A Weil Descent Attack against Elliptic Curve Cryptosystems over Quartic Extension Fields

Seigo Arita* Kazuto Matsuo*† Koh-ichi Nagao‡

Mahoro Shimura§

September 14, 2004

Abstract

This paper shows that many of elliptic curve cryptosystems over quartic extension fields of odd characteristics are reduced to genus two hyperelliptic curve cryptosystems over quadratic extension fields. Moreover, it shows that almost all of the genus two hyperelliptic curve cryptosystems over quadratic extension fields of odd characteristics come under Weil descent attack. This means that many of elliptic curve cryptosystems over quartic extension fields of odd characteristics can be attacked by Weil descent uniformly.

1 Introduction

Now, the elliptic curve cryptosystem is one of the most important public key cryptosystems. There have been found several attack methods for elliptic curve cryptosystems, such as MOV attack [15], Frey-Rück attack [8], SSSA attack [19, 21, 22], and Weil descent attack. Among them, the most problematic attack is Weil descent attack, because the class of the elliptic curves for which Weil descent attack efficiently works has not been determined yet.

Weil descent attack, of which idea was shown by Frey and Gangl [7], aims to break DLP on algebraic curve over composite fields. For a given algebraic curve A on a composite field K, using the technique of scalar restriction, we construct an algebraic curve C on a smaller field k to cover the curve A. By doing this, we can reduce DLP on A to DLP on C. Since the definition field k of C is smaller than that K of A, Gaudry method [12] could be more effective against DLP on C than against A, provided that genus of C is small enough.

Gaudry, Hess and Smart [13] firstly showed that some of (DLP on) elliptic curve of characteristic two are really attacked by Weil descent. Later, it was

*Graduate School of Information Security, Institute of Information Security, Japan

†The Research and Development Initiative of Chuo Univ., Japan

‡Dept. of Engineering, Kanto-Gakuin Univ., Japan

§Chuo University 21st Century Center Of Excellence Program, Japan

shown, by Galbraith [9] and [2], that some of hyperelliptic curve of characteristic two and some of elliptic curve of characteristic three are also attacked, respectively. Moreover Diem [6] has shown the existence of (hyper-)elliptic curves of general odd characteristics which can be attacked by Weil descent. However, elliptic or hyperelliptic curves attacked by those are very exceptional ones.

In this paper, we deal with elliptic curve cryptosystems over quartic extension fields. We show that many of those are reduced to genus two hyperelliptic curve cryptosystems over quadratic extension fields. Moreover, we show that almost all of the genus two hyperelliptic curve cryptosystems over quadratic extension fields of odd characteristics come under Weil descent attack. This means that many of elliptic curve cryptosystems over quartic extension fields of odd characteristics can be attacked by Weil descent uniformly.

The organization of the paper is as follows:

In Section 2, we show that many of elliptic curve cryptosystems over quartic extension fields are reduced to genus two hyperelliptic curve cryptosystems over quadratic extension fields. In Section 2.1, we introduce Scholten form of an elliptic curve over a quartic extension field, and we see that Scholten form is covered by a genus two hyperelliptic curve over a quadratic extension field. Then, in Section 2.2, we see that elliptic curves which can be expressed in Scholten form are ones with no two-torsions, or ones with full two-torsions.

In Section 3, we show Weil descent attack is effective in the almost all of the genus two hyperelliptic curve cryptosystems over quadratic extension field. In Section 3.1, given a genus two hyperelliptic curve over a quadratic extension, we construct an algebraic curve of genus nine over its subfield using the technique of scalar restriction. Then, in Section 3.2, we construct a C_{ab} model of the genus nine curve, and in Section 3.3, we explicitly reduce DLP on the hyperelliptic curve to DLP on the C_{ab} model in order to apply a variant of Gaudry method.

2 A Weil Descent Attack against Elliptic Curve Cryptosystems over Quartic Extension Fields

Suppose an elliptic curve defined over quartic extension field k_4 of k of odd characteristic in the Weierstrass form $E_w : y^2 = f(x)$ is given. Let k_2 be a quadratic extension of k in k_4. Let q denote the order of k. We show that the elliptic curve E_w has Scholten form [20], that is, it has a defining equation of the form $y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ with $a, b \in k_4$ if and only if $f(x)$ is irreducible over k_4 with $\mathrm{j}(E) \notin k_2$, or $f(x)$ is completely factored over k_4.

Moreover, we show an elliptic curve E_n in Scholten form has a double cover of genus two hyperelliptic curve $H : y^2 = a(x-c)^6 + b(x-c)^4(x-c^{q^2})^2 + b^{q^2}(x-c)^2(x-c^{q^2})^4 + a^{q^2}(x-c^{q^2})^6$, which is defined over k_2 ($c \in k_4$). Thus, we see that DLP on many of elliptic curves over quartic extension field k_4 of odd characteristics are reduced to DLP on genus two hyperelliptic curves over quadratic extension field k_2. Here, we notice that the corresponding hyperelliptic curve has a defining equation of the form $y^2 = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$, not necessarily to be an imaginary type.

2.1 Scholten from

Let $k = \mathbb{F}_q$ be a finite field of order q of characteristic different from 2. Let k_d denote the d-th degree extension of k. An elliptic curve E_n over k_4 is called **Scholten form** if it is defined by an equation

$$y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$$

with some $a, b \in k_4$.

Scholten [20] showed that the scalar restriction $\Pi_{k_2}^{k_4} E_n$ of Scholten form E_n is isomorphic to Jacobian of a genus 2 hyperelliptic curve over k_2, and gave a way to construct secure genus two hyperelliptic curve (constructive Weil descent). Moreover, he showed that an elliptic curve with full 2-torsions can be transformed into Scholten form, and observed that an elliptic curve with no 2-torsions can be also transformed experimentally.

We see in this paper that Scholten form E_n on k_4 is covered by a genus two hyperelliptic curve on k_2 in a different manner from Scholten [20], and clarify necessary and sufficient conditions for a given elliptic curve to be transformed into Scholten form.

Scholten form E_n has a double cover of genus two hyperelliptic curve

$$H : Y^2 = a(X-c)^6 + b(X-c)^4(X-c^{q^2}) + b^{q^2}(X-c)^2(X-c^{q^2})^4 + a^{q^2}(X-c^{q^2})^6.$$

Here, c denotes an element of k_4, not included in k_2. We notice that H is defined on k_2. A covering map Ψ from hyperelliptic curve H to Scholten form E_n is given by

$$(x, y) = \Psi(X, Y) = \left(\left(\frac{X-c}{X-c^{q^2}} \right)^2, \frac{Y}{(X-c^{q^2})^3} \right). \tag{1}$$

Remark 1. *The hyperelliptic curve H dose not depend on the choice of $c\,(\in k_4 - k_2)$. In fact, $H_0 : Y^2 = aX^6 + bX^4 + b^{q^2}X^2 + a^{q^2}$ is isomorphic to H via a map*

$$(X, Y) \longmapsto \left(\frac{X-c}{X-c^{q^2}}, \frac{Y}{(X-c^{q^2})^3} \right).$$

For a k_4-rational point P on Scholten form E_n, let $\{Q_1, Q_2\}$ be an inverse image of P by the covering map $\Psi : H \to E_n$. The covering map $\Psi : H \to E_n$ induces a homomorphism Ψ^* from $E_n(k_4)$ to Jacobian $J_H(k_4)$ of H over k_4:

$$\begin{array}{rcl} \Psi^* : E_n(k_4) & \to & J_H(k_4) \\ P & \mapsto & Q_1 + Q_2 - \infty_1 - \infty_2. \end{array}$$

Here, ∞_1, ∞_2 denote two points of H at infinity. By equation (1) of the covering map Ψ, we see that X-coordinates of Q_1 and Q_2 are roots of

$$(X-c)^2 - x(P)(X-c^{q^2})^2 = 0, \tag{2}$$

where $x(P)$ denotes the x-coordinate of the point P.

We take a composition of Ψ^* with trace map

$$\begin{array}{rcl} T : J_H(k_4) & \to & J_H(k_2) \\ \sum_i Q_i & \mapsto & \sum_i Q_i + Q_i^{q^2} \end{array}$$

to get a homomorphism $T \cdot \Psi^*$ from $E_n(k_4)$ to Jacobian $J_H(k_2)$ over k_2.

Lemma 1. *Let P be a k_4-rational point of Scholten form E_n. If the order of P is not less than $2q^2+2$, then we have $T \cdot \Psi^*(P) \neq 0$.*

Proof. We only have to show that the number of $P \in E_n(k_4)$ satisfying $T \cdot \Psi^*(P) = 0$ is at most $2q^2+1$. In order to do that, it suffices to show the number of $P \in E_n(k_4)$ with $x(P) \neq 1, \infty$ satisfying $T \cdot \Psi^*(P) = 0$ is at most $2q^2-2$.

Let $x(P) \neq 1, \infty$. Let $\{Q_1, Q_2\}$ be an inverse image of P by $\Psi : H \to E_n$. Let $A(X) = (X-c)^2 + (X-c^{q^2})^2$ and $B(X) = (X-c)^2 - (X-c^{q^2})^2$. Since X-coordinates of Q_1, Q_2 satisfies equation (2), we have

$$\frac{1}{2}(1-x(P))A(X) + \frac{1}{2}(1+x(P))B(X) = 0.$$

By making this monic, we have

$$\frac{1}{2}(A(X) - \frac{b+1}{b}B(X)) = 0$$

with $b = (-1+x(P))/2$.

Now we assume, in addition, that $T \cdot \Psi^*(P) = 0$. Then, since $\Psi^*(P) = -\Psi^*(P)^{q^2}$, the monic equation for X-coordinates of Q_1, Q_2 and the one for $Q_1^{q^2}, Q_2^{q^2}$ must be identical. So, noticing that $A(X), B(X)$ is transferred to $A(X), -B(X)$ respectively by q^2-Frobenius, we see

$$\left(\frac{b+1}{b}\right)^{q^2} = -\frac{b+1}{b}.$$

Since the number of such $b\,(\neq 0)$ are at most q^2-1, the number of P satisfying $T \cdot \Psi^*(P) = 0$ is at most $2q^2-2$. □

By Lemma 1, we see that the homomorphism $T \cdot \Psi^*$ from $E_n(k_4)$ to $J_H(k_2)$ is not trivial. So, it reduces DLP on $E_n(k_4)$ to DLP on $J_H(k_2)$. Thus, we know that DLP on Scholten form over k_4 is reduced to DLP on genus two hyperelliptic curve over k_2.

2.2 Which elliptic curves are in Scholten form?

Now, we consider necessary and sufficient conditions for an elliptic curve on k_4 in Weierstrass form to be transformed into Scholten form over k_4. In general, an isomorphism between elliptic curves (which are not necessarily in Weierstrass forms) is given by a linear transformation $x \to Ax + B, y \to Cy + Dx + E$ with constants A, B, C, D. If Weierstrass form $E_w : y^2 = f(x)$ on k_4 is transformed into Scholten form $E_n : y^2 = F(x)$ on k_4 by transformation $x \to Ax + B, y \to Cy + Dx + E$ over k_4, it is obvious that $D = E = 0$ and $F(x) = C^{-2} f(Ax+B)$.

