On the Decomposition of an Element of Jacobian of a Hyperelliptic Curve

Koh-ichi Nagao, nagao@kanto-gakuin.ac.jp,

Dept. of Engineering, Kanto-Gakuin Univ.

Abstract. In this manuscript, if a reduced divisor D_0 of hyperelliptic curve of genus g over extension field $\mathbb{F}_{q^n}$ is written by a linear sum of ng elements of $\mathbb{F}_{q^n}$-rational points of the hyperelliptic curve whose x-coordinates are in the base field $\mathbb{F}_q$, D_0 is noted by decomposed divisor and the set of such $\mathbb{F}_{q^n}$-rational points is noted by decomposed factor of D_0. We propose an algorithm which checks whether a reduced divisor is decomposed or not, and computes the decomposed factor, if it is decomposed. This algorithm needs the process for solving equations system of degree 2, $(n^2-n)g$ variables, and $(n^2-n)g$ equations over $\mathbb{F}_q$. Further, for the cases $(g,n)=(1,3),(2,2)$, and $(3,2)$, the concrete computations of decomposed factors is done by computer experiments.
Keywords Index calculus attack, Jacobian, Hyperelliptic curve, DLP, Weil descent attack

1 Introduction

In [6], Gaudry presents a frame work of the following attack for the DLP of the Jacobian of a curve C over extension field $\mathbb{F}_{q^n}$. A point of the Jacobian over extension field $\mathbb{F}_{q^n}$ has some representation of the form $(x_1, x_2, ...)$ with $x_i \in \mathbb{F}_{q^n}$. In this attack, the set of the potentially smooth elements of index calculus is taken as $B_0 = \{(x_1, x_2, ...)|x_1, x_2, .., x_{ng} \in \mathbb{F}_q\}$ where g is the genus of the curve. When the curve E is an elliptic curve, B_0 is taken as $B_0 = \{(x, y) \in E(\mathbb{F}_{q^n})|x \in \mathbb{F}_q\}$ and by the use of Semaev's formula [10], the decomposition of a $\mathbb{F}_{q^n}$ rational point of E into n elements of B_0 is checked by solving equations system of degree $n-1$, n variables and n equations over $\mathbb{F}_q$. However, in the other cases including hyperelliptic curve cases, there is no alternative formula working in the role of Semaev's formula, the decomposition may be complicated.
In this manuscript, we present an alternative attack. In this attack, the set of the potentially smooth elements is taken as

$$B_0 := \{P - \infty | P = (x, y) \in C(\mathbb{F}_{q^n}),\ x \in \mathbb{F}_q\}$$

where ∞ is some fixed point on $C(\mathbb{F}_{q^n})$. Note that when the curve is an elliptic curve, B_0 is the same as Gaudry's one. In the case that the curve being a hyperelliptic curve, ∞ is taken as the unique point at infinity. In this manuscript, we will show that the decomposition of a reduced divisor into ng elements of B_0 is checked by solving equation systems of degree 2, $(n^2-n)g$ variables, and $(n^2-n)g$ equations over $\mathbb{F}_q$ by the use of Riemann-Roch theorem (not using Semaev's formula). The complexity of the decomposition in the elliptic curve case may be the same as that of Gaudry's method using Semaev's formula.
Further let C be a hyperelliptic curve (including elliptic curve) of genus g of the form

$$C : y^2 = f(x), \text{ where } f(x) = x^{2g+1} + a_{2g}x^{2g} + ... + a_0$$

over $\mathbb{F}_{q^n}$ where characteristic of $\mathbb{F}_q$ is not 2 and $n \geq 2$. Let D_0 be a $\mathbb{F}_{q^n}$ rational point of Jacobian of C. Since D_0 has Mumford representation i.e. it is written as follows;

$$D_0 = (\phi_1(x), \phi_2(x)),$$

where $\phi_1(x) \in \mathbb{F}_{q^n}[x]$ is a monic polynomial with $\deg(\phi_1(x)) \leq g$ and $\phi_2(x) \in \mathbb{F}_{q^n}[x]$ satisfies $\deg(\phi_2(x)) < \deg(\phi_1(x))$ and $f(x) - \phi_2(x)^2 \equiv 0 \bmod \phi_1(x)$. Further, we will assume $\deg(\phi_1(x)) = g$. So, put $\phi_{i,j} \in \mathbb{F}_{q^n}$ by

$$\phi_1(x) = x^g + \phi_{1,g-1}x^{g-1} + ... + \phi_{1,1}x + \phi_{1,0},\ \phi_2(x) = \phi_{2,g-1}x^{g-1} + ... + \phi_{2,0}.$$

