On Security of Superelliptic Curves Based Cryptosystems against GHS Weil Descent Attacks

Takahiro Oda *, Tsutomu Iijima *, Mahoro Shimura †, Jinhui Chao *
Shigeo Tsujii ‡

Abstract— The GHS Weil descent attack by Gaudry, Hess and Smart was originally proposed to elliptic curves over finite fields of characteristic two [11]. Among a number of extensions of this attack, Diem treated the cases of hyperelliptic curves over finite fields of arbitrary odd characteristics [4]. His results were partially extended to algebraic curves of which the function fields are cyclic Galois extensions [14]. In this paper, we first improve the results in [14] and show a lower bound of genera of curves obtained by the GHS Weil descent attack. Then based on these results, a detailed analysis on security of superelliptic curves based cryptosystems is provided against various attacks.

Keywords: GHS Weil descent attack, superelliptic curves, function fields, Pollard’s rho algorithm, Gaudry’s algorithm, Adleman-DeMarrais-Huang algorithm

1 Introduction

The idea of Weil descent was introduced into elliptic curve based cryptosystems by Frey [6] was applied by Gaudry, Hess and Smart to propose the so-called GHS Weil descent attack [11]. In this algorithm, a hyperelliptic curve is constructed by the Weil descent 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 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 [10] of the Adleman-DeMarrais-Huang algorithm [1].

The GHS Weil descent attack has extended by many researchers, and security against these attacks has also discussed. It was extended by Galbraith to certain classes of hyperelliptic curves over characteristic two [10], and by Arita to some elliptic curves over finite fields of characteristic three [2]. Diem gave a general treatment of the GHS Weil descent attack on hyperelliptic curves over finite fields of arbitrary odd characteristics [4]. Recently, it was applied to special classes of both superelliptic curves and Artin-Schreier curves by Thériault [21][22]. Besides, Hess generalized the GHS Weil descent attack to arbitrary Artin-Schreier extensions [12][13]. Furthermore, a part of Diem’s results [4] were extended to algebraic curves of which the function fields are cyclic Galois extensions [14].

In this paper, we first discuss the GHS Weil descent attack on superelliptic curves. Then improvement of the results in [14] is shown to derive a tighter lower bound of curves obtained by the Weil restriction. Finally, based on these results, a detailed analysis on security of superelliptic curve based cryptosystems against the GHS Weil descent and other attack are presented.

Through this paper we assume that $K = F_{q^n}, k = F_q (n \neq 1)$ 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 for Superelliptic Curves

2.1 Superelliptic Curves

Definition 1. A superelliptic curve is defined by the following equation.

$$C/K : Y^r = f(X) := a_5 X^5 + \cdots + a_1 X + a_0 \quad (1)$$

Assume that the following conditions hold:

$$r | q - 1, \gcd(f(X), f'(X)) = 1, \gcd(r, \delta) = 1 \text{ or } r. \quad (2)$$

Here, $r | q - 1$ implies that $k$ contains a primitive $r$-th root of unity and $\gcd(\text{char}(k), r) = 1$. If $\gcd(r, \delta) = 1$, then the point at infinity is totally ramified. When $\gcd(r, \delta) = r$, it is unramified. Hereafter, $C$ denotes a superelliptic curve over $K$, $K(C)$ is the function field defined by the superelliptic curve $C$. Now since $k$ contains all $r$-th roots of unity and $\gcd(\text{char}(k), r) = 1$, $K(C)/K(x)$ is a Kummer extension. The function field $K(C)$ has the following properties.
Proposition 1. [20, p.196] Suppose that $K(C) = K(x, y)$ is defined by the following equation

$$C : Y^r = f(X) := c \prod_{i=1}^{s} p_i(X) \quad (3)$$

where $f(X)$ is factorized into $s (> 0)$ pairwise distinct irreducible monic polynomials $p_i(X) \in K[X]$ such that

$$r > c \neq 0, \text{char}(K) \not| r. \quad (4)$$

Then:

- $K$ is the full constant field of $K(C)$, and $[K(C) : K(x)] = r$. If $K$ contains a primitive $r$-th root of unity, $K(C)/K(x)$ is cyclic.
- Let $P_i$ (resp. $P_{\infty}$) 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 $K(C)/K(x)$. All places $Q_{\infty} \in \mathbb{P}K(C)$ with $Q_{\infty} | P_{\infty}$ have the ramification index $e(Q_{\infty} | P_{\infty}) = r/d$ where $d := \gcd(r, \delta)$.
- No places $P \in \mathbb{P}K(x)$ other than $P_1, \cdots, P_s, P_{\infty}$ ramify in $K(C)/K(x)$.
- The genus of $K(C)/K$ is

$$g = \frac{r - 1}{2} (\delta - 1) - \frac{d - 1}{2}, \text{ where } d := \gcd(r, \delta). \quad \square$$

2.2 GHS Weil Descent Attack

Below, we summarize main issues of the GHS Weil descent attack on superelliptic curves.

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

$$F' := K(C) \cdot \hat{\sigma}_{K/k}(K(C)) \cdots \hat{\sigma}_{K/k}^{n-1}(K(C)). \quad (5)$$

If $\gcd(n, r) = 1$, then $\hat{\sigma}_{K/k}$ can be extended to an automorphism of $F'/k(x)$ such that the order is $n$ [14]. Next, consider the fixed field of $F'$ by the automorphism $\hat{\sigma}_{K/k}$:

$$F := \{ \alpha \in F' \mid \hat{\sigma}_{K/k}(\alpha) = \alpha \}. \quad (6)$$

Moreover, the following mapping can be constructed as the composition of conorm and norm $[3][20]$:

$$N_{F/F} \circ \text{Con}, F/K(C) : Cl^0(K(C)) \rightarrow Cl^0(F). \quad (7)$$

This map will be called the GHS conorm-norm homomorphism as in the elliptic curve case [11]. Let $r$ be a prime number. If there exists no intermediate field $\mu$ of $K/k$ such that $\mu \subseteq K$ and $K(C)/\mu(x)$ is Galois, then a large prime order subgroup of $\# Cl^0(K(C))$ (therefore the DLP over $Cl^0(K(C))$) can be preserved by the GHS conorm-norm homomorphism [14].

Thus, a new curve is constructed by Weil restriction of the superelliptic curve over a finite field $K/k$, then the DLP over $Cl^0(K(C))$ is transformed to the DLP over $Cl^0(F)$. The new curve is defined over a smaller definition field $k$ and has genus bigger than the original curve. In this paper, when the DLP over $Cl^0(F)$ can be solved more efficiently than the DLP over $Cl^0(K(C))$, we consider the GHS Weil descent attack to be successful. In order to discuss the effectiveness of the GHS Weil descent attack on superelliptic curves in section 4, we need to estimate lower bounds of $g(F)$.

3 Genus of Function Field $F$

3.1 Lower Bound of $g(F)$

If $\gcd(n, r) = 1$, then the following lower bound of $g(F)$ is obtained in [14].

Theorem 1. Let $K/k$ be a finite field of extension degree $n$,

$$C/K : Y^r = f(X) := a_5X^5 + \cdots + a_1X + a_0,$$

$$r | q - 1, \gcd(f(X), f'(X)) = 1, \gcd(r, \delta) = 1 \text{ or } r.$$

We define

$$\alpha := 0 \text{ for } \gcd(r, \delta) = r, \alpha := 1 \text{ for } \gcd(r, \delta) = 1.$$

Applying the GHS Weil descent attack to the curve $C$, the resulting function field $F$ has the following properties.

Let $n := \prod_{p \text{ prime}} p^p$. If there exists no intermediate field $\mu$ of $K/k$ such that $\mu \subseteq K$ and $K(C)/\mu(x)$ is Galois, then we have

$$g(F) \geq \left( \prod_{i=1}^{m} \eta_i \right) \left[ \frac{1}{2} \left( \sum_{p, p' \neq 0} p^{n_p} \left( 1 - \frac{1}{r} \right) \right) - 1 \right] + 1,$$

with $1 \leq \eta \leq n, \eta | r, \eta > 1$. In particular, if $r$ is a prime number,

$$g(F) \geq r \left[ \frac{1}{2} \left( \sum_{p, p' \neq 0} p^{n_p} \left( 1 - \frac{1}{r} \right) \right) - 1 \right] + 1.$$

(8)
3.2 Improvement of the Lower Bound

Now, we show a new lower bound of \( g(F) \) which improves the lower bound (8).

