

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

Tsutomu Iijima ^{*} Fumiyuki Momose [†] Jinhui Chao ^{*}

2011/12/3

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 $(2, \dots, 2)$ 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 $(2, \dots, 2)$ covering C over k is presented without the isogeny condition. Explicit defining equations of such curves C_0/k_d and existential conditions of a model of C over k are also 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]. This attack maps the discrete logarithm problem (DLP) in the Jacobian of

^{*}Department of Information and System Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

[†]Department of Mathematics, 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.

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 [25] and a double-large-prime variation [12][21] 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 $\tilde{O}(q^{2-2/n'})$ [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][18][19][20][22][23]. 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

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

$$Res(\pi_*) : J(C) \longrightarrow Res_{k_d/k} J(C_0) \tag{3}$$

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 $(2, \dots, 2)$ covering of \mathbb{P}^1 are already classified for hyperelliptic curves of genus 1,2,3 [18][19][20]. Here, classification means to give a complete list of all such weak curves C_0 . In particular, defining equations are presented for these curves. Density of the weak curves are also obtained for certain cases.

In this paper, we first discuss the existence of a model of C over k . Then we show a general classification procedure for the odd characteristic case of hyperelliptic curves $C_0/k_d : y^2 = c \cdot f(x)$ of genus 1,2,3 with $(2, \dots, 2)$ covering C/k . By applying this procedure, we obtain a classification of these weak curves C_0 without isogeny condition. Specifically, we assume that $g(C) = d \cdot g(C_0) + e, e > 0$. Here, e is the dimension of $\ker(\text{Res}(\pi_*))$. Our approach for the classification is a representation theoretical one, to investigate action of the extension of $\text{Gal}(k_d/k)$ on $\text{cov}(C/\mathbb{P}^1)$. 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 . Furthermore, representation theoretical approach gives the condition for a model of C over k explicitly.

2 GHS attack and $(2, \dots, 2)$ covering

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 d is odd for the odd characteristic case. We will extend the condition in the case of any $d > 1$ and the odd characteristic in the section 4. 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:

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

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.

$$\begin{array}{ccc} J(C)(k_d) & \xleftarrow{\pi^*} & J(C_0)(k_d) \\ N \downarrow & \swarrow N \circ \pi^* & \\ J(C)(k) & & \end{array}$$

Hereafter, 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

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

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 $k_d(x, y, \sigma^1 y, \dots, \sigma^{n-1} y) \simeq k_d(C) / k_d(x)$ ($n \leq d$) is a $\overbrace{(2, \dots, 2)}^n$ type extension. Here, a $\overbrace{(2, \dots, 2)}^n$ covering is defined as a covering $\pi/k_d : C \longrightarrow \mathbb{P}^1$

$$C \longrightarrow \underbrace{C_0 \longrightarrow \mathbb{P}^1(x)}_2 \quad (5)$$

such that $\text{cov}(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$, here $\text{cov}(C/\mathbb{P}^1) := \text{Gal}(k_d(C)/k_d(x))$.

3 Representation of $\text{Gal}(k_d/k)$ on $\text{cov}(C/\mathbb{P}^1)$

Next, we consider the Galois group $\text{Gal}(k_d/k)$ acting on the covering group $\text{cov}(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$.

$$\text{Gal}(k_d/k) \times \text{cov}(C/\mathbb{P}^1) \longrightarrow \text{cov}(C/\mathbb{P}^1) \quad (6)$$

$$(\sigma_{k_d/k}^i, \phi) \longmapsto \sigma^i \phi := \sigma^i \phi \sigma^{-i} \quad (7)$$

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

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

Thus the representation of σ for given n, d is (we use the same notation for σ and its representation):

$$\sigma = \left(\begin{array}{cccc} \boxed{\spadesuit_1} & O & \cdots & O \\ O & \boxed{\spadesuit_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \boxed{\spadesuit_s} \end{array} \right) \begin{array}{l} \} n_1 \\ \\ \\ \} n_s \end{array} \quad (9)$$

