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

Tsutomu Iijima * Fumiyuki Momose † Jinhui Chao ‡

2009/12/10

Abstract

The GHS attack is known as a method to map the discrete logarithm problem(DLP) in the Jacobian of a curve C_0 defined over the d degree extension k_d of a finite field k to the DLP in the Jacobian of a new curve C over k which is a covering curve of C_0.

Recently, classification and density analysis were shown for all elliptic and hyperelliptic curves C_0/k_d of genus 2, 3 which possess $(2,\ldots,2)$ covering C/k of $\mathbb{P}^1$ under the isogeny condition (i.e. when $g(C) = d \cdot g(C_0)$). In this paper, we show a complete classification of small genus hyperelliptic curves C_0/k_d which possesses $(2,..,2)$ covering C over k without the isogeny condition. Our main approach is to use representation of the extension of $Gal(k_d/k)$ acting on $cov(C/\mathbb{P}^1)$. In the classification we restricted the group order or key-length of the DLP to certain range reasonable in cryptographic application. Explicit defining equations of such curves and the existence 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 [8] to elliptic curve cryptosystems. This idea is developed into the well-known GHS attack in [12]. This attack maps the discrete logarithm problem (DLP) in the Jacobian of a curve

*Koden Electronics 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

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 in [2][4][9] [10][15][16][17][20][25][26], and is conceptually generalized to the cover attack [6]. 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 [11], 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 [27] and a double-large-prime variation [13][24] 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 [5] can be applied with complexity of $\tilde{O}(q^{2-2/(g-1)})$. This algorithm is not only faster than Pollard's rho algorithm but also the fastest attack algorithm to curve based cryptosystems at present.

Recently, a thorough security analysis of elliptic and hyperelliptic curves C_0/k_d with weak covering C/k is shown in [3][21][22][23] under the following isogeny condition. Assuming that there exists a covering curve C/k of C_0/k_d,

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

such that for

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

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

is an isogeny, 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 isogeny condition, C_0/k_d which possesses covering curves C/k as $(2,\ldots,2)$ covering of $\mathbb{P}^1$ are classified for hyperelliptic curves of genus 1,2,3 in [3][14][21][22][23]. Density and defining equations are also presented for these curves. Further in [18], when $g(C) = d{\cdot}g(C_0){+}e, (e > 0, d = 2,3,4)$ for $g(C_0) = 1,2,3$ hyperelliptic curves in the cryptographic applications, certain classes of curves C_0/k_d which have weak coverings C/k were showed.

In this paper, we show a complete classification of hyperelliptic curves C_0/k_d of genus 1,2,3 with $(2,\ldots,2)$ covering C/k without isogeny condition. In particular, we assume that $g(C) = d \cdot g(C_0) + e, e > 0$. The classification is then restricted to a certain range of the group order or key-length reasonable for cryptographic applications. Our approach for the classification is a representation theoretical one, to investigate action of the extension of $Gal(k_d/k)$ on $cov(C/\mathbb{P}^1)$. We also present defining equations of these curves and existential conditions of a model of C over k explicitly.

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

Firstly, we summarize 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. Assume $\sigma_{k_d/k}$ is extended to an automorphism σ of order d in the separable closure of $k_d(x)$. The Galois closure of $k_d(C_0)/k(x)$ is $F' := k_d(C_0) \cdot \sigma(k_d(C_0)) \cdots \sigma^{d-1}(k_d(C_0))$ and the fixed field of F' by the automorphism σ is $F := \{\alpha \in F' \mid \sigma(\alpha) = \alpha\}$. The DLP in $Cl^0(k_d(C_0))$ is mapped to the DLP in $Cl^0(F)$ using the following composition of conorm and norm maps:

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

This map is called the conorm-norm homomorphism in the original GHS paper on the elliptic curve case [12].

This attack has been extended to wider classes of curves [2][4][9][10][15][16][17][25][26]. The GHS attack is conceptually generalized to the cover attack by Frey and Diem [6]. 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.

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

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

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

Then we have a tower of extensions of function fields such that $k_d(x, y, {}^{\sigma^1}y, \ldots, {}^{\sigma^{n-1}}y)$ $/k_d(x)$ $(n \leq d)$ 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 $cov(C/\mathbb{P}^1) := Gal(k_d(C)/k_d(x))$.

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

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

$$Gal(k_d/k) \curvearrowright cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n \tag{6}$$

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

$$\xi : Gal(k_d/k) \hookrightarrow Aut(cov(C/\mathbb{P}^1)) \simeq GL_n(\mathbb{F}_2) \tag{7}$$

