Classification of Elliptic/hyperelliptic Curves with Weak Coverings against GHS Attack without Isogeny Condition

Tsutomu Iijima * Fumiyuki Momose † Jinhui Chao ‡

2013/11/22

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. Recently, classification and density analysis were shown for all elliptic curves and hyperelliptic curves C_0/k_d of genus 2, 3 which possess $(2,\ldots,2)$ covering C/k of $\mathbb{P}^1$, therefore subjected to GHS attack, under the isogeny condition (i.e. when $g(C) = d \cdot g(C_0)$). In this paper, we first show a general classification procedure for the odd characteristic case. Our main approach is to use representation of the extension of $Gal(k_d/k)$ acting on $cov(C/\mathbb{P}^1)$. Then a classification of small genus hyperelliptic curves C_0/k_d which possesses $(2,..,2)$ covering C over k is presented without the isogeny condition. As a result, explicit defining equations of such curves C_0/k_d whose covering curves C have a model over k are presented.

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

1 Introduction

Let $k_d := \mathbb{F}_{q^d}, k := \mathbb{F}_q$ $(d > 1)$, q be a power of a prime number.

Weil descent was firstly introduced by Frey [7] to elliptic curve cryptosystems. This idea is developed into the well-known GHS attack in [11].

*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

The first manuscript was uploaded to the cryptology e-print archive on December 10, 2009.

This attack maps the discrete logarithm problem (DLP) in the Jacobian of a curve C_0 defined over the d degree extension field k_d of the finite field k to the DLP in the Jacobian of a curve C over k by a conorm-norm map. The GHS attack is further extended and analyzed by many researchers and is conceptually generalized to the cover attack [5]. The cover attack maps the DLP in the Jacobian of a curve C_0/k_d to the DLP in the Jacobian of a covering curve C/k of C_0 when a covering map or a non-constant morphism between C_0 and C exists.

If the DLP in the Jacobian of C_0 can be solved more efficiently in the Jacobian of C, we call C_0 a weak curve or say that it has weak covering C against GHS or cover attack. Thus, it is important and interesting to know what kind of curves C_0 have such coverings C, how many are they, etc..

It is known that the most efficient attack to DLP in the Jacobian of algebraic curve based systems is the index calculus algorithms. In [9], Gaudry first proposed his variant of the Adleman-DeMarrais-Huang algorithm [1] to attack hyperelliptic curve discrete logarithm problems, which is faster than Pollard's rho algorithm when the genus is larger than 4 but becomes impractical for large genera. Recently, a single-large-prime variation [26] and a double-large-prime variation [12][22] are proposed. These variations can be applied in the GHS attack if the curve C/k is a hyperelliptic curve of $g(C) \geq 3$. The complexity of these double-large-prime algorithms are $\tilde{O}(q^{2-2/g})$. On the other hand, when C/k is a non-hyperelliptic curve, Diem's recent proposal of a double-large-prime variation [4] can be applied with complexity of $\tilde{O}(q^{2-2/(g-1)})$. Besides, Gaudry showed a general algorithm solving discrete logarithms on Abelian varieties of dimension n' in running time $\tilde{O}(q^{2-2/n'})$ when q grows to infinity [10]. In particular, for elliptic curves over cubic extension field k_3, the running time is $\tilde{O}(q^{4/3})$.

Recently, security analyses of elliptic and hyperelliptic curves C_0/k_d with weak covering C/k were shown under the following isogeny condition [2][17][19][20][21][23][24]. Assume that there exists a covering curve C/k of C_0/k_d and

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

such that for

$$\begin{aligned} \pi_* \quad &: \quad J(C) \twoheadrightarrow J(C_0), & (2)\\ Res(\pi_*) \quad &: \quad J(C) \longrightarrow Res_{k_d/k} J(C_0) & (3) \end{aligned}$$

defines an isogeny over k, here $J(C)$ is the Jacobian variety of C and $Res_{k_d/k} J(C_0)$ is its Weil restriction. Then $g(C) = d \cdot g(C_0)$. Under this condition, the curves C_0/k_d which possess covering curves C/k as $(2, \ldots, 2)$ covering of $\mathbb{P}^1$ are already classified for hyperelliptic curves of genus 1,2,3 [17][19][20][21]. Here, classification means to give a complete list of all such weak curves C_0. In particular, defining equations are presented for these curves. Densities of the weak curves are also obtained for certain cases.

In this paper, we give a general classification procedure of hyperelliptic curves C_0 with $(2,\ldots,2)$ covering C/k for the odd characteristic case. By applying this procedure, we obtain a classification of weak hyperelliptic curves $C_0/k_d : y^2 = c \cdot f(x)$ of genus 1,2,3 without isogeny condition (i.e. $g(C) = d \cdot g(C_0) + e, e > 0$). Here, e is the dimension of $\ker(Res(\pi_*))$. Our approach for the classification is a representation theoretical one, to investigate action of the extension of $Gal(k_d/k)$ on $cov(C/\mathbb{P}^1)$. As a result, we obtain a complete list of defining equations of these weak curves C_0/k_d for small values of e which is corresponding to cryptographically meaningful classes of C_0.

2 GHS attack, $(2,\ldots,2)$ covering and Galois representation

Firstly, we review briefly the GHS attack and the cover attack. Let $k_d(C_0)$ be the function field of a curve C_0/k_d, $Cl^0(k_d(C_0))$ the class group of the degree 0 divisors of $k_d(C_0)$, $\sigma_{k_d/k}$ the Frobenius automorphism of k_d over k, x the transcendental element over k_d. Unless otherwise noted, we assume $\sigma_{k_d/k}$ is extended to an automorphism σ of order d in the separable closure of $k_d(x)$. It is showed by Diem [3] that $\sigma_{k_d/k}$ can extend an automorphism of the order d when C_0 is a hyperelliptic curve and d is odd for the odd characteristic case. In [17], we extended the condition in the case of any $d > 1$ and the odd characteristic. Then, the Galois closure of $k_d(C_0)/k(x)$ is $\mathcal{F}' := k_d(C_0) \cdot \sigma(k_d(C_0)) \cdots \sigma^{d-1}(k_d(C_0))$ and the fixed field of $\mathcal{F}'$ by the automorphism σ is $\mathcal{F} := \{\zeta \in \mathcal{F}' \mid \sigma(\zeta) = \zeta\}$. The DLP in $Cl^0(k_d(C_0)) \cong J(C_0)(k_d)$ is mapped to the DLP in $Cl^0(\mathcal{F}) \cong J(C)(k)$ using the following composition of conorm and norm maps:

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

This map is called the conorm-norm homomorphism in the original GHS paper on the elliptic curve case [11].

This attack has been extended to wider classes of curves. The GHS attack is conceptually generalized to the cover attack by Frey and Diem [5]. 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.

