Efficient Algorithms for the Construction of Hyperelliptic Cryptosystems

Tatsuaki Okamoto† Kouichi Sakurai‡

†NTT Laboratories
Nippon Telegraph and Telephone Corporation
1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan
‡Information Systems and Electronics Development Laboratory
Mitsubishi Electric Corporation
5-1-1, Ofuna, Kamakura, 247 Japan

Abstract

The jacobian of hyperelliptic curves, including elliptic curves as a special case, offers a good primitive for cryptosystems, since cryptosystems (discrete logarithms) based on the jacobians seem to be more intractable than those based on conventional multiplicative groups. In this paper, we show that the problem to determine the group structure of the jacobian can be characterized to be in NP ∩ co-NP, when the jacobian is a non-degenerate type ("non-half-degenerate"). We also show that the hyperelliptic discrete logarithm can be characterized to be in NP ∩ co-NP, when the group structure is non-half-degenerate. Moreover, we imply the reducibility of the hyperelliptic discrete logarithm to a multiplicative discrete logarithm. The extended Weil pairing over the jacobian is the key tool for these algorithms.

1 Introduction

The finite abelian groups play an important role in constructing many public-key cryptosystems and error correcting codes. The most typical member of the finite abelian groups is the multiplicative group of a finite field, and the first public-key cryptosystem (key-distribution system) was constructed on a multiplicative group [DH]. However, since the structure of multiplicative groups is very simple, certain special techniques [Odl, Cop1, Cop2] were developed that could attack some cryptosystems (or their discrete logarithms) based on multiplicative groups. On the contrary, the jacobians of hyperelliptic curves, including elliptic curves as a special case, offer a rich source of "naturally occuring" (more complex) finite abelian groups, and cryptosystems based on the jacobians seem to be more intractable than those based on multiplicative groups [Mil1, Kob1, MOV].

In order to use the jacobians for cryptosystems, we should determine their group structures and the intractability of their related cryptosystems (discrete logarithms). As for the group structure, Miller has shown an efficient algorithm of determining the structure of an *elliptic curve group*, using an oracle of factoring. As for the intractability of the discrete logarithm of the *elliptic curve*, it has been known that some specific elliptic discrete

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 267-278, 1992.

logarithms are as tractable as multiplicative discrete logarithms [MOV]. Thus it remained open whether these results about *elliptic curves* could be extended to *hyperelliptic curves*.

The hyperelliptic discrete logarithm has been characterized from the viewpoint of structural computational complexity [SIS]. According to their result, the hyperelliptic discrete logarithm was characterized as more intractable than the multiplicative discrete logarithm. More precisely, they have shown that a problem corresponding the hyperelliptic discrete logarithm is in NP $\cap$ co-AM, while a problem corresponding the multiplicative discrete logarithm is in NP $\cap$ co-NP. However, it remained open whether the problem corresponding to the hyperelliptic discrete logarithm is in NP $\cap$ co-NP.

In this paper, we extend the above results of elliptic curves to derive similar results for the *hyperelliptic curves*; we show that the problem to determine the group structure of the jacobian can be characterized to be in NP $\cap$ co-NP, when the jacobian is a non-degenerate type ("non-half-degenerate"), and show that some specific *hyperelliptic* discrete logarithms are as tractable as multiplicative discrete logarithms. Moreover, we partially solve the above-mentioned open problem regarding the characterization of the hyperelliptic discrete logarithms; we show that the problem corresponding the hyperelliptic discrete logarithm is in NP $\cap$ co-NP, when the group structure is non-half-degenerate. Note that this result does not state that the hyperelliptic discrete logarithm is as tractable as the multiplicative discrete logarithm. (The above result is only a characterization from the viewpoint of structural computational complexity.)

The extended Weil pairing defined over hyperelliptic curves plays an essential role throughout this paper. So, first, in section 3, we define the extended Weil pairing and introduce an efficient algorithm to compute the extended Weil pairing. Then, in section 4, we show that the problem corresponding to the group structure of the non-half-degenerate jacobian is in NP $\cap$ co-NP. Section 5 shows that the problem corresponding to the non-half-degenerate hyperelliptic discrete logarithm is in NP $\cap$ co-NP, and that some specific *hyperelliptic* discrete logarithms are as tractable as multiplicative discrete logarithms.

2 Hyperelliptic Curves and the Jacobian

This section briefly introduces the notions regarding the jacobians of hyperelliptic curves. For more detail, refer to [Kob2, Lan, Sil]

Let K be an arbitrary field, and let $\overline{K}$ denote its algebraic closure. Let C be a hyperelliptic curve of genus g over K, whose equation is of the form $v^2 + h(u)v = f(u)$, where $h(u)$ is a polynomial of degree at most g and $f(u)$ is a monic polynomial of degree $2g+1$. Here f and h have coefficients in K, and we assume that the curve has no singular point.

Let L be a field containing K. An L-point P denotes an infinite point O or $P_{x,y}$ where $(x \in L, y \in L)$ is a solution of the hyperelliptic curve equation. If σ is an automorphism of L over K, we let P^σ denote $P_{\sigma(x),\sigma(y)}$ and O^σ=O.

A divisor is a finite formal sum of $\overline{K}$-points $D = \sum m_i P_i$. We define the degree of D to be the integer $\sum m_i$. The divisors form an additive group $\boldsymbol{D}$, in which the divisors of degree 0 form a subgroup $\boldsymbol{D}^0$. Given $D = \sum m_i P_i \in \boldsymbol{D}$, we define $D^+ = \sum_{m_i>0} m_i P_i$. We say that $D \geq 0$ if $D = D^+$. Given two divisors $D_1 = \sum m_i P_i$ and $D_2 = \sum n_i P_i$ in $\boldsymbol{D}^0$, we define $\gcd(D_1, D_2) \in \boldsymbol{D}^0$ to be $(\sum \min(m_i, n_i) P_i)$.

