Weil Descent of Elliptic Curves over Finite Fields of Characteristic Three

Seigo Arita

NEC, Kawasaki Kanagawa, Japan
arita@ccm.cl.nec.co.jp

Abstract. The paper shows that some of elliptic curves over finite fields of characteristic three of composite degree are attacked by a more effective algorithm than Pollard's ρ method. For such an elliptic curve E, we construct a C_{ab} curve D on its Weil restriction in order to reduce the discrete logarithm problem on E to that on D. And we show that the genus of D is small enough so that D is attacked by a modified form of Gaudry's variant for a suitable E. We also see such a weak elliptic curve is easily constructed.

1 Introduction

An elliptic curve cryptosystem(ECC) is a discrete-logarithm-based public key cryptosystem using the Jacobian group of an elliptic curve[9,12]. In ECC, we must be careful to choose an elliptic curve. Many classes of week elliptic curves have been found since ECC was presented [11,4,19,15,18,16,14].

Recently, Gaudry, Hess and Smart[7] found new week elliptic curves. They show that some of elliptic curves over finite fields of characteristic two of composite degree are attacked by a more effective algorithm than Pollard's ρ method. They construct a hyperelliptic curve H on the Weil restriction of such an elliptic curve E, and show that the discrete logarithm problem(DLP) on E is reduced to that on H. Moreover they observe that for some such E, the genus of the corresponding H becomes small enough for the DLP on H to be attacked by Gaudry's variant [6].

This paper treats elliptic curves over finite fields of characteristic *three* of composite degree, and shows some of such elliptic curves are also attacked by a more effective algorithm than Pollard's ρ method.

We construct a C_{ab} curve [13,3] D on the Weil restriction of an elliptic curve E over a finite field of characteristic three of composite degree, and reduce the discrete logarithm problem(DLP) on E to that on D. Moreover, we clarify the condition for an elliptic curve E to correspond to a C_{ab} curve D of small genus, as well as the method to construct such E. Since Gaudry's variant is also effective for C_{ab} curves with a slight modification [2], this means that some of elliptic curves of characteristic three of composite degree are also attacked by a more effective algorithm than Pollard's ρ method, and that we can construct such weak elliptic curves effectively.

T. Okamoto (Ed.): ASIACRYPT 2000, LNCS 1976, pp. 248–258, 2000.

2 Computation of Weil Descent

We treat Weil descent of an elliptic curve E_a

$$Y^2 + Y = X^3 + aYX \tag{1}$$

defined over a finite field $\mathbb{F}_{q^n}$ of characteristic three. Here, for $q = 3^d$, we assume

$$\gcd(d, n) = 1. \tag{2}$$

Note E_a is not supersingular for nonzero a (Theorem 4.1. on [17]).

Let $\Omega = \{\omega, \omega^3, \cdots, \omega^{3^{n-1}}\}$ be a normal basis for $\mathbb{F}_{3^n} \mid \mathbb{F}_3$. By the condition (2), Ω is a basis also for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Substituting $Y = y_0\omega + y_1\omega^3 + \cdots + y_{n-1}\omega^{3^{n-1}}, X = x_0\omega + x_1\omega^3 + \cdots + x_{n-1}\omega^{3^{n-1}}$ for the defining equation (1) of E_a, and comparing coefficients of ω^i, we get n equations among $2n$ variables $\{y_0, \ldots, y_{n-1}, x_0, \ldots, x_{n-1}\}$. An abelian variety $A_a = \prod_{\mathbb{F}_{q^n}|\mathbb{F}_q} E_a$ defined by these n equations is called Weil restriction of E_a [5]. Moreover, taking an intersection of A_a and $(n-1)$ hyperplanes $y_0 = y_i (i = 1, \ldots, n-1)$, we get an algebraic curve C_a. C_a is an algebraic curve defined by n equations in $(n+1)$-dimensional affine space.

For an element $a \in \mathbb{F}_{q^n}$, let $A(a) \in M_n(\mathbb{F}_q)$ be a regular representation of a with respect to Ω :

$$a \cdot [\omega, \omega^3, \cdots, \omega^{3^{n-1}}] = [\omega, \omega^3, \cdots, \omega^{3^{n-1}}] \cdot A(a).$$

Using $A := A(a)$, the defining equations for C_a are given by

$$C_a : \begin{cases} x_{n-1}^3 - c_1 y(A_{11}x_0 + A_{12}x_1 + \cdots + A_{1n}x_{n-1}) = -c_1 y^2 + y \\ x_0^3 - c_1 y(A_{21}x_0 + A_{22}x_1 + \cdots + A_{2n}x_{n-1}) = -c_1 y^2 + y \\ \cdots \\ x_{n-2}^3 - c_1 y(A_{n1}x_0 + A_{n2}x_1 + \cdots + A_{nn}x_{n-1}) = -c_1 y^2 + y \end{cases} \tag{3}$$

Here, we put $y = y_i (i = 0, \ldots, n-1)$, and let the minimal polynomial of ω be $T^n + c_1 T^{n-1} + \cdots c_n$.

Putting

$$\boldsymbol{x} = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}, \quad \boldsymbol{e} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

(P is a matrix for a cyclic permutation), Equations (3) become

$$P\boldsymbol{x}^3 - c_1 yA\boldsymbol{x} = (-c_1 y^2 + y)\boldsymbol{e}. \tag{4}$$

Here, $\boldsymbol{x}^3$ denotes an vector gotten by cubing every components of $\boldsymbol{x}$.

