2005－ＣＳＥＣ－30（８）
2005／7／21

Superelliptic curve と C_{ab} curve を用いた暗号系の GHS Weil Descent 攻撃に対する安全性

飯島　努[†]　志村　真帆呂[†]　趙　晋輝[†]　辻井　重男[††]

† 中央大学
〒 112-8551 東京都文京区春日 1-13-27
†† 情報セキュリティ大学院大学
〒 221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
E-mail: †tiijima@chao.ise.chuo-u.ac.jp

あらまし　GHS Weil descent attack は、Gaudry, Hess, Smart によって標数２の楕円曲線暗号に対して構成された攻撃法である。本論文では、最初に曲線の代数関数体が有理関数体上 Galois 拡大となっている場合について、Weil restriction された関数体の正規性とその存在を述べる。特に Tame Galois 拡大となっているような C_{ab} curve と Tame 巡回拡大（これは superelliptic curve を含む）に対して、その genus の下界を与える。更にこれらの結果を superelliptic curve と genus が４または３の Tame Galois 拡大になる C_{ab} curve に適用し（a が素数の場合には、いつも Tame 巡回拡大として扱うことができるので、a が素数でない genus 4 または３の C_{ab} curve としては、C_{92} curve と C_{43} curve の２つのみである。）、Pollard の ρ 法・Gaudry のアルゴリズム・Adleman-DeMarrais-Huang アルゴリズムの計算量を比較することで GHS Weil descent 攻撃の有効性を考察する。

キーワード　GHS Weil descent 攻撃, superelliptic curve, C_{ab} curve, 代数関数体, Pollard の ρ 法, Gaudry のアルゴリズム, Adleman-DeMarrais-Huang アルゴリズム

On Security of Superelliptic Curves and C_{ab} Curves Based Cryptosystems against GHS Weil Descent Attack

Tsutomu IIJIMA[†], Mahoro SHIMURA[†], Jinhui CHAO[†], and Shigeo TSUJII[††]

† Chuo University
1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan
†† Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-shi, Kanagawa, 221-0835 Japan
E-mail: †tiijima@chao.ise.chuo-u.ac.jp

Abstract　The GHS Weil descent attack by Gaudry, Hess and Smart was originally proposed to elliptic curves over finite fields of characteristic two. In this paper, we consider GHS Weil descent attacks to algebraic curves whose function fields are Galois extensions of the rational function field. Lower bounds of genera of the function fields of their Weil restrictions are obtained when the function fields of the curves are tame Galois extensions. This class of curves can be divided into cyclic Galois extensions which contain superelliptic curves as a special case and non-cyclic Galois extensions which contain C_{ab} curves. If we restrict ourselves to genus four or three cases, there are only two such C_{ab} curves: C_{92}, C_{43}. Therefore, a detailed analysis on security against such attacks is shown for cryptosystems based on superelliptic curves and on C_{92}, C_{43}, Such analysis is based on the above theoretical results and computational complexity comparisons between Pollard's rho algorithm, Gaudry's variant of the ADH algorithm and Gaudry-Enge version of the ADH algorithm.

Key words　GHS Weil descent attack, superelliptic curves, C_{ab} curves, function fields, Pollard's rho algorithm, Gaudry's algorithm, Adleman-DeMarrais-Huang algorithm

1. Introduction

It was Frey who first suggested application of Weil descent to elliptic curve based cryptosystems [7]. Gaudry, Hess and Smart developed this idea to show the so-called GHS Weil descent attack [12]. In this algorithm, a hyperelliptic curve is constructed by the Weil restriction of an elliptic curve over a finite field of characteristic two and with a composite extension degree. This hyperelliptic curve is defined over a smaller definition field (a subfield of the original definition field) and has a bigger genus comparing with the original curve. The elliptic curve discrete logarithm problem (ECDLP) is then transformed to a hyperelliptic curve discrete logarithm problem (HECDLP) over the subfield, and finally the HECDLP is attacked by using e.g. Gaudry's variant [11] of the Adleman-DeMarrais-Huang algorithm [1].

The GHS Weil descent attack has been generalized by many researchers, and security against these attacks has been also discussed. For example, it was extended by Galbraith to certain classes of hyperelliptic curves over characteristic two [9], and by Arita to some elliptic curves over finite fields of characteristic three [2]. Diem generalized the GHS Weil descent attack to hyperelliptic curves over finite fields of arbitrary odd characteristics [5]. Recently, Diem's results are extended to several classes of both superelliptic curves and Artin-Schreier curves by Thériault [27] [28]. Besides, Hess generalized the GHS Weil descent attack to arbitrary Artin-Schreier extensions [14] [15]. Furthermore, a part of Diem's results were extended to algebraic fields whose function fields are cyclic Galois extensions [17].

In this paper, we first show a framework and algebraic structure for the GHS Weil descent attacks to algebraic curves whose function fields are Galois extensions of the rational function field. In fact, the curves with tame Galois function fields can be divided into cyclic and non-cyclic cases, corresponding to two important classes: superelliptic curves and C_{ab} curves, both have been used in cryptosystems [3] [10] [13]. The superelliptic curves are special cases of tame cyclic Galois extensions. For C_{ab} curves which belong to non-cyclic cases, if we restrict ourselves to genus four or three curves used in cryptosystems, there are only two such curves: C_{92} and C_{43}. Therefore, based on algebraic properties obtained in the next section, we evaluated genera, particularly their lower bounds, of the function fields of the Weil restrictions for curves with tame Galois function fields for both cyclic and non-cyclic cases. Non-Galois cases are also discussed in section 3. Furthermore, a detailed analysis on security against Weil descent attacks is shown for cryptosystems based on superelliptic curves and C_{92}, C_{43}. Such an analysis is based on the above theoretical results and comparisons of computational complexities between Pollard's rho algorithm to the original curve, the Gaudry-Enge version of the ADH algorithm and Gaudry's variant of the ADH algorithm to its Weil restriction. In particular, we showed classes of superelliptic curves and C_{92}, C_{43} curves which are safe against GHS Weil descent attack and also certain classes which should be avoided.