We define the order of a polynomial function $p(u, v)$ with coefficients in $\overline{K}$ at a point $P \in C$, denoted $\mathrm{ord}_P p$, as follows:

(1) Assume $P = P_{x,y}$ is a finite point. $p(u,v)$ can be reduced to the form $\overline{p}(u,v) = (u-x)^{r_0}(a_0(u) - b_0(u)v)$, where $(u-x)$ does not divide both a_0 and b_0. Let $r = r_0$ if $P \neq \bar{P}$ and $r = 2r_0$ if $P = \bar{P}$. Then, $\mathrm{ord}_{P_{x,y}} p = r$ if $a_0(x) - b_0(x)y \neq 0$, else, it equals to r plus the exponent of the highest power of $(u-x)$ which divides $a_0(u)^2 + h(u)a_0(u)b_0(u) - f(u)b_0(u)^2$.

(2) If $P = O$, then $\mathrm{ord}_O P = -\max(2\deg a,\ 2g+1+2\deg b)$.

To any $p(u,v)$ such that $\overline{p} \neq 0$, we associate the divisor $\mathrm{div}(p) = \sum (\mathrm{ord}_P p)P \in \boldsymbol{D}^0$. By rational function on C we mean a ratio of the form $p(u,v)/q(u,v)$ with $\overline{q} \neq 0$. $K(C)$ denotes the rational function field of curve C over field K. A divisor of the form $\mathrm{div}(p/q) = \mathrm{div}(p) - \mathrm{div}(q) \in \boldsymbol{D}^0$ is called principal. The quotient group $\boldsymbol{D}^0/\boldsymbol{P}$ is called the jacobian $\boldsymbol{J}$ of the curve C, where $\boldsymbol{P}$ is the subgroup of principal divisors. $\boldsymbol{O}$ denotes the identity element of $\boldsymbol{J}$, which is the element corresponding to $\boldsymbol{P}$. When two divisors D_1 and D_2 are in the same element of $\boldsymbol{J}$, D_1 is said to be *linearly equivalent* to D_2 and we denote $D_1 \sim D_2$. Then, there exists a rational function f such that $D_1 = D_2 + \mathrm{div}(f)$.

The support of a divisor $D = \sum m_i P_i$ is the set of points $P \in C$ for which $m_i \neq 0$. Now let $f \in \overline{K}(C)$ be a function such that $\mathrm{div}(f)$ and D have disjoint supports. Then, we define $f(D) = \prod f(P_i)^{m_i}$.

We associate to D the set of functions $L(D) = \{f \in \overline{K}(C) \mid \mathrm{div}(f) \geq -D\} \cup \{0\}$. $L(D)$ is a finite dimensional $\overline{K}$-vector space, and we denote its dimension $l(D)$.

Every $D \in \boldsymbol{D}^0$ can be uniquely represented as an element of $\boldsymbol{J}$ by a reduced divisor $D_1 = \sum m_i P_i - (\sum m_i)O$ with $\sum m_i \leq g$. This result follows from the Rieman-Roch theorem. We denote $(P), (Q)$ as the reduced divisors of $P, Q \in \boldsymbol{J}[m]$, and we also denote (D) as the reduced divisor such that $(D) \sim D$, where D is a divisor.

A semireduced divisor $D = \sum m_i P_i - (\sum m_i)O$ can be uniquely represented as the gcd of two divisors of functions of the form $a(u)$ and $b(u) - v$, where $a(u) = \prod (u - x_i)^{m_i}$ and $b(u)$ is the unique polynomial of degree $<$ deg $a(u)$ such that $b(x_i) = y_i$ for each i and $b(u)^2 + h(u)b(u) - f(u)$ is divisible by $a(u)$. A divisor D represented in the form $\gcd(a(u), (b(u) - v))$ is abbreviated $D = \mathrm{div}(a, b)$. D is reduced if and only if deg $a \leq g$.

3 Extension of the Weil Pairing

The Weil pairing was originally defined over elliptic curves by A. Weil [Sil]. Lang generalized the Weil pairing over the abelian varieties [Lan]. In this section, we define the extended Weil pairing on the jacobian of the hyperelliptic curves, which is a specific class of Lang's generalization, and show an expected polynomial time algorithm of computing the extended Weil pairing. We have two different ways to define the extended Weil pairing. One is suitable for the efficient computation of the pairing, and the other is suitable for proving some properties, although these definitions are equivalent. Here, we only show the definition that is suitable for the efficient computation of the pairing.

3.1 Definition of the extended Weil pairing

Definition 3.1 *Let C be a hyperelliptic curve defined over $\overline{K}$, and $\boldsymbol{J}$ be the Jacobian on C ($\boldsymbol{J} = \boldsymbol{D}^0/\boldsymbol{P}$). Let $\boldsymbol{J}[m]$ be $\boldsymbol{D}^0[m]/\boldsymbol{P}$ and μ_m be the set of m-th roots of the unity, where $\boldsymbol{D}^0[m]=\{D \mid D \in \boldsymbol{D}^0$ and $mD \in \boldsymbol{P}\}$ and the characteristic of K is prime to m.*

First, we define a function w_m

$$w_m : \boldsymbol{D}^0[m] \times \boldsymbol{D}^0[m] \to \mu_m$$

as follows; Let $X, Y \in \boldsymbol{D}^0[m]$, *and we assume* X, Y *are disjoint supports. Since* X *and* Y *have order* m, *there are functions* $f_X, f_Y \in \overline{K}$ *such that* $div(f_X) = mX$ *and* $div(f_Y) = mY$. *Then we define*

$$w_m(X, Y) := f_X(Y)/f_Y(X).$$

Then, we define a pairing (the extended Weil pairing)

$$e_m : \boldsymbol{J}[m] \times \boldsymbol{J}[m] \to \mu_m$$

as follows: Let $P, Q \in \boldsymbol{J}[m]$, *and* A *and* B *be divisors over* C *such that* $A \in P$ *and* $B \in Q$ *and they have disjoint supports. Since* $A, B \in \boldsymbol{D}^0[m]$, *we can define* $w_m(A, B)$. *Then we define*

$$e_m(P, Q) = w_m(A, B).$$

We will show an efficient algorithm based on the above definition.

