Weil descent attack against genus two hyperelliptic curve cryptosystems over even degree finite fields

Seigo Arita

Internet Systems Research Laboratories, NEC, Kawasaki Kanagawa, Japan,
s-arita@ab.jp.nec.com

Abstract. *The paper shows that genus two hyperelliptic curve cryptosystems over even degree finite fields come under Weil descent attack. Given a hyperelliptic curve of genus two over an even degree finite field, we construct an algebraic curve of genus eight over the subfield of the half-degree using the technique of Weil descent. We reduce DLP(Discrete Logarithm Problem) on the hyperelliptic curve to DLP on the new curve, and apply Gaudry attack against the C_{ab} model of the curve.*

1 Introduction

The concept of Weil descent attack was introduced by Frey[6], and Gaudry,Hess,Smart[9] showed that some of elliptic curve cryptosystems over finite fields of characteristic two are really attacked by Weil descent attack. It was shown that Weil descent attack can be applied also for some of hyperelliptic curve cryptosystems over finite fields of characteristic two and some of elliptic curve cryptosystems over finite fields of characteristic three, respectively by Galbraith[7] and Arita[4]. Moreover, Diem[5] found that there are some cases in which Weil descent attack seems to be possible even in general characteristics of elliptic or hyperelliptic curve cryptosystems.

In general, Weil descent attack could be applied against an algebraic curve cryptosystem over a composition field. Suppose an algebraic curve over a composition field is given. In Weil descent attack, using the technique of Weil descent, we construct a new algebraic curve of bigger genus than the original curve defined on the smaller subfield than the original field. We reduce DLP(Discrete Logarithm Problem) on the original curve to DLP on the new curve, and apply Gaudry attack[8] against the new curve.

Recently, genus two hyperelliptic curve over even degree finite fields are watched with interest [10, 11] because of its good property to compute the order of Jacobian group. The presented paper shows that genus two hyperelliptic curve cryptosystems over even degree finite fields come under Weil descent attack.

Given a hyperelliptic curve of genus two over an even degree finite field of order q^2, we construct an algebraic curve of genus eight over the subfield of order q using the technique of Weil descent. We explicitly reduce DLP on the hyperelliptic curve to DLP on the new curve, and apply a variant of Gaudry

attack[3] against the C_{ab} model[12, 2] of the new curve. Gaudry attack and its variant solves DLP on algebraic curve of genus g defined on a finite field of order q in the amount of computations $O(q^{\frac{2g}{g+1}})$ [9]. So, DLP on genus two hyperelliptic curve over an even degree finite field of order q^2 can be solved by Weil descent attack in the amount of computations $O(q^{\frac{16}{9}})$, which is less than $O(q^2)$ for Pollard's ρ-method.

In the paper, we assume that the characteristic of the definition field is not two, and we also assume some condition for hyperelliptic curves to be attacked. However, these assumptions seem to be only for simplicity. We believe in that Weil descent attack in the paper can be applied for all of the genus two hyperelliptic curve cryptosystems over even degree finite fields with a slight modification.

2 Weil descent of hyperelliptic curves and their GHS-sections

Let H be a genus two hyperelliptic curve defined on a finite field $K = F_{q^2}$ which is a quadratic extension field of a finite field $k = F_q$ of characteristic different from 2:

$$H : y^2 = x^5 + bx^4 + cx^3 + dx^2 + ex + f.$$

A scalar restriction $\Pi_{K/k}H$ of H with respect to the extension K/k is a two-dimensional abelian variety defined by the following two conjugate equations

$$\begin{aligned} y_1^2 &= x_1^5 + bx_1^4 + cx_1^3 + dx_1^2 + ex_1 + f, \\ y_2^2 &= x_2^5 + b^q x_2^4 + c^q x_2^3 + d^q x_2^2 + e^q x_2 + f^q. \end{aligned}$$

$\Pi_{K/k}H$ is geometrically defined on k. Let σ be q-th power Frobenius map. σ can be extended to the automorphism of the function field $K(x, y_1, y_2)$ of D by

$$\sigma(x_1) = x_2, \sigma(y_1) = y_2.$$

We should find an algebraic curve D on $\Pi_{K/k}H$ defined over k, and reduce DLP on the hyperelliptic curve H to DLP on the curve D in order to apply Gaudry attack[8].

In Weil descent attack, the choice of the above curve D on $\Pi_{K/k}H$ is critical. In the presented paper, just as in [9],[7], we let the curve D be the intersection of $\Pi_{K/k}H$ and hypersurface $(x :=)x_1 = x_2$, which we call 'GHS-section'. GHS-section D is an algebraic curve geometrically defined on k by the equations

$$\begin{aligned} y_1^2 &= x^5 + bx^4 + cx^3 + dx^2 + ex + f, \\ y_2^2 &= x^5 + b^q x^4 + c^q x^3 + d^q x^2 + e^q x + f^q. \end{aligned}$$

It is easily seen that GHS-section D is a nonsingular affine curve under

Assumption 1 $x^5 + bx^4 + cx^3 + dx^2 + ex + f$ contains no non-trivial factor defined on k.

In the paper, we assume Assumption 1. However, even without Assumption 1, the attack remains unchanged except for the more complicated details of construction of the C_{ab} model for D.

In cases of [9] and [7], GHS-sections D have huge genera. Since the complexity of Gaudry attack with respect to the genus g is $O(g!)$, the genus of the curve attacked by Gaudry attack should be not much greater than ten under the usual regions of security parameters. So, in [9] and [7] Weil descent attack can be applied only in special cases in which we can take the irreducible component of small genus of GHS-section D.

