A classification of elliptic curves with respect to the GHS attack in odd characteristic

Tsutomu Iijima * Fumiyuki Momose † Jinhui Chao ‡

2015/9/17

Abstract

The GHS attack is known to solve discrete logarithm problems (DLP) in the Jacobian of a curve C_0 defined over the d degree extension field k_d of $k := \mathbb{F}_q$ by mapping it to the DLP in the Jacobian of a covering curve C of C_0 over k. Recently, classifications for all elliptic curves and hyperelliptic curves C_0/k_d of genus 2,3 which possess $(2, ..., 2)$-covering C/k of $\mathbb{P}^1$ were shown under an isogeny condition (i.e. when $g(C) = d \cdot g(C_0)$). This paper presents a systematic classification procedure for hyperelliptic curves in the odd characteristic case. In particular, we show a complete classification of elliptic curves C_0 over k_d which have $(2, ..., 2)$-covering C/k of $\mathbb{P}^1$ for $d = 2, 3, 5, 7$. It has been reported by Diem[6] that the GHS attack fails for elliptic curves C_0 over odd characteristic definition field k_d with prime extension degree d greater than or equal to 11 since $g(C)$ become very large. Therefore, for elliptic curves over k_d with prime extension degree d, it is sufficient to analyze cases of $d = 2, 3, 5, 7$. As a result, a complete list of all elliptic curves C_0/k which possess $(2, ..., 2)$-covering C/k of $\mathbb{P}^1$ thus are subjected to the GHS attack with odd characteristic and prime extension degree d is obtained.

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

1 Introduction

Recently, attacks against cryptosystems defined over extension fields are under active research. On elliptic and hyperelliptic curves defined over extension fields $\mathbb{F}_{q^d}$, Gaudry [18] and Diem[9] showed algorithms to solve ECDLP

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

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

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

The first manuscript was uploaded to the cryptology e-print archive on August 11, 2015.

using Semaev's summation polynomials[37], which were then extended in [10] and also to plane curves[36]. These attacks were investigated further in [44][45][46]. Since these attacks are based on the properties of the extension fields as defining fields, they are generic attacks or all curves defined over such extension fields are subjected to the attacks. It was reported that under certain conditions it is possible to solve the ECDLP in subexponential time asymptotically. On the other hand, these attacks will be faster than Pollard's square-root algorithms only when the size of the definition field becomes very large[45].

Meanwhile, a much more powerful attack is known as the GHS attack which makes use of certain internal structure of elliptic and hyperelliptic curves defined over extension fields. Weil descent was firstly introduced by Frey[13] to elliptic curve cryptosystems. The idea was developed to the GHS attack by Gaudry, Hess, Smart[19]. The original GHS attack against elliptic curves has been extended to various classes of curves and generalized to the cover attack[8][11]. These attacks can be described as to compute the DLP in the Jacobian of a curve C_0 defined over the d degree extension field $k_d := \mathbb{F}_{q^d}$ of $k := \mathbb{F}_q$ by mapping it to the DLP in the Jacobian of a covering curve C of C_0 over k.

Analyses of the GHS attack until now were mainly based on genus analysis or evaluation of genus $g(C)$ of the covering curve C as a function of extension degree d of the definition field k_d of C_0. For characteristic two case, the genus $g(C)$ was analyzed in [19][30][31][22][23]. In particular, extension degrees within certain cryptographically useful range were investigated, and the extension fields over which $g(C)$ could be small are regarded as "weak fields". For odd characteristic, Diem[6] obtained a lower bound of genus $g(C)$ when C_0 are hyper-elliptic curves and showed that for elliptic curves C_0, $g(C)$ will be very large if $d \geq 11$ and d is a prime number.

On the other hand, these results by genus analysis do not guarantee but only assume the existence of the covering curve C. All curves C_0 defined on the weak fields are recommended to be avoid in cryptosystems despite that a curve could have and have not a covering.

In cryptographic applications, curves over extension fields with useful structure are often desirable to achieve high performance in implementation. Such curves include those over optimal extension fields(OEF), in the GLV method and GLS curves etc. For an example, the OEF are often used to obtain fast finite field arithmetic, since the extension degrees $d = 3, 5, 7$ are suitable for processors with 32 or 64 bit word length. In fact, when the extension degree d equals 3,5 or 7, it is still possible that there are elliptic curves C_0 defined over k_d which have no covering curves so will be secure against the GHS attack therefore usable in cryptosystems.

Therefore, problems still remained open e.g. which curves C_0/k_d are subjected to the GHS attacks and how many of them exist, or given a particular C_0, how to tell if the covering curve actually exists.

Researches for family of such weak curves started right after the proposal

of the GHS attack. In particular, special classes of curves which have covering so are subjected to the GHS attack have been reported in [19][15][42] [41][8][32][33][34]. For $d = 2, 3, 4, 5, 7$, Diem also showed examples for hyperelliptic curves of genus 1,2,3 which have covering[6][11].

A particularly interesting situation is when there exist a covering curve C/k of C_0/k_d and $\pi/k_d \ : \ C \ \twoheadrightarrow \ C_0$ such that

$$Res(\pi_*) \ : \ J(C) \rightarrow Res_{k_d/k} J(C_0) \tag{1}$$

defines an isogeny over k for $\pi_* \ : \ J(C) \ \twoheadrightarrow \ J(C_0)$, here $J(C)$ is the Jacobian variety of C and $Res_{k_d/k} J(C_0)$ is its Weil restriction. Then $g(C) = d \cdot g(C_0)$. This situation is called under the isogeny condition, which is the most favorable case for the GHS attack when $g(C)$ has the smallest possible size.

Such curves were found in [41] from 3 families of Kummer extensions which contain 4 classes of elliptic and hyperelliptic curves. In the table in [11] of C_0/k_d by Diem, there are 9 classes under the isogeny condition, among them 3 classes were in [41]. Recently, classifications for elliptic and hyperelliptic curves of genus 1,2,3 which possess $(2, ..., 2)$-covering of $\mathbb{P}^1$ under the isogeny condition were shown [21][28][32][33][34][38][39]. Density of such weak curves was also obtained for certain cases. For example, it turned out that more than a half of elliptic curves in Legendre form over odd characteristic cubic extension field and three quarters in the even characteristic case are subjected to the GHS attack[34][38][39]. Damage by the GHS attack to these curves are also serious. In fact, security of cryptosystems designed as 160bit key length will can be reduced to about 107bit key length.

Therefore, it is theoretically important and practically useful to have a complete list of all curves which have covering curves therefore are subjected to the GHS attack, in other words, to classify all these weak curves.

In order to answer the above question, we have to understand deeper properties of each curve and its covering curve, thus need approaches different from genus analysis. In this paper, we use Galois representation and ramification analysis to show a systematic procedure for classification of the elliptic/hyperelliptic curves over k_d with covering curves of $\mathbb{P}^1$ over k. In particular, we show a complete classification of elliptic curves C_0 over d degree extension field k_d which possess $(2, ..., 2)$-covering C/k of $\mathbb{P}^1$ in the case of $d = 2, 3, 5, 7$ in the section 5.