3.2 Miller's algorithm

This subsection introduces Miller's algorithm (algorithm 1 in [Mil2]), which is used in the extended Weil pairing algorithm.

Algorithm 1 (Miller's Algorithm) :

Input A hyperelliptic curve C with genus g, and a divisor $A \in \boldsymbol{D}^0$

Output A function f, and a reduced divisor B such that $A = B + \mathrm{div}(f)$

Step 1 Rewrite the divisor $A = a_1P_1 + a_2P_2 + \ldots + a_kP_k$ as a sum of reduced divisors $a_1(P_1 - O) + a_2(P_2 - O) + \ldots + a_k(P_k - O)$.

Step 2 Calculate a basis for the space $L(3gO)$ in the form $f_1, \ldots, f_d$ where $\mathrm{ord}_O f_1 > \mathrm{ord}_O f_2 > \mathrm{ord}_O > \ldots > \mathrm{ord}_O f_d$. (There is a one-to-one correspondence between reduced divisors and integral ideals of the ring of functions whose only poles are at O. Each ideal can be represented by means of the Grobner basis.)

Step 3 For each reduced divisor $(P_i - O)$, use doubling and addition repeatedly to compute a reduced divisor B and a function f such that $a_1(P_1 - O) + \ldots + a_k(P_k - O) = B + \mathrm{div}(f)$. This computation can be done by repeatedly using the following primitive computation: given two reduced divisors P and Q, compute a reduced divisor R and a function h such that $P + Q = R + \mathrm{div}(h)$. The following substeps show this computation.

- **Step 3-1** Find a function $s \in L(3gO - P^+ - Q^+)$, where $P = P^+ - gO, Q = Q^+ - gO$.
- **Step 3-2** Set $S = \mathrm{div}(s) + 3gO - P^+ - Q^+$.
- **Step 3-3** Find a function $t \in L(2gO - S)$, and set $T = \mathrm{div}(t) + 2gO - S$. Here $R = T - gO$, and $h = s/t$.

Step 4 Output B and f.

3.3 Extended Weil pairing algorithm

Here, we show an expected polynomial time algorithm for computing the extended Weil pairing. The Weil pairing is defined over two elements P, Q in $\boldsymbol{J}[m]$. However, in order to calculate the value of $e_m(P, Q)$ in an algorithm, P, Q must be given explicitly (or in a polynomial-size expression). Any element in $\boldsymbol{J}[m]$ can be uniquely represented by a *reduced divisor* from the Riemann-Roch theorem. Therefore, the reduced divisor is the best explicit representation of an element of $\boldsymbol{J}[m]$.

Algorithm 2 (Extended Weil pairing) :

Input (P), (Q) such that $P, Q \in \boldsymbol{J}[m]$

Output $e_m(P, Q)$

Step 1 Select two reduced divisors T and U over C randomly.

Step 2 Compute $((P) + T)$ and $((Q) + U)$. For this computation, we use Cantor's (Koblitz's) algorithm [Can, Kob2].

Step 3 Set $A = ((P) + T) - T$, and $B = ((Q) + U) - U$. (Note that $A - (P)$ is in $\boldsymbol{P}$, and that gO of $((P) + T)$ and gO of T are cancelled in A.)

Step 4 Compute functions f_A and f_B. For this computation, we use Algorithm 1 (Miller's algorithm).

Step 5 Compute $f_A(B)$ and $f_B(A)$. If either $f_A(B)$ or $f_B(A)$ is zero or undefined, then return to 1. Otherwise, compute $f_A(B)/f_B(A)$ as $e_m(P, Q)$.

Lemma 3.2 *Algorithm 2 is performed in expected polynomial time in* $\log q$.

Proof:

Let $1 = a_1, \ldots, a_t = m$ be an addition chain, which is used to compute functions f_A and f_B. T and U both have M^g candidates, where M is the number of K-points of curve C (note that M is not the number of $\boldsymbol{J}$). We define a bad pair (T, U) such that A (consists of at most $2g$ support points) is disjoint from $(a_i(Q + U))^+$ (consists of at most g support points) and $(a_iU)^+$ (consists of at most g support points), and B (consists of at most $2g$ support points) is disjoint from $(a_i(P+T))^+$ (consists of at most g support points) and $(a_iT)^+$ (consists of at most g support points). Therefore, the failure probability at step 5 of the above algorithm is at most $8tgM^{g-1}/M^{2g} = 8tg/M^{g+1}$. Hence, this failure probability is $O(g(\log q)/2^{(g+1)(\log q)})$ (or negligible). Thus, this algorithm is expected polynomial time in $\log q$. (The expected number of rounds from step 1 to 5 is almost 1.) ¶

Similarly, the extended Weil pairing can be computed in non-deterministic polynomial time.

3.4 Correctness of the definition

In this subsection, we show that the extended Weil pairing satisfies some properties that are needed for the intended applications.

