Decomposed Attack for the Jacobian of a Hyperelliptic Curve over an Extension Field

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

Dept. of Engineering, Kanto Gakuin Univ.,
1-50-1 Mutsuura Higashi Kanazawa-ku Yokohama 236-8501, Japan

Abstract. We study the solution of the discrete logarithm problem for the Jacobian of a curve of genus g defined over an extension field $\mathbb{F}_{q^n}$, by decomposed attack, considering a external elements B_0 given by points of the curve whose x-coordinates are defined in $\mathbb{F}_q$. In the decomposed attack, an element of the group which is written by a sum of some elements of external elements is called (potentially) decomposed and the set of the terms, that appear in the sum, is called decomposed factor. In order for the running of the decomposed attack, a test for the (potential) decomposeness and the computation of the decomposed factor are needed. Here, we show that the test to determine if an element of the Jacobian (i.e., reduced divisor) is written by an ng sum of the elements of the external elements and the computation of decomposed factor are reduced to the problem of solving some multivariable polynomial system of equations by using the Riemann-Roch theorem. In particular, in the case of a hyperelliptic curve, we construct a concrete system of equations, which satisfies these properties and consists of $(n^2-n)g$ quadratic equations. Moreover, in the case of $(g,n) = (1,3),(2,2)$ and $(3,2)$, we give examples of the concrete computation of the decomposed factors by using the computer algebra system Magma.

Keywords Decomposed Attack, Hyperelliptic curve, Discrete logarithm problem, Weil descent attack

1 Introduction

In this work, we treat the solution of the discrete logarithm problem of the Jacobians of a curve C of genus g defined over an extension field $\mathbb{F}_{q^n}$ $(n \geq 2)$ by decomposed attack. In particular, when C is a hyperelliptic curve and $ng(\geq 3)$ is a small integer, we give the concrete algorithm for computing what is called decomposed factors. In [5], Gaudry first proposes the decomposed attack for the Jacobian of a hyperelliptic curve defined over a general finite field $\mathbb{F}_q$ considering a external elements given by the $\mathbb{F}_q$-rational points of the curve. This attack is usually called 'Index Calculus'. However, the behavior of this attack is quite different to the normal index calculus. So, it must be called another name, since the theoritical experts (not computational experts) of the normal index calculus can seldom (or never?) understand properly, even thought such variations are widly used [3], [10]. In recent works of the decomposed attack, which are the

improvements of [5], it is known that the techniques of 1) using the rebalance [4] and 2) using external elements [14], [12], [6],which were usually called large prime variations in the past time, are available. On the contraly, the techniques of large prime variations of normal index calculus are known as no contribution to decreasing the complexities, it must be needed to rename another name.

In [7], Gaudry also presents the decomposed attack for an elliptic curve defined over an extension field $\mathbb{F}_{q^n}$ considering the external elements B_0 given by points of the curve whose x-coordinates lie in $\mathbb{F}_q$. Actually, Gaudry proposes also the rebalanced and the external element variations. In this methods, the test for the potential decomposedness of $P \in E(\mathbb{F}_{q^n})$ (i.e., for being a sum of n elements of the external elements) and the computation of the decomposed factor (i.e., the terms of the external elements whose summation equals to P) are reduced to the problem of solving some system of multivariable polynomial equations of degree 2^{n-1}, n variables, and n equations, using Semaev's formula [13]. Moreover, Gaudry generalizes this decomposed attack to the case of the abelian varieties defined over an extension field, including the case of Jacobians of curves. However, in the case of non-elliptic curves, Semaev's formulas are not available. It is, in principal, possible to derive a similar system of equations using group law. Unfortunately, such is cumbersome. In fact, in the case of the Jacobian of a hyperelliptic curve of genus g, the sum of ng generic points is needed. Assuming that an element of Jacobian is written by the Mumford representation and that the group law is done by the Cantor algorithm [2], since the Cantor algorithm needs $g-1$ times reduction steps, explosions of the degree and terms occur in this computation.

In this work, we show that instead of using the group law, another system of equations is obtained from the theory of Riemann-Roch spaces (only in the case of Jacobians of curves). With this tool, the system of the equations is now simple to compute, and its parameters are easily controlled. In particular, in the case of Jacobians of hyperelliptic curves, this system of the equations consists of $(n^2-n)g$ quadratic equations in $(n^2-n)g$ indeterminates.

