On Implementation of GHS Attack against Elliptic Curve Cryptosystems over Cubic Extension Fields of Odd Characteristics

Naoki Hashizume * Fumiyuki Momose † Jinhui Chao ‡

May 15, 2008

Abstract

In this paper, we present algorithms for implementation of the GHS attack to Elliptic curve cryptosystems (ECC). In particular, we consider two large classes of elliptic curves over cubic extension fields of odd characteristics which have weak covering curves against GHS attack, whose existence have been shown recently [16][17][18]. We show an algorithm to find definition equation of the covering curve and an algorithm to transfer DLP of the elliptic curve to Jacobian of the covering curve. An algorithm to test if the covering curve is hyperelliptic is also shown in the appendix.

keywords Elliptic curve cryptosystems, Discrete logarithm problem, GHS attack

1 Introduction

Elliptic curve cryptosystems (ECC) are known as one of the most secure cryptosystems. In particular, it has the same level of security as RSA and ElGamal cryptosystems by using much shorter key length. This is also desirable in implementation of compact and low cost cryptosystems. Against algebraic curve based cryptosystems, square root attacks are known such as the baby-step giant-step attack, Pollard's rho and lambda algorithms. Recently, index calculus attacks have been proposed for hyperelliptic curves

*Graduate School of Science and Engineering, Course of Information and System Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

†Department of Mathematics, Faculty of Science and Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

‡Department of Information and System Engineering, Faculty of Science and Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

of genera larger than 3 by Gaudry, Nagao, Gaudry-Theriault-Thome-Diem[1],[2],[3]and non-hyperelliptic curves of geneus larger than or equal to 3 by Diem[4].

A relatively new attack called GHS attack, which is based on the idea of Weil descent suggested by Frey[5], was proposed by Gaudry, Hess, and Smart in 2000 [6]. The GHS attack transfer the discrete logarithm problem (DLP) in the group of rational points of an elliptic curve E over an extension k_d of a finite field k to the DLP in the Jacobian variety of a new curve C of higher genus over the smaller definition field k.

The GHS attack has been already under extensive research. However, although theoretically interesting, its analysis seemed nontrivial[7],[8],[9],[10],[11],[12],[13],[14],[15]. The classes of the weak elliptic curves or curves for which the GHS attack efficiently works have not been fully understand, Besides, it seemed that the class of curves subjected to the GHS attack must be of special properties therefore the number of such curves will not be very large. Recently it is shown explicitly the existence of certain large classes of elliptic and hyperelliptic curves which are weak against GHS[16],[17],[18].

As we know that in modern cryptography, the most efficient and reliable approach for security analysis of a particular cryptosystem is, particularly if the security is not theoretically provable, to apply every possible attack to it in order to find its weak points. Only systems which have resisted all such attacks can be trusted in practical usage. Thus it is important and interesting to implement GHS attack to these weak curves.

A GHS attack consists of three parts: to find the curve C/k from E/k_d; to transfer the discrete logarithm on E/k_d to the Jacobian $J(C)/k$; then apply an index calculus algorithm to solve the discret logarithm in $J(C)/k$. As to the first part, it seemed to be nontrival to find the definition equation of a weak curve E/k_d. For the second parts, although a general strategy using norm-conorm map is well known, efficient and explict implementation algorithm seemed still unavailable and also nontrivial.

In this paper we show explicit procedures for the first two parts of GHS attack against two large classes of the elliptic curves over cubic extension fields of odd characteristics. These two classes, called Type I and Type II curves have been obtained in [16][17][18], both of them have non-hyperelliptic covering curves of genus three, which are subjected to the Diem's double-large-prime attack. We show an algorithm to explicitly construct these covering curve over k from the elliptic curves over the cubic extension of k with odd characteristics. Then an algorithm is shown to map the rational point on the elliptic curve to the divisor of the covering curve, in order to transfer the DLP. In appendex, we also show an algorithm to test if a Type I or II curve is hyperellipic. These algorithms are implemented and examples are shown.

2 Weak Covering C over k_3, char$k \neq 2$

Let $k = \mathbb{F}_q$ be a finite field of odd characteristic, and $k_d = \mathbb{F}_{q^d}$.

We consider the GHS attack against an algebraic curve C_0/k_d with genus $g_0 = g(C_0)$. A special case is when $g_0 = 1$ and $C_0 = E/k_d$ is an elliptic curve.

Assume that there exists an algebraic curve C/k such that

$$\pi/k_d : C \longrightarrow C_0 \tag{1}$$

is a covering defined over k_d, which induces the map

$$\pi_*/k_d : \mathrm{Jac}(C) \longrightarrow \mathrm{Jac}(C_0). \tag{2}$$

Assume the restriction of π_* onto k

$$\mathrm{Re}(\pi_*)/k : \mathrm{Jac}(C) \longrightarrow \mathrm{Re}_{k_d/k}(\mathrm{Jac}(C_0)) \tag{3}$$

defines an isogeny over k. Then C has genus $g(C) = dg_0$. Here, $\mathrm{Re}_{k_d/k}(\mathrm{Jac}(C_0))$ is the Weil restriction of $\mathrm{Jac}(C_0)$ with respect to extension field k_d/k.

Assume $g_0 = 1,\ d = 3,\ \mathrm{char}(k) \neq 2$.

According to [16][17][18], the elliptic curves C_0 which have weak covering C as genus three nonhyperelliptic curves can be divided into two types.

$$\begin{aligned} C_0/k_3: &\quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q) && (4)\\ \text{Type I}: &\quad \alpha,\ \beta \in k_3\backslash k,\ \#\{\alpha,\ \alpha^q, \beta,\ \beta^q\} = 4 && (5)\\ \text{Type II}: &\quad \alpha \in k_6\backslash(k_2 \cup k_3),\ \beta = \alpha^{q^3} && (6) \end{aligned}$$

These elliptic curves can be transformed to the following Legandre canonical forms:

- Type I:

$$C_0/k_3:\ y^2 = x(x-1)(x-\lambda),\ \lambda = \frac{(\beta-\alpha^q)(\beta^q-\alpha)}{(\beta-\alpha)(\beta^q-\alpha^q)} \tag{7}$$

- Type II:

$$C_0/k_3:\ y^2 = \mathrm{N}_{k_6/k_3}(\beta-\alpha^q)x(x-1)(x-\lambda),\ \lambda = \mathrm{N}_{k_6/k_3}\left(\frac{\alpha^q-\alpha}{\alpha^q-\beta}\right) \tag{8}$$

And $\#\{\lambda\} \approx \frac{1}{2}q^3$.

The discrete logarithm on C_0/k_3 has a complexity of $\tilde{O}(q^{4/3})$ against the Pollard's rho method. On the other hand, apply Diem's algorithm to nonhyperellitic C, the complexity of discrete logarithm reduces to $\tilde{O}(q)$.

In particular, define

$$\begin{aligned} \mu &:= \begin{pmatrix} \alpha^q & -\alpha \\ 1 & -1 \end{pmatrix} \lambda && (9)\\ A &:= \begin{pmatrix} -\mu+\alpha+\alpha^q & -\alpha^{1+q} \\ 1 & -\mu \end{pmatrix} && (10)\\ B &:= {}^{\sigma^2}\!A\ {}^{\sigma}\!A\ A. && (11) \end{aligned}$$

According to Lemma 3, 1,2 [16], the neccesary and sufficient condition for C_0 to be Type I is that the quadratic equation

$$B \cdot \beta = \beta \tag{12}$$

has a solution β.

Besides, the covering curve C of such a curve C_0 is hyperelliptic if and only if

$$\beta = A \cdot \alpha, \ ^{\exists}A \in \mathrm{GL}_2(k), \ \mathrm{Tr}A = 0. \tag{13}$$

Here $A \cdot \alpha$ denotes a PGL_2 action:

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad A \cdot \alpha := \frac{a\alpha + b}{c\alpha + d} \tag{14}$$

Hereafter we assume that α and β do not satisfy the condition (13). Then, the curve C is a nonhyperelliptic curve over k of genus three. We show in the appendix an algorithm to test if C is hyperelliptic.

In this paper, we show following two algorithms:

(i) how to construst the curve C/k, or to find the definition equation explicitly from the given curve C_0/k_d.

(ii) how to transfer from the DLP over C_0/k_d to the DLP over $J(C/k)$.

3 How to construct C/k from C_0/k_d

Assume C is a nonhyperelliptic curve of genus $dg_0 = 3$. Thus, its canonical embedding is a quartic curve in $\mathbb{P}^2$. Let σ be a qth power Frobenius map and σ satisfies

$$l(x) = \sum_{i=1}^{n} a_i x^i \quad \longmapsto \quad {}^{\sigma}l(x) = \sum_{i=1}^{n} {a_i}^q x^i \qquad ({}^{\forall}l(x) \in k_d[x]). \tag{15}$$

The embedding map is

$$C \quad \hookrightarrow \quad \mathbb{P}^2 \tag{16}$$

$$P \quad \longmapsto \quad \Big(\omega(P) : \ {}^{\sigma}\omega(P) : \ {}^{\sigma^2}\omega(P)\Big) \tag{17}$$

where $\omega = \frac{\mathrm{d}x}{y}$ and its conjugates generate the first cohomology group

$$H^0(C/k_3, \Omega^1) = \langle \omega, \ \ {}^{\sigma}\omega, \ \ {}^{\sigma^2}\omega \rangle. \tag{18}$$

We use hereafter the correspondence

$$\omega \longleftrightarrow X, \qquad {}^{\sigma}\omega \longleftrightarrow Y, \qquad {}^{\sigma^2}\omega \longleftrightarrow Z. \tag{19}$$

The Galois action on $H^0(C/k_3, \Omega^1)$ is a cyclic shift.

Now we consider the automorphism group of the first coholomogy group

$$Aut(H^0(C/k_3, \Omega^1)) = \{id, \ \phi, \ {}^{\sigma}\phi, \ {}^{\sigma^2}\phi\}. \tag{20}$$

The idenfity on $H^0(C/k_3, \Omega^1)$ is

$$id : \begin{cases} X & \longmapsto & X \\ Y & \longmapsto & Y \\ Z & \longmapsto & Z \end{cases} . \tag{21}$$

The bi-elliptic involution is to change the signs of both Y and Z

$$\phi : \begin{cases} X & \mapsto & X \\ Y & \longmapsto & -Y \\ Z & \longmapsto & -Z \end{cases} . \tag{22}$$

Then the bi-elliptic involusion under Galois action has the following form.

$$^{\sigma}\phi : \begin{cases} X & \longmapsto & -X \\ Y & \longmapsto & Y \\ Z & \longmapsto & -Z \end{cases} \tag{23}$$

The bi-elliptic involusion under action of σ^2 has the following form.

$$^{\sigma^2}\phi : \begin{cases} X & \longmapsto & -X \\ Y & \longmapsto & -Y \\ Z & \longmapsto & Z \end{cases} \tag{24}$$

3.1 Definition equation of C/k_3

The quartic curve C/k_3 has its definition equation invariant under $\mathrm{Gal}(k_3/k)$, thus in the following symmetric form.

$$\begin{aligned} C/k_3 \quad : \quad & aX^4 + a^qY^4 + a^{q^2}Z^4 \\ & +bX^3Y + b^qY^3Z + b^{q^2}Z^3X \\ & +cX^3Z + c^qY^3X + c^{q^2}Z^3Y \\ & +dX^2Y^2 + d^qY^2Z^2 + d^{q^2}Z^2X^2 \\ & +eX^2YZ + e^qXY^2Z + e^{q^2}XYZ^2 = 0. \end{aligned} \tag{25}$$

Since the definition equation of C is invarinat under the action of automorphisms of $\mathrm{Aut}(H^0(C, \Omega^1))$,

$$C = C + \phi(C) + {}^{\sigma}\phi(C) + {}^{\sigma^2}\phi(C).$$

On the other hand, since ϕ, ${}^{\sigma}\phi$, ${}^{\sigma^2}\phi$ change the signs of two variables, the terms with odd degrees of variables are cancelled each other.