Lemma 3.3 w_m *is well-defined.*

Lemma 3.4 *Let* $P, P', Q, Q' \in \boldsymbol{D}^0[m]$ *such that* $P - P'$ *(resp.* $Q - Q'$*)* $\in \boldsymbol{P}$. *Then*

$$w_m(P', Q) = w_m(P, Q), \qquad w_m(P, Q') = w_m(P, Q).$$

Lemma 3.4 implies that w_m induces a natural pairing e_m over $\boldsymbol{J}[m] \times \boldsymbol{J}[m]$. Therefore the definition that $e_m(P, Q) = w_m(A, B)$ makes sense.

Next we investigate some properties of e_m.

Theorem 3.5

(1) For any elements $P, Q \in \boldsymbol{J}[m]$,

$$e_m(P, Q) \in \mu_m.$$

(2) Alternating: For any elements $P, Q \in \boldsymbol{J}[m]$,

$$e_m(P, Q) = e_m(P, Q)^{-1}.$$

(3) Bilinear: For any elements $P_1, P_2, Q \in \boldsymbol{J}[m]$,

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q),$$

$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2).$$

(4) Identity: For any element $P \in \boldsymbol{J}[m]$, $e_m(P, P)$ *is 1.*

(5) Non-degeneracy: If $e_m(P, Q) = 1$ *for all* $P \in \boldsymbol{J}[m]$, *then* $Q = \boldsymbol{O}$.

4 Complexity of Determining Hyperelliptic Group Structure

This section shows that the problem to determine the group structure of a jacobian $\boldsymbol{J}$ over $\boldsymbol{F}_q$ can be characterized to be in NP $\cap$ co-NP, when $\boldsymbol{J}$ is "non-half-degenerate".

Let $\boldsymbol{J}$ be a jacobian over a field $\boldsymbol{F}_q$ with group structure $Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_{2g}}$ (simply we write $(n_1, n_2, \ldots, n_{2g})$), where $n_i \geq 1$ $(1 \leq i \leq 2g)$, and n_j divides n_i when $n_j < n_i$. (This comes from the property of finite abelian groups.) The maximal order of an element in $\boldsymbol{J}$ is n_1.

$(G_1, G_2, \ldots, G_{2g})$ be a *canonical generating tuple* for the abelian group of $\boldsymbol{J}$, if every element $X \in \boldsymbol{J}$ can be written uniquely as

$$X = a_1 G_1 + \ldots + a_g G_{2g},$$

where $0 \leq a_i < n_i$ and $n_i = \mathrm{Ord}(G_i)$. ($\mathrm{Ord}(G_i)$ denotes the order of G_i.)

$< G_1, \ldots, G_r >$ denotes the subgroup generated from $G_1, \ldots, G_r$. Note that $\langle G_1, G_2 \rangle$ and $\langle n_1, n_2 \rangle$ are used for denoting a paired property of the group structure (see Lemma 4.1 for the definition of "paired canonical generating tuple").

Lemma 4.1 *Let* $\boldsymbol{J}$ *be a jacobian over a field* $\boldsymbol{F}_q$ *and* $(G_1, G_2, \ldots, G_{2g})$ *(* $\mathrm{Ord}(G_i) = n_i$ *) be a canonical generating tuple of* $\boldsymbol{J}$, *where* $n_{2i} \leq n_{2i-1}$ *(but the other greater or smaller relations are not fixed). Let* h_i $(i = 1, \ldots, g)$ *be the homomorphism*

$$h_i : X \in \boldsymbol{J}_q[n_{2i-1}] \mapsto e_{n_{2i-1}}(G_{2i-1}, X),$$

and f_i $(i = 1, \ldots, g)$ *be the homomorphism*

$$f_i : \boldsymbol{J}_q[n_{2i-1}] \rightarrow \boldsymbol{J}_q[n_{2i-1}]/ < G(\boldsymbol{J}_q[n_{2i-1}]) - G_{2i} >,$$

where $\boldsymbol{J}_q[n]$ *denotes* $\{P \mid P \in \boldsymbol{J} \wedge nP = O\}$, *and* $G(\boldsymbol{J}_q[n_{2i-1}])$ *denotes* $\{G_j \mid n_j$ *devides* $n_{2i-1}\}$.

Then there exists a canonical generating tuple $(G_1, G_2, \ldots, G_{2g})$ *such that for all elements* $P, Q \in \boldsymbol{J}_q[n_{2i-1}]$,

$$h_i(P) = h_i(Q) \quad \textit{if and only if} \quad f_i(P) = f_i(Q).$$

The canonical generating tuple satisfying the above property is written as $(\langle G_1, G_2\rangle, \langle G_3, G_4\rangle, \ldots, \langle G_{2g-1}, G_{2g}\rangle)$ *and is called a paired canonical generating tuple. Here,* $(\langle n_1, n_2\rangle, \langle n_3, n_4\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$ *denotes its group structure. Without loss of generality, we assume that* $n_{2(i+j)-1} \leq n_{2i-1}$ $(i = 1, \ldots, g-1; j = 1, \ldots, g-i)$.

Proof:

We will show that we can construct a paired canonical generating tuple $(\langle G_1, G_2\rangle, \langle G_3, G_4\rangle, \ldots, \langle G_{2g-1}, G_{2g}\rangle)$ such that $f_i(P) = f_i(Q)$ (or $P - Q \in < G(\boldsymbol{J}_q[n_{2i-1}]) - G_{2i} >$) if and only if $e_{n_{2i-1}}(G_{2i-1}, P) = e_{n_{2i-1}}(G_{2i-1}, Q)$.