Since it has been proved by Diem[6] that elliptic curves C_0/k_d with prime $d \geq 11$ have huge $g(C)$ therefore are secure against the GHS attack, it is then sufficient to classify the elliptic curves C_0/k_d with covering C/k for $d = 2, 3, 5, 7$ in order to find all weak curves or to give a complete solution to the classification for odd characteristic with prime extension degrees. Therefore, the classification list in the section 5 provides a complete list of elliptic curves of odd characteristic with prime extension degrees subjected to the GHS attack. It turned out that there exist much more elliptic curves C_0/k_d which possess $(2, ..., 2)$-covering C/k than expected.

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

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

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

for elliptic curves in characteristic 2 case[19]. This attack has been extended to various classes of curves. It is also conceptually generalized to the cover attack by Frey and Diem[8][11]. When there exists an algebraic curve C/k and a covering $\pi/k_d : C \longrightarrow C_0$, the DLP in $J(C_0)(k_d)$ can be mapped to the DLP in $J(C)(k)$ by a pullback-norm map as in the following diagram.

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

Hereafter, we consider the following hyperelliptic curves over an extension field k_d in odd characteristic case given by

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

where $c \in k_d^{\times}$ and $f(x)$ is a monic polynomial in $k_d[x]$. Here, $C_0 \xrightarrow{2} \mathbb{P}^1(x)$ is a degree 2 covering over k_d. Then, C_0 has an n-tuple $\overbrace{(2, ..., 2)}^{n}$-covering C of $\mathbb{P}^1$ if C_0 has a covering. Thus, assume that C_0 has a $(2, ..., 2)$-covering C of $\mathbb{P}^1$. Here, a $(2, ..., 2)$-covering of $\mathbb{P}^1$ is defined as a covering $\pi/k_d : C \longrightarrow \mathbb{P}^1$ such that the covering group $\mathrm{cov}(C/\mathbb{P}^1) \cong \mathbb{F}_2^n$, where

$$\mathrm{cov}(C/\mathbb{P}^1) := \mathrm{Gal}(k_d(C)/k_d(x)). \tag{3}$$

In language of function fields, such a covering is a tower of extensions such that $k_d(x, y, {}^{\sigma^1}y, \ldots, {}^{\sigma^{n-1}}y) \cong k_d(C)$ is a $\overbrace{(2, ..., 2)}^{n}$ type extension with $n \leq d$.

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

In this section, we show general procedures to classify all curves C_0/k_d which possess the aforementioned $(2, ..., 2)$-covering C/k for given n, d. These procedures will output a complete list of such curves and their defining equations. The procedures will be applied to classify elliptic curves over k_d with prime extension degrees d of k in the next section.

3.1 Classification of Galois representation

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

$$\overbrace{\overbrace{(2,...,2)}^{n}}^{\overbrace{C \to \underbrace{C_0 \to \mathbb{P}^1(x)}_{2}}}} \tag{4}$$

In order to do that, we consider the Galois group $\mathrm{Gal}(k_d/k)$ acting on the covering group $\mathrm{cov}(C/\mathbb{P}^1) \cong \mathbb{F}_2^n$.

$$\begin{aligned} \mathrm{Gal}(k_d/k) \times \mathrm{cov}(C/\mathbb{P}^1) &\to \mathrm{cov}(C/\mathbb{P}^1) && (5)\\ (\sigma^i, \phi) &\mapsto {}^{\sigma^i}\phi := \sigma^i \phi \sigma^{-i} && (6) \end{aligned}$$

Here, one has an inclusion from $\mathrm{Gal}(k_d/k)$ into $\mathrm{Aut}(\mathrm{cov}(C/\mathbb{P}^1))$:

$$\mathrm{Gal}(k_d/k) \hookrightarrow \mathrm{Aut}(\mathrm{cov}(C/\mathbb{P}^1)) \cong GL_n(\mathbb{F}_2). \tag{7}$$

Hereafter, we use the same notation for σ and its representation. The representation of σ for given n and d has the following form in general :

$$\sigma = \begin{pmatrix} \Delta_1 & O & \cdots & O \\ O & \Delta_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \Delta_s \end{pmatrix} \begin{matrix} \}n_1 \\ \}n_2 \\ \\ \}n_s \end{matrix}, \ n = \sum_{i=1}^{s} n_i \tag{8}$$

where O stands for the zero matrix. The indecomposable subrepresentation

$$\Delta_i := \begin{pmatrix} \Omega_i & \Omega_i & \hat{O} & \cdots \\ \hat{O} & \Omega_i & \ddots & \ddots \\ \vdots & \ddots & \ddots & \Omega_i \\ \hat{O} & \cdots & \hat{O} & \Omega_i \end{pmatrix} \begin{matrix} \}n_i/l_i \\ \}n_i/l_i \\ \vdots \\ \}n_i/l_i \end{matrix} \tag{9}$$

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

Now, denote the minimal polynomial of σ as $F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x]$, one has $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots a_1\sigma + a_0$. The Galois action of $\mathrm{Gal}(k_d/k)$ on y can be expressed as

$${}^{\sigma^n}y \equiv \prod_{j=0}^{n-1} ({}^{\sigma^j}y)^{a_j} \qquad \mathrm{mod}\ k_d(x)^{\times}. \tag{10}$$

Therefore

$$^{\sigma^n}y^2 \equiv \prod_{j=0}^{n-1}(^{\sigma^j}y^2)^{a_j} \qquad \mod (k_d(x)^\times)^2. \tag{11}$$

As a result, the following necessary and sufficient condition is obtained for given n, d, σ :
C has a model over k_d if and only if

$$\begin{aligned} ^{F(\sigma)}y^2 &\equiv 1 \mod (k_d(x)^\times)^2 \quad \text{and} \\ ^{G(\sigma)}y^2 &\not\equiv 1 \mod (k_d(x)^\times)^2 \text{ for } {}^\forall G(x) \mid F(x), G(x) \neq F(x). \end{aligned} \tag{12}$$

In the rest of this paper, we assume (12) holds or C has a model over k_d.