2.2.1 The case of $f(x)$ being irreducible over k_4

First, we consider necessary and sufficient conditions for Weierstrass form $E_w : y^2 = f(x)$ to be transformed into Scholten form $E_n : y^2 = F(x)$ with $f(x)$ being irreducible over k_4.

Suppose Weierstrass form $E_w : y^2 = f(x)$ is transformed into Scholten form $E_n : y^2 = F(x)$ by transformation $x \to Ax + B, y \to Cy$ over k_4. Since $F(x) = C^{-2} f(Ax + B)$, $F(x)$ is also irreducible over k_4. Let δ be a root of $F(x) = ax^3 + bx^2 + b^{q^2} x + a^{q^2}$:

$$a\delta^3 + b\delta^2 + b^{q^2}\delta + a^{q^2} = 0.$$

Applying q^2-Frobenius and multiplying with $(\delta^{-q^2})^3$, we have

$$a(\delta^{-q^2})^3 + b(\delta^{-q^2})^2 + b^{q^2}\delta^{-q^2} + a^{q^2} = 0.$$

So, δ^{-q^2} is also a root of $F(x)$. This means that

$$\delta^{-q^2} = \delta \text{ or } \delta^{q^4} \text{ or } \delta^{q^8}.$$

However, if we suppose $\delta^{-q^2} = \delta$, then we have $\delta^{q^4-1} = (\delta^{q^2+1})^{q^2-1} = 1$, and $\delta \in k_4$, which contradicts the irreducibility of $F(x)$. Similarly, if $\delta^{-q^2} = \delta^{q^4}$, then $\delta^{-1} = \delta^{q^2}$ which also means $\delta \in k_4$. Therefore, we must have $\delta^{-q^2} = \delta^{q^8}$, that is, $\delta^{1+q^6} = 1$.

Summarizing,

Proposition 1. *Suppose that a monic cubic polynomial $f(x)$ is irreducible over k_4, and that Weierstrass form $E_w : y^2 = f(x)$ on k_4 is isomorphic to Scholten form $E_n : y^2 = F(x)$ over k_4. Then, for a root γ for $f(x)$, there are $A \in k_4^\times$ and $B \in k_4$ satisfying $\gamma = A\delta + B$ and $\delta^{1+q^6} = 1$.*

The contrary also holds:

Proposition 2. *Let $f(x)$ be an irreducible monic cubic polynomial over k_4. Suppose that there are $A \in k_4^\times$ and $B \in k_4$ satisfying $\gamma = A\delta + B$ and $\delta^{1+q^6} = 1$ for a root γ of $f(x)$. Let*

$$\begin{aligned} a &= -A^{2-q^2}\delta^{1+q^4-q^2}, \\ b &= -A(\delta + \delta^{q^4} + \delta^{-q^2}). \end{aligned}$$

Then, Weierstrass form $E_w : y^2 = f(x)$ on k_4 is transformed into Scholten form $E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ on k_4 by transformation $y \to ay, x \to ax + B$ over k_4.

Proof. Applying transformation $y \to y, x \to x + B$, we can suppose $B = 0$. For $f(x) = (x - \gamma)(x - \gamma^{q^4})(x - \gamma^{q^8})$,

$$\begin{aligned}\text{the coefficient of } x^2 &= -(\gamma + \gamma^{q^4} + \gamma^{q^8}) \\ &= -A(\delta + \delta^{q^4} + \delta^{-q^2}) \\ &= b,\end{aligned}$$

$$\begin{aligned}\text{the coefficient of } x &= \gamma\gamma^{q^4} + \gamma^{q^4}\gamma^{q^8} + \gamma^{q^8}\gamma \\ &= A^2(\delta^{1+q^4} + \delta^{q^4-q^2} + \delta^{1-q^2}) \\ &= -A^{2-q^2}\delta^{1+q^4-q^2} \cdot (-1) \cdot A^{q^2}(\delta^{q^2} + \delta^{-1} + \delta^{-q^4}) \\ &= ab^{q^2},\end{aligned}$$

Let $\epsilon = \delta^{1+q^4-q^2}$. Noticing that $\epsilon^{1+q^2} = 1$,

$$\begin{aligned}\text{the constant term} &= -\gamma^{1+q^4+q^8} \\ &= -A^3\epsilon \\ &= -A^{2q^2-1}\epsilon^{q^2} \cdot A^{4-2q^2}\epsilon^2 \\ &= a^{q^2}a^2.\end{aligned}$$

Therefore, we have

$$y^2 = x^3 + bx^2 + ab^{q^2}x + a^{q^2}a^2.$$

This is transformed into

$$E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$$

by transformation $y \to ay, x \to ax$. □

Next, for a root γ of a monic cubic irreducible polynomial $f(x)$ over k_4, we examine the condition of Proposition 2:

$$\exists A \in k_4^\times, B \in k_4, \text{satisfying } \gamma = A\delta + B, \delta^{1+q^6} = 1.$$

For $\gamma \in k_{12}$, let

$$\mathrm{d}(\gamma) = (\gamma^{q^2+q^4} - \gamma^{q^2+1}) + (\gamma^{q^6+q^8} - \gamma^{q^6+q^4}) + (\gamma^{q^{10}+1} - \gamma^{q^{10}+q^8}) \tag{3}$$

We note that $\mathrm{d}(\gamma)^{q^4} = \mathrm{d}(\gamma)$, $\mathrm{d}(\gamma)^{q^2} = -\mathrm{d}(\gamma)$.

Lemma 2. *For $\gamma \in k_{12} \setminus k_4$, we have $\mathrm{d}(\gamma) \neq 0$ if and only if γ satisfies the condition of Proposition 2. In such a case, A, B in the condition of Proposition 2 are given by*

$$\begin{aligned} B &= \mathrm{d}(\gamma)^{-1}(\gamma(\gamma^{q^6+q^8} - \gamma^{q^4+q^6}) + \gamma^{q^4}(\gamma^{q^{10}+1} - \gamma^{q^8+q^{10}}) \\ &\quad + \gamma^{q^8}(\gamma^{q^2+q^4} - \gamma^{1+q^2})), \\ C &= \mathrm{N}_{k_{12}|k_6}(\gamma - B), \\ A &= \begin{cases} \sqrt{C} & \text{if } C \in {k_2^\times}^2 \\ \sqrt{-C} & \text{if } C \notin {k_2^\times}^2 \end{cases}. \end{aligned}$$

Proof. ($\Rightarrow$) Suppose $\mathrm{d}(\gamma) \neq 0$. Since $\mathrm{N}_{k_4|k_2}$ is surjective, we only need to show $(\gamma - B)^{1+q^6} \in k_2$ for some $B \in k_4$ (For $A^{1+q^2} = A^{1+q^6} = (\gamma - B)^{1+q^6}$, let $\delta = (\gamma - B)/A$). For that sake, we see an equation for B:

$$(\gamma - B)^{q^2}(\gamma^{q^6} - B^{q^6})^{q^2} - (\gamma - B)(\gamma^{q^6} - B^{q^6}) = 0 \tag{4}$$

has a solution in k_4. Letting $B^{q^4} = B$, equation (4) is expanded as:

$$\gamma^{q^2+q^8} - \gamma^{q^2}B - B^{q^2}\gamma^{q^8} + B^{q^2+1} - (\gamma^{1+q^6} - \gamma B^{q^2} - B\gamma^{q^6} + B^{1+q^2}) = 0.$$

Collecting terms of B,

$$(\gamma^{q^2} - \gamma^{q^6})B + (\gamma^{q^8} - \gamma)B^{q^2} - \gamma^{q^2+q^8} + \gamma^{1+q^6} = 0. \tag{5}$$

Applying q^2-Frobenius,

$$(\gamma^{q^4} - \gamma^{q^8})B^{q^2} + (\gamma^{q^{10}} - \gamma^{q^2})B - \gamma^{q^4+q^{10}} + \gamma^{q^2+q^8} = 0. \tag{6}$$

Equations (5) and (6) are written with matrices as

$$\begin{pmatrix} \gamma^{q^2} - \gamma^{q^6} & \gamma^{q^8} - \gamma \\ \gamma^{q^{10}} - \gamma^{q^2} & \gamma^{q^4} - \gamma^{q^8} \end{pmatrix} \begin{pmatrix} B \\ B^{q^2} \end{pmatrix} = \begin{pmatrix} -\gamma^{1+q^6} + \gamma^{q^2+q^8} \\ -\gamma^{q^2+q^8} + \gamma^{q^4+q^{10}} \end{pmatrix} \tag{7}$$

The determinant of the coefficient matrix is computed to be

$$\begin{aligned} & (\gamma^{q^2} - \gamma^{q^6})(\gamma^{q^4} - \gamma^{q^8}) - (\gamma^{q^8} - \gamma)(\gamma^{q^{10}} - \gamma^{q^2}) \\ = \; & (\gamma^{q^2+q^4} - \gamma^{1+q^2}) + (\gamma^{q^6+q^8} - \gamma^{q^6+q^4}) + (\gamma^{1+q^{10}} - \gamma^{q^8+q^{10}}). \end{aligned}$$

This is equal to $\mathrm{d}(\gamma)$, which is not zero by assumption. Therefore,

$$\begin{pmatrix} B \\ B^{q^2} \end{pmatrix} = \mathrm{d}(\gamma)^{-1} \begin{pmatrix} \gamma^{q^4} - \gamma^{q^8} & -\gamma^{q^8} + \gamma \\ -\gamma^{q^{10}} + \gamma^{q^2} & \gamma^{q^2} - \gamma^{q^6} \end{pmatrix} \begin{pmatrix} -\gamma^{1+q^6} + \gamma^{q^2+q^8} \\ -\gamma^{q^2+q^8} + \gamma^{q^4+q^{10}} \end{pmatrix}.$$

So, we have

$$\begin{aligned} B &= \mathrm{d}(\gamma)^{-1}(\gamma(\gamma^{q^6+q^8} - \gamma^{q^4+q^6}) + \gamma^{q^4}(\gamma^{q^{10}+1} - \gamma^{q^8+q^{10}}) \\ &\quad + \gamma^{q^8}(\gamma^{q^2+q^4} - \gamma^{1+q^2})). \end{aligned}$$

For this B we have

$$B^{q^4} = \mathrm{d}(\gamma)^{-1}(\gamma^{q^4}(\gamma^{q^{10}+1}-\gamma^{q^8+q^{10}})+\gamma^{q^8}(\gamma^{q^2+q^4}-\gamma^{1+q^2})+\gamma(\gamma^{q^6+q^8}-\gamma^{q^4+q^6})),$$

which implies $B = B^{q^4}$, i.e., $B \in k_4$.