Let $\boldsymbol{J}[n_1]$ be defined over the algebraic closure field $\overline{\boldsymbol{F}}_q$ (see subsection 3.1), of which $\boldsymbol{J}$ is a subgroup. Since the group structure of $\boldsymbol{J}[n_1]$ is $(n_1)^{2g}$, there exist elements $\gamma_2, \ldots, \gamma_{2g}$ such that $(G_1, \gamma_2, \ldots, \gamma_{2g})$ is a canonical generating tuple for $\boldsymbol{J}[n_1]$, and $G_i = (n_1/n_i)\gamma_i$ $(i = 2, \ldots, 2g)$.

First, we will prove it when $i = 1$. An element $P \in \boldsymbol{J}$ whose order is the maximaum order, n_1, is selected, and set $G_1 = P$. Next, since h_1 is a linear map with the kernel, $\mathrm{Ker}(h_1)$, of co-dimension 1, there exists an element $\gamma_2 \in \boldsymbol{J}[n_1]$ such that $\mathrm{Ord}(\gamma_2) = n_1$ and $\gamma_2 \notin \mathrm{Ker}(h_1)$ (or $e_{n_1}(G_1, \gamma_2) \neq 1$). Therefore, when $(G_1, \gamma_2, \ldots, \gamma_{2g})$ is a canonical generating tuple for $\boldsymbol{J}[n_1]$, $< G_1, \gamma_3, \ldots, \gamma_{2g} > \in \mathrm{Ker}(h_1)$. Then, a canonical generating tuple for $\boldsymbol{J}$, $(G_1, G_2, \ldots, G_{2g})$ is determined by $G_i = (n_1/n_i)\gamma_i$ $(i = 2, \ldots, 2g)$.

Next, we will show that for all elements $P, Q \in \boldsymbol{J}_q[n_1]$,

$$h_1(P) = h_1(Q) \quad \text{if and only if} \quad f_1(P) = f_1(Q).$$

(If) Suppose that $f_1(P) = f_1(Q)$. Then by the definiton, there exists an integer c such that $P - Q = c_1G_1 + c_3G_3 + \cdots c_{2g}G_{2g}$. Using bilinearity and the identity of the extended Weil pairing, and the above mentioned property of the map h_1,

$$\begin{aligned} e_{n_1}(G_1, P) &= e_{n_1}(G_1, Q + c_1G_1 + c_3G_3 + \cdots c_{2g}G_{2g}) \\ &= e_{n_1}(G_1, Q)e_{n_1}(G_1, G_1)^{c_1}e_{n_1}(G_1, G_3)^{c_3} \cdots e_{n_1}(G_1, G_{2g})^{c_{2g}} \\ &= e_{n_1}(G_1, Q). \end{aligned}$$

(Only if) Suppose $f_1(P) \neq f_1(Q)$. Then there exists integers $c_1, c_2, \ldots c_{2g}$ such that $P - Q = c_1G_1 + c_2G_2 + c_3G_3 + \cdots c_{2g}G_{2g}$, where $c_2G_2 \neq \boldsymbol{O}$.

$$\begin{aligned} e_{n_1}(G_1, P) &= e_{n_1}(G_1, Q + c_1G_1 + c_2G_2 + \cdots c_{2g}G_{2g}) \\ &= e_{n_1}(G_1, Q)e_{n_1}(G_1, G_1)^{c_1}e_{n_1}(G_1, c_2G_2) \cdots e_{n_1}(G_1, c_{2g}G_{2g}) \\ &= e_{n_1}(G_1, Q)e_{n_1}(G_1, c_2G_2). \end{aligned}$$

Therefore, if $e_{n_1}(G_1, c_2G_2) \neq 1$, then the proof of this (Only if) part is completed.

Next, we will prove that $e_{n_1}(G_1, c_2G_2) \neq 1$. From the nongeneracy of the Weil pairing, c_2G_2 is O if and only if, for all elements $X = a_1G_1 + a_2\gamma_2 + \cdots a_{2g}\gamma_{2g}$ in $J[n_1]$ $(0 \leq a_i < n_1)$,

$$e_{n_1}(c_2G_2, X) = 1.$$

Then,

$$\begin{aligned} e_{n_1}(c_2G_2, X) &= e_{n_1}(c_2G_2, a_1G_1 + a_2\gamma_2 + \cdots a_{2g}\gamma_{2g}) \\ &= e_{n_1}(c_2G_2, G_1)^{a_1}. \end{aligned}$$

Hence, for all elements $X \in J[n_1]$, $e_{n_1}(c_2G_2, X) = 1$ if and only if $e_{n_1}(c_2G_2, G_1) = 1$. Therefore, c_2G_2 is O if and only if $e_{n_1}(c_2G_2, G_1) = 1$. By the condition, c_2G_2 is not O, so $e_{n_1}(c_2G_2, G_1) \neq 1$.

Hence the proof has been completed when $i = 1$. We can easily prove it sequentially when $i = 2, 3, \ldots, g$ in the same manner as $i = 1$, by considering the subgroup $< G_{2i-1}, G_{2i}, \ldots, G_{2g} >$ in place of J. ¶

From the above lemma, when $(\langle G_1, G_2\rangle, \langle G_3, G_4\rangle, \ldots, \langle G_{2g-1}, G_{2g}\rangle)$ is a *paired* canonical generating tuple, $\mathrm{Ord}(e_{n_{2i-1}}(G_{2i-1}, G_{2i})) = n_{2i}$, and $e_{n_{2i-1}}(G_{2i-1}, G_j) = 1$ $(j \neq 2i)$. Then, we can say that the g subgroups $< G_1, G_2 >, < G_3, G_4 >, \ldots, < G_{2g-1}, G_{2g} >$ are independent, in the sense that the extended Weil pairing of elements from two different subgroups is always 1.