Let S be the number of the ramification points $C/\mathbb{P}^1$ covering. By the Riemann-Hurwitz genus formula,

$$2g(C) - 2 = 2^n(-2) + 2^{n-1}S, \tag{13}$$

then

$$S = 4 + \frac{d \cdot g(C_0) + e - 1}{2^{n-2}}. \tag{14}$$

In general, we have to consider the following two types of Galois representations:

- Type A : ${}^\exists d_i \ s.t. \ d_i = d \ (= LCM\{d_i\})$
- Type B : $d_i \neq d$ for ${}^\forall d_i$

However, it turned out that only Type A appears in the cases of $d = 2, 3, 5, 7$. For these cases, the representations of σ are classified as follows :

- $d = 2, n = 2$
  $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{F}_2), \ F(x) = x^2 + 1$
- $d = 3, n = 3$
  $\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in M_3(\mathbb{F}_2), \ F(x) = (x+1)(x^2+x+1) = x^3 + 1$
- $d = 3, n = 2$
  $\sigma = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_2), \ F(x) = x^2 + x + 1$
- $d = 5, n = 5$
  $\sigma = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \Delta \end{pmatrix} \in M_5(\mathbb{F}_2), \ \Delta \in M_4(\mathbb{F}_2),$
  $F(x) = (x+1)(x^4 + x^3 + x^2 + x + 1) = x^5 + 1$

- $d = 5, n = 4$
  $\sigma = \begin{pmatrix} \Delta \end{pmatrix} \in M_4(\mathbb{F}_2),\ F(x) = x^4 + x^3 + x^2 + x + 1$
- $d = 7, n = 7$
  $\sigma = \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \Gamma_1 & O \\ \mathbf{0}^{\mathrm{T}} & O & \Gamma_2 \end{pmatrix} \in M_7(\mathbb{F}_2),\ \Gamma_1, \Gamma_2 \in M_3(\mathbb{F}_2),$
  $F(x) = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) = x^7 + 1$
- $d = 7, n = 6$
  $\sigma = \begin{pmatrix} \Gamma_1 & O \\ O & \Gamma_2 \end{pmatrix} \in M_6(\mathbb{F}_2),\ \Gamma_1, \Gamma_2 \in M_3(\mathbb{F}_2),$
  $F(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $d = 7, n = 4$
  $\sigma = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \Gamma_i \end{pmatrix} \in M_4(\mathbb{F}_2),\ \Gamma_1, \Gamma_2 \in M_3(\mathbb{F}_2),$
  $F(x) = (x+1)(x^3 + x + 1)$ or $(x+1)(x^3 + x^2 + 1)$
- $d = 7, n = 3$
  $\sigma = \begin{pmatrix} \Gamma_1 \end{pmatrix}$ or $\begin{pmatrix} \Gamma_2 \end{pmatrix} \in M_3(\mathbb{F}_2)$, then $F(x) = x^3 + x + 1$ or $x^3 + x^2 + 1$

This classification of Galois representation will be applied to classify elliptic curves over k_d with prime extension degree d in the section 4.

The situation when both Type A and Type B exist which involves composite extension degrees d will be reported later.

3.2 A condition for existence of C/k

Recall 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 $k_d[x]$, $F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x]$ is the minimal polynomial of σ. Thus $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$ since $F(\sigma) = 0$. Now, define $\hat{F}(x) \in \mathbb{F}_2[x]$ as a polynomial such that

$$x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]. \tag{15}$$

As mentioned previously, we assume that C is a model over k_d. Then, one has ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^{\times})^2$. Now, a model of C over k exists if and only if the extension σ of the Frobenius automorphism $\sigma_{k_d/k}$ is an automorphism of order d on $k_d(C)$ in the separable closure of $k_d(x)$. It is shown by Diem[6] that $\sigma_{k_d/k}$ extends to an automorphism of order d on the Galois closure of $k_d(C_0)/k(x)$ when C_0 is a hyperelliptic curve and d is odd in the odd characteristic case. Furthermore, this condition was generalized to all $d \geq 2$ in [28]. By using Lemma 6.1 in [28], we can determine $c \in k_d^{\times}$

as follows :

When $\hat{F}(1) = 0$, if c is a square in $k_d^\times$ then C has a model over k.
When $\hat{F}(1) = 1$, c can be either a square or a non-square in $k_d^\times$ in order that C has a model over k.

Example 3.1. *When* $d = 2, n = 2$,
$x^2 + 1 = (x + 1)^2$, $F(x) = (x + 1)^2, \hat{F}(x) = 1$.
Since $\hat{F}(x) = 1$, $\hat{F}(1) = 1$. *Therefore, c can be chosen as either* 1 *or a non-square in* $k_2^\times$ *and the curve C always has a model over k.*

Example 3.2. *When* $d = 3, n = 2$,
$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^2 + x + 1, \hat{F}(x) = x + 1$.
Since $\hat{F}(x) = x+1$, $\hat{F}(1) = 0$. *It follows that c needs to be a square* $c \in (k_3^\times)^2$ *(i.e.* $c = 1$*) for C to have a model over k.*

Example 3.3. *When* $d = 3, n = 3$,
$x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^3 + 1, \hat{F}(x) = 1$.
Since $\hat{F}(x) = 1$, $\hat{F}(1) = 1$. *c could be either* 1 *or a non-square in* $k_3^\times$ *and C always has a model over k.*

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

Recall that the condition ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$ and $\hat{F}(x) \in \mathbb{F}_2[x]$ is a polynomial such that $x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]$. We define the notation as follows:

$$b_i := 1 \quad \text{when there exists a ramification point } (\alpha^{q^i}, 0) \text{ on } C_0 \tag{16}$$
$$b_i := 0 \quad \text{otherwise for } i = 0, \ldots, d-1. \tag{17}$$

Here, α is either in k_d (i.e. $\alpha \in k_d \setminus k_v, v \mid_{\neq} d$) or in a 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 conjugates of α^{q^i} over k_d. Let $\Phi(x) := b_{d-1}x^{d-1} + \cdots + b_1 x + b_0$. Then $\Phi(x)$ defines a minimal Galois-invariant set of ramification points of $C_0/\mathbb{P}^1$ over k_d.

Now, since ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$, one has $F(x)\Phi(x) \equiv 0 \mod (x^d + 1)$. Then, $F(x)\Phi(x) \equiv 0 \mod (x^d + 1)$ if and only if $\Phi(x) \equiv 0 \mod \hat{F}(x)$. Therefore, for given d and n, it follows that

$$\Phi(x) \equiv a(x)\hat{F}(x) \mod (x^d + 1) \tag{18}$$

where there exists $a(x) \in \mathbb{F}_2[x]$ such that

$$GCD(a(x), F(x)) = 1 \text{ and } \deg a(x) < \deg F(x).$$

In fact, it can be proved that $\hat{F}(x)\mathbb{F}_2[x]/(x^d + 1) \cong \mathbb{F}_2[x]/(F(x))$. This suggests that one can find candidates of the ramification points of $C_0/\mathbb{P}^1$ if $a(x) \in \mathbb{F}_2[x]$ are determined for a given $\hat{F}(x) \in \mathbb{F}_2[x]$. Now, we intend to derive all candidates of the ramification points $\{(\alpha^{q^i}, 0) | b_i = 1\}$ on

C_0 for given d, n, σ. When d, n, σ are given, the minimal polynomial $F(x)$ of σ is determined as in the section 3.1. Thus, it is necessary to assume $GCD(F(x), a(x)) = 1$ in order to obtain $\Phi(x)$ for given d, n, σ.