Thus the equation of the curve C/k_3 is in the following form.

$$C/k_3 : \quad aX^4 + a^qY^4 + a^{q^2}Z^4 + bX^2Y^2 + b^qY^2Z^2 + b^{q^2}Z^2X^2 = 0. \qquad a, b \in k_3 \tag{26}$$

3.2 Evaluation of a and b

To find the coefficients a and b in (26), we subsitute into it $X = \frac{\mathrm{d}x}{y},\ Y = \frac{\mathrm{d}x}{{}^{\sigma}y},\ Z = \frac{\mathrm{d}x}{{}^{\sigma^2}y}$.

Since

$$\frac{1}{y^2} = \frac{(x-\alpha^{q^2})(x-\beta^{q^2})}{\mathrm{N}_{k_3/k}((x-\alpha)(x-\beta))},$$

$$\frac{1}{({}^{\sigma}y)^2} = \frac{(x-\alpha)(x-\beta)}{\mathrm{N}_{k_3/k}((x-\alpha)(x-\beta))},$$

we substitute these into (26) to obtain

$$\mathrm{Tr}_{k_3/k}(a(x-\alpha^{q^2})^2(x-\beta^{q^2})^2) + \mathrm{Tr}_{k_3/k}(b(x-\alpha)(x-\alpha^{q^2})(x-\beta)(x-\beta^{q^2})) = 0. \tag{27}$$

3.2.1 Type I

From expansion of (27) we can express the coefficients of each x^i as

$$x^4:\ \mathrm{Tr}(a)+\mathrm{Tr}(b) \tag{28}$$
$$x^3:\ -2\mathrm{Tr}(a(\alpha^{q^2}+\beta^{q^2})) - \mathrm{Tr}(b(\alpha+\beta+\alpha^{q^2}+\beta^{q^2})) \tag{29}$$
$$x^2:\ \mathrm{Tr}(a(\alpha^{2q^2}+4\alpha^{q^2}\beta^{q^2}+\beta^{2q^2})) + \mathrm{Tr}(b\{\alpha^{q^2+1}+(\alpha+\alpha^{q^2})(\beta+\beta^{q^2})+\beta^{q^2+1}\}) \tag{30}$$
$$x:\ -2\mathrm{Tr}(a(\alpha^{2q^2}\beta^{q^2}+\alpha^{q^2}\beta^{2q^2})) - \mathrm{Tr}(b\{\alpha^{q^2+1}(\beta+\beta^{q^2})+\beta^{q^2+1}(\alpha+\alpha^{q^2})\}) \tag{31}$$
$$1:\ \mathrm{Tr}(a\alpha^{2q^2}\beta^{2q^2}) + \mathrm{Tr}(b\alpha^{q^2+1}\beta^{q^2+1}) \tag{32}$$

which are identically zeros.

In order to calculate a, b explicitly, we express $a, b \in k_3$ on a k-basis of k_3.

$$a = a_0 + a_1\epsilon + a_2\epsilon^2\ (a_0,\ a_1,\ a_2 \in k) \tag{33}$$
$$b = b_0 + b_1\epsilon + b_2\epsilon^2\ (b_0,\ b_1,\ b_2 \in k) \tag{34}$$

where ϵ generates $k_3 = k(\epsilon)$.

Belows, we express the coefficients of x^i in (27) in terms of a_i, b_i.

First, in the coefficient of x^4, $\mathrm{Tr}(a)$ is given by

$$\mathrm{Tr}(a) = 3a_0 + \mathrm{Tr}(\epsilon)a_1 + \mathrm{Tr}(\epsilon^2)a_2. \tag{35}$$

Similarly,

$$\mathrm{Tr}(b) = 3b_0 + \mathrm{Tr}(\epsilon)b_1 + \mathrm{Tr}(\epsilon^2)b_2. \tag{36}$$

Next, in the coefficient of x^3, $\mathrm{Tr}(a(\alpha^{q^2}+\beta^{q^2}))$ is given by

$$\begin{aligned}
& \mathrm{Tr}(a(\alpha^{q^2}+\beta^{q^2})) \\
= & (\alpha^{q^2}+\beta^{q^2})(a_0+a_1\epsilon+a_2\epsilon^2) \\
& +(\alpha+\beta)(a_0+a_1\epsilon^q+a_2\epsilon^{2q})+(\alpha^q+\beta^q)(a_0+a_1\epsilon^{q^2}+a_2\epsilon^{2q^2}) \\
= & \mathrm{Tr}(\alpha+\beta)a_0+\mathrm{Tr}((\alpha+\beta)\epsilon^q)a_1+\mathrm{Tr}((\alpha+\beta)\epsilon^{2q})a_2. \qquad (37)
\end{aligned}$$

$\mathrm{Tr}(b(\alpha+\beta+\alpha^{q^2}+\beta^{q^2}))$ is given by

$$\begin{aligned}
& \mathrm{Tr}(b(\alpha+\beta+\alpha^{q^2}+\beta^{q^2})) \qquad (38) \\
= & (\alpha+\beta+\alpha^{q^2}+\beta^{q^2})(b_0+b_1\epsilon+b_2\epsilon^2)+(\alpha^q+\beta^q+\alpha+\beta)(b_0+b_1\epsilon^q+b_2\epsilon^{2q}) \\
& +(\alpha^{q^2}+\beta^{q^2}+\alpha^q+\beta^q)(b_0+b_1\epsilon^{q^2}+b_2\epsilon^{2q^2}) \\
= & \mathrm{Tr}(\alpha^q+\beta^q+\alpha+\beta)b_0+\mathrm{Tr}((\alpha^q+\beta^q+\alpha+\beta)\epsilon^q)b_1+\mathrm{Tr}((\alpha^q+\beta^q+\alpha+\beta)\epsilon^{2q})b_2.
\end{aligned}$$

In the coefficient of x^2, $\mathrm{Tr}(a(\alpha^{2q^2}+4\alpha^{q^2}\beta^{q^2}+\beta^{2q^2}))$ is given by

$$\begin{aligned}
& \mathrm{Tr}(a(\alpha^{2q^2}+4\alpha^{q^2}\beta^{q^2}+\beta^{2q^2})) \\
= & \mathrm{Tr}(\alpha^2+4\alpha\beta+\beta^2)a_0+\mathrm{Tr}((\alpha^2+4\alpha\beta+\beta^2)\epsilon^q)a_1+\mathrm{Tr}((\alpha^2+4\alpha\beta+\beta^2)\epsilon^{2q})a_2 \qquad (39)
\end{aligned}$$

and $\mathrm{Tr}(b\{\alpha^{q^2+1}+(\alpha+\alpha^{q^2})(\beta+\beta^{q^2})+\beta^{q^2+1}\})$ is given by

$$\begin{aligned}
& \mathrm{Tr}(b\{\alpha^{q^2+1}+(\alpha+\alpha^{q^2})(\beta+\beta^{q^2})+\beta^{q^2+1}\}) \\
= & \mathrm{Tr}(\alpha^{q+1}+(\alpha^q+\alpha)(\beta^q+\beta)+\beta^{q+1})b_0+\mathrm{Tr}(\{\alpha^{q+1}+(\alpha^q+\alpha)(\beta^q+\beta)+\beta^{q+1}\}\epsilon^q)b_1 \\
& +\mathrm{Tr}(\{\alpha^{q+1}+(\alpha^q+\alpha)(\beta^q+\beta)+\beta^{q+1}\}\epsilon^{2q})b_2. \qquad (40)
\end{aligned}$$

In the coefficient of x, $\mathrm{Tr}(a(\alpha^{2q^2}\beta^{q^2}+\alpha^{q^2}\beta^{2q^2}))$ is given by

$$\begin{aligned}
& \mathrm{Tr}(a(\alpha^{2q^2}\beta^{q^2}+\alpha^{q^2}\beta^{2q^2})) \\
& =\mathrm{Tr}(\alpha^2\beta+\alpha\beta^2)a_0+\mathrm{Tr}((\alpha^2\beta+\alpha\beta^2)\epsilon^q)a_1+\mathrm{Tr}((\alpha^2\beta+\alpha\beta^2)\epsilon^{2q})a_2. \qquad (41)
\end{aligned}$$

and $\mathrm{Tr}(b\{\alpha^{q^2+1}(\beta+\beta^{q^2})+\beta^{q^2+1}(\alpha+\alpha^{q^2})\})$ is given by

$$\begin{aligned}
& \mathrm{Tr}(b\{\alpha^{q^2+1}(\beta+\beta^{q^2})+\beta^{q^2+1}(\alpha+\alpha^{q^2})\}) \\
& =\mathrm{Tr}(\alpha^q\beta^q(\alpha+\beta)+\alpha\beta(\alpha^q+\beta^q))b_0+\mathrm{Tr}(\{\alpha^q\beta^q(\alpha+\beta)+\alpha\beta(\alpha^q+\beta^q)\}\epsilon^q)b_1 \\
& +\mathrm{Tr}(\{\alpha^q\beta^q(\alpha+\beta)+\alpha\beta(\alpha^q+\beta^q)\}\epsilon^{2q})b_2. \qquad (42)
\end{aligned}$$

In the constant term of (27), $\mathrm{Tr}(a\alpha^{2q^2}\beta^{2q^2})$ is given by

$$\mathrm{Tr}(a\alpha^{2q^2}\beta^{2q^2}) = \mathrm{Tr}(\alpha^2\beta^2)a_0+\mathrm{Tr}(\alpha^2\beta^2\epsilon^q)a_1+\mathrm{Tr}(\alpha^2\beta^2\epsilon^{2q})a_2. \qquad (43)$$

and $\mathrm{Tr}(b\alpha^{q^2+1}\beta^{q^2+1})$ is given by

$$\mathrm{Tr}(b\alpha^{q^2+1}\beta^{q^2+1}) = \mathrm{Tr}(\alpha^{q+1}\beta^{q+1})b_0+\mathrm{Tr}(\alpha^{q+1}\beta^{q+1}\epsilon^q)b_1+\mathrm{Tr}(\alpha^{q+1}\beta^{q+1}\epsilon^{2q})b_2. \qquad (44)$$

Combining the above equations yields the following system of simultaneous linear equations.