Through this paper we assume that $K = \mathbf{F}_{q^n}, k = \mathbf{F}_q$ $(n \neq 1)$ are finite fields, q is a power of a prime number, x is transcendental over K, $K(x)^{sep}$ is the separable closure of $K(x)$.

2. GHS Weil Descent Attack to Curves with Galois Function Fields

Bellow, we show a framework and consider its algebraic properties of the GHS Weil descent attack on algebraic curves whose function fields are Galois extensions of rational function fields, which is a generalization of GHS Weil descent attack.

Let L be a degree a Galois extension field of $K(x)$. Let $Cl^0(L)$ be the class group of the degree 0 divisors of L, $\sigma_{K/k}$ the Frobenius automorphism of K over k. $\sigma_{K/k}$ is extended to an automorphism $\bar{\sigma}_{K/k}$ of $K(x)^{sep}$. Consider the Galois closure of $L/k(x)$:

$$F' := L \cdot \bar{\sigma}_{K/k}(L) \cdots \bar{\sigma}_{K/k}^{n-1}(L). \qquad (1)$$

If $\gcd(n, a) = 1$, then $\sigma_{K/k}$ can be extended to an automorphism of $F'/k(x)$ such that its order is n.. Then, consider the fixed field of F' by the automorphism $\bar{\sigma}_{K/k}$:

$$F := \{\alpha \in F' \mid \bar{\sigma}_{K/k}(\alpha) = \alpha\}. \qquad (2)$$

Moreover, the following mapping can be constructed as the composition of conorm and norm maps [4] [26]:

$$N_{F'/F} \circ Con_{F'/L} : Cl^0(L) \longrightarrow Cl^0(F). \qquad (3)$$

This map will be called the GHS conorm-norm homomorphism as in the elliptic curve case [12]. In particular, if L is a prime order cyclic extension and there exists no intermediate field μ of K/k such that $\mu \subsetneq K$ and $L/\mu(x)$ is Galois, then a large prime order subgroup of $\#Cl^0(L)$ (therefore the DLP over $Cl^0(L)$) is preserved by the GHS conorm-norm homomorphism [17]. Thus, if a new curve is constructed by Weil restriction of the original curve over a finite field K/k, then the DLP over $Cl^0(L)$ is transformed to the DLP over $Cl^0(F)$. The new curve is defined over a smaller definition field k and it has a genus bigger than the original curve.

Now $[F' : K(x)] = \prod_{i=1}^{m} a_i$ $(1 \leqq {}^{\exists}m \leqq n, {}^{\exists}a_i \mid a,\ a_i > 1)$, and F' is regular over $\tilde{K}$ as $\tilde{K} := F' \cap \overline{K}$. We obtain the following results for $\bar{\sigma}_{K/k}$ and F'.

[Lemma 1] If $\gcd(n, a) = 1$, then the Frobenius automorphism $\sigma_{K/k}$ on $K(x)$ can be extended to an automorphism

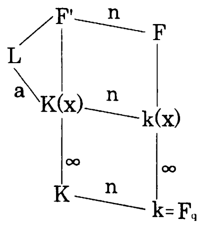

Fig. 1 Diagram of Fields

of $F'/k(x)$ of order n, and all such extensions are conjugate to each other in $\mathrm{Gal}(F'/k(x))$.

Proof) Similar to proof in [17]. □

Furthermore, existence and properties of the fixed field F of F' by $\bar{\sigma}_{K/k}$ is given in the following proposition.

[Proposition 1] If $\gcd(n, a) = 1$. Then either of the following statements hold:

- If F' is regular over K, then there exists a subextension F of $F'/k(x)$ such that it is regular over k and $KF = F'$;
- Otherwise, then F' is regular over $\tilde{K} \supsetneq K$, ${}^{\exists}\lambda \supsetneq k$ such that $\lambda K = \tilde{K}$. Further, there exists a subextension $F/\lambda(x)$ of $F'/\lambda(x)$ such that it is regular over λ and $\lambda KF = KF = F'$.

In both cases, all subextensions defined in such a way are isomorphic to each other.

Proof) Similar to proof in [17]. □

Notice that K is algebraically closed in the field F' if and only if F' is regular over K since k is a perfect field. Thus existence and regularity of the subfield F of F' were guaranteed by the above theorem. By using these properties of such constant field extensions, we can analyze genera of function fields F in the next section.

3. Genera of Function Fields F

3.1 The Case of Tame Cyclic Extensions

In this section, suppose that tame cyclic extensions $L := K(C) = K(x, y)$ is defined by the following equation

$$C : y^a = f(x) := c\prod_{i=1}^{s} p_i(x)^{l_i} \tag{4}$$

where $f(x)$ is factorized into $s(> 0)$ pairwisely distinct irreducible monic polynomials $p_i(x) \in K[x]$ such that $K \ni c \neq 0, \mathbf{Z} \ni l_i \neq 0$. We will assume $a \mid q-1$, $gcd(a, l_i) = 1$ for $1 \leqq i \leqq s$. $a \mid q-1$ implies that k contains a primitive a-th root of unity and $\gcd(\mathrm{char}(k), a) = 1$.