Definition 4.2 *Let J be a jacobian over F_q with a paired canonical generating tuple, $(\langle G_1, G_2\rangle, \ldots, \langle G_{2g-1}, G_{2g}\rangle)$. J is half-degenerate if there exist at least two cyclic subgroups, $< G_{2i-1} \neq O, G_{2i} = O >$, (or there exits at least two i's $\in \{1, 2, \ldots, g\}$ such that $G_{2i-1} \neq O$ and $G_{2i} = O$). J is non-half-degenerate if it is not half-degenerate, (or there exits at most one $i \in \{1, 2, \ldots, g\}$ such that $G_{2i-1} \neq O$ and $G_{2i} = O$).*

Lemma 4.3 *Let J be a jacobian over a field F_q with group structure $(\langle n_1, n_2\rangle, \langle n_3, n_4\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$. Then, $q - 1$ divisible by n_{2i} $(i = 1, \ldots, g)$.*

Proof:

Let $(\langle G_1, G_2\rangle, \langle G_3, G_4\rangle, \ldots, \langle G_{2g-1}, G_{2g}\rangle)$ be a *paired* canonical generating tuple of the abelian group of J. Consider the multiplicative group M_i $(i = 1, \ldots, g)$ consisting of values $e_{n_{2i-1}}(G_{2i-1}, X)$ where X ranges over the elements of $J_q[n_{2i-1}]$. This forms a multiplicative group from the bilinearity and identity of the extended Weil pairing, and the size of M_i is n_{2i} from Lemma 4.1. Since the values $e_{n_{2i-1}}(G_{2i-1}, X)$ are in the finite field F_q, group M_i is a subgroup of the multiplicative group F_q^*. Consequently, the size of group F_q^* is divisible by the size M_i, so $q - 1$ is divisible by n_{2i}. ¶

Lemma 4.4 *Let J be a jacobian over a field F_q. Assume that J is non-half-degenerate. Then the group structure of J is $(\langle n_1, n_2\rangle, \langle n_3, n_4\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$, if and only if there exists $2g$-tuple $(\langle P_1, P_2\rangle, \langle P_3, P_4\rangle, \ldots, \langle P_{2g-1}, P_{2g}\rangle)$ such that, for all $i = 1, \ldots, g$,*

$$\begin{gathered} \mathrm{Ord}(P_j) = n_j \quad (j = 1, \ldots, 2g), \\ \mathrm{Ord}(e_{n_{2i-1}}(P_{2i-1}, P_{2i})) = n_{2i}, \\ e_{n_{2i-1}}(P_{2i-1}, P_j) = 1 \quad (j \neq 2i;\ j \in \{1, \ldots, 2g\}), \\ e_{n_{2i}}(P_{2i}, P_j) = 1 \quad (j \neq 2i - 1;\ j \in \{1, \ldots, 2g\}), \\ N = n_1 \cdot \ldots \cdot n_{2g}, \end{gathered}$$

where $P_1, \ldots, P_{2g}$ be elements of J, and N be the number of elements of J.

Proof:

(Only if) Suppose that the group structure of $\boldsymbol{J}$ is $(\langle n_1, n_2\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$. Then, clearly there exists a generating tuple $(P_1, \ldots, P_{2g})$ which satisfies the above conditions.

(If) Suppose that there exists $2g$-tuple $(P_1, \ldots, P_{2g})$ which satisfies the above conditions. From Lemma 4.1, $e_{n_{2i-1}}(P_{2i-1}, P_j) = 1$ $(j \neq 2i)$ and $e_{n_{2i}}(P_{2i}, P_j) = 1$ $(j \neq 2i-1)$ implies that P_j $(j \neq 2i-1, 2i)$ is not included in subgroup $< P_{2i-1}, P_{2i} >$, if $P_{2i-1} \neq \boldsymbol{O}$, $P_{2i} \neq \boldsymbol{O}$ and $P_j \neq \boldsymbol{O}$. From the assumption that $\boldsymbol{J}$ is non-half-degenerate, there exists at most one $i \in \{1, \ldots, g\}$ such that $P_{2i-1} \neq \boldsymbol{O}$ and $P_{2i} = \boldsymbol{O}$. Therefore, the condition implies that each non-identity subgroup $< P_{2i-1}, P_{2i} >$ is independent from the other non-identity subgroups, and each subgroup has the structure (n_{2i-1}, n_{2i}), where non-identity subgroup $< P_{2i-1}, P_{2i} >$ denotes the subgroup such that $< P_{2i-1}, P_{2i} > \neq \boldsymbol{O}$ (or $P_{2i-1} \neq \boldsymbol{O}$). Therefore, $N = n_1 \cdot \ldots \cdot n_{2g}$ results in $(\langle P_1, P_2\rangle, \ldots, \langle P_{2g-1}, P_{2g}\rangle)$ being a paired canonical generating tuple. This concludes that the group structure is $(\langle n_1, n_2\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$. ¶

Then we show the main result of this section. The following theorem shows that a membership problem regarding the problem to determine the group structure of a jacobian is in NP ∩ co-NP, when the jacobian is non-half-degenerate.

