Classification of Elliptic/hyperelliptic Curves with Weak Coverings against GHS Attack under an Isogeny Condition

Tsutomu Iijima [*] Fumiyuki Momose [†] Jinhui Chao [‡]

2013/09/20

Abstract

The GHS attack is known as a method to map the discrete logarithm problem(DLP) in the Jacobian of a curve C_0 defined over the d degree extension k_d of a finite field k to the DLP in the Jacobian of a new curve C over k which is a covering curve of C_0. Such curves C_0/k_d can be attacked by the GHS attack and index calculus algorithms. In this paper, we will classify all elliptic curves and hyperelliptic curves C_0/k_d of genus 2, 3 which possess $(2,...,2)$ covering C/k of $\mathbb{P}^1$ under the isogeny condition (i.e. $g(C) = d \cdot g(C_0)$) in odd characteristic case. Our main approach is analysis of ramification points and representation of the extension of $Gal(k_d/k)$ acting on the covering group $cov(C/\mathbb{P}^1)$. Consequently, all explicit defining equations of such curves C_0/k_d and existential conditions of a model of C over k are provided.

Keywords : Weil descent attack, GHS attack, Elliptic curve cryptosystems, Hyperelliptic curve cryptosystems, Index calculus, Galois representation

Contents

1 Introduction **2**

2 GHS and cover attack **4**

3 Galois representation **5**

[*] Koden Electoronics Co.,Ltd, 2-13-24 Tamagawa, Ota-ku, Tokyo, 146-0095 Japan

[†] Department of Mathematics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

[‡] Department of Information and System Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

4 Classification of C_0/k_d with covering C/k 6
4.1 The case when σ is indecomposable 7
4.1.1 When d is even 7
4.1.2 When d is odd 8
4.2 The case when σ is decomposable 10

5 Defining equations of C_0/k_d for $c = 1$ or a square 11
5.1 σ : indecomposable 11
5.1.1 d : even 11
5.1.2 d : odd 11
5.2 σ : decomposable 13

6 Existence of a model of C over k and defining equations of C_0 14
6.1 Existential condition of a model of C over k 14
6.2 Defining equations of C_0 with nonsquare c 16
6.2.1 σ : indecomposable 16
6.2.2 σ : decomposable 17

7 A complete list of C_0/k_d with (2,...,2)-covering C/k 17

1 Introduction

Let q be a power of an odd prime, $k := \mathbb{F}_q, k_d := \mathbb{F}_{q^d}$. We consider in this paper algebraic curves C_0/k_d used in cryptographic applications, i.e. elliptic and hyperelliptic curves of genera $g_0 := g(C_0) = 1, 2, 3$.

It is known that one of the most powerful attacks to the cryptosystems based on hyperelliptic curves of genus $g \geq 3$ is the so-called double-large-prime variation by Gaudry-Thériault-Thomé-Diem [13] and Nagao [27], with complexities $\tilde{O}(q^{2-\frac{2}{g}})$ over $\mathbb{F}_q$. Hyperelliptic curves of genera 5 to 9 can be attacked by the algorithm more effectively than the square-root attacks. For $g = 3$, the computational cost is $\tilde{O}(q^{4/3})$, slightly faster than the square-root attacks. Therefore elliptic and hyperelliptic curve of genera less than or equal to 3 are supposed to be secure at present. Recently Diem proposed an attack under which non-hyperelliptic curves of low degrees and genera greater than or equal to 3 are weaker than hyperelliptic curves[4]. In particular, if C is a non-hyperelliptic curve over k of genus $g \geq 3$ such that $\deg C = d$, the complexity of Diem's double-large-prime variation [4] is $\tilde{O}(q^{2-\frac{2}{d-2}})$. When $d = g + 1$, it is $\tilde{O}(q^{2-\frac{2}{g-1}})$. For an example, genus 3 non-hyperelliptic curves over $\mathbb{F}_q$ can be attacked in an expected time $\tilde{O}(q)$.

Another generic attack to algebraic curve-based cryptosystem is the so-called Weil descent attack, or GHS attack in particular[7][12][9][23][3][15][16][31] [32][17] and cover attack[5]. The GHS attack, in term of cover attack, can be described as to map the DLP in the Jacobian of C_0/k_d to the DLP in the Jacobian of a covering curve C/k of C_0/k_d, then apply the index calculus algorithms. Recently, Gaudry proposed a general algorithm to solve discrete logarithms on Abelian varieties of dimension n' in running time $\tilde{O}(q^{2-2/n'})$ where q tends to infinity and the constant hidden in the $O(\cdot)$ grows very fast with n' [11]. For finite d and q, its fastest case is for elliptic curves over cubic extension field k_3 when the running time $\tilde{O}(q^{4/3})$ is the same as the GHS attack with the double-large-prime algorithm to genus 3 hyperelliptic curves C.

Therefore the most effective attack scenario at present is provided by GHS attack when the covering curve C exists and is a non-hyperelliptic curve in particular. In this paper, we will focus on this scenario.

Hereafter, we assume the following condition which we call "the isogeny condition": There is a covering map between C/k and C_0/k_d

$$\pi/k_d : C \quad \twoheadrightarrow \quad C_0 \tag{1}$$

such that for

$$\pi_* : \quad J(C) \quad \twoheadrightarrow \quad J(C_0), \tag{2}$$

$$Re(\pi_*) : \quad J(C) \quad \longrightarrow \quad Re_{k_d/k}J(C_0) \tag{3}$$

defines an isogeny over k, here $J(C)$ is the Jacobian variety of C and $Re_{k_d/k}J(C_0)$ is its Weil restriction with respect to the field extension k_d/d. Obviously $g(C) = d \cdot g_0$ under this condition.

Notice that in general $g(C) \geq d \cdot g_0$ and could be and are often very large(see [3]). Therefore, $J(C)$ has the smallest size under the isogeny condition and the discrete logarithm problem on $J(C)$ could be most easily solved.

It is then an interesting and important question to see what kind and how many curves C_0 are weak against GHS attack or having coverings so that they can be attacked by GHS attack, even though they could have been originally designed to be secure for cryptographic applications. In particular, to obtain a complete list of all weak curves or to classify these weak curves should be very useful for cryptosystem design.

The classification and density analysis of these weak curves are nontrivial problems. It was also expected that even if such curves did exist, they should be special therefore rare. In [25] a classification and density analysis is provided for odd characteristics and genus $1, 2, 3$ elliptic and hyperelliptic curves for extension degree $2, 3, 5$, under an isogeny condition. In [26], a detailed analysis for elliptic curves defined over cubic fields is provided. In particular, existence of either hyperelliptic and non-hyperelliptic covering C/k and densities of C_0 are presented. It is shown that actually the number of these weak curves could be large. For $g_0 = 1, d = 3$, if one chosen random elliptic curves E defined over k_3 in the Legendre form, then a half of them are weak therefore can not be used in cryptosystems since 160-bit systems could only have strength of 107 bits key-length under the proposed attack.