However, in our cases,

Proposition 1. *The genus of GHS-section D is eight.*

Proof. The function field $K(x, y_1, y_2)$ of GHS-section D is a quadratic extension of the hyperelliptic function field $K(x, y_1)$. Since there are only ten ramification points of degree two in the quadratic extension, Hurwitz formula says D is of genus eight □

Therefore, we don't need to take irreducible components of D. The only thing we have to do is to construct a model over k of GHS-section D against which we can apply Gaudry attack. If we can construct such a model, DLP on H can be solved by Gaudry attack in the amount of computations $O(q^{\frac{2g}{g+1}}) = O(q^{\frac{16}{9}})$ [9], which is less than $O(q^2)$ for Pollard's ρ-method.

Gaudry attack is extended for C_{ab} curves[3]. So, hereafter, we construct a C_{ab} model over k of GHS-section D.

3 C_{ab} model of GHS-section

In general, to construct a C_{ab} model of a given curve D, we need to choose a point, which we call a 'base point', and to determine all of the regular functions outside the base point on D.

Remember that GHS-section D is defined by two equations

$$y_1^2 = x^5 + bx^4 + cx^3 + dx^2 + ex + f,$$
$$y_2^2 = x^5 + b^q x^4 + c^q x^3 + d^q x^2 + e^q x + f^q.$$

Since the function field $K(x, y_1, y_2)$ of GHS-section D is a quadratic extension of the hyperelliptic function field $K(x, y_1)$, GHS-section D has (including multiplicities) two infinite places P_1 and P_2 over the unique infinite place P of $K(x, y_1)$. So, we choose the infinite place P_2 as the base point of C_{ab} model of D. As shown later, the place P_2 is defined on k. The property is useful to construct C_{ab} model over k, more than K.

To determine all of the regular functions outside the base point P_2, we need to know the 'value' of a given function at infinite places P_1 and P_2. So, first, we find local parameter expansions of infinite places P_1 and P_2.

3.1 Infinite places of GHS-section

Let $t := x^2/y_1$. t is a local parameter at a unique infinite place P of $K(x, y_1)$. Using t, x and y_1 are expanded as

$$x = t^{-2} + \alpha_0 + \alpha_2 t^2 + \cdots,$$
$$y_1 = t^{-5} + \beta_{-3} t^{-3} + \beta_{-1} t^{-1} + \cdots.$$

Substituting the above parameter expansion of x for the second equation of GHS-section D, we get

$$y_2^2 = t^{-10} + \gamma_{-8} t^{-8} + ...$$

Since the characteristic is different from 2, this has two distinct solutions $y201 = t^{-5}+\cdots$, and $y202 = -t^{-5}+\cdots$. This shows that the infinite place P of $K(x, y_1)$ is decomposed into two distinct infinite places P_1 and P_2 of $K(x, y_1, y_2)$, and those expansions by t are given by

$$\begin{aligned} P_1 = \{&x = t^{-2} + \alpha_0 + \alpha t^2 + \cdots, \\ &y_1 = t^{-5} + \beta_{-3} t^{-3} + \beta_{-1} t^{-1} + \beta_1 t + \cdots, \\ &y_2 = y201 = t^{-5} + \cdots\}, \end{aligned}$$

$$\begin{aligned} P_2 = \{&x = t^{-2} + \alpha_0 + \alpha t^2 + \cdots, \\ &y_1 = t^{-5} + \beta_{-3} t^{-3} + \beta_{-1} t^{-1} + \beta_1 t + \cdots, \\ &y_2 = y202 = -t^{-5} + \cdots\}. \end{aligned}$$

Obviously, the set of infinite places $\{P_1, P_2\}$ is fixed by the Frobenius map σ. Actually,

Proposition 2. *Every P_i is defined on k for $i = 1$ and 2.*

Proof. Let $f = y_1 + y_2$.

Suppose $\sigma(P_1) = P_2$. Then, by the above expansions we see

$$v_{P_1}(\sigma(f)) = v_{P_2}(f) \geq -3.$$

On the other hand, since y_1 and y_2 are conjugate over K/k, $\sigma(f) = f$. So,

$$v_{P_1}(\sigma(f)) = v_{P_1}(f) = -5.$$

This is a contradiction □

3.2 Regular functions outside the base point

We have to determine regular functions outside the base point P_2 on GHS-section D. Those functions are regular in $x - y_1 - y_2$ affine space. So, they are expressed by polynomials on x, y_1 and y_2 since D is nonsingular in the affine space by Assumption 1.

Since GHS-section D is of genus eight, assuming P_2 is not a Weierstrass point of D, the minimum generators of pole numbers at P_2 is $\{9, 10, 11, 12, 13, 14, 15, 16, 17\}$. So, polynomials $f_9, f_{10}, \ldots, f_{17}$, which is regular at P_1 and has pole order $9, 10, \ldots, 17$ at P_2 respectively, generate the algebra of regular functions outside P_2. Therefore, in order to determine the regular functions outside P_2, it is sufficient to construct the polynomials $f_9, f_{10}, \ldots, f_{17}$. (Even if P_2 is Weierstrass point, the situation is similar except for the members of the minimum generators of pole numbers at P_2.)

Let $f = \Sigma_i c_i M_i$ be a (non-constant) polynomial which is regular at P_1 with elements c_i in K and with monomials M_i on x, y_1, y_2. Suppose M_i are in the descending order with respect to the pole order at P_1. Then, since f is regular at P_1, the pole orders of M_1 and M_2 at P_1 must be the same.