Next, we define an equivalence such that $(b_0, b_1, \ldots, b_{d-1}) \sim (b_j, \ldots, b_{d-1}, b_0, \ldots, b_{j-1})$ or the $\Phi(x)$ with these coefficients are equivalent. In other words, equivalent $\Phi(x)$ have the coefficients invariant under cyclic permutations. Then all equivalent $\Phi(x)$'s belong to the same class of C_0.

Furthermore, $x^r a(x)\hat{F}(x) \equiv a(x)\hat{F}(x) \mod (x^d + 1)$ if and only if $x^r + 1 \equiv 0 \mod F(x)$ for $1 \leq r \leq d$. Thus, one has $r = d$. Therefore, the number of different $\Phi(x)$ in an equivalent class is $N := \#\{(\mathbb{F}_2[x]/(F(x)))^\times\}/d$. This means that one obtains all candidates of the ramification points of $C_0/\mathbb{P}^1$ if N different $\Phi(x)$'s are found such that they are not cyclic permutations of each other for given $\hat{F}(x)$.

From these facts, we obtain a procedure to derive all candidates of the ramification points $\{(\alpha^{q^i}, 0) | b_i = 1\}$ on C_0 for given d, n, σ.

Procedure 1:

1. Choose the polynomial $a(x) = 1$, then $\Phi(x) := \hat{F}(x)$ gives

   $$\left\{(\alpha^{q^i}, 0) \middle| \{0, ..., d-1\} \ni i \text{ s.t. } b_i = 1\right\}$$

   as a candidate of ramification points of $C_0/\mathbb{P}^1$.

   Here, α is either in $k_d \setminus k_v$ $(v|_{\neq} d)$ or in a certain extension $k_{d\tau} \setminus k_v$ $(v|_{\neq} d\tau, \tau \in \mathbb{N}_{>1})$ which happens only when $f(x)$ contains all conjugates of $\alpha^{q^i} \in k_{d\tau}$ over k_d. If $N = 1$, then this procedure is completed. If $N \geq 2$, then go to the next step.

2. Choose another polynomial $a(x) \in \mathbb{F}_2[x]$ such that $GCD(a(x), F(x)) = 1$ and $\deg a(x) < \deg F(x)$. Take $\Phi(x) := a(x)\hat{F}(x)$.

3. Check whether the coefficients of the new $\Phi(x)$ are cyclic permutation of those $\Phi(x)$'s obtained already (i.e. check whether $(b_0, b_1, \cdots, b_{d-1}) \sim (b_j, \cdots, b_{d-1}, b_0, \cdots, b_{j-1})$) for all obtained $\Phi(x)$'s. If yes, discard this $a(x)$. Go to step 2 again. If the new $\Phi(x)$ is not a cyclic permutation of any of the old ones, add $\{(\alpha^{q^i}, 0) | b_i = 1\}$ defined by $\Phi(x)$ to the candidates of the ramification points.

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

Example 3.4. *For $d = 2, n = 2$,*
$x^2 + 1 = (x + 1)^2$, $F(x) = (x + 1)^2, \hat{F}(x) = 1$.
Here, $N = 1$. Let $a(x) = 1$, then $\Phi(x) = a(x)\hat{F}(x) = 1$. Thus, there exists a candidate $(\alpha, 0)$ of ramification points on C_0.

Example 3.5. *For* $d = 3, n = 2$,
$x^3 + 1 = (x+1)(x^2+x+1), F(x) = x^2+x+1, \hat{F}(x) = x+1$.
Similarly, $N = 1$. *Let* $a(x) = 1$, *then* $\Phi(x) = x+1$. *Thus,* C_0 *has* $\{(\alpha, 0), (\alpha^q, 0)\}$ *as a candidate of ramification points.*

Example 3.6. *For* $d = 3, n = 3$,
$x^3 + 1 = (x+1)(x^2+x+1), F(x) = x^3+1, \hat{F}(x) = 1, N = 1$.
Choose $a(x) = 1$, *then* $\Phi(x) = 1$. *Consequently,* C_0 *has a candidate* $(\alpha, 0)$ *of ramification points.*

3.4 Defining equations of C_0

Finally, we show a procedure to find the equations of $C_0/k_d : y^2 = c \cdot f(x)$ with $(2, ..., 2)$-covering C/k of $\mathbb{P}^1$ for given $d, n, g(C_0), e$.

As mentioned previously, only Type (A) of Galois representations appears in the cases of $d = 2, 3, 5, 7$. In the following steps, we treat only Type (A).

Procedure 2:

1. Calculate $S = 4 + \frac{d \cdot g(C_0)+e-1}{2^{n-2}}$ for given $d, n, g(C_0), e$.
2. List up all the candidates of the ramification points of $C_0/\mathbb{P}^1$ by the Procedure 1 for all subrepresentations of σ except the trivial representation 1.
3. Take into account of $g(C_0)$ and S, find $f(x)$ from all combinations for candidates of ramification points which satisfy the condition ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$. Here $f(x)$ has to contain all conjugates $x - \alpha^{q^i}$ for every ramification points if we choose α in an extension field over k_d (i.e. $\alpha \in k_{d\tau} \setminus k_v$ where $v|_{\neq} d\tau$ and $\tau \in \mathbb{N}_{>1}$).
4. Determine $c \in k_d^\times$ so that C has a model over k as in the section 3.2.

In this way, one obtains all the defining equations of $C_0/k_d : y^2 = c \cdot f(x)$ with $(2, ..., 2)$-covering C/k of $\mathbb{P}^1$. The above operations will be explained in further details in the following section.

4 Classification of elliptic curves over k_d with prime extension degree d

Let S_0 be the number of the ramification points of $C_0/\mathbb{P}^1$.
By Abhyankar's lemma [40], one can find the upper bound of S as follows :

$$dS_0 \ \geq \ S = 4 + \frac{d \cdot g(C_0) + e - 1}{2^{n-2}} \geq max\{d, 2g(C_0) + 3\}. \tag{19}$$

Assume that $S_0 = 4$ since we treat elliptic curves C_0/k_d alone from this section.

4.1 Case $d = 2$

In this case, we have

$$8 \geq S = 4 + \frac{2 \cdot 1 + e - 1}{2^0} \geq 5 \ \text{ since } n = 2. \tag{20}$$

Therefore, e lies in the range of

$$3 \geq \ e \ \geq 0. \tag{21}$$

As an example, we consider the case of $e = 3$ below. By following the procedure to determine defining equations in the section 3.4, we obtain a class of elliptic curves

$$C_0/k_2 : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) \tag{22}$$

which has $(2, 2)$-covering C/k when $e = 3$.

The detailed steps of the Procedure 2 are shown as follows:

Example 4.1. $d = 2, n = 2, e = 3$

1. *From* $d = 2, n = 2, g(C_0) = 1, e = 3$, *one has* $S = 8$.