In this paper, we classify the elliptic and hyperelliptic curves which are subjected to the GHS attack or have covering curves under the isogeny condition. In particular, we classify all $(2,...,2)$-covering of C_0/k_d, i.e. those with covering groups of order 2^n for $1 < n \leq d$. Our main approach is analysis of ramification points and representation of the extension of $\mathrm{Gal}(k_d/k)$ acting on the covering group $cov(C/\mathbb{P}^1)$. Furthermore, existential conditions of a model of C over k are discussed. As a result, a complete list and explicit defining equations of such weak curves C_0/k_d are obtained, which is included in the section 7.

2 GHS and cover attack

Assume the Frobenius automorphism $\sigma_{k_d/k}$ extends to an automorphism σ of order d in the separable closure of $k_d(x)$. It is showed by Diem[3] that $\sigma_{k_d/k}$ extends to an automorphism of the order d when C_0 is a hyperelliptic curve and d is odd for the odd characteristic cases. In the section 6, we will show a generalization of the condition.

Under the assumption, the Galois closure of $k_d(C_0)/k(x)$ is $K := k_d(C_0)\cdot \sigma(k_d(C_0))\cdots\sigma^{d-1}(k_d(C_0))$ and the fixed field of K by the automorphism σ is $K' := \{\zeta \in K \mid \sigma(\zeta) = \zeta\}$. The original GHS attack maps the DLP in $Cl^0(k_d(C_0)) \cong J(C_0)(k_d)$ to the DLP in $Cl^0(K') \cong J(C)(k)$ using the following composition of conorm and norm maps:

$$N_{K/K'} \circ Con_{K/k_d(C_0)} : Cl^0(k_d(C_0)) \longrightarrow Cl^0(K')$$

for elliptic curves in characteristic 2 case [12]. This attack has been extended to various classes of curves. It is also conceptually generalized to the cover attack by Frey and Diem [5] as described briefly as follows. When there exist an algebraic curve C/k and a covering $\pi/k_d : C \longrightarrow C_0$, the DLP in $J(C_0)(k_d)$ can be mapped to the DLP in $J(C)(k)$ by a pullback-norm map, as in the following diagram.

$$\begin{tikzcd}
J(C)(k_d) \arrow[d, "N"'] & J(C_0)(k_d) \arrow[l, "\pi^*"'] \arrow[dl, "N\circ\pi^*"] \\
J(C)(k) &
\end{tikzcd}$$

Unless otherwise noted, we consider that following hyperelliptic curves with $g(C_0) \in \{1, 2, 3\}$ given by

$$C_0/k_d \quad : \quad y^2 = c \cdot f(x) \tag{4}$$

where $c \in k_d^\times$ and $f(x)$ is a monic polynomial in $k_d[x]$ such that

$$C_0 \xrightarrow{2} \mathbb{P}^1(x) \tag{5}$$

is a degree 2 covering over k_d . Then, we have a tower of extensions of function fields such that $k_d(x, y, {}^{\sigma^1}y, \ldots, {}^{\sigma^{n-1}}y) \simeq k_d(C)$ is a $\overbrace{(2, ..., 2)}^{n}$ type extension where $n \leq d$. Here, a $\overbrace{(2, \ldots, 2)}^{n}$ covering is defined as a covering π/k_d : $C \longrightarrow \mathbb{P}^1$ such that $cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$, here $cov(C/\mathbb{P}^1) := Gal(k_d(C)/k_d(x))$.

Lemma 2.1. *The isogeny condition is equivalent to the each of following two statements.*
(A)

$$^\forall I \subset cov(C/\mathbb{P}^1),\ [cov(C/\mathbb{P}^1) : I] = 2,$$
$$g(C/I) = \left\{ \begin{array}{ll} 0 & I \neq {}^{\sigma^i}H, {}^\forall i \\ g_0 & I \simeq {}^{\sigma^i}H, {}^\exists i \end{array} \right. \qquad or \quad C^I = C/I = \left\{ \begin{array}{ll} \mathbb{P}^1 & I \neq {}^{\sigma^i}H, {}^\forall i \\ {}^{\sigma^i}C_0 & I \simeq {}^{\sigma^i}H, {}^\exists i \end{array} \right.$$

here $C/H = C_0$

(B) There is $H \subset cov(C/\mathbb{P}^1)$*, a subgroup of index 2 such that the Tate module of* $J(C)$ *has the following decomposition*

$$V_l(J(C)) = \oplus_{i=0}^{d-1} \quad V_l(J(C))^{\sigma^i H}. \tag{6}$$

3 Galois representation

We will classify all n-tuple $(2, ..., 2)$ coverings $C/\mathbb{P}^1$ with degree 2 subcovering $C_0/\mathbb{P}^1$ as below.

$$\overbrace{C \longrightarrow \underbrace{C_0 \longrightarrow \mathbb{P}^1(x)}_{2}}^{\overbrace{(2, \cdots, 2)}^{n}} \tag{7}$$

In order to do that, we consider and classify the representation of $G(k_d/k)$ on cov$(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$. For simplicity, we denote hereafter $\sigma_{k_d/k}$ as σ.

$$\begin{array}{ccc} Gal(k_d/k) \times cov(C/\mathbb{P}^1) & \longrightarrow & cov(C/\mathbb{P}^1) \\ (\sigma^i, \phi) & \longmapsto & {}^{\sigma^i}\phi := \sigma^i \phi \sigma^{-i} \end{array} \tag{8, 9}$$

Here, one has a map onto $Aut(cov(C/\mathbb{P}^1))$.

$$Gal(k_d/k) \hookrightarrow Aut(cov(C/\mathbb{P}^1)) \simeq GL_n(\mathbb{F}_2) \tag{10}$$

The representation of σ for given n, d has the following form in general. (We use the same notation for σ and its representation in the rest of this paper):

$$\sigma = \begin{pmatrix} \Delta_1 & O & \cdots & O \\ O & \Delta_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \Delta_s \end{pmatrix} \begin{matrix} \}n_1 \\ \}n_2 \\ \\ \}n_s \end{matrix}, \quad n = \sum_{i=1}^{s} n_i \tag{11}$$

where O stands for the zero matrix. The indecomposable subrepresentations

$$\Delta_i := \begin{pmatrix} \Omega_i & \Omega_i & \hat{O} & \cdots \\ \hat{O} & \Omega_i & \ddots & \ddots \\ \vdots & \ddots & \ddots & \Omega_i \\ \hat{O} & \cdots & \hat{O} & \Omega_i \end{pmatrix} \begin{matrix} \}n_i/l_i \\ \}n_i/l_i \\ \vdots \\ \}n_i/l_i \end{matrix} \tag{12}$$

is an $n_i \times n_i$ matrix which has a form of an $l_i \times l_i$ block matrix. The sub-block Ω_i is an $n_i/l_i \times n_i/l_i$ matrix and $\hat{O}$ also the zero matrix. Here, we denote the characteristic polynomial of Ω_i as $f_i(x)$, the characteristic polynomial of Δ_i is $F_i(x) := f_i(x)^{l_i}$, $F(x) := LCM\{F_i(x)\}$ is the minimal polynomial of σ. Denoting $d_i :=$ord(Δ_i), one has $d = LCM\{d_i\}$.

