# On implementation of GHS attack against elliptic curve cryptosystems over cubic extension fields of odd characteristic

Naoki Hashizume, Fumiyuki Momose, and Jinhui Chao

ABSTRACT. In this paper, we present algorithms implementing the GHS attack against Elliptic curve cryptosystems (ECC). In particular, we consider two large classes of elliptic curves over cubic extension fields of odd characteristic which have weak covering curves against GHS attack, whose existence have been shown recently [17], [18], [19], [20]. We give algorithms to compute the defining equation of the covering curve and to transfer the DLP from the elliptic curve to the Jacobian of the covering curve. An algorithm to test if the covering curve is hyperelliptic is also given in the appendix.

# 1. Introduction

Elliptic curve cryptography is known as a rich source of secure and efficient cryptosystems. In particular, it can provide the same level of security as RSA and ElGamal cryptosystems while using much shorter key length. This property is also desirable in implementation of compact and low cost cryptosystems. Against cryptosystems based on low genus algebraic curves, the fastest known attacks (in general) are "square-root" attacks such as the baby-step giant-step attack, Pollard's rho and lambda algorithms. Recently, index calculus attacks have been proposed by Gaudry, Nagao, Gaudry-Thériault-Thomé-Diem [1], [2], [3] for hyperelliptic curves of genera larger than 3 and by Diem [4] for non-hyperelliptic curves of genera larger than or equal to 3.

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 transfers 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 already been investigated extensively. However, although theoretically interesting, its analysis seemed nontrivial [7], [8] [9], [10], [11], [12], [13], [14], [15], [16]. The classes of the weak elliptic curves or curves for which the GHS attack efficiently works have not yet been fully understood. At the beginning,

<sup>2010</sup> Mathematics Subject Classification. Primary 14G50,11T71, Secondary 11G25, 94A60. Key words and phrases. Elliptic curve cryptosystems, Discrete logarithm problem, GHS attack.

it seemed that the class of curves subjected to the GHS attack must be special so the number of such curves will not be very large. Recently, the existence of certain large classes of elliptic and hyperelliptic curves which are weak against GHS was shown [17], [18], [19], [20]. Further results on the subject can be found in [21], [22], [23].

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

A GHS attack consists of three steps: finding a covering curve C/k of an elliptic curve  $E/k_d$  where  $k_d$  is the degree d extension of a finite field k; transferring the discrete logarithm on  $E/k_d$  to the Jacobian J(C)/k; and finally, applying an index calculus algorithm to solve the discrete logarithm in J(C)/k. As to the first step, it seems to be nontrivial to find the defining equation of a weak curve  $E/k_d$ . Certain cases were discussed in [14], [15], [17]. For the second step, although a general strategy using norm-conorm map is well known, efficient and explicit implementation of the strategy does not seem to be available and appear to be nontrivial.

In this paper, we show explicit procedures for the first two steps of the GHS attack against two large classes of the elliptic curves over cubic extension fields of odd characteristic. These two classes, called Type I and Type II curves have been obtained in [17][18][19][20], both of them have non-hyperelliptic covering curves of genus three, which are subjected to Diem's double-large-prime attack. We present an algorithm to explicitly construct these covering curves C over k from the elliptic curves E over the cubic extension of k with odd characteristic. Then an algorithm is given to map the rational point on the elliptic curve E to the divisor of the covering curve C, in order to transfer the DLP. In the appendix, we also present an algorithm to test if a Type I or II curve is hyperellipic. These algorithms are implemented and examples are shown.

The first and third authors would like to dedicate the publication of this work to their friend, colleague, and collaborator, Fumiyuki Momose.

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

$$(2.1) \qquad \qquad \pi/k_d: C \longrightarrow C_0$$

is a covering defined over  $k_d$ , which induces the map

(2.2) 
$$\pi_*/k_d : \operatorname{Jac}(C) \longrightarrow \operatorname{Jac}(C_0).$$

Also assume the restriction of  $\pi_*$  onto k

(2.3) 
$$\operatorname{Re}(\pi_*)/k : \operatorname{Jac}(C) \longrightarrow \operatorname{Re}_{k_d/k}(\operatorname{Jac}(C_0))$$

defines an isogeny over k. Then C has genus  $g(C) = dg_0$ . Here,  $\operatorname{Re}_{k_d/k}(\operatorname{Jac}(C_0))$  is the Weil restriction of  $\operatorname{Jac}(C_0)$  with respect to extension field  $k_d/k$ . Throughout this paper, we will assume that  $g_0 = 1$ , d = 3,  $char(k) \neq 2$ .

According to [17][18][19][20], the elliptic curves  $C_0$  which have weak covering C as genus three nonhyperelliptic curves can be divided into two types.

(2.4) 
$$C_0/k_3: y^2 = (x - \alpha)(x - \alpha^q)(x - \beta)(x - \beta^q)$$

(2.5) Type I: 
$$\alpha, \beta \in k_3 \setminus k, \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4$$

(2.6) Type II: 
$$\alpha \in k_6 \setminus (k_2 \cup k_3), \ \beta = \alpha^{q^3}$$

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

• Type I:

(2.7) 
$$C_0/k_3: y^2 = x(x-1)(x-\lambda), \ \lambda = \frac{(\beta - \alpha^q)(\beta^q - \alpha)}{(\beta - \alpha)(\beta^q - \alpha^q)}$$

• Type II:

(2.8) 
$$C_0/k_3: y^2 = N_{k_6/k_3}(\beta - \alpha^q)x(x-1)(x-\lambda), \ \lambda = N_{k_6/k_3}\left(\frac{\alpha^q - \alpha}{\alpha^q - \beta}\right)$$

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  $\tilde{O}(q)$ .

Here we use  $M \cdot \gamma$  to denote a  $PGL_2$ -action as follows.

(2.9) 
$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(k), \quad \gamma \in \overline{k} \qquad M \cdot \gamma := \frac{a\gamma + b}{c\gamma + d}$$

Now, define

(2.10) 
$$\mu := \begin{pmatrix} \alpha^q & -\alpha \\ 1 & -1 \end{pmatrix} \cdot \lambda,$$
$$\begin{pmatrix} -\mu + \alpha + \alpha^q & -\alpha^{1+q} \end{pmatrix}$$

(2.11) 
$$A := \begin{pmatrix} -\mu + \alpha + \alpha^q & -\alpha^{1+q} \\ 1 & -\mu \end{pmatrix}$$

$$(2.12) B := {}^{\sigma}A {}^{\sigma}A A$$

According to Lemma 7, 1,2 [20], the necessary and sufficient condition for  $C_0$  to be Type I is that the quadratic equation

$$(2.13) B \cdot \beta = \beta$$

has a solution  $\beta$ .

Besides, by Lemma 4 [20], the covering curve C of such a curve  $C_0$  is hyperelliptic if and only if

(2.14) 
$$\beta = A \cdot \alpha, \ \exists A \in \operatorname{GL}_2(k), \ \operatorname{Tr} A = 0.$$

Hereafter we assume that  $\alpha$  and  $\beta$  do not satisfy Condition (2.14). 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 describe the following two algorithms:

(i) To construct the curve C/k, or to find the defining equation explicitly from the given curve  $C_0/k_d$ .

(ii) To transfer 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  $g = dg_0 = 3$ . Thus, its canonical embedding is a quartic curve in  $\mathbb{P}^2$ . Let  $\sigma$  be a q-th power Frobenius map satisfying

(3.1) 
$$l(x) = \sum_{i=1}^{n} a_i x^i \quad \longmapsto \quad {}^{\sigma} l(x) = \sum_{i=1}^{n} a_i {}^{q} x^i \qquad ({}^{\forall} l(x) \in k_d[x]).$$

The embedding map is

(3.3) 
$$P \longmapsto \left(\omega(P): {}^{\sigma}\omega(P): {}^{\sigma^2}\omega(P)\right)$$

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

(3.4) 
$$H^0(C/k_3, \Omega^1) = \langle \omega, \sigma^2 \omega \rangle.$$

We use hereafter the correspondence

(3.5) 
$$\omega \longleftrightarrow X, \quad {}^{\sigma}\omega \longleftrightarrow Y, \quad {}^{\sigma^2}\omega \longleftrightarrow Z.$$

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

(3.6) 
$$Aut(H^0(C/k_3, \Omega^1)) = \{id, \phi, {}^{\sigma}\phi, {}^{\sigma^2}\phi\}.$$

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

$$(3.7) id: \begin{cases} X & \longmapsto & X \\ Y & \longmapsto & Y \\ Z & \longmapsto & Z \end{cases}.$$

The bi-elliptic involution changes the signs of both Y and Z

(3.8) 
$$\phi : \begin{cases} X & \mapsto & X \\ Y & \longmapsto & -Y \\ Z & \longmapsto & -Z \end{cases}$$

Then the bi-elliptic involution under the Galois action of  $\sigma$  has the following form

(3.9) 
$${}^{\sigma}\phi: \left\{ \begin{array}{ccc} X & \longmapsto & -X \\ Y & \longmapsto & Y \\ Z & \longmapsto & -Z \end{array} \right.,$$

and the bi-elliptic involution under the action of  $\sigma^2$  has the following form

(3.10) 
$$\sigma^{2}\phi: \begin{cases} X & \longmapsto & -X \\ Y & \longmapsto & -Y \\ Z & \longmapsto & Z \end{cases}$$

Licensed to AMS.