Then, the representation of σ for given n, d is as follows:

$$\sigma = \begin{pmatrix} \boxed{\spadesuit_1} & O & \cdots & O \\ O & \boxed{\spadesuit_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \boxed{\spadesuit_s} \end{pmatrix} \begin{matrix} \}n_1 \\ \\ \\ \}n_s \end{matrix} \qquad n = \sum_{i=1}^{s} n_i \tag{8}$$

where the O is a zero matrix,

$$\boxed{\spadesuit_i} = \begin{pmatrix} \boxed{\star_i} & \boxed{\star_i} & \tilde{O} & \cdots \\ \tilde{O} & \boxed{\star_i} & \ddots & \ddots \\ \vdots & \ddots & \ddots & \boxed{\star_i} \\ \tilde{O} & \cdots & \tilde{O} & \boxed{\star_i} \end{pmatrix} \begin{matrix} 1 \\ \vdots \\ \\ l_i \end{matrix} \tag{9}$$

is an $n_i \times n_i$ matrix which has a form of an $l_i \times l_i$ block matrix. The sub-block $\boxed{\star_i}$ is an $n_i/l_i \times n_i/l_i$ matrix and $\tilde{O}$ is an $n_i/l_i \times n_i/l_i$ zero matrix. Here, if $F_i(x)$:=(the characteristic polynomial of $\boxed{\star_i})^{l_i}$, then $F(x) := LCM\{F_i(x)\}$ is the minimal polynomial of σ. Obviously, $F_i(\sigma) = 0$ and $F(\sigma) = 0$. When d_i :=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. $n = 2, d = 2$

$$\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{10}$$

$F(\sigma) = (\sigma + 1)^2 = 0$

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

$$\sigma = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \tag{11}$$

$F(\sigma) = \sigma^2 + \sigma + 1 = 0$

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

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{12}$$

$F(\sigma) = (\sigma + 1)(\sigma^2 + \sigma + 1) = 0$

Example 3.4. $n = 4, d = 6$

$$\sigma = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \textit{ or } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{13}$$

$F(\sigma) = (\sigma^2 + \sigma + 1)^2 = 0$ *or* $F(\sigma) = (\sigma + 1)^2(\sigma^2 + \sigma + 1) = 0.$
Notice that

$$\boxed{\star_1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \textit{ or } \boxed{\spadesuit_1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \boxed{\spadesuit_2} = \boxed{\star_2} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \textit{ respectively.} \tag{14}$$

4 Upper bound of e in $g(C) = dg(C_0) + e$

From now, we consider 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 $g(C) = d \cdot g(C_0) + e$ $(e > 0)$. Here, e can be regarded as the dimension of $\ker(Res(\pi_*))$. Firstly, for C_0 which are used in the cryptographic applications, we will 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

$$q^{g(C_0)d} \geq 2^{160}. \tag{15}$$

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

Remark 4.1. *In this paper, we discuss within $a \leq 320$. However, the procedures in the section 4.3 can apply to any a such that $q^{dg_0+e} \leq 2^a$. Besides, we notice that Lemma 5.1 and the procedure in the section 5.2 are independent of choice of the range.*

4.1 Case $g(C_0) = 1$

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

$$\begin{cases} q^{d+e} \leq 2^a \\ 2^{160} \leq q^d. \end{cases} \tag{16}$$

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

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

It follows that an upper bound of e is

$$e \leq \frac{(a-160)d}{160}. \tag{17}$$

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

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

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

$$\begin{cases} q^{2d+e} \leq 2^a \\ 2^{160} \leq q^{2d}. \end{cases} \tag{18}$$

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 $g_0 = 1, 2$ 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 $g_0 = 2$ respectively). Thus, one can assume

$$\begin{cases} q^{3d+e} \leq 2^a \\ 2^{180} \leq q^{3d}. \end{cases} \tag{19}$$

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 $g(C_0) = 1, 2, 3$.

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

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). See the example 3.4 again. We notice the left and right matrices are a type (A) and a type (B) respectively.

4.3.1 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 $n > 3$,

$$(n \leq)\ d \leq 4 + \frac{7}{2^{n-2}-2}. \tag{20}$$

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 $n > 4$,

$$(n \leq)\ d \leq 4 + \frac{15}{2^{n-2}-4}. \tag{21}$$

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

$$(5 \leq n \leq)\ d \leq 4 + \frac{61}{3(2^{n-2} - \frac{16}{3})}. \tag{22}$$

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

4.3.2 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 $\boxed{\spadesuit_i}$ in (8)). Here, if $g_0 = 1$ $(0 < e \leq d)$, then

$$d + e - 1 \leq 2d - 1 < 2^{n+1}. \tag{23}$$

On the other hand, it follows that

$$d + e - 1 \geq 2^{n-2}(q(d) - 4) \tag{24}$$

since $S = 4 + \frac{d+e-1}{2^{n-2}} \geq q(d)$. From (23)(24), one obtains

$$2^{n+1} > 2^{n-2}(q(d) - 4). \tag{25}$$

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 $2 \mid d$:
In this case, $n_i = l_i m_i, d_i = 2^{r_i} d_i^0$ $(2 \nmid d_i^0)$, then $d_i^0 \mid 2^{m_i} - 1$. 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

$$\boxed{\spadesuit_i} = \begin{pmatrix} \boxed{\star_i} & \boxed{\star_i} & \tilde{O} & \cdots \\ \tilde{O} & \boxed{\star_i} & \ddots & \ddots \\ \vdots & \ddots & \ddots & \boxed{\star_i} \\ \tilde{O} & \cdots & \tilde{O} & \boxed{\star_i} \end{pmatrix} \begin{matrix} 1 \\ \\ \\ l_i \end{matrix} \qquad (\boxed{\star_i})\ \}m_i. \tag{26}$$