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

In the rest of this paper, let q be a power of an odd prime. Assume C_0 is a hyperelliptic curve with $g(C_0) \in \{1, 2, 3\}$ given by

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

where $c \in k_d^{\times}$, $f(x)$ is a monic polynomial in $k_d[x]$. Then assume that we have a tower of extensions of function fields such that $k_d(x, y, {}^{\sigma^1}y, \ldots, {}^{\sigma^{n-1}}y) \simeq k_d(C)\ /k_d(x)$ $(n \leq d)$ is a $\overbrace{(2, \ldots, 2)}^{n}$ type extension. Here, a $\overbrace{(2, \ldots, 2)}^{n}$ covering is defined as a covering $\pi/k_d : C \longrightarrow \mathbb{P}^1$

$$\overbrace{C \longrightarrow \underbrace{C_0 \longrightarrow \mathbb{P}^1(x)}_{2}}^{\overbrace{(2,\ldots,2)}^{n}} \tag{5}$$

such that $cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$, here $cov(C/\mathbb{P}^1) := Gal(k_d(C)/k_d(x))$.
Furthermore, we consider the Galois group $Gal(k_d/k)$ acting on the covering group $cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$.

$$\begin{aligned} Gal(k_d/k) \times cov(C/\mathbb{P}^1) &\longrightarrow cov(C/\mathbb{P}^1) && (6)\\ (\sigma^i_{k_d/k}, \phi) &\longmapsto {}^{\sigma^i}\phi := \sigma^i \phi \sigma^{-i} && (7) \end{aligned}$$

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

$$\xi : Gal(k_d/k) \hookrightarrow Aut(cov(C/\mathbb{P}^1)) \simeq GL_n(\mathbb{F}_2) \tag{8}$$

3 Classification procedure of elliptic/hyperelliptic curves C_0 with weak coverings

From now, we give a general procedure to classify all weak curves C_0/k_d for given n, d. The procedure will output their defining equations and a complete list of such curves.

3.1 Classification of Galois representation

First of all, we classify the representation of σ. Then, the representation of σ for given n, d is (we use the same notation for σ and its representation):

$$\sigma = \begin{array}{c} \begin{pmatrix} \Delta_1 & O & \cdots & O \\ O & \Delta_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \Delta_s \end{pmatrix} \end{array} \begin{array}{l} \}n_1 \\ \\ \\ \}n_s \end{array} \tag{9}$$

is consisted of the diagonal blocks of matrices which are denoted by Δ_i's where $n = \sum_{i=1}^{s} n_i$ and the O's are zero matrices,

$$\Delta_i = \begin{array}{cc} \begin{pmatrix} \Omega_i & \Omega_i & \hat{O} & \cdots \\ \hat{O} & \Omega_i & \ddots & \ddots \\ \vdots & \ddots & \ddots & \Omega_i \\ \hat{O} & \cdots & \hat{O} & \Omega_i \end{pmatrix} & \begin{array}{c} 1 \\ \\ \vdots \\ \\ l_i \end{array} \end{array} \tag{10}$$

is an $n_i \times n_i$ matrix which has a form of an $l_i \times l_i$ block matrix. The sub-blocks Ω_i are $n_i/l_i \times n_i/l_i$ matrices and $\hat{O}$'s are $n_i/l_i \times n_i/l_i$ zero matrices. Here, if $F_i(x)$:=(the characteristic polynomial of $\Omega_i)^{l_i}$, then $F(x) := LCM\{F_i(x)\}$ is the minimal polynomial of σ. When d_i :=ord(Δ_i), $d = LCM\{d_i\}$.

Let S be the number of the ramification points of $C/\mathbb{P}^1$ covering. By the Riemann-Hurwitz theorem, $2g(C) - 2 = 2^n(-2) + 2^{n-1}S$, then $S = 4 + \frac{dg(C_0)+e-1}{2^{n-2}}$. Hereafter, we consider the following two types:

- Type (A) : $^{\exists}d_i$ s.t. $d_i = d$ $(= LCM\{d_i\})$
  then, $S = 4 + \frac{dg(C_0)+e-1}{2^{n-2}} \geq \max\{d, 2g(C_0) + 3\}$
- Type (B) : $d_i \neq d$ for $^{\forall}d_i$
  then, $S = 4 + \frac{dg(C_0)+e-1}{2^{n-2}} \geq \max\{q(d), 2g(C_0) + 4\}$

here $q(d) := \sum p_i^{e_i}$ for $d = \prod p_i^{e_i}$ (p_i's are distinct prime numbers).

The some examples for Type(A) and Type(B) are as follows:

Example 3.1. $n = 2, d = 2$

$$\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : Type(A),\ \ F(x) = (x+1)^2 = x^2 + 1. \tag{11}$$

Example 3.2. $n = 2, d = 3$

$$\sigma = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} : Type(A),\ \ F(x) = x^2 + x + 1. \tag{12}$$

Example 3.3. $n = 3, d = 3$

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} : Type(A), \tag{13}$$

$$F(x) = (x+1)(x^2 + x + 1) = x^3 + 1. \tag{14}$$

Example 3.4. $n = 3, d = 4$

$$\sigma = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} : Type(A),\ F(x) = (x+1)^3 = x^3 + x^2 + x + 1. \quad (15)$$

Example 3.5. $n = 4, d = 6$

$$\sigma = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : Type(A) \quad or \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : Type(B) \qquad (16)$$

Then, σ have the minimal polynomials as $F(x) = (x^2 + x + 1)^2$, or $F(x) = (x + 1)^2(x^2 + x + 1)$.

Remark 3.1. *See Example 3.5 again. Notice for the two cases:*

$$\begin{aligned} Type(A) : \sigma &= \begin{pmatrix} \Omega_1 & \Omega_1 \\ O & \Omega_1 \end{pmatrix}, \Omega_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ Type(B) : \sigma &= \begin{pmatrix} \Delta_1 & O \\ O & \Delta_2 \end{pmatrix}, \Delta_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \Delta_2 = \Omega_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Remark 3.2. *In the case without isogeny condition, we have to treat more variations of the representation σ which do not exist in the case under the isogeny condition. For example, Type(B) matrices do not appear under the isogeny condition for the odd characteristic case. Actually, Type(B) matrices contain Type(A) matrices as subrepresentations. Thus it is necessary for any $e \geq 0$ to classify by using a more systematical procedure than in the case under the isogeny condition [17][19][20][21].*

From now, we are considering the case of a hyperelliptic curve C_0/k_d for $g(C_0) \in \{1, 2, 3\}$ such that there is a covering $\pi/k_d : C \longrightarrow C_0$ and the covering curve C/k has genus $g(C) = d \cdot g(C_0) + e$ (Notice that the procedure in the section 3 and Lemma 3.1 are applicable to any $e \geq 0$).

3.2 Existence of a model of C over k

Recall that we consider C_0 as a hyperelliptic curve over k_d defined by $y^2 = c \cdot f(x)$ where $c \in k_d^\times$, $f(x)$ is a monic polynomial in $k_d[x]$. Denote by $F(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x]$ the minimal polynomial of

σ. Now $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$ since $F(\sigma) = 0$. Therefore

$$Gal(k_d/k) \curvearrowright \{^{\sigma^i}y\}_i \mod k_d(x)^\times \tag{17}$$

$$\Longrightarrow \quad {}^{\sigma^n}y \equiv \prod_{j=0}^{n-1} \left({}^{\sigma^j}y\right)^{a_j} \mod k_d(x)^\times \tag{18}$$

$$\Longrightarrow \quad {}^{\sigma^n}y^2 \equiv \prod_{j=0}^{n-1} \left({}^{\sigma^j}y^2\right)^{a_j} \mod \left(k_d(x)^\times\right)^2 \tag{19}$$

Here, we have the following necessary and sufficient condition for given n, d, σ :
C has a model over $k_d \Longleftrightarrow$

$$\begin{aligned} {}^{F(\sigma)}y^2 &= {}^{F(\sigma)}c \cdot {}^{F(\sigma)}f(x) = c^{F(q)} \cdot {}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2, \\ {}^{G(\sigma)}y^2 &\not\equiv 1 \mod (k_d(x)^\times)^2 \text{ for}^\forall G(x) \mid F(x), G(x) \neq F(x). \end{aligned} \tag{20}$$

Hereafter, we assume that C is a model over k_d.

