Scholten forms and elliptic/hyperelliptic curves with weak Weil restrictions

Fumiyuki Momose, Jinhui Chao

Dept. of Mathematics, and Dept. of Information and Sysytem Engineering
Chuo University, Tokyo, Japan
1-13-27, Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

November 21, 2005

Abstract

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 either index calculus attacks to hyperelliptic curves or Diem's recent attack to non-hyperelliptic curves. In particular, we show how to construct such coverings from these curves and analyze density of the curves for them such construction is possible.

keywords

Elliptic curves, Hyperelliptic curves, Non-hyperelliptic curves,
Index calculus attacks, Weil descent attack, Cover attack

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 [11][8][20][12][18] and the Weil descent attack or cover attack[9] [13][10] [16][5] [14][15] [21][22][7].

Among the index calculus attacks to curves other than elliptic curves, i.e. curves with genera greater than one, the double-large-prime variation[12][18] is the most powerful to hyperelliptic curves. It is known that the hyperelliptic curves of genera $g \geq 4$ but not too large can be attacked by these algorithms more effectively than the square-root attacks. In spite of a common believing that non-hyperelliptic curves should be harder to attack than hyperelliptic ones, Diem recently showed an attack under which non-hyperelliptic curves of low degrees and genera greater than three are weaker than hyperelliptic curves[6].

In particular, genus three non-hyperelliptic curves over $\mathbb{F}_q$ represented by degree 4 plane curves can be attacked in an expected time $\tilde{O}(q)$ by the double-large-prime variation of his attack, while the double-large-prime attack to genus three hyperelliptic curves cost $\tilde{O}(q^{4/3})$ and the square-root attacks cost $\tilde{O}(q^{3/2})$.

In this paper, we show explicitly classes of elliptic curves and hyperelliptic curves of low genera defined over extension fields, which have weak coverings, i.e. their Weil restrictions can be attacked effectively by one of the above two index calculus attacks. In particular, we show how to construct such coverings from these curves and analyze density of the curves for them such construction is possible.

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

2 A review of attacks to algebraic curve based cryptosystems

Below we review attacks to discrete logarithm on algebraic curve based systems and their complexities.

2.1 Key length and size of ground fields

Let q be a power of a odd prime. $k := \mathbb{F}_q, k_n := \mathbb{F}_{q^n}$.

Assume the key length of a finite abelian group used in a 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 an abelian variety A defined over k with dimension $\dim A = g (\geq 1)$

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,

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

2.2 Square-root Attacks on finite abelian groups

General attacks to discrete logarithm on an arbitraty abelian group, such as the Baby-step-giant-step attack or Pollard's rho-method or lambda-method are "square-root" attacks, i.e., they have computional costs of the square-root of the group order. For examples, their costs for A with different g are shown as follows:

$\dim A = g$	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	$\tilde{O}(l^{1/2})$	$\tilde{O}(l^{1/2})$	$\cdots$	$\tilde{O}(l^{1/2})$

2.3 Index calculus attacks on algebraic curve based systems

Now we consider the case when A is the Jacobian variety of an algebraic curve C, i.e., $A = J(C)$ and C/k is an algebraic curve defined over k, then g equals to the genus of C.

(1) When C is a hyperelliptic curve, the most powerful attack is the double-large-prime variation of index calculus by Gaudry-Theriault-Thome and Nagao [12], [18], with complexities as follows.

$g = g(C)$	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 genus $g \geq 3$, 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' is defined over k, the complexity of Diem's double-large-prime variation [6] are as follows.

$g = g(C)$	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 to C'/k with degree $d = g+1$.

2.4 Weil descent or covering attacks

Let C_0/k_n to be an algebraic curve over k_n with genus $g(C_0) \geq 1$.
If there exists an algebraic curve C defined over k and

$$\pi : C \twoheadrightarrow C_0$$

is a covering defined over k_n then

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

defines an isogeny over k.

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

2.5 Weil descent or covering attack + Index calculus

In this paper, we show explicit classes of elliptic curves and hyperelliptic curves of genus two and three defined on extension fields whose Weil restrictions can be effectively attacked by either of the index calculus algorithms for hyperelliptic curves and non-hyperelliptic curves.

Using the same symbols of the previous section, let $g_0 := g(C_0), g := g(C) = ng_0$. The discrete logarithm on C_0 will be attacked by index calculus algorithms in the following complexities.