**3.1. Defining equation of**  $C/k_3$ . The quartic curve  $C/k_3$  has its defining equation invariant under  $\text{Gal}(k_3/k)$ , thus in the following symmetric form.

(3.11) 
$$C/k_{3} : aX^{4} + a^{q}Y^{4} + a^{q^{2}}Z^{4} +bX^{3}Y + b^{q}Y^{3}Z + b^{q^{2}}Z^{3}X +cX^{3}Z + c^{q}Y^{3}X + c^{q^{2}}Z^{3}Y +dX^{2}Y^{2} + d^{q}Y^{2}Z^{2} + d^{q^{2}}Z^{2}X^{2} +eX^{2}YZ + e^{q}XY^{2}Z + e^{q^{2}}XYZ^{2} = 0.$$

Since the defining equation F = 0 of C is invariant under the action of automorphisms of Aut $(H^0(C, \Omega^1))$ , C will also be defined by  $F + \phi(F) + {}^{\sigma}\phi(F) + {}^{\sigma^2}\phi(F) = 0$ .

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

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

(3.12) 
$$C/k_3: aX^4 + a^qY^4 + a^{q^2}Z^4 + bX^2Y^2 + b^qY^2Z^2 + b^{q^2}Z^2X^2 = 0.$$
  
 $a, b \in k_3$ 

**3.2. Evaluation of** a and b. To find the coefficients a and b in (3.12), we substitute into it  $X = \frac{dx}{y}$ ,  $Y = \frac{dx}{\sigma_y}$ ,  $Z = \frac{dx}{\sigma^2_y}$ .

Since

(3.13) 
$$\frac{1}{y^2} = \frac{(x - \alpha^{q^2})(x - \beta^{q^2})}{N_{k_3/k}((x - \alpha)(x - \beta))},$$

(3.14) 
$$\frac{1}{(\sigma y)^2} = \frac{(x-\alpha)(x-\beta)}{N_{k_3/k}((x-\alpha)(x-\beta))}$$

we substitute these into (3.12) to obtain

(3.15) 
$$\operatorname{Tr}_{k_{3}/k}(a(x-\alpha^{q^{2}})^{2}(x-\beta^{q^{2}})^{2}) + \\\operatorname{Tr}_{k_{3}/k}(b(x-\alpha)(x-\alpha^{q^{2}})(x-\beta)(x-\beta^{q^{2}})) = 0.$$

3.2.1. Type I. From expansion of (3.15) we can express the coefficients of each  $x^i$  as

$$\begin{aligned} x^{4} &: \operatorname{Tr}(a) + \operatorname{Tr}(b) \\ x^{3} &: -2\operatorname{Tr}(a(\alpha^{q^{2}} + \beta^{q^{2}})) - \operatorname{Tr}(b(\alpha + \beta + \alpha^{q^{2}} + \beta^{q^{2}})) \\ x^{2} &: \operatorname{Tr}(a(\alpha^{2q^{2}} + 4\alpha^{q^{2}}\beta^{q^{2}} + \beta^{2q^{2}})) + \operatorname{Tr}(b\{\alpha^{q^{2}+1} + (\alpha + \alpha^{q^{2}})(\beta + \beta^{q^{2}}) + \beta^{q^{2}+1}\}) \\ x &: -2\operatorname{Tr}(a(\alpha^{2q^{2}}\beta^{q^{2}} + \alpha^{q^{2}}\beta^{2q^{2}})) - \operatorname{Tr}(b\{\alpha^{q^{2}+1}(\beta + \beta^{q^{2}}) + \beta^{q^{2}+1}(\alpha + \alpha^{q^{2}})\}) \\ 1 &: \operatorname{Tr}(a\alpha^{2q^{2}}\beta^{2q^{2}}) + \operatorname{Tr}(b\alpha^{q^{2}+1}\beta^{q^{2}+1}) \end{aligned}$$

which are identically zeros.

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

(3.16) 
$$a = a_0 + a_1 \epsilon + a_2 \epsilon^2 \ (a_0, \ a_1, \ a_2 \in k)$$

(3.17) 
$$b = b_0 + b_1 \epsilon + b_2 \epsilon^2 \ (b_0, \ b_1, \ b_2 \in k)$$

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

Belows, we express the coefficients of  $x^i$  in (3.15) in terms of  $a_i, b_i$ .

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

(3.18) 
$$\operatorname{Tr}(a) = 3a_0 + \operatorname{Tr}(\epsilon)a_1 + \operatorname{Tr}(\epsilon^2)a_2.$$

Similarly,

(3.19) 
$$\operatorname{Tr}(b) = 3b_0 + \operatorname{Tr}(\epsilon)b_1 + \operatorname{Tr}(\epsilon^2)b_2.$$

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

$$(3.20) \operatorname{Tr}(a(\alpha^{q^{2}} + \beta^{q^{2}})) = (\alpha^{q^{2}} + \beta^{q^{2}})(a_{0} + a_{1}\epsilon + a_{2}\epsilon^{2}) + (\alpha + \beta)(a_{0} + a_{1}\epsilon^{q} + a_{2}\epsilon^{2q}) + (\alpha^{q} + \beta^{q})(a_{0} + a_{1}\epsilon^{q^{2}} + a_{2}\epsilon^{2q^{2}}) = \operatorname{Tr}(\alpha + \beta)a_{0} + \operatorname{Tr}((\alpha + \beta)\epsilon^{q})a_{1} + \operatorname{Tr}((\alpha + \beta)\epsilon^{2q})a_{2}.$$

$$\begin{aligned} \operatorname{Tr}(b(\alpha+\beta+\alpha^{q^2}+\beta^{q^2})) & \text{ is given by} \\ (3.21) \quad \operatorname{Tr}(b(\alpha+\beta+\alpha^{q^2}+\beta^{q^2})) &= (\alpha+\beta+\alpha^{q^2}+\beta^{q^2})(b_0+b_1\epsilon+b_2\epsilon^2) \\ &+ (\alpha^q+\beta^q+\alpha+\beta)(b_0+b_1\epsilon^q+b_2\epsilon^{2q}) \\ &+ (\alpha^{q^2}+\beta^{q^2}+\alpha^q+\beta^q)(b_0+b_1\epsilon^{q^2}+b_2\epsilon^{2q^2}) \\ &= \operatorname{Tr}(\alpha^q+\beta^q+\alpha+\beta)b_0+\operatorname{Tr}((\alpha^q+\beta^q+\alpha+\beta)\epsilon^q)b_1 \\ &+ \operatorname{Tr}((\alpha^q+\beta^q+\alpha+\beta)\epsilon^{2q})b_2. \end{aligned}$$

In the coefficient of  $x^2$ ,  $\operatorname{Tr}(a(\alpha^{2q^2} + 4\alpha^{q^2}\beta^{q^2} + \beta^{2q^2}))$  is given by (3.22)  $\operatorname{Tr}(a(\alpha^{2q^2} + 4\alpha^{q^2}\beta^{q^2} + \beta^{2q^2})) = \operatorname{Tr}(\alpha^2 + 4\alpha\beta + \beta^2)a_0 + \operatorname{Tr}((\alpha^2 + 4\alpha\beta + \beta^2)\epsilon^{q})a_1 + \operatorname{Tr}((\alpha^2 + 4\alpha\beta + \beta^2)\epsilon^{2q})a_2)$ 

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

(3.23) 
$$\operatorname{Tr}(b\{\alpha^{q^{2}+1} + (\alpha + \alpha^{q^{2}})(\beta + \beta^{q^{2}}) + \beta^{q^{2}+1}\}) = \operatorname{Tr}(\alpha^{q+1} + (\alpha^{q} + \alpha)(\beta^{q} + \beta) + \beta^{q+1})b_{0} + \operatorname{Tr}(\{\alpha^{q+1} + (\alpha^{q} + \alpha)(\beta^{q} + \beta) + \beta^{q+1}\}\epsilon^{q})b_{1} + \operatorname{Tr}(\{\alpha^{q+1} + (\alpha^{q} + \alpha)(\beta^{q} + \beta) + \beta^{q+1}\}\epsilon^{2q})b_{2}$$