Regular representations $A(a)$ $(a \in \boldsymbol{F}_{q^n})$ are diagonalized simultaneously using a matrix T with the eigenvectors for the Frobenius automorphism $x \mapsto x^q$ as columns:

$$T^{-1}A(a)T = D(a^{(0)}, a^{(1)}, \cdots, a^{(n-1)}), \tag{5}$$

where $D(a, b, \ldots, z)$ denotes a diagonal matrix with $a, b, \ldots, z$ as diagonal elements, and $a^{(0)}, a^{(1)}, \cdots, a^{(n-1)}$ $(a^{(i)} := a^{q^i})$ is a whole of elements conjugate to a in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Putting

$$\boldsymbol{x} = T\boldsymbol{w}, \tag{6}$$

equation (4) becomes

$$T^{-1}PT^{(3)}\boldsymbol{w}^3 - c_1 y D(a^{(0)}, a^{(1)}, \cdots, a^{(n-1)})\boldsymbol{w} = (-c_1 y^2 + y)T^{-1}\boldsymbol{e}, \tag{7}$$

where $T^{(3)}$ denotes a matrix gotten by cubing every elements of T.

Lemma 1. *$T^{-1}PT^{(3)}$ is a diagonal matrix over $\mathbb{F}_{q^n}$.*

Proof. For any element $a \in \mathbb{F}_{q^n}$, by the definition of A,

$$a \cdot [\omega, \omega^3, \cdots, \omega^{3^{n-1}}] = [\omega, \omega^3, \cdots, \omega^{3^{n-1}}] \cdot A(a).$$

Cubing two sides,

$$a^3 \cdot [\omega^3, \omega^9, \cdots, \omega] = [\omega^3, \omega^9, \cdots, \omega] \cdot A(a)^{(3)}.$$

The left-hand side is equal to $a^3 \cdot [\omega, \omega^3, \cdots, \omega^{3^{n-1}}]P = [\omega, \omega^3, \cdots, \omega^{3^{n-1}}]A(a)^3 P$, and the right-hand side is $[\omega, \omega^3, \cdots, \omega^{3^{n-1}}]PA(a)^{(3)}$. So, we get

$$A(a)^3 = PA(a)^{(3)}P^{-1}.$$

Therefore we have

$$T^{-1}A(a)^3 T = T^{-1}PA(a)^{(3)}P^{-1}T = T^{-1}PT^{(3)} \cdot T^{(3)^{-1}}A(a)^{(3)}T^{(3)} \cdot T^{(3)^{-1}}P^{-1}T.$$

Thus, for any $a \in \boldsymbol{F}_{q^n}$,

$$T^{-1}A(a)^3 T \cdot T^{-1}PT^{(3)} = T^{-1}PT^{(3)} \cdot T^{(3)^{-1}}A(a)^{(3)}T^{(3)}.$$

However, $T^{-1}A(a)^3 T = T^{(3)^{-1}}A(a)^{(3)}T^{(3)} = D(a^{(1)^3}, \cdots, a^{(n-1)^3})$. So, $T^{-1}PT^{(3)}$ must be a diagonal matrix. □

In equation (7), putting

$$D(b_0, \cdots, b_{n-1}) = T^{-1}PT^{(3)} \quad (b_i \in \mathbb{F}_{q^n}) \tag{8}$$

$$\boldsymbol{d} = T^{-1}\boldsymbol{e}, \tag{9}$$

we get defining equations of C_a over $\mathbb{F}_{q^n}$:

$$w_i^3 - b_i^{-1}c_1 a^{(i)} y w_i = b_i^{-1}d_i(-c_1 y^2 + y) \quad (i = 0, 1, \ldots, n-1). \tag{10}$$

We note that b_i, c_1, d_i are determined only by n and d, independent from $a \in \mathbb{F}_{q^n}$.

Example: d=5,n=4

Let $d = 5,\ n = 4$. Let κ be a root of the irreducible polynomial $T^5+T^4+T^3+T^2-T+1$ over $\mathbb{F}_3$. κ is a primitive element of $\mathbb{F}_q$. Let ω be a root of the irreducible polynomial $T^4 - T^3 + T^2 + T - 1$ over $\mathbb{F}_3$(i.e. $c_1 = -1$). $\Omega = \{\omega, \omega^3, \omega^{3^2}, \omega^{3^3}\}$ is a normal basis of $\mathbb{F}_{3^n}$ over $\mathbb{F}_3$. Since d and n are prime to each other, Ω is a basis also for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