2.5.1 When C is a hyperelliptic curve

The double-large-prime attack to hyperelliptic curves costs

$$\tilde{O}(q^{2-\frac{2}{ng_0}}) = \tilde{O}(l^{\frac{2(ng_0-1)}{n^2g_0^2}})$$

2.5.2 When C is a non-hyperelliptic curve with degree $d = ng_0 + 1$

Diem's double-large-prime variation costs

$$\tilde{O}(q^{2-\frac{2}{ng_0-1}}) = \tilde{O}(l^{\frac{2(ng_0-2)}{(ng_0-1)ng_0}})$$

3 On Scholten forms

We first show some results on the so-called Scholtem forms of elliptic curves as a preparation of the rest of the paper. Assume hereafter char$k \neq 2$. More general results can also be proved for char$k = 2$ case but we omit them here.

3.1 Scholten forms over a quadratic extension field k_2

A Scholten form is defined as an elliptic curve in the form of [19]

$$E/k_2: \quad y^2 = \alpha x^3 + \beta x^2 + \beta^q x + \alpha^q. \tag{1}$$

Let

$$x := \left(\frac{t-\lambda^q}{t-\lambda}\right)^2, \quad \lambda \in k_2 \setminus k \tag{2}$$

$$S := (t-\lambda)^3 y \tag{3}$$

then one obtains a (2,2) covering

$$C \overset{2}{\underset{2}{\rightrightarrows}} E \overset{2}{\underset{2}{\rightrightarrows}} \mathbb{P}^1(x) \tag{4}$$

where

$$C/k: \; S^2 = \alpha(t-\lambda^q)^6 + \beta(t-\lambda^q)^4(t-\lambda)^2 + \beta^q(t-\lambda^q)(t-\lambda)^4 + \alpha^q(t-\lambda)^6 \tag{5}$$

3.2 A triangle of equivalences

Let C/k be an algebraic curve defined over k with genus $g(C) = 2$, ϕ the bi-elliptic involution acting on C defined over k_2, σ the Frobenius map and ι the hyperelliptic involution. Assume that ${}^{\sigma}\phi = \iota\phi$.

We can prove the equivalences in the following triangle.

$$\begin{tikzcd}
 & E \simeq C/\phi \arrow[dl, Leftrightarrow] \arrow[dr, Leftrightarrow] & \\
\{S - \text{form}\} \arrow[rr, Leftrightarrow] & & (a),\ (c)
\end{tikzcd}$$

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.

3.2.1 Elliptic curves with (2,2) coverings

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

$$\begin{tikzcd}
 & C \arrow[dl] \arrow[dr] & \\
E \arrow[dr] & & {}^{\sigma}E \arrow[dl] \\
 & \mathbb{P}^1(x) &
\end{tikzcd}$$

the elliptic curve E has the following form:

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

3.2.2 The case (a)

In the case (a), one has

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

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

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

which is unique up to a scalar modulo $k_2^{\times}$. Here $A\epsilon$ denotes a PGL_2 action:

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad A\epsilon := \frac{a\epsilon + b}{c\epsilon + d}$$

Proof: Since $PGL_2(k_2)$ acts on $k_6 \backslash k_2$ without fixed points, and $\#\{PGL_2(k_2)\} = \#\{k_6 \setminus k_2\}$. □

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

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

From the lemma 1, E is k_2-isomorphic to

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

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

Elliptic curves in forms of (a) or (c) can be transformed into the Scholten forms by PGL_2 actions.

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.

3.2.4 Weil descent attack on Scholten forms

It is proposed to apply the Weil descent attack to the Scholten forms in [19] [2]. The elliptic curves which have (2,2) covering over k_2 were classified in [17].

4 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.

4.1 The case $g_0 = 1$

Assume $C_0 = E$, an elliptic curve.

4.1.1 When $n = 3$

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

In this case, C is a hyperellptic curve over k of genus three [1]. E/k_3, which has C as its (2,2) covering, has the form of

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

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.