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

(3.24) 
$$\operatorname{Tr}(a(\alpha^{2q^{2}}\beta^{q^{2}} + \alpha^{q^{2}}\beta^{2q^{2}})) = \operatorname{Tr}(\alpha^{2}\beta + \alpha\beta^{2})a_{0} + \operatorname{Tr}((\alpha^{2}\beta + \alpha\beta^{2})\epsilon^{q})a_{1} + \operatorname{Tr}((\alpha^{2}\beta + \alpha\beta^{2})\epsilon^{2q})a_{2}.$$

and  $\operatorname{Tr}(b\{\alpha^{q^{2}+1}(\beta+\beta^{q^{2}})+\beta^{q^{2}+1}(\alpha+\alpha^{q^{2}})\})$  is given by (3.25)  $\operatorname{Tr}(b\{\alpha^{q^{2}+1}(\beta+\beta^{q^{2}})+\beta^{q^{2}+1}(\alpha+\alpha^{q^{2}})\}) =$   $\operatorname{Tr}(\alpha^{q}\beta^{q}(\alpha+\beta)+\alpha\beta(\alpha^{q}+\beta^{q}))b_{0}$   $+\operatorname{Tr}(\{\alpha^{q}\beta^{q}(\alpha+\beta)+\alpha\beta(\alpha^{q}+\beta^{q})\}\epsilon^{q})b_{1}$  $+\operatorname{Tr}(\{\alpha^{q}\beta^{q}(\alpha+\beta)+\alpha\beta(\alpha^{q}+\beta^{q})\}\epsilon^{2q})b_{2}.$ 

In the constant term of (3.15),  $\operatorname{Tr}(a\alpha^{2q^2}\beta^{2q^2})$  is given by (3.26)  $\operatorname{Tr}(a\alpha^{2q^2}\beta^{2q^2}) = \operatorname{Tr}(\alpha^2\beta^2)a_0 + \operatorname{Tr}(\alpha^2\beta^2\epsilon^q)a_1 + \operatorname{Tr}(\alpha^2\beta^2\epsilon^{2q})a_2.$ 

130

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

(3.27) 
$$\operatorname{Tr}(b\alpha^{q^{2}+1}\beta^{q^{2}+1}) = \operatorname{Tr}(\alpha^{q+1}\beta^{q+1})b_{0} + \operatorname{Tr}(\alpha^{q+1}\beta^{q+1}\epsilon^{q})b_{1} + \operatorname{Tr}(\alpha^{q+1}\beta^{q+1}\epsilon^{2q})b_{2}$$

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

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

From the equation (3.12), we can assume  $a_0 = 1$ . Accordingly, the simultaneous linear equations can be written as

$$(3.28) \qquad \begin{pmatrix} d_{11} & d_{12} & d_{13} & d_{14} & d_{15} \\ d_{21} & d_{22} & d_{23} & d_{24} & d_{25} \\ d_{31} & d_{32} & d_{33} & d_{34} & d_{35} \\ d_{41} & d_{42} & d_{43} & d_{44} & d_{45} \\ d_{51} & d_{52} & d_{53} & d_{54} & d_{55} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ b_0 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{pmatrix}.$$

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

Thus  $a_1$ ,  $a_2$ ,  $b_0$ ,  $b_1$ ,  $b_2$  can be obtained by solving the linear system of equations for the given set of  $\alpha$ ,  $\beta$  and  $\epsilon$ .

3.2.2. Type II. For Type II curves, the coefficients of  $x^i$  in Equation (3.15) are as follows.

First, the coefficient of  $x^4$  is

(3.29) 
$$\operatorname{Tr}(a) + \operatorname{Tr}(b) = 3a_0 + \operatorname{Tr}(\epsilon)a_1 + \operatorname{Tr}(\epsilon^2)a_2 + 3b_0 + \operatorname{Tr}(\epsilon)b_1 + \operatorname{Tr}(\epsilon^2)b_2 = 0.$$

Next, the coefficient of  $x^3$  is as follows:

$$\begin{aligned} (3.30) \ 2 \mathrm{Tr}(a(\alpha^{q^2} + \beta^{q^2})) + \mathrm{Tr}(b(\alpha + \beta + \alpha^{q^2} + \beta^{q^2})) &= 2 \mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha))a_0 \\ &+ 2 \mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\epsilon^q)a_1 \\ &+ 2 \mathrm{Tr}(\mathrm{Tr}_{k_6/k_3}(\alpha)\epsilon^{2q})a_2 \\ &+ \mathrm{Tr}(\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q + \mathrm{Tr}_{k_6/k_3}(\alpha))b_0 \\ &+ \mathrm{Tr}(\left[\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q + \mathrm{Tr}_{k_6/k_3}(\alpha)\right]\epsilon^q)b_1 \\ &+ \mathrm{Tr}(\left[\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q + \mathrm{Tr}_{k_6/k_3}(\alpha)\right]\epsilon^{2q})b_2 = 0. \end{aligned}$$

The coefficient of  $x^2$  is

$$\begin{aligned} (3.31) \ &\operatorname{Tr}(a(\alpha^{2q^2} + 4\alpha^{q^2}\beta^{q^2} + \beta^{2q^2})) + \\ &\operatorname{Tr}(b\{\alpha^{q^2+1} + (\alpha + \alpha^{q^2})(\beta + \beta^{q^2}) + \beta^{q^2+1}\}) \\ &= \operatorname{Tr}(\{\operatorname{Tr}_{k_6/k_3}(\alpha)\}^2 + 2\operatorname{N}_{k_6/k_3}(\alpha))a_0 \\ &+ \operatorname{Tr}([\{\operatorname{Tr}_{k_6/k_3}(\alpha)\}^2 + 2\operatorname{N}_{k_6/k_3}(\alpha)]\epsilon^q)a_1 \\ &+ \operatorname{Tr}([\operatorname{Tr}_{k_6/k_3}(\alpha)^2 + 2\operatorname{N}_{k_6/k_3}(\alpha)]\epsilon^{2q})a_2 \\ &+ \operatorname{Tr}(\{\operatorname{Tr}_{k_6/k_3}(\alpha)\}^{q+1} + \{\operatorname{N}_{k_6/k_3}(\alpha)\}^q + \operatorname{N}_{k_6/k_3}(\alpha))b_0 \\ &+ \operatorname{Tr}([\{\operatorname{Tr}_{k_6/k_3}(\alpha)\}^{q+1} + \{\operatorname{N}_{k_6/k_3}(\alpha)\}^q + \operatorname{N}_{k_6/k_3}(\alpha)]\epsilon^q)b_1 \\ &+ \operatorname{Tr}([\{\operatorname{Tr}_{k_6/k_3}(\alpha)\}^{q+1} + \{\operatorname{N}_{k_6/k_3}(\alpha)\}^q + \operatorname{N}_{k_6/k_3}(\alpha)]\epsilon^{2q})b_2 = 0. \end{aligned}$$

The coefficient of 
$$x$$
 is

$$(3.32) 2 \operatorname{Tr}(a(\alpha^{2q^{2}}\beta^{q^{2}} + \alpha^{q^{2}}\beta^{2q^{2}})) + \operatorname{Tr}(b\{\alpha^{q^{2}+1}(\beta + \beta^{q^{2}}) + \beta^{q^{2}+1}(\alpha + \alpha^{q^{2}})\}) = 2 \operatorname{Tr}(\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\operatorname{N}_{k_{6}/k_{3}}(\alpha))a_{0} + 2 \operatorname{Tr}(\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\operatorname{N}_{k_{6}/k_{3}}(\alpha)e^{q})a_{1} + 2 \operatorname{Tr}(\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\operatorname{N}_{k_{6}/k_{3}}(\alpha)e^{2q})a_{2} + \operatorname{Tr}(\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\{\operatorname{N}_{k_{6}/k_{3}}(\alpha)\}^{q} + \{\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\}^{q}\operatorname{N}_{k_{6}/k_{3}}(\alpha))b_{0} + \operatorname{Tr}([\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\{\operatorname{N}_{k_{6}/k_{3}}(\alpha)\}^{q} + \{\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\}^{q}\operatorname{N}_{k_{6}/k_{3}}(\alpha)]\epsilon^{q})b_{1} + \operatorname{Tr}([\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\{\operatorname{N}_{k_{6}/k_{3}}(\alpha)\}^{q} + \{\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\}^{q}\operatorname{N}_{k_{6}/k_{3}}(\alpha)]\epsilon^{2q})b_{2} = 0.$$

The constant term of (3.15) for Type II curves is

$$(3.33) \qquad \operatorname{Tr}(a\alpha^{2q^{2}}\beta^{2q^{2}}) + \operatorname{Tr}(b\alpha^{q^{2}+1}\beta^{q^{2}+1}) = \\ \operatorname{Tr}(\{\mathbf{N}_{k_{6}/k_{3}}(\alpha)\}^{2})a_{0} + \operatorname{Tr}(\{\mathbf{N}_{k_{6}/k_{3}}(\alpha)\}^{2}\epsilon^{q})a_{1} \\ + \operatorname{Tr}(\{\mathbf{N}_{k_{6}/k_{3}}(\alpha)\}^{2}\epsilon^{2q})a_{2} + \operatorname{Tr}(\{\mathbf{N}_{k_{6}/k_{3}}(\alpha)\}^{q+1})b_{0} \\ + \operatorname{Tr}(\{\mathbf{N}_{k_{6}/k_{3}}(\alpha)\}^{q+1}\epsilon^{q})b_{1} + \operatorname{Tr}(\{\mathbf{N}_{k_{6}/k_{3}}(\alpha)\}^{q+1}\epsilon^{2q})b_{2} = 0.$$