[Proposition 2] [26, p.196]

- K is the full constant field of L, $[L : K(x)] = a$, and $L/K(x)$ is cyclic.
- Let P_i(resp. P_∞) denote the zero of $p_i(x)$ (resp. the pole of x) in $K(x)$. The places $P_1, \cdots, P_s$ are totally ramified in $L/K(x)$. All places $Q_\infty \in \mathbb{P}_L$ with $Q_\infty \mid P_\infty$ have the ramification index $e(Q_\infty \mid P_\infty) = a/d$ where $d := \gcd(a, \Sigma_{i=1}^{s} l_i \deg p_i(x))$.
- No places $P \in \mathbb{P}_{K(x)}$ other than $P_1, \cdots, P_s, P_\infty$ ramify in $L/K(x)$.
- The genus of L/K is $g = \frac{a-1}{2}\left(\sum_{i=1}^{s} \deg p_i(x) - 1\right) - \frac{d-1}{2}$. □

If $\gcd(n, a) = 1$, then the following lower bound of $g(F)$ is obtained.

[Theorem 1] Assume $d = 1$ or a. Define $\alpha := 0$ for d =a, $\alpha := 1$ for $d = 1$. Applying the GHS Weil descent attack to the above tame cyclic extension field $L/K(x)$, the resulting function field F has the following properties.

Let $n := \prod_{p:prime} p^{n_p}$. If there exist no intermediate field μ of K/k such that $\mu \subsetneq K$ and $L/\mu(x)$ is Galois, then

$$g(F) \geqq \left(\prod_{i=1}^{\overline{m}} \overline{a}_i\right)\left[\frac{1}{2}\left\{\sum_{p, n_p \neq 0} p^{n_p}\left(1 - \frac{1}{a}\right)\right\} - 1\right] + 1,$$

with $1 \leqq {}^{\exists}\overline{m} \leqq n, {}^{\exists}\overline{a}_i \mid a,\ \overline{a}_i > 1$. In particular, if a is a prime number,

$$g(F) \geqq a^{\left\lceil \frac{\sum_{p, n_p \neq 0} p^{n_p}}{s+\alpha} \right\rceil}\left[\frac{1}{2}\left\{\sum_{p, n_p \neq 0} p^{n_p}\left(1 - \frac{1}{a}\right)\right\} - 1\right] + 1. \tag{5}$$

Proof) The proof is basically the same as the case of superelliptic curves [17]. □

This bound can be further improved as follows.

Let $\mathrm{Gal}\left(\overline{K}(x)/k(x)\right) \cong \mathrm{Gal}\left(\overline{K}/k\right) \ni \sigma_k$ denote the Frobenius automorphism of $\overline{K}(x)/k(x)$, which extends to $\bar{\sigma}_k$ in $K(x)^{sep}$. Denote $\sigma_k^i\left(\overline{K}(C)\right) := \bar{\sigma}_k^i\left(\overline{K}(C)\right)$. From this, $\sigma_k^i\left(\overline{K}(C)\right) = \overline{K}\sigma_{K/k}^i(K(C))$ and

$$\overline{K}F' = \overline{K}(C) \cdot \sigma_k\left(\overline{K}(C)\right) \cdots \sigma_k^{n-1}\left(\overline{K}(C)\right). \tag{6}$$

Then $\left[\overline{K}F' : \overline{K}(x)\right] = \prod_{i=1}^{\overline{m}} \overline{a}_i$ $(1 \leqq {}^{\exists}\overline{m} \leqq n, {}^{\exists}\overline{a}_i \mid a,\ \overline{a}_i > 1)$. If a is a prime number, then $\left[\overline{K}F' : \overline{K}(x)\right] = a^{\overline{m}}$.

[Definition 1] Let $\phi_a(n)$ be the multiplicative order of a *modulo* n. If $\gcd(n, a) = 1$. Then $\phi_a(n) = [\mathbf{F}_a[\zeta_n] : \mathbf{F}_a]$ where ζ_n is a primitive n-th root of unity [24, p.216]. □

One can obtain a lower bound of $\overline{m}$ as follows.

[Theorem 2] Let n, a be prime numbers $(n \neq a)$.

$$\text{Then } \overline{m} = \tau\phi_a(n) \text{ or } \overline{m} = 1 + \tau\phi_a(n) \quad \text{for some } \tau = 1, \cdots, \frac{n-1}{\phi_a(n)}. \tag{7}$$

Proof) The proof is basically the same as the case of superelliptic curves [17]. □

From this theorem, it is easily seen that $\overline{m} \geqq \phi_a(n)$. By using this and $g(F) \geqq a^{\overline{m}}\left[\frac{1}{2}\left\{n\left(1 - \frac{1}{a}\right)\right\} - 1\right] + 1$, one obtains.

[Theorem 3] Let n, a be prime numbers $(n \neq a)$. Then

$$g(F) \geqq a^{\phi_a(n)}\left[\frac{1}{2}\left\{n\left(1 - \frac{1}{a}\right)\right\} - 1\right] + 1. \tag{8}$$

□

This new lower bound (8) improves the lower bound (5) in the sense that it provides tighter estimates than (5) in most cases.

3.2 The Case of Cab Curves

[Definition 2] [21] [22] [23] A C_{ab} curve is defined by the following equation

$$C/K: \sum_{0 \leqq i \leqq b, 0 \leqq j \leqq a, ai+bj \leqq ab} \alpha_{ij} x^i y^j = 0 \qquad (9)$$
$$(\alpha_{ij} \in K, \alpha_{b0} \neq 0, \alpha_{0a} \neq 0),$$

where $\gcd(a,b)=1$ and C is non-singular on the affine plane.

□

Then C is an absolutely irreducible affine algebraic curve with exactly one K-rational place at infinity, and the infinity is totally ramified [20] [21] [22] [23]. Hereafter, we assume $\gcd(\mathrm{char}(k), a) = 1$, $\gcd(n, a) = 1$.