($\Leftarrow$) Suppose $\mathrm{d}(\gamma) = 0$, i.e.

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

If $(\gamma - B)^{1+q^6} \in k_2$ for some $B \in k_4$, then equation (7) has a solution B. Then, since the determinant of the coefficient matrix of equation (7) is equal to $\mathrm{d}(\gamma) = 0$, we must have

$$\frac{\gamma^{q^2} - \gamma^{q^6}}{\gamma^{q^{10}} - \gamma^{q^2}} = \frac{\gamma^{q^8} - \gamma}{\gamma^{q^4} - \gamma^{q^8}} = \frac{\gamma^{1+q^6} - \gamma^{q^2+q^8}}{\gamma^{q^2+q^8} - \gamma^{q^4+q^{10}}}.$$

So,

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

Expanding,

$$\gamma^{1+q^4+q^6} + \gamma^{q^4+q^8+q^{10}} + \gamma^{1+q^2+q^8} - \gamma^{1+q^4+q^{10}} - \gamma^{q^2+q^4+q^8} - \gamma^{1+q^6+q^8} = 0. \tag{9}$$

Adding γ^{q^4}-times equation (8) to equation (9),

$$\begin{aligned}&\gamma^{1+q^4+q^6} + \gamma^{1+q^2+q^8} - \\ &\gamma^{q^2+q^4+q^8} - \gamma^{1+q^6+q^8} + \gamma^{q^2+2q^4} - \gamma^{q^2+1+q^4} + \gamma^{q^6+q^8+q^4} - \gamma^{q^6+2q^4} = 0.\end{aligned}$$

However, the left-hand side is factored as

$$(\gamma^{q^6} - \gamma^{q^2})(\gamma - \gamma^{q^4})(\gamma^{q^4} - \gamma^{q^8}) = 0.$$

This implies $\gamma \in k_4$, which contradicts the assumption. $\square$

From Propositions 1 and 2 and Lemma 2, we have

Theorem 1. *Let $f(x)$ be an irreducible monic cubic polynomial over k_4. Let γ be a root of $f(x)$. The necessary and sufficient condition for Weierstrass form $y^2 = f(x)$ to be isomorphic to Scholten form over k_4 is that $\mathrm{d}(\gamma) \neq 0$. More precisely, in such a case, for*

$$\begin{aligned}B &= \mathrm{d}(\gamma)^{-1}(\gamma(\gamma^{q^6+q^8} - \gamma^{q^4+q^6}) + \gamma^{q^4}(\gamma^{q^{10}+1} - \gamma^{q^8+q^{10}}) \\ &\quad + \gamma^{q^8}(\gamma^{q^2+q^4} - \gamma^{1+q^2})),\\ C &= \mathrm{N}_{k_{12}|k_6}(\gamma - B),\\ A &= \begin{cases} \sqrt{C} & \text{if } C \in (k_2^\times)^2 \\ \sqrt{-C} & \text{if } C \notin (k_2^\times)^2 \end{cases},\end{aligned}$$

let

$$\begin{aligned} a &= -A^{2-q^2}\delta^{1+q^4-q^2} \\ b &= -A(\delta+\delta^{q^4}+\delta^{-q^2}). \end{aligned}$$

Weierstrass form $E_w : y^2 = f(x)$ on k_4 is transformed into Scholten form $E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ on k_4 by translation $y \to ay, x \to ax + B$ over k_4.

Next, we examine the condition $\mathrm{d}(\gamma) \neq 0$.

Lemma 3. *Let $f(x)$ be an irreducible monic cubic polynomial over k_4. For Weierstrass form $E_w : y^2 = f(x)$ on k_4, the condition $\mathrm{j}(E_w) \in k_2$ is equivalent to the condition that a root γ of $f(x)$ is given by*

$$\gamma = A\alpha + B$$

with some $A \in k_4^\times, B \in k_4$ and $\alpha \in k_6$.

Proof. ($\Rightarrow$) By the condition $\mathrm{j}(E_w) \in k_2$, we see that for some transformation $y \to Cy, x \to Ax + B$ ($C^2 = A^3$) over k_4, the elliptic curve $y^2 = C^{-2}f(Ax+B)$ becomes an elliptic curve $y^2 = (x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^4})$ over k_2, or its twist $y^2 = (x-D\alpha)(x-D\alpha^{q^2})(x-D\alpha^{q^4})$ over k_4 (D is a non-square in k_4). Then, we have $\gamma = A\alpha + B$ or $\gamma = AD\alpha + B$.

($\Leftarrow$) Applying transformation $x \to Ax + B, y \to A^{\frac{3}{2}}y$ over k_8 for $E_w : y^2 = f(x) = (x-\gamma)(x-\gamma^{q^4})(x-\gamma^{q^8})$, we have

$$\begin{aligned} y^2 &= A^{-3}(Ax+B-(A\alpha+B))(Ax+B-(A\alpha^{q^4}+B))(Ax+B-(A\alpha^{q^2}+B)) \\ &= (x-\alpha)(x-\alpha^{q^4})(x-\alpha^{q^2}). \end{aligned}$$

So, $\mathrm{j}(E_w) \in k_2$. ☐

Proposition 3. *Let $f(x)$ be an irreducible monic cubic polynomial over k_4. Let γ be a root of $f(x)$. If $\mathrm{j}(E_w) \in k_2$ for Weierstrass form $E_w : y^2 = f(x)$, then we have $\mathrm{d}(\gamma) = 0$.*

Proof. By Lemma 3, there are some $A \in k_4^\times, B \in k_4$ and $\alpha \in k_6$ satisfying

$$\gamma = A\alpha + B.$$

By Lemma 2, we know

$$\mathrm{d}(\gamma) = 0 \Longleftrightarrow \mathrm{d}(\gamma - B) = 0.$$

So, we can suppose $B = 0$, i.e. $\gamma = A\alpha$. Let

$$d_0(\gamma) = \gamma^{q^2+q^4} + \gamma^{q^6+q^8} + \gamma^{q^{10}+1},$$

then we have $\mathrm{d}(\gamma) = d_0(\gamma) - d_0(\gamma)^{q^2}$. So, to show the proposition, we only have to show $d_0(\gamma) \in k_2$. By $\gamma = A\alpha$,

$$\begin{aligned} d_0(\gamma) &= A^{1+q^2}(\alpha^{q^2+q^4} + \alpha^{1+q^2} + \alpha^{q^4+1}) \\ &= \mathrm{N}_{k_4|k_2}(A)\mathrm{T}_{k_6|k_2}(\alpha^{1+q^2}). \end{aligned}$$

□

When the characteristic of k is not there, we can show the contrary:

Proposition 4. *Let the characteristic of k be different from there (or two). Let $f(x)$ be an irreducible monic cubic polynomial over k_4. Let γ be a root of $f(x)$. If $\mathrm{d}(\gamma) = 0$, then we have $\mathrm{j}(E_w) \in k_2$ for Weierstrass form $E_w : y^2 = f(x)$.*

Proof. We can suppose

$$\gamma + \gamma^{q^4} + \gamma^{q^8} = 0, \tag{10}$$

by letting $\gamma = \gamma - \frac{1}{3}\mathrm{T}_{k_{12}|k_4}(\gamma)$ if necessary (we notice that $\mathrm{d}(\gamma)$ remains to be zero by Lemma 2). To show the proposition, it is sufficient to show

$$A := \frac{\gamma}{\gamma + \gamma^{q^6}} \in k_4$$

by Lemma 3 (If $\gamma + \gamma^{q^6} = \mathrm{T}_{k_{12}|k_6}(\gamma) = 0$, let $\gamma = a\gamma$ for some $a \in k_4$). Since

$$A - A^{q^4} = \frac{\gamma^{1+q^{10}} - \gamma^{q^4+q^6}}{(\gamma + \gamma^{q^6})(\gamma^{q^4} + \gamma^{q^{10}})},$$

it is sufficient to show

$$\gamma^{1+q^{10}} - \gamma^{q^4+q^6} = 0.$$

By the assumption $\mathrm{d}(\gamma) = 0$, we have

$$(\gamma^{q^{10}+1} - \gamma^{q^6+q^4}) + (\gamma^{q^2+q^4} - \gamma^{q^{10}+q^8}) + (\gamma^{q^6+q^8} - \gamma^{q^2+1}) = 0. \tag{11}$$

Using equation (10),

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

and

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

So, by equation (11), we see $\gamma^{1+q^{10}} - \gamma^{q^4+q^6} = 0$. □

Summarizing foregoing arguments, for an irreducible monic cubic polynomial $f(x)$ over k_4 and for its root γ, we have

$$\begin{array}{lcl} E_w : y^2 = f(x) \text{ can be Scholten form} & \stackrel{\text{Prop. 1, 2}}{\Longleftrightarrow} & \delta = A\gamma + B, \delta^{1+q^6} = 1 \\ & & (\exists A \in k_4^\times, B \in k_4) \\ & \stackrel{\text{Lemma 2}}{\Longleftrightarrow} & \mathrm{d}(\gamma) \neq 0 \\ & \stackrel{\text{Prop. 3, 4}}{\Longleftrightarrow} & \mathrm{j}(E_w) \notin k_2 \end{array}$$

Here, $\Leftarrow$ on the last line is shown only when the characteristic of k is not three.

Remark 2. *Even in the case of $j(E) \in k_2$, we could find an elliptic curve E' over k_4 with $j(E') \notin k_2$, which is isogenious to E. Then DLP on E also reduced to DLP on a genus two hyperelliptic curve on k via DLP on E' (See [10]).*

2.2.2 The case of $f(x)$ being reducible over k_4

Now, we consider the case of Weierstrass form $E_w : y^2 = f(x)$ with a reducible $f(x)$ over k_4.

First, we consider the case of $f(x)$ being a product of a linear polynomial and an irreducible quadratic polynomial over k_4. For such a $f(x)$, we assume Weierstrass form $E_w : y^2 = f(x)$ on k_4 is transformed into Scholten form $E_n : y^2 = F(x)$ by transformation $x \to Ax + B, y \to Cy$ over k_4. Then, (up to a scalar multiplication,) $F(x)$ also is a product of a linear polynomial $x - c$ and an irreducible polynomial $(x - \delta_1)(x - \delta_2)$ over $k_4(c \in k_4, \delta_i \in k_8 - k_4)$. As seen in Section 2.2.1, by the form of defining equation of Scholten form, $\delta_1^{-q^2}$ is also a root of $F(x)$. So, we have $\delta_1^{-q^2} = \delta_1$ or $\delta_1^{-q^2} = \delta_2$. If $\delta_1^{-q^2} = \delta_1$, then $\delta_1^{1+q^2} = 1$ and $\delta_1 \in k_4$ which is a contradiction. If $\delta_1^{-q^2} = \delta_2$, then $\delta_1^{q^4} = \delta_2 = \delta_1^{-q^2}$ and $\delta_1^{q^2} = \delta_1^{-1}$, which also implies $\delta_1 \in k_4$. Hence,

Proposition 5. *If a monic cubic polynomial $f(x)$ is a product of a linear polynomial and an irreducible quadratic polynomial over k_4, then Weierstrass form $E_w : y^2 = f(x)$ on k_4 is never k_4-isomorphic to Scholten form.*

From now on, in this section, we consider the case of $f(x)$ which is completely factored over k_4. Scholten [20] has already shown that Weierstrass form $E_w : y^2 = f(x)$ with such $f(x)$ is always transformed into Scholten form over k_4. Here, we show the same result in the way of Section 2.2.1, which is different from Scholten's method.