Note that there are $Q_1, .., Q_g \in C(\overline{\mathbb{F}}_{q^n})$ such that $D_0 \sim Q_1 + .. + Q_g - (g)\infty$.
Put

$$B_0 := \{P - \infty | P = (x, y) \in C(\mathbb{F}_{q^n}),\ x \in \mathbb{F}_q\}.$$

We see easily that $|Jac(C/\mathbb{F}_{q^n})| \approx q^{gn}$ and $|B_0| \approx q$, the probability that there are some $P_1, P_2, .., P_{ng} \in B_0$ (exactly ng elements) such that

$$D_0 + P_1 + P_2 + ... + P_{ng} - (ng)\infty \sim 0 \tag{1}$$

is $1/(gn)!$.

Definition 1 *If a reduced divisor D_0 (also assuming $\deg(\phi_1(x)) = g$) is written by the form (1), D_0 is called potentially B_0-smooth reduced divisor and $\{P_i\}_{i=1}^{ng}$ is called decomposed factors.*

In this manuscript, we will show the following theorem.

Theorem 1. *Let $V_1, V_2, ..., V_{(n^2-n)g}$ be variables and let D_0 be a reduced divisor of $C/\mathbb{F}_{q^n}$. Then there are some degree 2 polynomials*

$$C_{i,j} \in \mathbb{F}_q[V_1, V_2, ..., V_{(n^2-n)g}] \quad (0 \leq i \leq ng-1,\ 0 \leq j \leq n-1)$$

satisfying the following.
The condition that D_0 is potentially B_0-smooth is equivalent to the following 1) and 2).
1) The equations system $S = \{C_{i,j} = 0 \,|\, 0 \leq i \leq ng-1,\ 1 \leq j \leq n-1\}$ has some solution $\boldsymbol{v} = (v_0, .., v_{(n^2-n)g}) \in \mathbb{A}^{(n^2-n)g}(\mathbb{F}_q)$.
2) Let $c_j = C_{0,j}(v_0, .., v_{(n^2-n)g})$ for $0 \leq j \leq ng-1$. $G(x) = x^{ng} + c_{ng-1}x^{ng-1} + ... + c_0 \in \mathbb{F}_q[x]$ factors completely.
Moreover, if D_0 is potentially B_0-smooth, the x-coordinates of the decomposed factor are the solutions of $G(x) = 0$.

In the next section, we will construct such multivariable polynomials $\{C_{i,j}\}$.

2 Proof of the theorem

In this section, we prove the Theorem 1. Let $D = \sum_{P \in C(\overline{\mathbb{F}}_{q^n})} n_p P$, $n_p \in \mathbb{Z}$ be a divisor of $C/\mathbb{F}_{q^n}$. Put $\deg(D) := \sum_{P \in C(\overline{\mathbb{F}}_{q^n})} n_p$, and $L(D) := \{f \in \overline{\mathbb{F}}_{q^n}(C) \,|\, (f) + D \geq 0\}$. From Riemann-Roch Theorem (cf [7] Corollary A.4.2.3), we have the following lemma.

Lemma 1. (**Riemann-Roch**) *1) $L(D)$ is a $\mathbb{F}_{q^n}$ vector space.*
2) If $\deg(D) \geq 2g-1$, $dim\, L(D) = \deg(D) - g + 1$.

From the equation of C, we see $\mathrm{ord}_\infty x = 2$, and $\mathrm{ord}_\infty y = 2g+1$. Put $N_1 := \lfloor \frac{(n+1)g}{2} \rfloor$ and $N_2 := \lfloor \frac{ng-g-1}{2} \rfloor$.

Lemma 2. *1) $N_1 + N_2 = ng - 1$.*
2) $N_2 + g - 1 < N_1$.

Proof. trivial.

Lemma 3. *$\{1, x, x^2, .., x^{N_1}, y, xy, ...x^{N_2}y\}$ is a base of $L((ng+g)\infty)$.*

Proof. From $\mathrm{ord}_\infty x = 2$, $\mathrm{ord}_\infty y = 2g+1$, each element in the above list is in $L(\,(ng+g)\infty)$. The independence is from the definition of hyperelliptic curve. Thus, since the number of the elements of the list $N_1 + N_2 + 2 = ng + 2$ is the same as the dim $L((ng+g)\infty)$ (from lemma 1), we have this lemma.

