Scholten forms and curves with weak Weil restrictions

Fumiyuki Momose, Jinhui Chao

Dept. of Mathematics, and Dept. of Information and Sysytem Engineering
Chuo University, Tokyo, Japan

August 10, 2005

1 Introduction

It is known that besides the square-root algorithms such as Pollard's rho or lambda method, there are two generic attacks to algebraic curve based cryptosystems. i.e. the Gaudry and other's variations of the index calculus attack [9][6][10][13] and the Weil descent attack or covering attack[7][5].

Among the index calculus attacks, the double-large-prime variation[10][13] is the most powerful one to hyperelliptic curves. Recently, Diem showed an attack under which non-hyperelliptic curves with low degrees are weaker than hyperelliptic curves.[4].

In this paper, we show explicitly the classes of elliptic and hyperelliptic curves of low genera defined over extension fields, which have weak coverings, i.e. their Weil restrictions can be attacked by one of the above two index calculus attacks.

We will present results on odd characteristic cases. The even characteristic case will be reported in the near future.

1.1 Weil descent or Covering attack

Let q be a power of a odd prime. $k := \mathbb{F}_q, k_n := \mathbb{F}_{q^n}$.
Let C_0/k_n to be an algebraic curve over k_n with genus $g(C_0) \geq 1$.
If $\exists C/k$: an algebraic curve and

$$\pi : C \twoheadrightarrow C_0/k_n$$

is a covering defined over k_n such that

$$\pi_* : J(C) \longrightarrow \mathrm{Res}_{k_n/k}((J(C_0)))$$

defines an isogeny over k.

The covering attack as a generalization of the Weil descent attack is to transform the discrete logarithm problems over $J(C_0)/k_n$ to the discrete logarithm problems over $J(C)/k$.

1.2 Key length and size of ground field

Assume the key length of a finite abelian group used in cryptosystem is

$$l = \tilde{O}(2^{160})$$

here we use the symbol: $\tilde{O}(x) := O(x \log^m x)$.

Now consider a cryptosystem based on A/k: an abelian variety over k with $\dim A = g(\geq 1)$

Then one can assume the size of the definition field $k = \mathbb{F}_q$ to be

$$q = \tilde{O}\left(l^{\frac{1}{g}}\right)$$

For A/k_n, $k_n = \mathbb{F}_{q^n}$,

$$q = \tilde{O}\left(l^{\frac{1}{gn}}\right)$$

1.3 Square-root Attack on finite abelian groups

General attacks to an arbitraty abelian group, such as Baby-step-giant-step attack or Pollard's rho-method or lambda-method are "square-root" attack.

$\dim A = g$	1	2	$\cdots$	g
Attack cost	$\tilde{O}(q^{1/2})$	$\tilde{O}(q)$	$\cdots$	$\tilde{O}(q^{\frac{g}{2}})$
In term of l	$\tilde{O}(l^{1/2})$	$\tilde{O}(l^{1/2})$	$\cdots$	$\tilde{O}(l^{1/2})$

1.4 Index calculus attack on curve-based systems

Now we consider the case when A is the Jacobian variety of an algebraic curve C.
$A = J(C), C/k$: an algebraic curve

(1) When C is a hyperelliptic curve, the most powerful attack is the double-prime-variation by Gaudry-Theriault-Thome and Nagao [10], [13]

$g = g(C)$	1	2	$\cdots$	g
Attack cost	$\tilde{O}(q^{1/2})$	$\tilde{O}(q)$	$\cdots$	$\tilde{O}(q^{2-\frac{2}{g}})$
In term of l	$\tilde{O}(l^{1/2})$	$\tilde{O}(l^{1/2})$	$\cdots$	$\tilde{O}(l^{\frac{2(g-1)}{g^2}})$

(2) When C is a non-hyperelliptic curve of $g \geq 3$, one can almost always find a birational transform over k

$$C \overset{birat}{\dashrightarrow} C' \subset \mathbb{P}^2$$

such that $\deg C' = d \geq g + 1$

Notice that when C' is a hyperelliptic curve, one has $\deg C' = d(\geq g + 2)$

Then when C'/k

$g = g(C)$	3	$\cdots$	g
Attack cost	$\tilde{O}(q)$	$\cdots$	$\tilde{O}(q^{2-\frac{2}{d-2}})$
In term of l	$\tilde{O}(l^{1/3})$	$\cdots$	$\tilde{O}(l^{\frac{2(d-3)}{(d-2)(d-1)}})$
When $d = g+1$	$\tilde{O}(l^{1/3})$	$\cdots$	$\tilde{O}(l^{\frac{2(g-2)}{g(g-1)}})$

The last row is when one could transform C/k into C'/k with degree $d = g+1$.