As in Section 2.2.1, we have

Proposition 6. *If Weierstrass form $E_w : y^2 = f(x) = (x - \gamma_1)(x - \gamma_2)(x - \gamma_3)$ with three different elements $\gamma_1, \gamma_2, \gamma_3$ in k_4 is k_4-isomorphic to Scholten form, then we can suppose the following (i) or (ii) holds:*

(i) δ_i $(i=1,2,3)$ *defined by* $\gamma_i = A\delta_i + B$ *with some* $A \in k_4^\times, B \in k_4$ *satisfy* $\delta_1^{-q^2} = \delta_1,\ \delta_2^{-q^2} = \delta_2,\ \delta_3^{-q^2} = \delta_3.$

(ii) δ_i $(i=1,2,3)$ *defined by* $\gamma_i = A\delta_i + B$ *with some* $A \in k_4^\times, B \in k_4$ *satisfy* $\delta_1^{-q^2} = \delta_1,\ \delta_2^{-q^2} = \delta_3,\ \delta_3^{-q^2} = \delta_2.$

Proof. By assumption, Weierstrass form $E_w : y^2 = f(x)$ is transformed into Scholten form $E_n : y^2 = F(x)$ by transformation $x \to Ax + B, y \to Cy$ over k_4. Since $F(x) = C^{-2} f(Ax+B)$, $F(x)$ also is completely factored over k_4. Let roots of $F(x)$ be $\delta_1, \delta_2, \delta_3$. By the definition of Scholten form, $\delta_i^{-q^2}$ is a root of $F(x)$. The correspondence $\delta_i \mapsto \delta_i^{-q^2}$ has order one or two as a permutation of the set of roots $\{\delta_1, \delta_2, \delta_3\}$. □

The contrary holds also in this case:

Proposition 7. *Suppose distinct three elements* $\gamma_1, \gamma_2, \gamma_3$ *in* k_4 *satisfy the following condition (i) or (ii):*

(i) δ_i $(i=1,2,3)$ *defined by* $\gamma_i = A\delta_i + B$ *with some* $A \in k_4^\times, B \in k_4$ *satisfy* $\delta_1^{-q^2} = \delta_1,\ \delta_2^{-q^2} = \delta_2,\ \delta_3^{-q^2} = \delta_3.$

(ii) δ_i $(i=1,2,3)$ *defined by* $\gamma_i = A\delta_i + B$ *with some* $A \in k_4^\times, B \in k_4$ *satisfy* $\delta_1^{-q^2} = \delta_1,\ \delta_2^{-q^2} = \delta_3,\ \delta_3^{-q^2} = \delta_2.$

Let

$$\begin{aligned} a &= -A^{2-q^2}\delta_1\delta_2\delta_3, \\ b &= -A(\delta_1+\delta_2+\delta_3). \end{aligned}$$

Then, Weierstrass form $E_w : y^2 = f(x) = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)$ *on* k_4 *is transformed into Scholten form* $E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ *by transformation* $y \to ay, x \to ax + B$ *over* k_4.

Proof. We can suppose $B = 0$ by a transformation $y \to y, x \to x + B$. Under the assumption (i) or (ii), we have

$$\{\delta_1^{q^2}, \delta_2^{q^2}, \delta_3^{q^2}\} = \{\delta_1^{-1}, \delta_2^{-1}, \delta_3^{-1}\}.$$

For $f(x) = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)$,

$$\begin{aligned} \text{the coefficient of } x^2 &= -(\gamma_1+\gamma_2+\gamma_3) \\ &= -A(\delta_1+\delta_2+\delta_3) \\ &= b, \end{aligned}$$

$$\begin{aligned} \text{the coefficient of } x &= \gamma_1\gamma_2 + \gamma_2\gamma_3 + \gamma_3\gamma_1 \\ &= A^2(\delta_1\delta_2 + \delta_2\delta_3 + \delta_3\delta_1) \\ &= -A^{2-q^2}\delta_1\delta_2\delta_3 \cdot (-1) \cdot A^{q^2}(\delta_1^{q^2} + \delta_2^{q^2} + \delta_3^{q^2}) \\ &= ab^{q^2}, \end{aligned}$$

and

$$\begin{aligned}
\text{the constant term} &= -\gamma_1\gamma_2\gamma_3 \\
&= -A^3\delta_1\delta_2\delta_3 \\
&= -A^{2q^2-1}\delta_1^{q^2}\delta_2^{q^2}\delta_3^{q^2}\cdot A^{4-2q^2}(\delta_1\delta_2\delta_3)^2 \\
&= a^{q^2}a^2.
\end{aligned}$$

So, we have

$$y^2 = x^3 + bx^2 + ab^{q^2}x + a^{q^2}a^2.$$

By a transformation $y \to ay, x \to ax$, this is transformed into

$$E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}.$$

□

Let

$$\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3) = (\gamma_1\gamma_2^{q^2} + \gamma_2\gamma_3^{q^2} + \gamma_3\gamma_1^{q^2}) - (\gamma_1\gamma_3^{q^2} + \gamma_2\gamma_1^{q^2} + \gamma_3\gamma_2^{q^2}).$$

We have $\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)^{q^2} = -\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)$.

Lemma 4. *For distinct three elements $\gamma_1,\gamma_2,\gamma_3$ in k_4, $\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3) \neq 0$ is equivalent to the condition (i) in Proposition 7. In such a case, A, B in the condition (i) are given by*

$$\begin{aligned}
B &= \mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)^{-1}(\gamma_3\gamma_1^{1+q^2} + \gamma_1\gamma_2^{1+q^2} + \gamma_2\gamma_3^{1+q^2} \\
&\quad -(\gamma_2\gamma_1^{1+q^2} + \gamma_3\gamma_2^{1+q^2} + \gamma_1\gamma_3^{1+q^2})), \\
A &= \begin{cases} \sqrt{C} & \text{if } C \in k_2^{\times 2} \\ \sqrt{-C} & \text{if } C \notin k_2^{\times 2} \end{cases},
\end{aligned}$$

with $C = \mathrm{N}_{k_4|k_2}(\gamma_1 - B)$.

Proof. ($\Rightarrow$) Suppose $\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3) \neq 0$. We only need to show $\mathrm{N}_{k_4|k_2}(\gamma_1 - B) = \mathrm{N}_{k_4|k_2}(\gamma_2 - B) = \mathrm{N}_{k_4|k_2}(\gamma_3 - B) = C$ for some $B \in k_4$ (For $A^{1+q^2} = (\gamma_i - B)^{1+q^2}$, let $\delta_i = (\gamma_i - B)/A$). For that sake, it is sufficient to show an equation for B

$$(\gamma_1 - B)(\gamma_1^{q^2} - B^{q^2}) = (\gamma_2 - B)(\gamma_2^{q^2} - B^{q^2}) \tag{12}$$

$$(\gamma_2 - B)(\gamma_2^{q^2} - B^{q^2}) = (\gamma_3 - B)(\gamma_3^{q^2} - B^{q^2}) \tag{13}$$

has a solution in k_4. By equations (12),(13), we have

$$\begin{pmatrix} \gamma_1 - \gamma_2 & \gamma_1^{q^2} - \gamma_2^{q^2} \\ \gamma_2 - \gamma_3 & \gamma_2^{q^2} - \gamma_3^{q^2} \end{pmatrix} \begin{pmatrix} B^{q^2} \\ B \end{pmatrix} = \begin{pmatrix} -\gamma_2^{1+q^2} + \gamma_1^{1+q^2} \\ -\gamma_3^{1+q^2} + \gamma_2^{1+q^2} \end{pmatrix}. \tag{14}$$

The determinant of the coefficient matrix is computed to be

$$\begin{aligned}
& (\gamma_1-\gamma_2)(\gamma_2^{q^2}-\gamma_3^{q^2})-(\gamma_2-\gamma_3)(\gamma_1^{q^2}-\gamma_2^{q^2}) \\
= \quad & (\gamma_1\gamma_2^{q^2}+\gamma_2\gamma_3^{q^2}+\gamma_3\gamma_1^{q^2})-(\gamma_1\gamma_3^{q^2}+\gamma_2\gamma_1^{q^2}+\gamma_3\gamma_2^{q^2})
\end{aligned}$$

which is equal to $\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)\neq 0$. So,

$$B=\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)^{-1}(\gamma_3\gamma_1^{1+q^2}+\gamma_1\gamma_2^{1+q^2}+\gamma_2\gamma_3^{1+q^2}-(\gamma_2\gamma_1^{1+q^2}+\gamma_3\gamma_2^{1+q^2}+\gamma_1\gamma_3^{1+q^2}))$$

($\Leftarrow$) Suppose $\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)=0$, i.e.

$$(\gamma_1\gamma_2^{q^2}+\gamma_2\gamma_3^{q^2}+\gamma_3\gamma_1^{q^2})-(\gamma_1\gamma_3^{q^2}+\gamma_2\gamma_1^{q^2}+\gamma_3\gamma_2^{q^2})=0. \tag{15}$$

If we have $\mathrm{N}_{k_4|k_2}(\gamma_1-B)=\mathrm{N}_{k_4|k_2}(\gamma_2-B)=\mathrm{N}_{k_4|k_2}(\gamma_3-B)$ for some $B\in k_4$, then an equation (14) has a solution $B\in k_4$. Since the determinant of the coefficient matrix of equation(14) is equal to $\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)=0$, we must have

$$\frac{\gamma_1^{q^2}-\gamma_2^{q^2}}{\gamma_2^{q^2}-\gamma_3^{q^2}}=\frac{\gamma_2^{1+q^2}-\gamma_1^{1+q^2}}{\gamma_3^{1+q^2}-\gamma_2^{1+q^2}}.$$

So,

$$\gamma_1^{q^2}\gamma_3^{1+q^2}+\gamma_2^{q^2}\gamma_1^{1+q^2}+\gamma_3^{q^2}\gamma_2^{1+q^2}-(\gamma_1^{q^2}\gamma_2^{1+q^2}+\gamma_2^{q^2}\gamma_3^{1+q^2}+\gamma_3^{q^2}\gamma_1^{1+q^2})=0. \tag{16}$$