Then

$$d = LCM\{2^{r_i}d_i^0\} = 2^r \cdot LCM\{d_i^0\} \leq 2^r \cdot \prod d_i^0 \quad (27)$$

$$\leq 2^r \cdot \prod (2^{m_i} - 1) \quad (28)$$

$$< \begin{cases} 2^{r+\sum_{i\geq 1} m_i} & (m_1 \geq 2) \\ 2^{r+\sum_{i\geq 2} m_i} & (m_1 = 1). \end{cases} \quad (29)$$

On the other hand, we know

$$dg_0 + e - 1 \geq 2^{n-2}(q(d) - 4). \quad (30)$$

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

$$2d - 1 \geq 2^{n-2}(q(d) - 4). \quad (31)$$

From (29) (31), we obtain

$$2^{r+(\sum_{i\geq 1} m_i)+1} > 2^{n-2}(q(d) - 4) \quad (32)$$

$$2^{3+r+(\sum_{i\geq 1} m_i)-n} > q(d) - 4 \quad (33)$$

$$2^{3+r-2^{r-1}m_1} > q(d) - 4 \quad (34)$$

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 $g_0 = 3$.

From these upper bounds and the property of σ, we obtain a list of possible (g_0, n, d, e, S).
$(1,4,6,3,6), (2,5,12,9,8), (2,5,12,17,9), (2,5,14,13,9), (2,5,14,21,10),$
$(2,5,21,7,10), (2,5,21,15,11), (2,5,21,23,12), (2,5,21,31,13), (2,5,21,39,14),$
$(2,4,6,5,8), (2,4,6,9,9), (3,6,21,34,10), (3,6,28,29,11), (3,6,28,45,12),$
$(3,6,28,61,13), (3,5,21,2,12), (3,5,21,10,13), (3,5,21,18,14), (3,5,21,26,15),$
$(3,5,21,34,16), (3,5,21,42,17), (3,5,14,7,10), (3,5,14,15,11), (3,5,14,23,12),$
$(3,5,14,31,13), (3,5,12,13,10), (3,5,12,21,11), (3,4,6,7,10), (3,4,6,11,11).$

Next, within the above lists, we construct explicitly 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 $g(C) = d \cdot g(C_0) + e$ $(e > 0)$.

5 Elliptic/Hyperelliptic curves C_0 against GHS attack

5.1 Existence of a model of C over k

Here, we show conditions for existence of a model of C over k.

Consider that C_0 is 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. Define $\hat{F}(x) \in \mathbb{F}_2[x]$ as a polynomial such that $x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]$. We have the following necessary and sufficient condition:

C has a model over $k_d \Longleftrightarrow$

$$\begin{aligned} {}^{F(\sigma)}y^2 &\equiv {}^{F(\sigma)}c = c^{F(q)} \equiv 1 \mod (k_d(x)^\times)^2, \\ {}^{G(\sigma)}y^2 &\not\equiv 1 \mod (k_d(x)^\times)^2 \text{ for}^\forall G(x) \mid F(x), G(x) \neq F(x). \end{aligned} \tag{35}$$

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 $k_d(x)$.

Consequently, in the following lemma, we make the condition for c explicitly.

Lemma 5.1. *Assume the condition (35) holds. In order that the curve C has a model over k, c needs to be a square $c \in (k_d^\times)^2$ when $\hat{F}(1) = 0$. When $\hat{F}(1) = 1$, there is a $\phi \in cov(C/\mathbb{P}^1)$ such that $\sigma\phi$ has order d even if σ does not have order d. Therefore C always has a model over k.*

Proof: Let $M := \{\frac{b(x)}{a(x)} | k_d[x] \ni a(x), b(x) : \text{monic}\}$.
Now, one has

$$\begin{aligned} {}^{F(\sigma)}y &\equiv \epsilon c^{\frac{F(q)}{2}} \mod M, \qquad \text{here } \epsilon = \pm 1 \\ {}^{\hat{F}(\sigma)F(\sigma)}y &\equiv {}^{\hat{F}(\sigma)}\epsilon c^{\frac{\hat{F}(q)F(q)}{2}} \\ {}^{\sigma^d+1}y &\equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d+1}{2}} \\ {}^{\sigma^d}y &\equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d-1}{2}} y \end{aligned}$$