Now define the minimal polynomial of σ as $F(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x]$. Then $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$. The Galois action of $Gal(k_d/k)$ on y induces

$$^{\sigma^n}y \equiv \prod_{j=0}^{n-1} \left({}^{\sigma^j}y\right)^{a_j} \quad \mod k_d(x)^\times.$$

Therefore

$$^{\sigma^n}y^2 \equiv \prod_{j=0}^{n-1} \left({}^{\sigma^j}y^2\right)^{a_j} \quad \mod \left(k_d(x)^\times\right)^2.$$

As a result, we obtain the following necessary and sufficient condition for existence of a model of C over k_d given n, d, σ :

Indeed, C has a model over k_d if and only if

$$\begin{aligned} {}^{F(\sigma)}y^2 &\equiv 1 \mod (k_d(x)^\times)^2 \quad \text{and} \\ {}^{G(\sigma)}y^2 &\not\equiv 1 \mod (k_d(x)^\times)^2 \text{ for } {}^\forall G(x) \mid F(x), G(x) \neq F(x). \end{aligned} \tag{13}$$

4 Classification of C_0/k_d with covering C/k

Below, we show that, under the isogeny condition, the following combinations of n and d are all possible cases for genus $1, 2, 3$ hyperelliptic curves C_0/k_d with $(2, .., 2)$ covering C/k therefore subjected to the GHS attacks.

g_0	(n,d)
1	$(2,2),(2,3),(3,3),(3,7),(4,5)$
2	$(2,2),(2,3)$
3	$(2,2),(2,3),(3,7),(4,15)$

Hereafter, let S be the set of the ramification points in $\mathbb{P}^1$ of the covering $C/\mathbb{P}^1$. Then according to Riemann-Hurwitz genus formula,

$$2g(C)-2 \quad = \quad 2^n(0-2)+\#S\cdot 2^{n-1}(2-1)\cdot 1. \tag{14}$$

Here ramification indices equal 2, and the number of fibres on C over a ramification point on $\mathbb{P}^1$ is 2^{n-1}, since the ramification group is cyclic for $\gcd(char(k),2)=1$.

Therefore,

$$\#S=\frac{2g(C)-2+2^{n+1}}{2^{n-1}}=4+\frac{d\cdot g_0-1}{2^{n-2}}. \tag{15}$$

The coverings can be classified to the following four cases.

4.1 The case when σ is indecomposable

We will treat the cases when d is even and odd separately.

4.1.1 When d is even

Assume $d=2^r\cdot d'$ $(2\nmid d')$. Representation of an indecomposable σ is in the form of the following block matrix:

$$\sigma=\left.\begin{pmatrix}\Omega & \Omega & \hat{O} & \cdots\\ \hat{O} & \Omega & \ddots & \ddots\\ \vdots & \ddots & \ddots & \Omega\\ \hat{O} & \cdots & \hat{O} & \Omega\end{pmatrix}\right\} n \tag{16}$$

Here $n=l\cdot m$, Ω is in $M_m(\mathbb{F}_2)$ such that $\Omega^{d'}=I$, and

$$\sigma^{2^r}=\begin{array}{cc}\begin{pmatrix}\tilde{\Omega} & \hat{O} & \hat{O} & \cdots\\ \hat{O} & \tilde{\Omega} & \ddots & \ddots\\ \vdots & \ddots & \ddots & \hat{O}\\ \hat{O} & \cdots & \hat{O} & \tilde{\Omega}\end{pmatrix} & \begin{matrix}1\\ \\ \vdots\\ \\ l\end{matrix}\end{array},\sigma^d=(\sigma^{2^r})^{d'}=\begin{pmatrix}I & \hat{O} & \hat{O} & \cdots\\ \hat{O} & I & \ddots & \ddots\\ \vdots & \ddots & \ddots & \hat{O}\\ \hat{O} & \cdots & \hat{O} & I\end{pmatrix}. \tag{17}$$

Then, we have $2^{r-1}<l\leq 2^r$ and $\Omega\in M_m(\mathbb{F}_2)$, $\Omega\notin M_{m'}(\mathbb{F}_2)$ for $1\leq {}^\forall m'\leq m-1$. Since the minimal polynomial of Ω is in the form of $x^m+\tilde{a}_{m-1}x^{m-1}+\cdots+\tilde{a}_1x+\tilde{a}_0$, we have

$$d'|(2^m-1),\ d'\nmid(2^{m'}-1), 1\leq m'\leq m-1. \tag{18}$$

As we shown in the previous section, the number of the ramification points of $C/\mathbb{P}^1$ is $\#S = 4 + \frac{d \cdot g_0 - 1}{2^{n-2}}$. The numerator $d \cdot g_0 - 1$ of the fraction part in $\#S$ is odd since d is even. Then the denominator 2^{n-2} must be 1 since $\#S \in \mathbb{N}$. Therefore $n = 2$.

Now from $n = 2$, $l > 1$, one has $m = 1, l = n = 2$, By (18), $d' = 1$, $d = 2^r$. Since $2^{r-1} < 2 \leq 2^r = d$, $r = 1$, therefore $d = 2$. Thus we know that $(d, n) = (2, 2)$ is the only possibility.

In fact, the general form of σ only appear in cases when the isogeny condition does not hold, which will be reported elsewhere.

4.1.2 When d is odd

(a) $d = 2^n - 1$
By the Riemann-Hurwitz genus formula, $2dg_0 - 2 = 2^n(-2) + 2^{n-1} \cdot \#S$. Therefore

$$\#S = \frac{2d(g_0+1)}{2^{n-1}} = \frac{d(g_0+1)}{2^{n-2}}. \tag{19}$$

Now, since d is odd, there exists a natural number $t \in \mathbb{N}$ such that $g_0 + 1 = t \cdot 2^{n-2}$. Then $\#S = d \cdot t$. Below we consider cases with different g_0:

- $g_0 = 1$
  In this case, $t = \frac{2}{2^{n-2}} \in \mathbb{N}$. It is obvious that only $n = 2, 3$ are possible. Therefore we have $(n, d) = (2, 3), (3, 7)$ since $d = 2^n - 1$.