For

$$a = \kappa^{216}\omega^3 + \kappa^{95}\omega^2 + \kappa^{95}\omega, \tag{11}$$

defining equations of C_a over $\mathbb{F}_{q^n}$ are given by

$$\begin{cases} w_0^3 + (\kappa^{86}\omega^3 + \kappa^{168}\omega^2 + \kappa^{200}\omega + \kappa^{62})yw_0 = (\kappa^{162}\omega^3 + \kappa^{239}\omega^2 + \omega + \kappa^{19})(y^2 + y) \\ w_1^3 + (\kappa^{181}\omega^3 + \kappa^{207}\omega^2 + \kappa^{168}\omega + \kappa^{182})yw_1 = (\kappa^{142}\omega^3 + \kappa^{41}\omega^2 + \kappa^{239}\omega + \kappa^{238})(y^2 + y) \\ w_2^3 + (\kappa^{79}\omega^3 + \kappa^{60}\omega^2 + \kappa^{207}\omega + \kappa^{85})yw_2 = (\kappa^{121}\omega^3 + \kappa^{21}\omega^2 + \kappa^{41}\omega + \kappa^{201})(y^2 + y) \\ w_3^3 + (\kappa^{47}\omega^3 + \kappa^{200}\omega^2 + \kappa^{60}\omega + \kappa^{8})yw_3 = (\kappa^{118}\omega^3 + \omega^2 + \kappa^{21}\omega + \kappa^{220})(y^2 + y) \end{cases}$$

3 A Component D_a of the Curve C_a

We show that the curve C_a has a component D_a with small genus for a suitable $a \in \mathbb{F}_{q^n}$. We use notations in section 2.

Lemma 2. *For an element h in a function field of C_a over $\mathbb{F}_{q^n}$, let h^q denote the image of h by the Frobenius automorphism with respect to q (i.e. the generator of the Galois group* $\mathrm{Gal}(\mathbb{F}_{q^n}(y, x_0, \dots, x_{n-1}) \mid \mathbb{F}_q(y, x_0, \dots, x_{n-1})) \simeq \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ *). We have*

$$\begin{array}{l} w_0^q = w_1, w_1^q = w_2, \cdots, w_{n-1}^q = w_0 \\ a^{(0)q} = a^{(1)}, a^{(1)q} = a^{(2)}, \cdots, a^{(n-1)q} = a^{(0)} \\ b_0^q = b_1, b_1^q = b_2, \cdots, b_{n-1}^q = b_0 \\ d_0^q = d_1, d_1^q = d_2, \cdots, d_{n-1}^q = d_0 \end{array}$$

Proof. As $a^{(i)} = a^{q^i}$, claims for a_i are obvious. In equation (5), the i-th column of the matrix T is gotten by taking q-th power of every elements of the $(i-1)$-th column of T. So, the i-th row of the matrix T^{-1} is gotten by taking q-th power of every elements of the $(i-1)$-th row of T^{-1}. From this, we obtain claims for w_i and d_i. Claims for b_i are also gotten from equation (8) □

Putting

$$\alpha_i = -b_i^{-1}c_1a^{(i)}, \quad \beta_i = b_i^{-1}d_i, \quad f = -c_1y^2 + y \quad (i = 0, 1, \dots, n-1), \tag{12}$$

defining equations (10) become

$$w_i^3 + \alpha_i y w_i = \beta_i f \quad (i = 0, 1, \dots, n-1). \tag{13}$$

By Lemma 2, we have

$$\begin{array}{l} \alpha_0^q = \alpha_1, \alpha_1^q = \alpha_2, \dots, \alpha_{n-1}^q = \alpha_0, \\ \beta_0^q = \beta_1, \beta_1^q = \beta_2, \dots, \beta_{n-1}^q = \beta_0. \end{array} \tag{14}$$

For defining equations (13), put $F_0 = \mathbb{F}_{q^n}(y, w_0)$, $F_1 = \mathbb{F}_{q^n}(y, w_0, w_1)$, $\cdots$, $F = F_{n-1} = \mathbb{F}_{q^n}(y, w_0, w_1, \cdots, w_{n-1})$. F is a function field of C_a over $\mathbb{F}_{q^n}$. Put

$$I_i = \{\gamma \in \mathbb{F}_{q^n} \mid \gamma f = \delta^3 + \alpha_i y\delta \quad (\exists \delta \in F_{i-1})\} \quad (i = 1, \ldots, n-1). \tag{15}$$

I_i is a vector space over $\mathbb{F}_3$.

Proposition 1. *For $i = 1, \ldots, n-1$, put $J_i = \langle \alpha_0^{\frac{3}{2}(q^i-1)}\beta_0, \ \ldots, \ \alpha_{i-1}^{\frac{3}{2}(q-1)}\beta_{i-1}\rangle_{\mathbb{F}_3}$. Then we have $I_i \supseteq J_i \quad (i = 1, \ldots, n-1)$. Here, for i and j with $j < i$, $\alpha_i^{\frac{3}{2}(q^{i-j}-1)}\beta_j \in I_i$ corresponds to $\delta = \alpha_i^{\frac{1}{2}(q^{i-j}-1)}w_j$(see equation (15)).*

Proof. Let $i > j$. For $\gamma = (\frac{\alpha_i}{\alpha_j})^{\frac{1}{2}} = \alpha_j^{\frac{1}{2}(q^{i-j}-1)}$, we have

$$\begin{aligned}(\gamma w_j)^3 + \alpha_i y(\gamma w_j) &= \gamma^3(w_j^3 + \tfrac{\alpha_i}{\gamma^2} y w_j) \\ &= \alpha_j^{\frac{3}{2}(q^{i-j}-1)}(w_j^3 + \alpha_j y w_j) \\ &= \alpha_j^{\frac{3}{2}(q^{i-j}-1)}\beta_j f.\end{aligned}$$

So, $\alpha_j^{\frac{3}{2}(q^{i-j}-1)}\beta_j \in I_i$. □

Theorem 1. *If $\beta_i \in J_i$ holds for some i, then C_a has a component*

$$D_a : \begin{cases} w_0^3 + \alpha_0 y w_0 = \beta_0(-c_1 y^2 + y) \\ \cdots \\ w_{i-1}^3 + \alpha_{i-1} y w_{i-1} = \beta_{i-1}(-c_1 y^2 + y) \\ w_i = \delta_i \\ \cdots \\ w_{n-1} = \delta_{n-1} \end{cases}$$

($\exists \delta_i, \ldots, \delta_{n-1} \in F_{i-1}$).