$$\begin{cases}
3a_0 + \mathrm{Tr}(\epsilon)a_1 + \mathrm{Tr}(\epsilon^2)a_2 + 3b_0 + \mathrm{Tr}(\epsilon)b_1 + \mathrm{Tr}(\epsilon^2)b_2 = 0 \\
\\
2\mathrm{Tr}(\alpha+\beta)a_0 + 2\mathrm{Tr}((\alpha+\beta)\epsilon^q)a_1 + 2\mathrm{Tr}((\alpha+\beta)\epsilon^{2q})a_2 \\
+\mathrm{Tr}(\alpha^q+\beta^q+\alpha+\beta)b_0 + \mathrm{Tr}((\alpha^q+\beta^q+\alpha+\beta)\epsilon^q)b_1 + \mathrm{Tr}((\alpha^q+\beta^q+\alpha+\beta)\epsilon^{2q})b_2 = 0 \\
\\
\mathrm{Tr}(\alpha^2+4\alpha\beta+\beta^2)a_0 + \mathrm{Tr}((\alpha^2+4\alpha\beta+\beta^2)\epsilon^q)a_1 + \mathrm{Tr}((\alpha^2+4\alpha\beta+\beta^2)\epsilon^{2q})a_2 \\
+\mathrm{Tr}(\alpha^{q+1}+(\alpha^q+\alpha)(\beta^q+\beta)+\beta^{q+1})b_0 + \mathrm{Tr}(\{\alpha^{q+1}+(\alpha^q+\alpha)(\beta^q+\beta)+\beta^{q+1}\}\epsilon^q)b_1 \\
+\mathrm{Tr}(\{\alpha^{q+1}+(\alpha^q+\alpha)(\beta^q+\beta)+\beta^{q+1}\}\epsilon^{2q})b_2 = 0 \\
\\
2\mathrm{Tr}(\alpha^2\beta+\alpha\beta^2)a_0 + 2\mathrm{Tr}((\alpha^2\beta+\alpha\beta^2)\epsilon^q)a_1 + 2\mathrm{Tr}((\alpha^2\beta+\alpha\beta^2)\epsilon^{2q})a_2 \\
+\mathrm{Tr}(\alpha^q\beta^q(\alpha+\beta)+\alpha\beta(\alpha^q+\beta^q))b_0 + \mathrm{Tr}(\{\alpha^q\beta^q(\alpha+\beta)+\alpha\beta(\alpha^q+\beta^q)\}\epsilon^q)b_1 \\
+\mathrm{Tr}(\{\alpha^q\beta^q(\alpha+\beta)+\alpha\beta(\alpha^q+\beta^q)\}\epsilon^{2q})b_2 = 0 \\
\\
\mathrm{Tr}(\alpha^2\beta^2)a_0 + \mathrm{Tr}(\alpha^2\beta^2\epsilon^q)a_1 + \mathrm{Tr}(\alpha^2\beta^2\epsilon^{2q})a_2 \\
+\mathrm{Tr}(\alpha^{q+1}\beta^{q+1})b_0 + \mathrm{Tr}(\alpha^{q+1}\beta^{q+1}\epsilon^q)b_1 + \mathrm{Tr}(\alpha^{q+1}\beta^{q+1}\epsilon^{2q})b_2 = 0
\end{cases}$$

From the equation (26), we can assume $a_0 = 1$. Accordingly, the above simultaneous linear equations can be written as

$$\begin{pmatrix} d_{11} & d_{12} & d_{13} & d_{14} & d_{15} \\ d_{21} & d_{22} & d_{23} & d_{24} & d_{25} \\ d_{31} & d_{32} & d_{33} & d_{34} & d_{35} \\ d_{41} & d_{42} & d_{43} & d_{44} & d_{45} \\ d_{51} & d_{52} & d_{53} & d_{54} & d_{55} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ b_0 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{pmatrix}. \tag{45}$$

where d_{ij} are the coefficients of $a_1,\ a_2,\ b_0,\ b_1,\ b_2$ in each equation. e_i the negations of the coefficients of a_0.

Thus $a_1,\ a_2,\ b_0,\ b_1,\ b_2$ can be obtained by solution of the above linear equation given α, β and ϵ.

3.2.2 Type II

For Type II curves, the equation (27) have coefficents of x^i as follows.

First, the coefficient of x^4 is

$$\mathrm{Tr}(a) + \mathrm{Tr}(b) = 3a_0 + \mathrm{Tr}(\epsilon)a_1 + \mathrm{Tr}(\epsilon^2)a_2 + 3b_0 + \mathrm{Tr}(\epsilon)b_1 + \mathrm{Tr}(\epsilon^2)b_2 = 0. \tag{46}$$

Next, the coefficent of x^3 is as follows:

$$\begin{aligned}
& 2\mathrm{Tr}(a(\alpha^{q^2}+\beta^{q^2}))+\mathrm{Tr}(b(\alpha+\beta+\alpha^{q^2}+\beta^{q^2})) \\
= & \ 2\mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha))a_0+2\mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\epsilon^q)a_1+2\mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\epsilon^{2q})a_2 \\
+ & \ \mathrm{Tr}(\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q+\mathrm{Tr}_{k_6/k_3}(\alpha))b_0+\mathrm{Tr}(\left[\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q+\mathrm{Tr}_{k_6/k_3}(\alpha)\right]\epsilon^q)b_1 \\
+ & \ \mathrm{Tr}(\left[\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q+\mathrm{Tr}_{k_6/k_3}(\alpha)\right]\epsilon^{2q})b_2 \\
= & \ 0.
\end{aligned} \tag{47}$$

The coefficient of x^2 is

$$\begin{aligned}
& \mathrm{Tr}(a(\alpha^{2q^2}+4\alpha^{q^2}\beta^{q^2}+\beta^{2q^2}))+\mathrm{Tr}(b\{\alpha^{q^2+1}+(\alpha+\alpha^{q^2})(\beta+\beta^{q^2})+\beta^{q^2+1}\}) \\
= & \ \mathrm{Tr}(\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^2+2\mathrm{N}_{k_6/k_3}(\alpha))a_0+\mathrm{Tr}(\left[\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^2+2\mathrm{N}_{k_6/k_3}(\alpha)\right]\epsilon^q)a_1 \\
& +\mathrm{Tr}(\left[\mathrm{Tr}_{k_6/k_3}(\alpha)^2+2\mathrm{N}_{k_6/k_3}(\alpha)\right]\epsilon^{2q})a_2 \\
& +\mathrm{Tr}(\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^{q+1}+\{\mathrm{N}_{k_6/k_3}(\alpha)\}^q+\mathrm{N}_{k_6/k_3}(\alpha))b_0 \\
& +\mathrm{Tr}(\left[\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^{q+1}+\{\mathrm{N}_{k_6/k_3}(\alpha)\}^q+\mathrm{N}_{k_6/k_3}(\alpha)\right]\epsilon^q)b_1 \\
& +\mathrm{Tr}(\left[\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^{q+1}+\{\mathrm{N}_{k_6/k_3}(\alpha)\}^q+\mathrm{N}_{k_6/k_3}(\alpha)\right]\epsilon^{2q})b_2 \\
= & \ 0.
\end{aligned} \tag{48}$$

The coefficient of x is

$$\begin{aligned}
& 2\mathrm{Tr}(a(\alpha^{2q^2}\beta^{q^2}+\alpha^{q^2}\beta^{2q^2}))+\mathrm{Tr}(b\{\alpha^{q^2+1}(\beta+\beta^{q^2})+\beta^{q^2+1}(\alpha+\alpha^{q^2})\}) \\
= & \ 2\mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\mathrm{N}_{k_6/k_3}(\alpha))a_0+2\mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\mathrm{N}_{k_6/k_3}(\alpha)\epsilon^q)a_1 \\
& +2\mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\mathrm{N}_{k_6/k_3}(\alpha)\epsilon^{2q})a_2 \\
& +\mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\{\mathrm{N}_{k_6/k_3}(\alpha)\}^q+\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q\mathrm{N}_{k_6/k_3}(\alpha))b_0 \\
& +\mathrm{Tr}(\left[\mathrm{Tr}_{k_6/k_3}(\alpha)\{\mathrm{N}_{k_6/k_3}(\alpha)\}^q+\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q\mathrm{N}_{k_6/k_3}(\alpha)\right]\epsilon^q)b_1 \\
& +\mathrm{Tr}(\left[\mathrm{Tr}_{k_6/k_3}(\alpha)\{\mathrm{N}_{k_6/k_3}(\alpha)\}^q+\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q\mathrm{N}_{k_6/k_3}(\alpha)\right]\epsilon^{2q})b_2 \\
= & \ 0.
\end{aligned} \tag{49}$$

The constant term of (27) for Type II curves is

$$\begin{aligned}
& \mathrm{Tr}(a\alpha^{2q^2}\beta^{2q^2})+\mathrm{Tr}(b\alpha^{q^2+1}\beta^{q^2+1}) \\
= & \ \mathrm{Tr}(\{\mathrm{N}_{k_6/k_3}(\alpha)\}^2)a_0+\mathrm{Tr}(\{\mathrm{N}_{k_6/k_3}(\alpha)\}^2\epsilon^q)a_1+\mathrm{Tr}(\{\mathrm{N}_{k_6/k_3}(\alpha)\}^2\epsilon^{2q})a_2 \\
& +\mathrm{Tr}(\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{q+1})b_0+\mathrm{Tr}(\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{q+1}\epsilon^q)b_1+\mathrm{Tr}(\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{q+1}\epsilon^{2q})b_2 \\
= & \ 0.
\end{aligned} \tag{50}$$

Then one can also build and solve a system of simultaneous linear equations, as in the case of Type I, in $a_1,\ a_2,\ b_0,\ b_1,\ b_2$.

Hereafter, we assume that a, b are known.

3.3 Definition equation of C/k

Notice that X, Y, Z correspond to a basis $\omega,\ {}^{\sigma}\omega,\ {}^{\sigma^2}\omega$ of $H^0(C/k_3, \Omega^1)$. Since C is defined over k, the next step is to find a basis of $H^0(C/k, \Omega^1)$.

The necessary and sufficient condition for $\{\omega_1, \omega_2, \omega_3\}$ to be such a basis, i.e. $H^0(C/k, \Omega^1) = \langle \omega_1, \omega_2, \omega_3 \rangle$ is

$$\begin{aligned} \omega &= \gamma\omega_1 + \delta\omega_2 + \psi\omega_3,\ {}^{\exists}\gamma,\ \delta,\ \psi \in k_3 \qquad (51) \\ \text{s.t.}\quad \det(U) &\neq 0. \quad \text{where} \quad U := \begin{pmatrix} \gamma & \delta & \psi \\ \gamma^q & \delta^q & \psi^q \\ \gamma^{q^2} & \delta^{q^2} & \psi^{q^2} \end{pmatrix}. \qquad (52) \end{aligned}$$

We will use the following correspondence.

$$\omega_1 \longleftrightarrow \underline{x}, \quad \omega_2 \longleftrightarrow \underline{y}, \quad \omega_3 \longleftrightarrow \underline{z} \qquad (53)$$

Then $X,\ Y,\ Z$ are expressed as

$$\begin{cases} X = \gamma\underline{x} + \delta\underline{y} + \psi\underline{z} \\ Y = \gamma^q\underline{x} + \delta^q\underline{y} + \psi^q\underline{z} \\ Z = \gamma^{q^2}\underline{x} + \delta^{q^2}\underline{y} + \psi^{q^2}\underline{z} \end{cases}. \qquad (54)$$

or

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = U \begin{pmatrix} \underline{x} \\ \underline{y} \\ \underline{z} \end{pmatrix}. \qquad (55)$$