By subtracting $\gamma_1^{q^2}$ times equation (15) from equation (16),

$$\begin{aligned}
\gamma_1^{q^2}\gamma_3^{1+q^2}-\gamma_1^{q^2}\gamma_2\gamma_3^{q^2}+\gamma_3^{q^2}\gamma_2^{1+q^2}-\gamma_2^{q^2}\gamma_3^{1+q^2} & \\
-\gamma_1^{q^2}\gamma_2^{1+q^2}+\gamma_1^{q^2}\gamma_3\gamma_2^{q^2}-\gamma_3\gamma_1^{2q^2}+\gamma_2\gamma_1^{2q^2} &= 0, \\
(\gamma_3-\gamma_2)\{(\gamma_3-\gamma_1)(\gamma_1-\gamma_2)\}^{q^2} &= 0.
\end{aligned}$$

So, we have $\gamma_1=\gamma_2$ or $\gamma_2=\gamma_3$ or $\gamma_3=\gamma_1$ which is a contradiction. $\square$

By Proposition 7, and Lemma 4,

Theorem 2. *For distinct three elements $\gamma_1,\gamma_2,\gamma_3$ in k_4, suppose $\mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)\neq 0$. Let*

$$\begin{aligned}
B &= \mathrm{d}_2(\gamma_1,\gamma_2,\gamma_3)^{-1}(\gamma_3\gamma_1^{1+q^2}+\gamma_1\gamma_2^{1+q^2}+\gamma_2\gamma_3^{1+q^2} \\
&\quad -(\gamma_2\gamma_1^{1+q^2}+\gamma_3\gamma_2^{1+q^2}+\gamma_1\gamma_3^{1+q^2})), \\
C &= \mathrm{N}_{k_4|k_2}(\gamma_1-B), \\
A &= \begin{cases} \sqrt{C} & \text{if } C\in {k_2^\times}^2 \\ \sqrt{-C} & \text{if } C\notin {k_2^\times}^2 \end{cases}
\end{aligned}$$

and let

$$\begin{aligned}
\delta_i &= A^{-1}(\gamma_i-B) \ (i=1,2,3), \\
a &= -A^{2-q^2}\delta_1\delta_2\delta_3, \\
b &= -A(\delta_1+\delta_2+\delta_3).
\end{aligned}$$

Then, Weierstrass form $E_w : y^2 = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)$ on k_4 is transformed into Scholten form $E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ by a transformation $y \to ay, x \to ax + B$ over k_4.

Next we consider the case of $\mathrm{d}_2(\gamma_1, \gamma_2, \gamma_3) = 0$ for distinct three elements $\gamma_1, \gamma_2, \gamma_3$ in k_4. If the characteristic of k is not 3, we can assume $\gamma_2+\gamma_3-2\gamma_1 \neq 0$ without loss of generality. In fact, equations

$$\begin{aligned} \gamma_2 + \gamma_3 - 2\gamma_1 = 0, \\ \gamma_3 + \gamma_1 - 2\gamma_2 = 0, \\ \gamma_1 + \gamma_2 - 2\gamma_3 = 0 \end{aligned}$$

implies $3\gamma_2 = 3\gamma_3$.

Lemma 5. *Suppose the characteristic of k is not 3, and $\gamma_2 + \gamma_3 - 2\gamma_1 \neq 0$ for distinct three elements $\gamma_1, \gamma_2, \gamma_3$ in k_4. Then, if $\mathrm{d}_2(\gamma_1, \gamma_2, \gamma_3) = 0$, condition (ii) in Proposition 7 holds. In such a case, A, B in condition (ii) are given by*

$$\begin{aligned} A &= \frac{\alpha^2\gamma - \alpha\gamma^{2+q^2}}{\gamma^{2+2q^2} - \alpha^2}, \\ B &= -A + \gamma_1 \end{aligned}$$

with

$$\begin{aligned} \alpha &= (\gamma_2 - \gamma_1)(\gamma_3 - \gamma_1)^{q^2}, \\ \gamma &= \gamma_2 - \gamma_1. \end{aligned}$$

Proof. We can suppose $\gamma_1 = 0$ by a transformation $x \mapsto x + \gamma_1, y \mapsto y$. By assumption, we have $\gamma_2 \pm \gamma_3 \neq 0$. Moreover,

$$0 = \mathrm{d}_2(0, \gamma_2, \gamma_3) = \gamma_2\gamma_3^{q^2} - \gamma_2^{q^2}\gamma_3.$$

(We note that the property of $\mathrm{d}_2(\gamma_1, \gamma_2, \gamma_3) = 0$ remains valid under a transformation $x \mapsto x + \gamma_1, y \mapsto y$ by Lemma 4.)

So, we have $\alpha := \gamma_2\gamma_3^{q^2} \in k_2$. Let $\gamma = \gamma_2$. Roots of $f(x)$ are $0, \gamma, \frac{\alpha}{\gamma^{q^2}}$. By $\gamma_2 \pm \gamma_3 \neq 0$, we have $\alpha \pm \gamma^{1+q^2} \neq 0$.

Let $k_4 \ni A = \frac{\alpha^2\gamma - \alpha\gamma^{2+q^2}}{\gamma^{2+2q^2} - \alpha^2}$. By a transformation $x \mapsto x - A$, roots of $f(x)$ are transformed as follows:

$$\begin{array}{ccc} 0 & \mapsto & A \\ \gamma & \mapsto & A(1 + \frac{\gamma}{A}) \\ \frac{\alpha}{\gamma^{q^2}} & \mapsto & A(1 + \frac{\alpha}{A\gamma^{q^2}}) \end{array} .$$

Here, we let

$$\begin{aligned} \delta_2 &:= 1 + \frac{\gamma}{A} \\ &= \frac{\gamma^{2+2q^2} - \alpha\gamma^{1+q^2}}{\alpha^2 - \alpha\gamma^{1+q^2}}. \end{aligned}$$

and

$$\begin{aligned}\delta_3 &:= 1 + \frac{\alpha}{A\gamma^{q^2}} \\ &= \frac{\alpha\gamma^{1+q^2} - \alpha^2}{\alpha\gamma^{1+q^2} - \gamma^{2+2q^2}}.\end{aligned}$$

Then, since $\delta_2, \delta_3 \in k_2$ and $\delta_2 = \delta_3^{-1}$, δ_i's satisfy condition (ii) in Proposition 7. □

By Proposition 7 and Lemma 5,

Theorem 3. *Suppose the characteristic of* k *is not 3, and* $\mathrm{d}_2(\gamma_1, \gamma_2, \gamma_3) = 0$ *for distinct three elements* $\gamma_1, \gamma_2, \gamma_3$ *in* k_4*. Let*

$$\begin{aligned}\alpha &= (\gamma_2 - \gamma_1)(\gamma_3 - \gamma_1)^{q^2}, \\ \gamma &= \gamma_2 - \gamma_1, \\ A &= \frac{\alpha^2\gamma - \alpha\gamma^{2+q^2}}{\gamma^{2+2q^2} - \alpha^2}, \\ B &= -A + \gamma_1\end{aligned}$$

and let

$$\begin{aligned}\delta_i &= A^{-1}(\gamma_i - B) \ (i = 1, 2, 3), \\ a &= -A^{2-q^2}\delta_1\delta_2\delta_3, \\ b &= -A(\delta_1 + \delta_2 + \delta_3).\end{aligned}$$

Then, Weierstrass form $E_w : y^2 = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)$ *on* k_4 *is transformed into Scholten form* $E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ *by a transformation* $y \to ay, x \to ax + B$ *over* k_4*.*

2.3 Example

We take an example of an elliptic curve of Weierstrass form over a quartic extension field of prime order, and we see it is transformed into Scholten form, and see the Scholten form is covered by a genus two hyperelliptic curve over the quadratic field. We used Magma V.2.10 for computations below.

Let k be a prime field of characteristic $q = p = 71$, k_2 be its quadratic extension defined by an irreducible polynomial $o^2 - 2o + 7$, and k_4 be its quadratic extension defined by an irreducible polynomial $r^2 - or + 1$.

We generate randomly an elliptic curve of Weierstrass form $E_w : v_1^2 + 70u_1^3 + (o^{2058}r + o^{4231})u_1 + o^{3375}r + o^{2069} = 0$ on k_4 to have a prime order $n = 25404727$. Since $\mathrm{j}(E_w) = o^{1854}r + o^{2692} \notin k_2$, we have $\mathrm{d}(\gamma) \neq 0$ by Proposition 4. Hence, by Theorem 1, E_w is transformed into Scholten form $v^2 = au^3 + bu^2 + b^{q^2}u + a^{q^2}$ over k_4. In fact, let

$a = o^{2258}r + o^{214}$,
$b = o^{3519}r + o^{2654}$,
$B = -(o^{4167}r + o^{3302})$.

Then, by a transformation $\Pi_2^{(1)} : E_n \simeq E_w$ over k_4 defined by

$$u = a^{-1}(u_1 - B),$$
$$v = a^{-1}v_1,$$

E_w is transformed into $E_n : v^2 = au^3 + bu^2 + b^{q^2}u + a^{q^2} = (o^{2258}r + o^{214})u^3 + (o^{3519}r + o^{2654})u^2 + (o^{999}r + o^{3103})u + o^{4778}r + o^{355}$.

As seen in Section 2.1, Scholten form E_n is covered by a genus two hyperelliptic curve $H_0 : y_0^2 = a(x_0-c)^6 + b(x_0-c)^4(x_0-c^{q^2})^2 + b^{q^2}(x_0-c)^2(x_0-c^{q^2})^4 + a^{q^2}(x_0 - c^{q^2})^6 = o^{1463}x_0^6 + o^{666}x_0^5 + o^{2070}x_0^4 + o^{1093}x_0^3 + o^{794}x_0^2 + o^{315}x_0 + o^{1939}$. A morphism $\Pi_2^{(2)}$ from H_0 to E_n is given by

$$u = \left(\frac{x_0 - c}{x_0 - c^{q^2}}\right)^2,$$
$$v = \frac{y_0}{(x_0 - c^{q^2})^3}.$$

In the computations, we take $c = r$.

Let $F(x_0)$ denote the right-hand side of the equation for H_0. In order to make $F(x_0)$ monic, we apply a transformation $\Pi_2^{(3)} : H \simeq H_0$ defined by

$$y_1 = F(\beta)^{-1/2}(x_0 - \beta)^{-3}y_0,$$
$$x = 1/(x_0 - \beta)$$

with $\beta = 3$ (which makes $\alpha := F(\beta) = o^{2756}$ a square) to the equation for H_0. Then H_0 is transformed into a hyperelliptic curve $H : y_1^2 = x^6 + o^{2177}x^5 + o^{4311}x^4 + o^{2447}x^3 + o^{566}x^2 + o^{3664}x + o^{3747}$.