1.5 Weil descent or Covering Attack

In this paper, we show the weak classes of elliptic and hyperelliptic curves of genus two and three defined on extension fields against covering attack.

Let $C_0/k_n, C/k$: algebraic curves over k.

Consider a covering over k_n

$$\pi : \quad C \quad \twoheadrightarrow \quad C_0$$

then

$$\pi_* : J(C) \longrightarrow \mathrm{Res}_{k_n/k}\big(J(C_0)\big)$$

defines an isogeny over k.

Let $g := g(C), g_0 := g(C_0) = ng_0$

Then these weak curves C_0 will be attacked by index calculus algorithms of the following complexities.

1.5.1 When C is a hyperelliptic curve

The double-large-prime attack costs

$$\tilde{O}(q^{2-\frac{2}{n}}) = \tilde{O}(l^{\frac{2(n-1)}{n^2 g_0}})$$

1.5.2 When C is a non-hyperelliptic curve with degree $d = n+1$

The Diem's variation costs

$$\tilde{O}(q^{2-\frac{2}{n-1}}) = \tilde{O}(l^{\frac{2(n-2)}{n(n-1)g_0}})$$

2 Review of Scholten form

Assume hereafter char$k \neq 2$. In fact, we could obtain more general results but we omit them here.

2.1 Scholten form over a quadratic extension field k_2

A Scholten form is defined as an elliptic curve

$$E/k_2: \quad y^2 = \alpha x^3 + \beta x^2 + \beta^q x + \alpha^q$$

Let

$$\begin{aligned} x &:= \left(\frac{t-\lambda q}{t-\lambda}\right)^2, \quad \lambda \in k_2 \setminus k \\ S &:= (t-\lambda)^3 y \end{aligned}$$

then

$$C/k: \quad S^2 = \alpha(t-\lambda^q)^6 + \beta(t-\lambda^q)^4(t-\lambda)^2 + \beta^q(t-\lambda^q)(t-\lambda)^4 + \alpha^q(t-\lambda)^6$$

One has (2,2) coverings

$$C \xrightarrow{2} E \xrightarrow{2} \mathbb{P}^1(x)$$

2.2 A triangle of equivalences

Let C/k: an algebraic curve with genus $g(C) = 2$

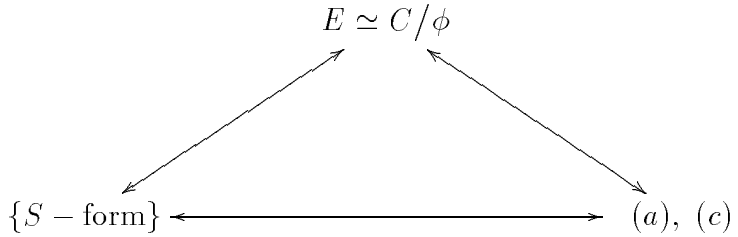
$\phi \curvearrowright C$: the bi-elliptic involution over k_2

σ: the Frobenius map

ι: the hyperelliptic involution

${}^{\sigma}\phi = \iota\phi$

We can prove the equivalences in the following triangle



Here $(a), (c)$ are among the following three cases for the elliptic curves:

$$E/k_2: \quad y^2 = f(x) \qquad \deg f(x) = 3$$

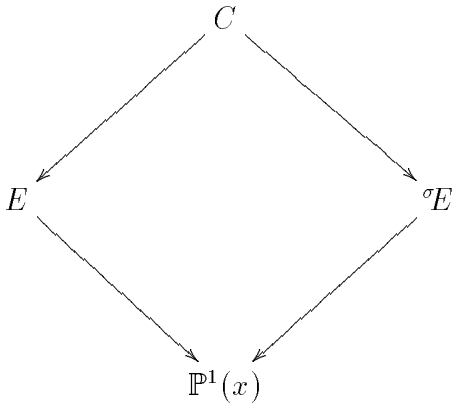
(a) : $f(x)$ is irreducible over k_2;

(b) : $f(x)$ is a product of a linear factor and a quadratic irreducible factor over k_2;

(c) : $f(x)$ is a product of three linear factors.