2. $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$*: indecomposable,* $F(x) = x^2 + 1, \hat{F}(x) = 1$.
   Now, $N = 1$. *Choose* $a(x) = 1$, *then* $\Phi(x) = a(x)\hat{F}(x) = 1$. *Thus, the ramification point of* $C_0/\mathbb{P}^1$ *takes the form of* $(\alpha, 0)$ *where* $\alpha \in k_2 \setminus k$ *or* $\alpha \in k_{2\tau} \setminus k_v$ $(v|_{\neq} 2\tau, \tau \in \mathbb{N}_{>1})$. *Notice that* $f(x)$ *contains all conjugates of* $\alpha \in k_{2\tau} \setminus k_v$ *over* k_2 *in the latter case.*

3. *For* $g(C_0) = 1$ *and* $S = 8$, *test all possibilities of* $f(x)$ *which has ramification points* $(\alpha, 0)$. *As a result, we obtain*

   $$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$$

   where $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ *are in the following five cases:*

   $$\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in k_2 \setminus k \ ; \tag{23}$$
   $$\alpha_1, \alpha_2 := \alpha_1^{q^2} \in k_4 \setminus k_2, \quad \alpha_3, \alpha_4 := \alpha_3^{q^2} \in k_4 \setminus k_2 \ ; \tag{24}$$
   $$\alpha_1, \alpha_2 := \alpha_1^{q^2} \in k_4 \setminus k_2, \quad \alpha_3, \alpha_4 \in k_2 \setminus k \ ; \tag{25}$$
   $$\alpha_1, \alpha_2 := \alpha_1^{q^2}, \alpha_3 := \alpha_1^{q^4} \in k_6 \setminus k_2 \cup k_3, \quad \alpha_4 \in k_2 \setminus k \ ; \tag{26}$$
   $$\alpha_1, \alpha_2 := \alpha_1^{q^2}, \alpha_3 := \alpha_1^{q^4}, \alpha_4 := \alpha_1^{q^6} \in k_8 \setminus k_4 \ . \tag{27}$$

4. *Since* $\hat{F}(1) = 1$, c *is a square in* $(k_2^{\times})^2$ *or 1.*

All defining equations for $d = 2$ including the above example can be found in the classification list of the section 5.

4.2 Case $d = 3$

From the classification of σ in the section 3.1, we know that only $n = 3$ or 2 are possible. Now, by (19), one has

$$14 \geq e \geq 0 \text{ when } n = 3,$$
$$6 \geq e \geq 0 \text{ when } n = 2.$$

Therefore, all values of possible e's are

$$e = 0, 2, 4, 6, 8, 10, 12, 14 \text{ when } n = 3,$$
$$e = 0, 1, 2, 3, 4, 5, 6 \text{ when } n = 2$$

since $S \in \mathbb{N}$.

As an example, we show the case of $n = 3$ and $e = 4$ below.

Example 4.2. $d = 3, n = 3, e = 4$

1. *One has* $S = 7$.
2. $\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & & \\ 0 & & \Delta \end{pmatrix}$, Δ *: indecomposable .*

   The minimal polynomial of σ *is* $F(x) = (x+1)(x^2+x+1) = x^3+1$, *then* $\hat{F}(x) = 1$. *Thus,* $N = 1$. *Choose* $a(x) = 1$, *then* $\Phi(x) = 1$. *Therefore, the only candidate of the ramification points of* $C_0/\mathbb{P}^1$ *is* $(\alpha, 0)$.

   Next, the minimal polynomial of the subrepresentation Δ *of* σ *is* $F(x) = x^2 + x + 1$, *then* $\hat{F}(x) = x + 1$. *As* $N = 1$, $\Phi(x) = x + 1$ *when* $a(x) = 1$. *Then* $C_0/\mathbb{P}^1$ *has* $\{(\alpha, 0), (\alpha^q, 0)\}$ *as the candidates of ramification points. Here,* $\alpha^{q^i} \in k_3 \setminus k$ *or* $\alpha^{q^i} \in k_{3\tau} \setminus k_v$ $(v|_{\neq 3\tau})$ *for* $b_i = 1$. *In the latter case it is necessary that* $f(x)$ *contains all conjugates of* $\alpha^{q^i} \in k_{3\tau}$ *over* k_3.

3. *From* $g(C_0) = 1$ *and* $S = 7$ *and the above candidates* $(\alpha, 0)$, $\{(\alpha, 0), (\alpha^q, 0)\}$, *we obtain* $f(x) = (x - \alpha_1)(x - \alpha_1^q)(x - \alpha_2)h_1(x)$ *where* $\alpha_1, \alpha_2 \in k_3 \setminus k$, $h_1(x) \in k[x]$, $\deg h_1(x) = 1$ or 0.
4. *Since* $\hat{F}(1) = 1$, $c \in k_3^\times$.

Consequently, the defining equation is obtained as $C_0/k_3 : y^2 = c(x - \alpha_1)(x - \alpha_1^q)(x - \alpha_2)h_1(x)$. In the same manner, we can treat also the case of $d = 3, n = 2$.

Remark 4.1. $d = 3, n = 2$

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

C_0 *has ramification points* $\{(\alpha, 0), (\alpha^q, 0)\}$. *Under the assumption* ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$, *we can find the equation* $f(x)$. *Then, we need to notice that* ${}^{\sigma^2+\sigma+1}h_1(x) \not\equiv 1 \mod (k_d(x)^\times)^2$ *when* $\deg h_1(x) \geq 1$.

Again, all results including the above example can be found in the classification list in the section 5.

4.3 Case $d = 5, 7$

Then, C_0 has the following candidates of ramification points on $\mathbb{P}^1$ when $g(C_0) = 1$.

- $d = 5, n = 5$
  $F(x) = x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1), \hat{F}(x) = 1$.
  The candidates of ramification points on $\mathbb{P}^1$ are as follows :
  $\{(\alpha, 0)\}, \{(\alpha, 0), (\alpha^q, 0), (\alpha^{q^2}, 0)\}, \{(\alpha, 0), (\alpha^q, 0), (\alpha^{q^3}, 0)\}$,
  and $\{(\alpha, 0), (\alpha^q, 0)\}, \{(\alpha, 0), (\alpha^{q^2}, 0)\}$ for the subrepresentation Δ of the section 3.1.

- $d = 5, n = 4$
  Similarly, $F(x) = x^4 + x^3 + x^2 + x + 1,\ \hat{F}(x) = x + 1$,
  $\{(\alpha, 0), (\alpha^q, 0)\}, \{(\alpha, 0), (\alpha^{q^2}, 0)\}, \{(\alpha, 0), (\alpha^q, 0), (\alpha^{q^2}, 0), (\alpha^{q^3}, 0)\}$.

- $d = 7, n = 7$
  $F(x) = x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1), \hat{F}(x) = 1$,
  $\{(\alpha, 0)\}, \{(\alpha, 0), (\alpha^{q^i}, 0), (\alpha^{q^j}, 0)\}$ where $(i, j) = (1, 2), (1, 4), (2, 4)$,
  and $\{(\alpha, 0), (\alpha^q, 0)\}, \{(\alpha, 0), (\alpha^{q^2}, 0)\}, \{(\alpha, 0), (\alpha^{q^3}, 0)\}, \{(\alpha, 0), (\alpha^{q^2}, 0), (\alpha^{q^3}, 0)\}$,
  $\{(\alpha, 0), (\alpha^q, 0), (\alpha^{q^3}, 0)\}$ for the subrepresentation of σ.