So, in order to construct a polynomial regular at P_1, we recursively take a suitable linear sum of polynomials which have the same pole order at P_1, until we get the polynomial regular at P_1. Note we can know the 'value' of polynomials at P_1 using local parameter expansions of P_1 in section 3.1. To get $f_9, f_{10}, \ldots, f_{17}$, it is sufficient to treat with polynomials of at most 9-th degree with respect to x and of at most 1-st degree with respect to y in the above recursions.

Using those polynomials $f_9, f_{10}, \ldots, f_{17}$, we can construct an explicit $C_{9,10,\cdots,17}$ model of GHS-section D over K [12]. To construct an $C_{9,10,\cdots,17}$ model C over k, instead of K, it is sufficient to use $g_i = \mathrm{Tr}_{K/k}(f_i)(i = 9, 10, \ldots, 17)$ instead of f_i since P_1 and P_2 are defined over k by Proposition 2. Here, $\mathrm{Tr}_{K/k}$ is defined by

$$\mathrm{Tr}_{K/k}(\Sigma a_{l,m,n} x^l y_1^m y_2^n) = \Sigma a_{l,m,n}^q x^l y_2^m y_1^n.$$

Note The pole order of a polynomial f at P_2 possibly decreases by taking $\mathrm{Tr}_{K/k}$. Even in the case, we can remain the pole order unchanged by using a suitable scalar product cf instead of f.

4 Reduction

In the last section, under the assumption that P_2 is not a Weierstrass point, we construct a $C_{9,10,\ldots,17}$ model C of GHS-section D over k:

$$\begin{aligned} K(x, y_1, y_2) &\overset{\Phi}{\to} K(f_9, f_{10}, \ldots, f_{17}) = K(g_9, g_{10}, \ldots, g_{17}) \\ &\overset{\mathrm{N}_{K/k}}{\to} k(g_9, g_{10}, \ldots, g_{17}) \end{aligned}$$

Making a composition of the birational function Φ with norm map $\mathrm{N}_{K/k}$, we obtain a morphism $\Psi_1 = (\mathrm{N}_{K/k} \cdot \Phi)^\star$ from Jacobian group (i.e. divisor class group of degree zero) of GHS-section D to Jacobian group of the $C_{9,10,\ldots,17}$ model C over k:

$$\begin{aligned} Cl^0(K(x, y_1, y_2)) &\overset{\Psi_1}{\to} Cl^0(k(g_9, g_{10}, \ldots, g_{17})) \\ \Sigma Q_i - nP_2 &\mapsto \mathrm{N}_{K/k}(\Sigma \Phi(Q_i) - n\infty) \end{aligned}$$

Let π be the projection from GHS-section D to the hyperelliptic curve H:

$$\begin{aligned} D &\xrightarrow{\pi} H \\ (x, y_1, y_2) &\mapsto (x, y_1) \end{aligned}$$

The projection π induces a morphism Ψ_2 from Jacobian group of the hyperelliptic curve H to Jacobian group of GHS-section D:

$$\begin{aligned} Cl^0(K(x, y_1)) &\xrightarrow{\Psi_2} Cl^0(K(x, y_1, y_2)) \\ Q_1 + Q_2 - 2P &\mapsto \pi^{-1}(Q_1) + \pi^{-1}(Q_2) - 2(P_1 + P_2) \end{aligned}$$

The composition $\Psi_2 \cdot \Psi_1$ reduces DLP on H to DLP on $C_{9,10,\ldots,17}$ model C over k.

The composition $\Psi_2 \cdot \Psi_1$ can be computed using ideals. Let $R = K[x, y_1]$ and $R_1 = K[x, y_1, y_2]$ be the coordinate ring of the hyperelliptic curve H and of GHS-section D respectively. Suppose an element of Jacobian group of H is given as an ideal ih of R. $w = \Psi_2(ih)$ is nothing but an ideal generated by ih in $R_1(\supset R)$. Since w itself includes P_1 as a double pole, taking a product with a polynomial g having P_1 as a double zero to vanish the pole at P_1, the image of w by Ψ_1 is computed by the elimination ideal as follows:

$$\begin{aligned} w &\leftarrow w \cdot g \\ v &\leftarrow \text{Eliminate}(w + \\ &\qquad (\check{g}_9 - g_9(x, y_1, y_2), \check{g}_{10} - g_{10}(x, y_1, y_2), \ldots, \\ &\qquad \check{g}_{17} - g_{17}(x, y_1, y_2)), \{x, y_1, y_2\}) \\ v &\leftarrow \text{Reduce}(v) \\ \Psi_1 \cdot \Psi_2(ih) &\leftarrow \text{jSum}(v, \tilde{v}) \end{aligned}$$

Here, $\text{Eliminate}(w+(\check{g}_9-g_9(x, y_1, y_2), \check{g}_{10}-g_{10}(x, y_1, y_2), \ldots, \check{g}_{17}-g_{17}(x, y_1, y_2), \{x, y_1, y_2\})$ denotes the ideal with respect to variables $\check{g}_i (i = 9, 10, .., 17)$ obtained by eliminating the variables x, y_1, y_2 from the ideal of the first argument. v can be seen as an ideal of the coordinate ring of C, which represents relations among $g_i (i = 9, 10, \ldots, 17)$ over w, that is $\Phi^\star(w)$. $\text{Reduce}(v)$ reduces the ideal v in the meaning of [2]. $\text{jSum}(v, \tilde{v})$ computes a sum of v and its conjugate $\tilde{v}$ in Jacobian of C, that is a norm of v with respect to K/k.