- $g_0 = 2$
  In the similar manner, $t = \frac{3}{2^{n-2}} \in \mathbb{N}$ therefore $(n, d) = (2, 3)$.

- $g_0 = 3$
  $t = \frac{4}{2^{n-2}} \in \mathbb{N}$ therefore $(n, d) = (2, 3), (3, 7), (4, 15)$.

In the above cases, the representations of σ are $n \times n$ matrices whose orders are d. Then we have the following minimal polynomial $F(x)$ as a degree n irreducible factor of $x^d + 1$ for each σ:

- $(n, d) = (2, 3)$
  Since $x^3 + 1 = (x+1)(x^2+x+1)$, we obtain $F(x) = x^2 + x + 1$.

- $(n, d) = (3, 7)$
  $F(x) = x^3 + x + 1$ or $F(x) = x^3 + x^2 + 1$ since $x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

- $(n, d) = (4, 15)$
  $F(x) = x^4 + x + 1$ or $F(x) = x^4 + x^3 + 1$ since $x^{15} + 1 = (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$.

(b) $d \neq 2^n - 1$
For given n and d, we know that

$$\sigma \in M_n(\mathbb{F}_2),\ \sigma \notin M_l(\mathbb{F}_2) \text{ for } \ 1 \leq {}^{\forall} l \leq n-1. \tag{20}$$

Since $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$, we have

$$d|(2^n - 1),\ d \nmid (2^l - 1). \tag{21}$$

Then $3d \leq 2^n - 1$. Obviously, $n \geq 4$. From the Riemann-Hurwitz formula,

$$\#S = 4 + \frac{dg_0 - 1}{2^{n-2}}. \tag{22}$$

Therefore, g_0 is odd, which means that $g_0 = 1$ or 3. On the one hand, we have

$$\begin{aligned} \#S = 4 + \frac{dg_0 - 1}{2^{n-2}} &\geq 2g_0 + 3 & (23)\\ dg_0 - 1 &\geq 2^{n-1}(2g_0 - 1) & (24)\\ 2^{n-2} - 1 &\geq 2^{n-1}g_0 - dg_0 = (2^{n-1} - d)g_0. & (25) \end{aligned}$$

From now, we consider $g_0 = 1$ and $g_0 = 3$:

- $g_0 = 1$
  Since $\#S = 4 + \frac{d-1}{2^{n-2}} \in \mathbb{N}$, there exists a natural number $t \in \mathbb{N}$ such that $d = 1 + 2^{n-2}t$. We have already known that $2^n - 1 \geq 3d$, which does not hold if $t \geq 2$. Therefore, only $t = 1$ is possible. Now, as $d|(2^n - 1)$, we have

  $$d = (1 + 2^{n-2})|(2^n - 1). \tag{26}$$

  Then $d \mid \left\{4(2^{n-2} + 1) - 5\right\}$ since $2^n - 1 = 4(2^{n-2} + 1) - 5$. Therefore, $(n, d) = (4, 5)$ is the only possibility. In this case, σ is a 4×4 matrix whose order is 5 and the minimal polynomial $F(x)$ is $x^4+x^3+x^2+x+1$.

- $g_0 = 3$
  We have $2^{n-2} - 1 \geq (2^{n-1} - d)3 = 3 \cdot 2^{n-1} - 3d$.
  Furthermore,

  $$3d \geq 3 \cdot 2^{n-2} - 2^{n-2} + 1 = 2^n + 2^{n-2} + 1, \tag{27}$$

  which is against

  $$2^n - 1 \geq 3d, \tag{28}$$

  so this case does not exist.

4.2 The case when σ is decomposable

As a $Gal(k_d/k)$-module, the representation of σ is a direct sum of indecomposable subrepresentations A_i.

$$cov(C/\mathbb{P}^1) = A_1 \oplus \cdots \oplus A_r,\ r \geq 2,\ \#A_i = 2^{n_i} \tag{29}$$

Define

$$A'_i := \bigoplus_{j \neq i} A_j. \tag{30}$$

Under the isogeny condition, we know that

$$A_j \cap {}^{\sigma^i}H = \{0\} \text{ and } A_j \not\subset {}^{\sigma^i}H \text{ for } i = 0, ..., n-1. \tag{31}$$

Therefore, it follows that

$$g(C/A_j) = 0 \text{ for } j = 1, ..., r. \tag{32}$$

A similar argument also apply to A'_i, therefore we have

$$C/A_j = C/A'_i = \mathbb{P}^1 \text{ for } i, j = 1, ..., r. \tag{33}$$

If $r \geq 3$,

$$C/(A'_i \cap A'_j) = C/(\oplus_{l \neq i,j} A_l) = \mathbb{P}^1 \text{ for } {}^{\forall} i, j. \tag{34}$$

Thus, one obtains the following covering

$$\begin{tikzcd}
 & & & C/\bigcap_{l\neq i} A'_l \arrow[dlll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drrr, dash] & & & \\
C/A'_1 \arrow[drrr, dash] & & \cdots C/A'_{i-1} \arrow[dr, dash] & & C/A'_{i+1} \cdots \arrow[dl, dash] & & C/A'_r \arrow[dlll, dash] \\
 & & & \mathbb{P}^1 & & &
\end{tikzcd}$$

Since $C/\bigcap_{l \neq i} A'_l = \mathbb{P}^1$, this implies one has a (2,..,2)-covering $\mathbb{P}^1/\mathbb{P}^1$ of degree $2^{\sum_{l \neq i} n_l}$. Now we consider $\overbrace{(2, ..., 2)}^{\nu}$-covering $\mathbb{P}^1 \longrightarrow \mathbb{P}^1$. By the Riemann-Hurwitz genus formula, when $char(k) \neq 2$, the number of the ramification points of this covering is $4 - \frac{1}{2^{\nu-2}}$. It follows that $\nu \leq 2$.

Therefore, we obtain $\sum_{l \neq i} n_l \leq 2$ for ${}^{\forall} i$. Thus, $r = 2$. Consequently, the only possibility is $n = n_1 + n_2 = 1 + 2 = 3, d = 3, g_0 = 1$ when σ is decomposable. This means that σ decomposes into a product of (1) and a 2×2 matrix whose order is 3 :

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{35}$$

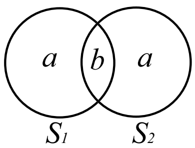
5 Defining equations of C_0/k_d for $c = 1$ or a square

Now we wish to determine the defining equations of C_0/k_d for given n, d. Hereafter, we assume that C is a model over k_d. In this section, we also assume that $c = 1$ (i.e. $c \in (k_d^\times)^2$) in (4). Then, it is sufficient to find a monic $f(x)$ in (4) such that C has a model over k_d (i.e. ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$). For $d = 2, 3$, it is possible to find $f(x)$ by using the Venn diagram to describe the sets of ramification points of ${}^{\sigma^{i-1}}C_0/\mathbb{P}^1$. In the section 6, we will treat explicit conditions for $c \in k_d^\times$ such that the curve C has a model over k, then determine the defining equations with nonsquare c.