3.2.1 Galois Extensions

Here, we consider curves C such that $K(C)/K(x)$ are the tame Galois extensions, which contain C_{ab} curves. We will discuss the case of non-Galois extensions briefly in 3.2.2 .

Again $\mathrm{Gal}\left(\overline{K}(x)/k(x)\right) \cong \mathrm{Gal}\left(\overline{K}/k\right) \ni \sigma_k$ denotes the Frobenius automorphism of $\overline{K}(x)/k(x)$, which extends to $\bar{\sigma}_k$ in $K(x)^{sep}$. Denote $\sigma_k^i\left(\overline{K}(C)\right) := \bar{\sigma}_k^i\left(\overline{K}(C)\right)$. From this, $\sigma_k^i\left(\overline{K}(C)\right) = \overline{K}\sigma_{K/k}^i(K(C))$ and

$$\overline{K}F' = \overline{K}(C) \cdot \sigma_k\left(\overline{K}(C)\right) \cdots \sigma_k^{n-1}\left(\overline{K}(C)\right). \qquad (10)$$

Then we have $\left[\overline{K}F' : \overline{K}(x)\right] = \prod_{i=1}^{\overline{m}} \overline{a}_i$ $(1 \leqq {}^{\exists}\overline{m} \leqq n, {}^{\exists}\overline{a}_i \mid a,\ \overline{a}_i > 1)$.

[Lemma 2] The following conditions are equivalent:

(1) $\overline{K}F'/\overline{K}(x)$ is ramified at a place $\wp \in \mathbb{P}_{\overline{K}(x)}$.

(2) There exists $i \in \{0, \cdots n-1\}$ such that $\sigma_k^i\left(\overline{K}(C)\right)/\overline{K}(x)$ is ramified.

Proof) Let $\wp \in \mathbb{P}_{\overline{K}(x)}, P' \in \mathbb{P}_{\overline{K}F'}, P' \mid \wp, P_i := P' \cap \sigma_k^i\left(\overline{K}(C)\right)$. We consider $\wp \in \mathbb{P}_{\overline{K}(x)}$ such that $\sigma_k^i\left(\overline{K}(C)\right)/\overline{K}(x)$ is ramified at $\wp$. Since $e(P_i \mid \wp) \mid a$, $\sigma_k^i\left(\overline{K}(C)\right)/\overline{K}(x)$ are tame (i.e. $\mathrm{char}(k) \nmid e(P_i \mid \wp)$). Then we can use Abhyankar's lemma [26, p.125] to prove the above equivalence. □

By Lemma 2, we can consider places of $\overline{K}(x)$ which ramify in at least one of the extensions $\sigma_k^i\left(\overline{K}(C)\right)$ in order to count places ramified in $\overline{K}F'/\overline{K}(x)$. Here, let $R := \{\wp \in \mathbb{P}_{\overline{K}(x)} \mid \wp$ is ramified in $\overline{K}(C)/\overline{K}(x)\}$. Now, regard a C_{ab} curve C as

$$f(y) := \sum_{0 \leqq i \leqq b, 0 \leqq j \leqq a, ai+bj \leqq ab} \alpha_{ij} x^i y^j \in \overline{K}(x)[y]. \qquad (11)$$

Let $d(f)$ be the discriminant of f. Denote $\varepsilon := \deg_x(d(f))$. Then $\#R \leqq \varepsilon + 1$. On the other hand $\sigma_k^i(\overline{K}(C))/\overline{K}(x)$ is ramified at $\sigma_k^i(R)$. From this, $\overline{K}F'/\overline{K}(x)$ is ramified at $\cup_{i=0}^{n-1}\sigma_k^i(R)$. Hereafter let $t := \# \cup_{i=0}^{n-1} \sigma_k^i(R)$. Hence $t \leqq \overline{m} \cdot \#R \leqq \overline{m}(\varepsilon+1) \leqq n(\varepsilon+1)$. Therefore we obtain

$$\overline{m} \geqq \left\lceil \frac{t}{\varepsilon+1} \right\rceil. \qquad (12)$$

Let $P|\wp$ be ramified where $\wp \in \cup_{i=0}^{n-1}\sigma_k^i(R)$, $P \in \mathbb{P}_{\sigma_k^i(\overline{K}(C))}$. By using Abhyankar's lemma [26, p.125], $e(P'|\wp) \mid a$ for all $P' \in \mathbb{P}_{\overline{K}F'}$ which are ramified over $\wp$. Since $\gcd(\mathrm{char}(\overline{K}), a) = 1$, $\overline{K}F'/\overline{K}(x)$ is tame. Here, by using [26, p.95 Cor III.5.6],

$$2g\left(\overline{K}F'/\overline{K}\right) - 2 = \left[\overline{K}F' : \overline{K}(x)\right]\left(2g\left(\overline{K}(x)/\overline{K}\right) - 2\right)$$
$$+ \sum_{\wp \in \cup_{i=0}^{n-1}\sigma_k^i(R)} \sum_{P'|\wp} \left(e\left(P' \mid \wp\right) - 1\right) \deg P'. \qquad (13)$$

Now, $\left[\overline{K}F' : \overline{K}(x)\right] = \prod_{i=1}^{\overline{m}} \overline{a}_i$, $g(\overline{K}(x)/\overline{K}) = 0$, $\deg P' = 1$. Since $\overline{K}F'/\overline{K}(x)$ is a Galois extension, $e(\wp)f(\wp)u = [\overline{K}F' : \overline{K}(x)] = \prod_{i=1}^{\overline{m}} \overline{a}_i$. Thus,

