PAPER *Special Section on Discrete Mathematics and Its Applications*

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

Seigo ARITA[†a)], **Kazuto MATSUO**[†,††], **Koh-ichi NAGAO**[†††], ***Members***, ***and*** **Mahoro SHIMURA**[††††], ***Nonmember***

SUMMARY This paper proposes a Weil descent attack against elliptic curve cryptosystems over quartic extension fields. The scenario of the attack is as follows: First, one reduces a DLP on a Weierstrass form over the quartic extention of a finite field k to a DLP on a special form, called Scholten form, over the same field. Second, one reduces the DLP on the Scholten form to a DLP on a genus two hyperelliptic curve over the quadratic extension of k. Then, one reduces the DLP on the hyperelliptic curve to one on a C_{ab} model over k. Finally, one obtains the discrete-log of original DLP by applying the Gaudry method to the DLP on the C_{ab} model. In order to carry out the scenario, this paper shows that many of elliptic curve discrete-log problems over quartic extension fields of odd characteristics are reduced to genus two hyperelliptic curve discrete-log problems over quadratic extension fields, and that almost all of the genus two hyperelliptic curve discrete-log problems 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 uniformly.

key words: *elliptic curve cryptosystems, hyperelliptic curve cryptosystems, Weil descent attack, Scholten form, C_{ab} curves*

1. Introduction

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 [17], Frey-Rück attack [11], SSSA attack [21], [23], [24] 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 [9], aims to break DLP on algebraic curve over composite fields. For a given algebraic curve A over a composite field K, by using the technique of scalar restriction, we construct an algebraic curve C over a smaller field k to cover the curve A. 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 [14] could be more effective against DLP on C than against A, provided that genus of C is small enough.

In the first place, Gaudry, Hess and Smart [15] showed that some of (DLP on) elliptic curve of characteristic two are really attacked by Weil descent. Later, it was shown, by Galbraith [13] and [2], that some of hyperelliptic curve of characteristic two and some of elliptic curve of characteristic three are also attacked, respectively. Moreover Diem [7] showed the existence of (hyper-)elliptic curves of general odd characteristics which can be attacked by Weil descent. However, (hyper-)elliptic curves attacked by those are very exceptional ones.

Besides Thériault [26] proposed Weil descent attack for some special hyperelliptic curves defined over $\mathbb{F}_{q^2}$ or $\mathbb{F}_{q^3}$. On the other hand, Scholten [22] showed that an elliptic curve of a special form over the quadratic extension of a finite field k is covered by a hyperelliptic curve over k and also elliptic curves with full rational two-torsions can be represented by that form.

This paper deals with an attack against elliptic curve cryptosystems over quartic extension fields. The scenario of the attack proposed in this paper is as follows: First, one reduces a DLP on a Weierstrass form over the quartic extention of a finite field k to a DLP on a Scholten form over the same field. Second, one reduces the DLP on the Scholten form to a DLP on a genus two hyperelliptic curve over the quadratic extension of k. Then, one reduces the DLP on the hyperelliptic curve to one on a C_{ab} model over k. Finally, one obtains the discrete-log of the original DLP by applying the Gaudry method to the DLP on the C_{ab} model.

In order to carry out the scenario, first this paper shows that many of DLP on elliptic curves over quartic extension fields are reduced to those on genus two hyperelliptic curves over quadratic extension fields. Corresponding result of this part is obtained for elliptic curves with full two-torsions by Scholten [22]. However, we concern ourselves mainly about elliptic curves with no rational two-torsions due to cryptographically requirement and we need more explicit formula for reductions in order to deal with DLPs on them. So, this paper prepares two independent sections to describe explicit reduction, which is not stated in [22], from elliptic curve cryptosystems with no two-torsions over quartic extension fields to hyperelliptic curve ones over quadratic extension fields. Second, this paper shows in the explicit constructive way 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

Manuscript received August 18, 2005.
Manuscript revised November 9, 2005.
Final manuscript received December 26, 2005.