---

[1] This was also mentioned in [5] footnote 6

We have a diagram as follows, where E' is k_3-isogenous to E (of degree two).

$$\begin{tikzcd}
 & & C \arrow[dl] \arrow[dr, "2"] & \\
 & E' \arrow[dl, "2"'] & & \mathbb{P}^1(t) \arrow[ddll, "(2,2)\ covering"] \\
\mathbb{P}^1 \arrow[dr, "2"'] & & & \\
 & \mathbb{P}^1(x) & &
\end{tikzcd}$$

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

$$\begin{aligned} N(t-\beta) &= t^3 - a_1t^2 + b_1t - c_1 \\ F(t) &= t^4 - 2b_1t^2 + 8c_1t + (b_1^2 - 4a_1c_1) \end{aligned}$$

Thus one obtains the following defining equation[2] for C/k

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

The following table shows a comparison of complexities between the square-root attacks to the elliptic curve E/k_3, which is the most effective attacks known for genus one curves, and the double-large-prime attacks to the genus three hyperelliptic curve C/k.

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 $C \longrightarrow E \longrightarrow \mathbb{P}^1(x)$ is four

Except for the case that the covering $C \longrightarrow E$ corresponds to the covering $C \longrightarrow E'$ in the case (i), C is a non-hyperelliptic curve over k. We will show how to construct such a C in the section 5.

The elliptic curves E/k_3 which have C as their $(2,2)$ covering can be divided into the following two types.[3]

$$\text{Type I:} \qquad E: \quad y^2 = (x-\epsilon)(x-\epsilon^q)(x-\beta)(x-\beta^q) \tag{6}$$

$$\epsilon, \beta \in k_3 \setminus k, \quad \#\{\epsilon, \epsilon^q, \beta, \beta^q\} = 4 \tag{7}$$

$$\text{Type II:} \qquad E: \quad y^2 = (x-\alpha)\left(x-\alpha^{q^3}\right)(x-\alpha^q)\left(x-\alpha^{q^4}\right) \tag{8}$$

$$\alpha \in k_6 \setminus \{k_2 \cup k_3\} \tag{9}$$

Type I:

Using $PGL_2(k)$ action, the Type I elliptice curve E can be transformed by a k-isomorphism to

$$E \underset{/k}{\simeq} \quad y^2 = x(x-1)(x-\lambda) \tag{10}$$

$$\lambda = \tfrac{\beta-\epsilon^q}{\beta-\epsilon} \cdot \tfrac{\beta^q-\epsilon}{\beta^q-\epsilon^q} \tag{11}$$

To count the number of such λ, consider a $PGL_2(k)$ action on λ

$$\mu = \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \lambda \tag{12}$$

then since $\lambda \neq 0, 1, \infty$, $\mu \neq \epsilon, \epsilon^q$. Define

---

[2] Another form of the defining equation was obtained by N. Theriault [4] Th.22.10.3

[3] The equation (6) of Type I was also given as Eq.(10) in [7] as an example.

$$A =: \begin{pmatrix} -\mu + \epsilon + \epsilon^q & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix} \tag{13}$$

and

$$B :={}^{\sigma^2}\!A\ {}^{\sigma}\!A\ A. \tag{14}$$

Then we have

Lemma 3.

1.

$$A\beta = \beta^q \tag{15}$$

2.

$$B \not\equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \quad \mod k_3^\times \tag{16}$$

$$B\beta = \beta \tag{17}$$

3.

$$B\beta = \beta \implies A\beta = \beta^q \tag{18}$$

4. Let the discriminant

$$D := (TrB)^2 - 4(\det B) \quad (\in k) \tag{19}$$

then there exist such β *given a* λ *if and only if* $D \in (k)^2$*;*

5.

$$D = 0 \Longrightarrow \left.\begin{array}{l} \exists C \in GL_2(k), \quad C^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod} k^\times) \\ \beta = C\epsilon \end{array}\right\} \tag{20}$$

Since $PGL_2(k)$ acts on $k_3 \setminus k$ transitively, fix an ϵ. Then one can easily find β from λ as solutions of a quadratic equation obtained from (17), hence find elliptic curves which have the covering C.

Corollary 1. *For the elliptic curves (10) having the covering* C *or defined by the* λ *in (11),*

$$\#\{\lambda\} \approx \frac{1}{2}q^3. \tag{21}$$

Type II:

The Type II elliptice curve E can be transformed by a k_3-isomorphism to

$$E \underset{/k_3}{\simeq} \qquad y^2 = ex(x-1)(x-\lambda) \tag{22}$$

$$\begin{cases} \lambda = \left(\frac{\alpha^q - \alpha^{q^3}}{\alpha^q - \alpha}\right)^{1+q^3} \\ e \equiv N_{k_6/k_3}\left(\alpha^q - \alpha\right) \bmod \left(k_3^\times\right)^2 \end{cases} \tag{23}$$

We omit the details but just state the conclusion that the correspondence

$$PGL_2(k)\backslash\{\alpha\} \longrightarrow \{\lambda\}$$

is generically $2:1$. When the correspondence is 1-1,

$$\exists! A \in PGL_2(k) \quad s.t. \quad A\alpha = \alpha^{p^3}$$

From which such α can be easily found.