For the details of Reduce and jSum, we refer [2].

5 Examples

5.1 Example 1

We illustrate our method of Weil descent attack by explaining an example. In the following computation, we used Magma Ver2.7-2.

Let k be a prime field of characteristic $p = 71$, and K be its quadratic extension defined by an irreducible polynomial $a^2 - 2a + 7$. a is a primitive element of K. We take a genus two hyperelliptic curve

$$H : y_1^2 = x^5 + a^{48}x^4 + a^{33}x^3 + a^9x^2 + a^{26}x + a^{31}$$

over K (Coefficients are randomly selected).

Computing expansions by the local parameter $t = x^2/y_1$ of infinite places P_1, P_2 of GHS-section D of $\Pi_{K/k}H$ as in Section 3.1, we get

$$\begin{aligned}
P_1 = \{ & \\
x &= t^{-2} + a^{2568} + a^{2553}t^2 + a^{3825}t^4 + a^{4716}t^6 + a^{4511}t^8 + a^{174}t^{10} + a^{4065}t^{12} + a^{4196}t^{14} + \ldots, \\
y_1 &= t^{-5} + a^{3000}t^{-3} + a^{2603}t^{-1} + a^{2961}t + a^{2701}t^3 + a^{3955}t^5 + a^{201}t^7 + a^{201}t^9 + a^{2795}t^{11} + \ldots, \\
y_2 &= t^{-5} + a^{3197}t^{-3} + a^{4420}t^{-1} + a^{3921}t + a^{3709}t^3 + a^{2562}t^5 + a^{2702}t^7 + a^{3976}t^9 + a^{2139}t^{11} + \ldots\},
\end{aligned}$$

$$\begin{aligned}
P_2 = \{ & \\
x &= t^{-2} + a^{2568} + a^{2553}t^2 + a^{3825}t^4 + a^{4716}t^6 + a^{4511}t^8 + a^{174}t^{10} + a^{4065}t^{12} + a^{4196}t^{14} + \ldots, \\
y_1 &= t^{-5} + a^{3000}t^{-3} + a^{2603}t^{-1} + a^{2961}t + a^{2701}t^3 + a^{3955}t^5 + a^{201}t^7 + a^{201}t^9 + a^{2795}t^{11} + \ldots, \\
y_2 &= 70t^{-5} + a^{677}t^{-3} + a^{1900}t^{-1} + a^{1401}t + a^{1189}t^3 + a^{42}t^5 + a^{182}t^7 + a^{1456}t^9 + a^{4659}t^{11} + \ldots\}.
\end{aligned}$$

Using these expansions, we get polynomials regular at P_1 $g_9, g_{10}, \ldots, g_{17}$ with pole orders $9, 10, \ldots, 17$ at P_2 respectively as in Section 3.2:

$$\begin{aligned}
g_9 &= a^{1332}x^3y_1 + a^{3852}x^3y_2 + a^{1476}x^2y_1 + a^{3996}x^2y_2 + xy_1^3 + 70xy_1^2y_2 + 70xy_1y_2^2 + \\
&\quad a^{637}xy_1 + xy_2^3 + a^{4907}xy_2 + a^{4617}y_1^3 + a^{2097}y_1^2y_2 + a^{2727}y_1y_2^2 + a^{4096}y_1 + a^{207}y_2^3 + a^{3536}y_2 \\
g_{10} &= x^3 + 21x^2 + 67x + 27y_1^2 + 17y_1y_2 + 27y_2^2 + 42 \\
g_{11} &= a^{2844}x^3y_1 + a^{324}x^3y_2 + a^{3385}x^2y_1 + a^{3455}x^2y_2 + a^{2017}xy_1 + a^{2087}xy_2 + a^{2283}y_1 + a^{813}y_2 \\
g_{12} &= 60x^2 + 70xy_1^2 + 2xy_1y_2 + 70xy_2^2 + 30x + a^{2923}y_1^2 + 42y_1y_2 + a^{893}y_2^2 + 43 \\
g_{13} &= x^3y_1 + x^3y_2 + a^{2228}x^2y_1 + a^{1948}x^2y_2 + a^{480}xy_1 + a^{3840}xy_2 + 27y_1^3 + 44y_1^2y_2 + \\
&\quad 44y_1y_2^2 + a^{2975}y_1 + 27y_2^3 + a^{4585}y_2 \\
g_{14} &= 70x^2y_1^2 + 2x^2y_1y_2 + 70x^2y_2^2 + 36x^2 + a^{3492}xy_1^2 + a^{972}xy_2^2 + 17x + 63y_1^2 + 66y_1y_2 + 63y_2^2 + 60 \\
g_{15} &= a^{4533}x^2y_1 + a^{4323}x^2y_2 + a^{4591}xy_1 + a^{3401}xy_2 + a^{2844}y_1^3 + a^{2196}y_1^2y_2 + a^{4716}y_1y_2^2 + \\
&\quad a^{1059}y_1 + a^{324}y_2^3 + a^{4629}y_2 \\
g_{16} &= 2x^3y_1y_2 + 21x^2y_1^2 + 21x^2y_2^2 + 62x^2 + a^{1911}xy_1^2 + a^{4641}xy_2^2 + 41x + 49y_1^4 + 44y_1^2y_2^2 + \\
&\quad a^{3045}y_1^2 + 24y_1y_2 + 49y_2^4 + a^{4515}y_2^2 + 16 \\
g_{17} &= a^{3659}x^2y_1 + a^{2749}x^2y_2 + a^{2521}xy_1^3 + axy_1^2y_2 + a^{71}xy_1y_2^2 + a^{4040}xy_1 + a^{2591}xy_2^3 + \\
&\quad a^{4600}xy_2 + a^{2212}y_1^3 + a^{537}y_1^2y_2 + a^{2847}y_1y_2^2 + a^{4656}y_1 + a^{812}y_2^3 + a^{2976}y_2
\end{aligned}$$