[†]The authors are with Institute of Information Security, Yokohama-shi, 221-0835 Japan.
[††]The author is with the RDI of Chuo Univ., Tokyo, 112-8551 Japan.
[†††]The author is with the Dept. of Engineering, Kanto-Gakuin Univ., Yokohama-shi, 236-8501 Japan.
[††††]The author is with Chuo Univ. 21st Century Center of Excellence Program, Tokyo, 112-8551 Japan.
a) E-mail: arita@iisec.ac.jp

DOI: 10.1093/ietfec/e89–a.5.1246

many of elliptic curve cryptosystems over quartic extension fields of odd characteristics can be attacked by Weil descent uniformly.

The organization of this paper is as follows: Sect. 2 introduces Scholten form of an elliptic curve over a quartic extension field, and shows the explicit reduction formula from the Scholten form to the Jacobian of a genus two hyperelliptic curve over a quadratic extension field. Section 3 shows the conditions for an elliptic curve in Weierstrass form to be transformed into Scholten form and the explicit reduction formula from Weierstrass form to Scholten form. Then Sect. 4 explicitly reduces DLP on a genus two hyperelliptic curve over a quadratic extension to DLP on a C_{ab} model in order to apply Gaudry method. Finally, Sect. 5 shows examples of the proposed attack which include one for a 160-bit DLP.

2. A Weil Descent of DLP on Scholten Form

Let $k = \mathbb{F}_q$ be a finite field of characteristic different from two. 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 $a, b \in k_4$. Scholten [22] 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

$$\begin{aligned} H : Y^2 \;=\; & a(X-c)^6 + b(X-c)^4(X-c^{q^2}) \\ & + b^{q^2}(X-c)^2(X-c^{q^2})^4 + a^{q^2}(X-c^{q^2})^6 \end{aligned}$$

over k_2, where c denotes an element of $k_4 \setminus k_2$, and gave a way to construct secure genus two hyperelliptic curve.

Our Weil descent attack needs a efficiently computable map from $E_n(k_2)$ to the Jacobian of H over k_4, so that this section presents one.

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 $c \in k_4 \setminus k_2$. 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 Ψ induces a homomorphism Ψ^* from $E_n(k_4)$ to the Jacobian $\mathrm{Jac}_H(k_4)$ of H over k_4: $\Psi^* : P \in E_n(k_4) \mapsto Q_1 + Q_2 - \infty_1 - \infty_2 \in \mathrm{Jac}_H(k_4)$. Here, ∞_1, ∞_2 denote two points of H at infinity. By (1), we see that X-coordinates of Q_1, 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 $T : \sum_i Q_i \in \mathrm{Jac}_H(k_4) \mapsto \sum_i Q_i + Q_i^{q^2} \in \mathrm{Jac}_H(k_2)$ to get a homomorphism $T \cdot \Psi^*$ from $E_n(k_4)$ to Jacobian $\mathrm{Jac}_H(k_2)$ 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 $2q^2 + 1$. 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 (2), $\frac{1}{2}(A(X) - \frac{b+1}{b}B(X)) = 0$ with $b = (-1 + x(P))/2$. Now we assume 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. Since $A(X), B(X)$ is transferred to $A(X), -B(X)$ respectively by q^2-th Frobenius automorphism, we see $\left(\frac{b+1}{b}\right)^{q^2} = -\frac{b+1}{b}$. Since the number of such $b\,(\neq 0)$ is at most $q^2 - 1$, the number of P satisfying $T \cdot \Psi^*(P) = 0$ is at most $2q^2 - 2$. □

Lemma 1 shows that the homomorphism $T \cdot \Psi^*$ from $E_n(k_4)$ to $\mathrm{Jac}_H(k_2)$ is not trivial. So, the homomorphism reduces DLP on $E_n(k_4)$ to DLP on $\mathrm{Jac}_H(k_2)$.

3. Transformation of Weierstrass Form

This section considers necessary and sufficient conditions for an elliptic curve over k_4 in Weierstrass form to be transformed into Scholten form over k_4. In general, an isomorphism between elliptic curves is given by a linear transformation $x \to Ax + B, y \to Cy + Dx + E$ with constants A, B, C, D. If Weierstrass form $E_w : y^2 = f(x)$ over k_4 is transformed into Scholten form $E_n : y^2 = F(x)$ over k_4 by transformation $x \to Ax + B, y \to Cy + Dx + E$ over k_4, it is obvious that $D = E = 0$ and $F(x) = C^{-2}f(Ax + B)$. Scholten [22] has already shown that an elliptic curve with full two-torsions can be transformed into Scholten form, and observed that an elliptic curve with no two-torsions can be also transformed experimentally. So, this section only considers 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, which is a cryptographically common setting. Moreover, this section shows a map from E_w to E_n which is needed for our attack.