[Theorem 4]

$$g\left(\overline{K}F'/\overline{K}\right) = -\prod_{i=1}^{\overline{m}} \overline{a}_i + \frac{1}{2}\prod_{i=1}^{\overline{m}} \overline{a}_i \sum_{\wp \in \cup_{i=0}^{n-1}\sigma_k^i(R)} \left(1 - \frac{1}{e(\wp)}\right) + 1 \qquad (14)$$

$$\geqq \tilde{a}^{\overline{m}}\left(\frac{\tilde{a}-1}{2\tilde{a}}t - 1\right) + 1 \qquad (15)$$

$$\geqq \tilde{a}^{\lceil \frac{t}{\varepsilon+1} \rceil}\left(\frac{\tilde{a}-1}{2\tilde{a}}t - 1\right) + 1, \qquad (16)$$

where $\tilde{a}$ is the minimal natural number such that $\tilde{a} \mid a$ and $\tilde{a} > 1$. Furthermore, $g\left(\overline{K}F'/\overline{K}\right) = g(F'/\kappa') = g(F/\kappa)$ $(\kappa' := \overline{K} \cap F', \kappa := \overline{K} \cap F)$. □

We will analyze C_{92} and C_{43} by using (14)(16) in section 4.

3.2.2 Non-Galois Extensions

Now, we discuss the case of non-Galois extensions $K(C)/K(x)$ briefly.

Let N be the Galois closure of $K(C)/K(x)$. Then, consider the Galois closure of $N/k(x)$:

$$F' := N \cdot \bar{\sigma}_{K/k}(N) \cdots \bar{\sigma}_{K/k}^{n-1}(N). \qquad (17)$$

Then the existence and properties of Weil restriction can be proved by using N and $a' := \prod_{i=1}^{l} b_i$ $(1 \leqq {}^{\exists}l \leqq a, {}^{\exists}b_i \mid a,\ b_i > 1)$ in place of L and a in section 2 respectively, e.g. we can obtain the similar results as Lemma 1 and Prop 1.

Furthermore, again $\mathrm{Gal}\left(\overline{K}(x)/k(x)\right) \cong \mathrm{Gal}\left(\overline{K}/k\right) \ni \sigma_k$ denotes the Frobenius automorphism of $\overline{K}(x)/k(x)$, which extends to $\bar{\sigma}_k$ in $K(x)^{sep}$ as well as in 3.2.1. Let $\overline{N}$ be the Galois closure of $\overline{K}(C)/\overline{K}(x)$. Denote $\sigma_k^i\left(\overline{N}\right) := \bar{\sigma}_k^i\left(\overline{N}\right)$. From this,

$$\overline{K}F' = \overline{N} \cdot \sigma_k\left(\overline{N}\right) \cdots \sigma_k^{n-1}\left(\overline{N}\right). \qquad (18)$$

Then we have $\left[\overline{K}F' : \overline{K}(x)\right] = \prod_{i=1}^{\overline{m}} \overline{a'}_i$ $(1 \leqq {}^{\exists}\overline{m} \leqq n, {}^{\exists}\overline{a'}_i \mid a',\ \overline{a'}_i > 1)$. Consequently $\overline{K}F'/\overline{K}(x)$ is tame. We can obtain the similar equation to (14) for genera.

4. Analyses of the GHS Weil Descent Attack

4.1 Analysis for Superelliptic Curves

In this section, we analyze security of superelliptic curves based cryptosystems against the GHS Weil descent attack shown in section 2. Besides, a comparison is provided between Pollard's rho algorithm and Adlemen-DeMarrais-Huang algorithm.

[Definition 3] A superelliptic curve is defined by the following equation.

$$C/K : y^a = f(x) := \alpha_b x^b + \cdots + \alpha_1 x + \alpha_0 \qquad (19)$$

Assuming that the following conditions hold:

$$a \,|\, q-1,\ \gcd(f(x), f'(x)) = 1,\ \gcd(a,b) = 1 \text{ or } a. \qquad (20)$$

□

Here, $a \,|\, q-1$ implies that k contains a primitive a-th root of unity and $\gcd(\mathrm{char}(k), a) = 1$. If $\gcd(a,b) = 1$, then the point at infinity is totally ramified. When $\gcd(a,b) = a$, it is unramified. Now since k contains all a-th roots of unity and $\gcd(\mathrm{char}(k), a) = 1$, $K(C)/K(x)$ is a Kummer extension.

First we compare between complexities of Pollard's rho algorithm over $Cl^0(K(C))$ and Gaudry's algorithm [11] over $Cl^0(F)$. Complexities of both algorithms are known as follows.

- Cost of Pollard's rho algorithm

$$C_P := O\left(g(K(C))^2 q^{\frac{g(K(C))n}{2}} (\log q^n)^2\right) \qquad (21)$$

- Cost of Gaudry's algorithm

$$C_G := O\left(g(F)^3 q^2 (\log q)^2 + g(F)^2 (g(F)!) q (\log q)^2\right) \qquad (22)$$

Now let $h := \log_2\left(q^{g(K(C))n}\right)$, then

$$q = 2^{\frac{h}{g(K(C))n}}. \qquad (23)$$

From (21) (23),

$$n^2 g(K(C))^2 q^{\frac{g(K(C))n}{2}} = n^2 g(K(C))^2 2^{\frac{h}{2}}. \qquad (24)$$

Similarly from (22) (23),

$$g(F)^3 q^2 + g(F)^2 (g(F)!) q = g(F)^3 2^{\frac{2h}{g(K(C))n}} + g(F)^2 (g(F)!) 2^{\frac{h}{g(K(C))n}}. \qquad (25)$$

Consider cryptographic applications, we assume in (24) and (25) that $h \geqq 160$. We can prove:

[Theorem 5] Let n, a be prime numbers ($n \geqq 5, n \neq a$), and let C be a superelliptic curve which is non-hyperelliptic curve ($b \geqq 3$), $g(K(C)) \leqq 4$, $h \leqq 546$. Then we have $C_P < C_G$. □

Thus for the above cases, the GHS Weil descent attack using Gaudry's algorithm does not provide a faster attack than Pollard's rho algorithm.