Under this assumption, we introduce conditions for existence of a model of C over k. Now we know a model of C over k exists iff 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 $k_d(x)$. Diem showed in [3] that the Frobenius automorphism $\sigma_{k_d/k}$ on $k_d(x)$ is extended to an automorphism of $\mathcal{F}'/k_d(x)$ of order d when d is odd. Furthermore, we extended the condition in the case of any $d > 1$. In the following lemma, explicit conditions for c are shown in case of any $d > 1$. For the rest of this paper, define $\hat{F}(x) \in \mathbb{F}_2[x]$ as a polynomial such that $x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]$.

Lemma 3.1. *[17] 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 $\hat{F}(1) = 1$, there is a $\phi \in cov(C/\mathbb{P}^1)$ such that $\sigma\phi$ has order d if σ does not have order d, so we can adopt such $\sigma\phi$ instead of σ. Therefore C always has a model over k when $\hat{F}(1) = 1$.*

Proof: See [17]. □

Example 3.6. $n = 2, d = 2$
$x^2 + 1 = (x + 1)^2$, $F(x) = (x + 1)^2, \hat{F}(x) = 1$
Since $\hat{F}(x) = 1$, $\hat{F}(1) = 1$. Therefore, c should be 1 or a non-square element in k_2 in order that the curve C has a model over k under the assumption ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$.

Example 3.7. $n = 2, d = 3$
$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^2 + x + 1, \hat{F}(x) = x + 1$
Since $\hat{F}(x) = x+1$, $\hat{F}(1) = 0$. It follows that c is a square element $c \in (k_3^\times)^2$ (i.e. $c = 1$).

Example 3.8. $n = 3, d = 3$
$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^3 + 1, \hat{F}(x) = 1$
Since $\hat{F}(x) = 1$, $\hat{F}(1) = 1$. Similarly, we obtain that c is 1 or a non-square element in k_3.

Example 3.9. $n = 3, d = 4$
$x^4 + 1 = (x + 1)^4, F(x) = (x + 1)^3, \hat{F}(x) = x + 1$
In this case, $\hat{F}(1) = 0$. Consequently, $c \in (k_4^\times)^2$.

Example 3.10. $n = 4, d = 6$
$x^6 + 1 = (x + 1)^2(x^2 + x + 1)^2$

1. $F(x) = (x^2 + x + 1)^2, \hat{F}(x) = (x + 1)^2$
   Now, $\hat{F}(1) = 0$ since $\hat{F}(x) = x^2 + 1$. Hence c is a square element $c \in (k_6^\times)^2$.

2. $F(x) = (x + 1)^2(x^2 + x + 1), \hat{F}(x) = x^2 + x + 1$
   Then, $\hat{F}(1) = 1$. As a result, c is 1 or a non-square element in k_6.

3.3 Ramification points analysis of $C_0/\mathbb{P}^1$

Recall that the condition ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$ and $\hat{F}(x) \in \mathbb{F}_2[x]$ is a polynomial such that $x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]$. We will define the following notation as $b_i = 1$ when there exists a ramification point $(\alpha^{q^i}, 0)$ on C_0 and let $b_i = 0$ otherwise for $i = 0, \ldots, d-1$. Here, α is either in k_d ($\alpha \in k_d \setminus k_v, v \mid_{\neq} d$) or in certain extension of k_d ($\alpha \in k_{d\tau} \setminus k_v, v \mid_{\neq} d\tau, {}^\exists\tau \in \mathbb{N}_{>1}$) if $f(x)$ contains all conjugate factors of α^{q^i} over k_d. Let $\Phi(x) := b_{d-1}x^{d-1} + \cdots + b_1x + b_0$. Then $\Phi(x)$ defines a minimal Galois-invariant set of ramification points of $C_0/\mathbb{P}^1$ over k_d.

Since ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$, $F(x)\Phi(x) \equiv 0 \mod (x^d+1)$. Then, $F(x)\Phi(x) \equiv 0 \mod (x^d + 1) \Leftrightarrow \Phi(x) \equiv 0 \mod \hat{F}(x)$. Therefore, it follows that $\Phi(x) \equiv a(x)\hat{F}(x) \mod (x^d + 1)$ for given n, d (${}^\exists a(x) \in \mathbb{F}_2[x]$, $\deg a(x) < \deg F(x)$). Additionally, we can prove that $\hat{F}(x)\mathbb{F}_2[x]/(x^d+1) \cong \mathbb{F}_2[x]/(F(x))$. This suggests that we can know candidates of the ramification points of $C_0/\mathbb{P}^1$ if $a(x) \in \mathbb{F}_2[x]$ are determined for given $\hat{F}(x) \in \mathbb{F}_2[x]$. Hereafter, we assume that $\gcd(F(x), a(x)) = 1$ in order to treat $\Phi(x)$ corresponding to given $F(x)$. Next, we define the equivalence relation such that $(b_0, b_1, \ldots, b_{d-1}) \sim (b_j, \ldots, b_{d-1}, b_0, \ldots, b_{j-1})$ (i.e. the coefficients of $\Phi(x)$'s are cyclic permutation of each other), then corresponding $\Phi(x)$'s belong to the same class of C_0. Furthermore, $x^r a(x)\hat{F}(x) \equiv a(x)\hat{F}(x) \mod (x^d + 1)$ $\Leftrightarrow x^r + 1 \equiv 0 \mod F(x)$ for $1 \le r \le d$. Thus, we obtain that $r = d$. From these results, the number of the classes of C_0 is $N := \#\{(\mathbb{F}_2[x]/(F(x)))^\times\}/d$. This means that we obtain candidates of the ramification points of $C_0/\mathbb{P}^1$ if N different $\Phi(x)$'s are found so that they are not cyclic permutation of each other for given $\hat{F}(x)$. From these facts, we obtain a procedure to derive candidates of the ramification points $\{(\alpha^{q^i}, 0) | b_i = 1\}$ on C_0 for given n, d, σ.

1. Choose a polynomial $a(x) = 1$, then $\Phi(x) := \hat{F}(x)$ gives ramification points $\{(\alpha^{q^i}, 0) | b_i = 1\}$ on C_0. If $N = 1$, then this procedure is completed. If $N \geq 2$, then repeat step $2 \sim 4$ until N different $a(x)$'s are found so that the coefficients of $\Phi(x)$'s are not cyclic permutation of each other.

2. Choose another polynomial $a(x)$ such that $(a(x), F(x)) = 1$ and $\deg a(x) < \deg F(x)$ are satisfied. Next, define $\Phi(x) := a(x)\hat{F}(x)$.

3. Check whether all $\Phi(x)$'s are cyclic permutation of each other or not. If so, discard such $a(x)$. Go to step 2 again. If they are not cyclic permutation of each others, we add $\{(\alpha^{q^i}, 0) | b_i = 1\}$ defined by $\Phi(x)$ to the candidates.

4. Check whether N different $a(x)$'s are found. If yes, then this procedure is completed. Otherwise, return to step 2.

Example 3.11. $n = 2, d = 2$
$x^2 + 1 = (x+1)^2$, $F(x) = (x+1)^2, \hat{F}(x) = 1$
Now, $N = 1$. Choose $a(x) = 1$, then $\Phi(x) = a(x)\hat{F}(x) = 1$. Thus, there exists a ramification point $(\alpha, 0)$ on C_0 as a candidate.