2.2.1 Elliptic curves with (2,2) coverings

Since the following diagram is a $(2,2)$ covering,



the elliptic curve E has the following form:

$$\begin{aligned} E/k_2: \quad y^2 &= a g(x)(x-\alpha) \\ g(x) &\in k[x], \quad \deg g(x) = 2, \text{ or } 3 \\ \alpha &\in k_2 \setminus k. \end{aligned}$$

2.2.2 Case (a)

In the case (a), one has

$$\begin{aligned} E: \quad y^2 &= a\,(x-\theta)\left(x-\theta^{q^2}\right)\left(x-\theta^{q^4}\right) \\ a \in k_2 \qquad & \theta \in k_6 \setminus k_2 \end{aligned}$$

Lemma 1. *Fix an $\epsilon \in k_3 \setminus k$, then*

$$\exists A \in GL_2(k_2), \quad s.t. \quad A \cdot \epsilon = \theta$$

which is unique up to a scalar modulo $k_2^\times$

Proof:
Since $PGL_2(k_2)$ acts on $k_6 \setminus k_2$ without fixed points, and $|PGL_2(k_2)| = |k_6 \setminus k_2|$. $\square$

Remark: If one denotes

$$\begin{aligned} \theta &= a\epsilon^2 + b\epsilon + c \\ a,b,c &\in k_2, \quad (a,b) \neq (0,0) \end{aligned}$$

and

$$\epsilon^3 = r\epsilon + e, \qquad r,e \in k$$

then A can be written in an explicit form as

$$A = \begin{pmatrix} a(ar+c)-b^2 & a^2e-bc \\ a & -b \end{pmatrix}$$

From the lemma 1, E is isogenous to

$$\begin{aligned} y^2 &= a'(x-\epsilon)(x-\epsilon^q)\left(x-\epsilon^{q^2}\right)(x-\alpha) \\ &= a'g(x)(x-\alpha) \\ \text{here} \quad g(x) &:= (x-\epsilon)(x-\epsilon^q)\left(x-\epsilon^{q^2}\right) \in k[x] \end{aligned}$$

2.2.3 Transformation from $(a),(c)$ to Scholten forms

For the case (a), one can use

$$B = \begin{pmatrix} 1 & -\alpha^q \\ 1 & -\alpha \end{pmatrix}$$

For the case (c), the transform is similiar.

2.2.4 Weil descent attack on Scholten forms

It is proposed by Arita-Matsuo-Nagao to apply Weil descent attack to the Scholten forms. These authors also classified completely the elliptic curves which have (2,2) covering over k_2.[12].

3 Weil restriction obtained by (2,2,...,2) coverings

Assume C_0 is a hyperelliptic curve,

$$C \longrightarrow C_0 \xrightarrow{2} \mathbb{P}^1(x)$$

is a $(2,2,...,2)$ covering of degree 2^r for $r=n$ or $n-1$, and

$$g_0 := g(C_0), \quad g := g(C) = ng_0.$$

Lemma 2. .

(1) $\ker\left(J(C) \longrightarrow Res_{k_n/k}(J(C_0))\right) \subset J(C)[2^{r-1}]$
(2) If C is hyperellptic, then the above kernel can be described explicitly.

Below, we classify the types of the covering $C \longrightarrow C_0$ using the Riemann-Hurwitz formula.

3.1 Case $g_0 = 1$

Assume $C_0 = E$, an elliptic curve.

3.1.1 When $n = 3$

(i) When the degree of the covering $C \longrightarrow C_0 \longrightarrow \mathbb{P}^1(x)$ is eight.

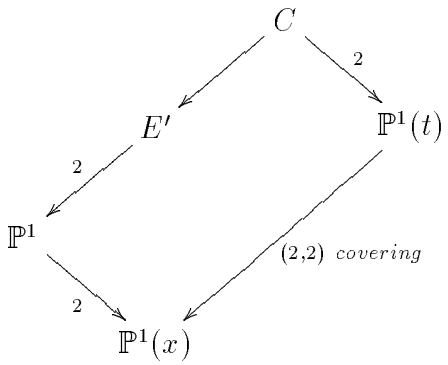
In this case, C is a hyperellptic curve of genus three over k, and $E = C_0/k_3$, which has C as its (2,2) covering, has the form of

$$\begin{aligned} E/k_3: \quad y^2 &= eg(x)(x-\alpha)(x-\alpha^q) \\ \text{here} \qquad & \alpha \in k_3 \setminus k, \\ & g(x) \in k[x], \quad \deg g(x) = 1 \text{ or } 2, \\ & e \in k_3^{\times} \end{aligned}$$

Then E become the case (c) under an isogeny of degree 2 and

$$\#\{k_3 - \text{Isomorphic classes of } E\} = O(q^2)$$

Next we show how to explicitly construct C/k.