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

$$\boxed{\spadesuit_i} = \begin{pmatrix} \boxed{\star_i} & \boxed{\star_i} & \hat{O} & \cdots \\ \hat{O} & \boxed{\star_i} & \ddots & \ddots \\ \vdots & \ddots & \ddots & \boxed{\star_i} \\ \hat{O} & \cdots & \hat{O} & \boxed{\star_i} \end{pmatrix} \begin{array}{l} 1 \\ \vdots \\ l_i \end{array} \quad (10)$$

is an $n_i \times n_i$ matrix which has a form of an $l_i \times l_i$ block matrix. The sub-blocks $\boxed{\star_i}$ 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 $F_i(x) := (\text{the characteristic polynomial of } \boxed{\star_i})^{l_i}$, then $F(x) := LCM\{F_i(x)\}$ is the minimal polynomial of σ . When $d_i := \text{ord}(\boxed{\spadesuit_i})$, $d = LCM\{d_i\}$. The examples of the representation of σ for given n and d are as follows:

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

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

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

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

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

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, F(x) = (x+1)(x^2 + x + 1) = x^3 + 1. \quad (13)$$

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

$$\sigma = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, F(x) = (x+1)^3 = x^3 + x^2 + x + 1. \quad (14)$$

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

$$\sigma = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (15)$$

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

4 Existence of a model of C over k

In this paper, 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 $F(x) \in \mathbb{F}_2[x]$ the minimal polynomial of σ . Here, we have the following

necessary and sufficient condition for given n, d, σ :
 C has a model over $k_d \iff$

$$\begin{aligned} F(\sigma)y^2 &= F(\sigma)c \cdot F(\sigma)f(x) = c^{F(q)} \cdot F(\sigma)f(x) \equiv 1 \pmod{(k_d(x)^\times)^2}, \\ G(\sigma)y^2 &\not\equiv 1 \pmod{(k_d(x)^\times)^2} \text{ for } \forall G(x) \mid F(x), G(x) \neq F(x). \end{aligned} \quad (16)$$

Firstly, we show 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 for the odd characteristic case. We extend the condition in the case of any $d > 1$. In the following lemma, we show explicitly the condition for c 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 4.1. *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 $\hat{F}(1) = 1$, there is a $\phi \in \text{cov}(C/\mathbb{P}^1)$ 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: Let $M := \{\frac{b(x)}{a(x)} \mid k_d[x] \ni a(x), b(x) : \text{monic}\}$.

Since $F(\sigma)f(x) \equiv 1 \pmod{(k_d(x)^\times)^2}$, we have

$$F(\sigma)y^2 \equiv F(\sigma)c = c^{F(q)} \pmod{(k_d(x)^\times)^2} \quad (17)$$

$$F(\sigma)y \equiv \epsilon c^{\frac{F(q)}{2}} \pmod{M}, \quad \text{here } \epsilon = \pm 1 \quad (18)$$

$$\hat{F}(\sigma)F(\sigma)y \equiv \hat{F}(\sigma)\epsilon c^{\frac{\hat{F}(q)F(q)}{2}} \quad (19)$$

$$\sigma^{d+1}y \equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d+1}{2}} \quad (20)$$

$$\sigma^d y \equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d-1}{2}} y \quad (21)$$

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 $\exists \phi \in \text{cov}(C/\mathbb{P}^1)$ such that $(\sigma\phi)^d = 1$.

Suppose $d = 2^r \cdot d'$ ($2 \nmid d'$). Since ${}^\sigma\phi := \sigma\phi\sigma^{-1}$, we have

$$(\sigma\phi)^d = \sigma\phi\sigma^{-1} \cdot \sigma^2\phi\sigma^{-2} \cdots \sigma^d\phi\sigma^{-d} \cdot \sigma^d \quad (22)$$

$$= \sigma\phi \sigma^2\phi \cdots \sigma^d\phi \sigma^d \quad (23)$$

$$= \sigma\phi \sigma^2\phi \cdots \sigma^{2^r d'}\phi \sigma^d. \quad (24)$$

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

$$I \text{ as the identity matrix, } J := \left. \left(\begin{array}{cccc} 0 & 1 & & O \\ \vdots & \ddots & \ddots & \\ \vdots & O & \ddots & 1 \\ 0 & \dots & \dots & 0 \end{array} \right) \right\} m \leq 2^r.$$

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

$$\left(\begin{array}{cc} \spadesuit & O \\ O & * \end{array} \right) \text{ where } \spadesuit := I + J. \quad (25)$$