Suppose that 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 $F(x) = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$, then δ^{-q^2} is also a root of $F(x)$. This means that δ^{-q^2} equals δ or δ^{q^4} or δ^{q^8}. However, if $\delta^{-q^2} = \delta$, then $\delta^{q^4-1} = (\delta^{q^2+1})^{q^2-1} = 1$, 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 $\delta^{-q^2} = \delta^{q^8}$, i.e. $\delta^{1+q^6} = 1$. Summarizing, we have the following proposition.

Proposition 1. *Suppose that a monic cubic polynomial $f(x)$ is irreducible over k_4, and that Weierstrass form $E_w : y^2 = f(x)$ over 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 $a = -A^{2-q^2}\delta^{1+q^4-q^2}$, $b = -A(\delta+\delta^{q^4}+\delta^{-q^2})$. Then, Weierstrass form $E_w : y^2 = f(x)$ over k_4 is transformed into Scholten form $E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ over 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 $B = 0$. We have $y^2 = x^3 + bx^2 + ab^{q^2}x + a^{q^2}a^2$. This is transformed into E_n 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: $^\exists A \in k_4^\times, B \in k_4$, satisfying $\gamma = A\delta + B, \delta^{1+q^6} = 1$. For $\gamma \in k_{12}$, let $\mathrm{d}(\gamma) = (\gamma^{q^2+q^4} - \gamma^{q^2+1}) + (\gamma^{q^6+q^8} - \gamma^{q^6+q^4}) + (\gamma^{q^{10}+1} - \gamma^{q^{10}+q^8})$.

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

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

Proof. (⇒) 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 $A^{1+q^2} = A^{1+q^6} = (\gamma - B)^{1+q^6}$, $\delta = (\gamma - B)/A$). For the sake, we see an equation for B:

$$(\gamma - B)^{q^2}(\gamma^{q^6} - B^{q^6})^{q^2} - (\gamma - B)(\gamma^{q^6} - B^{q^6}) = 0 \tag{3}$$

has a solution in k_4. By letting $B^{q^4} = B$ and collecting terms of B, (3) is transformed into

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

By applying q^2-th Frobenius automorphism,

$$(\gamma^{q^4} - \gamma^{q^8})B^{q^2} + (\gamma^{q^{10}} - \gamma^{q^2})B - \gamma^{q^4+q^{10}} + \gamma^{q^2+q^8} = 0. \tag{5}$$

Equations (4) and (5) are written with matrices as

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

The determinant of the coefficient matrix is computed to be $(\gamma^{q^2+q^4} - \gamma^{1+q^2}) + (\gamma^{q^6+q^8} - \gamma^{q^6+q^4}) + (\gamma^{1+q^{10}} - \gamma^{q^8+q^{10}}) = \mathrm{d}(\gamma)$. Therefore, $B = \mathrm{d}(\gamma)^{-1}(\gamma(\gamma^{q^6+q^8} - \gamma^{q^4+q^6}) + \gamma^{q^4}(\gamma^{q^{10}+1} - \gamma^{q^8+q^{10}}) + \gamma^{q^8}(\gamma^{q^2+q^4} - \gamma^{1+q^2}))$. For this B we have $B = B^{q^4}$, i.e., $B \in k_4$.
(⇐) Suppose $\mathrm{d}(\gamma) = 0$, i.e.

$$
\begin{aligned}
&(\gamma^{q^2+q^4} - \gamma^{q^2+1}) + (\gamma^{q^6+q^8} - \gamma^{q^6+q^4}) + \\
&\qquad (\gamma^{q^{10}+1} - \gamma^{q^{10}+q^8}) = 0.
\end{aligned} \tag{7}
$$