5.1 σ : indecomposable

5.1.1 d : even

From the section 4.1.1, the only possibility here is $d = 2, n = 2$. Thus, $\#S = 2g_0 + 3$. Let S_i be the set of ramification points of ${}^{\sigma^{i-1}}C_0/\mathbb{P}^1$ for $i = 1, 2$. Then $S = S_1 \cup S_2$. For $d = 2, n = 2$, the ramification points of ${}^{\sigma^{i-1}}C_0/k_2$ for $i = 1, 2$ and C/k on $\mathbb{P}^1$ can be represented by the following Venn diagram.



Here, $b := \#(S_1 \cap S_2)$, $a := \#S_1 - b = \#S_2 - b$. As a result, we obtain the following simultaneous equations :

$$\begin{cases} a + b = 2g_0 + 2 \\ 2a + b = \#S. \end{cases} \tag{36}$$

From Riemann-Hurwitz genus formula, $\#S = 5, 7, 9$ for $g_0 = 1, 2, 3$. By solving the above simultaneous equations, one obtains $(a, b) = (1, 3), (1, 5), (1, 7)$ for $g_0 = 1, 2, 3$ respectively. Consequently, the defining equations C_0/k_2 are

$$y^2 = (x - \alpha)h(x) \tag{37}$$

where $h(x) \in k[x]$, $\alpha \in k_2 \setminus k$, $\deg h(x) = 2, \cdots, 7$.

5.1.2 d : odd

(a) $d = 2^n - 1$

In this case, all possibilities for (n, d) are $(2, 3)(3, 7)(4, 15)$ from the section 4.1.2. Recall that $F(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}_2[x]$ is the minimal polynomial of σ. Then $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$. Here, we define a homomorphism M of $k_d(x)^\times$ as

$$\begin{aligned} M : k_d(x)^\times &\longrightarrow k_d(x)^\times && (38)\\ \mu &\longmapsto \prod_{i=0}^{d-1} \left({}^{\sigma^i}\mu\right)^{b_i}. && (39)\end{aligned}$$

The sequence $\{b_i \in \mathbb{F}_2 | i = 0, \ldots, d-1\}$ is defined as follows:

$$b_0 = b_1 = \cdots = b_{n-1} = 1, \tag{40}$$

$$b_{n+j} := \sum_{i=0}^{n-1} a_{n-i} b_{n+i} \text{ for } j = 0, 1, \ldots, d-1-n. \tag{41}$$

Then one can verify that

$$^{F(\sigma)}\left\{\prod_{i=0}^{d-1} \left({}^{\sigma^i}\mu\right)^{b_i}\right\} \equiv 1 \mod \left(k_d(x)^\times\right)^2. \tag{42}$$

Consequently, we have the following defining equation of C_0/k_d. Recall that $\#S = d \cdot t$. Assume t is decomposed into $t := t_1 + t_2 + \cdots + t_r$, $\alpha_i \in k_{d \cdot t_i}$, $k_d(\alpha_i) = k_{d \cdot t_i}$, $\left\{{}^{\sigma^\iota}\alpha_i\right\}_\iota \cap \left\{{}^{\sigma^\iota}\alpha_j\right\}_\iota = \emptyset$ $(i \neq j)$. Then we have

$$f(x) = \prod_{i=1}^{r} N_{k_{d \cdot t_i}/k_d}\left(M(x-\alpha_i)\right) = \prod_{i=1}^{r} N_{k_{d \cdot t_i}/k_d}\left(\prod_{j=0}^{d-1} {}^{\sigma^j}(x-\alpha_i)^{b_j}\right). \tag{43}$$

Recall the following minimal polynomial $F(x)$ for each (n, d):

- $(n, d) = (2, 3)$: $F(x) = x^2 + x + 1$
- $(n, d) = (3, 7)$: $F(x) = x^3 + x + 1$ or $F(x) = x^3 + x^2 + 1$
- $(n, d) = (4, 15)$: $F(x) = x^4 + x + 1$ or $F(x) = x^4 + x^3 + 1$.

Then one obtains the defining equations C_0/k_3 as follows:

- $g_0 = 1, d = 3, n = 2$
  $\#S = d \cdot t = 3 \cdot 2$, $F(x) = x^2 + x + 1$
  Then we have the following two cases.

  1. $t = t_1 + t_2 = 1 + 1$
     $\alpha_1, \alpha_2 \in k_3, \{\alpha_1, \alpha_1^q, \alpha_1^{q^2}\} \cap \{\alpha_2, \alpha_2^q, \alpha_2^{q^2}\} = \emptyset$
     $f(x) = \prod_{i=0}^{2}\left({}^{\sigma^i}(x-\alpha_1)^{b_i}\right)\prod_{j=0}^{2}\left({}^{\sigma^j}(x-\alpha_2)^{b_j}\right)$
     Since $b_1 = b_2 = 1, a_0 = a_1 = a_2 = 1, b_2 = a_2 b_0 + a_1 b_1 = 0$,
     $C_0/k_3 : y^2 = (x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$

2. $t = t_1 = 2$

$\alpha_1 \in k_6, k(\alpha_1) = k_6$

$$\begin{aligned} C_0/k_3 : y^2 &= N_{k_6/k_3}\left(\prod_{i=0}^{2} {}^{\sigma^i}(x-\alpha_1)^{b_i}\right) \\ &= (x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^3})(x-\alpha_1^{q^4}) \end{aligned}$$

- $g_0 = 1, d = 7, n = 3$

  Since $\#S = d \cdot t = 7 \cdot 1 = 7$, then $t = t_1$.

  $\alpha \in k_7, k(\alpha) = k_7$

$$\begin{aligned} C_0/k_7 : y^2 &= M(x-\alpha) = \prod_{i=0}^{6} ({}^{\sigma^i}(x-\alpha))^{b_i} \\ &= \begin{cases} (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4}) & \text{if } F(x) = x^3+x+1 \\ (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^5}) & \text{if } F(x) = x^3+x^2+1 \end{cases} \end{aligned}$$

Lists of all defining equations for $g_0 = 2, 3$ are given in the table of the final section.