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

(3.34) 
$$\omega = \gamma \omega_1 + \delta \omega_2 + \psi \omega_3, \ \exists \gamma, \ \delta, \ \psi \in k_3$$
(2.25) such that  $\det(U)$  ( 0, where  $U$ ,  $\begin{pmatrix} \gamma & \delta & \psi \\ \gamma^q & \delta^q & \gamma^{\prime q} \end{pmatrix}$ 

(3.35) such that 
$$\det(U) \neq 0$$
. where  $U := \begin{pmatrix} \gamma^q & \delta^q & \psi^q \\ \gamma^{q^2} & \delta^{q^2} & \psi^{q^2} \end{pmatrix}$ 

We will use the following correspondence.

$$(3.36) \qquad \qquad \omega_1 \longleftrightarrow \underline{x}, \quad \omega_2 \longleftrightarrow \underline{y}, \quad \omega_3 \longleftrightarrow \underline{z}$$

Then X, Y, Z are expressed as

(3.37) 
$$\begin{cases} X = \gamma \underline{x} + \delta \underline{y} + \psi \underline{z} \\ Y = \gamma^{q} \underline{x} + \delta^{\overline{q}} \underline{y} + \psi^{q} \underline{z} \\ Z = \gamma^{q^{2}} \underline{x} + \delta^{\overline{q}^{2}} \underline{y} + \psi^{q^{2}} \underline{z} \end{cases}$$

or

(3.38) 
$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = U \begin{pmatrix} \frac{x}{y} \\ \frac{z}{z} \end{pmatrix}.$$

Given  $\gamma$ ,  $\delta$ ,  $\psi$ , one substitutes (3.37) into (3.12) to obtain a definition equation of the curve C/k as

$$\begin{array}{rcl} (3.39) \ C/k: & \operatorname{Tr}(a\gamma^4 + b\gamma^{2q+2})\underline{x}^4 \\ & +\operatorname{Tr}(4a\gamma^3\delta + \{2\gamma^{q+2}\delta^q + 2\gamma^{2q+1}\delta\}b)\underline{x}^3\underline{y} \\ & +\operatorname{Tr}(4a\gamma^3\phi + \{2\gamma^{q+2}\psi^q + 2\gamma^{2q+1}\psi\}b)\underline{x}^3\underline{z} \\ & +\operatorname{Tr}(6a\gamma^2\delta^2 + \{\gamma^2\delta^{2q} + \gamma^{2q}\delta^2 + 4\gamma^{q+1}\delta^{q+1}\}b)\underline{x}^2\underline{y}^2 \\ & +\operatorname{Tr}(12a\gamma^2\delta\psi + \{2\gamma^2\delta^q\psi^q + 4\gamma^{q+1}\delta\psi^q + 2\gamma^{2q}\delta\psi + 4\gamma^{q+1}\delta^q\psi\}b)\underline{x}^2\underline{y}\underline{z} \\ & +\operatorname{Tr}(6a\gamma^2\psi^2 + \{\gamma^2\psi^{2q} + \gamma^{2q}\psi^2 + 4\gamma^{q+1}\psi^{q+1}\}b)\underline{x}^2\underline{z}^2 \\ & +\operatorname{Tr}(4a\gamma\delta^3 + \{2\gamma^q\delta^{q+2} + 2\gamma\delta^{2q+1}\}b)\underline{x}\underline{y}^3 \\ & +\operatorname{Tr}(12a\gamma\delta\psi^2 + \{2\gamma^q\delta^q\psi^2 + 2\gamma\delta\psi^{2q} + 4\gamma^q\delta\psi^{q+1} + 4\gamma\delta^q\psi^{q+1}\}b)\underline{x}\underline{y}\underline{z}^2 \\ & +\operatorname{Tr}(12a\gamma\delta\psi^2 + \{2\gamma^q\delta^q\psi^{q+2} + 2\gamma\delta\psi^{2q+1}\}b)\underline{x}\underline{z}^3 \\ & +\operatorname{Tr}(4a\gamma\psi^3 + \{2\gamma^q\psi^{q+2} + 2\gamma\psi^{2q+1}\}b)\underline{x}\underline{z}^3 \\ & +\operatorname{Tr}(4a\delta^3\psi + \{2\delta^{q+2}\psi^q + 2\delta^{2q+1}\psi\}b)\underline{y}^3\underline{z} \\ & +\operatorname{Tr}(4a\delta\psi^3 + \{2\delta^q\psi^{q+2} + 2\delta\psi^{2q+1}\}b)\underline{y}\underline{z}^3 \\ & +\operatorname{Tr}(4a\delta\psi^3 + \{2\delta^q\psi^{q+2} + 2\delta\psi^{2q+1}\}b)\underline{y}\underline{z}^3 \\ & +\operatorname{Tr}(a\psi^4 + b\psi^{2q+2})\underline{z}^4 \\ & = 0. \end{array}$$

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

Define

(3.40) 
$$\omega_1 = \omega + {}^{\sigma}\omega + {}^{\sigma^2}\omega$$

(3.41) 
$$\omega_2 = \epsilon \omega + \epsilon^{q \sigma} \omega + \epsilon^{q^2 \sigma^2} \omega$$

(3.42) 
$$\omega_3 = \epsilon^2 \omega + \epsilon^{2q} \sigma \omega + \epsilon^{2q^2} \sigma^2 \omega$$

Then

(3.43) 
$$\begin{pmatrix} \frac{x}{y} \\ \frac{y}{z} \end{pmatrix} = V \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

The Vandermonde's matrix

(3.44) 
$$V = \begin{pmatrix} 1 & 1 & 1 \\ \epsilon & \epsilon^q & \epsilon^{q^2} \\ \epsilon^2 & \epsilon^{2q} & \epsilon^{2q^2} \end{pmatrix}$$

has its determinant as

(3.45) det(V) =  $N(\epsilon - \epsilon^q) = (\epsilon - \epsilon^q)(\epsilon^q - \epsilon^{q^2})(\epsilon^{q^2} - \epsilon) = N(\epsilon - \epsilon^q) \neq 0$ then  $\{\omega_i\}$  is a basis of  $H^0(C/k, \Omega^1)$ . We can take  $U = V^{-1}$  or

(3.46) 
$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = U \begin{pmatrix} \frac{x}{y} \\ \frac{y}{z} \end{pmatrix}$$

and the inverse matrix can be expressed by

(3.47) 
$$U = V^{-1} = \begin{pmatrix} \gamma & \delta & \psi \\ \gamma^q & \delta^q & \psi^q \\ \gamma^{q^2} & \delta^{q^2} & \psi^{q^2} \end{pmatrix}.$$

Thus, one has

(3.48) 
$$\gamma = \frac{\epsilon^{2q^2+q} - \epsilon^{q^2+2q}}{\det(V)}, \ \delta = \frac{\epsilon^{2q} - \epsilon^{2q^2}}{\det(V)} \text{ and } \psi = \frac{\epsilon^{q^2} - \epsilon^q}{\det(V)}.$$

Now we have  $a, b, \underline{x}, \underline{y}, \underline{z}$  and  $\gamma, \delta, \psi$  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 is usually assumed to follow the normconorm map. However, previous works on the subject do not give this map explicitly and its description is not trivial. Here we use the 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  $\pi^*$  the pullback map induced by the cover map  $\pi/k_3$ :  $C \to C_0$ . i.e.,

(4.1) 
$$\pi^*: \operatorname{Jac}(C_0/k_3) \to \operatorname{Jac}(C/k_3)$$
$$P - P_0 \mapsto D_P - D_{P_0}$$

where  $P - P_0$  is a divisor of  $\text{Jac}(C_0/k_3)$  and  $D_P = \sum_i e_i Q_i$  a divisor of  $\text{Jac}(C/k_3)$ 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.

134

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

(4.2) 
$$\operatorname{Tr}_{k_3/k}: \operatorname{Jac}(C/k_3) \to \operatorname{Jac}(C/k)$$
$$D_P \mapsto D_P + {}^{\sigma}D_P + {}^{\sigma^2}D_P$$

which corresponds to the norm map of the function fields.

Then the transfer map is a homomorphism defined by the composition of  $\pi^*$  with the trace map

(4.3) 
$$\chi := \operatorname{Tr}_{k_3/k} \circ \pi^* : \operatorname{Jac}(C_0/k_3) \longrightarrow \operatorname{Jac}(C/k).$$

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 consists in finding an integer  $\lambda$  such that  $P_2 = \lambda P_1$ . Since the group of points on  $C_0$  and the group  $\operatorname{Jac}(C_0)$  are isomorphic, we can transfer from  $P_2 = \lambda P_1$  to

(4.4) 
$$(P_2 - P_\infty) = \lambda (P_1 - P_\infty)$$

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

Finally, the homomorphism  $\chi$  transfers the above discrete logarithm to the discrete logarithm on  $\operatorname{Jac}(C/k)$  which is to find  $\lambda$  such that

(4.5) 
$$(\chi(P_2) - \chi(P_\infty)) = \lambda(\chi(P_1) - \chi(P_\infty)).$$

So, it suffices to find  $\pi$ .