If $(\gamma - B)^{1+q^6} \in k_2$ for some $B \in k_4$, then (6) has a solution B. Then, since the determinant of the coefficient matrix of (6) 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, $\gamma^{1+q^4+q^6} + \gamma^{q^4+q^8+q^{10}} + \gamma^{1+q^2+q^8} - \gamma^{1+q^4+q^{10}} - \gamma^{q^2+q^4+q^8} - \gamma^{1+q^6+q^8} = 0$. By adding γ^{q^4}-times (7) to this equation, $(\gamma^{q^6} - \gamma^{q^2})(\gamma - \gamma^{q^4})(\gamma^{q^4} - \gamma^{q^8}) = 0$. This implies $\gamma \in k_4$, which contradicts the assumption. □

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, Weierstrass form $E_w : y^2 = f(x)$ over k_4 is transformed into Scholten form $E_n : y^2 = ax^3 + bx^2 + b^{q^2}x + a^{q^2}$ over k_4 by translation $y \to ay, x \to ax + B$ over k_4 for $a = -A^{2-q^2}\delta^{1+q^4-q^2}$, $b = -A(\delta + \delta^{q^4} + \delta^{-q^2})$ with A, B given in Lemma 2.*

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 $E_w : y^2 = f(x)$ over k_4, the condition $j(E_w) \in k_2$ 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. (⇒) By the condition $j(E_w) \in k_2$, 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 $\gamma = AD\alpha + B$.
(⇐) Applying transformation $x \to Ax + B, y \to A^{\frac{3}{2}}y$ over k_8 for $E_w : y^2 = f(x) = (x - \gamma)(x - \gamma^{q^4})(x - \gamma^{q^8})$,

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

So, $j(E_w) \in k_2$. □

Proposition 3. *Let $f(x)$ be an irreducible monic cubic polynomial over k_4. Let γ be a root of $f(x)$. If $j(E_w) \in k_2$ 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 that $\mathrm{d}(\gamma) = 0 \Leftrightarrow \mathrm{d}(\gamma - B) = 0$. 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 $\mathrm{d}(\gamma) = d_0(\gamma) - d_0(\gamma)^{q^2}$. So, we only have to show $d_0(\gamma) \in k_2$. By $\gamma = A\alpha$, $d_0(\gamma) = A^{1+q^2}(\alpha^{q^2+q^4} + \alpha^{1+q^2} + \alpha^{q^4+1}) = \mathrm{N}_{k_4|k_2}(A)\mathrm{T}_{k_6|k_2}(\alpha^{1+q^2})$. □

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

Proposition 4. *Suppose that the characteristic of k is different from three (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 $j(E_w) \in k_2$ for Weierstrass form $E_w : y^2 = f(x)$.*

Proof. We can suppose

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

by letting $\gamma = \gamma - \frac{1}{3}\mathrm{T}_{k_{12}|k_4}(\gamma)$ if necessary. Note that $\mathrm{d}(\gamma)$ remains to be zero by Lemma 2. 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 $\mathrm{d}(\gamma) = 0$,

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

By using (8), $\gamma^{q^2+q^4} - \gamma^{q^{10}+q^8} = \gamma^{1+q^{10}} - \gamma^{q^4+q^6}$, and $\gamma^{q^6+q^8} - \gamma^{q^2+1} = -\gamma^{q^4+q^6} + \gamma^{1+q^{10}}$. So, by (9), we see $\gamma^{1+q^{10}} - \gamma^{q^4+q^6} = 0$. □

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

$E_w : y^2 = f(x)$ can be Scholten form

$\overset{\text{Prop. 1, 2}}{\Longleftrightarrow}$ $\delta = A\gamma + B, \delta^{1+q^6} = 1$ ($\exists A \in k_4^\times, B \in k_4$)

$\overset{\text{Lemma 2}}{\Longleftrightarrow}$ $\mathrm{d}(\gamma) \neq 0$

$\overset{\text{Prop. 3, 4}}{\Longleftrightarrow}$ $j(E_w) \notin k_2$

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

4. A Weil Descent of DLP on Genus Two Hyperelliptic Curves

This section shows that Weil descent attack is effective in almost all of the genus two hyperelliptic curve cryptosystems (that is, those satisfying Assumption 1 shown later) 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 by 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 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 [25], or $O(q^{\frac{17}{9}})$ by [16], [19]. 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 results of previous sections, that Weil descent attack is effective in many of the elliptic curve cryptosystems over quartic extension fields of odd characteristics.