Let $\Pi_2 = \Pi_2^{(1)} \cdot \Pi_2^{(2)} \cdot \Pi_2^{(3)} : H \to E_w$. Take a point $G = (o^{387}r + o^{397}, o^{166}r + o^{1205})$ of order n on E_w. By the definition of $\Pi_2^{(i)} (i = 1, 2, 3)$, an inverse image $J = \Pi_2^*(G)$ of G via map $\Pi_2 : H \to E_w$ is computed to be zeros of

$$\begin{aligned} J &= \{a((\beta - c)x + 1)^2 - (G_x + \beta_2)((\beta - c^{q^2})x + 1)^2, \\ &\quad a\alpha^{1/2}y_1 - G_y((\beta - c^{q^2})x + 1)^3\} \\ &= \{(o^{353}r + o^{4196})x^2 + (o^{1900}r + o^{1805})x + o^{1922}r + o^{2318}, \\ &\quad (o^{3720}r + o^{1533})x^3 + (o^{1693}r + o^{4323})x^2 + (o^{3636}r + o^{1592})y_1 \\ &\quad +(o^{1256}r + o^{3701})x + o^{2686}r + o^{3725}\}, \end{aligned}$$

which, as an ideal of $k_4[x, y_1]$, represents an element of Jacobian of hyperelliptic curve H corresponding to G (G_x, G_y denotes x-coordinate and y-coordinate of G, respectively). We verified that discrete logarithm is preserved from G to J.

3 A Weil Descent Attack against Hyperelliptic Curve Cryptosystems over Quadratic Extension Fields

Here, we show Weil descent attack is effective in the almost all of the genus two hyperelliptic curve cryptosystems over quadratic extension field of odd characteristics.

Given a genus two hyperelliptic curve over a quadratic extension field k_2 of order q^2, we construct an algebraic curve of genus nine over the subfield k of order q using the technique of scalar restriction. We explicitly reduce DLP on the hyperelliptic curve to DLP on the new curve, and apply a variant [1] of Gaudry method against C_{ab} model [16, 4] of the curve. It solves DLP on the C_{ab} model over k in the amount of computations $O(q^{\frac{9}{5}})$, moreover new variants of Gaudry method solves in $O(q^{\frac{34}{19}})$ by [23], or $O(q^{\frac{17}{9}})$ by [17, 14]. Thus, DLP on genus two hyperelliptic curve over quadratic extension field k_2 can be solved by Weil descent attack in the amount of computations less than $O(q^2)$ via Pollard's ρ-method.

This means, with the result of Section 2, that Weil descent attack is effective in many of the elliptic curve cryptosystems over quartic extension fields of odd characteristics.

3.1 Weil descent of hyperelliptic curves and their GHS-sections

Let H be a genus two hyperelliptic curve defined on a finite field $k_2 = \mathbb{F}_{q^2}$ which is a quadratic extension of a finite field $k = F_q$ of characteristic different from 2:

$$H : y^2 = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f.$$

A scalar restriction $\Pi_{k_2/k}H$ of H with respect to the extension k_2/k is a two-dimensional algebraic variety defined by the following two conjugate equations

$$\begin{aligned} y_1^2 &= x_1^6 + ax_1^5 + bx_1^4 + cx_1^3 + dx_1^2 + ex_1 + f, \\ y_2^2 &= x_2^6 + a^q x_1^5 + b^q x_2^4 + c^q x_2^3 + d^q x_2^2 + e^q x_2 + f^q. \end{aligned}$$

Notice $\Pi_{k_2/k}H$ is geometrically defined on k. Let σ denote q-th Frobenius automorphism of k_2/k. σ can be extended to the automorphism of $\Pi_{k_2/k}H$ by

$$\sigma(x_1) = x_2, \sigma(y_1) = y_2.$$

In Weil descent attack, we should find an algebraic curve D on $\Pi_{k_2/k}H$, which is defined on k and is of genus as small as possible, and we reduce DLP on the hyperelliptic curve H to DLP on the curve D against which we apply Gaudry method [12]. Since the complexity of Gaudry method is $O(g!)$ with respect to genus g, the genus of D should be less than ten or around in the usual region of security parameters.

As seen above, in Weil descent attack, the choice of the curve D on $\Pi_{K/k}H$ is critical. In the presented paper, just as in [13] and [9], we let D be the intersection of $\Pi_{k_2/k}H$ and a hypersurface $(x :=)x_1 = x_2$, which we call 'GHS-section'. GHS-section D is an algebraic curve geometrically defined on k by equations

$$\begin{aligned} y_1^2 &= x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f, \\ y_2^2 &= x^6 + a^q x^5 + b^q x^4 + c^q x^3 + d^q x^2 + e^q x + f^q. \end{aligned}$$

Proposition 8. *If $F(x) := x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$ does not contain any non-trivial factor over k, then GHS-section D is a nonsingular affine curve.*

Proof. Suppose D is a singular curve. Since Jacobian matrix J of D is

$$J = \begin{pmatrix} F'(x) & 2y_1 & 0 \\ \bar{F}'(x) & 0 & 2y_2 \end{pmatrix}$$

with $\bar{F} := \sigma(F)$, both y_1 and y_2 must be zero on singular points. So, F and $\bar{F}$ contain non-trivial irreducible common factor a over k_2. Then, since $\bar{a}$ is also irreducible over k_2, we have $a = \bar{a}$ or a and $\bar{a}$ are prime to each other. However, by assumption, we cannot have $a = \bar{a}$, so a and $\bar{a}$ are prime to each other. Hence, $a\bar{a}$ be a factor over k of F, which is a contradiction. □

For simplicity, from now on we assume

Assumption 1 $F(x)$ does not contain any non-trivial factor over k,

for hyperelliptic curve $H : y^2 = F(x)$ to be attacked. However, even without Assumption 1, the attack remains unchanged except for the more complicated details of construction of C_{ab} model for D.

In cases of [13] and [9], GHS-sections D have huge genera. Remember that the complexity of Gaudry attack with respect to genus g is $O(g!)$. So, in [13] and [9] Weil descent attack can be applied only in special cases in which we can take irreducible components of small genus of GHS-section D.

However, in our cases,

Proposition 9. *The genus of GHS-section D is nine.*

Proof. Under Assumption 1, as seen in the proof of Proposition 8, $F(x)$ and $\bar{F}(x)$ are prime to each other. So, GHS-section D has twelve ramification points over H. Then, for genus g of D, by Hurwitz formula, we have $2g - 2 = 2 \cdot (2 \cdot 2 - 2) + 12 = 16$, which means $g = 9$. □

Therefore, we don't need to take irreducible components of D. The only thing we have to do is to construct a model over k of GHS-section D against which we can apply Gaudry attack. If we can construct such a model, DLP on H can be solved by Gaudry attack in the amount of computations $O(q^{\frac{2g}{g+1}}) = O(q^{\frac{9}{5}})$ [13], which is less than $O(q^2)$ for Pollard's ρ-method.

Gaudry attack is extended to C_{ab} curves [1] and for which we have an efficient addition algorithms in Jacobian [4]. So, hereafter, we construct a C_{ab} model over k of GHS-section D.

3.2 C_{ab} model of GHS-section

In general, to construct a C_{ab} model of a given curve D, we need to choose a point on D, which we call a "base point", and need to determine all of the regular functions outside the base point on D.

Remember that GHS-section D is defined by two equations

$$\begin{aligned} y_1^2 &= x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f, \\ y_2^2 &= x^6 + a^qx^5 + b^qx^4 + c^qx^3 + d^qx^2 + e^qx + f^q. \end{aligned}$$

Since GHS-section D is a double cover of hyperelliptic curve $y_1^2 = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$, GHS-section D has four points P_1, P_2, P_3 and P_4 at infinity. As seen later, P_4 is fixed by the automorphism σ. We choose the point P_4 at infinity as the base point of C_{ab} model of D. The property of P_4 being fixed by σ will be useful to construct C_{ab} model over k.

To determine all of the regular functions outside the base point P_4, we need to know the 'value' of a given function at points P_1, P_2, P_3, P_4 at infinity. First, we find local parameter expansions of coordinate functions at those points at infinity.

3.2.1 Points of GHS-section at infinity

Let $t := x^2/y_1$. t is a common local parameter of hyperelliptic curve H at points Q_1, Q_2 at infinity. Removing y_1 from the first equation of D with t, we get

$$t^{-2}x^4 = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f.$$

This has two solutions $x = -t^{-1} + \alpha_0^{(1)} + \alpha_1^{(1)}t + \cdots$ and $x = t^{-1} + \alpha_0^{(2)} + \alpha_1^{(2)}t + \cdots$, which give local parameter expansions of x at Q_1 and Q_2, respectively. Substituting this for x of $y_1 = t^{-1}x^2$, we get a local parameter expansion $y_1 = t^{-3} + \beta_{-2}^{(i)}t^{-2} + \beta_{-1}^{(i)}t^{-1} + \cdots$ of y_1 at Q_i $(i = 1, 2)$. Moreover, substituting local parameter expansion of x at Q_i for x in the second equation $y_2^2 = x^6 + a^qx^5 + b^qx^4 + c^qx^3 + d^qx^2 + e^qx + f^q$ of D, we get $y_2 = -t^{-3} + \gamma_{-2}^{(2i-1)}t^{-2} + \gamma_{-1}^{(2i-1)}t^{-1} + \cdots$ and $y_2 = t^{-3} + \gamma_{-2}^{(2i)}t^{-2} + \gamma_{-1}^{(2i)}t^{-1} + \cdots$, which give local parameter expansions of y_2 at two points of D at infinity over $Q_i (i = 1, 2)$, respectively. Thus, we get the following local parameter expansions of points P_1, P_2, P_3, P_4 on D at infinity:

$$
\begin{aligned}
P_1 &= \{x = -t^{-1} + \alpha_0^{(1)} + \alpha_1^{(1)} t + \cdots, \\
&\quad\ y_1 = t^{-3} + \beta_{-2}^{(1)} t^{-2} + \beta_{-1}^{(1)} t^{-1} + \cdots, \\
&\quad\ y_2 = -t^{-3} + \gamma_{-2}^{(1)} t^{-2} + \gamma_{-1}^{(1)} t^{-1} + \cdots\}, \\
P_2 &= \{x = -t^{-1} + \alpha_0^{(1)} + \alpha_1^{(1)} t + \cdots, \\
&\quad\ y_1 = t^{-3} + \beta_{-2}^{(1)} t^{-2} + \beta_{-1}^{(1)} t^{-1} + \cdots, \\
&\quad\ y_2 = t^{-3} + \gamma_{-2}^{(2)} t^{-2} + \gamma_{-1}^{(2)} t^{-1} + \cdots\}, \\
P_3 &= \{x = t^{-1} + \alpha_0^{(2)} + \alpha_1^{(2)} t + \cdots, \\
&\quad\ y_1 = t^{-3} + \beta_{-2}^{(2)} t^{-2} + \beta_{-1}^{(2)} t^{-1} + \cdots, \\
&\quad\ y_2 = -t^{-3} + \gamma_{-2}^{(3)} t^{-2} + \gamma_{-1}^{(3)} t^{-1} + \cdots\} \\
P_4 &= \{x = t^{-1} + \alpha_0^{(2)} + \alpha_1^{(2)} t + \cdots, \\
&\quad\ y_1 = t^{-3} + \beta_{-2}^{(2)} t^{-2} + \beta_{-1}^{(2)} t^{-1} + \cdots, \\
&\quad\ y_2 = t^{-3} + \gamma_{-2}^{(4)} t^{-2} + \gamma_{-1}^{(4)} t^{-1} + \cdots\}.
\end{aligned}
$$

The set of points at infinity $\{P_1, P_2, P_3, P_4\}$ is obviously invariant under the automorphism σ. Moreover,

Proposition 10. *P_4 is fixed by σ.*

Proof. Let $v_P(f)$ denote the valuation of a function f at point P.