In fact,  $\pi$  can be factored into

(4.6) 
$$\pi/k_3 = \pi_1 \circ \pi_2$$

where  $\pi_1/k_3$  is the map from  $C/k_3$  defined by (3.12) to  $C_0/k_3$  and  $\pi_2/k_3$  is an isomorphism from  $C/k_3$  defined by the equation (3.39) of C/k to  $C/k_3$  defined by (3.12), which can be represented by (3.46) where the matrix U is known.

We find  $\pi_1$  as follows.

Let s, t be  $s = \frac{Y}{X}$ ,  $t = \frac{Z}{X}$  then (3.12) becomes

(4.7) 
$$C: \ a + a^q s^4 + a^{q^2} t^4 + b s^2 + b^q s^2 t^2 + b^{q^2} t^2 = 0.$$

Additionally let u, v be  $u = s^2, v = t^2$  then (4.7) becomes

(4.8) 
$$a + a^{q}u^{2} + a^{q^{2}}v^{2} + bu + b^{q}uv + b^{q^{2}}v = 0$$

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

Below, we first consider the case of Type I curves.

**4.1. Type I.** Since (4.8) is a genus zero curve, we choose the point on it  $(u_0, v_0), u_0 = (\alpha\beta)^{-q^2+1}, v_0 = (\alpha\beta)^{-q^2+q}$  by letting x = 0 in u and v.

Then a point (u, v) of (4.8) 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

(4.9) 
$$v - (\alpha\beta)^{-q^2+q} = l(u - (\alpha\beta)^{-q^2+1}).$$

The slope l can be written as

(4.10) 
$$l = \frac{v - (\alpha\beta)^{-q^2 + q}}{u - (\alpha\beta)^{-q^2 + 1}}.$$

Licensed to AMS.

Substituting  $u = \frac{(x-\alpha)(x-\beta)}{(x-\alpha^{q^2})(x-\beta^{q^2})}, v = \frac{(x-\alpha^q)(x-\beta^q)}{(x-\alpha^{q^2})(x-\beta^{q^2})}$  into (4.9), the denominator of *l* becomes (4.11)  $u - (\alpha\beta)^{-q^2+1} = \frac{\{1 - (\alpha\beta)^{-q^2+1}\}x^2 + (-\alpha - \beta + \alpha\beta^{-q^2+1} + \alpha^{-q^2+1}\beta)x}{(x-\alpha^{q^2})(x-\beta^{q^2})}.$ 

The numerator of l becomes

(4.12) 
$$v - (\alpha\beta)^{-q^2+q} = \frac{\{1 - (\alpha\beta)^{-q^2+q}\}x^2 + (-\alpha^q - \beta^q + \alpha^q\beta^{-q^2+q} + \alpha^{-q^2+q}\beta^q)x}{(x - \alpha^{q^2})(x - \beta^{q^2})}.$$

In the sequal,

(4.13) 
$$l = \frac{\{1 - (\alpha\beta)^{-q^2+q}\}x + (-\alpha^q - \beta^q + \alpha^q\beta^{-q^2+q} + \alpha^{-q^2+q}\beta^q)}{\{1 - (\alpha\beta)^{-q^2+1}\}x + (-\alpha - \beta + \alpha\beta^{-q^2+1} + \alpha^{-q^2+1}\beta)}$$

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

(4.14) 
$$G_{11} := 1 - (\alpha \beta)^{-q^2 + q}$$

(4.15) 
$$G_{12} := -\alpha^q - \beta^q + \alpha^q \beta^{-q^2+q} + \alpha^{-q^2+q} \beta^q$$

(4.16) 
$$G_{21} := 1 - (\alpha \beta)^{-q^2 + 1}$$

(4.17) 
$$G_{22} := -\alpha - \beta + \alpha \beta^{-q^2+1} + \alpha^{-q^2+1} \beta.$$

Then l can be expressed by the action of the matrix G on x. Indeed, rewrite (4.13) as

(4.18) 
$$l = G \cdot x \quad \text{s.t.} \quad G := \begin{pmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{pmatrix} \in \operatorname{GL}_2(k_3).$$

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

(4.19) 
$$x = G^{-1}l = \frac{G_{22}l - G_{12}}{-G_{21}l + G_{11}}$$

Now that we expressed x in terms of l, we try to express x directly in terms of X, Y and Z.

Substituting  $s = \frac{Y}{X}$ ,  $t = \frac{Z}{X}$  into l, one has

(4.20) 
$$l = \frac{Z^2 - (\alpha\beta)^{-q^2 + q} X^2}{Y^2 - (\alpha\beta)^{-q^2 + 1} X^2}.$$

Therefore

$$(4.21) \quad x = G^{-1} \cdot l = \frac{G_{22}Z^2 - G_{22}(\alpha\beta)^{-q^2+q}X^2 - G_{12}Y^2 + G_{12}(\alpha\beta)^{-q^2+1}X^2}{-G_{21}Z^2 + G_{21}(\alpha\beta)^{-q^2+q}X^2 + G_{11}Y^2 - G_{11}(\alpha\beta)^{-q^2+1}X^2}.$$

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

(4.22) 
$$\frac{(x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)}{{}^{\sigma}y^{\sigma^2}y} = st.$$

Licensed to AMS.

Then

(4.23) 
$$y = \frac{st \operatorname{N}_{k_3/k}(y)}{(x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)}.$$

To find  $N_{k_3/k}(y)$ , use the definition of  $C_0$  again

(4.24) 
$$N_{k_3/k}(y^2) = N_{k_3/k}(x-\alpha)^2 N_{k_3/k}(x-\beta)^2.$$

Now  $N_{k_3/k}(y)$  is expressed in terms of x as

(4.25) 
$$N_{k_3/k}(y) = \pm N_{k_3/k}(x-\alpha)N_{k_3/k}(x-\beta).$$

Hence, y can be written as

(4.26) 
$$y = \pm st(x - \alpha^{q^2})(x - \beta^{q^2})$$

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

Similar to x, y can also be expressed in terms of X, Y and Z.

(4.27) 
$$y = st(x - \alpha^{q^2})(x - \beta^{q^2}) \\ = \frac{YZ}{X^2}(x - \alpha^{q^2})(x - \beta^{q^2}).$$

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

First, denote x as a fraction  $x = \frac{x_2}{x_1}$ . Then x, y and z can be expressed as

(4.28) 
$$x = \frac{x_2}{x_1}, \ y = \frac{YZ}{X^2} \left(\frac{x_2}{x_1} - \alpha^{q^2}\right) \left(\frac{x_2}{x_1} - \beta^{q^2}\right), \ z = 1.$$

Thus one obtains the projective coordinates of  $C_0$  as

(4.29) 
$$x = x_1 x_2 X^2, \ y = Y Z (x_2 - \alpha^{q^2} x_1) (x_2 - \beta^{q^2} x_1), \ z = x_1^2 X^2.$$

Now  $\pi_1$  can be expressed as

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

such that

$$(4.30) \ x = \{-(\alpha\beta)^{-2q^2+2}G_{11}G_{12} + (\alpha\beta)^{-2q^2+q+1}G_{11}G_{22} \\ + (\alpha\beta)^{-2q^2+q+1}G_{12}G_{21} - (\alpha\beta)^{-2q^2+2q}G_{21}G_{22}\}X^6 \\ + \{2(\alpha\beta)^{-q^2+1}G_{11}G_{12} - (\alpha\beta)^{-q^2+q}G_{11}G_{22} - (\alpha\beta)^{-q^2+q}G_{12}G_{21}\}X^4Y^2 \\ + \{-(\alpha\beta)^{-q^2+1}G_{11}G_{22} - (\alpha\beta)^{-q^2+1}G_{12}G_{21} + 2(\alpha\beta)^{-q^2+q}G_{21}G_{22}\}X^4Z^2 \\ - G_{11}G_{12}X^2Y^4 + (G_{11}G_{22} + G_{12}G_{21})X^2Y^2Z^2 - G_{21}G_{22}X^2Z^4, \end{cases}$$