Lemma 4. *$\{\phi_1(x), \phi_1(x)x, ..., \phi_1(x)x^{N_1-g}, (y-\phi_2(x)), (y-\phi_2(x))x, ..., (y-\phi_2(x))x^{N_2}\}$ is a base of $L((ng)\infty - D_0) = L((ng+g)\infty - \sum_{i=1}^{g} Q_i)$.*

Proof. From the definition of $\phi_1(x)$ and $\phi_2(x)$, each elements in the list have zero at each Q_i. Since $\deg(\phi_1(x)) = g$, $\deg(\phi_2(x)) \leq g-1$, and $N_2 + g - 1 < N_1$(from lemma 2), each elements in the list has atmost $(ng+g)$ pole at ∞. Then they are in $L((ng)\infty - D_0)$. Now, we show the independence. Assume they are not independent, there are some non zero $f_1(x), f_2(x) \in \overline{\mathbb{F}}_{q^n}[x]$ such that $\phi_1(x)f_1(x) + (y - \phi_2(x))f_2(x) = 0$. However, the relation $\phi_1(x)f_1(x) + (y-\phi_2(x))f_2(x) = 0$ induces $yf_2(x) \in \overline{\mathbb{F}}_{q^n}[x]$ and $f_1(x) = f_2(x) = 0$. It is a contradiction and so, they are independent. On the other hands, the number of the elements of the list is $N_1 + N_2 + 2 - g = ng - g + 2$ from Lemma 2, which is the same as the dim $L((ng)\infty - D_0)$. So we have this lemma.

Form this lemma, an element $h \in L((ng)\infty - D_0)$ is written by

$$h(x,y) = \phi_1(x)(A_0 + A_1x + ... + A_{N_1-g}x^{N_1-g}) + (y - \phi_2(x))(B_0 + B_1x + ..., B_{N_2}x^{N_2}) \tag{2}$$

where A_i,B_i are parameters moving in $\overline{\mathbb{F}}_{q^n}$.
When $ng+g$ is even, assume $A_{N_1-g} = 0$ and we have the order of the zero of $h(x,y)$ is truly less than $ng+g$ and $\mathrm{div}(h(x,y))$ is not written by the form of (1). Similarly, when $ng+g$ is odd, assume $B_{N_2} = 0$ and we have the order of the zero of $h(x,y)$ is truly less than $ng+g$ and $\mathrm{div}(h(x,y))$ is not written by the form of (1). So, we can assume that $A_{N_1-g} \neq 0$ if $ng+g$ is even and that $B_{N_2} \neq 0$ if $ng+g$ is odd.
Further, we compute the cross points of $h(x,y) = 0$ on C. For this purpose, y must be eliminated. From $h(x,y) = 0$, y is written by

$$y = \frac{(A_0 + A_1x + ... + A_{N_1-g}x^{N_1-g}) - \phi_2(x)(B_0 + B_1x + ..., B_{N_2}x^{N_2})}{B_0 + B_1x + ..., B_{N_2}x^{N_2}} \tag{3}$$

By this y's representation, the number of the parameters must be decrement. So, put $A_{N_1-g} = 1$ when $ng+g$ is even and put $B_{N_2} = -1$ when $ng+g$ is odd. Also put $M_1 = \begin{cases} N_1 - g & \text{when } ng+g \text{ is even} \\ N_1 - g - 1 & \text{when } ng+g \text{ is odd} \end{cases}$,

$M_2 = \begin{cases} N_2 - 1 & \text{when } ng+g \text{ is even} \\ N_2 & \text{when } ng+g \text{ is odd} \end{cases}$. Note that $M_1 + M_2 = ng - g - 1$ form lemma 2. Put

$$S(x) := -(\text{denominator of (3)})^2 f(x) + (\text{numerator of (3)})^2.$$

(Remember that $y^2 = f(x)$ is the equation of C) From the construction, $S(x)$ is monic polynomial of degree $ng+g$, whose coefficients are degree 2 polynomials in $\mathbb{F}_{q^n}[A_0, .., A_{M_1}, B_0, .., B_{M_2}]$. and $\phi_1(x)|S(x)$. Put $g(x) := S(x)/\phi_1(x)$. Since $\phi_1(x)$ is monic polynomial in $\mathbb{F}_{q^n}[x]$, $g(x)$ is also monic polynomial of degree ng, whose coefficients are degree 2 polynomials in $\mathbb{F}_{q^n}[A_0, .., A_{M_1}, B_0, .., B_{M_2}]$. Put $C_i \in \mathbb{F}_{q^n}[A_0, .., A_{M_1}, B_0, .., B_{M_2}]$ by i-th coefficient of $g(x)$, i.e.,