Note that our method is expected to be more efficient, if Diem's index calculus method [8] for non-singular plane curves is applicable instead of Gaudry method. However, that scenario seems to be infeasible, because a projection of our C_{ab} model onto a plane has many singularities in general.

Note also that Thériault [26] shows Weil descent attack for some special hyperelliptic curves defined over k_2, which are defined by $y^2 = (x - a)h(x)$ with $a \in k_2 \setminus k$ and $h(x) \in k[x]$ (not in $k_2[x]$). For those special hyperelliptic curves, Thériault's attack is more efficient than the attack proposed in this section, even though the latter is applicable to almost all hyperelliptic curves over k_2. By incorporating Thériault's attack, it is possible to improve our method in some special cases. However, taking into consideration the aim of this paper that is to attack elliptic curves over quartic extension fields k_4 through hyperelliptic curves over k_2, it seems difficult to find and characterize the family of elliptic curves over k_4 corresponding to such special hyperelliptic curves over k_2 attacked by the method of [26]. Besides, an elliptic curve of no two-torsions which is our main interesting is not covered by Thériault's curve, because Thériault's one is with at least one two-torsion.

4.1 Weil Descent of Hyperelliptic Curves and Their GHS-Sections

Let H be a genus two hyperelliptic curve defined over $k_2 = \mathbb{F}_{q^2}$ which is the quadratic extension of $k = \mathbb{F}_q$ 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

$$y_1^2 = x_1^6 + ax_1^5 + bx_1^4 + cx_1^3 + dx_1^2 + ex_1 + f,$$
$$y_2^2 = x_2^6 + a^q x_1^5 + b^q x_2^4 + c^q x_2^3 + d^q x_2^2 + e^q x_2 + f^q.$$

Note that $\Pi_{k_2/k}H$ is geometrically defined over 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 $\sigma(x_1) = x_2$ and $\sigma(y_1) = y_2$.

For Weil descent attack, we should find an algebraic curve D on $\Pi_{k_2/k}H$, which is defined over 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 [14]. 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 over $\Pi_{K/k}H$ is critical. In this paper, just as in [13], [15], 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 over k by equations

$$y_1^2 = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f, \quad (10)$$
$$y_2^2 = x^6 + a^q x^5 + b^q x^4 + c^q x^3 + d^q x^2 + e^q x + f^q. \quad (11)$$

Proposition 5. *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 the 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], [15], GHS-sections D have huge genera. Remember that the complexity of Gaudry method with respect to genus g is $O(g!)$. So, in [13], [15], 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 6. *The genus of GHS-section D is nine.*

Proof. Under Assumption 1, as seen in the proof of Proposition 5, $F(x)$ 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 do not 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 method. If we can construct such a model, DLP on H can be solved by Gaudry method in the amount of computations $O(q^{\frac{17}{9}})$ [1], [15], [16], [19], which is less than $O(q^2)$ for Pollard's ρ-method. So, hereafter, we construct a C_{ab} model over k of GHS-section D.

4.2 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 (10), (11). 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, 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.

4.2.1 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, 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 $y_2^2 = x^6 + a^q x^5 + b^q x^4 + c^q x^3 + d^q x^2 + e^q x + f^q$ 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:

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

$$
\begin{aligned}
& y_1 = t^{-3} + \beta^{(2)}_{-2}t^{-2} + \beta^{(2)}_{-1}t^{-1} + \cdots, \\
& y_2 = -t^{-3} + \gamma^{(3)}_{-2}t^{-2} + \gamma^{(3)}_{-1}t^{-1} + \cdots\}, \\
P_4 = \{ & x = t^{-1} + \alpha^{(2)}_0 + \alpha^{(2)}_1 t + \cdots, \\
& y_1 = t^{-3} + \beta^{(2)}_{-2}t^{-2} + \beta^{(2)}_{-1}t^{-1} + \cdots, \\
& y_2 = t^{-3} + \gamma^{(4)}_{-2}t^{-2} + \gamma^{(4)}_{-1}t^{-1} + \cdots\}.
\end{aligned}
$$

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

Proposition 7. *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, $\sigma(P_4) = P_4$. □

4.2.2 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 of x, y_1, y_2 since D is nonsingular in the affine space by Assumption 1.