$$\begin{aligned} (4.31) \quad y &= \{ (\alpha\beta)^{-q^2+2}G_{11}^2 + (\alpha\beta)^{-2q^2+2}(\alpha^{q^2} + \beta^{q^2})G_{11}G_{12} \\ &- 2(\alpha\beta)^{-q^2+q+1}G_{11}G_{21} - (\alpha\beta)^{-2q^2+q+1}(\alpha^{q^2} + \beta^{q^2})G_{11}G_{22} \\ &+ (\alpha\beta)^{-2q^2+2}G_{12}^2 - (\alpha\beta)^{-2q^2+q+1}(\alpha^{q^2} + \beta^{q^2})G_{12}G_{21}^2 \\ &- 2(\alpha\beta)^{-2q^2+q+1}G_{12}G_{22} + (\alpha\beta)^{-q^2+2q}G_{21}^2 \\ &+ (\alpha\beta)^{-2q^2+2q}G_{22}^2 \}X^4YZ \\ &+ \{ -2\alpha\beta G_{11}^2 - 2(\alpha\beta)^{-q^2+1}(\alpha^{q^2} + \beta^{q^2})G_{11}G_{12} + 2(\alpha\beta)^q G_{11}G_{21} \\ &+ (\alpha\beta)^{-q^2+q}(\alpha^{q^2} + \beta^{q^2})G_{12}G_{21} - 2(\alpha\beta)^{-q^2+1}G_{12}^2 \\ &+ (\alpha\beta)^{-q^2+q}(\alpha^{q^2} + \beta^{q^2})G_{12}G_{21} + 2(\alpha\beta)^{-q^2+q}G_{12}G_{22} \}X^2Y^3Z \\ &+ \{ 2\alpha\beta G_{11}G_{21} + (\alpha\beta)^{-q^2+1}(\alpha^{q^2} + \beta^{q^2})G_{11}G_{22} \\ &+ (\alpha\beta)^{-q^2+q}(\alpha^{q^2} + \beta^{q^2})G_{12}G_{21} - 2(\alpha\beta)^{-q^2+q}G_{22}^2 \}X^2YZ^3 \\ &+ \{ (\alpha\beta)^{-q^2+q}(\alpha^{q^2} + \beta^{q^2})G_{12}G_{21} - 2(\alpha\beta)^{-q^2+q}G_{22}^2 \}YZ^3 \\ &+ \{ (\alpha\beta)^{q^2}G_{11}^2 + (\alpha^{q^2} + \beta^{q^2})G_{11}G_{12} + G_{12}^2 \}Y^5Z \\ &- \{ 2(\alpha\beta)^{q^2}G_{11}G_{21} + (\alpha^{q^2} + \beta^{q^2})G_{11}G_{22} \\ &+ (\alpha^{q^2} + \beta^{q^2})G_{12}G_{21} + 2G_{12}G_{22} \}Y^3Z^3 \\ &+ \{ (\alpha\beta)^{q^2}G_{21}^2 + (\alpha^{q^2} + \beta^{q^2})G_{21}G_{22} + G_{22}^2 \}YZ^5, \end{aligned}$$

$$(4.32) \quad z = \{(\alpha\beta)^{-2q^2+2}G_{11}^2 - 2(\alpha\beta)^{-2q^2+q+1}G_{11}G_{21} + (\alpha\beta)^{-2q^2+2q}G_{21}^2\}X^6 \\ + \{-2(\alpha\beta)^{-q^2+1}G_{11}^2 + 2(\alpha\beta)^{-q^2+q}G_{11}G_{21}\}X^4Y^2 \\ + \{2(\alpha\beta)^{-q^2+1}G_{11}G_{21} - 2(\alpha\beta)^{-q^2+q}G_{21}^2\}X^4Z^2 \\ + G_{11}^2X^2Y^4 - 2G_{11}G_{21}X^2Y^2Z^2 + G_{21}^2X^2Z^4.$$

**4.2. Type II.** Calculation for Type II curves is similar to Type I, what we need is to confirm that (4.21), (4.27) are defined over  $k_3$ .

For (4.21), first the entries of the matrix G,  $G_{11}$ ,  $G_{12}$ ,  $G_{21}$ ,  $G_{22}$  become

(4.33) 
$$G_{11} = 1 - \{N_{k_6/k_3}(\alpha)\}^{-q^2+q}$$

$$(4.34) G_{12} = -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^q + \{\mathrm{N}_{k_6/k_3}(\alpha)\}^q \{\mathrm{Tr}_{k_6/k_3}(\alpha)\}^{-q^2}$$

(4.35)  $G_{21} = 1 - \{N_{k_6/k_3}(\alpha)\}^{-q^2+1}$ 

(4.36) 
$$G_{22} = -\operatorname{Tr}_{k_6/k_3}(\alpha) + \operatorname{N}_{k_6/k_3}(\alpha) \{\operatorname{Tr}_{k_6/k_3}(\alpha)\}^{-q^2}.$$

Thus x can be expressed as (4.37)

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

which has only coefficients in  $k_3$ .

Next, (4.27) becomes

(4.38) 
$$y = \frac{YZ}{X^2} (x - \alpha^{q^2}) (x - \beta^{q^2})$$
$$= \frac{YZ}{X^2} (x^2 - \{\operatorname{Tr}_{k_6/k_3}(\alpha)\}^{q^2} x + \{\operatorname{N}_{k_6/k_3}(\alpha)\}^{q^2})$$

which also has coefficients in  $k_3$ . 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 with an elliptic curve E in Legendre form and a base point  $P_E$  of E.  $P_E$  and its *m*-multiple  $mP_E$  are mapped to points P and mP on an elliptic curve  $C_0$  which is isomorphic to E. Then we find the associated  $\chi(P)$  and  $\chi(mP)$  in  $\operatorname{Jac}(C)$ .

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 Legendre form.

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

5.1.1. Testing for Type I curves. Let  $\alpha = \epsilon + 1$ , then

 $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$   $a_{11} = 238798614356861922\epsilon + 457061445124994566$   $a_{12} = 685592167687491848\epsilon^{2} + 685592167687491847\epsilon + 1152921504606851052$   $a_{21} = 1$   $a_{22} = 924390782044353769\epsilon + 457061445124994564$   $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$   $b_{11} = 2\epsilon^{2} + \epsilon + 477597228713723848$   $b_{12} = 1152921504606851050\epsilon^{2} + 1152921504606851050\epsilon + 1152921504606851052$   $b_{21} = \epsilon^{2} + \epsilon + 1152921504606851052$   $b_{22} = 1152921504606851051\epsilon^{2} + 1152921504606851052\epsilon + 477597228713723844$ 

The quadratic equation  $b_{21}x^2 + (b_{22} - b_{11})x - b_{12} = 0$  has two solutions:  $\{\epsilon^2 + 2\epsilon + 1, 733677321113450670\epsilon^2 + 524055229366750479\epsilon + 209622091746700193\}$  Therefore, E is Type I. Take  $\beta = \epsilon^2 + 2\epsilon + 1 = \alpha^2$ , we know that E is  $k_3$ -isomorphic to

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

In fact, to test for Type I curves, we chose  $\lambda = 2, ..., 10001$ , the average time to test each curve was 0.0356858 second. Among these curves, 5018 were of Type I.

5.1.2. Finding the defining equation of the covering curve C/k. The covering C/k of  $C_0/k_3$  is found using the algorithm shown in Section 4.

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

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

5.1.3. Transferring the DLP. The isomorphism from E to  $C_0, \iota: E \to C_0$  is

$$\begin{split} \iota: E &\to C_{0} \\ (x:y:z) &\mapsto (x_{C_{0}}:y_{C_{0}}:z_{C_{0}}) \\ x_{C_{0}} &= (364080906763379389\epsilon^{2} + 963836771592621382\epsilon \\ &+ 45113745901700524)x^{2} + (697163568297605614\epsilon^{2} \\ &+ 434818842429256188\epsilon + 651968585745464837)xz \\ &+ (1110165463009250121\epsilon^{2} + 159411805327734998\epsilon \\ &+ 1139314830835562614)z^{2}, \\ y_{C_{0}} &= (103276516251305235\epsilon^{2} + 814915306056127686\epsilon \\ &+ 861572657639767622)yz, \\ z_{C_{0}} &= (883436713213250245\epsilon^{2} + 38740486277729303\epsilon \\ &+ 1108413203079573589)x^{2} + (614045874632256899\epsilon^{2} \\ &+ 476034365815665715\epsilon + 725151688441932395)xz \\ &+ (1080996664374642930\epsilon^{2} + 29168798634607191\epsilon \\ &+ 130243006693127807)z^{2}. \end{split}$$

The inverse map  $\iota^{-1}$  is

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

For example, take a base point on E

$$P_E = (326484750616207568\epsilon^2 + 398950984132538563\epsilon + 1105635074365709877 : 155216221479156187\epsilon^2 + 406624014520210471 + 708450555015860225 + 1)$$

 $+496624914529310471\epsilon + 708459555015860335:1)$ 

which has a prime order :

 $ord(P_E) = 383123885216476279036490868125406665879768163968774759.$ 

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

```
P = (382583549840633528\epsilon^2 + 1049745021810473522\epsilon
```

```
+527223886793925136:297304679459601150\epsilon^{2}
```

```
+626540460794459518\epsilon + 906489884274840212:1).
```

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

$$D_P = Q_1 + Q_2$$

 $\begin{array}{rcl} q_1 &=& 712456629299217053\epsilon^2 + 953676660329800786\epsilon + 707524424701837646\\ q_2 &=& 666557349447958527\epsilon^2 + 352353429259986813\epsilon + 1073895093206451353\\ q_3 &=& 805061362249374584\epsilon^2 + 1042799979746437227\epsilon + 880598497458186947\\ q_4 &=& 527740077639497471\epsilon^2 + 947552956030900685\epsilon + 390269122338929978\\ Q_1 &=& (q_1:\ q_2:\ 1) \in C/k_3, \qquad Q_2 = (q_3:\ q_4:\ 1) \in C/k_3\\ &\qquad \chi(P) = D_P + {}^{\sigma}D_P + {}^{\sigma^2}D_P\\ &\qquad {}^{\sigma}D_P &=& {}^{\sigma}Q_1 + {}^{\sigma}Q_2, \qquad {}^{\sigma^2}D_P = {}^{\sigma^2}Q_1 + {}^{\sigma^2}Q_2\\ &\qquad {}^{\sigma}Q_1 &=& (q_1{}^q:\ q_2{}^q:\ 1), \qquad {}^{\sigma^2}Q_2 = (q_3{}^q:\ q_4{}^q:\ 1)\\ &\qquad {}^{\sigma^2}Q_1 &=& (q_1{}^{q^2}:\ q_2{}^{q^2}:\ 1), \qquad {}^{\sigma^2}Q_2 = (q_3{}^{q^2}:\ q_4{}^{q^2}:\ 1). \end{array}$ The time needed to map  $P_E$  to  $\chi(P)$  is 17.578 seconds.