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

- Case $F(1) = 1$:
  We notice $\hat{F}(1) = 0$ in this case. From ${}^{\sigma^d}y \equiv c^{\frac{q^d-1}{2}} y$, it follows that $c^{\frac{q^d-1}{2}} = 1$. Hence $c \in (k_d^\times)^2$.
- Case $F(1) = 0$:
  Here, we consider further two possibilities of $\hat{F}(1) = 0$ and $\hat{F}(1) = 1$.
  (a) $\hat{F}(1) = 0$
  From ${}^{\sigma^d}y \equiv c^{\frac{q^d-1}{2}} y$, we know $c \in (k_d^\times)^2$.
  (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 ${}^\exists \phi \in cov(C/\mathbb{P}^1)$ such that $(\sigma\phi)^d = 1$.
Indeed, suppose $d = 2^r \cdot d_1$ $(2 \nmid d_1)$. Since ${}^\sigma\phi = \sigma\phi\sigma^{-1}$, we have

$$\begin{aligned}
(\sigma\phi)^d &= \sigma\phi\sigma^{-1} \cdot \sigma^2\phi\sigma^{-2} \cdots \sigma^d\phi\sigma^{-d} \cdot \sigma^d \\
&= {}^\sigma\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^d}\phi\ \sigma^d \\
&= {}^\sigma\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r d_1}}\phi\ \sigma^d \\
&= (\phi\ {}^\sigma\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r-1}}\phi)^{d_1}\ \sigma^d.
\end{aligned}$$

Here we use the additive notation of the Galois action on $\mathrm{cov}(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$. Define

$$J := \left.\begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 \\ 0 & \dots & 0 & 0 \end{pmatrix}\right\} m \leq 2^r .$$

Then $J^m = O$. Choose $\phi := {}^t(0, 0, \dots, 1)$. Now, ${}^{\sigma^i}\phi$ corresponds to $(I + J)^i \cdot {}^t(0, \dots 0, 1)$. Since

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

where O is the zero matrix, it follows that

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

On the other hand, σ^d is an element in the center of $Gal(k_d(C)/k(x))$, i.e., $\sigma^d \in Z(Gal(k_d(C)/k(x))) = \{1, \psi\}$. Thus, in the multiplicative notation,

$$(\sigma\phi)^d = (\phi\ {}^\sigma\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r-1}}\phi)^{d_1}\ \sigma^d = \begin{cases} 1^{d_1} \cdot 1 = 1 & \text{if } m < 2^r \\ \psi^{d_1} \cdot \psi = 1 & \text{if } m = 2^r. \end{cases}$$

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

□

5.2 The defining equations of C_0

Finally, we show how to derive the defining equations of C_0/k_d for candidates of (n, d, g_0, e, S). Suppose ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^{\times})^2$ is satisfied. Recall $x^d + 1 = F(x)\hat{F}(x)$. 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 $i = 0, \ldots, d-1$. Let $\phi(x) := b_{d-1}x^{d-1} + \cdots + b_1x + b_0$. We know that $F(x)\phi(x) \equiv 0 \mod x^d + 1 \Leftrightarrow \phi(x) \equiv 0 \mod \hat{F}(x)$. Hence ${}^{\exists}a(x) \in \mathbb{F}_2[x]$, $(a(x), F(x)) = 1$, $\deg a(x) < \deg F(x)$, $\phi(x) \equiv a(x)\hat{F}(x) \mod x^d + 1$ for given n, d.

Further, we define the equivalence $(b_0, b_1, \ldots, b_{d-1}) \sim (b_j, \ldots, b_{d-1}, b_0, \ldots, b_{j-1})$, then corresponding $\phi(x)$'s belong to the same class of C_0. Indeed, $x^r a(x)\hat{F}(x) \equiv a(x)\hat{F}(x) \mod x^d + 1 \Leftrightarrow x^r + 1 \equiv 0 \mod \hat{F}(x)$ for $1 \le r \le d$. Since $\hat{F}(x)\mathbb{F}_2[x]/(x^d + 1) \cong \mathbb{F}_2[x]/(F(x))$, the number of the classes of C_0 is $N := \#\{(\mathbb{F}_2[x]/(F(x)))^{\times}\}/d$.

From the facts, we obtain a procedure to derive the defining equations of C_0 is as follows:

1. Choose a polynomial $a(x) = 1$, then $\phi(x) = \hat{F}(x)$ defines a class of C_0. If $N = 1$, then this procedure is completed.
2. If $N \neq 1$, choose another polynomial $a(x)$ satisfied the above condition and define $\phi(x) = a(x)\hat{F}(x)$.
3. Find the class of C_0 defined by $\phi(x)$.
4. Repeat step 2,3 until $N - 1$ different polynomials $a(x)$ are found so that the coefficients of $\phi(x)$ defined by $a(x)$ are not cyclic permutation of each others (See the example 5.4 as an instance of $N \neq 1$).