Let \( \text{Gal}(K(x)/k(x)) \cong \text{Gal}(K/k) \cong \sigma_k \) denote the Frobenius automorphism of \( K(x)/k(x) \), which extends to \( \sigma_k \) in \( K(x) \) \( \text{exp} \). Denote \( \sigma_k^i (K(C)) := \sigma_k^i (K) \). From this, \( \sigma_k^i (K(C)) = \mathcal{K} \sigma_k^i (K(C)) \) and

\[
\mathcal{K} F' = \mathcal{K}(C) \cdot \sigma_k (K(C)) \cdots \sigma_k^{n-1} (K(C)).
\]

Then, we have \( \mathcal{K} F' : K(x) = \prod_{r=1}^{m} r \cdot (1 \leq \frac{\beta}{G} \leq n, r, \tau_i > 1) \). Hereafter let \( r \) be a prime number. Then we can assume \( \mathcal{K} F' : K(x) = r^\mu \).

Definition 2. Let \( \phi_r(n) \) be the multiplicative order of \( r \mod n \). Recall gcd(\( n, r \)) = 1. Then \( \phi_r(n) = [F_r;\mathbb{Z}_n] : F_r \) where \( \mathbb{Z}_n \) is a primitive \( n \)-th root of unity [19, p.216].

Following this definition, we wish to find a lower bound of \( \mathcal{K} \).

Theorem 2. Let \( n, r \) be prime numbers \( (n \neq r) \).

Then \( \mathcal{K} = \tau \phi_r(n) \) or \( \mathcal{K} = 1 + \tau \phi_r(n) \) (10) for some \( \tau = 1, \ldots, n - 1 \).

From this theorem, it is easily seen that \( \mathcal{K} \geq \phi_r(n) \). By using this and

\[
g(F) \geq r^\mathcal{K} \left[ \frac{1}{2} \left\{ n \left( 1 - \frac{1}{r} \right) \right\} - 1 \right] + 1,
\]

we obtain a new lower bound of \( g(F) \).

Theorem 3. Let \( n, r \) be prime numbers \( (n \neq r) \). Then

\[
g(F) \geq r^\phi_r(n) \left[ \frac{1}{2} \left\{ n \left( 1 - \frac{1}{r} \right) \right\} - 1 \right] + 1.
\]


This new lower bound (11) improves the lower bound (8) in the sense that it provides tighter estimate than (8) in most cases.

Example 1. For \( n = 7 \), the lower bounds of \( g(F) \) is calculated by using (8) and (11). \( \delta = 3 \) is assumed in (8).

\[
\begin{array}{|c|c|c|c|}
\hline
r & 3 & 5 & 11 \\
\hline
(11) & g(F) \geq 973 & g(F) \geq 28126 & g(F) \geq 2005 \\
(8) & g(F) \geq 37 & g(F) \geq 99 & g(F) \geq 265 \\
\hline
\end{array}
\]

4 Analysis of the GHS Weil Descent Attack for Supercubic Curves

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

4.1 Effect of GHS Weil Descent Attack

Here, we estimate the genus of the function field \( F \) by using (11). Appendix 1 shows the lower bounds of \( g(F) \) running with prime numbers \( n = 7 \sim 100 \) and \( r = 3 \sim 100 \).

Theorem 4. Let gcd(\( n, r \)) = 1, and \( r, n \) be prime numbers \( (r \neq n) \), \( C \) is a superelliptic curve which is non-hyperelliptic curve. Then

\[
\begin{align*}
& n \geq 7 \implies g(F) \geq 70, \\
& n \geq 11 \implies g(F) \geq 91.
\end{align*}
\]

Proof)

First, when \( 7 \leq n \leq 100 \) and \( 3 \leq r \leq 100 \), \( g(F) \geq 70(n = 7, r = 29) \) from Appendix 1. Then the second smallest lower bound is 91(\( n = 13, r = 3 \)).