Given $\gamma,\ \delta,\ \psi$, one substitutes (54) into (26) to obtain a definition equation of the curve C/k as

$$\begin{aligned}
C/k: \quad & \mathrm{Tr}(a\gamma^4+b\gamma^{2q+2})\underline{x}^4\\
&+\mathrm{Tr}(4a\gamma^3\delta+\{2\gamma^{q+2}\delta^q+2\gamma^{2q+1}\delta\}b)\underline{x}^3\underline{y}\\
&+\mathrm{Tr}(4a\gamma^3\psi+\{2\gamma^{q+2}\psi^q+2\gamma^{2q+1}\psi\}b)\underline{x}^3\underline{z}\\
&+\mathrm{Tr}(6a\gamma^2\delta^2+\{\gamma^2\delta^{2q}+\gamma^{2q}\delta^2+4\gamma^{q+1}\delta^{q+1}\}b)\underline{x}^2\underline{y}^2\\
&+\mathrm{Tr}(12a\gamma^2\delta\psi+\{2\gamma^2\delta^q\psi^q+4\gamma^{q+1}\delta\psi^q+2\gamma^{2q}\delta\psi+4\gamma^{q+1}\delta^q\psi\}b)\underline{x}^2\underline{y}\underline{z}\\
&+\mathrm{Tr}(6a\gamma^2\psi^2+\{\gamma^2\psi^{2q}+\gamma^{2q}\psi^2+4\gamma^{q+1}\psi^{q+1}\}b)\underline{x}^2\underline{z}^2\\
&+\mathrm{Tr}(4a\gamma\delta^3+\{2\gamma^q\delta^{q+2}+2\gamma\delta^{2q+1}\}b)\underline{x}\underline{y}^3\\
&+\mathrm{Tr}(12a\gamma\delta^2\psi+\{2\gamma^q\delta^2\psi^q+4\gamma\delta^{q+1}\psi^q+4\gamma^q\delta^{q+1}\psi+2\gamma\delta^{2q}\psi\}b)\underline{x}\underline{y}^2\underline{z}\\
&+\mathrm{Tr}(12a\gamma\delta\psi^2+\{2\gamma^q\delta^q\psi^2+2\gamma\delta\psi^{2q}+4\gamma^q\delta\psi^{q+1}+4\gamma\delta^q\psi^{q+1}\}b)\underline{x}\underline{y}\underline{z}^2\\
&+\mathrm{Tr}(4a\gamma\psi^3+\{2\gamma^q\psi^{q+2}+2\gamma\psi^{2q+1}\}b)\underline{x}\underline{z}^3\\
&+\mathrm{Tr}(a\delta^4+b\delta^{2q+2})\underline{y}^4\\
&+\mathrm{Tr}(4a\delta^3\psi+\{2\delta^{q+2}\psi^q+2\delta^{2q+1}\psi\}b)\underline{y}^3\underline{z}\\
&+\mathrm{Tr}(6a\delta^2\psi^2+\{\delta^2\psi^{2q}+\delta^{2q}\psi^2+4\delta^{q+1}\psi^{q+1}\}b)\underline{y}^2\underline{z}^2\\
&+\mathrm{Tr}(4a\delta\psi^3+\{2\delta^q\psi^{q+2}+2\delta\psi^{2q+1}\}b)\underline{y}\underline{z}^3\\
&+\mathrm{Tr}(a\psi^4+b\psi^{2q+2})\underline{z}^4\\
&=0.
\end{aligned} \tag{56}$$

3.4 Find a basis of $H^0(C/k,\Omega^1)$ to determine $\gamma,\ \delta$ and ψ

In this section, we give explicitly a basis of $H^0(C/k,\Omega^1)$ and determine $\gamma,\ \delta$ and ψ.

Define

$$\omega_1 = \omega + {}^{\sigma}\omega + {}^{\sigma^2}\omega \tag{57}$$

$$\omega_2 = \epsilon\omega + \epsilon^q\ {}^{\sigma}\omega + \epsilon^{q^2}\ {}^{\sigma^2}\omega \tag{58}$$

$$\omega_3 = \epsilon^2\omega + \epsilon^{2q}\ {}^{\sigma}\omega + \epsilon^{2q^2}\ {}^{\sigma^2}\omega. \tag{59}$$

Then

$$\begin{pmatrix}\underline{x}\\ \underline{y}\\ \underline{z}\end{pmatrix} = V\begin{pmatrix}X\\ Y\\ Z\end{pmatrix}. \tag{60}$$

The Vandermonde's matrix

$$V=\begin{pmatrix}1 & 1 & 1\\ \epsilon & \epsilon^q & \epsilon^{q^2}\\ \epsilon^2 & \epsilon^{2q} & \epsilon^{2q^2}\end{pmatrix} \tag{61}$$

has its determinant as

$$\det(V)=N(\epsilon-\epsilon^q)=(\epsilon-\epsilon^q)(\epsilon^q-\epsilon^{q^2})(\epsilon^{q^2}-\epsilon)=N(\epsilon-\epsilon^q)\neq 0 \tag{62}$$

then $\{\omega_i\}$ is a basis of $H^0(C/k, \Omega^1)$. We can take $U = V^{-1}$ or

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = U \begin{pmatrix} \underline{x} \\ \underline{y} \\ \underline{z} \end{pmatrix} \tag{63}$$

and the inverse matrix can be expressed by

$$U = V^{-1} = \begin{pmatrix} \gamma & \delta & \psi \\ \gamma^q & \delta^q & \psi^q \\ \gamma^{q^2} & \delta^{q^2} & \psi^{q^2} \end{pmatrix}. \tag{64}$$

Thus, one has

$$\gamma = \frac{\epsilon^{2q^2+q} - \epsilon^{q^2+2q}}{\det(V)}, \ \delta = \frac{\epsilon^{2q} - \epsilon^{2q^2}}{\det(V)} \text{ and } \psi = \frac{\epsilon^{q^2} - \epsilon^{q}}{\det(V)}. \tag{65}$$

Now we have a, b, $\underline{x}, \underline{y}, \underline{z}$ and γ, δ, ψ explicitly thus the definition equation of C/k.

4 Transfer DLP from C_0/k_3 to C/k

The transfer of DLP from C_0/k_d to C/k was known to use norm-conorm map. However, this map seemed not given explicitly and not trivial. Here we use language of divisors instead of function fields to give an explicit map from $Jac(C_0/k_3)$ to $Jac(C/k)$.

The transfer map consists of a trace and a pullback map.

Denote by π^* the pullback map induced by the cover map $\pi/k_3 : \ C \to C_0$. i.e.,

$$\begin{aligned} \pi^* : \ \mathrm{Jac}(C_0/k_3) \ &\to \ \mathrm{Jac}(C/k_3) \\ P - P_0 \ &\mapsto \ D_P - D_{P_0} \end{aligned} \tag{66}$$

where $P - P_0$ is a divisor of $\mathrm{Jac}(C_0/k_3)$ and $D_P = \sum_i e_i Q_i$ a divisor of $\mathrm{Jac}(C/k_3)$ s.t. $\pi(Q_i) = P, \ e_i$ is the ramification index at Q_i.

This map corresponds to the conorm map of the function fields.

Denote the trace map of divisor groups (Here it is not as before on k_3/k but on the divisor group)

$$\begin{aligned} \mathrm{Tr}_{k_3/k} : \ \mathrm{Jac}(C/k_3) \ &\to \ \mathrm{Jac}(C/k) \\ D_P \ &\mapsto \ D_P + {}^{\sigma}D_P + {}^{\sigma^2}D_P \end{aligned} \tag{67}$$

which corresponds to the norm map of the function fields.

Then the transfer map is a homomorphism defined by the composition of π^* with the trace map

$$\chi := \mathrm{Tr}_{k_3/k} \circ \pi^* : \mathrm{Jac}(C_0/k_3) \longrightarrow \mathrm{Jac}(C/k). \tag{68}$$

Given $P_1,\ P_2$, two points on C_0 such that $P_2 \in \langle P_1 \rangle$, the elliptic curve discrete logarithm problem is to find an integer λ s.t. $P_2 = \lambda P_1$. Since the group of points on C_0 and the group $\mathrm{Jac}(C_0)$ are isomorphic, we can transfer from $P_2 = \lambda P_1$ to

$$(P_2 - P_\infty) = \lambda(P_1 - P_\infty) \tag{69}$$

on $\mathrm{Jac}(C_0)$ where P_∞ is the point at infinity.

Finally, the homomorphism χ transfers the above discrete logarithm to the discret logarithm on $\mathrm{Jac}(C/k)$ which is to find λ such that

$$(\chi(P_2) - \chi(P_\infty)) = \lambda(\chi(P_1) - \chi(P_\infty)). \tag{70}$$

So, it suffices to find π.

In fact, π can be factored into

$$\pi/k_3 = \pi_1 \circ \pi_2 \tag{71}$$

where π_1/k_3 is the map from C/k_3 defined by (26) to C_0 and π_2/k_3 is an isomorphism from C/k_3 defined by the equation (56) of C/k to C/k_3 defined by (26) which can be represented by (63) where the matrix U is known.

We find π_1 as follows.

Let $s,\ t$ be $s = \frac{Y}{X},\ t = \frac{Z}{X}$ then (26) becomes

$$C:\ a + a^q s^4 + a^{q^2} t^4 + bs^2 + b^q s^2 t^2 + b^{q^2} t^2 = 0. \tag{72}$$

Additionally let $u,\ v$ be $u = s^2,\ v = t^2$ then (72) becomes

$$a + a^q u^2 + a^{q^2} v^2 + bu + b^q uv + b^{q^2} v = 0 \tag{73}$$

which can be identified with $\mathbb{P}^1(k_3)$, while C is its $(2,2)$-covering.

Below, we first consiter Type I case.

4.1 Type I

Since (73) is a genus zero curve, we choose the point on it $u_0 = (\alpha\beta)^{-q^2+1},\ v_0 = (\alpha\beta)^{-q^2+q}$ when $x = 0$.

Then a point (u, v) of (73) are uniquely determined by a line which has slope l and passes through the point $(u_0, v_0) = ((\alpha\beta)^{-q^2+1},\ (\alpha\beta)^{-q^2+q})$ and the point $(u,\ v)$.