Example 3.12. $n = 2, d = 3$
$x^3 + 1 = (x+1)(x^2+x+1), F(x) = x^2 + x + 1, \hat{F}(x) = x + 1$
Similarly, $N = 1$. Choose $a(x) = 1$, then $\Phi(x) = x + 1$. C_0 has ramification points $\{(\alpha, 0), (\alpha^q, 0)\}$ on C_0.

Example 3.13. $n = 3, d = 3$
$x^3 + 1 = (x+1)(x^2+x+1), F(x) = x^3 + 1, \hat{F}(x) = 1, N = 1$
Choose $a(x) = 1$, then $\Phi(x) = 1$. Consequently, C_0 has a ramification point $(\alpha, 0)$ on C_0.

Example 3.14. $n = 3, d = 4$
$x^4 + 1 = (x+1)^4, F(x) = (x+1)^3, \hat{F}(x) = x + 1, N = 1$
Choose $a(x) = 1$, then $\Phi(x) = x+1$. C_0 has ramification points $\{(\alpha, 0), (\alpha^q, 0)\}$ on C_0.

Example 3.15. $n = 4, d = 6$
$x^6 + 1 = (x+1)^2(x^2+x+1)^2$

1. $F(x) = (x^2+x+1)^2, \hat{F}(x) = (x+1)^2, N = 2$
Now, choose $a(x) = 1$ and $a(x) = x + 1$, then $\Phi(x) = x^2 + 1$ and $\Phi(x) = x^3 + x^2 + x + 1$. In these cases, C_0 has ramification points $\{(\alpha, 0), (\alpha^{q^2}, 0)\}$ or $\{(\alpha, 0), (\alpha^q, 0), (\alpha^{q^2}, 0), (\alpha^{q^3}, 0)\}$ as candidates.

2. $F(x) = (x+1)^2(x^2+x+1), \hat{F}(x) = x^2 + x + 1, N = 1$
Now, choose $a(x) = 1$, then $\Phi(x) = x^2 + x + 1$. In the case, C_0 has ramification points $\{(\gamma, 0), (\gamma^q, 0), (\gamma^{q^2}, 0)\}$.

3.4 Defining equations of C_0

The procedure in the section 3.3 gave us how to drive the candidates of the ramification points $\{(\alpha^{q^i}, 0)\}$ on C_0 ($\alpha \in k_d \setminus k_v, v \mid_{\neq} d$ or $\alpha \in k_{d\tau} \setminus k_v, v \mid_{\neq} d\tau, \tau \in \mathbb{N}_{>1}$ if $f(x)$ contains all conjugate factors of α^{q^i} over k_d). Below, we show main steps to find the defining equations for every weak curve C_0.

1. Calculate the number of the ramification points of $C/\mathbb{P}^1$ covering $S = 4 + \frac{dg(C_0)+e-1}{2^{n-2}}$ for given $n, d, g(C_0), e$ using Riemann-Hurwitz formula and test if σ is Type (A) or (B) as in the section 3.1.

2. Derive the candidates of the ramification points on C_0 by the procedure in the section 3.3 for all subrepresentations of σ except the trivial representation (1). If σ is a Type (B) matrix, then it consists of Type (A) matrices as sub-blocks. Therefore, we can make repeated use of the results obtained for Type (A) matrices in the section 3.3.

3. Find $f(x)$ to try all combinations of polynomials which contain all conjugate factors of $x - \alpha^{q^i}$ for each ramification point and have the right degree of genus $g(C_0)$.

4. Determine $c \in k_d^\times$ so that C has a model over k by using Lemma 3.1 in the section 3.2.

The above operations are explained in further details in the following examples.

Example 3.16. *$n = 2, d = 2, g(C_0) = 2, e = 1, g(C) = 5$, σ : Type A*
In this case, we can know that $f(x)$ has a factor $x - \alpha_i$ as in Example 3.11 ($\alpha_i \in k_2 \setminus k$ or $\alpha_i \in k_{2\tau} \setminus k_v, v \mid_{\neq} 2\tau, \tau \in \mathbb{N}_{>1}$ if $f(x)$ contains all conjugate factors of α_i over k_2). Since $S = 4 + (d \cdot g(C_0) + e - 1)/2^{n-2} = 8$, we have the following two forms as candidates of C_0/k_2:
(a) $S = \#\{\alpha_1, \alpha_1^q\} + \#\{\alpha_2, \alpha_2^q\} + 4 = 2 + 2 + 4$
$\quad C_0/k_2 : \quad y^2 = (x - \alpha_1)(x - \alpha_2)h_1(x)$.
(b) $S = \#\{\alpha_1, \alpha_1^q\} + \#\{\alpha_2, \alpha_2^q\} + \#\{\alpha_3, \alpha_3^q\} + \#\{\alpha_4, \alpha_4^q\} = 2 + 2 + 2 + 2$
$\quad C_0/k_2 : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$.
Here, $h_1(x) \in k[x]$, $\deg h_1(x) \in \{4, 3\}$, $\prod(x - \alpha_i) \in k_2[x] \backslash k[x]$. As $g(C_0) = 2$ in this case, (a) should be chosen from two forms. We remark the ramification points are $\alpha_1, \alpha_2 \in k_2 \setminus k$ or $\alpha_1 \in k_4 \setminus k_2$, $\alpha_2 := \alpha_1^{q^2}$ in consideration of conjugate factors of α_1 over k_2. Recall Example 3.6. $\hat{F}(1) = 1$ since $\hat{F}(x) = 1$. Let η be 1 or a non-square element in k_2. As a result, we obtain $C_0/k_2 : y^2 = \eta(x - \alpha_1)(x - \alpha_2)h_1(x)$. Now, $g(C) = d \cdot g(C_0) + e = 5$. Roughly, the attacking costs on $J(C/k)$ is lower than on $J(C/k_d)$ as follows:

C_0/k_d :	C/k : *hyper*	C/k : *non-hyper*
$\tilde{O}(q^{\frac{d \cdot g(C_0)}{2}}) = \tilde{O}(q^2)$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g(C_0)+e}}) = \tilde{O}(q^{8/5})$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g(C_0)+e-1}}) = \tilde{O}(q^{3/2})$

Example 3.17. $n=3, d=3, g(C_0)=2, e=3, g(C)=9$, σ *: Type A*
Now, $f(x)$ has a factor $x-\alpha$. Additionally, consider also $(n,d)=(2,3)$, then $(x-\alpha)(x-\alpha^q)|f(x)$. Since $S=4+(d\cdot g(C_0)+e-1)/2^{n-2}=8$, there exist two cases as follows:
(1) $S=3+5$
$C_0/k_3 : y^2=\eta(x-\alpha)h_1(x)$
Here, $\alpha\in k_3\setminus k, h_1(x)\in k[x]$, $\deg h_1(x)\in\{5,4\}$.
(2) $S=3+3+2$
$C_0/k_3 : y^2=\eta(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)h_1(x)$
Here, $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)\in k_3[x]\setminus k[x], h_1(x)\in k[x]$, $\deg h_1(x)\in\{2,1\}$. The ramification points are $\alpha_1,\alpha_2\in k_3\setminus k$ or $\alpha_1\in k_6\setminus(k_2\cup k_3)$, $\alpha_2:=\alpha_1^{q^3}$. Remark that $\eta:=1$ or a non-square element in k_3. The rough estimation of the attacking costs between $J(C_0/k_d)$ and $J(C/k)$ is as follows:

C_0/k_d :	C/k : *hyper*	C/k : *non-hyper*
$\tilde{O}(q^{\frac{d\cdot g(C_0)}{2}})=\tilde{O}(q^3)$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e}})=\tilde{O}(q^{16/9})$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e-1}})=\tilde{O}(q^{7/4})$

Example 3.18. $n=3, d=3, g(C_0)=2, e=1, g(C)=7$, σ *: Type A*
Similarly, we consider factors $x-\alpha$ and $(x-\alpha)(x-\alpha^q)$. Now $S=4+(d\cdot g(C_0)+e-1)/2^{n-2}=7$. Consequently, we obtain $C_0/k_3 : y^2=\eta(x-\alpha)(x-\alpha^q)h_1(x)$ when $S=3+4$. Here, $\alpha\in k_3\setminus k, h_1(x)\in k[x]$, $\deg h_1(x)\in\{4,3\}$, $\eta:=1$ or a non-square element in k_3. The rough estimation between the attacking costs is as follows:

C_0/k_d :	C/k : *hyper*	C/k : *non-hyper*
$\tilde{O}(q^{\frac{d\cdot g(C_0)}{2}})=\tilde{O}(q^3)$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e}})=\tilde{O}(q^{12/7})$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e-1}})=\tilde{O}(q^{5/3})$

Example 3.19. $n=3, d=4, g(C_0)=2, e=1, g(C)=9$, σ *: Type A*
Recall that $(x-\alpha)(x-\alpha^q)|f(x)$ ($\alpha\in k_4\setminus k_2$ or $\alpha\in k_{4\tau}\setminus k_v, v\nmid 4\tau, \tau\in\mathbb{N}_{>1}$ if $f(x)$ contains all conjugate factors of α^{q^i} over k_4) when $(n,d)=(3,4)$, and $(x-\beta)|f(x)$ ($\beta\in k_2\setminus k$ or $\beta\in k_{2\tau}\setminus k_v, v\nmid 2\tau, \tau\in\mathbb{N}_{>1}$ if $f(x)$ contains all conjugate factors of β over k_2) when $(n,d)=(2,2)$. Then, $S=4+(d\cdot g(C_0)+e-1)/2^{n-2}=8$. Since $g(C_0)=2$, we obtain $C_0/k_4 : y^2=(x-\alpha)(x-\alpha^q)h_1(x)$ when $S=4+4$. Here, $\alpha\in k_4\setminus k_2, h_1(x)\in k[x]$, $\deg h_1(x)\in\{4,3\}$. The comparison similar to the above examples is as follows:

C_0/k_d :	C/k : *hyper*	C/k : *non-hyper*
$\tilde{O}(q^{\frac{d\cdot g(C_0)}{2}})=\tilde{O}(q^4)$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e}})=\tilde{O}(q^{16/9})$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e-1}})=\tilde{O}(q^{7/4})$

Example 3.20. $n=4, d=6, g(C_0)=1, e=3, g(C)=9$, σ *: Type A*
In this case, consider the combination of $(x-\alpha)(x-\alpha^{q^2})|f(x)$ and $(x-$

$\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})|f(x)$. Now, $S = 4+(d\cdot g(C_0)+e-1)/2^{n-2} = 6$. Since $g(C_0) = 1$, we obtain $C_0/k_6 : y^2 = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$ $(\alpha \in k_6 \setminus (k_3 \cup k_2))$ when $S = 6+0$. The comparison between attacking costs is :

C_0/k_d :	C/k : *hyper*	C/k : *non-hyper*
$\tilde{O}(q^{\frac{d\cdot g(C_0)}{2}}) = \tilde{O}(q^3)$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e}}) = \tilde{O}(q^{16/9})$	$\tilde{O}(q^{2-\frac{2}{d\cdot g(C_0)+e-1}}) = \tilde{O}(q^{7/4})$

Example 3.21. *$n = 4, d = 6, g(C_0) = 1, e = 3, g(C) = 9$, σ : Type B*
We know $(x-\gamma)(x-\gamma^q)(x-\gamma^{q^2})|f(x)$ as in Example 3.15. Next, consider all proper subrepresentations of σ except the trivial representation (1). Derive candidates of the ramification points for $(n,d) = (3,3),(2,3),(2,2)$. From the results of Example 3.13, 3.12 and 3.11, they have been already obtained : $(x-\alpha)|f(x)$, $(x-\alpha)(x-\alpha^q)|f(x)$ and $(x-\beta)|f(x)$ (Here, $\alpha \in k_3 \setminus k$ or $\alpha \in k_{3\tau} \setminus k_v, v \nmid 3\tau, \tau \in \mathbb{N}_{>1}$, and $\beta \in k_2 \setminus k$ or $\beta \in k_{2\tau} \setminus k_v, v \nmid 2\tau, \tau \in \mathbb{N}_{>1}$respectively). Finally, find $f(x)$ to try all combinations of polynomials which contain all conjugate factors of the aboves to consider that C_0/k_6 have $g(C_0) = 1$ and $S = 6$. In this case, it follows that C_0/k_6 has the form $y^2 = \eta(x-\alpha)(x-\alpha^q)(x-\beta)h_1(x)$ when $S = 3+2+1$. Here, $\alpha \in k_3 \setminus k$, $\beta \in k_2 \setminus k$, $h_1(x) \in k[x]$, $\deg h_1(x) \in \{1,0\}$, $\eta := 1$ or a non-square element in k_6. The comparison between attacking costs is the same as Example 3.20.

See the lists in the section 5 for other defining equations C_0/k_d.

4 Classification of elliptic/hyperelliptic curves C_0 for crypto usage without isogeny condition

From now, we apply the procedure in the section 3 to classify C_0/k_d without isogeny condition. Here, we consider cases of a hyperelliptic curve C_0/k_d for $g(C_0) \in \{1,2,3\}$ such that there is a covering $\pi/k_d : C \longrightarrow C_0$ and the covering curve C/k has genus $g(C) = d \cdot g(C_0) + e$ $(e > 0)$.

4.1 Upper bound of e in $g(C) = dg(C_0) + e$ $(e > 0)$

Firstly, since C_0 are used in the cryptographic applications, we need to restrict C_0 to a practically meaningful class. Thus we will tentatively estimate an upper bound of e for $g(C_0) \in \{1,2,3\}$. In algebraic curve based cryptosystems, the standard key length is above 160 bits at present. This means the size of the Jacobian of C_0/k_d is

$$q^{g(C_0)d} \geq 2^{160}. \tag{21}$$

Next, we assume that the size of Jacobian of C/k is $q^{dg(C_0)+e} \leq 2^a$.

Remark 4.1. *Hereafter, we discuss within $a \leq 320$. Meanwhile, Lemma 3.1 and the procedures in the previous section can apply to also $q^{dg(C_0)+e} > 2^{320}$. The classification of these cases will be reported in the near future.*

4.1.1 Case $g(C_0) = 1$

Then, we have the following situation for $g(C_0) = 1$

$$\begin{cases} q^{d+e} \leq 2^a \\ 2^{160} \leq q^d. \end{cases} \tag{22}$$

Now, since $\frac{q^{d+e}}{q^d} \leq \frac{2^a}{2^{160}}$, $q^e \leq 2^{a-160}$. Consequently,

$$\log q^e \leq \log 2^{a-160}.$$

It follows that an upper bound of e is

$$e \leq \frac{(a-160)d}{160}. \tag{23}$$

Now, $e \leq d$ is obtained since we treat $a \leq 320$.