$E' \sim_{/k_3} E$

First, the bi-elliptic involution ϕ on $\mathbb{P}^1(t)$ can be expressed as follows.

$$\begin{aligned} \phi &= \begin{pmatrix} \beta & b \\ 1 & -\beta \end{pmatrix} \\ \text{here} \qquad 4\beta &= \alpha^{q^2} \\ D &= (\beta - \beta^q)\left(\beta - \beta^{q^2}\right) \\ b &= D - \beta^2 \end{aligned}$$

Denote again the Frobenius map over k as σ, one can see that on $\mathbb{P}^1(t)$

$$\phi \cdot {}^{\sigma}\phi = {}^{\sigma}\phi \cdot \phi = {}^{\sigma^2}\phi$$

Now we consider the covering of degree 2:

$$\mathbb{P}^1 \xrightarrow{2} \mathbb{P}^1(x).$$

Then $\mathbb{P}^1$ is defined by

$$\begin{aligned} \mathbb{P}^1: \quad Y^2 &= g(x) = ax^2 + bx + c, \quad a,b,c \in k, \quad (a,b) \neq (0,0) \\ y &= \left(t + \phi(t) - {}^{\sigma}\phi(t) - {}^{\sigma^2}\phi(t)\right) Y \end{aligned}$$

and

$$\begin{aligned} x &= t + \phi(t) + {}^{\sigma}\phi(t) + {}^{\sigma^2}\phi(t) \\ &= \frac{F(t)}{N(t-\beta)}, \qquad N(\cdot) := N_{k_3/k}(\cdot) \end{aligned}$$

Assume that $\beta \in k_3 \setminus k$ satisfies the following equation:

$$\beta^3 - a_1\beta^2 + b_1\beta - c_1 = 0, \qquad \exists a_1, b_1, c_1 \in k.$$

then

$$\begin{aligned} N(t-\beta) &= t^3 - a_1 t^2 + b_1 t - c_1 \\ F(t) &= t^4 - 2b_1 t^2 + 8c_1 t + (b_1^2 - 4a_1 c_1) \end{aligned}$$

Thus one obtains the following definition equation for C/k

$$\begin{aligned} C/k: \quad S^2 &= aF(t)^2 + bF(t)N(t-\beta) + cN(t-\beta)^2 \\ S &= N(t-\beta)Y \end{aligned}$$

Now we can compare the security of the genus three hyperelliptic curve C/k under square-root attacks with the elliptic curve E/k_3 under the double-large-prime attacks.

Attack to E/k_3	$\tilde{O}(q^{3/2})$	$\tilde{O}(l^{1/2})$
Attack to C/k	$\tilde{O}(q^{4/3})$	$\tilde{O}(l^{4/9})$

(ii) When the degree of the covering $C \longrightarrow C_0 \longrightarrow \mathbb{P}^1(x)$ is four.

Then one can see C is a non-hyperelliptic curve over k.

The elliptic curves E/k_3 which have C as their $(2,2)$ covering can be divided into the following two types.

$$\begin{aligned} &\text{Type 1:} \qquad E: \quad y^2 = (x-\alpha)\left(x-\alpha^q\right)(x-\beta)\left(x-\beta^q\right) \\ &\qquad\qquad\qquad\qquad \alpha, \beta \in k_3 \setminus k, \quad \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4 \\ &\text{Type 2:} \qquad E: \quad y^2 = (x-\alpha)\left(x-\alpha^{q^3}\right)\left(x-\alpha^q\right)\left(x-\alpha^{q^4}\right) \\ &\qquad\qquad\qquad\qquad \alpha \in k_6 \setminus \{k_2 \cup k_3\} \end{aligned}$$

The Type 1 elliptice curve E can be transformed by a k-isomorphism to

$$E \underset{/k}{\simeq} \quad y^2 = ex(x-1)(x-\lambda)$$

$$\begin{cases} \lambda = \frac{\beta-\alpha}{\beta-\alpha^q} \cdot \frac{\beta^q-\alpha^q}{\beta^q-\alpha} \\ e\lambda \in \left(k_3^{\times}\right)^2 \end{cases}$$