Proof. Suppose $\beta_i \in J_i$ holds for some i. For j with $j \geq i$, we have $\beta_j = \beta_i^{q^{j-i}} \in J_i^{q^{j-i}} \subset J_j$ by (14). So, by Proposition 1, $\beta_j \in I_j \quad (\forall j \geq i)$. Then, by the definition of I_j, this means that the equation $w_j^3 + \alpha_j y w_j = \beta_j f \quad (j \geq i)$ for w_j has a root $w_j = \delta_j$ already in F_{i-1}. □

From Theorem 1, we see that C_a has a component D_a of the smaller genus if we choose $a \in \mathbb{F}_{q^n}$ such that $\beta_i \in J_i$ holds for the smaller i.

Proposition 2. *Suppose n is a multiple of 4. Let $\omega \in \mathbb{F}_{q^n}$ be a root of the irreducible polynomial $T^4 - T^3 + T^2 + T - 1$ over $\mathbb{F}_3$, and γ be any $(q-1)/2$-th root of unity in $\mathbb{F}_q$, and δ be a root of $\delta^{\frac{3}{2}(q-1)} = \omega - \omega^3 - \omega^9$ in $\mathbb{F}_{q^n}$(the root exists since the order of the right-hand side is a divisor of $2(q^n-1)/(q-1)$). Then for $a = -b_0 c_1^{-1}\beta_0^{\frac{2}{3}}\gamma\delta$, we have $\beta_2 \in J_2$.*

Proof. By equation (12), we have $\alpha_0 = -b_0^{-1} c_1 a$. We will find α_0 such that

$$\beta_2 = \alpha_0^{\frac{3}{2}(q^2-1)} \beta_0 + \alpha_1^{\frac{3}{2}(q-1)} \beta_1. \tag{16}$$

By (14), we see $\beta_2 = \beta_0^{q^2}, \beta_1 = \beta_0^q, \alpha_1 = \alpha_0^q$. So, equation (16) becomes

$$\beta_0^{q^2} = \alpha_0^{\frac{3}{2}(q^2-1)} \beta_0 + \alpha_0^{\frac{3}{2}(q^2-q)} \beta_0^q.$$

Putting $\epsilon = \beta_0^{-\frac{2}{3}}, \quad \delta = \epsilon \alpha_0$, this becomes

$$\delta^{\frac{3}{2}(q^2-1)} + \delta^{\frac{3}{2}(q^2-q)} = 1.$$

Moreover, putting $z = \delta^{\frac{3}{2}(q-1)}$, this is

$$z^q + z^{q+1} = 1. \tag{17}$$

By condition (2), the extension $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ and the extension $\mathbb{F}_{3^n} \mid \mathbb{F}_3$ has the isomorphic Galois group. So, Frobenius automorphism $x \mapsto x^q$ in $\mathbb{F}_{q^n}$ becomes $x \mapsto x^3$ when restricted to $\mathbb{F}_{3^n}$. Therefore, equation (17) becomes $z^4 + z^3 = 1$ over $\mathbb{F}_{3^n}$. This has a root in $\mathbb{F}_{3^n}$ when n is a multiple of 4. For example, with ω as above, we can take $z = \omega - \omega^3 - \omega^9$ $\square$

Example: d=5,n=4

Let $d = 5,\ n = 4$. We constructed a in equation (11) using Proposition 2. In fact, for a in equation (11), C_a has a component

$$D_a : \begin{cases} w_0^3 + (\kappa^{86}\omega^3 + \kappa^{168}\omega^2 + \kappa^{200}\omega + \kappa^{62}) y w_0 = (\kappa^{162}\omega^3 + \kappa^{239}\omega^2 + \omega + \kappa^{19})(y^2 + y) \\ w_1^3 + (\kappa^{181}\omega^3 + \kappa^{207}\omega^2 + \kappa^{168}\omega + \kappa^{182}) y w_1 = (\kappa^{142}\omega^3 + \kappa^{41}\omega^2 + \kappa^{239}\omega + \kappa^{238})(y^2 + y) \\ w_2 = (\kappa^{198}\omega^3 + \kappa^{50}\omega^2 + \kappa^{186}\omega + \kappa^{223}) w_0 + (\kappa^{128}\omega^3 + \kappa^{163}\omega^2 + \kappa^{135}\omega + \kappa^{223}) w_1 \\ w_3 = (\kappa^{168}\omega^3 + \kappa^{184}\omega^2 + \kappa^{95}\omega + \kappa^{179}) w_0 + (\kappa^{184}\omega^3 + \kappa^{198}\omega^2 + \kappa^{171}\omega + \kappa^{199}) w_1 \end{cases}. \tag{18}$$