(b) $d \neq 2^n - 1$

Since $x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$, when $(n, d) = (4, 5)$, σ has the minimal polynomial $F(x) = x^4 + x^3 + x^2 + x + 1$. Recall that we need ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$ in order that C is a model over k_d. If this condition is satisfied, $f(x)$ has following three possibilities for $\alpha \in k_5 \setminus k$:

$$\begin{aligned} (x-\alpha)(x-\alpha^q) &\mid f(x) \quad \text{or} \\ (x-\alpha)(x-\alpha^{q^2}) &\mid f(x) \quad \text{or} \\ (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3}) &\mid f(x). \end{aligned}$$

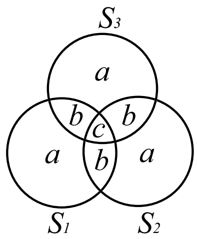
For $g_0 = 1$ and $\#S = 4 + 1 = 5$, it follows that

$$C_0/k_5 : y^2 = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3}). \tag{44}$$

5.2 σ : decomposable

Recall that there exists the only case of $g_0 = 1, n = 3, d = 3$ when σ is decomposable and $\#S$ is the number of ramification points of $C/\mathbb{P}^1$. By Riemann-Hurwitz genus formula, $\#S = 4 + \frac{dg_0 - 1}{2^{n-2}} = 5$. Let S_i be the set of ramification points of ${}^{\sigma^{i-1}}C/\mathbb{P}^1$. Then, $\#S = \#(S_1 \cup S_2 \cup S_3)$. Now, $\#S_1 = \#S_2 = \#S_3 = 2g_0 + 2 = 4$ since $g_0 = 1$. Here, we define a, b, c as follows:

$$\begin{aligned} c &:= \#(S_1 \cap S_2 \cap S_3) \\ b &:= \#(S_1 \cap S_2) - c = \#(S_2 \cap S_3) - c = \#(S_3 \cap S_1) - c \\ a &:= \#S_1 - (2b + c) = \#S_2 - (2b + c) = \#S_3 - (2b + c). \end{aligned}$$



Then we obtain the simultaneous equations as follows :

$$\begin{cases} a+2b+c = 2g_0+2 \\ 3a+3b+c = \#S. \end{cases} \tag{45}$$

In the case of $g_0 = 1, n = 3, d = 3, \#S = 5$, the solution of the equation is $a = 0, b = 1, c = 2$. Thus the defining equation is

$$C_0/k_3 : y^2 = (x-\alpha)(x-\alpha^q)h(x) \tag{46}$$

where $\alpha \in k_3 \setminus k$, $h(x) \in k[x], \deg h(x) = 2$ or 1. In fact, C is a hyperelliptic curve (see [26]). Notice that there do not exist other cases except $g_0 = 1, n = 3, d = 3$ when σ is decomposable.

6 Existence of a model of C over k and defining equations of C_0

6.1 Existential condition of a model of C over k

Finally, we discuss conditions for existence of a model of C over k. One knows that model of C over k exists if and only if the extension σ of the Frobenius automorphism $\sigma_{k_d/k}$ is an automorphism of $k_d(C)$ of order d in the separable closure of $k_d(x)$. In this section, we define $\hat{F}(x) \in \mathbb{F}_2[x]$ as the polynomial such that $x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]$.

Lemma 6.1. *In order that the curve C has a model over k, when $\hat{F}(1) = 0$, c needs to be a square: $c \in (k_d^\times)^2$. When $\hat{F}(1) = 1$, if σ does not have order d, there is a $\phi \in cov(C/\mathbb{P}^1)$ such that $\sigma\phi$ has order d so we can adopt $\sigma\phi$ instead of σ. Therefore C always has a model over k when $\hat{F}(1) = 1$.*

Proof: Let $Q := \{\frac{b(x)}{a(x)} | k_d[x] \ni a(x), b(x) : \text{monic}\}$.
Since ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$, we have

$$\begin{aligned} {}^{F(\sigma)}y^2 &\equiv {}^{F(\sigma)}c = c^{F(q)} \mod (k_d(x)^\times)^2 & (47)\\ {}^{F(\sigma)}y &\equiv \epsilon c^{\frac{F(q)}{2}} \mod Q, \qquad \text{here } \epsilon = \pm 1 & (48)\\ {}^{\hat{F}(\sigma)F(\sigma)}y &\equiv {}^{\hat{F}(\sigma)}\epsilon c^{\frac{\hat{F}(q)F(q)}{2}} & (49)\\ {}^{\sigma^d+1}y &\equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d+1}{2}} & (50)\\ {}^{\sigma^d}y &\equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d-1}{2}} y & (51) \end{aligned}$$

We first consider two possibilities of $F(1) = 1$ and $F(1) = 0$ respectively.

- Case $F(1) = 1$:

  We notice $\hat{F}(1) = 0$ in this case. Now, ${}^{\sigma^d}y \equiv c^{\frac{q^d-1}{2}}y$. In order that σ has order d (i.e. ${}^{\sigma^d}y \equiv y$), c needs to be a square $c \in (k_d^\times)^2$.

- Case $F(1) = 0$:

  Here, we consider further two possibilities of $\hat{F}(1) = 0$ and $\hat{F}(1) = 1$.
  (a) $\hat{F}(1) = 0$
  Similarly, ${}^{\sigma^d}y \equiv c^{\frac{q^d-1}{2}}y$. c should be a square element in $k_d^\times$.
  (b) $\hat{F}(1) = 1$
  Then ${}^{\sigma^d}y \equiv \epsilon c^{\frac{q^d-1}{2}}y$.
  If $\epsilon = +1$ and $c \in (k_d^\times)^2$, then σ has order d (i.e. ${}^{\sigma^d}y = y$).
  If $\epsilon = -1$ or $c \notin (k_d^\times)^2$, then σ has order $2d$.
  However, we can show that in this case there is a $\phi \in cov(C/\mathbb{P}^1)$ such that $(\sigma\phi)^d = 1$.
  Indeed, suppose $d = 2^r \cdot d'$ $(2 \nmid d')$. Since ${}^{\sigma}\phi := \sigma\phi\sigma^{-1}$, we have

$$\begin{aligned}
(\sigma\phi)^d &= \sigma\phi\sigma^{-1}\cdot\sigma^2\phi\sigma^{-2}\cdots\sigma^d\phi\sigma^{-d}\cdot\sigma^d && (52)\\
&= {}^{\sigma}\phi\ {}^{\sigma^2}\phi\cdots{}^{\sigma^d}\phi\ \sigma^d && (53)\\
&= {}^{\sigma}\phi\ {}^{\sigma^2}\phi\cdots{}^{\sigma^{2^r d'}}\phi\ \sigma^d. && (54)
\end{aligned}$$