[Remark 1] Here, we compared C_P with the lower bounds of C_G. When $h = \log_2\left(q^{g(K(C))n}\right)$ exceeds certain value (depending a prime number n), C_P becomes larger than the lower bounds of C_G. In fact the upper bound of $h = \log_2\left(q^{g(K(C))n}\right)$ such that $C_P < C_G$ can be showed as follows: if $n = 5$, $C_P < C_G$ for $h \leqq 546$, if $n = 13$, $C_P < C_G$ for $h \leqq 971$, if $n = 11$, $C_P < C_G$ for $h \leqq 10770$. Such upper bound of $h = \log_2\left(q^{g(K(C))n}\right)$ increases when the lower bound of $g(F)$ increases.

[Remark 2] If we increase q (i.e. h) with fixed n, a, and b, $g(F)$ has an upper bound (by the equation (13) of superelliptic curve cases). Hence $C_P > C_G$ when h is large enough. Although it does not mean that C_P becomes greater than C_G as soon as h exceeds the upper bound in Remark 1, the DLP over $Cl^0(F)$ has less cost than the DLP over$Cl^0(K(C))$ for large key lengths. This is also the same in theorem 6.

Moreover when $g(F)$ is larger, Enge and Gaudry's improvement [6] of the subexponential algorithm by Adleman-DeMarrais-Huang [1] should be employed. Bellow, we compare between complexities of Pollard's rho algorithm on $Cl^0(K(C))$ and the ADH algorithm on $Cl^0(F)$. Complexities of Enge-Gaudry's algorithm [6] are known as follows.

- Cost of Enge-Gaudry's algorithm [6]

$$C_A := O\left(e^{(\sqrt{2}+o(1))\sqrt{\log q^{g(F)}}\sqrt{\log\log q^{g(F)}}}\right), \text{when } \frac{g(F)}{\log q} \to \infty. \qquad (26)$$

Recall $h = \log_2\left(q^{g(K(C))n}\right)$, then $q = 2^{\frac{h}{g(K(C))n}}$. From (21) (23),

$$n^2 g(K(C))^2 2^{\frac{h}{2}} \left(\frac{h}{g(K(C))n} \log 2\right)^2 = 2^{\frac{h}{2}} h^2 (\log 2)^2. \qquad (27)$$

Similarly from (23) (26),

$$e^{\sqrt{2}\sqrt{\log q^{g(F)}}\sqrt{\log\log q^{g(F)}}}$$
$$= e^{\sqrt{2}\sqrt{g(F)\frac{h}{g(K(C))n}\log 2}\sqrt{\log g(F) + \log\frac{h}{g(K(C))n} + \log 2}}. \qquad (28)$$

By calculating lower bounds of $g(F)$ using (5) and (8), we obtain the extent when (28) > (27).

[Theorem 6] Let n, a be prime numbers ($n \geqq 7, n \neq 13, n \neq a$), and let C be a superelliptic curve which is non-hyperelliptic curve ($b \geqq 3$), $g(K(C)) \leqq 4$, $h \leqq 1765$. Then we have $C_P < C_A$. □

Thus for the above cases, the GHS Weil descent attack using the ADH algorithm does not provide a faster attack than Pollard's rho algorithm.

[Remark 3] Here, we compared C_P with the lower bounds of C_A. When $h = \log_2\left(q^{g(K(C))n}\right)$ exceeds certain value (depending a prime number n), C_P become larger than the lower bounds of C_A. If $n = 13, b = 4, 5, 6, h \geqq 160$, C_P become larger than the lower bound of C_A. In fact the upper bound of $h = \log_2\left(q^{g(K(C))n}\right)$ such that $C_P < C_A$ can be showed as follows: if $n = 11$, $C_P < C_A$ for $h \leqq 1765$, (In particular, the value of (28) become slightly larger than (27) when $h = 1766, n = 11, b = 5, 6$.) and if $n = 7$, $C_P < C_A$ for $h \leqq 5025$. Furthermore if $n \geqq 17$, the upper bound of $h = \log_2\left(q^{g(K(C))n}\right)$ such that $C_P < C_A$ becomes larger. Such upper bound of $h = \log_2\left(q^{g(K(C))n}\right)$ increases when the lower bound of $g(F)$ increases.

4.2 Analyses for C_{92} Curves and C_{43} Curves

Finally, a comparison is provided between Pollard's rho algorithm and Gaudry's algorithm for C_{ab} curves C. In particular, we analyze C_{92} curves and C_{43} curves whose function fields $K(C)/K(x)$ are tame Galois extensions. (They have the genus 4 and 3 respectively.)

4.2.1 C_{92} Curves

We consider a C_{92} curve C such that $K(C)/K(x)$ is a tame Galois extension. Now, regard C as

$$\begin{aligned} f(y) := {} & \alpha_{09}y^9 + \alpha_{08}y^8 + \cdots + \alpha_{02}y^2 + \alpha_{01}y + \alpha_{11}xy + \alpha_{12}xy^2 \\ & + \alpha_{13}xy^3 + \alpha_{14}xy^4 + \alpha_{10}x + \alpha_{00} \in \overline{K}(x)[y]. \end{aligned}$$