- $d = 7, n = 6$
  $F(x) = (x^3 + x + 1)(x^3 + x^2 + 1), \hat{F}(x) = x + 1$,
  $\{(\alpha, 0), (\alpha^q, 0)\}, \{(\alpha, 0), (\alpha^{q^2}, 0)\}, \{(\alpha, 0), (\alpha^{q^3}, 0)\}$,
  $\{(\alpha, 0), (\alpha^{q^i}, 0), (\alpha^{q^j}, 0), (\alpha^{q^\ell}, 0)\}$ where $(i, j, \ell) = (1, 2, 3), (1, 3, 4), (2, 4, 5)$.

- $d = 7, n = 4$
  In this case, σ have the following minimal polynomials :

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

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

  The candidates of the ramification points are :

  $(a)\ \{(\alpha, 0), (\alpha^{q^2}, 0), (\alpha^{q^3}, 0)\},\ (b)\ \{(\alpha, 0), (\alpha^q, 0), (\alpha^{q^3}, 0)\}$.

- $d = 7, n = 3$
  In the similar manner, the following candidates are obtained :

  (a) $F(x) = x^3 + x + 1,\ \hat{F}(x) = (x+1)(x^3 + x^2 + 1)$,
  $\{(\alpha, 0), (\alpha^q, 0), (\alpha^{q^2}, 0), (\alpha^{q^4}, 0)\}$

  (b) $F(x) = x^3 + x^2 + 1,\ \hat{F}(x) = (x+1)(x^3 + x + 1)$,
  $\{(\alpha, 0), (\alpha^{q^2}, 0), (\alpha^{q^3}, 0), (\alpha^{q^4}, 0)\}$

Here, $\alpha^{q^i} \in k_d \setminus k$ for $b_i = 1$ or $\alpha^{q^i} \in k_{d\tau} \setminus k_v$ $(v|_{\neq d\tau})$ when $f(x)$ contains all conjugate factors of $\alpha^{q^i} \in k_{d\tau}$ over k_d. We can then classify C_0/k_d from the above candidates for all possible e's in (19). All classification results for $d = 5, 7$ are listed in the section 5.

4.4 When d is a prime and $d \geq 11$

Until now, we have classified elliptic curves C_0 over k_d which possess $(2, ..., 2)$-covering C over k for $d = 2, 3, 5, 7$. In fact, even when $d \geq 11$, it is possible to classify elliptic curves C_0/k_d which possess covering curve C/k in the same way.

In [6], upper and lower bounds of $g(C)$ for elliptic curves C_0 over k_d had been obtained to show that $g(C)$ becomes so large that the GHS attack fails for prime extension degree $d \geq 11$. In particular, these bounds are for $d = 11$, $20481 \geq g(C) \geq 1793$, and for $d = 17$, $2097153 \geq g(C) \geq 833$, then the latter provides a lower bound for prime $d \geq 11$.

Below, we show examples for $d = 11, 17$ in which it is possible to calculate the upper and lower bounds of the $g(C)$ explicitly and in more details based on analysis of Galois representation.

For $d = 11$, since the polynomial factorization of $x^{11} + 1$ over $\mathbb{F}_2$ is

$$x^{11} + 1 = (x + 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1),$$

one knows that either $n = 10$ or 11. Then, by using (19), upper and the lower bounds of $g(C)$ are obtained as follows :

$$\begin{aligned} 20481 &\geq g(C) \geq 3585 \quad \text{for } n = 11, \\ 10241 &\geq g(C) \geq 1793 \quad \text{for } n = 10. \end{aligned}$$

For $d = 17$, from

$$x^{17} + 1 = (x + 1)(x^8 + x^5 + x^4 + x^3 + 1)(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1),$$

one knows that either $n = 9$ or $n = 8$. Therefore, when C exists, tighter upper and lower bounds of $g(C)$ are obtained by (19) as follows :

$$\begin{aligned} 8193 &\geq g(C) \geq 1665 \quad \text{for } n = 9, \\ 4097 &\geq g(C) \geq 833 \quad \text{for } n = 8. \end{aligned}$$

5 List of classification

Let $C_0/k_d : y^2 = c \cdot h_d(x)h_1(x)$ where $h_d(x) \in k_d[x] \setminus k[x]$, $h_1(x) \in k[x]$. η denotes 1 or a non-square in $k_d^\times$.

We present a list of complete classification for elliptic curves C_0/k_d with (2,...,2)-covering C/k. Classes of such curves are referred as Cases. Explanations on marks in the list are follows :

1. "References" in the line of a Case cites the papers where the curves have been found before, while Cases with blank spaces are newly found in this paper.

2. Marks $*$ in "Remark" indicates that there are more than one possibility for α_i. For Cases without the mark $*$ in "Remark", $\alpha_i \in k_d \setminus k$. For Cases with the mark $*$ in "Remark", either $\alpha_i \in k_d \setminus k$ or $\alpha_i \in k_{d\tau} \setminus k_v$ ($v|_{\neq} d\tau, \tau \in \mathbb{N}_{>1}$) where the latter happens only when $h_d(x)$ contains all conjugate factors of $\alpha^{q^i} \in k_{d\tau}$ over k_d.

   For Cases with the mark $*$ in "Remark", all possibilities of α_i's are as follows :

   Case 2 $d = 2, n = 2, e = 1$
   $\alpha_1, \alpha_2 \in k_2 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^2} \in k_4 \setminus k_2$.

   Case 3 $d = 2, n = 2, e = 2$
   $\alpha_1, \alpha_2, \alpha_3 \in k_2 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^2} \in k_4 \setminus k_2, \quad \alpha_3 \in k_2 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^2}, \alpha_3 := \alpha_1^{q^4} \in k_6 \setminus k_2 \cup k_3$.

   Case 4 $d = 2, n = 2, e = 3$
   $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in k_2 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^2} \in k_4 \setminus k_2, \quad \alpha_3, \alpha_4 := \alpha_3^{q^2} \in k_4 \setminus k_2$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^2} \in k_4 \setminus k_2, \quad \alpha_3, \alpha_4 \in k_2 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^2}, \alpha_3 := \alpha_1^{q^4} \in k_6 \setminus k_2 \cup k_3, \quad \alpha_4 \in k_2 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^2}, \alpha_3 := \alpha_1^{q^4}, \alpha_4 := \alpha_1^{q^6} \in k_8 \setminus k_4$.

   Case 5 $d = 3, n = 2, e = 0$
   $\alpha_1, \alpha_2 \in k_3 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^3} \in k_6 \setminus k_2 \cup k_3$.

   Case 9 $d = 3, n = 3, e = 6$
   $\alpha_1, \alpha_2 \in k_3 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^3} \in k_6 \setminus k_2 \cup k_3$.