The equation of the line is

$$v - (\alpha\beta)^{-q^2+q} = l(u - (\alpha\beta)^{-q^2+1}). \tag{74}$$

The slope l can be written as

$$l = \frac{v - (\alpha\beta)^{-q^2+q}}{u - (\alpha\beta)^{-q^2+1}}. \tag{75}$$

Substituting $u = \dfrac{(x-\alpha)(x-\beta)}{(x-\alpha^{q^2})(x-\beta^{q^2})}$, $v = \dfrac{(x-\alpha^q)(x-\beta^q)}{(x-\alpha^{q^2})(x-\beta^{q^2})}$ into (74), the denominator of l becomes

$$u - (\alpha\beta)^{-q^2+1} = \frac{\{1-(\alpha\beta)^{-q^2+1}\}x^2 + (-\alpha-\beta+\alpha\beta^{-q^2+1}+\alpha^{-q^2+1}\beta)x}{(x-\alpha^{q^2})(x-\beta^{q^2})}. \quad (76)$$

The numerator of l becomes

$$v - (\alpha\beta)^{-q^2+q} = \frac{\{1-(\alpha\beta)^{-q^2+q}\}x^2 + (-\alpha^q-\beta^q+\alpha^q\beta^{-q^2+q}+\alpha^{-q^2+q}\beta^q)x}{(x-\alpha^{q^2})(x-\beta^{q^2})}. \quad (77)$$

In the sequal,

$$l = \frac{\{1-(\alpha\beta)^{-q^2+q}\}x + (-\alpha^q-\beta^q+\alpha^q\beta^{-q^2+q}+\alpha^{-q^2+q}\beta^q)}{\{1-(\alpha\beta)^{-q^2+1}\}x + (-\alpha-\beta+\alpha\beta^{-q^2+1}+\alpha^{-q^2+1}\beta)}. \quad (78)$$

Define $G_{11},\ G_{12},\ G_{21},\ G_{22} \in k_3$

$$G_{11} := 1-(\alpha\beta)^{-q^2+q} \quad (79)$$
$$G_{12} := -\alpha^q-\beta^q+\alpha^q\beta^{-q^2+q}+\alpha^{-q^2+q}\beta^q \quad (80)$$
$$G_{21} := 1-(\alpha\beta)^{-q^2+1} \quad (81)$$
$$G_{22} := -\alpha-\beta+\alpha\beta^{-q^2+1}+\alpha^{-q^2+1}\beta. \quad (82)$$

Then l can be expressed by x under the action of the matrix G.

$$l = G\cdot x \quad \text{s.t.} \quad G := \begin{pmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{pmatrix} \in \mathrm{GL}_2(k_3). \quad (83)$$

In particular, x is now the image of l under action of G^{-1}:

$$x = G^{-1}l = \frac{G_{22}l - G_{12}}{-G_{21}l + G_{11}}. \quad (84)$$

Now we have expressed x by l, to find π_1 next we try to express x by X, Y, Z directly. Substituting $s = \dfrac{Y}{X}$, $t = \dfrac{Z}{X}$ into l, one has

$$l = \frac{Z^2-(\alpha\beta)^{-q^2+q}X^2}{Y^2-(\alpha\beta)^{-q^2+1}X^2}. \quad (85)$$

Therefore

$$x = G^{-1}l = \frac{G_{22}Z^2 - G_{22}(\alpha\beta)^{-q^2+q}X^2 - G_{12}Y^2 + G_{12}(\alpha\beta)^{-q^2+1}X^2}{-G_{21}Z^2 + G_{21}(\alpha\beta)^{-q^2+q}X^2 + G_{11}Y^2 - G_{11}(\alpha\beta)^{-q^2+1}X^2}. \quad (86)$$

To find y, one can use the definition equation of Type I curve $C_0 : y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)$,

$$\frac{(x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)}{{}^{\sigma}y^{\sigma^2}y} = st. \tag{87}$$

Then

$$y = \frac{st\mathrm{N}_{k_3/k}(y)}{(x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)}. \tag{88}$$

To find $\mathrm{N}_{k_3/k}(y)$, use the definition of C_0 again

$$\mathrm{N}_{k_3/k}(y^2) = \mathrm{N}_{k_3/k}(x-\alpha)^2\mathrm{N}_{k_3/k}(x-\beta)^2. \tag{89}$$

Now $\mathrm{N}_{k_3/k}(y)$ is expressed by x as

$$\mathrm{N}_{k_3/k}(y) = \pm\mathrm{N}_{k_3/k}(x-\alpha)\mathrm{N}_{k_3/k}(x-\beta). \tag{90}$$

Hence, y can be written as

$$y = \pm st(x-\alpha^{q^2})(x-\beta^{q^2}) \tag{91}$$

and we use $y = st(x-\alpha^{q^2})(x-\beta^{q^2})$ hereafter.

Similar to x, y can also be expressed by $X,\ Y,\ Z$.

$$\begin{aligned} y &= st(x-\alpha^{q^2})(x-\beta^{q^2}) \\ &= \frac{YZ}{X^2}(x-\alpha^{q^2})(x-\beta^{q^2}). \end{aligned} \tag{92}$$

From the coordinates $x,\ y$ of the affice curve C_0, one can obtain projective coordinates of C_0 as follows.

First, denote x as a fraction $x = \dfrac{x_2}{x_1}$ where x_1 denotes the numerator and x_2 the denomenator.

Then $x,\ y,\ z$ can be expressed as

$$x = \frac{x_2}{x_1},\ y = \frac{YZ}{X^2}\left(\frac{x_2}{x_1} - \alpha^{q^2}\right)\left(\frac{x_2}{x_1} - \beta^{q^2}\right),\ z = 1. \tag{93}$$

Thus one obtains the projective coordinates of C_0 as

$$x = x_1x_2X^2,\ y = YZ(x_2 - \alpha^{q^2}x_1)(x_2 - \beta^{q^2}x_1),\ z = {x_1}^2X^2. \tag{94}$$

Now π_1 can be expressed as

$$\begin{aligned} \pi_1 :\ C &\rightarrow C_0 \\ (X,\ Y,\ Z) &\mapsto (x,\ y,\ z) \end{aligned}$$

such that

$$
\begin{aligned}
x &= \{-(\alpha\beta)^{-2q^2+2}G_{11}G_{12}+(\alpha\beta)^{-2q^2+q+1}G_{11}G_{22}+(\alpha\beta)^{-2q^2+q+1}G_{12}G_{21}-(\alpha\beta)^{-2q^2+2q}G_{21}G_{22}\}X^6 \\
&\quad +\{2(\alpha\beta)^{-q^2+1}G_{11}G_{12}-(\alpha\beta)^{-q^2+q}G_{11}G_{22}-(\alpha\beta)^{-q^2+q}G_{12}G_{21}\}X^4Y^2 \\
&\quad +\{-(\alpha\beta)^{-q^2+1}G_{11}G_{22}-(\alpha\beta)^{-q^2+1}G_{12}G_{21}+2(\alpha\beta)^{-q^2+q}G_{21}G_{22}\}X^4Z^2-G_{11}G_{12}X^2Y^4 \\
&\quad +(G_{11}G_{22}+G_{12}G_{21})X^2Y^2Z^2-G_{21}G_{22}X^2Z^4, \qquad (95)
\end{aligned}
$$

$$
\begin{aligned}
y &= \{(\alpha\beta)^{-q^2+2}{G_{11}}^2+(\alpha\beta)^{-2q^2+2}(\alpha^{q^2}+\beta^{q^2})G_{11}G_{12}-2(\alpha\beta)^{-q^2+q+1}G_{11}G_{21} \\
&\quad -(\alpha\beta)^{-2q^2+q+1}(\alpha^{q^2}+\beta^{q^2})G_{11}G_{22}+(\alpha\beta)^{-2q^2+2}{G_{12}}^2-(\alpha\beta)^{-2q^2+q+1}(\alpha^{q^2}+\beta^{q^2})G_{12}G_{21} \\
&\quad -2(\alpha\beta)^{-2q^2+q+1}G_{12}G_{22}+(\alpha\beta)^{-q^2+2q}{G_{21}}^2+(\alpha\beta)^{-2q^2+2q}(\alpha^{q^2}+\beta^{q^2})G_{21}G_{22} \\
&\quad +(\alpha\beta)^{-2q^2+2q}{G_{22}}^2\}X^4YZ \\
&\quad +\{-2\alpha\beta G_{11}^2-2(\alpha\beta)^{-q^2+1}(\alpha^{q^2}+\beta^{q^2})G_{11}G_{12}+2(\alpha\beta)^qG_{11}G_{21}+(\alpha\beta)^{-q^2+q}(\alpha^{q^2}+\beta^{q^2})G_{11}G_{22} \\
&\quad -2(\alpha\beta)^{-q^2+1}{G_{12}}^2+(\alpha\beta)^{-q^2+q}(\alpha^{q^2}+\beta^{q^2})G_{12}G_{21}+2(\alpha\beta)^{-q^2+q}G_{12}G_{22}\}X^2Y^3Z \\
&\quad +\{2\alpha\beta G_{11}G_{21}+(\alpha\beta)^{-q^2+1}(\alpha^{q^2}+\beta^{q^2})G_{11}G_{22}+(\alpha\beta)^{-q^2+1}(\alpha^{q^2}+\beta^{q^2})G_{12}G_{21} \\
&\quad +2(\alpha\beta)^{-q^2+1}G_{12}G_{22}-2(\alpha\beta)^q{G_{21}}^2-2(\alpha\beta)^{-q^2+q}(\alpha^{q^2}+\beta^{q^2})G_{21}G_{22}-2(\alpha\beta)^{-q^2+q}{G_{22}}^2\}X^2YZ^3 \\
&\quad +\{(\alpha\beta)^{q^2}{G_{11}}^2+(\alpha^{q^2}+\beta^{q^2})G_{11}G_{12}+{G_{12}}^2\}Y^5Z \\
&\quad -\{2(\alpha\beta)^{q^2}G_{11}G_{21}+(\alpha^{q^2}+\beta^{q^2})G_{11}G_{22}+(\alpha^{q^2}+\beta^{q^2})G_{12}G_{21}+2G_{12}G_{22}\}Y^3Z^3 \\
&\quad +\{(\alpha\beta)^{q^2}{G_{21}}^2+(\alpha^{q^2}+\beta^{q^2})G_{21}G_{22}+{G_{22}}^2\}YZ^5, \qquad (96)
\end{aligned}
$$

$$
\begin{aligned}
z &= \{(\alpha\beta)^{-2q^2+2}{G_{11}}^2-2(\alpha\beta)^{-2q^2+q+1}G_{11}G_{21}+(\alpha\beta)^{-2q^2+2q}{G_{21}}^2\}X^6 \\
&\quad +\{-2(\alpha\beta)^{-q^2+1}{G_{11}}^2+2(\alpha\beta)^{-q^2+q}G_{11}G_{21}\}X^4Y^2 \\
&\quad +\{2(\alpha\beta)^{-q^2+1}G_{11}G_{21}-2(\alpha\beta)^{-q^2+q}{G_{21}}^2\}X^4Z^2 \\
&\quad +{G_{11}}^2X^2Y^4-2G_{11}G_{21}X^2Y^2Z^2+{G_{21}}^2X^2Z^4. \qquad (97)
\end{aligned}
$$

4.2 Type II

Calculation for Type II curves is similar to Type I, what we need is to confirm that (86), (92) are defined over k_3.

For (86), first the entries of the matrix G, $G_{11},\ G_{12},\ G_{21},\ G_{22}$ become

$$
\begin{aligned}
G_{11} &= 1-\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{-q^2+q} && (98)\\
G_{12} &= -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q+\{\mathrm{N}_{k_6/k_3}(\alpha)\}^q\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^{-q^2} && (99)\\
G_{21} &= 1-\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{-q^2+1} && (100)\\
G_{22} &= -\mathrm{Tr}_{k_6/k_3}(\alpha)+\mathrm{N}_{k_6/k_3}(\alpha)\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^{-q^2}. && (101)
\end{aligned}
$$

Thus x can be expressed as,

$$
x=\frac{G_{22}Z^2-G_{22}\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{-q^2+q}X^2-G_{12}Y^2+G_{12}\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{-q^2+1}X^2}{-G_{21}Z^2+G_{21}\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{-q^2+q}X^2+G_{11}Y^2-G_{11}\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{-q^2+1}X^2} \qquad (102)
$$

which has only k_3-coefficients.

Next, (92) becomes,

$$\begin{aligned} y &= \frac{YZ}{X^2}(x-\alpha^{q^2})(x-\beta^{q^2}) \\ &= \frac{YZ}{X^2}(x^2-\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^{q^2}x+\{\mathrm{N}_{k_6/k_3}(\alpha)\}^{q^2}) \end{aligned} \tag{103}$$

which is also k_3-coefficients. Thus we are done.

5 Computer experiments

The computation environment as follows.