$$g(x) = x^{ng} + C_{ng-1}x^{ng-1} + ... + C_0.$$

The zeros of $g(x) = 0$ are the x-coordinate of the cross points of $h(x, y) = 0$ on C except $Q_1, ..., Q_g$. Thus, we have the following lemma.

Lemma 5. *The condition that D_0 is potentially B_0-smooth reduced divisor is equivalent to the following;*
There are some $A_0, .., A_{M_1}, B_0, ...B_{M_2} \in \mathbb{F}_{q^n}$ such that $g(x) \in \mathbb{F}_q[x]$ and $g(x) \in \mathbb{F}_q[x]$ factors completely in $\mathbb{F}_q[x]$.

Further, we find the $\{A_i\}_{i=0}^{M_1}, \{B_i\}_{i=0}^{M_2}$ such that $g(x) \in \mathbb{F}_q[x]$. Let $[\alpha_0(= 1), \alpha_1, .., \alpha_{n-1}]$ be a base of $\mathbb{F}_{q^n}/\mathbb{F}_q$. We will fix this base. Let $A_{i,j}$ $(0 \leq i \leq M_1, 0 \leq j \leq n-1)$, $B_{i,j}$ $(0 \leq i \leq M_2, 0 \leq j \leq n-1)$, be new parameters such that

$$A_i = \sum_{j=0}^{n-1} A_{i,j}\alpha_j \; (0 \leq i \leq M_1), \quad B_i = \sum_{j=0}^{n-1} B_{i,j}\alpha_j \; (0 \leq i \leq M_2).$$

Note that the number of the parameters $\{A_{i,j}\}, \{B_{i,j}\}$ is

$$(M_1 + M_2 + 2)n = (N_1 + N_2 - g + 1)n = (n^2 - n)g.$$

For the simplicity, put $\{V_1, V_2, ..., V_{(n^2-n)g}\}$ by $\cup_{j=0}^{n-1}((\cup_{i=0}^{M_1}\{A_{i,j}\}) \cup (\cup_{i=0}^{M_2}\{B_{i,j}\}))$. Then C_i is written by

$$C_i = \sum_{j=0}^{n-1} C_{i,j}\alpha_j, \quad C_{i,j} \in \mathbb{F}_q[V_1, V_2, ..., V_{(n^2-n)g}].$$

The condition $g(x) \in \mathbb{F}_q[x]$ is equivalent to the condition that there are some $v_1, v_2, ..., v_{(n^2-n)g} \in \mathbb{F}_q$

$$C_{i,j}(v_1, v_2, ..., v_{(n^2-n)g}) = 0 \text{ for } 0 \leq i \leq ng-1, \; 1 \leq j \leq n-1.$$

Moreover, when $g(x) \in \mathbb{F}_q[x]$, $g(x) = x^{ng} + C_{0,ng-1}x^{ng-1} + ... + C_{0,0}$. The condition that $g(x)$ factors completely in $\mathbb{F}_q[x]$ is equivalent to the above condition and $G(x) := x^{ng} + c_{ng-1}x^{ng-1} + ... + c_0$ factors completely in $\mathbb{F}_q[x]$ where $c_j = C_{0,j}(v_1, v_2, ..., v_{(n^2-n)g})$. In this case, the solutions of $G(x) = 0$ are the x-coordinates of the decomposed factor. Then, we finish the proof of Theorem 1.