4.1.2 Case $g(C_0) = 2, 3$

Similarly, when $g(C_0) = 2$, assume that

$$\begin{cases} q^{2d+e} \leq 2^a \\ 2^{160} \leq q^{2d}. \end{cases} \tag{24}$$

Then $e \leq 2d$ if $a \leq 320$. When $g(C_0) = 3$, the double-large-prime algorithms have the cost of $\tilde{O}(q^{\frac{4}{3}d})$. Accordingly, the condition $q^{3d} \geq 2^{180}$ (i.e. $q^{\frac{4}{3}d} \geq 2^{80}$) should be adopted instead of $q^{3d} \geq 2^{160}$ ($q^{\frac{4}{3}d} \geq 2^{71.11\cdots}$) to keep the same security level with $g(C_0) = 1, 2$ hyperelliptic curves (the costs of attack to each DLP are $q^{\frac{d}{2}} \geq 2^{80}$ for $g(C_0) = 1$, $q^d \geq 2^{80}$ for $g(C_0) = 2$ as a key length of more than 2^{160} respectively). Thus, one can assume

$$\begin{cases} q^{3d+e} \leq 2^a \\ 2^{180} \leq q^{3d}. \end{cases} \tag{25}$$

Consequently, $e \leq \frac{7}{3}d$ when $a \leq 320$. In the next subsection, we enumerate the candidates of n, d, e, S within these bounds of e for $g(C_0) = 1, 2, 3$.

4.2 The candidates of (n, d, e, S)

4.2.1 σ : Type (A)

• Case $g(C_0) = 1$:
From the above, $d + e - 1 \geq 2^{n-2}d - 2^n$ when $g(C_0) = 1$. Since we assume $0 < e \leq d$, $2d-1 \geq d+e-1 \geq 2^{n-2}d-2^n$. Then $2^n-1 \geq (2^{n-2}-2)d$ $(n \geq 3)$. Now, if $n > 3$,

$$(n \leq)\ d \leq 4 + \frac{7}{2^{n-2} - 2}. \tag{26}$$

Consequently, it follows that $n \geq 6$ is not within the candidates. From this result and the property of σ, the candidates of 4-triple (n, d, e, S) are: $(5,5,4,5), (4,4,1,5), (4,5,4,6), (4,6,3,6), (4,7,6,7), (3,3,2,6), (3,4,1,6), (3,4,3,7), (3,7,2,8), (3,7,4,9), (3,7,6,10), (2,2,1,6), (2,2,2,7), (2,3,1,7), (2,3,2,8), (2,3,3,9)$.
• Case $g(C_0) = 2$:
Similarly, when $g(C_0) = 2$, since we assume $0 < e \leq 2d$, $4d-1 \geq 2d+e-1 \geq 2^{n-2}d - 2^n$. Then, if $n > 4$,

$$(n \leq)\ d \leq 4 + \frac{15}{2^{n-2} - 4}. \tag{27}$$

Thus the candidates of (n, d, e, S) are: $(4,4,5,7), (4,5,3,7), (4,5,7,8), (4,6,1,7), (4,6,5,8), (4,6,9,9), (4,7,3,8), (4,7,7,9), (4,7,11,10), (4,15,15,15), (4,15,19,16), (4,15,23,17), (4,15,27,18), (3,3,1,7), (3,3,3,8), (3,3,5,9), (3,4,1,8), (3,4,3,9), (3,4,5,10), (3,4,7,11), (3,7,1,11), (3,7,3,12), (3,7,5,13), (3,7,7,14), (3,7,9,15), (3,7,11,16), (3,7,13,17), (2,2,1,8), (2,2,2,9), (2,2,3,10), (2,2,4,11), (2,3,1,10), (2,3,2,11), (2,3,3,12), (2,3,4,13), (2,3,5,14), (2,3,6,15)$.
• Case $g(C_0) = 3$:
Next, if $g(C_0) = 3$ $(0 < e \leq \frac{7}{3}d)$, then

$$(5 \leq n \leq)\ d \leq 4 + \frac{61}{3(2^{n-2} - \frac{16}{3})}. \tag{28}$$

Hence possible (n, d, e, S) are: $(5,8,17,9), (4,4,9,9), (4,5,6,9), (4,5,10,10), (4,6,3,9), (4,6,7,10), (4,6,11,11), (4,7,4,10), (4,7,8,11), (4,7,12,12), (4,7,16,13), (4,15,4,16), (4,15,8,17), (4,15,12,18), (4,15,16,19), (4,15,20,20), (4,15,24,21), (4,15,28,22), (4,15,32,23), (3,3,2,9), (3,3,4,10), (3,3,6,11), (3,4,1,10), (3,4,3,11), (3,4,5,12), (3,4,7,13), (3,4,9,14), (3,7,2,15), (3,7,4,16), (3,7,6,17), (3,7,8,18), (3,7,10,19), (3,7,12,20), (3,7,14,21), (3,7,16,22), (2,2,1,10), (2,2,2,11), (2,2,3,12), (2,2,4,13), (2,3,1,13), (2,3,2,14), (2,3,3,15), (2,3,4,16), (2,3,5,17), (2,3,6,18), (2,3,7,19)$.

4.2.2 σ : Type (B)

• Case $2 \nmid d$:
Now, $d = LCM\{d_i\} \leq \prod d_i \leq \prod(2^{n_i} - 1) < 2^n$. ($d_i$ is the order of Δ_i in

(9)). Here, if $g(C_0) = 1$ $(0 < e \leq d)$, then

$$d + e - 1 \leq 2d - 1 < 2^{n+1}. \tag{29}$$

On the other hand, it follows that

$$d + e - 1 \geq 2^{n-2}(q(d) - 4) \tag{30}$$

since $S = 4 + \frac{d+e-1}{2^{n-2}} \geq q(d)$. From (29)(30), one obtains

$$2^{n+1} > 2^{n-2}(q(d) - 4). \tag{31}$$

Consequently, $12 > q(d)$. Besides, we have $20 > q(d)$ for $g(C_0) = 2$ $(0 < e \leq 2d)$ since $2^{n-2}(q(d) - 4) \leq 2d + e - 1 < 2^{n+2}$. By the similar manner, $26 > q(d)$ when $g(C_0) = 3$ $(0 < e \leq \frac{7}{3}d)$.