- OS: Windows XP Professional SP2
- CPU: Pentium4 3.2GHz
- Memory: 1.5GB
- Programming language: Magma ver.2.13-14

We start from an elliptic curve E in Legandre form and a base point P_E of E. P_E and its m-multiple mP_E are mapped to a point P and mP on an elliptic curve C_0 which is isomorphic to E. Then we find $\chi(P)$ and $\chi(mP)$ in $\mathrm{Jac}(C)$.

5.1 Type I

$$q = 1152921504606851053,\ k = \mathbb{F}_q,\ k_3 = k[x]/\langle x^3-2\rangle,\ {}^{\exists}\epsilon\ \in k_3 \text{ s.t. } \epsilon^3-2=0$$

$$\lambda = 685592167687491848\epsilon^2 + 685592167687491847\epsilon + 3$$

The elliptic curve E is in projective Legandre form.

$$E/k_3:\ y^2z = x(x-z)(x-\lambda z)$$

5.1.1 Test of Type I curves

Let $\alpha = \epsilon + 1$, then

$$\begin{aligned} A &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \\ a_{11} &= 238798614356861922\epsilon + 457061445124994566 \\ a_{12} &= 685592167687491848\epsilon^2 + 685592167687491847\epsilon + 1152921504606851052 \\ a_{21} &= 1,\ a_{22} = 924390782044353769\epsilon + 457061445124994564 \end{aligned}$$

$$
\begin{aligned}
B &= \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\
b_{11} &= 2\epsilon^2 + \epsilon + 477597228713723848 \\
b_{12} &= 1152921504606851050\epsilon^2 + 1152921504606851050\epsilon + 1152921504606851044 \\
b_{21} &= \epsilon^2 + \epsilon + 1152921504606851052 \\
b_{22} &= 1152921504606851051\epsilon^2 + 1152921504606851052\epsilon + 477597228713723844
\end{aligned}
$$

The quadratic equation $b_{21}x^2 + (b_{22} - b_{11})x - b_{12} = 0$ has two solutions:

$$\left\{\epsilon^2 + 2\epsilon + 1,\ 733677321113450670\epsilon^2 + 524055229366750479\epsilon + 209622091746700193\right\}$$

Therefore, E is Type I. Take $\beta = \epsilon^2 + 2\epsilon + 1 = \alpha^2$, we know that E is k_3-isomorphic to

$$C_0/k_3 :\ y^2z^2 = (x - \alpha z)(x - \alpha^q z)(x - \beta z)(x - \beta^q z).$$

In fact, to test of Type I curves, we chosen $\lambda = 2, ..., 10001$, the average time to test each curve is 0.0356858 second. Among these curves, 5018 are Type I.

5.1.2 Finding definition equation of covering curve C/k

The covering C/k of C_0/k_3 is found using the algorithm shown in the section 4.

$$
\begin{aligned}
C/k \quad : \quad & 997145058967064651\underline{x}^3\underline{y} + 588586465123877340\underline{x}^3\underline{z} \\
+ \quad & 907131123326719637\underline{x}^2\underline{y}^2 + 896716725805328597\underline{x}^2\underline{yz} \\
+ \quad & 973749290975691411\underline{x}^2\underline{z}^2 + 1024819115206089825\underline{xy}^3 \\
+ \quad & 280456204442426083\underline{xy}^2\underline{z} + 318544658202842297\underline{xyz}^2 \\
+ \quad & 1088870309906470439\underline{xz}^3 + 973749290975691411\underline{y}^4 \\
+ \quad & 294293232561938670\underline{y}^3\underline{z} + 1120895907256660746\underline{y}^2\underline{z}^2 \\
+ \quad & 537516640893478926\underline{yz}^3 + 975051090665865291\underline{z}^4 = 0
\end{aligned}
$$

To find the C/k from E takes 0.500 seconds, where 0.063 second is used to test if E is Type I, the rest 0.437 is used to build C/k.

5.1.3 Transfer of DLP

The isomorphism from E to C_0, $\iota:\ E\to C_0$ is,

$$
\begin{aligned}
\iota:\ E &\rightarrow C_0\\
(x:y:z) &\mapsto (x_{C_0}:y_{C_0}:z_{C_0})\\
x_{C_0} &= (364080906763379389\epsilon^2+963836771592621382\epsilon+45113745901700524)x^2\\
&+ (697163568297605614\epsilon^2+434818842429256188\epsilon+651968585745464837)xz\\
&+ (1110165463009250121\epsilon^2+159411805327734998\epsilon+1139314830835562614)z^2,\\
y_{C_0} &= (103276516251305235\epsilon^2+814915306056127686\epsilon+861572657639767622)yz,\\
z_{C_0} &= (883436713213250245\epsilon^2+38740486277729303\epsilon+1108413203079573589)x^2\\
&+ (614045874632256899\epsilon^2+476034365815665715\epsilon+725151688441932395)xz\\
&+ (1080996664374642930\epsilon^2+29168798634607191\epsilon+130243006693127807)z^2.
\end{aligned}
$$

The inverse map ι^{-1} is

$$
\begin{aligned}
\iota^{-1}:\ C_0 &\rightarrow E\\
(x:y:z) &\mapsto (x_E:y_E:z_E)\\
x_E &= (228530722562497283\epsilon^2+924390782044353770\epsilon+228530722562497284)x^2\\
&+ (467329336919359205\epsilon^2+218262830768132642\epsilon+1152921504606851049)xz\\
&+ (467329336919359205\epsilon^2+249066506151226564\epsilon+685592167687491850)z^2,\\
y_E &= (1098530568356793848\epsilon^2+364091151918511417\epsilon+156909573516618064)yz,\\
z_E &= x^2+(218262830768132643\epsilon+1152921504606851051)xz\\
&+ (685592167687491847\epsilon^2+934658673838718410\epsilon+1)z^2.
\end{aligned}
$$

For an example, take a base point on E

$$
\begin{aligned}
E\ni P_E &= (326484750616207568\epsilon^2+398950984132538563\epsilon+1105635074365709877\\
&: 155216221479156187\epsilon^2+496624914529310471\epsilon+708459555015860335:1)
\end{aligned}
$$

has a prime order 383123885216476279036490868125406665879768163968774759

Under the isomorphism ι, P_E is mapped to $P=\iota(P_E)$ on C_0.

$$
\begin{aligned}
P &= (382583549840633528\epsilon^2+1049745021810473522\epsilon+527223886793925136\\
&: 297304679459601150\epsilon^2+626540460794459518\epsilon+906489884274840212:1)
\end{aligned}
$$

From P one obtaines D_P and $\chi(P)$ as follows:

$$D_P=Q_1+Q_2$$

$$
\begin{aligned}
q_1 &= 712456629299217053\epsilon^2+953676660329800786\epsilon+707524424701837646\\
q_2 &= 666557349447958527\epsilon^2+352353429259986813\epsilon+1073895093206451353\\
q_3 &= 805061362249374584\epsilon^2+1042799797746437227\epsilon+880598497458186947\\
q_4 &= 527740077639497471\epsilon^2+947552956030900685\epsilon+390269122338929978\\
Q_1 &= (q_1:\ q_2:\ 1)\in C/k_3,\qquad Q_2=(q_3:\ q_4:\ 1)\in C/k_3
\end{aligned}
$$

$$\chi(P) = D_P + {}^{\sigma}D_P + {}^{\sigma^2}D_P$$

$$\begin{aligned}
{}^{\sigma}D_P &= {}^{\sigma}Q_1 + {}^{\sigma}Q_2, \qquad {}^{\sigma^2}D_P = {}^{\sigma^2}Q_1 + {}^{\sigma^2}Q_2 \\
{}^{\sigma}Q_1 &= ({q_1}^q : {q_2}^q : 1), \qquad {}^{\sigma}Q_2 = ({q_3}^q : {q_4}^q : 1) \\
{}^{\sigma^2}Q_1 &= ({q_1}^{q^2} : {q_2}^{q^2} : 1), \qquad {}^{\sigma^2}Q_2 = ({q_3}^{q^2} : {q_4}^{q^2} : 1).
\end{aligned}$$

The time needs to calculate from P_E to $\chi(P)$ is 17.578 seconds.

Now let

$$m = 3232659103212686645141292240094896701519089729553765 19.$$

$$\begin{aligned}
E \ni\ & mP_E = (7923102218628168 38\epsilon^2 + 180893695299760122\epsilon + 952490131358998041 \\
: \ & 669346193997384009\epsilon^2 + 488209130112427093\epsilon + 787028498315590410 : 1).
\end{aligned}$$

This mP_E is also mapped to $C_0 \ni mP = \iota(mP_E)$,

$$\begin{aligned}
mP &= (306607799499267855\epsilon^2 + 445518833785785499\epsilon + 141583952331989134 \\
&: 585481570718467983\epsilon^2 + 205882509018091440\epsilon + 573359644129055255 : 1)
\end{aligned}$$

One then from mP calculates D_{mP} and $\chi(mP)$ as follows.

$$D_{mP} = Q_1 + Q_2$$

$$\begin{aligned}
q_1 &= 1062802094539799458\epsilon^2 + 296237055839945308\epsilon + 1057758671244525799 \\
q_2 &= 344189168181796656\epsilon^2 + 529982675029763103\epsilon + 1134629167237810190 \\
q_3 &= 666903385786606500\epsilon^2 + 44288219254827598\epsilon + 362073667770795536 \\
q_4 &= 8690116147489311\epsilon^2 + 330243703134573774\epsilon + 1048131323955608138 \\
Q_1 &= (q_1 : q_2 : 1) \in C/k_3, \qquad Q_2 = (q_3 : q_4 : 1) \in C/k_3
\end{aligned}$$

$$\chi(mP) = D_{mP} + {}^{\sigma}D_{mP} + {}^{\sigma^2}D_{mP}$$

$$\begin{aligned}
{}^{\sigma}D_{mP} &= {}^{\sigma}Q_1 + {}^{\sigma}Q_2, \qquad {}^{\sigma^2}D_{mP} = {}^{\sigma^2}Q_1 + {}^{\sigma^2}Q_2 \\
{}^{\sigma}Q_1 &= ({q_1}^q : {q_2}^q : 1), \qquad {}^{\sigma}Q_2 = ({q_3}^q : {q_4}^q : 1) \\
{}^{\sigma^2}Q_1 &= ({q_1}^{q^2} : {q_2}^{q^2} : 1), \qquad {}^{\sigma^2}Q_2 = ({q_3}^{q^2} : {q_4}^{q^2} : 1)
\end{aligned}$$

The time taken from mP_E to calculate $\chi(mP)$ is 9.859 seconds.

In fact, given $\{2^i P_E | 0 \le i \le 999\}$, the average time to calculate $\chi(2^i P)$ is 17.8545 seconds.