The following equations hold among $g_9, g_{10}, \ldots, g_{17}$, which define $C_{9,10,\ldots,17}$ curve C over k in $g_9 - g_{10} - \cdots - g_{17}$ affine space.

$$g_{10}^2 - (9g_9g_{11} + 58g_9^2 + 35g_{16} + 11g_{14} + 19g_{12} + 29g_{10}) = 0$$

$$g_{10}g_{11} - (2g_9g_{12} + 15g_9g_{10} + 45g_{17} + 17g_{15} + 47g_{13} + 16g_{11} + 27g_9) = 0$$
$$g_{10}g_{12} - (25g_9g_{13} + 59g_9g_{11} + 15g_9^2 + 7g_{16} + 43g_{14} + 62g_{12} + 27g_{10}) = 0$$
$$g_{10}g_{13} - (35g_9g_{14} + 53g_9g_{12} + 49g_9g_{10} + 12g_{17} + 44g_{15} + 22g_{13} + 16g_{11} + 68g_9) = 0$$
$$g_{10}g_{14} - (65g_9g_{15} + 63g_9g_{13} + 12g_9g_{11} + 45g_9^2 + 9g_{16} + 21g_{14} + 14g_{12} + g_{10}) = 0$$
$$g_{10}g_{15} - (8g_9g_{16} + 30g_9g_{14} + 50g_9g_{12} + 48g_9g_{10} + 58g_{17} + 59g_{15} + 65g_{13} + 2g_{11} + 3g_9) = 0$$
$$g_{10}g_{16} - (47g_9g_{17} + 63g_9g_{15} + 46g_9g_{13} + 27g_9g_{11} + 36g_9^2 + 61g_{16} + 8g_{14} + 29g_{12} + 63g_{10}) = 0$$
$$g_{10}g_{17} - (5g_9^3 + 28g_9g_{16} + 46g_9g_{14} + 39g_9g_{12} + 32g_9g_{10} + 5g_{17} + 6g_{15} + 29g_{13} + 4g_{11} + 64g_9) = 0$$
$$g_{11}g_{17} - (40g_9^2g_{10} + 53g_9g_{17} + 14g_9g_{15} + 10g_9g_{13} + 10g_9g_{11} + 52g_9^2 + g_{16} + 68g_{14} + 17g_{12} + 2g_{10}) = 0$$

We take two elements ih_1 and ih_2 of Jacobian of the hyperelliptic curve H:

$$\begin{aligned} ih_1 &= \{y_1 + a^{3334}x + a^{4925}, x^2 + a^{3249}x + a^{4945}\} \\ ih_2 &= 22947908 \cdot ih_1 \\ &= \{y_1 + a^{1479}x + a^{4455}, x^2 + a^{3965}x + a^{4919}\} \end{aligned}$$

Computing $ic_i = \Psi_1 \cdot \Psi_2(ih_i)$, we get following two elements ic_1 and ic_2 of Jacobian of $C_{9,10,\ldots,17}$ curve C:

$$\begin{aligned} ic_1 = \{ & \\ & g_{15}^2 + 24g_{15} + 11g_{14} + 30g_{13} + 24g_{12} + 25g_{11} + 19g_{10} + 54g_9 + 66, \\ & g_{14}g_{15} + 70g_{15} + 31g_{14} + 4g_{13} + 9g_{12} + 23g_{11} + 45g_{10} + 39g_9 + 5, \\ & g_{14}^2 + 32g_{15} + 59g_{14} + 37g_{12} + g_{11} + 35g_{10} + 2g_9 + 15, \\ & g_{13}g_{15} + 66g_{15} + 4g_{14} + 4g_{13} + 65g_{12} + 13g_{11} + 3g_{10} + 38g_9 + 12, \\ & g_{13}g_{14} + 38g_{15} + 68g_{14} + 54g_{13} + 7g_{12} + 37g_{11} + g_{10} + 44g_9 + 2, \\ & g_{12}g_{15} + 29g_{15} + 33g_{14} + 37g_{13} + 55g_{12} + 20g_{11} + 41g_{10} + 44g_9 + 22, \\ & g_{13}^2 + 62g_{15} + 49g_{14} + 44g_{13} + 54g_{12} + 61g_{11} + 11g_{10} + 17, \\ & g_{12}g_{14} + g_{14} + 43g_{13} + 33g_{12} + 20g_{11} + 56g_{10} + 2g_9 + 24, \\ & g_{11}g_{15} + 2g_{15} + 44g_{14} + 41g_{13} + 8g_{12} + 35g_{11} + 25g_{10} + 14g_9 + 53, \\ & g_{12}g_{13} + 28g_{15} + 8g_{14} + 39g_{13} + 9g_{12} + 17g_{11} + 14g_{10} + 52g_9 + 5, \\ & g_{11}g_{14} + 46g_{15} + 20g_{14} + 68g_{13} + 53g_{12} + 38g_{11} + 23g_{10} + 14g_9 + 65, \\ & g_{10}g_{15} + 24g_{15} + 45g_{14} + 51g_{13} + 11g_{12} + 7g_{11} + 14g_{10} + 63g_9 + 51, \\ & g_{12}^2 + 60g_{15} + 26g_{14} + 7g_{13} + 42g_{12} + g_{11} + 3g_{10} + 60g_9 + 66, \\ & g_{11}g_{13} + 34g_{15} + 10g_{14} + 53g_{13} + 62g_{12} + 26g_{11} + 15g_{10} + 13g_9 + 46, \\ & g_{10}g_{14} + 12g_{15} + 21g_{14} + 45g_{12} + 17g_{11} + 24g_{10} + 24g_9 + 34, \\ & g_9g_{15} + 36g_{15} + 68g_{14} + 32g_{13} + 41g_{12} + 15g_{11} + 32g_{10} + 44g_9 + 52, \\ & g_{11}g_{12} + 25g_{15} + 40g_{14} + 47g_{13} + 56g_{12} + 35g_{11} + 62g_{10} + 11g_9 + 40, \\ & g_{10}g_{13} + 60g_{15} + 36g_{14} + 42g_{13} + 68g_{12} + 30g_{11} + 25g_{10} + 10g_9 + 3, \\ & g_9g_{14} + 33g_{15} + 23g_{14} + 26g_{13} + 68g_{12} + 68g_{11} + 51g_{10} + 48g_9 + 30, \end{aligned}$$