Example 5.1. $n = 2, d = 2$ *(Type A)*
From $x^2 + 1 = (x + 1)^2$, $F(x) = (x + 1)^2, \hat{F}(x) = 1$. *Now, choose* $a(x) = 1$ *since* $N = 1$, *then* $\phi(x) = 1$. *Thus, there exists a ramification point* $\alpha \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 2 \mid d')$ *on* C_0.
• *Case* $g_0 = 2, e = 1, S = 8$
The form of $C_0/\mathbb{F}_{q^2}$ *is* $y^2 = c \cdot h_2(x)h_1(x)$. *Here,* $h_1(x) \in \mathbb{F}_q[x]$, $h_2(x) \in \mathbb{F}_{q^2}[x] \setminus \mathbb{F}_q[x]$, $\deg h_2(x) = 2, \deg h_1(x) \in \{4, 3\}$, $c := 1$ *or a non-square element in* $\mathbb{F}_{q^2}$ *because* $\hat{F}(1) = 1$. *Then* $h_2(x) = (x - \alpha_1)(x - \alpha_2)$ *since* $S = 2/\mathbb{F}_{q^2} + 2/\mathbb{F}_{q^2} + 4/\mathbb{F}_q$ *is satisfied (Note that* $2/\mathbb{F}_{q^2}$ *and* $4/\mathbb{F}_q$ *mean the numbers of fixed points over* $\mathbb{F}_{q^2}$ *and* $\mathbb{F}_q$ *respectively). In this case, notice the ramification points* $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *or* $\alpha_1, \alpha_2 \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$, $\alpha_2 := \alpha_1^{q^2}$ *(i.e.* $d' = 2, 4$*). See the list in the Appendix for details.*
• *Case* $g_0 = 1, e = 2, S = 7$
The form of $C_0/\mathbb{F}_{q^2}$ *is* $y^2 = c \cdot h_2(x)h_1(x)$. *Here,* $h_1(x) \in \mathbb{F}_q[x]$, $h_2(x) \in \mathbb{F}_{q^2}[x] \setminus \mathbb{F}_q[x]$, $\deg h_2(x) = 3, \deg h_1(x) \in \{1, 0\}$, $c := 1$ *or a non-square element in* $\mathbb{F}_{q^2}$. *Then* $h_2(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ *since* $S = 2/\mathbb{F}_{q^2} +$

$2/\mathbb{F}_{q^2} + 2/\mathbb{F}_{q^2} + 1/\mathbb{F}_q$. *In this case, the ramification points are* $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *or* $\alpha_1 \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ $\alpha_2 := \alpha_1^{q^2}$ $\alpha_3 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *or* $\alpha_1 \in \mathbb{F}_{q^6} \setminus (\mathbb{F}_{q^2} \cup \mathbb{F}_{q^3})$ $\alpha_2 := \alpha_1^{q^2}$ $\alpha_3 := \alpha_1^{q^4}$ *(i.e.* $d' = 2, 4, 6$*).*

Example 5.2. $n = 2, d = 3$ *(Type A)*
$x^3 + 1 = (x+1)(x^2+x+1), F(x) = x^2 + x + 1, \hat{F}(x) = x + 1$. *Now, choose* $a(x) = 1$ *since* $N = 1$*, then* $\phi(x) = x+1$. *Consequently,* C_0 *has ramification points* $\alpha, \alpha^q \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 3 \mid d')$. *However, there is no class of* C_0 *within the list of the previous section.*

Example 5.3. $n = 3, d = 3$ *(Type A)*
$F(x) = (x+1)(x^2+x+1), \hat{F}(x) = 1$. *Similarly,* C_0 *has a ramification point* $\alpha \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 3 \mid d')$. *In this case, consider also* $(n, d) = (2, 3)$ *(i.e. ramification points* $\alpha, \alpha^q \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 3 \mid d')$*).*
• *Case* $g_0 = 2, e = 3, S = 8$
Then, there exist two cases as follow:

1. $S = 3/\mathbb{F}_{q^3} + 5/\mathbb{F}_q$
   $C_0/\mathbb{F}_{q^3}$ *is* $y^2 = c \cdot (x - \alpha)h_1(x)$. *Here,* $\alpha \in \mathbb{F}_{q^3}, h_1(x) \in \mathbb{F}_q[x]$, $\deg h_1(x) \in \{5, 4\}$, $c := 1$ *or a non-square element in* $\mathbb{F}_{q^3}$.
2. $S = 3/\mathbb{F}_{q^3} + 3/\mathbb{F}_{q^3} + 2/\mathbb{F}_q$
   $C_0/\mathbb{F}_{q^3}$ *is* $y^2 = c \cdot (x - \alpha_1)(x - \alpha_1^q)(x - \alpha_2)(x - \alpha_2^q)h_1(x)$. *Here,* $(x - \alpha_1)(x - \alpha_1^q)(x - \alpha_2)(x - \alpha_2^q) \in \mathbb{F}_{q^3}[x] \setminus \mathbb{F}_q[x], h_1(x) \in \mathbb{F}_q[x]$, $\deg h_1(x) \in \{2, 1\}$, $c := 1$ *or a non-square element in* $\mathbb{F}_{q^3}$. *In this case, the ramification points are* $\alpha_1, \alpha_2 \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ *or* $\alpha_1 \in \mathbb{F}_{q^6} \setminus (\mathbb{F}_{q^2} \cup \mathbb{F}_{q^3})$ $\alpha_2 := \alpha_1^{q^3}$.

Example 5.4. $n = 4, d = 6$ *(Type A)*
$x^6 + 1 = (x+1)^2(x^2+x+1)^2$.