5.2 Type II

Assume

$$k = \mathbb{F}_q,\ q = 1152921504606850871$$

$$\begin{aligned}
k[x] &\ni a(x) = x^3 + 943550857826445658x^2 + 1018916892242739535x \\
&+ 475736851389393367 \\
k_3 &= k[x]/\langle a(x)\rangle,\ {}^{\exists}\epsilon\ \in k_3 \text{ s.t. } a(\epsilon) = 0
\end{aligned}$$

$$\begin{aligned}
k_3[x] &\ni b(x) = x^2 + (595455718590278195\epsilon^2 + 926100813892756385\epsilon \\
&+ 508785546940475093)x + 463189347482206220\epsilon^2 + 936329421988414364\epsilon \\
&+ 172788951250122324 \\
k_6 &= k_3[x]/\langle b(x)\rangle,\ {}^{\exists}\eta\ \in k_6 \text{ s.t. } b(\eta) = 0
\end{aligned}$$

$$\alpha = \eta + \epsilon,\ \beta = \alpha^{q^3}$$

Suppose one has three isomorphic elliptic curves:

$$\begin{aligned}
C_0/k_3 &: \quad y^2z^2 = (x - \alpha z)(x - \alpha^q z)(x - \beta z)(x - \beta^q z) \\
E_\lambda/k_3 &: \quad y^2 z = \mathrm{N}_{k_6/k_3}(\beta - \alpha^q)x(x - z)(x - \lambda z),\ \lambda = \mathrm{N}_{k_6/k_3}\left(\frac{\alpha^q - \alpha}{\alpha^q - \beta}\right) \\
E/k_3 &: \quad y^2 z = x(x - z)(x - \lambda z),\ \lambda = \mathrm{N}_{k_6/k_3}\left(\frac{\alpha^q - \alpha}{\alpha^q - \beta}\right)
\end{aligned}$$

5.2.1 Find definition equation of the covering curve C/k

Using the algorithm in the section 4, one find the definition equation of C/k as follows.

$$\begin{aligned}
C/k \quad : \quad & 261966538672930061\underline{x}^4 + 719520632819288417\underline{x}^3\underline{y} \\
+ \quad & 711206123750751637\underline{x}^3\underline{z} + 556061188891864603\underline{x}^2\underline{y}^2 \\
+ \quad & 311605282877609888\underline{x}^2\underline{y}\underline{z} + 775851849086806638\underline{x}^2\underline{z}^2 \\
+ \quad & 982040544271606073\underline{x}\underline{y}^3 + 860780141350083361\underline{x}\underline{y}^2\underline{z} \\
+ \quad & 853202732103761301\underline{x}\underline{y}\underline{z}^2 + 953674572673705028\underline{x}\underline{z}^3 \\
+ \quad & 1020431679265907920\underline{y}^4 + 609659296596817935\underline{y}^3\underline{z} \\
+ \quad & 954717973652630225\underline{y}^2\underline{z}^2 + 717468332466366860\underline{y}\underline{z}^3 \\
+ \quad & 1023160869085822939\underline{z}^4 = 0
\end{aligned}$$

Calculation of C/k takes 0.500 second.

5.2.2 Transfer of DLP

We first find the isomorphism from E to E_λ, $\xi:\ E \to E_\lambda$ as follows.

$$\begin{array}{rcl}
\xi:\ E & \to & E_\lambda \\
(x:y:z) & \mapsto & (x_{E_\lambda}:y_{E_\lambda}:z_{E_\lambda}) \\
x_{E_\lambda} & = & (508394311291495279\epsilon^2+644802231052062119\epsilon+115125795437003532)x, \\
y_{E_\lambda} & = & (177549366635458744\epsilon^2+533904715816049699\epsilon+115337281084752855)y, \\
z_{E_\lambda} & = & (508394311291495279\epsilon^2+644802231052062119\epsilon+115125795437003532)z
\end{array}$$

Its inverse map ξ^{-1} is

$$\begin{array}{rcl}
\xi^{-1}:\ E_\lambda & \to & E \\
(x:y:z) & \mapsto & (x_E:y_E:z_E) \\
x_E & = & (953930729849692988\epsilon^2+810853815288336082\epsilon+251110930387145558)x, \\
y_E & = & (1138672552244146500\epsilon^2+82385099258240519\epsilon+13496951135910011)y, \\
z_E & = & (953930729849692988\epsilon^2+810853815288336082\epsilon+251110930387145558)z
\end{array}$$

Next we calculate the isomorphism from E_λ to C_0, $\tau:\ E_\lambda \to C_0$ as follows.

$$\begin{array}{rcl}
\tau:\ E_\lambda & \to & C_0 \\
(x:y:z) & \mapsto & (x_{C_0}:y_{C_0}:z_{C_0}) \\
x_{C_0} & = & (510834712742882221\epsilon^2+459409699423611549\epsilon+472370343629151306)x^2z \\
 & + & (23471605822501754\epsilon^2+309377569878570651\epsilon+7799912042878324)xyz \\
 & + & (931076450504798462\epsilon^2+525743454321773525\epsilon+30041499258217822)xz^2 \\
 & + & (977818514557529265\epsilon^2+765506242357294185\epsilon+252827041845239982)yz^2 \\
 & + & (1000370112565854753\epsilon^2+328209714163922360\epsilon+293352898935549091)z^3, \\
y_{C_0} & = & (1102768582695395466\epsilon^2+801656811370788382\epsilon+1017012503317150212)x^3 \\
 & + & (162397320242107152\epsilon^2+559604911348892417\epsilon+312861297828079035)x^2z \\
 & + & (558782202587610802\epsilon^2+590994009401290871\epsilon+1152361677914957201)xz^2 \\
 & + & (11735802911250877\epsilon^2+731149537242710761\epsilon+3899956021439162)y^2z \\
 & + & (764240535732840601\epsilon^2+875626294947314353\epsilon+1076372293311177227)yz^2 \\
 & + & (48504428759686342\epsilon^2+341476326696745685\epsilon+96595209872171953)z^3, \\
z_{C_0} & = & (1105978292961847363\epsilon^2+534166364849709569\epsilon+1137321680521094223)x^2z \\
 & + & (700411960197286424\epsilon^2+396739544391375873\epsilon+141613337225890943)xz^2 \\
 & + & (1019981124724128614\epsilon^2+858207083874918419\epsilon+885871207426547152)z^3
\end{array}$$

The inverse map τ^{-1} is

$$\begin{array}{rcl}
\tau^{-1}: \ C_0 & \rightarrow & E_\lambda \\
(x:y:z) & \mapsto & (x_{E_\lambda}:y_{E_\lambda}:z_{E_\lambda}) \\
x_{E_\lambda} & = & (118031724417309434\epsilon^2+350724518050046294\epsilon+1076063691653845190)x^2z \\
& + & (670405242279340424\epsilon^2+845948962475385428\epsilon+764269400807635885)xz^2 \\
& + & (118031724417309434\epsilon^2+350724518050046294\epsilon+1076063691653845190)yz^2 \\
& + & (335044387858599 10\epsilon^2+683030287832610661\epsilon+617705016327370265)z^3, \\
y_{E_\lambda} & = & (916858055772232003\epsilon^2+451472468506758283\epsilon+153715625906011362)x^3 \\
& + & (294627282375680470\epsilon^2+920917626394396329\epsilon+13034806790794087)x^2z \\
& + & (916858055772232003\epsilon^2+451472468506758283\epsilon+153715625906011362)xyz \\
& + & (410075187838725568\epsilon^2+280227746762147164\epsilon+841519322959781078)xz^2 \\
& + & (482516262327510447\epsilon^2+306972542131465443\epsilon+388652103799214986)yz^2 \\
& + & (574942304842369359\epsilon^2+1073906081772340197\epsilon+240967744611792259)z^3, \\
z_{E_\lambda} & = & (979613630890391737\epsilon^2+873389934362453645\epsilon+48321338448744427)z^3
\end{array}$$

For an example, a base point on E is chosen as

$$\begin{array}{rcl}
E \ni P_E & = & (832338441672439527\epsilon^2+369146262528272140\epsilon+788595051686438200 \\
& : & 916492546448194121\epsilon^2+805387000881236587\epsilon+244343815529721159:1)
\end{array}$$

P_E has a prime order : $\mathrm{ord}(P_E) = 383123885216476097596869443538990953306902164540505859$.

This base point is mapped by ξ, τ to a point on C_0.

First, P_E is mapped to $E_\lambda \ni P_{E_\lambda} = \xi(P_E)$ as follows.

$$\begin{array}{rcl}
P_{E_\lambda} & = & (832338441672439527\epsilon^2+369146262528272140\epsilon+788595051686438200 \\
& : & 418553404991940047\epsilon^2+588606626377609234\epsilon+1115855807315016888:1)
\end{array}$$

Next, it is mapped to $C_0 \ni P = \tau(P_{E_\lambda})$

$$\begin{array}{rcl}
P & = & (1003935588241243168\epsilon^2+895066217057986955\epsilon+382773722993550439 \\
& : & 678187206200284353\epsilon^2+191639213584321008\epsilon+673955618306920562:1)
\end{array}$$

Now we find D_P and $\chi(P)$ as follows.

$$D_P = Q_1 + Q_2$$

$$\begin{array}{rcl}
q_1 & = & 1117937506258149424\epsilon^2+644917233207069268\epsilon+165251471146963260 \\
q_2 & = & 403047038883440000\epsilon^2+653044510390728782\epsilon+817374729039765305 \\
q_3 & = & 994819008370064408\epsilon^2+979271450995116569\epsilon+737452330843672573 \\
q_4 & = & 154176739126340404\epsilon^2+1152026966659272902\epsilon+1072497119895785670 \\
Q_1 & = & (q_1: \ q_2: \ 1) \in C/k_3, \qquad Q_2 = (q_3: \ q_4: \ 1) \in C/k_3
\end{array}$$

$$\chi(P) = D_P + {}^{\sigma}D_P + {}^{\sigma^2}D_P$$

$$\begin{aligned} {}^{\sigma}D_P &= {}^{\sigma}Q_1 + {}^{\sigma}Q_2, \qquad {}^{\sigma^2}D_P = {}^{\sigma^2}Q_1 + {}^{\sigma^2}Q_2 \\ {}^{\sigma}Q_1 &= ({q_1}^q : \ {q_2}^q : \ 1), \qquad {}^{\sigma}Q_2 = ({q_3}^q : \ {q_4}^q : \ 1) \\ {}^{\sigma^2}Q_1 &= ({q_1}^{q^2} : \ {q_2}^{q^2} : \ 1), \qquad {}^{\sigma^2}Q_2 = ({q_3}^{q^2} : \ {q_4}^{q^2} : \ 1) \end{aligned}$$

To calculte $\chi(P)$ from P_E takes 21.062 seconds.