The Type 2 elliptice curve E can be transformed by a k-isomorphism to

$$E \underset{/k}{\simeq} \qquad y^2 = ex(x-1)(x-\lambda)$$

$$\begin{cases} \lambda = \frac{\alpha^q-\alpha}{\alpha^q-\alpha^{q^2}} \cdot \frac{\alpha^{q^4}-\alpha^{q^3}}{\alpha^{q^4}-\alpha} = \left(\frac{\alpha^q-\alpha}{\alpha^q-\alpha^{q^3}}\right)^{1+q^3} \\ e\left(\alpha^q-\alpha^{q^3}\right)^{1+q^3} \in \left(k_3^{\times}\right)^2 \end{cases}$$

Lemma 3. *For $q \geq 41$*

$$(1) \qquad \forall \lambda \in k_3 \setminus k, \qquad \exists \alpha, \beta \in k_3 \setminus k, \qquad \#\left\{\alpha, \alpha^q, \beta, \beta^q\right\} = 4$$
$$s.t. \quad \lambda = \frac{\beta-\alpha}{\beta-\alpha^q} \cdot \frac{\beta^q-\alpha^q}{\beta^q-\alpha}$$

$$(2) \qquad \forall \lambda \in k_3 \setminus k \qquad \exists \alpha \in k_6 \setminus \{k_3 \cup k_2\}$$
$$s.t. \quad \lambda = \left(\frac{\alpha^q-\alpha}{\alpha^q-\alpha^{q^3}}\right)^{1+q^3}$$

Theorem 1. *If $q \geq (2 \times 1953)^2$ and*

$$E/k_3 : \qquad y^2 = ex(x-1)(x-\lambda) \qquad \lambda \in k_3 \setminus k$$

Then E is k-isomorphic to an elliptic curve either Type I or II.

$$E \underset{/k}{\simeq} \text{ an elliptic curve of either Type I or Type II.}$$

Furthermore, using an isogeny of degree 2, we have

Corollary 1. *The number of k_3-isomorphism classes of the elliptic curves defined over k_3 which belong to Type I or Type II is almost*

$$\frac{1}{2}q^3 + \frac{1}{3}q^3 = \frac{5}{6}q^3$$

i.e. such curves have a density of $5/12$

Since C is a degree 4 non-hyperelliptic curve over k, the discrete logarithms on the above E and on C attacked by Diem's variation have the following complexities.

Attack to E/k_3	$\tilde{O}(q^{3/2})$	$\tilde{O}(l^{1/2})$
Attack to C/k	$\tilde{O}(q)$	$\tilde{O}(l^{1/3})$

The explicit construction of the covering $C \longrightarrow E$ will be discussed in the following section.

3.1.2 When $n = 5$

In this case, the (2,2,2,2) covering C of E is a non-hyperelliptic curve over k. The elliptic curve E/k_5 with C as its covering has a form of

$$E: \quad y^2 = (x-\alpha)(x-\alpha^q)\left(x-\alpha^{q^2}\right)\left(x-\alpha^{q^3}\right)$$
$$\alpha \in k_5 \setminus k$$

The number of k_5-isomorphism classes of such E=$O(q^2)$

Assume the deg$C$ $=$ d, the complexity of Diem's variation to C is $\tilde{O}(q^{2-\frac{2}{d-2}}) = \tilde{O}(l^{\frac{2(d-3)}{n(d-2)}})$. If $d = 6$ then

Attack to E/k_5	$\tilde{O}(q^{5/2})$	$\tilde{O}(l^{1/2})$
Attack to C/k	$\tilde{O}(q^{3/2})$	$\tilde{O}(l^{3/10})$

3.2 The case $g_0 = 2$

3.2.1 When $n = 2$

The curve C_0 is of the form

$$C_0: \quad y^2 = e(x-\alpha)g(x)$$
$$\alpha \in k_2 \setminus k, \quad g(x) \in k[x], \quad \deg g(x) = m = 4 \text{ or } 5$$
$$\#\{k_2 - \text{isomorphic classes of } C_0\} = O(q^4)$$

Now we show how to construct the covering C/k. First define

$$\begin{aligned} u &:= y + {}^{\sigma}y \\ v &:= \eta(y - {}^{\sigma}y) \quad s.t. \quad {}^{\sigma}\eta = -\eta \qquad (\neq 0) \\ t &:= \frac{v}{u} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &:= \begin{pmatrix} \eta(e\alpha - e^q\alpha^q) & -(e\alpha + e^q\alpha^q) \\ \eta(e - e^q) & -(e + e^q) \end{pmatrix} \\ G(X,Y) &:= Y^m g(\frac{X}{Y}), \quad m := \deg g(x) \\ S &:= \left(c(t^2+\eta^2) + d\eta^2 t\right)^3 u \end{aligned}$$

then the C/k can be constructed as follows when $m = 4$ and 5.