$$
\begin{aligned}
&g_{11}^2 + 53g_{15} + 29g_{14} + 33g_{13} + 40g_{12} + g_{11} + 39g_{10} + 19g_9 + 42,\\
&g_{10}g_{12} + 36g_{15} + 25g_{14} + 49g_{13} + 13g_{12} + 57g_{10} + 56g_9 + 6,\\
&g_9g_{13} + 58g_{15} + 53g_{14} + 27g_{13} + g_{12} + 69g_{11} + 64g_{10} + 33g_9 + 38,\\
&g_{10}g_{11} + 15g_{15} + 34g_{14} + 15g_{13} + 49g_{12} + 14g_{11} + 70g_{10} + 7g_9 + 54,\\
&g_9g_{12} + 49g_{15} + 30g_{14} + 25g_{13} + 48g_{12} + 39g_{11} + 15g_{10} + 11g_9 + 63,\\
&g_{10}^2 + 42g_{15} + 10g_{14} + 54g_{13} + 68g_{12} + 64g_{11} + 36g_{10} + 42g_9 + 26,\\
&g_9g_{11} + 17g_{15} + 44g_{14} + 21g_{13} + 14g_{12} + 18g_{11} + 6g_{10} + 64g_9 + 2,\\
&g_9g_{10} + 2g_{15} + 12g_{14} + 23g_{13} + 33g_{12} + 59g_{11} + 65g_{10} + 29g_9 + 62,\\
&g_9^2 + 14g_{15} + 29g_{14} + 65g_{13} + 33g_{12} + 13g_{11} + 9g_{10} + 52g_9 + 38,\\
&g_{17} + 31g_{15} + 68g_{14} + 21g_{13} + 70g_{12} + 55g_{11} + 66g_{10} + 19g_9 + 44,\\
&g_{16} + 67g_{14} + g_{12} + 28g_{10} + 61\},
\end{aligned}
$$

$$
\begin{aligned}
ic_2 = \{&\\
&g_{15}^2 + 2g_{15} + 37g_{14} + 24g_{13} + 61g_{12} + 2g_{11} + 2g_{10} + 20g_9 + 26,\\
&g_{14}g_{15} + 18g_{15} + 37g_{14} + 23g_{13} + 51g_{12} + 23g_{11} + 4g_{10} + 51,\\
&g_{14}^2 + 2g_{15} + 13g_{14} + 45g_{13} + 64g_{12} + g_{11} + 11g_{10} + 55g_9 + 61,\\
&g_{13}g_{15} + 13g_{15} + 10g_{14} + 61g_{13} + 7g_{12} + 10g_{11} + 49g_{10} + 69g_9 + 4,\\
&g_{13}g_{14} + 64g_{15} + 23g_{14} + 3g_{13} + 9g_{12} + 70g_{11} + 3g_{10} + 41g_9 + 56,\\
&g_{12}g_{15} + 11g_{15} + 55g_{14} + 68g_{13} + 46g_{12} + 61g_{11} + 67g_{10} + 35g_9 + 25,\\
&g_{13}^2 + 49g_{15} + 6g_{14} + 65g_{13} + 48g_{12} + 36g_{11} + 49g_{10} + 63g_9 + 63,\\
&g_{12}g_{14} + 21g_{15} + g_{14} + 32g_{13} + 40g_{12} + 46g_{11} + 23g_{10} + 70g_9 + 56,\\
&g_{11}g_{15} + 70g_{15} + 35g_{14} + 70g_{13} + 22g_{12} + 38g_{11} + 52g_{10} + 17g_9 + 46,\\
&g_{12}g_{13} + 12g_{15} + 50g_{14} + 25g_{13} + 47g_{12} + 8g_{11} + 47g_{10} + 25g_9 + 55,\\
&g_{11}g_{14} + 62g_{15} + 19g_{14} + 22g_{13} + 27g_{12} + 32g_{11} + 21g_{10} + 2g_9 + 41,\\
&g_{10}g_{15} + 30g_{15} + 27g_{14} + 61g_{13} + 5g_{12} + 44g_{11} + 24g_{10} + 53g_9 + 27,\\
&g_{12}^2 + 66g_{15} + 27g_{14} + 26g_{13} + 61g_{12} + 69g_{11} + 38g_{10} + 12g_9 + 33,\\
&g_{11}g_{13} + 34g_{15} + 52g_{14} + 70g_{13} + 33g_{12} + 11g_{11} + 12g_{10} + 21g_9 + 40,\\
&g_{10}g_{14} + 32g_{15} + 24g_{14} + 27g_{13} + 12g_{12} + 43g_{11} + 59g_{10} + 46g_9 + 29,\\
&g_9g_{15} + 62g_{15} + 59g_{14} + 55g_{13} + 43g_{12} + 27g_{11} + 68g_{10} + 17g_9 + 62,\\
&g_{11}g_{12} + 35g_{15} + 43g_{14} + 42g_{13} + 17g_{12} + 21g_{11} + 57g_{10} + 29g_9 + 25,\\
&g_{10}g_{13} + 66g_{15} + 4g_{14} + 29g_{13} + 16g_{12} + 6g_{11} + 48g_{10} + 3g_9 + 27,\\
&g_9g_{14} + 56g_{15} + 7g_{14} + 49g_{13} + 62g_{12} + 67g_{11} + 21g_{10} + 25g_9 + 27,\\
&g_{11}^2 + 36g_{15} + 14g_{14} + 67g_{13} + 31g_{12} + 68g_{11} + 14g_{10} + 30g_9 + 38,\\
&g_{10}g_{12} + 70g_{15} + 10g_{14} + 58g_{13} + 49g_{12} + 69g_{11} + 36g_{10} + 57g_9 + 68,\\
&g_9g_{13} + 16g_{15} + 18g_{14} + 51g_{12} + 28g_{11} + 64g_{10} + 4g_9 + 23,\\
&g_{10}g_{11} + 62g_{15} + 64g_{14} + 40g_{13} + 46g_{12} + 68g_{11} + 61g_{10} + 58g_9 + 41,
\end{aligned}
$$