3 Example

In this section, we state the three computational experiments of the decomposition of elements of Jacobian. The computations are done by using Windows XP preinstalled HP Notebook (CPU:Pentium M 2GHz, RAM:1GB). We compute three cases 1) $(g, n) = (1, 3)$, 2) $(g, n) = (2, 2)$, 3) $(g, n) = (3, 2)$, where g and n are the genus and the extension degree of definition field of the chosen hyperelliptic/elliptic curve respectively. In all cases, one trial, which means the judge whether a given element of Jacobian is decomposed or not and the computation of decomposed factor, if it is decomposed, is done by within 1 second. Since the probability that an element of Jacobian is decomposed is $1/(gn)!$, the times for obtaining one potentially B_0-smooth reduced divisor are within 6 sec, 24 sec, and 720 sec respectively. Further, we will give the three examples.
Case 1. Let $q = 1073741789$(prime number), $\mathbb{F}_{q^3} := \mathbb{F}_q[t]/(t^3+456725524* t^2 + 251245663 * t + 746495860)$, and let $E/\mathbb{F}_{q^3}$ be an elliptic curve defined by $y^2 = x^3 + (1073741788 * t^2 + t) * x + (126 * t + 3969)$ and $P_0 := (t, t + 63) \in E$. We investigate whether $nP_0 : n = 1, 2, ..30$ are decomposed and find the following 7 decompositions. ($24P_0$ is written by 2 forms.)

$$2P_0 = (1050861583, 6509843 * t^2 + 387051565 * t + 920296030)$$
$$+(742900894, 362262801 * t^2 + 6480079 * t + 886701711)$$
$$+(571975376, 938916909 * t^2 + 910769097 * t + 139897863)$$
$$5P_0 = ((806296922, 113931706 * t^2 + 863383473 * t + 133427995)$$
$$+(797256157, 360646567 * t^2 + 663390692 * t + 1012046566)$$
$$+(389333914, 986077188 * t^2 + 829314065 * t + 687783827)$$
$$8P_0 = (1063441336, 113661172 * t^2 + 942865616 * t + 744283566)$$
$$+(894045278, 863335768 * t^2 + 637284565 * t + 937810737)$$
$$+(694935460, 740353309 * t^2 + 505910431 * t + 597402219)$$
$$20P_0 = (996570058, 341336613 * t^2 + 450680674 * t + 72874200)$$
$$+(141768271, 589122734 * t^2 + 930205049 * t + 713557032)$$
$$+(73505168, 432994198 * t^2 + 405986289 * t + 233154172)$$
$$24P_0 = (529735815, 20343700 * t^2 + 780030904 * t + 490121669)$$
$$+(515960254, 269821984 * t^2 + 561547517 * t + 348990487)$$
$$+(207183771, 712543643 * t^2 + 356522343 * t + 895634732)$$
$$= (818683055, 1034251164 * t^2 + 705927333 * t + 1062879754),$$
$$(754504105, 23461217 * t^2 + 961620879 * t + 1015889110)$$
$$+(489159707, 271295793 * t^2 + 600348670 * t + 1022482426)$$
$$26P_0 = (628174301, 138296704 * t^2 + 104824480 * t + 858118320)$$
$$+(371888603, 417445284 * t^2 + 850151153 * t + 126970733)$$
$$(55411433, 560274594 * t^2 + 609956706 * t + 821692494)$$

Case 2. Let $q = 1073741789$(prime number), $\mathbb{F}_{q^2} := \mathbb{F}_q[t]/(t^2+746495860* t + 206240189)$, and let $C/\mathbb{F}_{q^2}$ be a hyperelliptic curve defined by

$$y^2 = x^5 + (673573223 * t + 771820244) * x + 6 * t + 9$$

and

$$D_0 := (x^2 + 1073741787 * t * x + 327245929 * t + 867501600,$$

$(1023168391 * t + 350252228) * x + 658555356 * t + 446913597) \in Jac(C)$ (Mumford representation). We investigate whether $nD_0 : n = 1, 2, ..100$ are decomposed and find the following 9 decompositions. ($71D_0$ is written by 2 forms.)

$6D_0 \sim (1025731975, 776505688{*}t{+}911495013){+}(728060789, 648475468{*}t{+}1067025179)$

${+}(341799975, 145077925{*}t{+}187604034){+}(61964999, 227570631{*}t{+}639782700){-}4\infty$

$19D_0 \sim (1039361498, 15180988{*}t{+}396695374){+}(828360115, 179412594{*}t{+}719919461){-}4\infty$

${+}(483171045, 677645208{*}t{+}604714840){+}(34566209, 753841024{*}t{+}14375633){-}4\infty$

$33D_0 \sim (970690833, 608141084{*}t{+}889165804){+}(260086243, 894605411{*}t{+}261264640)$

${+}(208957980, 43330622{*}t{+}581461318){+}(190782894, 124873649{*}t{+}510328990){-}4\infty$