When $m = 4$

$$C: \quad S^2 = (ad-bc)\eta^2 \times \left(c(t^2+\eta^2) + d\eta^2 t\right) \times G\left(a(t^2+\eta^2) + b\eta^2 t, c(t^2+\eta^2) + d\eta^2 t\right)$$

When $m = 5$

$$C: \quad S^2 = (ad-bc)\eta^2 \times G\left(a(t^2+\eta^2) + b\eta^2 t, c(t^2+\eta^2) + d\eta^2 t\right)$$

If one applies the double-large-prime attack to these two genus four hyperelliptic curves, the complexities will be

Attack to C_0/k_2	$\tilde{O}(q^2)$	$\tilde{O}(l)$
Attack to C/k	$\tilde{O}(q^{3/2})$	$\tilde{O}(l^{3/8})$

3.2.2 When $n = 3$

In this case, C is a non-hyperelliptic curve over k

The C_0 with C as its covering have the following three forms:

$$C_0^{(1)}: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)(x-\gamma)(x-\gamma^q)$$
$$\alpha, \beta, \gamma \in k_3 \setminus k$$

$$C_0^{(2)}: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)\left(x-\beta^{q^3}\right)\left(x-\beta^{q^4}\right)$$
$$\alpha \in k_3 \setminus k, \quad \beta \in k_6 \setminus (k_2 \cup k_3)$$

$$C_0^{(3)}: \quad y^2 = (x-\alpha)(x-\alpha^q)\left(x-\alpha^{q^3}\right)\left(x-\alpha^{q^4}\right)\left(x-\alpha^{q^6}\right)\left(x-\alpha^{q^7}\right)$$
$$\alpha \in k_9 \setminus k_3$$

$$\#\left\{k_3 - \text{isomorphic classese of } C_0^{(i)}\right\} = O(q^6)$$

If one applies the double-large-prime attack to C_0 and Diem's variation to the non-hyperelliptic curve C, the complexities are as follows.

Attack to $C_0^{(i)}/k_3$	$\tilde{O}(q^3)$	$\tilde{O}(l^{1/2})$
Attack to C/k	$\tilde{O}(q^{2-\frac{2}{d-2}})$	$\tilde{O}(l^{\frac{d-3}{3(d-2)}})$
Attack to $C/k, d = 7$	$\tilde{O}(q^{\frac{8}{5}})$	$\tilde{O}(l^{\frac{4}{15}})$

3.3 When $g_0 = 3, C_0$ is a hyperelliptic curve

3.3.1 When $n = 2$

In the case, C is a hyperelliptic curve over k of genus 6.

The C_0 with such C as its covering has the form:

$$C_0: \quad y^2 = e(x-\alpha)g(x)$$
$$\alpha \in k_2 \setminus k, \quad g(x) \in k[x], \quad \deg g(x) = m = 6 \text{ or } 7$$

$$\#\{k_2 - \text{isomorphic classes of } C_0\} = O(q^6)$$

The construction of C is the same as in the case of $g_0 = 2, n = 2$

When one applies the double-large-prime attack to C, one has complexities

Attack to C_0/k_2	$\tilde{O}(q^{8/3})$	$\tilde{O}(l^{4/9})$
Attack to C/k	$\tilde{O}(q^{\frac{5}{3}})$	$\tilde{O}(l^{\frac{5}{18}})$

3.3.2 When $n = 3$

The C is a non-hyperelliptic curve over k.