$$g_9g_{12} + 48g_{15} + 34g_{14} + 20g_{13} + 19g_{12} + 55g_{11} + 2g_{10} + 54g_9 + 45,$$
$$g_{10}^2 + 15g_{15} + 28g_{14} + 8g_{13} + 48g_{12} + 49g_{11} + 43g_{10} + 25g_9 + 6,$$
$$g_9g_{11} + 11g_{15} + 52g_{14} + 26g_{13} + 41g_{12} + 4g_{11} + 68g_{10} + 2g_9 + 10,$$
$$g_9g_{10} + 21g_{15} + 15g_{14} + 51g_{13} + 33g_{12} + 49g_{11} + 36g_{10} + 41g_9 + 63,$$
$$g_9^2 + g_{15} + 21g_{14} + g_{13} + 54g_{12} + 70g_{11} + 16g_{10} + 65g_9 + 54,$$
$$g_{17} + 51g_{15} + 17g_{14} + 44g_{13} + 16g_{12} + 32g_{11} + 65g_{10} + 30g_9,$$
$$g_{16} + 28g_{14} + 52g_{12} + 25g_{10} + 42\}.$$

We verified that

$$ic_2 = 22947908 \cdot ic_1.$$

6 Example 2

We take the hyperelliptic curve with 160 bits Jacobian computed by Matuo,Chao,Tsujii[11]. In the following computation, we used Magma Ver2.7-2.

Let k be the quadratic extension of the prime field of characteristic $p = 2^{20}-5$ defined by the irreducible polynomial $o^2 - 90247o + 719293$, and let K be the quadratic extension of k defined by the irreducible polynomial $r^2 - (987525o + 922395)r + 883232o + 496324$.

With $a = -1048570r$, for

$$b = 0$$
$$c = 508797a^3 + 672555a^2 + 940125a + 153314$$
$$d = 330843a^3 + 367275a^2 + 910087a + 1002854$$
$$e = 488395a^3 + 873290a^2 + 734350a + 7072$$
$$f = 180553a^3 + 25142a^2 + 806296a + 724502$$

Matuo,Chao,Tsujii[11] showed that the hyperelliptic curve $H : y_1^2 = x^5 + bx^4 + cx^3 + dx^2 + ex + f$ over K has Jacobian group of order $n = 37 \cdot 79 \cdot 6055499440163 \cdot 82566515265200206423105450287439$.

It turns out that GHS-section D of $\Pi_{K/k}H$ has the $C_{9,10,\ldots,17}$ model C over k in $g_9 - g_{10} - \cdots - g_{17}$ affine space with defining equations

$$g_{10}^2 - ((771753o + 64319)g_9g_{11} + (101175o + 528929)g_9^2 + (153638o + 895367)g_{16} + 427952o + 220416)g_{14} + (1035163o + 747982)g_{12} + (151152o + 313754)g_{10}) = 0$$
$$g_{10}\, g_{11} - ((303495o + 843209)g_9g_{12} + (486196o + 569381)g_9g_{10} + (88408o + 186217)g_{15} + (335264o + 959530)g_{11} + (1010969o + 63665)g_9) = 0$$
$$g_{10}\, g_{12} - ((771753o + 64319)g_9g_{13} + (164575o + 966646)g_9^2 + (965062o + 655630)g_{16} + (750323o + 230129)g_{14} + (303453o + 767920)g_{12} + (325132o + 587653)g_{10}) = 0$$
$$g_{10}\, g_{13} - ((441581o + 410724)g_9g_{14} + (1042732o + 876444)g_9g_{12} + (583095o + 185233)g_9g_{10} + (88408o + 186217)g_{17} + (696698o + 161783)g_{15} + (335264o + 959530)g_{13} + (653418o + 472013)g_{11} +$$