$35D_0 \sim (699447787, 267523741{*}t{+}562899544){+}(559470007, 197827114{*}t{+}99971197)$

${+}(472594781, 579187919{*}t{+}266558458){+}(453661772, 449424806{*}t{+}977318920){-}4\infty$

$48D_0 \sim (1009979214, 959734525{*}t{+}990871450){+}(995813251, 44186049{*}t{+}288496638)$

${+}(521299995, 556594200{*}t{+}468424666){+}(17946008, 977064852{*}t{+}1071618742){-}4\infty$

$71D_0 \sim (1019155056, 573896856{*}t{+}103042116){+}(944470217, 829781939{*}t{+}184620624)$

${+}(727156004, 462612591{*}t{+}582877732){+}(281900623, 553507533{*}t{+}42660552){-}4\infty$

$\sim (502979299, 412632304{*}t{+}1036827718){+}(74527656, 927651409{*}t{+}452588110)$

${+}(50078888, 801072540{*}t{+}888737005){+}(2986754, 556402789{*}t{+}236723678){-}4\infty$

$73D_0 \sim (843747137, 682161676{*}t{+}600252618){+}(829302257, 145878028{*}t{+}853397395)$

${+}(290487906, 645896278{*}t{+}279001181){+}(184873704, 567002729{*}t{+}620354511){-}4\infty$

$80D_0 \sim (907811987, 216534804{*}t{+}936839244){+}(808513243, 873487475{*}t{+}273845273)$

${+}(520893378, 757248670{*}t{+}381150138){+}(486203744, 494475019{*}t{+}791571132){-}4\infty$

Case 3. Let $q = 1073741789$(prime number), $\mathbb{F}_{q^2} := \mathbb{F}_q[t]/(t^2+746495860* t + 206240189)$, and let $C/\mathbb{F}_{q^2}$ be a hyperelliptic curve defined by

$$y^2 = x^7 + (111912375 * t + 1046743132) * x + 6 * t + 9$$

and

$$D_0 := (x^2 + 1073741787 * t * x + 327245929 * t + 867501600,$$

$(473621736 * t + 256126568) * x + 145989647 * t + 687383736) \in Jac(C)$ (Mumford representation). We investigate whether $nD_0 : n = 1, 2, ..3000$ are decomposed and find the following 6 decompositions.

$414D_0 \sim (1001437837, 752632260{*}t{+}700158497){+}(747112084, 656073918{*}t{+}400137619)$

${+}(620249588, 127943213{*}t{+}635474623){+}(614180498, 206297635{*}t{+}445250468)$

${+}(515769009, 607297126{*}t{+}554290493){+}(488549466, 627952783{*}t{+}854182612){-}6\infty$

$657D_0 \sim (939617127, 695261735{*}t{+}239531611){+}(933351280, 935312661{*}t{+}961494096)$
${+}(799612924, 341923983{*}t{+}677495100){+}(294787599, 279723229{*}t{+}760003067)$
${+}(273118782053704103{*}t{+}577497766){+}(153381525, 983211238{*}t{+}517037777){-}6\infty$
$921D_0 \sim (1034634787, 400751409{*}t{+}829801342){+}(763888873, 757155774{*}t{+}829936954)$
${+}(619620874, 800641683{*}t{+}200272230){+}(603032615, 115219564{*}t{+}655011145)$
${+}(436423191, 285214454{*}t{+}450812747){+}(125198811, 884750621{*}t{+}123305741){-}6\infty$
$1026D_0 \sim (1024020017, 267457905{*}t{+}41452942){+}(794174628, 615676821{*}t{+}723336407)$
${+}(738567269, 433647609{*}t{+}128304659){+}(629287731, 465842490{*}t{+}789390318)$
${+}(435082408, 878213106{*}t{+}603353206){+}(79621979, 479459622{*}t{+}672937516){-}6\infty$
$1121D_0 \sim (764081031, 812350603{*}t{+}347878564){+}(673426715, 687737442{*}t{+}381588704)$
${+}(6102522082007139{*}t{+}99219637){+}(467560104, 619342780{*}t{+}228756808)$
${+}(179787786, 333322906{*}t{+}75482151){+}(59221667, 860686653{*}t{+}625301206){-}6\infty$
$2289D_0 \sim (729358563, 482925408{*}t{+}170057124){+}(529840657, 42328987{*}t{+}857983002)$
${+}(514618236, 436901100{*}t{+}416530686){+}(350106356, 183495333{*}t{+}950710579)$
${+}(175898979, 411808870{*}t{+}427518366){+}(96240558, 703780413{*}t{+}461022225){-}6\infty$

4 Estimation of the complexity of solving DLP

In this section, we estimate the complexity of the index calculus using this decomposition for fixed g, n and q going to infinity. Moreover, the estimation is done by without concerning the term of poly(q). The complexity is essentially the same as that of Gaudry [6]. However, after [6] appears, the new variant of the index calculus by the use of two large primes [9], [5] appears, and a little improvement is done. So we summarize the results.