Here, $\sigma^i\phi$ corresponds to $(I + J)^i \cdot {}^t(\overbrace{0, \dots, 0}^m, 1)$. 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

$$I + (I + J) + \cdots + (I + J)^{2^r-1} = \begin{cases} O & \text{if } m < 2^r \\ \left(\begin{array}{cccc} 0 & \dots & 0 & 1 \\ 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 \end{array} \right) & \text{if } m = 2^r, \end{cases} \quad (26)$$

where O is the zero matrix, it follows that

$$\phi \sigma\phi \sigma^2\phi \cdots \sigma^{2^r-1}\phi = \begin{cases} {}^t(0, 0, \dots, 0) & \text{if } m < 2^r \\ \psi := {}^t(1, 0, \dots, 0) & \text{if } m = 2^r. \end{cases} \quad (27)$$

On the other hand, σ^d is an element in the center of $\text{Gal}(\mathcal{F}'/k(x))$, i.e., $\sigma^d \in Z(\text{Gal}(\mathcal{F}'/k(x))) = \{1, \psi\}$. When $\text{ord}(\sigma) = 2d$, $\sigma^d = \psi$. Furthermore, notice that $m = 2^r$ in the case of (b). Thus, in the multiplicative notation,

$$(\sigma\phi)^d = (\phi \sigma\phi \sigma^2\phi \cdots \sigma^{2^r-1}\phi)^{d'} \sigma^d = \psi^{d'} \cdot \psi = 1 \quad (28)$$

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

□

Example 4.1. $n = 2, d = 2$

$$x^2 + 1 = (x + 1)^2, F(x) = (x + 1)^2, \hat{F}(x) = 1$$

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 $F^{(\sigma)}f(x) \equiv 1 \pmod{(k_d(x)^\times)^2}$.

Example 4.2. $n = 2, d = 3$

$$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^2 + x + 1, \hat{F}(x) = x + 1$$

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 4.3. $n = 3, d = 3$

$$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^3 + 1, \hat{F}(x) = 1$$

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 4.4. $n = 3, d = 4$

$$x^4 + 1 = (x + 1)^4, F(x) = (x + 1)^3, \hat{F}(x) = x + 1$$

In this case, $\hat{F}(1) = 0$. Consequently, $c \in (k_4^\times)^2$.

Example 4.5. $n = 4, d = 6$

$$x^6 + 1 = (x + 1)^2(x^2 + x + 1)^2$$

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 .

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

From now, we show a 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.

5.1 Ramification points of C_0/\mathbb{P}^1

Also for the rest of this paper, we assume the condition $F^{(\sigma)}f(x) \equiv 1 \pmod{(k_d(x)^\times)^2}$. Recall that $\hat{F}(x) \in \mathbb{F}_2[x]$ 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 $i = 0, \dots, d - 1$. 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 ${}^{F(\sigma)}f(x) \equiv 1 \pmod{(k_d(x)^\times)^2}$, $F(x)\Phi(x) \equiv 0 \pmod{(x^d+1)}$. Then, $F(x)\Phi(x) \equiv 0 \pmod{(x^d+1)} \Leftrightarrow \Phi(x) \equiv 0 \pmod{\hat{F}(x)}$. Therefore, it follows that $\Phi(x) \equiv a(x)\hat{F}(x) \pmod{(x^d+1)}$ 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 $(b_0, b_1, \dots, b_{d-1}) \sim (b_j, \dots, b_{d-1}, b_0, \dots, b_{j-1})$ (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, $x^r a(x)\hat{F}(x) \equiv a(x)\hat{F}(x) \pmod{(x^d+1)} \Leftrightarrow x^r + 1 \equiv 0 \pmod{F(x)}$ for $1 \leq r \leq d$. 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 show a procedure to derive candidates of the ramification points $\{(\alpha^{q^i}, 0) \mid b_i = 1\}$ on C_0 for given n, d, σ .

1. Choose a polynomial $a(x) = 1$, then $\Phi(x) := \hat{F}(x)$ gives ramification points $\{(\alpha^{q^i}, 0) \mid b_i = 1\}$ on C_0 . If $N = 1$, then this procedure is completed. If $N \geq 2$, then repeat step 2 ~ 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 $\{(\alpha^{q^i}, 0) \mid b_i = 1\}$ 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 5.1. $n = 2, d = 2$

$$x^2 + 1 = (x + 1)^2, F(x) = (x + 1)^2, \hat{F}(x) = 1$$

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 5.2. $n = 2, d = 3$

$$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^2 + x + 1, \hat{F}(x) = x + 1$$

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 5.3. $n = 3, d = 3$

$$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^3 + 1, \hat{F}(x) = 1, N = 1$$

Choose $a(x) = 1$, then $\Phi(x) = 1$. Consequently, C_0 has a ramification point $(\alpha, 0)$ on C_0 .