Let $\sigma(P_4) = P_1$. By the expansions of y_1, y_2 at P_4, we know $v_{P_4}(y_1 - y_2) \geq -2$. On the other hand, we have $v_{P_4}(y_1 - y_2) = v_{P_1{}^\sigma}(y_1 - y_2) = v_{P_1}(y_2 - y_1)$. By the expansions y_1, y_2 at P_1, we see $v_{P_1}(y_2 - y_1) = -3$, so $v_{P_4}(y_1 - y_2) = -3$, which is a contradiction. Similarly, we know $\sigma(P_4) \neq P_3$.

Let $\sigma(P_4) = P_2$. By the expansion of x at P_4, we have $v_{P_4}(x - t^{-1}) \geq 0$. On the other hand, $v_{P_4}(x - t^{-1}) = v_{P_2{}^\sigma}(x - t^{-1}) = v_{P_2}(x - (t^{-1})^\sigma)$. We have $x - (t^{-1})^\sigma = x - y_2/x^2 = -2t^{-1} + \cdots$ at P_2. So, $v_{P_4}(x - t^{-1}) = v_{P_2}(x - (t^{-1})^\sigma) = -1$, which is also a contradiction.

Thus, $\sigma(P_4) = P_4$. ◻

3.2.2 Regular functions outside the base point

We have to determine regular functions outside the base point P_4 on GHS-section D. Those functions are regular in $x - y_1 - y_2$ affine space. So, they are expressed by polynomials on x, y_1 and y_2 since D is nonsingular in the affine space by Assumption 1.

Since GHS-section D is of genus nine by Proposition 9, assuming P_4 is not a Weierstrass point of D, the minimum generators of pole numbers at P_4 is $\{10, 11, \ldots, 19\}$. So, polynomials $f_{10}, f_{11}, \ldots, f_{19}$, which has the unique pole of order $10, 11, \ldots, 19$ at P_4, respectively, generate the algebra of regular functions outside P_4. (Even if P_4 is a Weierstrass point, the situation is similar except for members of the minimum generators of pole numbers at P_4.)

In order to construct such a polynomial f_i regular away P_4, we recursively take a suitable linear sum of polynomials which have the same pole order at P_i, until we get a polynomial regular at P_i for $i = 1, 2, 3$. Notice we can know the 'value' of polynomials at P_i using local parameter expansions of P_i in Section 3.2.1.

Using those polynomials $f_{10}, f_{11}, \ldots, f_{19}$, we can construct an explicit $C_{10,11,\cdots,19}$ model with a base point P_4 of GHS-section D over k_2 [16]. To construct an $C_{10,11,\cdots,19}$ model C over k, instead of k_2, it is sufficient to use $g_i = \mathrm{Tr}_{k_2/k}(f_i)$ ($i = 10, 11, \ldots, 19$) instead of f_i. Here, $\mathrm{Tr}_{k_2/k}$ is defined as

$$\mathrm{Tr}_{k_2/k}(\Sigma a_{l,m,n} x^l y_1^m y_2^n) = \Sigma a_{l,m,n}^q x^l y_2^m y_1^n.$$

We notice that g_i is regular away P_4 and the pole order of g_i at P_4 remains to be i by Proposition 10.

3.3 Reduction

In Section 3.2, we construct $C_{10,11,\ldots,19}$ model C over k_2 and k of GHS-section D:

$$\begin{array}{rcl} k_2(x, y_1, y_2) & \overset{\phi^*}{\simeq} & k_2(f_{10}, f_{11}, \ldots, f_{19}) \\ & = & k_2(g_{10}, g_{11}, \ldots, g_{19}). \end{array}$$

Let the isomorphism from $C_{10,11,\ldots,19}$ model C to GHS-section D, corresponding to ϕ^*, be

$$\begin{array}{rcl} \phi : C & \overset{\sim}{\to} & D \\ (g_{10}, g_{11}, \ldots, g_{19}) & \mapsto & (x, y_1, y_2). \end{array}$$

Let π be a projection from GHS-section D to hyperelliptic curve H:

$$\begin{array}{rcl} \pi : D & \to & H \\ (x, y_1, y_2) & \mapsto & (x, y_1). \end{array}$$

The composition $\Pi_1 := \pi \cdot \phi$ is a map from C to H.

As in Section 2, we suppose hyperelliptic curve H is a double-cover of an elliptic curve E on k_4 with a map Π_2:

$$\Pi_2 : H \to E.$$

Let $\Pi = \Pi_2 \cdot \Pi_1 : C \to E$, which induces a morphism Ψ between Jacobians:

$$\Psi : E(k_4) \overset{\Pi^*}{\to} \mathrm{Jac}_{k_4}(C) \overset{\mathrm{Norm}_{k_4/k}}{\to} \mathrm{Jac}_k(C).$$

Proposition 11. *Let G be an element of $E(k_4)$ of prime order n, which is larger enough than the degree of Π^*. Moreover, suppose n^2 does not divide the order of Jacobian $\mathrm{Jac}_{k_4}(C)$. Then, G does not vanish under Ψ.*

Proof. Since the order n of G is large enough, G does not vanish under Π^*. By the theory of Weil descent, there is a surjection from $\mathrm{Jac}_k(C)$ to $E(k_4)$. So, there is an element of order n in $\mathrm{Jac}_k(C)$. Then, by the assumption that n^2 does not divide the order of Jacobian $\mathrm{Jac}_{k_4}(C)$, $\Pi^*(G)$ must belong to $\mathrm{Jac}_k(C)$, as pointed out by Galbraith, and Smart [11] in a more general situation. So it does not vanish under $\mathrm{Norm}_{k_4/k}$. □

By Proposition 11, we can suppose DLP on an elliptic curve E on k_4 is reduced to DLP on $C_{10,11,\ldots,19}$ curve C on k by homomorphism Ψ. Details of the way to compute homomorphism Ψ are illustrated through examples.

3.4 Examples

We show examples which shows DLP on elliptic curves on a quartic extension field k_4 is reduced to DLP on $C_{10,11,\ldots,19}$ curves on the subfield k. In the computations below, we used Magma V.2.10.

3.4.1 Example 1

Let k be a prime field of characteristic $q = p = 71$, k_2 be its quadratic extension defined by an irreducible polynomial o^2-2o+7, and k_4 be its quadratic extension defined by an irreducible polynomial $r^2 - or + 1$.

We have seen in Section 2.3 that an elliptic curve $E_w : v_1^2 + 70u_1^3 + (o^{2058}r + o^{4231})u_1 + o^{3375}r + o^{2069} = 0$ on k_4, which has a prime order $n = 25404727$, is covered by a genus two hyperelliptic curve $H : y_1^2 = x^6 + o^{2177}x^5 + o^{4311}x^4 + o^{2447}x^3 + o^{566}x^2 + o^{3664}x + o^{3747}$ on k_2 via map $\Pi_2 = \Pi_2^{(1)} \cdot \Pi_2^{(2)} \cdot \Pi_2^{(3)} : H \to E_w$.

As in Section 3.2.1, We take GHS-section D of the scalar restriction $\Pi_{k_2/k}H$ of H. Parameter expansions with respect to $t = x^2/y_1$ of points P_1, P_2, P_3, P_4 at infinity on D are computed as follows:

P_1 :
$$x = 70t^{-1} + o^{4265} + o^{261}t + o^{4535}t^2 + o^{2836}t^3 + \cdots$$
$$y_1 = t^{-3} + o^{2177}t^{-2} + o^{4111}t^{-1} + o^{3867} + o^{3086}t + \cdots$$
$$y_2 = 70t^{-3} + o^{2713}t^{-2} + o^{4163}t^{-1} + o^{3058} + o^{4299}t + \cdots$$

P_2 :
$$x = 70t^{-1} + o^{4265} + o^{261}t + o^{4535}t^2 + o^{2836}t^3 + \cdots$$
$$y_1 = t^{-3} + o^{2177}t^{-2} + o^{4111}t^{-1} + o^{3867} + o^{3086}t + \cdots$$
$$y_2 = t^{-3} + o^{193}t^{-2} + o^{1643}t^{-1} + o^{538} + o^{1779}t + \cdots$$

P_3 :
$$x = t^{-1} + o^{4265} + o^{2781}t + o^{4535}t^2 + o^{316}t^3 + \cdots$$
$$y_1 = t^{-3} + o^{4697}t^{-2} + o^{4111}t^{-1} + o^{1347} + o^{3086}t + \cdots$$
$$y_2 = 70t^{-3} + o^{193}t^{-2} + o^{4163}t^{-1} + o^{538} + o^{4299}t + \cdots$$

P_4 :
$x = t^{-1} + o^{4265} + o^{2781}t + o^{4535}t^2 + o^{316}t^3 + \cdots$
$y_1 = t^{-3} + o^{4697}t^{-2} + o^{4111}t^{-1} + o^{1347} + o^{3086}t + \cdots$
$y_2 = t^{-3} + o^{2713}t^{-2} + o^{1643}t^{-1} + o^{3058} + o^{1779}t + \cdots$.

As in Section 3.2.2, with these parameter expansions, we obtain functions $f_{10}, f_{11}, \ldots, f_{19}$ on D which has the unique pole at P_4 of order $10, 11, \ldots, 19$, respectively. Appling $\mathrm{Tr}_{k_2/k}$ to them, we obtain

$$\begin{aligned} g_{10} &= o^{1264}x^3y_1^2 + 3x^3y_1y_2 + o^{271}x^3y_1 + \cdots + o^{1754}y_2, \\ g_{11} &= o^{1386}x^3y_1^2 + x^3y_1y_2 + o^{2108}x^3y_1 + \cdots + o^{630}y_2, \\ &\vdots \\ g_{19} &= o^{3534}x^3y_1^2 + 41x^3y_1y_2 + o^{3210}x^3y_1 + \cdots + o^{1622}y_2. \end{aligned}$$

Every g_i has the unique pole at P_4 of order i as well as f_i.