By computing the discriminant of f, $\varepsilon := \deg_x(d(f)) = 16$. Since $R := \{\wp \in \mathbb{P}_{\overline{K}(x)} \mid \wp \text{ is ramified in } \overline{K}(C)/\overline{K}(x)\} \leqq \varepsilon + 1 = 17$, it follows that $t := \#\cup_{i=0}^{\overline{m}}\sigma_k^i(R) \leqq \overline{m} \cdot \#R \leqq \overline{m} \cdot 17$. Therefore $\overline{m} \geqq \left\lceil \frac{t}{17} \right\rceil$. Similar to 3.2, we obtain

$$g(F) = -\prod_{i=1}^{\overline{m}} \overline{a}_i + \frac{1}{2}\prod_{i=1}^{\overline{m}} \overline{a}_i \sum_{\wp \in \cup_{i=0}^{n-1}\sigma_k^i(R)} \left(1 - \frac{1}{e(\wp)}\right) + 1 \tag{29}$$

$$\geqq 3^{\left\lceil \frac{t}{17} \right\rceil}\left(\frac{1}{3}t - 1\right) + 1. \tag{30}$$

By substituting the lower bound of $g(F)$ by (30) and $g(K(C)) = 4$ into (24) (25), we obtained the following result.

Conditions	The extent of t such that $C_P < C_G$
(1) $h \leqq 160, n \leqq 100$	$t \geqq 18$
(2) $h \leqq 320, n \leqq 100$	$t \geqq 18$
(3) $h \leqq 640, n \leqq 100$	$t \geqq 26$
(4) $h \leqq 1280, n \leqq 100$	$t \geqq 35$

Thus we found that $C_P < C_G$ when $t \geqq 35$ under the above conditions.

Next we consider $t \leqq 34$. By substituting the value of $g(F)$ by (29) and $g(K(C)) = 4$ into (24) (25), we show curves such that $C_P > C_G$ for $t \leqq 34$, $h := \log_2\left(q^{g(K(C))n}\right) \leqq 1280$, $n \leqq 100$ in Appendix.

Symbols used in the table of Appendix are:
$t := \#\cup_{i=0}^{\overline{m}}\sigma_k^i(R)$ i.e. the total number of places $\wp \in \mathbb{P}_{\overline{K}(x)}$ ramified in $\overline{K}F'/\overline{K}(x)$
A : the total number of places $\wp \in \mathbb{P}_{\overline{K}(x)}$ such that $e(\wp) = 3$
B : the total number of places $\wp \in \mathbb{P}_{\overline{K}(x)}$ such that $e(\wp) = 9$
E : the value of possible $\prod_{i=1}^{\overline{m}} \overline{a}_i$ $(1 \leqq {}^{\exists}\overline{m} \leqq n, {}^{\exists}\overline{a}_i \mid 9,\ \overline{a}_i > 1)$
△ : $C_P > C_G$
○ : $C_P < C_G$

[Remark 4] Within $3 \leqq t \leqq 34$, $h \leqq 1280$, $n \leqq 100$, $E \geqq 27$, the curves when $C_P < C_G$ are denoted other than the triangular marks and $(t, A, B) = (3, 3, 0)$. Besides, $(t, A, B) = (3, 3, 0)$ has an impossible combination of $g(F)$. Since $\overline{K}F' \neq \overline{K}(x)$, only the cases $\left[\overline{K}F' : \overline{K}(x)\right] = \prod_{i=1}^{\overline{m}} \overline{a}_i \geqq 27$ are considered.
We should avoid to use such C_{92} curves in cryptosystems having parameters with triangular marks.

4.2.2 C_{43} Curves

Consider a C_{43} curve such that $K(C)/K(x)$ is a tame Galois extension. Similarly, $\varepsilon := \deg_x(d(f)) = 9$. Since $R := \{\wp \in \mathbb{P}_{\overline{K}(x)} \mid \wp \text{ is ramified in } \overline{K}(C)/\overline{K}(x)\} \leqq \varepsilon + 1 = 10$, $t := \#\cup_{i=0}^{\overline{m}}\sigma_k^i(R) \leqq \overline{m} \cdot \#R \leqq \overline{m} \cdot 10$. Therefore $\overline{m} \geqq \left\lceil \frac{t}{10} \right\rceil$. Similar to 3.2, we obtain

$$g(F) = -\prod_{i=1}^{\overline{m}} \overline{a}_i + \frac{1}{2}\prod_{i=1}^{\overline{m}} \overline{a}_i \sum_{\wp \in \cup_{i=0}^{n-1}\sigma_k^i(R)} \left(1 - \frac{1}{e(\wp)}\right) + 1 \tag{31}$$

$$\geqq 2^{\left\lceil \frac{t}{10} \right\rceil}\left(\frac{1}{4}t - 1\right) + 1. \tag{32}$$

By substituting the lower bound of $g(F)$ by (32) and $g(K(C)) = 3$ into (24) (25), we obtained.

Conditions	The extent such that $C_P < C_G$
(1) $h \leqq 160, n \leqq 100$	$t \geqq 21$
(2) $h \leqq 320, n \leqq 100$	$t \geqq 25$
(3) $h \leqq 640, n \leqq 100$	$t \geqq 31$
(4) $h \leqq 1280, n \leqq 100$	$t \geqq 33$

Thus we found that $C_P < C_G$ when $t \geqq 33$ under the above conditions.

Next consider $t \leqq 32$. Similarly, by substituting the value of $g(F)$ by (31) and $g(K(C)) = 3$ into (24) (25), we can obtain curves such that $C_P > C_G$ for $t \leqq 32$, $h := \log_2\left(q^{g(K(C))n}\right) \leqq 1280$, $n \leqq 100$ (since the table requires larger space, it is omitted here).

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] S. Arita, "Algorithms for Computations in Jacobian Group of C_{ab} Curve and Their Application to Discrete-Log Based Public Key Cryptosystems," IEICE Trans. Vol.J82-A, no.8,pp.1291–1299 ,1999, in Japanese.

[4] C. Chevalley, "Introduction to the theory of algebraic functions of one variable Mathematical Surveys Volume 6," American Mathematical Society, 1951.