4 C_{ab} Model of the Component D_a

In this section, we assume that the curve C_a has the following form of component D_a (see Proposition 2):

$$D_a : \begin{cases} w_0^3 + \alpha_0 y w_0 = \beta_0(-c_1 y^2 + y) \\ w_1^3 + \alpha_1 y w_1 = \beta_1(-c_1 y^2 + y) \\ w_2 = \gamma_2 \\ \cdots \\ w_{n-1} = \gamma_{n-1} \end{cases}, \tag{19}$$

where, $\gamma_2, \ldots, \gamma_{n-1} \in F_1 = \mathbb{F}_{q^n}(y, w_0, w_1)$. D_a has a unique point P_∞ at infinity as a space curve in the space of y, w_0, w_1. In this section, we construct a nonsingular model of the component D_a by a C_{ab} curve [13,3] over $\mathbb{F}_q$, and determines its genus. In the below, we call a model by a C_{ab} curve just as C_{ab} model.

Because D_a has a singular point (at the origin), we need some tasks to construct its nonsingular C_{ab} model. Theoretically, by computing the integral closure $\tilde{R}$ of the coordinate ring R of D_a using the algorithm of Jong [8] and by determining functions in $\tilde{R}$ with small pole numbers at P_∞, we can construct a nonsingular C_{ab} model of D_a using those functions [10]. However, we do the task more directly and easily as seen in Algorithm 1.

Let $v_{P_\infty}(h)$ denote an order of a function h on D_a at the point P_∞. Since P_∞ is totally ramified over $\mathbb{F}_{q^n}(y, w_0)$, we see $v_{P_\infty}(y) = -9,\ v_{P_\infty}(w_0) = -6,\ v_{P_\infty}(w_1) = -6$. Comparing the values of w_0 and w_1 at P_∞, we get $v_{P_\infty}(\beta_1^{\frac{1}{3}} w_0 - \beta_0^{\frac{1}{3}} w_1) = -m,\quad m < 6$.

By Lemma[Determination of defining equations](p1410) in [13], we can construct a singular $C_{m,6,9}$ model of D_a over $\mathbb{F}_{q^n}$ using three functions $\beta_1^{\frac{1}{3}} w_0 - \beta_0^{\frac{1}{3}} w_1$, w_0, and y. In order to get a singular $C_{m,6,9}$ model R of D_a over $\mathbb{F}_q$, we can use three functions

$$s := \mathrm{Tr}(\beta_1^{\frac{1}{3}} w_0 - \beta_0^{\frac{1}{3}} w_1),\ t := \mathrm{Tr}(w_0),\ w := y, \tag{20}$$

where, Tr is a trace of an extension

$$\mathbb{F}_{q^n}(y, w_0, \ldots, w_{n-1}) = \mathbb{F}_{q^n}(y, x_0, \ldots, x_{n-1}) \ \mid\ \mathbb{F}_q(y, x_0, \ldots, x_{n-1}).$$

Note $Tr(w_0) = w_0 + w_1 + \cdots + w_{n-1}$ by Lemma 2.

We normalize the singular C_{ab} model R as follows:

Algorithm 1 (Normalization of a singular C_{ab} model)
Input: $R = \mathbb{F}_q[x_1, \ldots, x_n]/I$*:* $C_{a_1,\ldots,a_n}$ *model*
Output: its normalization R

$J \leftarrow$ *the radical of the ideal of singular points in* R
WHILE $J \neq (1)$ **DO**
  $y \in \mathrm{Hom}_R(J, J) \setminus R$
  $n \leftarrow n + 1$
  $x_n \leftarrow y$
  $a_n \leftarrow -v_{P_\infty}(y)$
  $R \leftarrow \mathbb{F}_q[x_1, \ldots, x_n]/I$; $C_{a_1,\ldots,a_n}$ *model constructed by* $x_1, \ldots, x_n$
  $J \leftarrow$ *the radical of the ideal of singular points in* R

For the method for computation of $\mathrm{Hom}_R(J, J)$ $(\subset \tilde{R})$, see [20] Section 2.2.

Example: d=5,n=4

Let $d = 5,\ n = 4$. For $a = \kappa^{216}\omega^3 + \kappa^{95}\omega^2 + \kappa^{95}\omega$, the component D_a was given by equation (18). In this case, functions s, t, w in (20) are calculated as

$$\begin{cases} s = (\kappa^6\omega^3 + \kappa^{49}\omega^2 + \kappa^{100}\omega + \kappa^{71})w_0 + (\kappa^{190}\omega^3 + \kappa^5\omega^2 + \kappa^{89}\omega + \kappa^{192})w_1 \\ t = (\kappa^{151}\omega^3 + \kappa^{200}\omega^2 + \kappa^{195}\omega + \kappa^{66})w_0 + (\kappa^{53}\omega^3 + \kappa^{113}\omega^2 + \kappa^{221}\omega + \kappa^{35})w_1 \\ w = y \end{cases}.$$

First, assuming $m = 5$, we construct a $C_{5,6,9}$ model of D_a using functions s, t, w (If $m < 5$ in fact, then we would fail in constructing the $C_{5,6,9}$ model and we would know it) :

$$\begin{cases} \kappa^{88}sw + \kappa^{60}s^3 + tw = 0 \\ w + \kappa^{176}sw + \kappa^{64}s^3 + \kappa^{22}t^3 + w^2 = 0 \\ \kappa^{159}s^3 + \kappa^{131}s^4 + \kappa^{42}s^3t + \kappa^{88}st^3 + \kappa^{159}s^3w + t^4 = 0 \end{cases}.$$