- *Case(a)*
  $F(x) = (x^2+x+1)^2, \hat{F}(x) = (x+1)^2$. *Now, choose* $a(x) = 1$ *and* $a(x) = x+1$ *since* $N = 2$*, then* $\phi(x) = x^2+1$ *and* $\phi(x) = x^3+x^2+x+1$. *In these cases,* C_0 *has ramification points* α, α^{q^2} *or* $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3} \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 6 \mid d')$.
- *Case(b)*
  $F(x) = (x+1)^2(x^2+x+1), \hat{F}(x) = (x^2+x+1)$. *Now, choose* $a(x) = 1$ *since* $N = 1$*, then* $\phi(x) = x^2+x+1$. *In the case,* C_0 *has ramification points* $\alpha, \alpha^q, \alpha^{q^2} \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 6 \mid d')$.

Example 5.5. $n = 4, d = 6 = 2 \cdot 3$ *(Type B)*
$x^6 + 1 = (x+1)^2(x^2+x+1)^2, F(x) = (x+1)^2(x^2+x+1)$.
Then we consider the candidates of $(n, d) = (2, 2), (2, 3), (3, 3)$ *(i.e. ramification points* $\beta \in \mathbb{F}_{q^{e'}} \setminus \mathbb{F}_{q^{l'}}$ $(l' \mid_{\neq} e', 2 \mid e')$ *and* $\alpha, \alpha^q \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 3 \mid d')$ *or* $\beta \in \mathbb{F}_{q^{e'}} \setminus \mathbb{F}_{q^{l'}}$ $(l' \mid_{\neq} e', 2 \mid e')$ *and* $\alpha \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 3 \mid d')$*.*

Lists are shown in the Appendices for all defining equations C_0.

References

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

[2] S. Arita, "Weil descent of elliptic curves over finite fields of characteristic three," Advances in Cryptology-ASIACRYPTO 2000, Springer-Verlag, LNCS 1976, pp.248–258, 2000.

[3] J. Chao, "Elliptic and hyperelliptic curves with weak coverings against Weil descent attack," Talk at the 11th Elliptic Curve Cryptography Workshop, 2007.

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

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

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

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

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

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

[10] S. Galbraith, F. Hess, and N. Smart, "Extending the GHS Weil descent attack," Advances in Cryptology-EUROCRYPTO 2002, Springer-Verlag, LNCS 2332, pp.29–44, 2002.

[11] 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.

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

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

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

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

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

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

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

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

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

[21] 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

[22] 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

[23] 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

[24] 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

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

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

[27] 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) : $^{\exists}d_i = d$

Here, $h_1(x) \in \mathbb{F}_q[x]$, $h_d(x) \in \mathbb{F}_{q^d}[x] \setminus \mathbb{F}_{q^j}[x]$ $(j \mid_{\neq} d)$,
$\eta :=$ 1 or a non-square element in $\mathbb{F}_{q^d}$.
$\alpha, \gamma \in \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^j}$ $(j \mid_{\neq} d)$, $\alpha_i \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', d \mid d')$.
Notice $d' = d, 2d, \ldots, \max\{i\}d$ for i in the tables.

$C_0/k_d : y^2 = c \cdot h(x)h_1(x)$
(1) $n = 4, d = 4$
Then $h(x) = h_d(x)$.

(n, d, g_0, e, S)	$h_d(x)$	$\deg h_1(x)$	c
$(4, 4, 1, 1, 5)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	$1, 0$	η
$(4, 4, 2, 5, 7)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	$3, 2$	η
$(4, 4, 3, 9, 9)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	$5, 4$	η
	$(x-\alpha)(x-\gamma^q)(x-\gamma^{q^2})$	$5, 4$	η

(2) $n = 4, d = 5$
$h(x) = h_d(x)$

(n, d, g_0, e, S)	$h_d(x)$	$\deg h_1(x)$	c
$(4, 5, 3, 10, 10)$	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)(x-\alpha_i^{q^2})(x-\alpha_i^{q^3})$	0	1

(3) $n = 4, d = 6$
$h(x) = h_d(x)$

(n, d, g_0, e, S)	$h_d(x)$	$\deg h_1(x)$	c
$(4, 6, 1, 3, 6)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$	0	1
$(4, 6, 2, 9, 9)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	3,2	η

(4) $n = 4, d = 7$
$h(x) = h_d(x)$

(n, d, g_0, e, S)	$h_d(x)$	$\deg h_1(x)$	c
$(4, 7, 2, 7, 9)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$2, 1$	η
	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$2, 1$	η
$(4, 7, 2, 11, 10)$	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})$	$3, 2$	η
	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	$3, 2$	η
$(4, 7, 3, 8, 11)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$4, 3$	η
	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$4, 3$	η
$(4, 7, 3, 12, 12)$	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})$	$5, 4$	η
	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	$5, 4$	η

Here, $\alpha \in \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^j}$ $(j \mid_{\neq} d)$, $\alpha_i \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', d \mid d')$.
$C_0/k_d : y^2 = c \cdot h(x)h_1(x)$
(5) $n = 3, d = 3$
$h(x) = h_d(x)$