The C_0 with C as its covering has the following four forms.

$$C_0^{(1)}: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)(x-\gamma)(x-\gamma^q)(x-\delta)(x-\delta^q)$$
$$\alpha, \beta, \gamma, \delta \in k_3 \setminus k$$

$$C_0^{(2)}: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)(x-\gamma)(x-\gamma^q)\left(x-\gamma^{q^3}\right)\left(x-\gamma^{q^4}\right)$$
$$\alpha, \beta \in k_3 \setminus k, \quad \gamma \in k_6 \setminus (k_2 \cup k_3)$$

$$C_0^{(3)}: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)\left(x-\beta^{q^3}\right)\left(x-\beta^{q^4}\right)\left(x-\beta^{q^6}\right)\left(x-\beta^{q^7}\right)$$
$$\alpha \in k_3 \setminus k, \quad \beta \in k_9 \setminus k_3$$

$$C_0^{(4)}: \quad y^2 = (x-\alpha)(x-\alpha^q)\left(x-\alpha^{q^3}\right)\left(x-\alpha^{q^4}\right)\left(x-\alpha^{q^6}\right)\left(x-\alpha^{q^7}\right)\left(x-\alpha^{q^9}\right)\left(x-\alpha^{q^{10}}\right)$$
$$\alpha \in k_{12} \setminus (k_6 \cup k_4)$$

$$\#\{k_3 - \text{isomorphic classes of } C_0\} = O(q^9)$$

If one applies Diem's variation on these non-hyperelliptic curves, the complexities are as follows.

Attack to $C_0^{(i)}/k_3$	$\tilde{O}(q^4)$	$\tilde{O}(l^{4/9})$
Attack to C/k	$\tilde{O}(q^{2-\frac{2}{d-2}})$	$\tilde{O}(l^{\frac{2(d-3)}{9(d-2)}})$
Attack to $C/k, d = 10$	$\tilde{O}(q^{\frac{7}{4}})$	$\tilde{O}(l^{\frac{7}{36}})$

4 Construction of covering $C \longrightarrow E$ for the case 3.1.1.(ii)

Since $C \longrightarrow C_0 \longrightarrow \mathbb{P}^1(x)$ is a (2,2) covering, the action of the bi-elliptic involution ϕ on $H^0(C/k_3, \Omega^1)$ can be expressed as

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad {}^{\sigma}\phi = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad {}^{\sigma^2}\phi = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

i.e.,

$$\phi(\omega) = \omega, \qquad \phi({}^{\sigma}\omega) = -{}^{\sigma}\omega, \qquad \phi({}^{\sigma^2}\omega) = -{}^{\sigma^2}\omega$$

If one makes correspondence

$$\omega \longleftrightarrow \text{ line } \ \ell$$

using the canonical embedding of C into $\mathbb{P}^2$, then C can be expressed as

$$C: \quad \alpha\ell^4 + \alpha^q\, {}^{\sigma}\ell^4 + \alpha^{q^2}\, {}^{\sigma^2}\ell^4 + \beta\ell^{2+2\sigma} + \beta^q\ell^{2\sigma+2\sigma^2} + \beta^{q^2}\ell^{2\sigma^2+2} = 0$$

Lemma 4. *For $q \geq 41$*

$$\begin{aligned} &\forall \alpha, \beta \in k_3 \setminus k \qquad \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4 \\ &\exists \lambda \in k_3 \quad s.t. \quad Tr_{k_3/k}(\alpha\lambda^4 + \beta\lambda^{2+2q}) = 0 \end{aligned}$$

According to this lemma, one can always use variable change

$$\ell \longmapsto \lambda^{-1}\ell$$

so one can assume

$$Tr_{k_3/k}(\alpha + \beta) = 0$$

Next, we use the correspondences

$$\ell \longleftrightarrow X \qquad {}^{\sigma}\ell \longleftrightarrow Y \qquad {}^{\sigma^2}\ell \longleftrightarrow Z$$

one obtains a defining equation of C over k_3

$$C: \quad \alpha X^4 + \alpha^q Y^4 + \alpha^{q^2} Z^4 + \beta X^2 Y^2 + \beta^q Y^2 Z^2 + \beta^{q^2} Z^2 X^2 = 0$$

Let

$$y := \frac{Y}{X}, \quad z := \frac{Z}{X}$$

$$C: \quad \alpha + \alpha^q y^4 + \alpha^{q^2} z^4 + \beta y^2 + \beta^q y^2 z^2 + \beta^{q^2} z^2 = 0$$

Then

$$\phi(y) = -y, \qquad \phi(z) = -z.$$

Next, let

$$u := y^2, \qquad v := z^2, \qquad w := yz$$

then the E/k_3 can be expressed as

$$\begin{aligned} E/k_3: \quad &\alpha + \alpha^q u^2 + \alpha^{q^2} v^2 + \beta u + \beta^q uv + \beta^{q^2} v^2 = 0 \\ &w^2 = uv \end{aligned}$$