Now take $m = 1820961003701098475297391705524591167096265226905077 09$, mP_E is

$$\begin{aligned} E \ni \ & mP_E = (522521730599820536\epsilon^2 + 443211485181667680\epsilon + 408033332463290588 \\ : \ & 191091537075096495\epsilon^2 + 622369471011935091\epsilon + 865873192897372210 : 1) \end{aligned}$$

mP_E is also mapped first to $E_\lambda \ni mP_{E_\lambda} = \xi(mP_E)$,

$$\begin{aligned} mP_{E_\lambda} &= (522521730599820536\epsilon^2 + 443211485181667680\epsilon + 408033332463290588 \\ &: \ 872463812381179496\epsilon^2 + 234010666736627778\epsilon + 346552211766968750 : 1) \end{aligned}$$

It is then mapped to $C_0 \ni mP = \tau(mP_{E_\lambda})$:

$$\begin{aligned} mP &= (457134269332727797\epsilon^2 + 1093275824725039274\epsilon + 664447513560384851 \\ &: \ 955617022224051997\epsilon^2 + 777335844438891994\epsilon + 420110831598890971 : 1) \end{aligned}$$

From mP, one can find D_{mP} and $\chi(mP)$ as follows.

$$D_{mP} = Q_1 + Q_2$$

$$\begin{aligned} q_1 &= 30078314732782878\epsilon^2 + 988992501393194153\epsilon + 673404688332712109 \\ q_2 &= 1148714815680333640\epsilon^2 + 423917326839288390\epsilon + 503765461488992377 \\ q_3 &= 734788579677917913\epsilon^2 + 689260085345531 54\epsilon + 77740516941101348 \\ q_4 &= 750968410676713515\epsilon^2 + 683426730428696431\epsilon + 823046869633863637 \\ Q_1 &= (q_1 : \ q_2 : \ 1) \in C/k_3, \ Q_2 = (q_3 : \ q_4 : \ 1) \in C/k_3 \end{aligned}$$

$$\chi(mP) = D_{mP} + {}^{\sigma}D_{mP} + {}^{\sigma^2}D_{mP}$$

$$\begin{aligned} {}^{\sigma}D_{mP} &= {}^{\sigma}Q_1 + {}^{\sigma}Q_2, \ {}^{\sigma^2}D_{mP} = {}^{\sigma^2}Q_1 + {}^{\sigma^2}Q_2 \\ {}^{\sigma}Q_1 &= ({q_1}^q : \ {q_2}^q : \ 1), \ {}^{\sigma}Q_2 = ({q_3}^q : \ {q_4}^q : \ 1) \\ {}^{\sigma^2}Q_1 &= ({q_1}^{q^2} : \ {q_2}^{q^2} : \ 1), \ {}^{\sigma^2}Q_2 = ({q_3}^{q^2} : \ {q_4}^{q^2} : \ 1) \end{aligned}$$

Calculations from mP_E to $\chi(mP)$ take 11.281 seconds.

In fact, given $\{2^i P_E | 0 \leq i \leq 999\}$, the average time to find $\chi(2^i P)$ is 23.155937 seconds.

6 Conclusion

We shown two algorithms to implement the GHS attack against elliptic curve cryptosystems over cubic extension fields of odd characteristics and the results of the computer simulation. The first algorithm is to build definition equation of the nonhyperelliptic covering C/k of the elliptic curve C_0/k_3. The second algorithm transfers explicitly the DLP over C_0/k to the DLP over $\mathrm{Jac}(C/k)$. These DLP over $\mathrm{Jac}(C/k)$ can be solved using Diem's double-large-prime algorithm.

References

[1] P. Gaudry, "An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves," *Advances in cryptology - EUROCRYPT 2000*, Springer-Verlag, LNCS1807, pages 19-34, 2000.

[2] K.Nagao "Improvement of Theriault algorithm of index calculus of Jacobian of hyperelliptic curves of small genus", preprint 2004.

[3] P. Gaudry, N. Thériault, E. Thomé, and C. Diem, "A double large prime variation for small genus hyperelliptic index calculus," Math. Comp. 76, pp.475–492, 2007.

[4] C. Diem, "Index calculus in class groups of plane curves of small degree," an extensive preprint from ANTS VII, 2005. Available from http://www.math.uni-leipzig.de/ diem/preprints/small-degree.ps

[5] G. Frey,"How to disguise an elliptic curve," Talk at the 2nd Elliptic Curve Cryptography Workshop, 1998.

[6] P. Gaudry, F. Hess and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves," J. Cryptol, 15, pp.19–46, 2002.

[7] A.Menezes, and M.Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart," Topics in Cryptology CT-RSA 2001, Springer-Verlag, LNCS 2020, pp.308-318, 2001.

[8] S.D.Galbraith "Weil descent of Jacobians," Discrete Applied Mathmatics, vol.128 no.1, pp.165-180, 2003.

[9] N.Thériault, "Weil descent attack for Kummer extensions," J.Ramanujan Math. Soc, vol.18, pp.281-312, 2003.

[10] N.Thériault, "Weil descent attack for Artin-Schreier curves," preprint, 2003, available at http://www.math.toronto.edu/ganita/papers/wdasc.pdf

[11] F.Hess, "The GHS attack revisited," Advances in cryptology EUROCRYPTO 2003, Springer-Verlag, LNCS 2656, pp.374-387, 2003.

[12] F.Hess, "Generalizing the GHS Attack on the Elliptic Curve Discrete Logarithm," LMS J. Comput. Math. vol.7, pp.167-192, 2004.

[13] C. Diem, "The GHS attack in odd characteristic," *J.Ramanujan Math*, Soc 18, pages.1-32, 2003.

[14] C. Diem and J. Sholten, “Cover attack,” preprint, 2003. Available from http://www.math.uni-leipzig.de/ diem/preprints/english.html

[15] H. Cohen, G. Frey(editors); R. Avanzi, C. Doche et al.(authors), *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall/CRC, 2005.

[16] F. Momose, J. Chao, “Scholten forms and elliptic/hyperelliptic curves with weak Weil restrictions,” preprint, 2005. http://eprint.iacr.org/2005/277

[17] F. Momose and J. Chao “Classification of Weil restrictions obtained by $(2,\dots,2)$ coverings of $\mathbb{P}^1$,” preprint, 2006. http://eprint.iacr.org/2006/347

[18] Jinhui Chao,”Elliptic and Hyperelliptic curves with Weak Covering against Weil descent attacks”, 2007 International Workshop on Elliptic Curve Cryptosystems, ECC2007, Sept., 2007.

Appendix: On condition (13) of hyperellipticity

Type I

By (13), $\beta = A\cdot\alpha = \dfrac{a\alpha+b}{c\alpha+d}$ $(a,\ b,\ c,\ d\ \in k)$. Combining with $\mathrm{Tr}A=0$, one has the following variation of the condition (13)

$$\begin{aligned} C \text{ is hyperelliptic} \quad &\iff \quad \beta = A\cdot\alpha,\ A\in \mathrm{GL}_2(k), \mathrm{Tr}A = 0 && (104)\\ &\iff \quad \text{Either (i) or (ii) is true.} \\ &\quad\ \ \left\{\begin{array}{l} \text{(i)}\ \ A = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix},\ \beta = A\cdot\alpha = \frac{a\alpha+b}{-a} = -\alpha - b', \\ \qquad\qquad\qquad\qquad\qquad \textit{or} \qquad \alpha+\beta = -b' \in k \\ \text{(ii)}\ \ A = \begin{pmatrix} a & b \\ 1 & -a \end{pmatrix},\ \beta = A\cdot\alpha = \frac{a\alpha+b}{\alpha-a} \end{array}\right. && (105) \end{aligned}$$

In particular, the condition (ii) means $\beta = \dfrac{a\alpha+b}{\alpha-a}$, or

$$\alpha\beta - (\alpha+\beta)a - b \ = \ 0 \tag{106}$$

Sine any element $l \in k_3$ can be expressed on a basis $\{1,\ \epsilon,\ \epsilon^2\}$ as

$$l = l_0 + l_1\epsilon + l_2\epsilon^2 \qquad l_0,\ l_1,\ l_2 \in k$$

assume

$$\alpha \ = \ \alpha_0 + \alpha_1\epsilon + \alpha_2\epsilon^2, \tag{107}$$
$$\beta \ = \ \beta_0 + \beta_1\epsilon + \beta_2\epsilon^2 \tag{108}$$

Then

$$\alpha\beta \ = \ (\alpha\beta)_0 + (\alpha\beta)_1\epsilon + (\alpha\beta)_2\epsilon^2 \tag{109}$$
$$-(\alpha+\beta)a \ = \ -(\alpha_0+\beta_0)a - (\alpha_1+\beta_1)a\epsilon - (\alpha_2+\beta_2)a\epsilon^2 \tag{110}$$

(106) becomes

$$\begin{aligned}
&\alpha\beta-(\alpha+\beta)a-b\\
=\ &\{(\alpha\beta)_0-(\alpha_0+\beta_0)a-b\}+\{(\alpha\beta)_1-(\alpha_1+\beta_1)a\}\epsilon+\{(\alpha\beta)_2-(\alpha_2+\beta_2)a\}\epsilon^2\\
=\ &0 \qquad (111)
\end{aligned}$$

Therefore condition (ii) can be replaced by existance of solutions in the following linear equations in $a,\ b$

$$\begin{cases} -(\alpha_0+\beta_0)a-b+(\alpha\beta)_0=0\\ -(\alpha_1+\beta_1)a+(\alpha\beta)_1=0\\ -(\alpha_2+\beta_2)a+(\alpha\beta)_2=0 \end{cases} \qquad (112)$$

When one wishes to find a nonhyperelliptic curve, the condition (13) has to be avoided. Therefore neither (i) nor (ii) should hold for α and β. This means

$$\overline{\text{(i)}} \qquad \alpha+\beta\notin k \qquad (113)$$

$$\overline{\text{(ii)}} \qquad \text{The system of equations } \begin{cases} -(\alpha_0+\beta_0)a-b+(\alpha\beta)_0=0\\ -(\alpha_1+\beta_1)a+(\alpha\beta)_1=0\\ -(\alpha_2+\beta_2)a+(\alpha\beta)_2=0 \end{cases} \qquad (114)$$

has no solution.

Define

$$B:=\begin{pmatrix} -(\alpha_0+\beta_0) & -1\\ -(\alpha_1+\beta_1) & 0\\ -(\alpha_2+\beta_2) & 0 \end{pmatrix},\ B':=\begin{pmatrix} -(\alpha_0+\beta_0) & -1 & -(\alpha\beta)_0\\ -(\alpha_1+\beta_1) & 0 & -(\alpha\beta)_1\\ -(\alpha_2+\beta_2) & 0 & -(\alpha\beta)_2 \end{pmatrix} \qquad (115)$$

$\overline{\text{(ii)}}$ holds if and only if $\operatorname{rank} B\neq\operatorname{rank} B'$.

In other words, to obtain a nonhyperelliptic covering curve C/k, one only needs to choose α and β such that $\alpha+\beta\notin k$ and $\operatorname{rank} B\neq\operatorname{rank} B'$.

Type II

For Type II case, since $\alpha+\beta=\mathrm{Tr}_{k_6/k_3}(\alpha),\ \alpha\beta=\mathrm{N}_{k_6/k_3}(\alpha)$, $\overline{\text{(i)}}$ and $\overline{\text{(ii)}}$ in Type I can be replaced by

$$\begin{cases} \overline{\text{(i)}} \qquad \mathrm{Tr}_{k_6/k_3}(\alpha)\notin k\\ \overline{\text{(ii)}} \qquad \text{the system of equations } \begin{cases} -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_0a-b+\{\mathrm{N}_{k_6/k_3}(\alpha)\}_0=0\\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_1a+\{\mathrm{N}_{k_6/k_3}(\alpha)\}_1=0\\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_2a+\{\mathrm{N}_{k_6/k_3}(\alpha)\}_2=0 \end{cases}\\ \qquad\quad \text{has no solutions.} \end{cases}$$

Define

$$B := \begin{pmatrix} -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_0 & -1 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_1 & 0 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_2 & 0 \end{pmatrix}, \ B' := \begin{pmatrix} -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_0 & -1 & -\{\mathrm{N}_{k_6/k_3}(\alpha)\}_0 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_1 & 0 & -\{\mathrm{N}_{k_6/k_3}(\alpha)\}_1 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_2 & 0 & -\{\mathrm{N}_{k_6/k_3}(\alpha)\}_2 \end{pmatrix} \tag{116}$$

then $\overline{\text{(ii)}}$ holds if and only if rank $B \neq$ rank B'.

Thus, to obtain a nonhyperelliptic covering for a Type II curve, one needs to choose α and β such that $\mathrm{Tr}_{k_6/k_3}(\alpha) \notin k$ and rank $B \neq$ rank B'.