• Case $2 \mid d$:

In this case, $n_i = l_i m_i, d_i = 2^{r_i} d_i'$ $(2 \nmid d_i')$, then $d_i' \mid 2^{m_i} - 1$. Let $r := \max\{r_i\}$. Here, we obtain $2^{r_i - 1} + 1 \leq l_i \leq 2^{r_i}$ for $r_i \geq 1$. Accordingly, $2^{r-1} + 1 \leq l_1 \leq 2^r$ when we assume l_1 with $r_1 \geq 1$. Now, notice that

$$\Delta_i = \begin{array}{c} \begin{pmatrix} \Omega_i & \Omega_i & \hat{O} & \cdots \\ \hat{O} & \Omega_i & \ddots & \ddots \\ \vdots & \ddots & \ddots & \Omega_i \\ \hat{O} & \cdots & \hat{O} & \Omega_i \end{pmatrix} \end{array} \begin{array}{c} 1 \\ \\ \\ l_i \end{array} \qquad (\Omega_i)\ \}m_i. \tag{32}$$

Then

$$\begin{aligned} d = LCM\{2^{r_i} d_i'\} = 2^r \cdot LCM\{d_i'\} &\leq 2^r \cdot \prod d_i' && (33) \\ &\leq 2^r \cdot \prod (2^{m_i} - 1) && (34) \\ &< \begin{cases} 2^{r + \sum_{i \geq 1} m_i} & (m_1 \geq 2) \\ 2^{r + \sum_{i \geq 2} m_i} & (m_1 = 1). \end{cases} && (35) \end{aligned}$$

On the other hand, we know

$$dg(C_0) + e - 1 \geq 2^{n-2}(q(d) - 4). \tag{36}$$

Hence, if $g(C_0) = 1$ $(0 < e \leq d)$, then

$$2d - 1 \geq 2^{n-2}(q(d) - 4). \tag{37}$$

From (35) (37), we obtain

$$\begin{aligned} 2^{r + (\sum_{i \geq 1} m_i) + 1} &> 2^{n-2}(q(d) - 4) && (38) \\ 2^{3 + r + (\sum_{i \geq 1} m_i) - n} &> q(d) - 4 && (39) \\ 2^{3 + r - 2^{r-1} m_1} &> q(d) - 4 && (40) \end{aligned}$$

for $m_1 \geq 2$. Similarly, $2^{3+r-2^{r-1}-1} > q(d) - 4$ for $m_1 = 1$. Therefore, we obtain $8 > q(d)$. In the same way, we have $12 > q(d)$ and $15 > q(d)$ for $g(C_0) = 2$ and $g(C_0) = 3$ respectively.

From these upper bounds and the property of σ, we obtain a list of possible $(g(C_0), n, d, e, S)$:
$(1,4,6,3,6), (2,5,12,9,8), (2,5,12,17,9), (2,5,14,13,9), (2,5,14,21,10),$
$(2,5,21,7,10), (2,5,21,15,11), (2,5,21,23,12), (2,5,21,31,13), (2,5,21,39,14),$
$(2,4,6,5,8), (2,4,6,9,9), (3,6,21,34,10), (3,6,28,29,11), (3,6,28,45,12),$
$(3,6,28,61,13), (3,5,21,2,12), (3,5,21,10,13), (3,5,21,18,14), (3,5,21,26,15),$
$(3,5,21,34,16), (3,5,21,42,17), (3,5,14,7,10), (3,5,14,15,11), (3,5,14,23,12),$
$(3,5,14,31,13), (3,5,12,13,10), (3,5,12,21,11), (3,4,6,7,10), (3,4,6,11,11)$.

Within these lists, we construct explicitly all classes of hyperelliptic curves C_0/k_d for $g(C_0) \in \{1,2,3\}$ such that there is a covering $\pi/k_d : C \longrightarrow C_0$ and the covering curve C/k has genus $g(C) = d \cdot g(C_0) + e$ $(e > 0)$. Lists for all defining equations C_0/k_d are given in the section 5. The classification for $a > 320$ will be reported in the near future.

5 Lists of classifications

5.1 Classification for the case when σ is Type (A)

Let $h_1(x) \in k[x]$, $h_d(x) \in k_d[x] \setminus k_u[x]$ $(u \mid_{\neq} d)$, $\eta := 1$ or a non-square element in k_d, $\alpha, \gamma \in k_d \setminus k_v$ $(v \mid_{\neq} d)$, $\alpha_i \in k_{\tau_i} \setminus k_{w_i}$ $(w_i \mid_{\neq} \tau_i)$. Here, choose α_i and $\tau_i \in \{d, 2d, \cdots, max\{i\}d\}$ such that $h_d(x) \in k_d[x] \setminus k_u[x]$ $(u \mid_{\neq} d)$. Refer to the section 3 as an example of how to choose α_i and τ_i. Let $C_0/k_d : y^2 = c \cdot h_d(x)h_1(x)$.

$C_0/k_d : y^2 = c \cdot h_d(x)h_1(x)$

$(n, d, g(C_0), e, S)$	c	$h_d(x)$	$\deg h_1(x)$
$(4, 4, 1, 1, 5)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	$1, 0$
$(4, 4, 2, 5, 7)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	$3, 2$
$(4, 4, 3, 9, 9)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	$5, 4$
	η	$(x-\alpha)(x-\gamma^q)(x-\gamma^{q^2})$	$5, 4$
$(4, 5, 3, 10, 10)$	1	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)(x-\alpha_i^{q^2})(x-\alpha_i^{q^3})$	0
$(4, 6, 1, 3, 6)$	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$	0
$(4, 7, 2, 7, 9)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$2, 1$
	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$2, 1$
$(4, 7, 2, 11, 10)$	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})$	$3, 2$
	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	$3, 2$
$(4, 7, 3, 8, 11)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$4, 3$
	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$4, 3$
$(4, 7, 3, 12, 12)$	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})$	$5, 4$
	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	$5, 4$
$(3, 3, 1, 2, 6)$	η	$x-\alpha$	$3, 2$
$(3, 3, 2, 1, 7)$	η	$(x-\alpha)(x-\alpha^q)$	$4, 3$
$(3, 3, 2, 3, 8)$	η	$x-\alpha$	$5, 4$
	η	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$2, 1$
$(3, 3, 2, 5, 9)$	η	$(x-\alpha)(x-\alpha^q)(x-\gamma)$	$3, 2$
$(3, 3, 3, 2, 9)$	η	$(x-\alpha)(x-\alpha^q)$	$6, 5$
$(3, 3, 3, 4, 10)$	η	$x-\alpha$	$7, 6$
	η	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$4, 3$
$(3, 3, 3, 6, 11)$	η	$(x-\alpha)(x-\alpha^q)(x-\gamma)$	$5, 4$
	η	$\prod_{i=1}^{3}(x-\alpha_i)(x-\alpha_i^q)$	$2, 1$
$(2, 2, 1, 1, 6)$	η	$\prod_{i=1}^{2}(x-\alpha_i)$	$2, 1$
$(2, 2, 1, 2, 7)$	η	$\prod_{i=1}^{3}(x-\alpha_i)$	$1, 0$
$(2, 2, 2, 1, 8)$	η	$\prod_{i=1}^{2}(x-\alpha_i)$	$4, 3$
$(2, 2, 2, 2, 9)$	η	$\prod_{i=1}^{3}(x-\alpha_i)$	$3, 2$
$(2, 2, 2, 3, 10)$	η	$\prod_{i=1}^{4}(x-\alpha_i)$	$2, 1$
$(2, 2, 2, 4, 11)$	η	$\prod_{i=1}^{5}(x-\alpha_i)$	$1, 0$

$(n, d, g(C_0), e, S)$	c	$h_d(x)$	$\deg h_1(x)$
$(2, 2, 3, 1, 10)$	η	$\prod_{i=1}^{2}(x-\alpha_i)$	$6, 5$
$(2, 2, 3, 2, 11)$	η	$\prod_{i=1}^{3}(x-\alpha_i)$	$5, 4$
$(2, 2, 3, 3, 12)$	η	$\prod_{i=1}^{4}(x-\alpha_i)$	$4, 3$
$(2, 2, 3, 4, 13)$	η	$\prod_{i=1}^{5}(x-\alpha_i)$	$3, 2$

Let $\beta \in k_2 \setminus k$, $\beta_j \in k_{\omega_j} \setminus k_{\rho_j}$ $(\rho_j \mid_{\neq} \omega_j)$, $h_2(x) \in k_2[x] \setminus k[x]$.
Here, choose β_j and $\omega_j \in \{d, 2d, \cdots, max\{j\}d\}$ such that $h_2(x) \in k_2[x]\setminus k[x]$.
Let $C_0/k_d : y^2 = c \cdot h_d(x)h_2(x)h_1(x)$.