Since GHS-section D is of genus nine by Proposition 6, by 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 $i = 1, 2, 3$. Note that we can know the "value" of polynomials at P_i using local parameter expansions of P_i in Sect. 4.2.1.

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 [18]. 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 $\mathrm{Tr}_{k_2/k}(\Sigma a_{l,m,n} x^l y_1^m y_2^n) = \Sigma a_{l,m,n} x^l y_1^m y_2^n + \Sigma a^q_{l,m,n} x^l y_2^m y_1^n$. Note that g_i is regular away P_4 and the pole order of g_i at P_4 remains to be i by Proposition 7.

4.3 Reduction

In Sect. 4.2, we construct $C_{10,11,\ldots,19}$ model C over k_2 and k of GHS-section D: $k_2(x, y_1, y_2) \overset{\phi^*}{\simeq} k_2(f_{10}, f_{11}, \ldots, f_{19}) = k_2(g_{10}, g_{11}, \ldots, g_{19})$.

Let the isomorphism from $C_{10,11,\ldots,19}$ model C to GHS-section D, corresponding to ϕ^*, be $\phi : (g_{10}, g_{11}, \ldots, g_{19}) \in C \overset{\sim}{\mapsto} (x, y_1, y_2) \in D$. Let π be a projection from GHS-section D to hyperelliptic curve H: $\pi : (x, y_1, y_2) \in D \mapsto (x, y_1) \in H$. The composition $\Pi_1 := \pi \cdot \phi$ is a map from C to H.

As seen in Sect. 2, we suppose hyperelliptic curve H is a double-cover of an elliptic curve E over k_4 with a map Π_2: $H \to E$. Let $\Pi = \Pi_2 \cdot \Pi_1 : C \to E$, which induces a morphism Ψ between Jacobians:

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

Proposition 8. *Let G be an element of $E(k_4)$ of prime order n, which is extremely larger than the degree of Π^*. Moreover, suppose n^2 does not divide the order of Jacobian $\mathrm{Jac}_C(k_4)$. 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 [9], there is a surjection from $\mathrm{Jac}_C(k)$ to $E(k_4)$. So, there is an element of order n in $\mathrm{Jac}_C(k)$. Then, by the assumption that n^2 does not divide the order of Jacobian $\mathrm{Jac}_C(k_4)$, $\Pi^*(G)$ must belong to $\mathrm{Jac}_k(C)$, as pointed out by Galbraith, and Smart [12] in a more general situation. So it does not vanish under $\mathrm{Norm}_{k_4/k}$. □

By Proposition 8, we can suppose DLP on an elliptic curve E over k_4 is reduced to DLP on $C_{10,11,\ldots,19}$ curve C over k by homomorphism Ψ. Details of the way to compute homomorphism Ψ are illustrated through examples.

5. Examples

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

5.1 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 randomly generate an elliptic curve of Weierstrass form $E_w : v_1^2 + 70u_1^3 + (o^{2058}r + o^{4231})u_1 + o^{3375}r + o^{2069} = 0$ over k_4 with a prime order $n = 25404727$. Since $j(E_w) = o^{1854}r + o^{2692} \notin k_2$, 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 Sect. 2, 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

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

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.

As seen in Sect. 4.2.1, 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:

$$\begin{aligned} P_1 &: x = 70t^{-1} + o^{4265} + o^{261}t + o^{4535}t^2 + o^{2836}t^3 + \cdots, \\ &\quad y_1 = t^{-3} + o^{2177}t^{-2} + o^{4111}t^{-1} + o^{3867} + o^{3086}t + \cdots, \\ &\quad y_2 = 70t^{-3} + o^{2713}t^{-2} + o^{4163}t^{-1} + o^{3058} + o^{4299}t + \cdots, \\ P_2 &: x = 70t^{-1} + o^{4265} + o^{261}t + o^{4535}t^2 + o^{2836}t^3 + \cdots, \\ &\quad y_1 = t^{-3} + o^{2177}t^{-2} + o^{4111}t^{-1} + o^{3867} + o^{3086}t + \cdots, \\ &\quad y_2 = t^{-3} + o^{193}t^{-2} + o^{1643}t^{-1} + o^{538} + o^{1779}t + \cdots, \\ P_3 &: x = t^{-1} + o^{4265} + o^{2781}t + o^{4535}t^2 + o^{316}t^3 + \cdots, \\ &\quad y_1 = t^{-3} + o^{4697}t^{-2} + o^{4111}t^{-1} + o^{1347} + o^{3086}t + \cdots, \\ &\quad y_2 = 70t^{-3} + o^{193}t^{-2} + o^{4163}t^{-1} + o^{538} + o^{4299}t + \cdots, \\ P_4 &: x = t^{-1} + o^{4265} + o^{2781}t + o^{4535}t^2 + o^{316}t^3 + \cdots, \\ &\quad y_1 = t^{-3} + o^{4697}t^{-2} + o^{4111}t^{-1} + o^{1347} + o^{3086}t + \cdots, \\ &\quad y_2 = t^{-3} + o^{2713}t^{-2} + o^{1643}t^{-1} + o^{3058} + o^{1779}t + \cdots. \end{aligned}$$

As seen in Sect. 4.2.2, 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. Applying $\mathrm{Tr}_{k_2/k}$ 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 over k in $g_{10} - g_{11} - \cdots - g_{19}$ affine space:

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

Now, we compute an image of J via map Π_1^*. Remember $\Pi_1 = \pi \cdot \phi : C \to D \to H$ (See Sect. 4.3). 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 $R_2 = k[\breve{g}_{10}, \ldots, \breve{g}_{19}]$ 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, 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 by using an elimination ideal as follows:

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

where $\mathrm{Eliminate}(\cdot, \{x, y_1, y_2\})$ 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^*. $\mathrm{Reduce}(J)$ 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 $\mathrm{jSum}(J, \tilde{J})$ 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 $J = \Psi(G) = \mathrm{Norm}_{k_4/k} \cdot \Pi_1^* \cdot \Pi_2^*(G)$:

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

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

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

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 over k_4 is actually reduced to DLP on $C_{10,11,\ldots,19}$ curve C over k.

5.2 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

$$E_w : v_1^2 = u_1^3 + ((773569929047o + 698785454132)r$$
$$+892468792697o + 773390597884)u_1$$
$$+ (245022657483o + 657619174138)r$$
$$+ 721187940068o + 865450731541$$

over k_4 has a 160-bit prime order n:

1287200406650928609777376029597716043015507861907.

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

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

A point $G = (1, (448960196430o + 540742096931)r + 521019129313o + 684726004416)$ on E_w is mapped to an element

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

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

Acknowledgments

The authors would like to thank the editor and the reviewers for their comments, which improved the manuscript. A part of this work was supported by "The Research on Security and Reliability in Electronic Society," Chuo University 21st Century COE Program.