  Now, we choose $\phi := {}^t(\overbrace{0, 0, \ldots, 1}^{m}, 0, \ldots, 0) \in cov(C/\mathbb{P}^1)$. Define

$$I \text{ as the identity matrix, } J := \left.\begin{pmatrix} 0 & 1 & & O \\ \vdots & \ddots & \ddots & \\ \vdots & O & \ddots & 1 \\ 0 & \cdots & \cdots & 0 \end{pmatrix}\right\} m \le 2^r .$$

  Then $J^m = O$. We notice that the representation of σ is

$$\begin{pmatrix} \Delta & O \\ O & * \end{pmatrix} \text{ where } \Delta := I + J. \qquad (55)$$

  Here, ${}^{\sigma^i}\phi$ corresponds to $(I+J)^i \cdot {}^t(\overbrace{0, \ldots 0, 1}^{m})$. Now, since ${}^{\sigma^{2^r}}\phi = \phi$, $(\sigma\phi)^d = (\phi\ {}^{\sigma}\phi\ {}^{\sigma^2}\phi\cdots{}^{\sigma^{2^r-1}}\phi)^{d'}\ \sigma^d$. Furthermore, since

$$I+(I+J)+\cdots+(I+J)^{2^r-1} = \begin{cases} O & \text{if } m < 2^r \\ \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix} & \text{if } m = 2^r, \end{cases} \qquad (56)$$

where O is the zero matrix, it follows that

$$\phi\ {}^{\sigma}\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r-1}}\phi = \begin{cases} {}^{t}(0,0,\ldots,0) & \text{if } m < 2^r \\ \psi := {}^{t}(1,0,\ldots,0) & \text{if } m = 2^r. \end{cases} \tag{57}$$

On the one hand, define K as the Galois closure of $k_d(C_0)/k(x)$, σ^d is an element in the center of $Gal(K/k(x))$, i.e., $\sigma^d \in Z(Gal(K/k(x))) = \{1, \psi\}$. When $\mathrm{ord}(\sigma) = 2d$, $\sigma^d = \psi$. Furthermore, notice that $m = 2^r$ in the case of (b). Thus, in the multiplicative notation,

$$(\sigma\phi)^d = (\phi\ {}^{\sigma}\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r-1}}\phi)^{d'}\ \sigma^d = \psi^{d'} \cdot \psi = 1 \tag{58}$$

As a result, we can adopt the above $\sigma\phi$ instead of σ.

$\square$

Consequently, we can determine defining equations of all classes of $C_0/k_d : y^2 = c \cdot f(x)$ whose covering curves C has a model over k under the isogeny condition. When $\hat{F}(1) = 0$, c has to be a square in k_d or can be regarded as 1, which has been treated in previous section.

6.2 Defining equations of C_0 with nonsquare c

In this section, we will treat only the defining equations of C_0 with nonsquare c . The defining equations of all classes of C_0/k_d can be found in the table in the section 7.

6.2.1 σ : indecomposable

• $g_0 = 1, n = 2, d = 2$
Here, $x^2 + 1 = (x+1)^2$, thus $F(x) = (x+1)^2, \hat{F}(x) = 1$.
Since $\hat{F}(x) = 1$, $\hat{F}(1) = 1$. From Lemma 6.1, c can be arbitrary elements in $k_2^\times$ in order that the curve C has a model over k. Extending the result of the section 5, we obtain

$$C_0/k_2 : y^2 = \eta(x - \alpha)h(x) \tag{59}$$

where $h(x) \in k[x]$, $\alpha \in k_2 \setminus k$, $\deg h(x) = 3$ or 2, $\eta =$ either 1 for a square or a non-square element in k_2.

In the same manner, we can determine c also for $g_0 = 2, 3$ as follows.
• $g_0 = 2, n = 2, d = 2$

$$C_0/k_2 : y^2 = \eta(x - \alpha)h(x) \tag{60}$$

where $h(x) \in k[x]$, $\alpha \in k_2 \setminus k$, $\deg h(x) = 5$ or 4, $\eta =$ either 1 for a square or a non-square element in k_2.
• $g_0 = 3, n = 2, d = 2$

$$C_0/k_2 : y^2 = \eta(x - \alpha)h(x) \tag{61}$$

where $\deg h(x) = 7$ or 6.

Thus the curves (59)(60)(61) contain (37) as a subcase.

6.2.2 σ : decomposable

Here, there exists only the case of $g_0 = 1, n = 3, d = 3$. Since $x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^3 + 1, \hat{F}(x) = 1$, then $\hat{F}(1) = 1$. Therefore c is either 1 or a non-square element in k_3. Then we obtain the defining equation of C_0/k_3 as

$$C_0/k_3 : y^2 = \eta(x - \alpha)(x - \alpha^q)h(x) \tag{62}$$

where $\eta =$ either 1 or a non-square element in k_3, $\alpha \in k_3 \setminus k$, $h(x) \in k[x], \deg h(x) = 2$ or 1. Notice that the curves (62) extends the class of (46).

7 A complete list of C_0/k_d with (2,...,2)-covering C/k

Curves in the following list are all classes of hyperelliptic curves C_0/k_d for $g(C_0) \in \{1, 2, 3\}$ which possess $(2, ..., 2)$ covering C/k of $\mathbb{P}^1$ under the isogeny condition. Here, $C_0/k_d : y^2 = c \cdot h_d(x)h(x)$, $h_d(x) \in k_d[x] \setminus k_u[x]$, $u||d$, $h(x) \in k[x]$, $\alpha \in k_d \setminus k_v, v||d$ (here $a||b$ means $a|b$ and $a \neq b$), $\eta =$ either 1 or a non-square element in k_d.