Next, when \( 100 \leq n \leq 200 \) and \( 3 \leq r \leq 100 \), \( g(F) \geq 405765(n = 127, r = 19) \) by using (11).

Otherwise, if \( r = 2, n = 200, \phi_r(n) = 1 \), then \( g(F) \geq 2 \times (100 - 1) + 1 = 99 \). By monotonic increase of (11), it follows that \( g(F) \geq 99 \) for \( n \geq 200 \). Similarly, \( g(F) \geq 148 \) for \( n \geq 5 \) and \( r \geq 100 \).

Pollard’s rho algorithm is currently the fastest general algorithm for solving DLP on finite abelian groups. In [10], Gaudry proposed a variant of the Adlamen-DeMarrais-Huang algorithm (hereafter we call it ADH algorithm) [1] to attack hyperelliptic curve discrete logarithm problems. The Gaudry’s algorithm is faster than the Pollard’s rho algorithm when the genus is more than 4 (about 3~9). In addition, it is known that the Gaudry’s algorithm is faster than the ADH algorithm when the genus is comparatively small. However the Gaudry’s algorithm is not efficient for large genera, since the complexity contains the large multiplicative factor \( g \). Thus it is difficult for the GHS Weil descent attack using the Gaudry’s algorithm to succeed for superelliptic curves satisfy the above theorem.

4.2 Comparison with Pollard’s rho and ADH Algorithms

Next we compare between the complexity of the Pollard’s rho algorithm over \( C^p(K(C)) \) and the Gaudry’s algorithm [10] over \( C^p(F) \). The complexities of both algorithms are given as follows.

- Cost of the Pollard’s rho algorithm

\[
C_P := O \left( g(K(C))^2 q \frac{g(K(C))}{\log q^n} \right) \cdot \left( \log q^n \right)^2. \tag{12}
\]

- Cost of the Gaudry’s algorithm

\[
C_G := O \left( g(F)^3 q^2 (\log q)^2 + g(F)^2 (g(F))! q (\log q)^2 \right). \tag{13}
\]

Now let be \( a := \log_2 \left( q^g(K(C))^n \right) \), then

\[
q = 2^\frac{a}{\mathcal{K}^\mu}. \tag{14}
\]
From (12) (14),
\[ n^2 g(K(C))^2 \frac{q^{n(K(C))n}}{2} = n^2 g(K(C))^2 2^a. \] (15)

Similarly from (13) (14),
\[ g(F)^3 q^2 + g(F)^2 (g(F))^a q = g(F)^3 2^{\pi(n(K(C))n)} + g(F)^2 (g(F))^2 2^{\pi(n(K(C))n)}. \] (16)

Now consider in cryptographic applications, we assume in (15) and (16) that \( a \geq 160 \). By calculating (15) and the lower bounds of (16) using the lower bounds (8) and (11), we obtained the following result.

Notice that we considered \( g(K(C)) \leq 4 \) in order to simplify comparison here. Besides, the range of \( a = \log_2 (q^{g(K(C))n}) \) is also restricted.

**Theorem 5.** Let \( n, r \) be prime numbers \((n \geq 5, n \neq r)\), and let \( C \) be a superelliptic curve which is non-hyperelliptic curve, \( g(K(C)) \leq 4, a \leq 546 \). Then we have \( C_P < C_G \).

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

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

Moreover when \( g(F) \) is larger, Enge and Gaudry’s improvement [5] of the subexponential algorithm by Adleman-DeMarrais-Huang [1] should be employed. Bellow, we compare between complexities of the Pollard’s rho algorithm on \( C_P(K(C)) \) and the ADH algorithm on \( C_P(F) \). Complexity of Enge-Gaudry’s algorithm [5] is known as follows.

- **Cost of the Enge-Gaudry’s algorithm [5]**

  \[ C_A := O \left( (\sqrt{q(a(1)+\log q^{g(F)})} \sqrt{\log \log q^{g(F)}} \right) \] (17)

  when \( \frac{g(F)}{\log q} \to \infty \).