References

[1] S. Arita, "Gaudry's variant against C_{ab} curves," IEICE Trans. Fundamentals, vol.E83-A, no.9, pp.1809–1814, Sept. 2000.
[2] S. Arita, "Weil descent of elliptic curves over finite fields of characteristic three," ASIACRYPT 2000, LNCS 1976, pp.248–258, Springer-Verlag, 2000.
[3] S. Arita, "A Weil descent attack against genus two hyperelliptic curve cryptosystems over quadratic extention fields," IEICE Technical Report, ISEC2002-62, 2002.
[4] S. Arita, "An addition algorithm in Jacobian of C_{ab} curves," Discrete Appl. Math., vol.130, no.1, pp.13–31, 2003.
[5] S. Arita, "A Weil descent attack against elliptic curve cryptosystems over quartic fields II," Proc. SCIS2004, pp.903–908, 2004.
[6] S. Arita, K. Matsuo, K. Nagao, and M. Shimura, "A weil descent attack against elliptic curve cryptosystems over quartic extension fields," Cryptology ePrint Archive, Report 2004/240, 2004.
[7] C. Diem, "The GHS attack in odd characteristic," J. Ramanujan Math. Soc., vol.18, no.1, pp.1–32, 2003.
[8] C. Diem, "Index calculus in class groups of plane curves of small degree," Cryptology ePrint Archive, Report 2005/119, 2005.
[9] G. Frey and H. Gangl, "How to disguise an elliptic curve (Weil descent)," Talk at ECC'98, 1998.
[10] G. Frey and E. Kani, "Curves of genus 2 covering elliptic curves and an arithmetical application," Arithmetic Algebraic Geometry, PM 89, pp.153–176, Birkhäuser, 1991.
[11] G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," Math. Comp., vol.62, pp.865–874, 1994.
[12] S. Galbraith and N. Smart, "A cryptographic application of Weil descent," Cryptography and Coding, LNCS 1746, pp.191–200, Springer-Verlag, 1999.
[13] S. Galbraith, "Weil descent of Jacobians," Discrete Appl. Math., vol.128, no.1, pp.165–180, 2003.
[14] P. Gaudry, "An algorithm for solving the discrete log problem on hyperelliptic curves," EUROCRYPT 2000, LNCS 1807, pp.19–34, Springer-Verlag, 2000.
[15] P. Gaudry, F. Hess, and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves," J. Cryptol., vol.15, no.1, pp.19–46, 2002.
[16] P. Gaudry, N. Thériault, and E. Thomé, "A double large prime variation for small genus hyperelliptic index calculus," Cryptology ePrint Archive, Report 2004/153, 2004.
[17] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite fields," Proc. STOC, pp.80–89, 1991.
[18] S. Miura, "Linear codes on affine algebraic curves," IEICE Trans. Fundamentals (Japanese Edition), vol.J81-A, no.10, pp.1398–1421, Oct. 1998.
[19] K. Nagao, "Improvement of Thériault algorithm of index calculus for Jacobian of hyperelliptic curves of small genus," Cryptology ePrint Archive, Report 2004/161, 2004.
[20] K. Nagao, S. Arita, K. Matsuo, and M. Shimura, "A Weil descent attack against elliptic curve cryptosystems over quartic fields I," Proc. SCIS2004, pp.897–902, 2004.
[21] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves," Commentarii Mathematici Universitatis Sancti Pauli, vol.47, no.1, 1998.
[22] J. Scholten, "Weil restriction of an elliptic curve over a quadratic extension," preprint, http://www.esat.kuleuven.ac.be/˜jscholte/weilres.ps, 2003.
[23] I. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p," Math. Comp., vol.67, pp.353–356, 1998.
[24] N. Smart, "The discrete logarithm problem on elliptic curves of trace one," J. Cryptology, vol.12, no.3, pp.193–196, 1999.

[25] N. Thériault, "Index calculus attack for hyperelliptic curves of small genus," ASIACRYPT 2003, LNCS 2894, pp.75–92, Springer-Verlag, 2003.
[26] N. Thériault, "Weil descent attack for Kummer extensions," J. Ramanujan Math. Soc., vol.18, no.3, pp.281–312, 2003.

Seigo Arita was born in 1963. He has been interested in prime numbers, algebraic curves and now cryptographic protocols. He is with Institute of Information Security, Kanagawa, Japan. He is a member of JMS.

Kazuto Matsuo received the B.E., M.E., and D.E. degrees from Chuo University, Tokyo, Japan in 1986, 1988, and 2001, respectively. He joined Toyo Communication Equipment Co., LTD from 1988 to 2001. He is currently a professor in the graduate school of information security at the Institute of Information Security, Yokohama, Japan, and also a professor of the Research and Development Initiative of Chuo University.

Koh-ichi Nagao received the B.S., M.S., and Ph.D. degrees in mathematical science from Kobe University, Osaka University, and Kyushu University, in 1987, 1989, and 1996 respectively. In 1998, he joined the Department of Engineering at Kanto Gakuin University. Since April 2001, he is an assistant professor at the same university.

Mahoro Shimura received the B.S. from the Department of Mathematics, Waseda University in 1991 in mathematics, and the M.S. and the D.S. from the Department of Mathematical Science, Waseda University in 1993 and 2001, respectively both in mathematics. He was a research associate at Science and Engineering, Waseda University from 1999 to 2001. He is a research fellow of Chuo University 21st Century Center of Excellence Program from 2003.