Definition 4.5 *HESTR is a language, or membership problem such that*

$HESTR = \{\langle C, g, q, (m_1, \ldots, m_{2g})\rangle \mid$ *the group structure of the jacobian* $\boldsymbol{J}$ *of curve* C, $(\langle n_1, n_2\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$, *satisfies* $n_i \geq m_i$, $(1, \ldots, 2g)$. $\}$,

where C *is a hyperelliptic curve with genus* g *defined over* $\boldsymbol{F}_q$ *(*q *is a prime power),* m_i *is a positive integer.*

Theorem 4.6 *HESTR is in NP ∩ co-NP, when* $\boldsymbol{J}$ *is non-half-degenerate.*

Proof:

If a nondeterministic machine shows a witness that $(\langle n_1, n_2\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$ is the group structure of $\boldsymbol{J}$, the witness is used for both HESTR and the complement of HESTR. When $\boldsymbol{J}$ is non-half-degenerate, the witness is $(P_1, P_2, ..., P_{2g})$ which satisfies the conditions of Lemma 4.4, factors of the number of the elements of $\boldsymbol{J}$, N, and appropriate reduced divisors T and U for computing the extended Weil pairing value (see Algorithm 2). Then, from Lemma 4.4, a poly-time machine can check the group structure using the extended Weil paring and factoring (for checking orders). Here, the poly-time machine can compute N by Pila's algorithm [Pil]. (Note that $(P_1, P_2, ..., P_{2g})$ is a generating tuple of this group.) Since the extended Weil pairing can be computed in polynomial-time by using appropriate T and U, HESTR is in NP ∩ co-NP. ¶

Theorem 4.6 can be written as follows, using the notion of the promise problem [ESY]: Let (Q_1, R_1) be a promise problem such that Q_1 is the promise that $\boldsymbol{J}$ is non-half-degenerate, and R_1 is the property that HESTR is true. Then (Q_1, R_1) is in NPP ∩ co-NPP, and (Q_1, R_1) has a solution in NP ∩ co-NP.

Note that generally the fact that (Q, R) is in NPP ∩ co-NPP does not imply that (Q, R) has a solution in NP ∩ co-NP (see [ESY]). However, (Q_1, R_1) above has a solution in NP ∩ co-NP, since the witness of R_1 can also be the witness of Q_1 (or Q_1 is in NP), while generally promise Q is not in NP.

5 Complexity of Hyperelliptic Discrete Logarithm

This section introduces two results about the difficulty of the hyperelliptic discrete logarithm; one is the characterization of the problem from the viewpoint of the structural complexity theory. This improves on the result of [SIS]. The other is the reduction of the hyperelliptic curve discrete logarithms to the conventional multiplicative discrete logarithms, which is an extension of the result by [MOV].

5.1 Discrete logarithms over the Jacobians

Definition 5.1 *Let $P \in \boldsymbol{J}$ over $\boldsymbol{F}_q$ be an element of maximum order n_1, and let $R \in \boldsymbol{J}$. The* hyperelliptic curve logarithm problem *is the following: Given P and R, determine the unique integer l, $0 \leq l \leq n_1 - 1$, such that $R = lP$, provided that such an integer exists.*

Definition 5.2 *HEDL is a language, or membership problem such that*

$$HEDL = \{\langle C, g, q, P, R, l_0\rangle \mid \text{there exists } l \text{ such that } l \leq l_0 \text{ and } R = lP.\ \},$$

where C is a hyperelliptic curve with genus g over $\boldsymbol{F}_q$ and $P \in \boldsymbol{J}$ over $\boldsymbol{F}_q$ be an element of maximum order n_1, and let $R \in \boldsymbol{J}$.

5.2 HEDL is NP ∩ co-NP when non-half-degenerate

Theorem 5.3 *HEDL is NP ∩ co-NP, when $\boldsymbol{J}$ is non-half-degenerate.*

Proof:

When $< C, g, q, P, R, l_0 >$ is in HEDL, then integer l that satisfies $R = lP$ and $l \leq l_0$ is the witness for the input in HEDL. Clearly the computation of $R = lP$ and $l \leq l_0$ is deterministic polynomial time. Therefore, HEDL is in NP.

There are two cases in which $< C, g, q, P, R, l_0 >$ is not in HEDL. One is the case where there exists l' such that $R = l'P$ and $l' \not\leq l_0$. The other case is where l does not exist such that $R = lP$. In the former case, l' is the witness for the input not in HEDL. In the latter case, when $\boldsymbol{J}$ is non-half-degenerate, the group structure, its witness, $(P_1, \ldots, P_{2g})$ etc., (Theorem 4.6), and a vector $(a_1, \ldots, a_{2g})$ such that $P = P_1$ and $R = a_1P_1 + \cdots + a_{2g}P_{2g}$ are the witness for the input not in HEDL. This is because l does not exist such that $R = lP$ if and only if there exists i such that $a_i \neq 0$ and $i \neq 1$. Here, Theorem 4.6 guarantees the existence of the witness for the group structure for HEDL, when $\boldsymbol{J}$ is non-half-degenerate. Therefore, HEDL is in co-NP. ¶

Similarly to Theorem 4.6, Theorem 5.3 can be written as follows, using the notion of the promise problem [ESY]: Let (Q_1, R_2) be a promise problem such that Q_1 is the promise that $\boldsymbol{J}$ is non-half-degenerate, and $R_2$is the property that HEDL is true. Then (Q_1, R_2) is in NPP ∩ co-NPP, and (Q_1, R_2) has a solution in NP ∩ co-NP.