This model has a single singular point at the origin, and the radical J of its ideal is (w, t, s). Calculating $\mathrm{Hom}(J, J)$, we get $x := (w^2 + w)/s \in \tilde{R} \setminus R$. Since $v_{P_\infty}(x) = -13$, now we can construct a $C_{5,6,9,13}$ model of D_a using s, t, w, and x:

$$\begin{cases} \kappa^{88}sw + \kappa^{60}s^3 + tw = 0 \\ \kappa^{154}sw + \kappa^{42}s^3 + \kappa^{220}sx + t^3 = 0 \\ w - sx + w^2 = 0 \\ \kappa^{60}s^2 + \kappa^{88}sx + \kappa^{60}s^2w + tx = 0 \\ \kappa^{55}w + \kappa^{176}sx + \kappa s^2w + \kappa^{137}s^4 + \kappa^{170}s^3t + \kappa^{203}s^2t^2 + wx = 0 \\ \kappa^{110}w + \kappa^{137}s^3 + \kappa^{170}s^2t + \kappa^{203}st^2 + \kappa^{231}sx + \kappa^{56}s^2w + \kappa^{192}s^4 + \kappa^{225}s^3t \\ \quad + \kappa^{16}s^2t^2 + \kappa s^2x + \kappa^{230}s^5 + \kappa^{142}s^4t + x^2 = 0 \end{cases}.$$

This model also has a single singular point at the origin, and the radical J of its ideal is (s, t, w, x). Calculating $\mathrm{Hom}(J, J)$, we get $u := (\kappa^{13}stw + \kappa^{13}st)/x, v := (\kappa^{170}stw + \kappa^{203}t^2w + \kappa^{170}st + \kappa^{203}t^2)/x \in \tilde{R} \setminus R$. Since $v_{P_\infty}(u) = -7, v_{P_\infty}(v) = -8$, now we can construct a $C_{5,6,7,8,9}$ model of D_a using s, t, u, v, w :

$$\begin{cases} w^2 + s^2v + \kappa^{198}s^2t + \kappa^{64}s^3 + \kappa^{176}sw + w = 0 \\ vw + \kappa^8s^2u + \kappa^{170}s^2t = 0 \\ uw + \kappa^{134}s^2t = 0 \\ v^2 + \kappa^{142}s^2t + \kappa^{230}s^3 + \kappa^{137}sw + \kappa sv + \kappa^{110}su + \kappa^{166}st + \kappa^{230}s^2 + \kappa^{129}u + \kappa^{49}t + \kappa^{16}s = 0 \\ uv + \kappa^{194}s^3 + \kappa^{222}sw + \kappa^8sv + \kappa^{95}su + \kappa^{189}st + \kappa^{13}t = 0 \\ tw + \kappa^{60}s^3 + \kappa^{88}sw = 0 \\ u^2 + \kappa^{65}sw + \kappa^{93}sv + \kappa^{129}su + \kappa^{190}st + \kappa^{37}s^2 + \kappa^{65}s = 0 \\ tv + \kappa^{181}sw + \kappa^{88}sv + \kappa^{124}su + \kappa^{64}st + \kappa^{153}s^2 + \kappa^{181}s = 0 \\ tu + \kappa^{173}sv + \kappa^{209}su = 0 \\ t^2 + \kappa^{47}su + \kappa^{88}st = 0 \end{cases}. \tag{21}$$

This is a nonsingular C_{ab} model.

Thus, for $a = \kappa^{216}\omega^3 + \kappa^{95}\omega^2 + \kappa^{95}\omega$, we succeeded in constructing a nonsingular C_{ab} model (21) of D_a. Since the gap sequence at P_∞ of (21) is (1,2,3,4), we know its genus is four.

5 The Reduction

We constructed the C_{ab} curve D_a of genus 4 over $\mathbb{F}_q$ on the Weil restriction $A_a = \prod_{\mathbb{F}_{q^n}|\mathbb{F}_q} E_a$ for the value of a given by Proposition 2. Tracing the route, we can construct the morphism Φ from D_a to A_a over $\mathbb{F}_q$ easily. From the definition of Weil restriction, the morphism Φ is also the morphism from D_a to E_a over $\mathbb{F}_{q^n}$. So, Φ induces the morphism Φ^* between jacobians over $\mathbb{F}_{q^n}$;

$$\Phi^* : E_a(\mathbb{F}_{q^n}) \to J_{D_a}(\mathbb{F}_{q^n}).$$

By taking a composition with the norm map, we get the morphism Ψ from $E_a(\mathbb{F}_{q^n})$ to $J_{D_a}(\mathbb{F}_q)$;

$$\Psi = \mathrm{Norm}_{\mathbb{F}_{q^n}|\mathbb{F}_q} \circ \Phi^* : E_a(\mathbb{F}_{q^n}) \to J_{D_a}(\mathbb{F}_q),$$

which reduces DLP on $E_a(\mathbb{F}_{q^n})$ to DLP on $J_{D_a}(\mathbb{F}_q)$. Since the genus of D_a is 4, Gaudry's variant against $J_{D_a}(\mathbb{F}_q)$ is more effective than Pollard's ρ method against $E_a(\mathbb{F}_{q^n})$ [7,2].