(n,d,g_0,e,S)	$h_d(x)$	$\deg h_1(x)$	c
$(3,3,1,2,6)$	$x-\alpha$	$3,2$	η
$(3,3,2,1,7)$	$(x-\alpha)(x-\alpha^q)$	$4,3$	η
$(3,3,2,3,8)$	$x-\alpha$	$5,4$	η
	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$2,1$	η
$(3,3,2,5,9)$	$(x-\alpha)(x-\alpha^q)(x-\gamma)$	$3,2$	η
$(3,3,3,2,9)$	$(x-\alpha)(x-\alpha^q)$	$6,5$	η
$(3,3,3,4,10)$	$x-\alpha$	$7,6$	η
	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$4,3$	η
$(3,3,3,6,11)$	$(x-\alpha)(x-\alpha^q)(x-\gamma)$	$5,4$	η
	$\prod_{i=1}^{3}(x-\alpha_i)(x-\alpha_i^q)$	$2,1$	η

(6) $n = 3, d = 4$ $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\beta_i \in \mathbb{F}_{q^{e'}} \setminus \mathbb{F}_{q^{l'}}$ $(l' \mid_{\neq} e', 2 \mid e')$, $h_2(x) \in \mathbb{F}_{q^2}[x] \setminus \mathbb{F}_q[x]$
$h(x) = h_d(x)h_2(x)$

(n,d,g_0,e,S)	$h_d(x)$	$h_2(x)$	$\deg h_1(x)$	c
$(3,4,1,1,6)$	$(x-\alpha)(x-\alpha^q)$	1	$2,1$	1
$(3,4,1,3,7)$	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$1,0$	1
$(3,4,2,1,8)$	$(x-\alpha)(x-\alpha^q)$	1	$4,3$	1
$(3,4,2,3,9)$	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$3,2$	1
$(3,4,2,5,10)$	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$	1	$2,1$	1
	$(x-\alpha)(x-\alpha^q)$	$(x-\beta_1)(x-\beta_2)$	$2,1$	1
$(3,4,2,7,11)$	$(x-\alpha)(x-\alpha^q)$	$\prod_{i=1}^{3}(x-\beta_i)$	$1,0$	1
	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$1,0$	1
$(3,4,3,1,10)$	$(x-\alpha)(x-\alpha^q)$	1	$6,5$	1
$(3,4,3,3,11)$	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$5,4$	1
$(3,4,3,5,12)$	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	1	$4,3$	1
	$(x-\alpha)(x-\alpha^q)$	$(x-\beta_1)(x-\beta_2)$	$4,3$	1
$(3,4,3,7,13)$	$(x-\alpha)(x-\alpha^q)$	$\prod_{i=1}^{3}(x-\beta_i)$	$3,2$	1
	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$3,2$	1
$(3,4,3,9,14)$	$(x-\alpha)(x-\alpha^q)$	$\prod_{i=1}^{4}(x-\beta_i)$	$2,1$	1
	$\prod_{i=1}^{2}(x-\alpha_i)(x-\alpha_i^q)$	$(x-\beta_1)(x-\beta_2)$	$2,1$	1
	$\prod_{i=1}^{3}(x-\alpha_i)(x-\alpha_i^q)$	1	$2,1$	1

(7) $n = 2, d = 2$
$h(x) = h_d(x)$

(n, d, g_0, e, S)	$h_d(x)$	$\deg h_1(x)$	c
$(2, 2, 1, 1, 6)$	$(x - \alpha_1)(x - \alpha_2)$	$2, 1$	η
$(2, 2, 1, 2, 7)$	$\prod_{i=1}^{3}(x - \alpha_i)$	$1, 0$	η
$(2, 2, 2, 1, 8)$	$\prod_{i=1}^{2}(x - \alpha_i)$	$4, 3$	η
$(2, 2, 2, 2, 9)$	$\prod_{i=1}^{3}(x - \alpha_i)$	$3, 2$	η

(n, d, g_0, e, S)	$h_d(x)$	$\deg h_1(x)$	c
$(2, 2, 2, 3, 10)$	$\prod_{i=1}^{4}(x - \alpha_i)$	$2, 1$	η
$(2, 2, 2, 4, 11)$	$\prod_{i=1}^{5}(x - \alpha_i)$	$2, 1$	η
$(2, 2, 3, 1, 10)$	$\prod_{i=1}^{2}(x - \alpha_i)$	$6, 5$	η
$(2, 2, 3, 2, 11)$	$\prod_{i=1}^{3}(x - \alpha_i)$	$5, 4$	η
$(2, 2, 3, 3, 12)$	$\prod_{i=1}^{4}(x - \alpha_i)$	$4, 3$	η
$(2, 2, 3, 4, 13)$	$\prod_{i=1}^{5}(x - \alpha_i)$	$3, 2$	η

B Classification for type (B): $^{\forall}d_i \neq d$

Here, $h_1(x) \in \mathbb{F}_q[x]$, $\eta := 1$ or a non-square element in $\mathbb{F}_{q^d}$.

$C_0/k_d : y^2 = c \cdot h(x)h_1(x)$
(1) $n = 6, d = 28 = 7 \cdot 4$, $\alpha \in \mathbb{F}_{q^7} \setminus \mathbb{F}_q, \beta \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$
Then $h(x) = h_7(x)h_4(x)$.