Now let

m = 323265910321268664514129224009489670151908972955376519.

 $E \ni mP_E = (792310221862816838\epsilon^2 + 180893695299760122\epsilon + 952490131358998041 : 669346193997384009\epsilon^2$ 

 $+488209130112427093\epsilon+787028498315590410:1).$ 

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

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

One then maps mP to  $D_{mP}$  and  $\chi(mP)$  as follows.

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

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

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

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

### 5.2. Type II. Assume

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

 $\begin{aligned} k[x] & \ni \quad a(x) = x^3 + 943550857826445658x^2 + 1018916892242739535x \\ & + 475736851389393367 \end{aligned}$ 

$$k_3 = k[x]/\langle a(x) \rangle, \ \exists \epsilon \in k_3 \text{ s.t. } a(\epsilon) = 0$$

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

$$\alpha = \eta + \epsilon, \ \beta = \alpha^q$$

and consider the three isomorphic elliptic curves:

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

$$E_\lambda/k_3 : y^2 z = \mathcal{N}_{k_6/k_3}(\beta - \alpha^q)x(x - z)(x - \lambda z), \ \lambda = \mathcal{N}_{k_6/k_3}\left(\frac{\alpha^q - \alpha}{\alpha^q - \beta}\right)$$
  

$$E/k_3 : y^2 z = x(x - z)(x - \lambda z), \ \lambda = \mathcal{N}_{k_6/k_3}\left(\frac{\alpha^q - \alpha}{\alpha^q - \beta}\right)$$

5.2.1. Finding defining equation of the covering curve C/k. Using the algorithm in Section 4, one finds the defining equation of C/k as follows.

Computing 
$$C/k$$
 takes 0.500 second.

5.2.2. Transferring the DLP. We first find the isomorphism from E to  $E_{\lambda}$ ,  $\xi : E \to E_{\lambda}$  as follows.

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

Its inverse map  $\xi^{-1}$  is

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

Next we compute the isomorphism from  $E_{\lambda}$  to  $C_0, \tau : E_{\lambda} \to C_0$  as follows.

$$\begin{array}{lll} \tau: E_{\lambda} & \rightarrow & C_{0} \\ (x:y:z) & \mapsto & (x_{C_{0}}:y_{C_{0}}:z_{C_{0}}) \\ x_{C_{0}} & = & (510834712742882221\epsilon^{2} + 459409699423611549\epsilon \\ & +472370343629151306)x^{2}z + (23471605822501754\epsilon^{2} \\ & +309377569878570651\epsilon + 7799912042878324)xyz \\ & +(931076450504798462\epsilon^{2} + 525743454321773525\epsilon \\ & +30041499258217822)xz^{2} + (977818514557529265\epsilon^{2} \\ & +765506242357294185\epsilon + 252827041845239982)yz^{2} \\ & +(1000370112565854753\epsilon^{2} + 328209714163922360\epsilon \\ & +293352898935549091)z^{3}, \\ y_{C_{0}} & = & (1102768582695395466\epsilon^{2} + 801656811370788382\epsilon \\ & +1017012503317150212)x^{3} + (162397320242107152\epsilon^{2} \\ & +559604911348892417\epsilon + 312861297828079035)x^{2}z \\ & +(558782202587610802\epsilon^{2} + 590994009401290871\epsilon \\ & +1152361677914957201)xz^{2} + (11735802911250877\epsilon^{2} \\ & +731149537242710761\epsilon + 3899956021439162)y^{2}z \\ & +(764240535732840601\epsilon^{2} + 875626294947314353\epsilon \\ & +1076372293311177227)yz^{2} + (48504428759686342\epsilon^{2} \\ & +341476326696745685\epsilon + 96595209872171953)z^{3}, \\ z_{C_{0}} & = & (1105978292961847363\epsilon^{2} + 534166364849709569\epsilon \\ & +1137321680521094223)x^{2}z + (700411960197286424\epsilon^{2} \\ & +396739544391375873\epsilon + 141613337225890943)xz^{2} \\ & +(1019981124724128614\epsilon^{2} + 858207083874918419\epsilon \\ & +885871207426547152)z^{3} \end{array}$$

The inverse map  $\tau^{-1}$  is

For example, a base point on E is chosen as

$$E \ni P_E = (832338441672439527\epsilon^2 + 369146262528272140\epsilon + 788595051686438200 : 916492546448194121\epsilon^2 + 805387000881236587\epsilon + 244343815529721159 : 1)$$

 $P_E$  has a prime order :

 $ord(P_E) = 383123885216476097596869443538990953306902164540505859.$ 

This base point is mapped by  $\xi$ ,  $\tau$  to a point on  $C_0$ .

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

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

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

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

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

$$D_P = Q_1 + Q_2$$

Licensed to AMS.

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

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

Now take m=182096100370109847529739170552459116709626522690507709,  $mP_E \in E$  is

$$mP_E = (522521730599820536\epsilon^2 + 443211485181667680\epsilon +408033332463290588 : 191091537075096495\epsilon^2 +622369471011935091\epsilon + 865873192897372210 : 1)$$

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

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

and then to  $mP = \tau(mP_{E_{\lambda}}) \in C_0$ :

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

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

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

 $\begin{array}{rcl} q_1 &=& 30078314732782878\epsilon^2 + 988992501393194153\epsilon + 673404688332712109 \\ q_2 &=& 1148714815680333640\epsilon^2 + 423917326839288390\epsilon + 503765461488992377 \\ q_3 &=& 734788579677917913\epsilon^2 + 68926008534553154\epsilon + 77740516941101348 \\ q_4 &=& 750968410676713515\epsilon^2 + 683426730428696431\epsilon + 823046869633863637 \\ Q_1 &=& (q_1:\ q_2:\ 1) \in C/k_3,\ Q_2 = (q_3:\ q_4:\ 1) \in C/k_3 \\ &\qquad \chi(mP) = D_{mP} + {}^{\sigma}D_{mP} + {}^{\sigma^2}D_{mP} \\ &\qquad {}^{\sigma}D_{mP} &=& {}^{\sigma}Q_1 + {}^{\sigma}Q_2,\ {}^{\sigma^2}D_{mP} = {}^{\sigma^2}Q_1 + {}^{\sigma^2}Q_2 \\ &\qquad {}^{\sigma}Q_1 &=& (q_1{}^q:\ q_2{}^q:\ 1),\ {}^{\sigma^2}Q_2 = (q_3{}^q:\ q_4{}^q:\ 1) \\ &\qquad {}^{\sigma^2}Q_1 &=& (q_1{}^{q^2}:\ q_2{}^{q^2}:\ 1),\ {}^{\sigma^2}Q_2 = (q_3{}^{q^2}:\ q_4{}^{q^2}:\ 1) \end{array}$ 

Computing  $\chi(mP)$  from  $mP_E$  takes 11.281 seconds.

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

#### 6. Conclusion

We presented two algorithms to implement the GHS attack against elliptic curve cryptosystems over cubic extension fields of odd characteristic and the results of the computer simulation. The first algorithm obtains the defining equation for 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 Jac(C/k). These DLP over Jac(C/k) can then be solved using Diem's double-large-prime algorithm.