Among those $g_{10}, g_{11}, \ldots, g_{19}$, we have following relations $r_{22}, r_{23}, \ldots, r_{31}$ which define $C_{10,11,\ldots,19}$ curve C on k in $g_{10} - g_{11} - \cdots - g_{19}$ affine space:

$$\begin{aligned} r_{22} &= g_{11}^2 - (5g_{10}g_{12} + 42g_{10}g_{11} + 18g_{10}^2 + \cdots + 25), \\ r_{23} &= g_{11}g_{12} - (26g_{10}g_{13} + 38g_{10}g_{12} + \cdots + 58), \\ &\vdots \\ r_{31} &= g_{12}g_{19} - (9g_{10}^2g_{11} + 62g_{10}^3 + 10g_{10}g_{19} + \cdots + 28). \end{aligned}$$

As seen in Section 2.3, a point $G = (o^{387}r + o^{397}, o^{166}r + o^{1205})$ on E_w of order n is mapped via Π_2^* to the element J of Jacobian of H:

$$\begin{aligned} J = \{ &(o^{353}r + o^{4196})x^2 + (o^{1900}r + o^{1805})x + o^{1922}r + o^{2318}, \\ &(o^{3720}r + o^{1533})x^3 + (o^{1693}r + o^{4323})x^2 + (o^{3636}r + o^{1592})y_1 \\ &+(o^{1256}r + o^{3701})x + o^{2686}r + o^{3725}\}. \end{aligned}$$

Now, we compute an image of J via map Π_1^*. Remember $\Pi_1 = \pi \cdot \phi : C \to D \to H$ (see Section 3.3). Let $R = k_4[x, y_1]$ be a coordinate ring of H and $R_1 = k_4[x, y_1, y_2]$ be a coordinate ring of D, and $R_2 = k[\check{g}_{10}, \ldots, \check{g}_{19}]$ be a coordinate ring of C. J is an ideal of R. $J := \pi^*(J)$ is nothing but an ideal generated by J in R_1. J corresponds to a divisor with poles of the first order at P_1, P_2, P_3, and at P_4. We make those poles at P_1, P_2, P_3 vanish by taking the product of J with a polynomial with zeros at P_1, P_2, P_3, e.g. $h_{13} := 40g_{13} + 7g_{12} + 44g_{11} + 12g_{10} + 31$. Then an image of $h_{13}J$ (which is in the same ideal class of J) under ϕ^* can be computed using an elimination ideal as follows:

$$\begin{aligned} J &\leftarrow J \cdot h_{13} \\ J &\leftarrow \mathrm{Eliminate}(J + \{\check{g}_{10} - g_{10}(x, y_1, y_2), \check{g}_{11} - g_{11}(x, y_1, y_2), \cdots, \\ &\quad\ \check{g}_{19} - g_{19}(x, y_1, y_2)\}, \{x, y_1, y_2\}) \\ J &\leftarrow \mathrm{Reduce}(J), \end{aligned}$$

where Eliminate$(\cdot, \{x, y_1, y_2\})$ denotes an ideal in R_2 obtained by eliminating the variables x, y_1, y_2 from the ideal of the first argument, which shows relations among $g_i (i = 10, 11, \ldots, 19)$ over J, that is the image of J by Π_1^*. Reduce(J) reduces an ideal J (for details, see [4]).

Finally, we compute $\mathrm{Norm}_{k_4/k}(J)$:

$$J \leftarrow \mathrm{jSum}(\mathrm{jSum}(J, \tilde{J}), \mathrm{jSum}(\tilde{\tilde{J}}, \tilde{\tilde{\tilde{J}}})),$$

where jSum$(J, \tilde{J})$ denotes a sum of J and its conjugate $\tilde{J}$ over k in Jacobian of C. For details of Reduce and jSum, see [4].

Thus, we have computed $J = \Psi(G) = \mathrm{Norm}_{k_4/k} \cdot \Pi_1^* \cdot \Pi_2^*(G)$:

$$\begin{aligned} J \quad = \quad & \{g_{17}^2 + 37g_{17} + 21g_{16} + 49g_{15} + 33g_{14} + \cdots + 59, \\ & g_{16}g_{17} + 45g_{17} + 15g_{16} + 45g_{15} + 21g_{14} + \cdots + 63, \\ & \ldots \\ & g_{18} + 24g_{17} + 27g_{16} + 31g_{15} + 64g_{14} + \cdots + 64\} \end{aligned}$$

which denotes an element of Jacobian over k of $C_{10,11,\ldots,19}$ curve C (for simplicity, we use the letter g for $\breve{g}$) corresponding to G on E_w.

Similarly, $m = 25415194$-times point $G_m = (o^{637}r + o^{224}, o^{1671}r + o^{3481})$ of G is mapped to an element

$$\begin{aligned} J_m \quad = \quad & \{g_{17}^2 + 6g_{17} + 70g_{16} + 66g_{15} + 15g_{14} + \cdots + 68, \\ & g_{16}g_{17} + 5g_{17} + 20g_{16} + 56g_{15} + 16g_{14} + \cdots + 11, \\ & \ldots \\ & g_{18} + 23g_{17} + 34g_{16} + 65g_{15} + 18g_{14} + \cdots + 4\} \end{aligned}$$

of Jacobian of C. We verified that m-times element of J is actually equal to J_m in Jacobian of C. Thus, we verified that DLP on elliptic curve E_w on k_4 is actually reduced to DLP on $C_{10,11,\ldots,19}$ curve C on k.

3.4.2 Example 2

We show an example of group of 160-bit order.

Let k be the prime field of characteristic $q = p = 2^{40} - 2^{35} - 1$, k_2 be its quadratic extension defined by an irreducible polynomial $o^2 + 352619714346$, and k_4 be its quadratic extension defined by an irreducible polynomial $r^2 + 702753204573o + 465976829831$.

An elliptic curve

$$\begin{aligned} E_w \quad : \quad & v_1^2 = u_1^3 + ((773569929047o + 698785454132)r + 892468792697o \\ & +773390597884)u_1 + (245022657483o + 657619174138)r \\ & +721187940068o + 865450731541 \end{aligned}$$

on k_4 has a 160-bit prime order

$$n = 1287200406650928609777376029597716043015507861907.$$

As in Example 1, we found that DLP on E_w is reduced to DLP on the following $C_{10,11,\ldots,19}$ curve C:

$$g_{11}^2 - (671010913434 g_{10}g_{12} + 306446345201 g_{10}g_{11} + 205461673669 g_{10}^2 + \cdots$$
$$+675147796101) = 0,$$
$$g_{11}g_{12} - (752537421825 g_{10}g_{13} + 1016531429604 g_{10}g_{12} + 897328181722 g_{10}g_{11}$$
$$+ \cdots + 1053682994222) = 0,$$
$$\vdots$$
$$g_{12}g_{19} - (128634052382 g_{10}^2 g_{11} + 950367786029 g_{10}^3 + 457707828730 g_{10}g_{19}$$
$$+ \cdots + 665817232135) = 0.$$

A point

$$G = (1, (4489601964300 + 540742096931)r + 521019129313o + 684726004416)$$

on E_w is mapped to an element

$$\begin{aligned} J \quad = \quad & \{g_{17}^2 + 3720685308 g_{17} + 760318447938 g_{16} + \cdots + 930677256954, \\ & g_{16}g_{17} + 725294630540 g_{17} + 222096222048 g_{16} + \cdots + 752506763900, \\ & \cdots, \\ & g_{18} + 942200891029 g_{17} + 935848743981 g_{16} + \cdots + 234904933666\} \end{aligned}$$

of Jacobian of C. We verified that discrete-log is preserved from G to J.

4 Conclusion

This paper showed that Weil descent attack is effective uniformly in many of elliptic curves on quartic fields of odd characteristic or hyperelliptic curves on quadratic fields of odd characteristic. However, our attack is estimated to be effective with groups of around 210 bits or longer. To attack (hyper-)elliptic curve cryptosystems with 160-bit group in the real world, we need some works to make the method more efficient.

References

[1] S. Arita. Gaudry's variant against C_{ab} curves. *IEICE Trans.*, E83-A(9):1809–1814, 2000.

[2] S. Arita. Weil descent of elliptic curves over finite fields of characteristic three. In T. Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000*, number 1976 in Lecture Notes in Computer Science, pages 248–258. Springer-Verlag, 2000.

[3] S. Arita. A Weil descent attack against genus two hyperellptic curve cryptosystems over quadratic extention fields. Technical Report ISEC2002-62, IEICE, Japan, 2002. in Japanese.

[4] S. Arita. An addition algorithm in Jacobian of C_{ab} curves curves. *Discrete Applied Mathematics*, 130(1):13–31, 2003.

[5] S. Arita. A Weil descent attack against elliptic curve cryptosystems over quartic fields II. In *Proc. of SCIS2004*, pages 903–908, 2004. in Japanese.

[6] C. Diem. The GHS attack in odd characteristic. *J. Ramanujan Math. Soc.*, 18(1):1–32, 2003.

[7] G. Frey and H. Gangl. How to disguise an elliptic curve (Weil descent). Talk at ECC '98, The 2nd Workshop on Elliptic Curve Cryptography, U. Waterloo, `http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/frey.ps`, 1998.

[8] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[9] S. D. Galbraith. Weil descent of Jacobians. *Discrete Applied Mathematics*, 128(1):165–180, 2003.

[10] S. D. Galbraith, F. Hess, and N. P. Smart. Extending the GHS Weil descent attack. In L. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, number 2332 in Lecture Notes in Computer Science, pages 29–44. Springer-Verlag, 2002.

[11] S. D. Galbraith and N. P. Smart. A cryptographic application of weil descent. In M. Walker, editor, *Cryptography and Coding: 7th IMA International Conference, Cirencester, UK, December 1999*, number 1746 in Lecture Notes in Computer Science, pages 191–200. Springer-Verlag, 1999.

[12] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 19–34. Springer-Verlag, 2000.

[13] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15(1):19–46, 2002.

[14] P. Gaudry and E. Thomé. A double large prime variation for small genus hyperelliptic index calculus. Cryptology ePrint Archive, Report 2004/153, 2004. `http://eprint.iacr.org/`.

[15] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite fields. In *Proc. of STOC*, pages 80–89, 1991.

[16] S. Miura. Linear codes on affine algebraic curves. *IEICE Trans. A*, J81-A(10):1398–1421, 1998. in Japanese.

[17] K. Nagao. Improvement of Thériault algorithm of index calculus for Jacobian of hyperelliptic curves of small genus. Cryptology ePrint Archive, Report 2004/161, 2004. `http://eprint.iacr.org/`.

[18] K. Nagao, S. Arita, K. Matsuo, and M. Shimura. A Weil descent attack against elliptic curve cryptosystems over quartic fields I. In *Proc. of SCIS2004*, pages 897–902, 2004. in Japanese.

[19] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Commentarii Mathematici Universitatis Sancti Pauli*, 47(1), 1998.

[20] J. Scholten. Weil restriction of an elliptic curve over a quadratic extension. preprint, `http://www.esat.kuleuven.ac.be/~jscholte/weilres.ps`, 2003.

[21] I. A. Semaev. Evaluation of discrete logarithms in a group of p–torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67:353–356, 1998.

[22] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.

[23] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In C. S. Laih, editor, *Advances in Cryptology - ASIACRYPT 2003*, number 2894 in Lecture Notes in Computer Science, pages 75–92. Springer-Verlag, 2003.