Furthermore, if one uses

$$s := \frac{1}{t}, \quad t := \frac{v}{u}, \quad h := \frac{w}{u}$$

then the defining equation of E becomes

$$\begin{aligned} E: \quad & \alpha s^2 + \alpha^q + \alpha^{q^2} t^2 + \beta s + \beta^q t + \beta^{q^2} st = 0 \\ & h^2 = t \end{aligned}$$

Now according the condition $Tr_{k_3/k}(\alpha + \beta) = 0$, one can assume

$$s = 1 + \ell(t - 1)$$

then

$$t = \frac{\alpha(1-\ell)^2 + \beta(1-\ell) + \alpha^q}{\alpha\ell^2 + \beta^{q^2}\ell + \alpha^{q^2}}$$

If one define

$$S := \left(\alpha\ell^2 + \beta^{q^2}\ell + \alpha^{q^2}\right) h$$

Then the defining equation of E becomes

$$E: \quad S^2 = \left(\alpha\ell^2 + \beta^{q^2}\ell + \alpha^{q^2}\right)\left\{\alpha(1-\ell)^2 + \beta(1-\ell) + \alpha^q\right\}$$

Now define

$$D := \beta^2 - 4\alpha^{1+q}$$

We consider two cases according to whether D is a quadratic residue or not.

4.1 Case $D \in \left(k_3^\times\right)^2$

$$E \underset{/k}{\simeq} \qquad y^2 = ex(x-1)(x-\lambda)$$

$$e\epsilon \in \left(k_3^\times\right)^2$$

here $$\lambda = \frac{2\alpha+\beta+\beta^{q^2}+\sqrt{D}-\sqrt{D^q}}{2\alpha+\beta+\beta^{q^2}-\sqrt{D}-\sqrt{D^q}} \cdot \frac{2\alpha+\beta+\beta^{q^2}-\sqrt{D}+\sqrt{D^q}}{2\alpha+\beta+\beta^{q^2}+\sqrt{D}+\sqrt{D^q}}$$

$$\epsilon = \left(2\alpha + \beta + \beta^{q^2} - \sqrt{D} + \sqrt{D^q}\right)\left(2\alpha + \beta + \beta^{q^2} + \sqrt{D} - \sqrt{D^q}\right)$$

4.2 Case $D \notin \left(k_3^\times\right)^2$

$$E \underset{/k}{\simeq} \qquad y^2 = ex(x-1)(x-\eta^{1+q^3})$$

$$e\epsilon \in \left(k_3^\times\right)^2$$

here $$\eta = \frac{2\alpha+\beta+\beta^{q^2}+\sqrt{D}-\sqrt{D^q}}{2\alpha+\beta+\beta^{q^2}-\sqrt{D}-\sqrt{D^q}}$$

$$\epsilon = \left(2\alpha + \beta + \beta^{q^2} - \sqrt{D} + \sqrt{D^q}\right)^{1+q^3}$$

References

[1] L.Adleman, J.DeMarrais, and M.Huang, "A subexpotential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields," Algorithmic Number Theory, Springer-Verlag, LNCS 877, pp.28-40, 1994.

[2] S. Arita, K. Matsuo, K. Nagao, M. Shimura "A Weil descent attack against elliptive curve cryptosystems over quartic extension field I" Proceedings of SCIS2004, IEICEI Japan 2004.

[3] C.Diem, "The GHS attack in odd characteristic," J.Ramanujan Math.Soc, vol.18 no.1, pp.1-32, 2003.

[4] C. Diem, "Index calculus in class groups of plane curves of small degree", preprint, April, 2005.

[5] C. Diem, J. Scholten, "Cover attaks, a report for the AREHCC project", preprint Oct. 2003.

[6] A.Enge, and P.Gaudry, "A general framework for subexponential discrete logarithm algorithms," Acta Arith.,vol.102, pp.83-103, 2002.

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

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

[9] P.Gaudry, "An Algorithm for solving the discrete logarithm problem on hyperelliptic curves," Advances in cryptology EUROCRYPTO 2000, Springer-Verlag, LNCS 1807, pp.19-34, 2000.

[10] P.Gaudry, N.Theriault, E.Thome " A double large prime variation for small genus hyperelliptic index calculus" Preprint, Feb.2005.

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

[12] F. Momose, J. Chao, M. Shimura "On Weil descent of elliptic curves over quadratic extensions" Proceedings of SCIS2005, pp.787-792, 2005

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