Example: d=5,n=4

Let $d = 5,\ n = 4$. For $a = \kappa^{216}\omega^3 + \kappa^{95}\omega^2 + \kappa^{95}\omega$, we constructed a nonsingular C_{ab} model (21) of D_a. The morphism Φ from (the C_{ab} model of) D_a to A_a is given by

$$\Phi\colon \begin{array}{ccc} D_a & \longrightarrow & A_a, \\ (s,t,u,v,w) & \mapsto & (\kappa^{55}s + \kappa^{209}t, \kappa^{223}s + \kappa^{209}t, \kappa^{193}s + \kappa^{209}t, \kappa^{55}s + \kappa^{209}t, w, w, w, w). \end{array}$$

As the morphism from D_a to E_a, Φ can be written as

$$\Phi : \begin{array}{ccc} D_a & \longrightarrow & E_a, \\ (s,t,u,v,w) & \mapsto & ((\kappa^{81}\omega^3 + \kappa^{202}\omega^2 + \kappa^{193})s + \kappa^{209}t, w). \end{array}$$

For example, take a point $P_1 = (\kappa^4\omega^3 + \kappa^{225}\omega^2 + \kappa^{42}\omega + \kappa^{187}, \kappa^{187}\omega^3 + \kappa^{94}\omega^2 + \kappa^{197}\omega + \kappa^{239})$ of the prime order 78427 on E_a. Then P_1 is pulled back to $J_{D_a}(\mathbb{F}_{q^n})$ by Φ (In the below, an element in the jacobian of D_a is expressed by a Gröebner basis w.r.t. $C_{5,6,7,8,9}$ order of the corresponding ideal ([1])) ;

$$\begin{aligned}
&\Phi^*(P_1) \\
&= (\quad u^2 + (\kappa^{231}\omega^3 + \kappa^{107}\omega^2 + \kappa^{70}\omega + \kappa^2)u + (\kappa^{194}\omega^3 + \kappa^{204}\omega^2 + \kappa^{12}\omega + \kappa^{229})s \\
&\qquad + \kappa^{205}\omega^3 + \kappa^{43}\omega^2 + \kappa^{203}\omega + \kappa^{118}, \\
&\qquad su + (\kappa^4\omega^3 + \kappa^{66}\omega^2 + \kappa^{229}\omega + \kappa^{34})u + (\kappa^{201}\omega^3 + \kappa^{228}\omega^2 + \kappa^{236}\omega + \kappa^{221})s \\
&\qquad + \kappa^7\omega^3 + \kappa^{87}\omega^2 + \kappa^{78}\omega + \kappa^{55}, \\
&\qquad s^2 + (\kappa^{62}\omega^3 + \kappa^{190}\omega^2 + \kappa^{33}\omega + \kappa^{64})u + (\kappa^{125}\omega^3 + \kappa^{187}\omega^2 + \kappa^{108}\omega + \kappa^{155})s \\
&\qquad + \kappa^{70}\omega^3 + \kappa^{40}\omega^2 + \kappa^{163}\omega + \kappa^{191}, \\
&\qquad w + \kappa^{66}\omega^3 + \kappa^{215}\omega^2 + \kappa^{76}\omega + \kappa^{118}, \\
&\qquad v + (\kappa^{183}\omega^3 + \kappa^{62}\omega^2 + \kappa^{183})u + (\kappa^{208}\omega^3 + \kappa^{72}\omega^2 + \kappa^{69}\omega + \kappa^{88})s + \kappa^{168}\omega^3 \\
&\qquad + \kappa^{86}\omega^2 + \kappa^{202}\omega + \kappa^{36}, \\
&\qquad t + (\kappa^{114}\omega^3 + \kappa^{235}\omega^2 + \kappa^{226})s + \kappa^{158}\omega^3 + \kappa^{137}\omega^2 + \kappa^{196}\omega + \kappa^{99} \quad).
\end{aligned}$$

By taking its norm to $\mathbb{F}_q$-coefficients, we get the element j_1 in $J_{D_a}(\mathbb{F}_q)$ corresponding to P_1;

$$\begin{aligned}
j_1 = \ & \Psi(P_1) \\
= \ & \mathrm{Norm}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\Phi^*(P_1)) \\
= (\ & u^2 + \kappa^{230}u + \kappa^7 t + \kappa^{45}s + \kappa^{11}, \\
& tu + \kappa^{106}u + \kappa^{203}t + \kappa^{194}s + \kappa^{227}, \\
& su + \kappa^{50}u + \kappa^{98}t + \kappa^{8}s + \kappa^{154}, \\
& t^2 + \kappa^{119}u + \kappa^{95}t + \kappa^{90}s + \kappa^{100}, \\
& st + \kappa^{111}u + \kappa^{13}t + \kappa^{38}s + \kappa^{70}, \\
& s^2 + \kappa^{13}u + \kappa^{76}t + \kappa^{6}s + \kappa^{132}, \\
& w + \kappa^{125}u + \kappa^{193}t + \kappa^{192}s + \kappa^{188}, \\
& v + \kappa^{131}u + \kappa^{135}t + \kappa^{30}s + \kappa^{56} \ ).
\end{aligned}$$