$C_0/k_d : y^2 = c \cdot h_d(x)h(x)$

g_0	n, d	c	$h_d(x)$	$\deg(h(x))$
1	$2, 2$	η	$x - \alpha$	3 or 2
	$2, 3$	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$ Either $\alpha_1, \alpha_2 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}$ C:Hyper $\iff {}^{\exists}A \in GL_2(k), \alpha_2 = A \cdot \alpha_1, Tr(A) = 0$ [26]	0
	$3, 3$	η	$(x-\alpha)(x-\alpha^q)$	2 or 1
	$4, 5$	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$	0
	$3, 7$	1	(1) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$ (2) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^5})$	0
2	$2, 2$	η	$x - \alpha$	5 or 4
	$2, 3$	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$ Either $\alpha_1, \alpha_2, \alpha_3 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3 \in k_3 \setminus k$ or $\alpha_1 \in k_9 \setminus k_3, \alpha_2 = \alpha_1^{q^3}, \alpha 3 = \alpha_1^{q^6}$	0
3	$2, 2$	η	$x - \alpha$	7 or 6
	$2, 3$	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$ $\times(x-\alpha_4)(x-\alpha_4^q)$ Either $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3, \alpha_4 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3 \in k_6 \setminus (k_2 \cup k_3), \alpha_4 = \alpha_3^{q^3}$ or $\alpha_1 \in k_9 \setminus k_3, \alpha_2 = \alpha_1^{q^3}, \alpha_3 = \alpha_1^{q^6}, \alpha_4 \in k_3 \setminus k$ or $\alpha_1 \in k_{12} \setminus (k_6 \cup k_4), \alpha_2 = \alpha_1^{q^3}, \alpha_3 = \alpha_1^{q^6}, \alpha_4 = \alpha_1^{q^9}$	0
	$3, 7$	1	(1) $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^2})(x-\alpha_1^{q^4})$ $\times(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^2})(x-\alpha_2^{q^4})$ (2) $(x-\alpha_1)(x-\alpha_1^{q^2})(x-\alpha_1^{q^3})(x-\alpha_1^{q^4})$ $\times(x-\alpha_2)(x-\alpha_2^{q^2})(x-\alpha_2^{q^3})(x-\alpha_2^{q^4})$ Either $\alpha_1, \alpha_2 \in k_7 \setminus k$ or $\alpha_1 \in k_{14} \setminus (k_2 \cup k_7), \alpha_2 = \alpha_1^{q^7}$	0
	$4, 15$	1	(1) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$ $\times(x-\alpha^{q^7})(x-\alpha^{q^{10}})(x-\alpha^{q^{11}})(x-\alpha^{q^{13}})$ (2) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$ $\times(x-\alpha^{q^5})(x-\alpha^{q^7})(x-\alpha^{q^8})(x-\alpha^{q^{11}})$ $\alpha \in k_{15} \setminus (k_3 \cup k_5)$	0

References

[1] L. Adleman, J. DeMarrais, and M. Huang, "A subexponential 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] J. Chao, "Elliptic and hyperelliptic curves with weak coverings against Weil descent attack," Talk at the 11th Elliptic Curve Cryptography Workshop, 2007.

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

[4] C. Diem, "Index calculus in class groups of plane curves of small degree," an extensive preprint from ANTS VII, 2005. Available from http://www.math.uni-leipzig.de/ diem/preprints/small-degree.ps

[5] C. Diem, "A study on theoretical and practical aspects of Weil-restrictions of varieties," dissertation, 2001.

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

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

[8] G. Fujisaki, "Fields and Galois theory," Iwanami, 1991, in Japanese.

[9] S. Galbraith, "Weil descent of jacobians," Discrete Applied Mathematics, 128 no.1, pp.165–180, 2003.

[10] P. Gaudry, "An algorithm for solving the discrete logarithm problem on hyperelliptic curves," Advances is Cryptology-EUROCRYPTO 2000, Springer-Verlag, LNCS 1807, pp.19–34, 2000.

[11] P. Gaudry, "Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem," J. Symbolic Computation, vol.44,12, pp.1690–1702, 2009.

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

[13] P. Gaudry, N. Thériault, E. Thomé, and C. Diem, "A double large prime variation for small genus hyperelliptic index calculus," Math. Comp. 76, pp.475–492, 2007.

[14] N. Hashizume, F. Momose and J. Chao "On implementation of GHS attack against elliptic curve cryptosystems over cubic extension fields of odd characteristics ," preprint, 2008. Available from http://eprint.iacr.org/2008/215

[15] F. Hess, "The GHS attack revisited," Advances in Cryptology-EUROCRYPTO 2003, Springer-Verlag, LNCS 2656, pp.374–387, 2003.

[16] F. Hess, "Generalizing the GHS attack on the elliptic curve discrete logarithm," LMS J. Comput. Math.7 , pp.167–192, 2004.

[17] T. Iijima, M. Shimura, J. Chao, and S. Tsujii, "An extension of GHS Weil descent attack," IEICE Trans. Vol.E88-A, no.1,pp97–104 ,2005.

[18] T. Iijima, F. Momose, and J. Chao "On certain classes of elliptic/hyperelliptic curves with weak coverings against GHS attack," Proc. of SCIS2008, IEICE Japan, 2008.

[19] T. Iijima, F. Momose, and J. Chao "Classification of Weil restrictions obtained by $(2, \ldots, 2)$ coverings of $\mathbb{P}^1$ without isogeny condition in small genus cases," Proc. of SCIS2009, IEICE Japan, 2009.

[20] T. Iijima, F. Momose, and J. Chao "Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack without isogeny condition," Proc. of SCIS2010, IEICE Japan, 2010.

[21] T. Iijima, F. Momose, and J. Chao "Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack without isogeny condition," preprint, 2009. Available from http://eprint.iacr.org/2009/613.

[22] S. Lang, "Algebra (Revised Third Edition)," Graduate Text in Mathematics, no.211, Springer-Verlag, 2002.

[23] 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.

[24] F. Momose and J. Chao "Classification of Weil restrictions obtained by $(2, \ldots, 2)$ coverings of $\mathbb{P}^1$," preprint, 2006. Available from http://eprint.iacr.org/2006/347

[25] F. Momose and J. Chao "Scholten forms and elliptic/hyperelliptic curves with weak Weil restrictions," preprint, 2005. Available from http://eprint.iacr.org/2005/277

[26] F. Momose and J. Chao "Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristics," J. Ramanujan Math.Soc, 28 no.3, pp.299–357, 2013.

[27] K. Nagao, "Improvement of Thériault algorithm of index calculus for jacobian of hyperelliptic curves of small genus," preprint, 2004. Available from http://eprint.iacr.org/2004/161

[28] M. Shimura, F. Momose, and J. Chao "Elliptic curves with weak coverings over cubic extensions of finite fields with even characteristic," Proc. of SCIS2010, IEICE Japan, 2010.

[29] M. Shimura, F. Momose, and J. Chao "Elliptic curves with weak coverings over cubic extensions of finite fields with even characteristic II," Proc. of SCIS2011, IEICE Japan, 2011.

[30] H. Stichtenoth, "Algebraic function fields and codes," Universitext, Springer-Verlag, 1993.

[31] N.Thériault, "Weil descent attack for Kummer extensions," J. Ramanujan Math. Soc, 18, pp.281–312, 2003.

[32] N.Thériault, "Weil descent attack for Artin-Schreier curves," preprint, 2003. Available from http://homepage.mac.com/ntheriau/weildescent.pdf

[33] N.Thériault, "Index calculus attack for hyperelliptic curves of small genus," Advances in Cryptology-ASIACRYPT 2003, LNCS 2894, pp.75–92, 2003