$(n,d,g(C_0),e,S)$	c	$h_d(x)$	$h_2(x)$	$\deg h_1(x)$
$(3,4,1,1,6)$	1	$(x-\alpha)(x-\alpha^q)$	1	$2,1$
$(3,4,1,3,7)$	1	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$1,0$
$(3,4,2,1,8)$	1	$(x-\alpha)(x-\alpha^q)$	1	$4,3$
$(3,4,2,3,9)$	1	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$3,2$
$(3,4,2,5,10)$	1	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	1	$2,1$
	1	$(x-\alpha)(x-\alpha^q)$	$\prod_{j=1}^{2}(x-\beta_i)$	$2,1$
$(3,4,2,7,11)$	1	$(x-\alpha)(x-\alpha^q)$	$\prod_{j=1}^{3}(x-\beta_i)$	$1,0$
	1	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$1,0$
$(3,4,3,1,10)$	1	$(x-\alpha)(x-\alpha^q)$	1	$6,5$
$(3,4,3,3,11)$	1	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$5,4$
$(3,4,3,5,12)$	1	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	1	$4,3$
	1	$(x-\alpha)(x-\alpha^q)$	$\prod_{j=1}^{2}(x-\beta_i)$	$4,3$
$(3,4,3,7,13)$	1	$(x-\alpha)(x-\alpha^q)$	$\prod_{j=1}^{3}(x-\beta_j)$	$3,2$
	1	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$3,2$
$(3,4,3,9,14)$	1	$(x-\alpha)(x-\alpha^q)$	$\prod_{j=1}^{4}(x-\beta_j)$	$2,1$
	1	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$\prod_{j=1}^{2}(x-\beta_j)$	$2,1$
	1	$\prod_{i=1}^{3}(x-\alpha_i)(x-\alpha_i^q)$	1	$2,1$

5.2 Classification for the case when σ is Type (B)

Here, $h_v(x) \in k_v[x] \setminus k_w[x]$ $(w \mid_{\neq} v)$, $\eta := 1$ or a non-square element in k_d.
(1) $n = 6, d = 28$, $\alpha \in k_7 \setminus k, \beta \in k_4 \setminus k_2$
$C_0/k_d : y^2 = c \cdot h_7(x)h_4(x)h_1(x)$

$(n,d,g(C_0),e,S)$	c	$h_7(x)$	$h_4(x)$	$\deg h_1(x)$
$(6,28,3,61,13)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	$2,1$
	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	$2,1$

(2) $n = 5, d = 12$, $\alpha \in k_4 \setminus k_2, \beta \in k_3 \setminus k$
$C_0/k_d : y^2 = c \cdot h_4(x)h_3(x)h_1(x)$

$(n,d,g(C_0),e,S)$	c	$h_4(x)$	$h_3(x)$	$\deg h_1(x)$
$(5,12,2,17,9)$	η	$(x-\alpha)(x-\alpha^q)$	$(x-\beta)(x-\beta^q)$	$2,1$
$(5,12,3,21,11)$	η	$(x-\alpha)(x-\alpha^q)$	$(x-\beta)(x-\beta^q)$	$4,3$

(3) $n=5, d=14,\ \alpha \in k_7 \setminus k, \beta \in k_2 \setminus k,\ \ \beta_1, \beta_2 \in k_2 \setminus k$ or $\beta_1 \in k_4 \setminus k_2$, $\beta_2 := \beta_1^{q^2},\ \ C_0/k_d : y^2 = c \cdot h_7(x)h_2(x)h_1(x)$

$(n,d,g(C_0),e,S)$	c	$h_7(x)$	$h_2(x)$	$\deg h_1(x)$
$(5,14,2,21,10)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$x-\beta$	$1,0$
	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$x-\beta$	$1,0$
$(5,14,3,23,12)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$x-\beta$	$3,2$
	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$x-\beta$	$3,2$
$(5,14,3,31,13)$	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$\prod_{i=1}^2(x-\beta_i)$	$2,1$
	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$\prod_{i=1}^2(x-\beta_i)$	$2,1$
	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})$	$x-\beta$	$4,3$
	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	$x-\beta$	$4,3$

(4) $n=5, d=21,\ \alpha \in k_7 \setminus k, \beta \in k_3 \setminus k,\ \ \beta_1, \beta_2 \in k_3 \setminus k$ or $\beta_1 \in k_6 \setminus (k_2 \cup k_3)$, $\beta_2 := \beta_1^{q^3},\ \ C_0/k_d : y^2 = c \cdot h_7(x)h_3(x)h_1(x)$

$(n,d,g(C_0),e,S)$	c	$h_7(x)$	$h_3(x)$	$\deg h_1(x)$
$(5,21,2,7,10)$	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	0
	1	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	0
$(5,21,3,2,12)$	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	$2,1$
	1	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	$2,1$
$(5,21,3,10,13)$	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$\prod_{i=1}^2(x-\beta_i)(x-\beta_i^q)$	0
	1	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$\prod_{i=1}^2(x-\beta_i)(x-\beta_i^q)$	0

(5) $n=4, d=6,\ \alpha \in k_3 \setminus k,\ \beta \in k_2 \setminus k,\ \gamma \in k_6 \setminus (k_2 \cup k_3)$, $\ \ \alpha_1, \alpha_2 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3)$, $\alpha_2 := \alpha_1^{q^3}$, $\ \beta_1, \beta_2 \in k_2 \setminus k$ or $\beta_1 \in k_4 \setminus k_2$, $\beta_2 := \beta_1^{q^2}$,
$C_0/k_d : y^2 = c \cdot h_3(x)h_2(x)h_1(x)$

$(n,d,g(C_0),e,S)$	c	$h_3(x)$	$h_2(x)$	$\deg h_1(x)$
$(4,6,1,3,6)$	η	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$1,0$
$(4,6,2,5,8)$	η	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$3,2$
$(4,6,2,9,9)$	η	$x-\alpha$	$x-\beta$	$4,3$
	η	$\prod_{i=1}^2(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$1,0$
	η	$(x-\alpha)(x-\alpha^q)$	$\prod_{j=1}^2(x-\beta_j)$	$2,1$
$(4,6,3,7,10)$	η	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$5,4$
$(4,6,3,11,11)$	η	$x-\alpha$	$x-\beta$	$6,5$
	η	$\prod_{i=1}^2(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$3,2$
	η	$(x-\alpha)(x-\alpha^q)$	$\prod_{j=1}^2(x-\beta_j)$	$4,3$

$C_0/k_d : y^2 = c \cdot h_6(x)h_1(x)$

$(n,d,g(C_0),e,S)$	c	$h_6(x)$	$\deg h_1(x)$
$(4,6,2,9,9)$	η	$(x-\gamma)(x-\gamma^q)(x-\gamma^{q^2})$	$3,2$

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, 2006. 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] 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.

[10] 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.

[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] 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.

[13] 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

[14] 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.

[15] 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.

[16] 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.

[17] T. Iijima, F. Momose and J. Chao "Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack under an isogeny condition," preprint, 2013. Available from http://eprint.iacr.org/2013/487

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

[19] 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

[20] 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

[21] 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.

[22] 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

[23] 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.

[24] 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.

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

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