5.3 Reducing hyperelliptic logarithms to multiplicative logarithms

Definition 5.4 *Let $\boldsymbol{J}$ be a jacobian over $\boldsymbol{F}_q$ with a paired canonical generating tuple, $(\langle G_1, G_2\rangle, \ldots, \langle G_{2g-1}, G_{2g}\rangle)$, and its group structure be $(\langle n_1, n_2\rangle, \ldots, \langle n_{2g-1}, n_{2g}\rangle)$. Let*

$(\langle G_1, \gamma_2\rangle, \ldots, \langle \gamma_{2g-1}, \gamma_{2g}\rangle)$ *be the paired canonical generating tuple of* $\boldsymbol{J}[n_1]$, *where* $G_i = (n_1/n_i)\gamma_i$ $(i = 2, \ldots, 2g)$. *Then,* $\boldsymbol{J}^{(1)}[n_1]$ *denotes* $< \gamma_{2i-1}, \gamma_{2i} >$.

Algorithm 3 (Reduction of HEDL) :

Input An element $P \in \boldsymbol{J}$ over $\boldsymbol{F}_q$ of maximum order n_1, and $R \in \boldsymbol{J}$.

Output An integer l such that $R = lP$.

Step 1 Determine the smallest integer k such that $\boldsymbol{J}(F_{q^k})$ includes $\boldsymbol{J}^{(1)}[n_1]$, where P is the first element, G_1, of the paired canonical generating tuple of $\boldsymbol{J}[n_1]$.

Step 2 Find $Q \in \boldsymbol{J}(F_{q^k})$ such that $\alpha = e_{n_1}(P, Q)$ has order n_1.

Step 3 Compute $\beta = e_{n_1}(R, Q)$

Step 4 Compute l, the discrete logarithm of β to the base α in F_{q^k}.

Note that the output of the above algorithm is correct since

$$\beta = e_{n_1}(R, Q) = e_{n_1}(lP, Q) = e_{n_1}(P, Q)^l = \alpha^l.$$

Remark: Similar to algorithm 2 of [MOV], the above algorithm is incomplete as we do not provide methods for determining k, or for finding the point Q. In the final version of this paper, we will show algorithms to find k and Q for some specific hyperelliptic curves.

6 Conclusion

In this paper, we have shown that the problem to determine the group structure of the jacobian can be characterized to be in NP $\cap$ co-NP, when the jacobian is non-half-degenerate. Moreover, we have shown that the hyperelliptic discrete logarithm can be characterized to be as tractable as the multiplicative discrete logarithm from the viewpoint of structural computational complexity, when the jacobian is non-half-degenerate. It is an open problem to eliminate the condition of non-half-degeneracy for the jacobian in our results.

Acknowledgments

Authors would like to sincerely thank Neal Koblitz for pointing out serious mistakes in the abstract version of this paper and for invaluable suggestions. We also would like to thank Joan Feigenbaum for introducing us to Neal Koblitz, and her kind support. We wish to thank Hiroki Shizuya for his useful suggestions and discussions. We also thank Toshiya Itoh for his sending us several useful documents. The first author would like to thank Kenji Koyama, Alfred Menezes and Scott Vanstone for their useful discussions.

References

[Can] D. Cantor, "Computing in the Jacobian of a Hyperelliptic Curve", *Math. Comp.*, 48, pp.95–101 (1987).

[Cop1] D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two", *IEEE Transactions on Information Theory*, **IT-30**, 587–594 (1984).

[Cop2] D. Coppersmith, A. Odlyzko and R. Schroeppel, "Discrete logarithms in $GF(p)$", *Algorithmica*, 1 (1986), 1-15.

[DH] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol.IT-22, No.6, pp.644–654 (1976).

[ElG] T. ElGamal, "A subexponential-time algorithm for computing discrete logarithms over $GF(p^2)$", *IEEE Transactions on Information Theory*, **IT-31**, pp.473–481 (1985).

[ESY] S. Even, A.L. Selman and Y. Yacobi, "The Complexity of Promise Problems with Applications to Public-Key Cryptography", *Information and Control*, **61**, pp.159-173 (1984).

[Ful] W. Fulton, "Algebraic Curves," Benjamin, New York, 1969.

[Kal] B. Kaliski, "A pseudorandom bit generator based on elliptic logarithms", *Advances in Cryptology: Proceedings of Crypto '86*, Lecture Notes in Computer Science, **293**, Springer-Verlag, pp.84–103 (1987).

[Kob1] N. Koblitz, "Elliptic Curve Cryptosystems", *Math. Comp.*, 48, pp.203–209 (1987).

[Kob2] N. Koblitz, "Hyperelliptic Cryptosystems", *Journal of Cryptology*, Vol.1, pp.139–150 (1989).

[Knu] D. Knuth, The Art of Computer Programming, Vol. 2. Reading, MA: Addison-Wesley, 1981.

[Lan] S. Lang, Abelian Varieties, Interscience, New York, 1959.

[MOV] A.J. Menezes, T. Okamoto, S.A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", *Proc. of STOC'91*, pp.80–89 (1991).

[Mil1] V. Miller, "Uses of elliptic curves in cryptography", *Proc. of Crypto '85*, pp.417–426 (1986).

[Mil2] V. Miller, "Short programs for functions on curves", unpublished manuscript, 1986.

[Odl] A. Odlyzko, "Discrete logarithms and their cryptographic significance", *Proc. of Eurocrypt '84*, pp.224–314, (1985).

[Pil] J. Pila, "Frobenius Maps of Abelian Varieties and Finding Roots of Unity in Finite Fields", *PhD Thesis of Stanford Univ.*, (1988)

[Sch1] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p", *Mathematics of Computation*, **44**, pp.483–494 (1985).

[Sch2] R. Schoof, "Nonsingular plane cubic curves over finite fields", *Journal of Combinatorial Theory*, **A 46**, pp.183–211 (1987).

[Sil] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[SIS] H. Shizuya, T. Itoh, K.Sakurai, "On the Complexity of Hyperelliptic Discrete Logarithm Problem", to appear in *Proc. of Eurocrypt '91*.