Example 5.4. $n = 3, d = 4$

$$x^4 + 1 = (x + 1)^4, F(x) = (x + 1)^3, \hat{F}(x) = x + 1, N = 1$$

Choose $a(x) = 1$, then $\Phi(x) = x + 1$. C_0 has ramification points $\{(\alpha, 0), (\alpha^q, 0)\}$ on C_0 .

Example 5.5. $n = 4, d = 6$

$$x^6 + 1 = (x + 1)^2(x^2 + x + 1)^2$$

$$1. F(x) = (x^2 + x + 1)^2, \hat{F}(x) = (x + 1)^2, N = 2$$

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 $\{(\gamma, 0), (\gamma^q, 0), (\gamma^{q^2}, 0)\}$.

5.2 Defining equations of C_0

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 $\pi/k_d : C \rightarrow C_0$ and the covering curve C/k has genus $g(C) = d \cdot g(C_0) + e$ (Notice that the procedure in the section 5 and Lemma 4.1 are applicable to any $e \geq 0$). Let S be the number of fixed points of C/\mathbb{P}^1 covering. By the Riemann-Hurwitz theorem, $2g - 2 = 2^n(-2) + 2^{n-1}S$, then $S = 4 + \frac{dg_0 + e - 1}{2^{n-2}}$. Hereafter, we consider the following two types:

- Type (A) : $\exists d_i$ s.t. $d_i = d$ ($= LCM\{d_i\}$)
then, $S = 4 + \frac{dg_0 + e - 1}{2^{n-2}} \geq \max\{d, 2g_0 + 3\}$
- Type (B) : $d_i \neq d$ for $\forall d_i$
then, $S = 4 + \frac{dg_0 + e - 1}{2^{n-2}} \geq \max\{q(d), 2g_0 + 4\}$

here $q(d) := \sum p_i^{e_i}$ for $d = \prod p_i^{e_i}$ (p_i 's are distinct prime numbers). Notice that a Type(B) matrix has Type(A) matrices as subrepresentations.

Remark 5.1. See Example 3.5 again. We notice the left and right matrices are a Type (A) and a Type (B) respectively. Notice for the two cases:

$$\begin{aligned} \text{Type(A)} : \sigma &= \begin{pmatrix} \boxed{\star_1} & \boxed{\star_1} \\ O & \boxed{\star_1} \end{pmatrix}, \boxed{\star_1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \text{Type(B)} : \sigma &= \begin{pmatrix} \boxed{\spadesuit_1} & O \\ O & \boxed{\spadesuit_2} \end{pmatrix}, \boxed{\spadesuit_1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \boxed{\spadesuit_2} = \boxed{\star_2} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

The procedure in the section 5.1 showed us how to drive the candidates of the ramification points $\{(\alpha^{q^i}, 0)\}$ on C_0 ($\alpha \in k_d \setminus k_v, v \nmid d$ or $\alpha \in k_{d\tau} \setminus k_v, v \nmid d\tau, \tau \in \mathbb{N}_{>1}$ 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 fixed points of C/\mathbb{P}^1 covering $S = 4 + \frac{dg_0 + e - 1}{2^{n-2}}$ for given n, d, g_0, e using Riemann-Hurwitz formula and test if σ is Type (A) or (B).
2. If Type (A) case and σ : irreducible, go to step 3 with ramification points $\{(\alpha^{q^i}, 0) | b_i = 1\}$ on C_0 obtained by using the procedure in the section 5.1.
Otherwise, go to step 3 with ramification points obtained from all subrepresentations of σ except the trivial representation (1) by the procedure in the section 5.1. Notice that the Type (B) matrix has Type (A) matrices as sub-blocks. Therefore, we can reuse the results for Type (A) in the section 5.1.
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_0 .