Recall \( a = \log_2 (q^{g(K(C)))n}) \), then \( q = 2^{\pi(n(K(C))n)} \). From (12) (14),
\[ n^2 g(K(C))^2 2^a \left( \frac{a}{g(K(C)^n} \log 2 \right)^2 = 2^a a^2 (\log 2)^2. \] (18)

By calculating lower bounds of \( g(F) \) using (8) and (11), we obtain the extent when (19) > (18).

Notice that as in Theorem 5, we considered only \( g(K(C)) \leq 4 \) in order to simplify comparison. The range of \( a = \log_2 (q^{g(K(C))n}) \) is also restricted.

**Theorem 6.** Let \( n, r \) be prime numbers \((n \geq 7, n \neq r)\), and let \( C \) be a superelliptic curve which is non-hyperelliptic curve, \( g(K(C)) \leq 4, a \leq 1765 \). 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 the Pollard’s rho algorithm.

**Remark 2.** Here, we compared \( C_P \) with the lower bounds of \( C_A \). When \( a = \log_2 (q^{g(K(C))n}) \) exceeds certain value (depending on a prime number \( n \)), \( C_P \) become larger than the lower bounds of \( C_A \). If \( n = 13, \delta = 4, 5, 6, a \geq 160 \), \( C_P \) become larger than the lower bound of \( C_A \). In fact the upper bound of \( a = \log_2 (q^{g(K(C))n}) \) such that \( C_P < C_A \) can be showed as follows: if \( n = 11 \), \( C_P < C_A \) for \( a \leq 1765 \) (In particular, the value of (19) become slightly larger than (18) when \( a = 1766, n = 11, \delta = 5, 6. \)), if \( n = 7 \), \( C_P < C_A \) for \( a \leq 5025 \). Furthermore if \( n \geq 17 \), the upper bound of \( a = \log_2 (q^{g(K(C))n}) \) such that \( C_P < C_A \) become larger. Such upper bound of \( a = \log_2 (q^{g(K(C))n}) \) increases when the lower bound of \( g(F) \) increases.

Finally we estimate the group size \#\( C_P(F) \) when \#\( C_P(K(C)) \geq 2^{100} \). Since
\[ \log_2 q^{g(F)} = \frac{q(F) a}{g(K(C)) n}, \] (20)
by calculating the lower bounds of \( q^{g(F)} \) using (8) and (11), we obtained lower bounds of the group size \#\( C_P(F) \).

**Theorem 7.** Let \( n, r \) be prime numbers \((n \geq 7, n \neq r)\), and let \( C \) be a superelliptic curve which is non-hyperelliptic curve, \( g(K(C)) \leq 4, q^{g(K(C))n} \geq 2^{160} \). Then we have \( q^{g(F)} \geq 2^{280} \) except that \( n = 13, \delta = 4, 5, 6. \)

**Remark 3.** If \( n = 13, \delta = 4, r = 3 \) \((g(K(C))) = 3)\), \( q^{g(F)} \geq 2^{273} \). Similarly \( q^{g(F)} \geq 2^{280} \) for \( n = 13, \delta = 5, r = 3 \) \((g(K(C))) = 4)\), and \( q^{g(F)} \geq 2^{280} \) for \( n = 13, \delta = 6, r = 3 \) \((g(K(C))) = 4)\).

The fastest subexponential algorithms known for computing discrete logarithms (e.g. in the multiplicative group) become infeasible for a group size of 1024 bit. Therefore, the GHS Weil descent attack will not be efficient even if we could find and apply certain subexponential algorithm such as the ADH algorithm to attack DL on \( C_P(F) \) when \( q^{g(F)} \) is very large (e.g. \( q^{g(F)} \geq 2^{1024} \) [18].

In conclusion, DL on the above superelliptic curves will be infeasible for subexponential algorithms solving DL problems in the present state-of-art. (February, 14, 2005 Revised).
References


If $r = 3, 5$, then $g(K(C)) \leq 4$.