$(771237o + 439004)g_9) = 0$

$g_{10}\ g_{14} - ((796561o + 60058)g_9g_{15} + (46926o + 779564)g_9g_{11} + (110462o + 539063)g_9^2 +$
$(37279o + 902307)g_{10}) = 0$

$g_{10}\ g_{15} - ((771753o + 64319)g_9g_{16} + (561423o + 486068)g_9g_{12} + (1042233o + 344521)g_9g_{10} +$
$(350671o + 483189)g_{17} + (1004866o + 658831)g_{15} + (250565o + 799642)g_{13} +$
$(196123o + 176883)g_{11} + (266961o + 244390)g_9) = 0$

$g_{10}\ g_{16} - ((303495o + 843209)g_9g_{17} + (345631o + 584296)g_9g_{15} + (494538o + 544840)g_9g_{11} +$
$(66715o + 766721)g_9^2 + (797211o + 820301)g_{16} + (166165o + 103141)g_{14} + (430077o + 127050)g_{12} +$
$(427377o + 133754)g_{10}) = 0$

$g_{10}\ g_{17} - ((689327o + 587917)g_9^3 + (923118o + 200870)g_9g_{16} + (694643o + 245137)g_9g_{14} +$
$(59046o + 798937)g_9g_{12} + (747385o + 885060)g_9g_{10} + (624993o + 372655)g_{17} +$
$(590272o + 404433)g_{15} + (17221o + 176159)g_{13} + (664234o + 927473)g_{11} + (956788o + 227196)g_9) = 0$

$g_{11}\ g_{17} - ((864944o + 634201)g_9^2g_{10} + (134726o + 861529)g_9g_{17} + (989839o + 717491)g_9g_{15} +$
$(494538o + 544840)g_9g_{13} + (30212o + 375190)g_9g_{11} + (779234o + 12084)g_9^2 + (750938o + 34430)g_{16} +$
$(357117o + 235196)g_{14} + (204646o + 748532)g_{12} + (924714o + 1010813)g_{10}) = 0$

An element

$$\begin{aligned} ih = \{&y_1 + (965929r^3 + 1006006r^2 + 519774r + 29405)x + \\ &324543r^3 + 764628r^2 + 150227r + 965852, \\ x^2 + &(999114r^3 + 901550r^2 + 623461r + 322760)x + \\ &951621r^3 + 460095r^2 + 433083r + 192480\} \end{aligned}$$

of Jacobian group of the hyperelliptic curve H has an order n equal to the group order.

We verified that the image $ic = \Psi_1 \cdot \Psi_2(ih)$ has the same order n in Jacobian of $C_{9,10,\ldots,17}$ curve C over k.

Thus (even if the order of Jacobian group of H was the almost prime), DLP on the hyperelliptic curve H over K is reduced to DLP on $C_{9,10,\ldots,17}$ curve C over k, and is solved by Gaudry attack in the amount of computations $O((\#k)^{\frac{2g}{g+1}}) = O(2^{71.1\ldots})$. This means eight bits of loss of security, ignoring O-constants.

7 Conclusion

The paper shows that DLP on genus two hyperelliptic curve over even degree finite fields of order q^2 can be solved by Weil descent attack in the amount of computations $O(q^{\frac{16}{9}})$, which is less than $O(q^2)$ for Pollard's ρ-method.

We assume that the characteristic of the definition field is different from two and hold the Assumption 1 for hyperelliptic curves. However, these assumptions seem to be only for simplicity. We believe in that our method of Weil descent

attack can be applied for all of the genus two hyperelliptic curve cryptosystems over even degree finite fields with a slight modification.

In estimating the amount of computations, we ignore O-constants. We need more detailed experiments to see to what extent our method of Weil descent attack is more effective than Pollard's ρ-method in the real world.

References

1. L. M. Adleman, J. DeMarrais, and M. D. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobian of large genus hyperelliptic curves over finite fields, ANTS-I, Springer-Verlag LNCS 877, 1994, 28–40.
2. S.Arita, An Addition Algorithm in Jacobian of C_{ab} Curves, Discrete Applied Mathematics, to appear.
3. S. Arita, Gaudry's variant against C_{ab} curves, IEICE TRANS. FOUND., E83-A (2000), 1809-1814.
4. S. Arita, Weil descent of elliptic curves over finite fields of characteristic three, ASIACRYPT 2000, LNCS 1976, pp.248–258, Kyoto, 2000.
5. C. Diem, The GHS-attack in odd characteristic, preprint, 2001. Available from http://www.exp-math.uni-essen.de/ diem/english.html.
6. G.Frey, How to disguise an elliptic curve, Talk at Waterloo workshop on the ECDLP, http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/ slides.html, 1998.
7. S.D.Galbraith, Weil Descent of Jacobians, preprint at the University of Bristol, 2000.
8. P.Gaudry, An algorithm for solving the discrete logarithm problem on hyperelliptic curves, EUROCRYPT 2000, Springer-Verlag LNCS 1807, 2000, 19-34.
9. P.Gaudry, F.Hess, and N.P.Smart, Constructive and destructive facets of Weil descent on elliptic curves, to appear in J. Cryptology.
10. N. Kanayama, K. Nagao, and S. Uchiyama, Generating hyperelliptic curves of genus 2 suitable for cryptography, Proc. of SCI 2002, 2002.
11. K. Matsuo, J. Chao, and S. Tsujii, An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields, ANTS-V, Springer-Verlag LNCS 2369, 2002, 461–474.
12. S. Miura, Linear Codes on Affine Algebraic Curves, Trans. of IEICE, vol. J81-A, No. 10, 1398-1421, Oct. 1998.