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

Example 5.6. $n = 2, d = 2, g_0 = 2, e = 1, g = 5$ (Type A)

In this case, we can know that $f(x)$ has a factor $x - \alpha_i$ as in Example 5.1 ($\alpha_i \in k_2 \setminus k$ or $\alpha_i \in k_{2\tau} \setminus k_v, v \nmid 2\tau, \tau \in \mathbb{N}_{>1}$ if $f(x)$ contains all conjugate factors of α_i over k_2). Since $S = 4 + (d \cdot g_0 + e - 1)/2^{n-2} = 8$, we have the following two forms as candidates of C_0/k_2 :

$$(a) S = \#\{\alpha_1, \alpha_1^q\} + \#\{\alpha_2, \alpha_2^q\} + 4 = 2 + 2 + 4$$

$$C_0/k_2 : y^2 = (x - \alpha_1)(x - \alpha_2)h_1(x).$$

$$(b) S = \#\{\alpha_1, \alpha_1^q\} + \#\{\alpha_2, \alpha_2^q\} + \#\{\alpha_3, \alpha_3^q\} + \#\{\alpha_4, \alpha_4^q\} = 2 + 2 + 2 + 2$$

$$C_0/k_2 : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4).$$

Here, $h_1(x) \in k[x]$, $\deg h_1(x) \in \{4, 3\}$, $\prod(x - \alpha_i) \in k_2[x] \setminus k[x]$. As $g_0 = 2$ 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 4.1. $\hat{F}(1) = 1$ 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, $g = d \cdot g_0 + e = 5$. Roughly, the attacking costs on $J(C/k)$ is lower than on $J(C/k_d)$ as follows:

$C_0/k_d :$	$C/k : \text{hyper}$	$C/k : \text{non-hyper}$
$\tilde{O}(q^{\frac{d \cdot g_0}{2}}) = \tilde{O}(q^2)$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e}}) = \tilde{O}(q^{8/5})$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e - 1}}) = \tilde{O}(q^{3/2})$

Example 5.7. $n = 3, d = 3, g_0 = 2, e = 3, g = 9$ (Type A)

Now, $f(x)$ has a factor $x - \alpha$. Additionally, consider also $(n, d) = (2, 3)$ (i.e. $(x - \alpha_i)(x - \alpha_i^q) | f(x)$). Since $S = 4 + (d \cdot g_0 + e - 1)/2^{n-2} = 8$, 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:

$C_0/k_d :$	$C/k : \text{hyper}$	$C/k : \text{non-hyper}$
$\tilde{O}(q^{\frac{d \cdot g_0}{2}}) = \tilde{O}(q^3)$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e}}) = \tilde{O}(q^{16/9})$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e - 1}}) = \tilde{O}(q^{7/4})$

Example 5.8. $n = 3, d = 3, g_0 = 2, e = 1, g = 7$ (Type A)

Similarly, we consider factors $x - \alpha$ and $(x - \alpha)(x - \alpha^q)$. Now $S = 4 + (d \cdot g_0 + e - 1)/2^{n-2} = 7$. 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:

$C_0/k_d :$	$C/k : \text{hyper}$	$C/k : \text{non-hyper}$
$\tilde{O}(q^{\frac{d \cdot g_0}{2}}) = \tilde{O}(q^3)$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e}}) = \tilde{O}(q^{12/7})$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e - 1}}) = \tilde{O}(q^{5/3})$

Example 5.9. $n = 3, d = 4, g_0 = 2, e = 1, g = 9$ (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, $S = 4 + (d \cdot g_0 + e - 1)/2^{n-2} = 8$. Since $g_0 = 2$, 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:

$C_0/k_d :$	$C/k : \text{hyper}$	$C/k : \text{non-hyper}$
$\tilde{O}(q^{\frac{d \cdot g_0}{2}}) = \tilde{O}(q^4)$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e}}) = \tilde{O}(q^{16/9})$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e - 1}}) = \tilde{O}(q^{7/4})$

Example 5.10. $n = 4, d = 6, g_0 = 1, e = 3, g = 9$ (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, $S = 4 + (d \cdot g_0 + e - 1)/2^{n-2} = 6$. Since $g_0 = 1$, 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 :

$C_0/k_d :$	$C/k : \text{hyper}$	$C/k : \text{non-hyper}$
$\tilde{O}(q^{\frac{d \cdot g_0}{2}}) = \tilde{O}(q^3)$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e}}) = \tilde{O}(q^{16/9})$	$\tilde{O}(q^{2 - \frac{2}{d \cdot g_0 + e - 1}}) = \tilde{O}(q^{7/4})$

Example 5.11. $n = 4, d = 6, g_0 = 1, e = 3, g = 9$ (Type B)

We know $(x - \gamma)(x - \gamma^q)(x - \gamma^{q^2})|f(x)$ as in Example 5.5. 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 5.3, 5.2 and 5.1, 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 $g_0 = 1$ 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 5.10.