   Case 10 $d = 3, n = 3, e = 8$
   $\alpha_1, \alpha_2, \alpha_3 \in k_3 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^3} \in k_6 \setminus k_2 \cup k_3, \quad \alpha_3 \in k_3 \setminus k$.

   Case 11 $d = 3, n = 3, e = 10$
   $\alpha_1, \alpha_2, \alpha_3 \in k_3 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^3} \in k_6 \setminus k_2 \cup k_3, \quad \alpha_3 \in k_3 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^3}, \alpha_3 := \alpha_1^{q^6} \in k_9 \setminus k_3$.

   Case 12 $d = 3, n = 3, e = 14$
   $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in k_3 \setminus k$;
   $\alpha_1, \alpha_2 := \alpha_1^{q^3} \in k_6 \setminus k_2 \cup k_3, \quad \alpha_3, \alpha_4 := \alpha_3^{q^3} \in k_6 \setminus k_2 \cup k_3$;

$\alpha_1, \alpha_2 := \alpha_1^{q^3} \in k_6 \setminus k_2 \cup k_3, \quad \alpha_3, \alpha_4 \in k_3 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^3}, \alpha_3 := \alpha_1^{q^6} \in k_9 \setminus k_3, \quad \alpha_4 \in k_3 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^3}, \alpha_3 := \alpha_1^{q^6}, \alpha_4 := \alpha_1^{q^9} \in k_{12} \setminus k_4 \cup k_6$.

Case 14 $d = 5, n = 4, e = 20$
$\alpha_1, \alpha_2 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5} \in k_{10} \setminus k_2 \cup k_5$.
Case 20 $d = 5, n = 5, e = 60$
$\alpha_1, \alpha_2 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5} \in k_{10} \setminus k_2 \cup k_5$.
Case 21 $d = 5, n = 5, e = 84$
$\alpha_1, \alpha_2, \alpha_3 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5} \in k_{10} \setminus k_2 \cup k_5, \quad \alpha_3 \in k_5 \setminus k$.
Case 22 $d = 5, n = 5, e = 92$
$\alpha_1, \alpha_2, \alpha_3 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5} \in k_{10} \setminus k_2 \cup k_5, \quad \alpha_3 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5}, \alpha_3 := \alpha_1^{q^{10}} \in k_{15} \setminus k_3 \cup k_5$.
Case 23 $d = 5, n = 5, e = 124$
$\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5} \in k_{10} \setminus k_2 \cup k_5, \quad \alpha_3, \alpha_4 := \alpha_3^{q^5} \in k_{10} \setminus k_2 \cup k_5$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5} \in k_{10} \setminus k_2 \cup k_5, \quad \alpha_3, \alpha_4 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5}, \alpha_3 := \alpha_1^{q^{10}} \in k_{15} \setminus k_3 \cup k_5, \quad \alpha_4 \in k_5 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^5}, \alpha_3 := \alpha_1^{q^{10}}, \alpha_4 := \alpha_1^{q^{15}} \in k_{20} \setminus k_4 \cup k_5$.

Case 27 $d = 7, n = 6, e = 154$
$\alpha_1, \alpha_2 \in k_7 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7} \in k_{14} \setminus k_2 \cup k_7$.
Case 33 $d = 7, n = 7, e = 378$
$\alpha_1, \alpha_2 \in k_7 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7} \in k_{14} \setminus k_2 \cup k_7$.
Case 34 $d = 7, n = 7, e = 538$
$\alpha_1, \alpha_2, \alpha_3 \in k_7 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7} \in k_{14} \setminus k_2 \cup k_7, \quad \alpha_3 \in k_7 \setminus k$.
Case 35 $d = 7, n = 7, e = 570$
$\alpha_1, \alpha_2, \alpha_3 \in k_7 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7} \in k_{14} \setminus k_2 \cup k_7, \quad \alpha_3 \in k_7 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7}, \alpha_3 := \alpha_1^{q^{14}} \in k_{21} \setminus k_3 \cup k_7$.
Case 36 $d = 7, n = 7, e = 762$
$\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in k_7 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7} \in k_{14} \setminus k_2 \cup k_7, \quad \alpha_3, \alpha_4 := \alpha_3^{q^7} \in k_{14} \setminus k_2 \cup k_7$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7} \in k_{14} \setminus k_2 \cup k_7, \quad \alpha_3, \alpha_4 \in k_7 \setminus k$;
$\alpha_1, \alpha_2 := \alpha_1^{q^7}, \alpha_3 := \alpha_1^{q^{14}} \in k_{21} \setminus k_3 \cup k_7, \quad \alpha_4 \in k_7 \setminus k$;

$$\alpha_1, \alpha_2 := \alpha_1^{q^7}, \alpha_3 := \alpha_1^{q^{14}}, \alpha_4 := \alpha_1^{q^{21}} \in k_{28} \setminus k_4 \cup k_7 \ .$$

3. Mark † in "Remark" of a Case indicates that it does not include certain its subcases, all of which are explained as follows:

   • Case 9 does not include Case 6.
   • Case 10 does not include Case 5.
   • Case 11 does not include Case 8.
   • Case 12 does not include Case 5 and Case 10.

   • Case 14 does not include Case 13.
   • Case 18 does not include Case 13 and Case 14.
   • Case 19 does not include Case 15.
   • Case 21 does not include Case 13, Case 14, and Case 18.
   • Case 22 does not include Case 15 and Case 19.
   • Case 23 does not include Case 13, Case 14, Case 18, and Case 21.

   • Case 27 does not include Case 24 and Case 26.
   • Case 31 does not include Case 24, Case 26, and Case 27.
   • Case 32 does not include Case 25 and Case 28.
   • Case 33 does not include Case 29.
   • Case 34 does not include Case 24, Case 26, Case 27, and Case 31.
   • Case 35 does not include Case 25, Case 28, and Case 32.
   • Case 36 does not include Case 24, Case 26, Case 27, Case 31, and Case 34.

$$C_0/k_d : y^2 = c \cdot f(x) := c \cdot h_d(x)h_1(x),\ h_d(x) \in k_d[x] \setminus k[x]\ ,\ h_1(x) \in k[x]$$