Similarly, for the point $P_2 = 45821 \cdot P_1 = (\kappa^{188}\omega^3 + \kappa^{141}\omega^2 + \kappa^{10}\omega + \kappa^{238}, \kappa^{34}\omega^3 + \kappa^{186}\omega^2 + \kappa^{234}\omega + \kappa^{82})$, we have

$$\begin{aligned}
j_2 = \ & \Psi(P_2) \\
= (\ & u^2 + \kappa^{118}u + \kappa^{150}t + \kappa^{127}s + \kappa^{130}, \\
& tu + \kappa^{208}u + \kappa^{31}t + \kappa^{145}s + \kappa^{118}, \\
& su + \kappa^{192}u + \kappa^{42}t + \kappa^{27}s + \kappa^{134}, \\
& t^2 + \kappa^{217}u + \kappa^{17}t + \kappa^{136}s + \kappa^{12}, \\
& st + \kappa^{231}u + \kappa^{168}t + \kappa^{144}s + \kappa^{6}, \\
& s^2 + \kappa^{229}u + \kappa^{70}t + \kappa^{132}s + \kappa^{26}, \\
& w + \kappa^{234}u + \kappa^{185}t + \kappa^{157}s + \kappa^{106}, \\
& v + \kappa^{215}u + \kappa^{119}t + \kappa^{142}s + \kappa^{37} \ ).
\end{aligned}$$

We verified that j_2 is actually equal to $45821 \cdot j_1$, using the addition algorithm in the jacobian of C_{ab} curve [1].

6 The Cryptographic Implications

We saw an example of an elliptic curve E_a over a finite field of characteristics 3, DLP on which is reduced to DLP on C_{ab} curve D_a of genus 4, and is attacked by Gaudry's variant effectively than by Pollard's ρ method. The values of a giving such week elliptic curves E_a are obtained by Proposition 2. Proportion of such values of a is small. So, a randomly generated E_a is safe.

However, consider the following scenario. First we construct such a weak elliptic curve E_a by Proposition 2. Then, we apply some isogeny against E_a to get a new elliptic curve E'. In the almost case, E' itself cannot be attacked by Weil descent technique. However, since we know the isogeny, we can reduce DLP on E' to DLP on E_a, and so we can solve DLP on E' more effectively than the others without the knowledge of the isogeny.

It seems difficult to check whether the given elliptic curve is obtained as the image of some isogeny of such a week E_a, or not.

References

1. S. Arita, “Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log-based public key cryptosystems,” Conference on The Mathematics of Public Key Cryptography, Toronto, 1999.
2. S. Arita, “Gaudry’s variant against C_{ab} curve,” LNCS 1751, Proceedings of PKC 2000, pp. 58-67, Melbourne, 2000.
3. S. Arita, “Construction of Secure C_{ab} Curves Using Modular Curves,” ANTS VI, pp.113–126, Leiden, 2000.
4. G.Frey and H.-G.Rück, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”, Mathematics of Computation, 62 (1994), 865-874.
5. S. Galbraith and N. Smart, “A Cryptographic Application of Weil Descent,” HP Labs Tech. Report, HPL-1999-70 .
6. P.Gaudry, “A variant of the Adleman-DeMarris-Huang algorithm and its application to small genera,” Conference on The Mathematics of Public Key Cryptography, Toronto, 1999.
7. P. Gaudry, F. Hess and N. Smart, “Constructive and destructive facets of Weil descent on elliptic curves,” HP Labs Tech. Report, HPL-2000-10.
8. T. de Jong, “An algorithm for computing integral closure,” J. Symbolic Comp., vol. 26, no.3, pp. 36-47, 1998.
9. N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, 48(1987), pp. 203-209.
10. R. Matsumoto, “Constructing Algebraic Geometry Codes on the Normalization of a Singular C_{ab} Curve,” Trans. of IEICE, vol. E82-A, no. 9, 1981-1985, Sep. 1999.
11. A.Menezes, T.Okamoto, and S.Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field”, Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 80-89, 1991.
12. V.S. Miller, “Use of elliptic curves in cryptography,” CRYPTO ’85(LNCS 218), pp. 417-426, 1986.
13. S. Miura, “Linear Codes on Affine Algebraic Curves”, Trans. of IEICE, vol. J81-A, no. 10, 1398-1421, Oct. 1998.
14. H.-G.Rück, “On the discrete logarithm in the divisor class group of curves,” Math. Comp.,68(226),pp.805-806,1999.
15. T.Satoh, K.Araki, “Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves”, COMMENTARII MATHEMATICI UNIVERSITATIS SANCTI PAULI, vol. 47, No. 1, 81-92, 1998.
16. I.A.Semaev, “Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p,” Math. Comp. 67, pp. 353-356, 1998.
17. J.H.Silverman, “The Arithmetic of Elliptic Curves”, Springer-Verlag, 1986.
18. P.N.Smart, “The discrete logarithm problem on elliptic curves of trace one,” J. Cryptology 12, 193-196 (1999).
19. S. Uchiyama, T. Saitoh “A Note on the Discrete Logarithm Problem on Elliptic Curves of Trace Two,” Proc. of the 1998 Engineering Sciences Society Conference of IEICE, pp. 231-232.
20. W. V. Vasconcelos, “Computational Methods in Commutative Algebra and Algebraic Geometry”, Springer, 1998.