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

6 Classification of elliptic/hyperelliptic curves C_0 without isogeny condition

Here, we apply the procedure in section 5 to classify C_0/k_d . In particular, 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 $g(C) = d \cdot g(C_0) + e$ ($e > 0$).

6.1 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

$$q^{g(C_0)d} \geq 2^{160}. \quad (29)$$

Next, we assume that the size of Jacobian of C/k is $q^{dg_0+e} \leq 2^a$.

Remark 6.1. *Hereafter, we discuss within $a \leq 320$. Meanwhile, Lemma 4.1 and the procedures in the previous section can apply to any $e \geq 0$ and $q^{dg_0+e} > 2^{320}$. The treatment of these cases will be reported in the near future.*

6.1.1 Case $g(C_0) = 1$

Then, we have the following situation for $g_0 = 1$

$$\begin{cases} q^{d+e} \leq 2^a \\ 2^{160} \leq q^d. \end{cases} \quad (30)$$

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

$$e \leq \frac{(a-160)d}{160}. \quad (31)$$

When we assume $a \leq 320$, $e \leq d$ is obtained.

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

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

$$\begin{cases} q^{2d+e} \leq 2^a \\ 2^{160} \leq q^{2d}. \end{cases} \quad (32)$$

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 $q^{3d} \geq 2^{160}$ ($q^{\frac{4}{3}d} \geq 2^{71.11\dots}$) to keep the same security level with $g_0 = 1, 2$ hyperelliptic curves (the costs of attack to each DLP are $q^{\frac{d}{2}} \geq 2^{80}$ for $g_0 = 1$, $q^d \geq 2^{80}$ for $g_0 = 2$ as a key length of more than 2^{160} respectively). Thus, one can assume

$$\begin{cases} q^{3d+e} \leq 2^a \\ 2^{180} \leq q^{3d}. \end{cases} \quad (33)$$

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

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

6.2.1 Type (A)

- Case $g_0 = 1$:

From the above, $d + e - 1 \geq 2^{n-2}d - 2^n$ when $g_0 = 1$. 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 $n > 3$,

$$(n \leq) d \leq 4 + \frac{7}{2^{n-2} - 2}. \quad (34)$$

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 $g_0 = 2$:

Similarly, when $g_0 = 2$, since we assume $0 < e \leq 2d$, $4d - 1 \geq 2d + e - 1 \geq 2^{n-2}d - 2^n$. Then, if $n > 4$,

$$(n \leq) d \leq 4 + \frac{15}{2^{n-2} - 4}. \quad (35)$$

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 $g_0 = 3$:

Next, if $g_0 = 3$ ($0 < e \leq \frac{7}{3}d$), then

$$(5 \leq n \leq) d \leq 4 + \frac{61}{3(2^{n-2} - \frac{16}{3})}. \quad (36)$$

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

6.2.2 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 \spadesuit_i in

(9)). Here, if $g_0 = 1$ ($0 < e \leq d$), then

$$d + e - 1 \leq 2d - 1 < 2^{n+1}. \quad (37)$$

On the other hand, it follows that

$$d + e - 1 \geq 2^{n-2}(q(d) - 4) \quad (38)$$

since $S = 4 + \frac{d+e-1}{2^{n-2}} \geq q(d)$. From (37)(38), one obtains

$$2^{n+1} > 2^{n-2}(q(d) - 4). \quad (39)$$

Consequently, $12 > q(d)$. Besides, we have $20 > q(d)$ for $g_0 = 2$ ($0 < e \leq 2d$) since $2^{n-2}(q(d) - 4) \leq 2d + e - 1 < 2^{n+2}$. By the similar manner, $26 > q(d)$ when $g_0 = 3$ ($0 < e \leq \frac{7}{3}d$).