(n, d, g_0, e, S)	$h_7(x)$	$h_4(x)$	$\deg h_1(x)$	c
$(6, 28, 3, 61, 13)$	$(x - \alpha)(x - \alpha^q)(x - \alpha^{q^2})(x - \alpha^{q^4})$	$(x - \beta)(x - \beta^q)$	$2, 1$	η
	$(x - \alpha)(x - \alpha^{q^2})(x - \alpha^{q^3})(x - \alpha^{q^4})$	$(x - \beta)(x - \beta^q)$	$2, 1$	η

(2) $n = 5, d = 12 = 4 \cdot 3$, $\alpha \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}, \beta \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$
$h(x) = h_4(x)h_3(x)$

(n, d, g_0, e, S)	$h_4(x)$	$h_3(x)$	$\deg h_1(x)$	c
$(5, 12, 2, 17, 9)$	$(x - \alpha)(x - \alpha^q)$	$(x - \beta)(x - \beta^q)$	$2, 1$	η
$(5, 12, 3, 21, 11)$	$(x - \alpha)(x - \alpha^q)$	$(x - \beta)(x - \beta^q)$	$4, 3$	η

(3) $n = 5, d = 14 = 7 \cdot 2$, $\alpha \in \mathbb{F}_{q^7} \setminus \mathbb{F}_q, \beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\beta_i \in \mathbb{F}_{q^{d'}} \setminus \mathbb{F}_{q^{j'}}$ $(j' \mid_{\neq} d', 2 \mid d')$, $h_2(x) \in \mathbb{F}_{q^2}[x] \setminus \mathbb{F}_q[x]$
$h(x) = h_7(x)h_2(x)$

(n,d,g_0,e,S)	$h_7(x)$	$h_2(x)$	$\deg h_1(x)$	c
$(5,14,2,21,10)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$x-\beta$	$1,0$	η
	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$x-\beta$	$1,0$	η
$(5,14,3,23,12)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$x-\beta$	$3,2$	η
	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$x-\beta$	$3,2$	η
$(5,14,3,31,13)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$\prod_{i=1}^2(x-\beta_i)$	$2,1$	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
	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	$x-\beta$	$4,3$	η

$C_0/k_d : y^2 = c\cdot h(x)h_1(x)$
(4) $n=5, d=21=7\cdot 3,\ \alpha\in\mathbb{F}_{q^7}\setminus\mathbb{F}_q, \beta\in\mathbb{F}_{q^3}\setminus\mathbb{F}_q,\ \beta_i\in\mathbb{F}_{q^{d'}}\setminus\mathbb{F}_{q^{j'}}\ (j'\mid_{\neq} d', 3\mid d'),\ h_3(x)\in\mathbb{F}_{q^3}[x]\setminus\mathbb{F}_q[x]$
$h(x)=h_7(x)h_3(x)$

(n,d,g_0,e,S)	$h_7(x)$	$h_3(x)$	$\deg h_1(x)$	c
$(5,21,2,7,10)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	0	1
	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	0	1
$(5,21,3,2,12)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	$2,1$	1
	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	$(x-\beta)(x-\beta^q)$	$2,1$	1
$(5,21,3,10,13)$	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	$\prod_{i=1}^2(x-\beta_i)(x-\beta_i^q)$	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	1

(5) $n=4, d=6=3\cdot 2,\ \alpha\in\mathbb{F}_{q^3}\setminus\mathbb{F}_q,\ \alpha_i\in\mathbb{F}_{q^{d'}}\setminus\mathbb{F}_{q^{j'}}(j'\mid_{\neq} d', 3\mid d'),$ $\beta\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q,\ \beta_i\in\mathbb{F}_{q^{e'}}\setminus\mathbb{F}_{q^{l'}}\ (l'\mid_{\neq} e', 2\mid e'),\ h_3(x)\in\mathbb{F}_{q^3}[x]\setminus\mathbb{F}_q[x],\ h_2(x)\in\mathbb{F}_{q^2}[x]\setminus\mathbb{F}_q[x]$
$h(x)=h_3(x)h_2(x)$

(n,d,g_0,e,S)	$h_3(x)$	$h_2(x)$	$\deg h_1(x)$	c
$(4,6,1,3,6)$	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	0	η
$(4,6,2,5,8)$	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$3,2$	η
$(4,6,2,9,9)$	$x-\alpha$	$x-\beta$	$4,3$	η
	$\prod_{i=1}^2(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$1,0$	η
	$(x-\alpha)(x-\alpha^q)$	$\prod_{i=1}^2(x-\beta_i)$	$2,1$	η
$(4,6,3,7,10)$	$(x-\alpha)(x-\alpha^q)$	$x-\beta$	$5,4$	η
$(4,6,3,11,11)$	$x-\alpha$	$x-\beta$	$6,5$	η
	$\prod_{i=1}^2(x-\alpha_i)(x-\alpha_i^q)$	$x-\beta$	$3,2$	η
	$(x-\alpha)(x-\alpha^q)$	$\prod_{i=1}^2(x-\beta_i)$	$4,3$	η