from `http://www.exp-math.uni-essen.de/diem/english.html`.

[6] G.Frey, How to disguise an elliptic curve, Talk at Waterloo workshop on the ECDLP, `http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`, 1998.

[7] S.D.Galbraith, Weil Descent of Jacobians, preprint at the University of Bristol, 2000.

[8] P.Gaudry, An algorithm for solving the discrete logarithm problem on hyperelliptic curves, EUROCRYPT 2000, Springer-Verlag LNCS 1807, 2000, 19-34.

[9] P.Gaudry, F.Hess, and N.P.Smart, Constructive and destructive facets of Weil descent on elliptic curves, to apper in J. Cryptology.

[10] D. Mumford, Tata lectures on theta II, Progress in Mathematics, no. 43, Birkhäuser, 1984.

[11] S. Paulus and A. Stein, Computing real and imaginary arithmetics for divisor class groups of hyperelliptic curves, ANTS-III, LNCS 1423, Springer-Verlag, 1998, pp. 576–591.

[12] N. Thériault, Index calculus attack for hyperelliptic curves of small genus, ASIACRYPT2003, LNCS 2894, Springer-Verlag, 2003, pp. 75–92.

[13] J.W.S Cassels, E.V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, Cambridge 1996.