• Case 2 | 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

$$\boxed{\spadesuit}_i = \begin{pmatrix} \boxed{\star}_i & \boxed{\star}_i & \hat{O} & \cdots \\ \hat{O} & \boxed{\star}_i & \ddots & \ddots \\ \vdots & \ddots & \ddots & \boxed{\star}_i \\ \hat{O} & \cdots & \hat{O} & \boxed{\star}_i \end{pmatrix} \begin{matrix} 1 \\ \\ \\ l_i \end{matrix} \quad (\boxed{\star}_i) \} m_i. \quad (40)$$

Then

$$d = LCM\{2^{r_i} d'_i\} = 2^r \cdot LCM\{d'_i\} \leq 2^r \cdot \prod d'_i \quad (41)$$

$$\leq 2^r \cdot \prod (2^{m_i} - 1) \quad (42)$$

$$< \begin{cases} 2^{r+\sum_{i \geq 1} m_i} & (m_1 \geq 2) \\ 2^{r+\sum_{i \geq 2} m_i} & (m_1 = 1). \end{cases} \quad (43)$$

On the other hand, we know

$$d g_0 + e - 1 \geq 2^{n-2}(q(d) - 4). \quad (44)$$

Hence, if $g_0 = 1$ ($0 < e \leq d$), then

$$2d - 1 \geq 2^{n-2}(q(d) - 4). \quad (45)$$

From (43) (45), we obtain

$$2^{r+(\sum_{i \geq 1} m_i)+1} > 2^{n-2}(q(d) - 4) \quad (46)$$

$$2^{3+r+(\sum_{i \geq 1} m_i)-n} > q(d) - 4 \quad (47)$$

$$2^{3+r-2^{r-1}m_1} > q(d) - 4 \quad (48)$$

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 $g_0 = 2$ and $g_0 = 3$ respectively.

From these upper bounds and the property of σ , we obtain a list of possible (g_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 the above lists, we constructed explicitly all classes of hyperelliptic curves C_0/k_d for $g(C_0) \in \{1, 2, 3\}$ such that there is a covering $\pi/k_d : C \rightarrow C_0$ and the covering curve C/k has genus $g(C) = d \cdot g(C_0) + e$ ($e > 0$). Lists for all defining equation C_0/k_d are shown in the Appendices.

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 in 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 $(2, \dots, 2)$ 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] S. Lang, “*Algebra (Revised Third Edition)*,” *Graduate Text in Mathematics*, no.211, Springer-Verlag, 2002.
- [18] F. Momose and J. Chao “Classification of Weil restrictions obtained by $(2, \dots, 2)$ coverings of \mathbb{P}^1 ,” preprint, 2006. Available from <http://eprint.iacr.org/2006/347>
- [19] 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>
- [20] F. Momose and J. Chao “Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristics,” preprint, 2009. Available from <http://eprint.iacr.org/2009/236>

- [21] 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>
- [22] 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.
- [23] 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.
- [24] H. Stichtenoth, “Algebraic function fields and codes,” Universitext, Springer-Verlag, 1993.
- [25] N.Thériault, “Index calculus attack for hyperelliptic curves of small genus,” Advances in Cryptology-ASIACRYPT 2003, LNCS 2894, pp.75–92, 2003

Appendices

A Classification for Type (A) : $\exists d_i = d$

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 $\tau_i \in \{d, 2d, \dots, \max\{i\}d\}$ such that $h_d(x) \in k_d[x] \setminus k_u[x]$ ($u \mid \neq d$). Refer to Example 5.6 $(n, d, g_0, e, S) = (2, 2, 2, 1, 8)$ as an example of how to choose α_i and τ_i . Let $C_0/k_d : y^2 = c \cdot h_d(x)h_1(x)$.

(n, d, g_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
$(2, 2, 3, 1, 10)$	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 $\beta \in k_2 \setminus k$, $\beta_j \in k_{\omega_j} \setminus k_{\rho_j}$ ($\rho_j \nmid \omega_j$), $h_2(x) \in k_2[x] \setminus k[x]$.

Here, choose β_j and $\omega_j \in \{d, 2d, \dots, \max\{j\}d\}$ 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_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	$(x - \alpha)(x - \alpha^q)$	$\prod_{j=1}^2 (x - \beta_j)$	2, 1
(3, 4, 2, 7, 11)	1	$(x - \alpha)(x - \alpha^q)$	$\prod_{j=1}^3 (x - \beta_j)$	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	$(x - \alpha)(x - \alpha^q)$	$\prod_{j=1}^2 (x - \beta_j)$	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

B Classification for Type (B): $\forall d_i \neq d$

Here, $h_v(x) \in k_v[x] \setminus k_w[x]$ ($w \nmid v$), $\eta := 1$ 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_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_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_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_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_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_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