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

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

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

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

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

[10] S.D. Galbraith, S. Paulus, and N. Smart, "Arithmetic on superelliptic curves," Math. Comput. 71, No.237, pp.393-405, 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] R. Harasawa, J. Suzuki, "A Fast Jacobian Group Arithmetic Scheme for Algebraic Curve Cryptography," IEICE Trans. Vol.E84-A, no.1,pp130–139 ,2001.

[14] F. Hess, "The GHS Attack Revisited," Advances in cryptology-EUROCRYPTO 2003, Springer-Verlag, LNCS 2656, pp.374–387, 2003.

[15] F. Hess, "Generalizing the GHS Attack on the Elliptic Curve Discrete Logarithm," LMS J. Comput. Math.7 , pp.167–192, 2004.

[16] B. Huppert, "Endliche Gruppen," Springer-Verlag, 1967, in German.

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

[19] 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.

[20] R. Matsumoto, "Using C_{ab} Curves in the Function Field Sieve," IEICE Trans. Vol.E82-A, no.3,pp551–552 ,1999.

[21] S. Miura, "The study of error coding codes based on algebraic geometry," Dr. thesis, 1997, in Japanese.

[22] S. Miura, "Algebraic geometric codes on certain plane curves," IEICE Trans. Vol.J75-A, no.11,pp1736–1745 ,1992, in Japanese.

[23] S. Miura, "Linear codes on affine algebraic curves," IEICE Trans. Vol.J81-A, no.10,pp1398–1421 ,1998, in Japanese.

[24] Y. Morita, "Introduction to algebra," Shoukabou, 1996, in Japanese.

[25] T.Oda, T.Iijima, M.Shimura, J.Chao, and S.Tsujii "On Security of Superelliptic Curves Based Cryptosystems against GHS Weil Descent Attack," IEICE, Japan, Proc.of SCIS2005, 2005.

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

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

[28] N.Thériault, "Weil descent attack for Artin-Schreier Curves," preprint, 2003.
Available from http://www.math.toronto.edu/ganita/papers /wdasc.pdf

[29] K. Yamazaki, "Rings and modules," Iwanami, 1991, in Japanese.

Appendix

C_{92} Curves when $C_P > C_G$

t	A	B	E				t	A	B	E	t	A	B	E
			27	81	243	729				27				27
3	0	3	△	△	△	○	8	6	2	△	11	11	0	△
3	1	2	△	△	△	○	8	7	1	△	12	0	12	△
3	2	1	△	△	△	△	8	8	0	△	12	1	11	△
4	0	4	△	△	○	○	9	0	9	△	12	2	10	△
4	1	3	△	△	○	○	9	1	8	△	12	3	9	△
4	2	2	△	△	○	○	9	2	7	△	12	4	8	△
4	3	1	△	△	△	○	9	3	6	△	12	5	7	△
4	4	0	△	△	△	○	9	4	5	△	12	6	6	△
5	0	5	△	△	○	○	9	5	4	△	12	7	5	△
5	1	4	△	△	○	○	9	6	3	△	12	8	4	△
5	2	3	△	△	○	○	9	7	2	△	12	9	3	△
5	3	2	△	△	○	○	9	8	1	△	12	10	2	△
5	4	1	△	△	○	○	9	9	0	△	12	11	1	△
5	5	0	△	△	○	○	10	0	10	△	12	12	0	△
6	0	6	△	○	○	○	10	1	9	△	13	5	8	△
6	1	5	△	○	○	○	10	2	8	△	13	6	7	△
6	2	4	△	○	○	○	10	3	7	△	13	7	6	△
6	3	3	△	△	○	○	10	4	6	△	13	8	5	△
6	4	2	△	△	○	○	10	5	5	△	13	9	4	△
6	5	1	△	△	○	○	10	6	4	△	13	10	3	△
6	6	0	△	△	○	○	10	7	3	△	13	11	2	△
7	0	7	△	○	○	○	10	8	2	△	13	12	1	△
7	1	6	△	○	○	○	10	9	1	△	13	13	0	△
7	2	5	△	○	○	○	10	10	0	△	14	9	5	△
7	3	4	△	○	○	○	11	0	11	△	14	10	4	△
7	4	3	△	○	○	○	11	1	10	△	14	11	3	△
7	5	2	△	○	○	○	11	2	9	△	14	12	2	△
7	6	1	△	○	○	○	11	3	8	△	14	13	1	△
7	7	0	△	△	○	○	11	4	7	△	14	14	0	△
8	0	8	△	○	○	○	11	5	6	△	15	13	2	△
8	1	7	△	○	○	○	11	6	5	△	15	14	1	△
8	2	6	△	○	○	○	11	7	4	△	15	15	0	△
8	3	5	△	○	○	○	11	8	3	△				
8	4	4	△	○	○	○	11	9	2	△				
8	5	3	△	○	○	○	11	10	1	△				

$t := \# \cup_{i=0}^{\overline{m}} \sigma_k^i(R)$ i.e. the total number of places $\wp \in \mathbb{P}_{\overline{K}(x)}$ ramified in $\overline{K}F'/\overline{K}(x)$

A : the total number of places $\wp \in \mathbb{P}_{\overline{K}(x)}$ such that $e(\wp) = 3$

B : the total number of places $\wp \in \mathbb{P}_{\overline{K}(x)}$ such that $e(\wp) = 9$

E : the value of possible $\prod_{i=1}^{\overline{m}} \overline{a}_i$ $(1 \leqq {}^{\exists}\overline{m} \leqq n, {}^{\exists}\overline{a}_i \mid 9,\ \overline{a}_i > 1)$

△ : $C_P > C_G$

○ : $C_P < C_G$