Case	d	n	e	$g(C)$	c	$h_d(x)$	$\deg h_1(x)$	Remark	Reference
1	2	2	0	2	η	$x-\alpha$	3 , 2		[11][28][41]
2	2	2	1	3	η	$(x-\alpha_1)(x-\alpha_2)$	2 , 1	$*$	
3	2	2	2	4	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$	1 , 0	$*$	
4	2	2	3	5	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$	0	$*$	
5	3	2	0	3	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$	0	$*$	[6][11][28]
6	3	3	0	3	η	$(x-\alpha)(x-\alpha^q)$	2 , 1		[28][41]
7	3	3	2	5	η	$(x-\alpha)$	3 , 2		[41]
8	3	3	4	7	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)$	1 , 0		
9	3	3	6	9	η	$(x-\alpha_1)(x-\alpha_2)$	2 , 1	$*$ †	
10	3	3	8	11	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^q)$	0	$*$ †	
11	3	3	10	13	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$	1 , 0	$*$ †	
12	3	3	14	17	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$	0	$*$ †	
13	5	4	0	5	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$	0		[6][11][28]
14	5	4	20	25	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$	0	$*$ †	
					1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^{q^2})$	0		
					1	$(x-\alpha_1)(x-\alpha_1^{q^2})(x-\alpha_2)(x-\alpha_2^{q^2})$	0	$*$ †	
15	5	5	12	17	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	1 , 0		
					η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	1 , 0		
16	5	5	20	25	η	$(x-\alpha)(x-\alpha^q)$,	2 , 1		
					η	$(x-\alpha)(x-\alpha^{q^2})$	2 , 1		
17	5	5	28	33	η	$(x-\alpha)$	3 , 2		
18	5	5	44	49	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^2})$	0	†	
					η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^3})$	0	†	
19	5	5	52	57	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)$	1 , 0	†	
					η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^{q^2})$	1 , 0	†	
20	5	5	60	65	η	$(x-\alpha_1)(x-\alpha_2)$	2 , 1	$*$	
21	5	5	84	89	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^q)$	0	$*$ †	
					η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^{q^2})$	0	$*$ †	
22	5	5	92	97	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$	1 , 0	$*$ †	
23	5	5	124	129	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$	0	$*$ †	
24	7	3	0	7	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$	0		[6][11][28]
					1	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})(x-\alpha^{q^4})$	0		[28]
25	7	4	10	17	η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})$	1 , 0		
					η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})$	1 , 0		
26	7	6	42	49	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$	0		
					1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^3})(x-\alpha^{q^4})$	0		
					1	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^4})(x-\alpha^{q^5})$	0		

$$C_0/k_d : y^2 = c \cdot f(x) := c \cdot h_d(x)h_1(x),\ h_d(x) \in k_d[x] \setminus k[x]\ ,\ h_1(x) \in k[x]$$

Case	d	n	e	$g(C)$	c	$h_d(x)$	$\deg h_1(x)$	Remark	Reference
27	7	6	154	161	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$	0	$*$ †	
					1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^{q^2})$	0	†	
					1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^{q^3})$	0	†	
					1	$(x-\alpha_1)(x-\alpha_1^{q^2})(x-\alpha_2)(x-\alpha_2^{q^2})$	0	$*$ †	
					1	$(x-\alpha_1)(x-\alpha_1^{q^2})(x-\alpha_2)(x-\alpha_2^{q^3})$	0	†	
					1	$(x-\alpha_1)(x-\alpha_1^{q^3})(x-\alpha_2)(x-\alpha_2^{q^3})$	0	$*$ †	
28	7	7	122	129	η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$	1 , 0		
					η	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^4})$	1 , 0		
					η	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^4})$	1 , 0		
29	7	7	154	161	η	$(x-\alpha)(x-\alpha^{q^i}),\ i=1,2,3$	2 , 1		
30	7	7	186	193	η	$x-\alpha$	3 , 2		
31	7	7	314	321	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^2})$	0	†	
					η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^4})$	0	†	
					η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^{q^2})(x-\alpha_2^{q^4})$	0	†	
					η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^{q^2})(x-\alpha_2^{q^3})$	0	†	
					η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^3})$	0	†	
32	7	7	346	353	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^{q^i})$ $i=1,2,3$	1 , 0	†	
33	7	7	378	385	η	$(x-\alpha_1)(x-\alpha_2)$	2 , 1	$*$ †	
34	7	7	538	545	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^{q^i})$ $i=1,2,3$	0	$*$ †	
35	7	7	570	577	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$	1 , 0	$*$ †	
36	7	7	762	769	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$	0	$*$ †	

6 Conclusions

In this paper, we have shown procedures for classification of hyperelliptic curves C_0/k_d with $(2,...,2)$-covering C/k. By application of the procedures, we obtained a complete list of all elliptic curves C_0/k_d which posses $(2,...,2)$-covering C/k with respect to the GHS attack of odd characteristic and prime extension degree d. It is found out that the number of elliptic curves C_0/k_d with $(2,...,2)$-covering C/k is much larger than was expected from the classes of weak curves discovered until now. Meanwhile, when the extension degree d increased, there are more of elliptic curves C_0/k_d possess covering curves C with larger genera $g(C)$ which affirm prediction based on known analysis results.

Future research on security of elliptic curve-based cryptosystems against the GHS attack include isomorphism and isogeny analysis between curves

and investigation on implementation and computational complexities on covering curves.

Acknowledgements

The authors would like to thank for helpful comments and supports of Takayuki Hosogaya and Prof. Mahoro Shimura.

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] I. Blake, G. Seroussi, and N. Smart, "Advances in elliptic curve cryptography," Cambridge Univ Press, 2005.

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

[5] H. Cohen, G. Frey et al., "Handbook of elliptic and hyperelliptic curve cryptography," Chapman & Hall/CRC, 2005.

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

[7] 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

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

[9] C. Diem, "On the discrete logarithm problem in elliptic curves", Compositio Mathematica 147, pp75-104, 2011

[10] C. Diem, "On the discrete logarithm problem in elliptic curves II", Algebra & Number Theory 7, pp.1281-1323, 2013

[11] C. Diem and J. Sholten, "cover attack," preprint, 2003. Available from http://www.math.uni-leipzig.de/ diem/preprints/english.html

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

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

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

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

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.

[21] 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

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

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

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

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

[30] 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.

[31] A. Menezes, E. Teske, and A. Weng "Weak fields for ECC," Topics in Cryptology CT-RSA 2004, Springer-Verlag, LNCS2964 , pp.366–386, 2004.

[32] 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

[33] 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

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

[35] 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

[36] K. Nagao, "Decomposition formula of the Jacobian group of plane curve", preprint, 2013, Available from http://eprint.iacr.org/2013/548

[37] I. Semaev, "Summation polynomials and the discrete logarithm problem on elliptic curves", preprint, 2004. Available from http://eprint.iacr.org/2004/031

[38] 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.

[39] 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.

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

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

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

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

[44] J.C.Faugère, L.Perret, C.Petit, and G.Renault, "Improving the complexity of index calculus algorithms in elliptic curves over binary field," Advances in Cryptology-EUROCRYPTO 2012, Springer-Verlag, LNCS 7237, pp.27–44, 2012.

[45] C.Petit nad J.J.Quisquater, "On polynomial systems arising from a Weil descent," Advances in Cryptology-ASIACRYPTO 2012, Springer-Verlag, LNCS 7658, pp.451–466, 2012.

[46] M.Shantz and E.Teske, "Solving the elliptic curve discrete logarithm problem using Semaev polynomials, Weil descent and Gröbner basis methods - an experimental study," Number Theory and Cryptography, Springer-Verlag, LNCS 8260, pp.94–107, 2013.