Lemma 4. *For the elliptic curves (22) having the covering C or defined by the λ in (23),*

$$\#\{\lambda\} \approx \frac{1}{2}q^3. \tag{24}$$

Since C is a degree 4 non-hyperelliptic curve over k, the attacks to the above E/k_3 by the square-root methods and to C/k by Diem's double-large-prime variation have the following complexities.

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

4.1.2 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

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

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

Assume $\deg(C) = d$, the complexity of Diem's double-large-prime 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 the complexities for the square-root attack to E/k_5 and Diem's attack to C/k are as follows.

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

4.2 The case $g_0 = 2$

4.2.1 When $n = 2$

The curve C_0 in this case is in the form

$$\begin{array}{rcl} C_0 : \ y^2 & = & e(x-\alpha)g(x) \\ & & \alpha \in k_2 \setminus k, \quad g(x) \in k[x], \quad \deg g(x) = m = 4 \ \text{ or } \ 5 \end{array}$$

$$\#\{k_2 - \text{isomorphic classes of } C_0\} = O(q^4)$$

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

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

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

<u>When $m = 4$</u>

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

<u>When $m = 5$</u>

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

If one applies either the square-root or the double-large-prime attack to C_0/k_2 and the double-large-prime attack to these two genus four hyperelliptic curves C/k, the complexities will be

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

4.2.2 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:

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

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

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

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

If one applies the double-large-prime attack to $C_0^{(i)}/k_3$ and Diem's variation to the non-hyperelliptic curve C/k, 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 $C/k, d=7$	$\tilde{O}(q^{\frac{8}{5}})$	$\tilde{O}(l^{\frac{4}{15}})$

4.3 The case $g_0 = 3$ and C_0 is a hyperelliptic curve

4.3.1 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:

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

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

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 these hyperelliptic curve C_0/k_2 and C/k defined on different fields, one has complexities

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

4.3.2 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.

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

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

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

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

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

If one applies the double-large-prime variation to the hyperelliptic curve $C_0^{(i)}/k_3$ and Diem's double-large-prime variation on the non-hyperelliptic curve C/k, 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 $C/k, d = 10$	$\tilde{O}(q^{\frac{7}{4}})$	$\tilde{O}(l^{\frac{7}{36}})$

5 Construction of covering $C \longrightarrow E$ for the case 4.1.1(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 defines correspondence

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

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

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

For $q \geq 37$, $C(k) \neq \emptyset$, then we obtain

Lemma 5. *When $q \geq 37$,*

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

According to this lemma, one can use the variable change

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

so that it can be assumed that

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

Next, by use of 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

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

Furthermore, if one defines

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

then the defining equation of E becomes

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

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 defines

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

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]

5.1 The case $D \in \left(k_3^\times\right)^2$

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

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

here

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

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

5.2 The case $D \notin \left(k_3^\times\right)^2$

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

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

here

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

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

---

[4] The case 5.1 is also studied by K.Nagao with certain conditions.

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, IEICE Japan 2004.

[3] I.F. Black, G.Seroussi and N.Smart, ”Advances in elliptic curve cryptography”, Cambridge University Press 2005.

[4] H. Cohn, G. Frey, “Handbook of elliptic and hyperelliptic curve cryptography”, Chapman & Hall, 2006

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

[6] C. Diem, “Index calculus in class groups of plane curves of small degree”, preprint, April, 2005.

[7] C. Diem, J. Scholten, “Cover attaks, a report for the AREHCC project”, preprint Oct. 2003.

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

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

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

[11] 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.

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

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

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

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

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

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

[18] K.Nagao “Improvement of Theriault algorithm of index calculus of Jacobian of hyperelliptic curves of small genus”, preprint 2004.

[19] Jasper Scholten ”Weil restriction of an elliptic curve over a quadratic extension”, available at (http://homes.esat.kuleuven.be/ jscholte/

[20] N.Thériault, ”Index calculus attack for hyperelliptic curves of small genus”, Advances in Cryptology - ASIACRYPT 2003, Lecture Notes in Computer Science, 2894, 75–92, 2003

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

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