For a while, we review the index calculus of the Jacobian of a curve $C/\mathbb{F}_q$. First, Gaudry pointed out that taking $B_0 = \{P | P \in C(\mathbb{F}_q\}$ as a set of smooth elements and the index calculus works well. The complexity of the part of collecting smooth divisors is $O(q)$ and that of solving linear algebra is $O(q^2)$ (poly(q) terms is omitted). Gaudry and Harley (cf.[3]) proposed the improvement that taking B, a subset of B_0 as as a set of smooth elements and doing the rebalance between the collecting part and the linear algebra part. The complexity is $O(q^{2g/(g+1)})$. Further, $B_0 \backslash B$ is called a set of large prime. Thérialut [11] proposed the improvement using of the almost smooth divisor, which is written by one large prime and other smooth elements. The complexity is $O(q^{(4g-2)/(2g+1)})$. Finally, the author [9] and Gaudry et al. [5] proposed the improvement using of the 2-almost smooth divisor, which is written by 2 large primes and other smooth elements. The complexity is $O(q^{(2g-2)/g)})$.

Now, we give the estimation of the complexity as follows. Let G be a group and let $B_0 \subset G$ be a subset. Also let N be a positive integer. Assume the following i),ii),iii),iv):

i) The probability that $g \in G$ is written by $g = g_1 + .. + g_N$ for some $g_i \in B_0$ is $O(1)$.

ii) For a $g \in G$ written by $g = g_1 + .. + g_N$ with $g_i \in B_0$, the cost of computing $g_1, .., g_n$ from g is $O(1)$.

iii) For the $g's \in G$ written by $g = g_1 + .. + g_N$ with $g_i \in B_0$, the distribution of $\{\cup_{\text{Such } g\text{'s}} \{g_i\}\}$ is uniform.

iv) $|B_0|^2 \ll |G|$.

Let $B \subset B_0$ be a subset.

Definition 2 *1) A element of $g \in G$ written by $g = g_1 + .. + g_N$ for $g_1, ...g_n \in B$ is called smooth group element.*
2) A element of $g \in G$ written by $g = g_1 + .. + g_N$ for one $g_i \in B_0 \backslash B$ and other $\{g_j\} \in B$ is called almost smooth group element.
3) A element of $g \in G$ written by $g = g_1 + .. + g_N$ for two $g_{i1}, g_{i2} \in B_0 \backslash B$ and other $\{g_j\} \in B$ is called 2-almost smooth group element.

Lemma 6. *Then we have the following 1),2),3).*
1) The complexity of the index calculus taking B as a set of smooth elements by the rebalanced method is minimized at $|B| = O(|B_0|^{N/(N-1)})$ and it is $O(|B_0|^{(2N)/(N+1)})$.
2) The complexity of the index calculus taking B as a set of smooth elements and $B_0 \backslash B$ taking as large prime by the one lage prime method is minimized at $|B| = O(|B_0|^{(2N-1)/(2N+1)})$ and it is $O(|B_0|^{(4N-2)/(2N+1)})$.
3) The complexity of the index calculus taking B as a set of smooth elements and $B_0 \backslash B$ taking as large prime by the two lage prime method is minimized at $|B| = O(|B_0|^{(N-1)/N})$ and it is $O(|B_0|^{(2N-2)/(2N)})$.