#### References

- Pierrick Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, Advances in cryptology—EUROCRYPT 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 19–34, DOI 10.1007/3-540-45539-6.2. MR1772021
- [2] Nicolas Thériault, Index calculus attack for hyperelliptic curves of small genus, Advances in cryptology—ASIACRYPT 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 75–92, DOI 10.1007/978-3-540-40061-5\_5. MR2093253
- [3] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, A double large prime variation for small genus hyperelliptic index calculus, Math. Comp. 76 (2007), no. 257, 475–492, DOI 10.1090/S0025-5718-06-01900-4. MR2261032
- [4] Claus Diem, An index calculus algorithm for plane curves of small degree, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 543–557, DOI 10.1007/11792086\_38. MR2282948
- [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. P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, J. Cryptology 15 (2002), no. 1, 19–46, DOI 10.1007/s00145-001-0011-x. MR1880933
- [7] Alfred Menezes and Minghua Qu, Analysis of the Weil descent attack of Gaudry, Hess and Smart, Topics in cryptology—CT-RSA 2001 (San Francisco, CA), Lecture Notes in Comput. Sci., vol. 2020, Springer, Berlin, 2001, pp. 308–318, DOI 10.1007/3-540-45353-9\_23. MR1907106
- [8] Alfred Menezes, Edlyn Teske, and Annegret Weng, Weak fields for ECC, Topics in cryptology—CT-RSA 2004, Lecture Notes in Comput. Sci., vol. 2964, Springer, Berlin, 2004, pp. 366–386, DOI 10.1007/978-3-540-24660-2.28. MR2092257
- Steven D. Galbraith, Weil descent of Jacobians, Discrete Appl. Math. 128 (2003), no. 1, 165–180, DOI 10.1016/S0166-218X(02)00443-2. International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR1991424
- [10] Nicolas Thériault, Weil descent attack for Kummer extensions, J. Ramanujan Math. Soc. 18 (2003), no. 3, 281–312. MR2007146
- [11] Nicolas Thériault, Weil descent attack for Kummer extensions, J. Ramanujan Math. Soc. 18 (2003), no. 3, 281–312. MR2007146
- [12] Florian Hess, The GHS attack revisited, Advances in cryptology—EUROCRYPT 2003, Lecture Notes in Comput. Sci., vol. 2656, Springer, Berlin, 2003, pp. 374–387, DOI 10.1007/3-540-39200-9\_23. MR2090430
- F. Hess, Generalising the GHS attack on the elliptic curve discrete logarithm problem, LMS J. Comput. Math. 7 (2004), 167–192, DOI 10.1112/S146115700000108X. MR2087095
- [14] Claus Diem, The GHS attack in odd characteristic, J. Ramanujan Math. Soc. 18 (2003), no. 1, 1–32. MR1966526
- [15] C. Diem and J. Sholten, "Cover attack". Preprint, 2003. Available at http://www.math.unileipzig.de/ diem/preprints/english.html
- [16] H. Cohen, G. Frey(ed), Handbook of elliptic and hyperelliptic curve cryptography, Chapman & Hall/CRC, 2005.

- [17] F. Momose, J. Chao, "Scholten forms and elliptic/hyperelliptic curves with weak Weil restrictions". Preprint, 2005. Available at http://eprint.iacr.org/2005/277
- [18] F. Momose and J. Chao "Classification of Weil restrictions obtained by (2,...,2) coverings of P<sup>1</sup>," Preprint, 2006. Available at http://eprint.iacr.org/2006/347
- [19] J. Chao, "Elliptic and hyperelliptic curves with weak covering against Weil descent attacks", 2007 International Workshop on Elliptic Curve Cryptosystems, ECC2007, Sept., 2007.
- [20] Fumiyuki Momose and Jinhui Chao, Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristic, J. Ramanujan Math. Soc. 28 (2013), no. 3, 299–357. MR3113387
- [21] T. Iijima, F. Momose, and J. Chao "Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack without isogeny condition," Preprint, 2009. Available at http://eprint.iacr.org/2009/613.
- [22] T. Iijima, F. Momose and J. Chao "Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack under an isogeny condition," Preprint, 2013. Available at http://eprint.iacr.org/2013/487.
- [23] T. Iijima, F. Momose, and J. Chao "A classification of elliptic curves with respect to the GHS attack in odd characteristic," Preprint, 2015. Available at http://eprint.iacr.org/2015/805.

#### Appendix: On Condition (2.14) of hyperellipticity

**Type I.** By (2.14),  $\beta = A \cdot \alpha = \frac{a\alpha + b}{c\alpha + d}$  (a, b, c,  $d \in k$ ). Combining with  $\operatorname{Tr} A = 0$ , one has the following variation of Condition (2.14)

(6.1) *C* is hyperelliptic 
$$\iff \beta = A \cdot \alpha, \ A \in \operatorname{GL}_2(k), \operatorname{Tr} A = 0$$
  
 $\iff \text{Either (i) or (ii) is true.}$   
(6.2) 
$$\begin{cases} (i) \ A = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}, \\ \beta = A \cdot \alpha = \frac{a\alpha + b}{-a} = -\alpha - b', \\ or \quad \alpha + \beta = -b' \in k \\ (ii) \ A = \begin{pmatrix} a & b \\ 1 & -a \end{pmatrix}, \ \beta = A \cdot \alpha = \frac{a\alpha + b}{\alpha - a} \end{cases}$$

In particular, Condition (ii) means  $\beta = \frac{a\alpha + b}{\alpha - a}$ , or

(6.3) 
$$\alpha\beta - (\alpha + \beta)a - b = 0$$

Since any element  $l \in k_3$  can be expressed, using the basis  $\{1, \epsilon, \epsilon^2\}$  as

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

assume

(6.4) 
$$\alpha = \alpha_0 + \alpha_1 \epsilon + \alpha_2 \epsilon^2,$$

$$(6.5) \qquad \qquad \beta = \beta_0 + \beta_1 \epsilon + \beta_2 \epsilon^2$$

Then

(6.6) 
$$\alpha\beta = (\alpha\beta)_0 + (\alpha\beta)_1\epsilon + (\alpha\beta)_2\epsilon^2$$

(6.7) 
$$-(\alpha+\beta)a = -(\alpha_0+\beta_0)a - (\alpha_1+\beta_1)a\epsilon - (\alpha_2+\beta_2)a\epsilon^2$$

(6.3) becomes

(6.8)  

$$\begin{aligned} &\alpha\beta - (\alpha + \beta)a - b \\ &= \{(\alpha\beta)_0 - (\alpha_0 + \beta_0)a - b\} + \{(\alpha\beta)_1 - (\alpha_1 + \beta_1)a\}\epsilon \\ &+ \{(\alpha\beta)_2 - (\alpha_2 + \beta_2)a\}\epsilon^2 \end{aligned}$$
(6.9)  

$$= 0$$

Therefore Condition (ii) can be replaced by the existence of solutions in the following linear equations in a, b

(6.10) 
$$\begin{cases} -(\alpha_0 + \beta_0)a - b + (\alpha\beta)_0 = 0\\ -(\alpha_1 + \beta_1)a + (\alpha\beta)_1 = 0\\ -(\alpha_2 + \beta_2)a + (\alpha\beta)_2 = 0 \end{cases}$$

When one wishes to find a nonhyperelliptic curve, Condition (2.14) has to be avoided. Therefore neither (i) nor (ii) should hold for  $\alpha$  and  $\beta$ . This means

 $(6.11) \quad \overline{(i)} \quad \alpha + \beta \notin k$ 

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

has no solution.

Define

(6.13) 
$$B := \begin{pmatrix} -(\alpha_0 + \beta_0) & -1 \\ -(\alpha_1 + \beta_1) & 0 \\ -(\alpha_2 + \beta_2) & 0 \end{pmatrix}, B' := \begin{pmatrix} -(\alpha_0 + \beta_0) & -1 & -(\alpha\beta)_0 \\ -(\alpha_1 + \beta_1) & 0 & -(\alpha\beta)_1 \\ -(\alpha_2 + \beta_2) & 0 & -(\alpha\beta)_2 \end{pmatrix}$$

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

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

**Type II.** For the Type II case, since  $\alpha + \beta = \operatorname{Tr}_{k_6/k_3}(\alpha)$ ,  $\alpha\beta = N_{k_6/k_3}(\alpha)$ ,  $\overline{(i)}$  and  $\overline{(ii)}$  in Type I can be replaced by

$$\begin{array}{ll} \overline{(\mathrm{i})} & \operatorname{Tr}_{k_{6}/k_{3}}(\alpha) \notin k \\ \hline \overline{(\mathrm{ii})} & \operatorname{The system of equations:} \\ & has no solution. \end{array} \left\{ \begin{array}{l} -\{\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\}_{0}a - b + \{\operatorname{N}_{k_{6}/k_{3}}(\alpha)\}_{0} = 0 \\ -\{\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\}_{1}a + \{\operatorname{N}_{k_{6}/k_{3}}(\alpha)\}_{1} = 0 \\ -\{\operatorname{Tr}_{k_{6}/k_{3}}(\alpha)\}_{2}a + \{\operatorname{N}_{k_{6}/k_{3}}(\alpha)\}_{2} = 0 \end{array} \right.$$

Define

$$\begin{array}{l} (6.14) \\ B := \begin{pmatrix} -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_0 & -1 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_1 & 0 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_2 & 0 \end{pmatrix}, B' := \begin{pmatrix} -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_0 & -1 & -\{\mathrm{N}_{k_6/k_3}(\alpha)\}_0 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_1 & 0 & -\{\mathrm{N}_{k_6/k_3}(\alpha)\}_1 \\ -\{\mathrm{Tr}_{k_6/k_3}(\alpha)\}_2 & 0 & -\{\mathrm{N}_{k_6/k_3}(\alpha)\}_2 \end{pmatrix}$$

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

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

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 ENGI-NEERING, CHUO UNIVERSITY, 1-13-27 KASUGA, BUNKYO-KU, TOKYO 112-8551, JAPAN Email address: jchao@ise.chuo-u.ac.jp