Proof. In every cases, the cost of the part of linear algebra is $O(|B|^2)$ and by the rebalance, which is needed for minimizing the complexity, it is the same as the cost of the collecting divisors. So, we only estimate the optimized size $|B|$.
1)**The case of rebalanced method.** The probability that $g \in G$ is smooth group element is $O(|B/B_0|^N)$. So, the cost to obtain one smooth group element g is $O(|B_0/B|^N)$. We must have $O(|B|)$ number of such g. So

$$|B_0/B|^N \cdot |B| \approx |B|^2$$

where the left hand side is the cost for collecting enough smooth group elements. Thus we have $|B| = O(|B_0|^{(2N)/(N+1)})$.
2) **The case of one large prime.** The probability that $g \in G$ is almost smooth group element is $O(|B/B_0|^{N-1})$. Let V_1 is the set of almost collecting almost smooth group elements. So the cost of collecting V_1 is $O(|V_1| \cdot |B_0/B|^{N-1})$ which equals to $O(|B|^2)$. In this method, the number of the smooth group elements obtained from the elimination of large prime form V_1 is $|V_1|^2/|B_0|$. So, $|V_1|^2/|B_0| \approx |B|$. Thus, we have $|B| = O(|B_0|^{(2N-1)/(2N+1)}$.
3) **The case of two large primes.** The probability that $g \in G$ is 2-almost smooth group element is $O(|B/B_0|^{N-2})$. Let V_2 is the set of almost collecting 2-almost smooth group elements. So the cost of collecting V_2 is $O(|V_2| \cdot |B_0/B|^{N-2}))$ which equals to $O(|B|^2)$. In this method, $|V_2| \geq O(|B_0|)$ is needed. So, $|B_0| \cdot |B_0/B|^{N-2} \approx |B|^2$. Thus we have $|B| = O(|B_0|^{(N-1)/N})$.

Applying this lemma for the index calculus for the Jacobian of a curve over an extension field, Note that $B_0 = \{P - \infty \,|x(P) \in \mathbb{F}_q\}$, $|B_0| \approx q$, $N = ng$ and we have the following theorem.

Theorem 2. *1) The complexity of the index calculus by the rebalanced method is $O(q^{(2ng)/(ng+1)})$.*
2) The complexity of the index calculus by the one lage prime method is $O(q^{(4ng-2)/(2ng+1)})$.
3) The complexity of the index calculus by the two lage prime method is $O(q^{(2ng-2)/(2ng)})$.

5 Conclusion

In this manuscript, we propose an algorithm which checks whether a reduced divisor is decomposed or not, and computes the decomposed factor, if it is decomposed. From this algorithm, the concrete computations of decomposed factors are done by computer experiments when the pairs of the genus of the hyperelliptic curve and the degree of extension field are $(1, 3), (2, 2)$, and $(3, 2)$.

Acknowledgment

The author would like to thank Professor Kazuto Matsuo in Institute of Information Security for useful comments and fruitful discussions.

References

1. M. Adleman, J. DeMarrais, M.-D. 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, ANTS-I, LNCS 877, Springer-Verlag, 1994, pp. 28-40.
2. C. Diem, An Index Calculus Algorithm for Plane Curves of Small Degree, Algorithmic Number Theory - ANTS VII, LNCS 4076, 2006
3. A. Enge, P. Gaudry, A general framework for subexponential discrete logarithm algorithms, *Acta Arith.,* **102**, no. 1, 2002, pp. 83–103.
4. P.Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, *Eurocrypt 2000*, LNCS 1807, Springer-Verlag, 2000, pp. 19–34.
5. P. Gaudry, E. Thomé, Thériault, C. Diem, A double large prime variation for small genus hyperelliptic index calculus, Math. Comp. 76, 2007, pp.475–492. http://eprint.iacr.org/2004/153/
6. P. Gaudry, Index calculus for abelian varieties and the elliptic curve discrete logarithm problem, preprint, 2004. http://eprint.iacr.org/2004/073
7. M. Hindry, J. H. Silverman, Diophantine Geometry An introduction, Graduate Texts in Math. 201, Springer, 2000.
8. B. A. LaMacchia, A. M. Odlyzko, Solving large sparse linear systems over finite fields, *Crypto '90*, LNCS 537, Springer-Verlag, 1990, pp. 109–133.
9. K. Nagao, Improvement of Thériault Algorithm of Index Calculus for Jacobian of Hyperelliptic Curves of Small Genus, preprint, http://eprint.iacr.org/2004/161
10. I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Preprint, 2004.
11. N. Thériault, Index calculus attack for hyperelliptic curves of small genus, ASIACRYPT2003, LNCS 2894, Springer-Verlag, 2003, pp. 75–92.
12. D. H. Wiedemann, Solving sparse linear equations over finite fields, *IEEE Trans. Inform. Theory*, **IT-32**, no.1, 1986, pp.54–62.