So, under the heuristic assumption that this system of the equations is (essentially) projectively 0-dimensional, the computational amount for solving this system of equations is estimated by $O(2^{(n^2-n)g \cdot C})$ where C is some constant less than 3. In the case of an elliptic curve (i.e., $g=1$), this computational amount heuristically equals to that of Gaudry's original equations system using Semaev's formula.

2 Decomposed attack for the Jacobian of a general plane curve

In this section, we present an overview of the decomposed attack for the Jacobian of a general plane curve using the Riemann-Roch theorem. Let C_a be the affine curve of genus g defined over an extension field $\mathbb{F}_{q^n}$ (i.e., $n \geq 2$) given by the equation $f(x,y)=0$, and let C be the corresponding non-singular complete curve. Assume that C_a is non-singular. From this, we have a canonical embedding $\iota : C_a \to C$. It is also assumed that $C \backslash \iota(C_a)$ only consists of a single $\mathbb{F}_{q^n}$-valued point, which is denoted by ∞ and is called the point at infinity. These assumptions are true for hyperelliptic curves so there is no problem for the main

results of this work. Let D_0 be a divisor of the form

$$D_0 = Q_1 + .. + Q_g - (g)\infty \tag{1}$$

where $Q_1, .., Q_g \in C(\overline{\mathbb{F}}_{q^n})$ and the multiset $\{Q_1, .., Q_g\}$ is stable under the action of Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^n}/\mathbb{F}_{q^n})$. Put $\phi_1(x) := \prod_{i=1}^{g}(x - x(Q_i))$, and this is noted in $\mathbb{F}_{q^n}[x]$.

Also put

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

as the external elements. (Strictly saying, B_0 must be a subset of $\mathrm{Jac}_C(\mathbb{F}_{q^n})$, and it is the set of the elements of the divisors $P - \infty$ where P has the above properties. Here, the term "$-\infty$" is omitted for simplicity.)

Assumption 1 *(heuristic assumption) The number of the multisets $\boldsymbol{P} = \{P_1, .., P_{ng}\}$ with $P_i \in B_0$, which satisfy the relation $\sum_{i=1}^{ng} P_i \sim \sum_{i=1}^{ng} P'_i$ for some different ($\boldsymbol{P} \neq \boldsymbol{P'}$) multiset $\boldsymbol{P'} = \{P'_1, .., P'_{ng}\}$ with $P'_i \in B_0$, is less than $q^{ng-\varepsilon}$, where ε is some positive constant.*

Here, we shortly state the validity of this assumption in the case of hyperelliptic curve. Let $C : y^2 = f(x)$ be the equation of hyperelliptic curve. For any $P = (x, y) \in C$, put $\bar{P} = (x, -y) \in C$. So, there are series of trivial relations $P + \bar{P} \sim P' + \bar{P'}$ for any $P, P' \in B_0$. The number of the multisets satisfying the condition of Assumption 1 and coming from these trivial relations is only $O(q^{ng-1})$ and it seems to be no series including many trivial relations. So, Assumption 1 seems to be valid.

In the following, we assume Assumption 1. From this assumption, we see easily that since "the number of the divisors of the form(1)"$\approx q^{gn}$ and $|B_0| \approx q$, the probability, that there are some $P_1, P_2, .., P_{ng} \in B_0$ (exactly ng elements, $P_i = P_j$ for some $i \neq j$ being allowed) such that

$$\begin{aligned} D_0 + P_1 + P_2 + ... + P_{ng} - (ng)\infty \\ = \textstyle\sum_{i=1}^{g} Q_i + P_1 + P_2 + ... + P_{ng} - (ng + g)\infty \sim 0, \end{aligned} \tag{2}$$

is approximately $1/(gn)!$, when $q \gg ng$.

Definition 1 *If a divisor D_0 is written by the form (2) for some $P_1, P_2, .., P_{ng} \in B_0$ (exactly ng elements, $P_i = P_j$ for some $i \neq j$ being allowed), D_0 is called potentially decomposed and in this case, the multiset $\{P_i\}_{i=1}^{ng}$ is called decomposed factor.*

We now fix D_0 and discuss how it can be tested that D_0 is potentially decomposed and the decomposed factor can be computed. So, $Q_1, ..., Q_g$ and $\phi_1(x)$, which are depended on D_0, are also fixed.

Let $D = \sum_{P \in C(\overline{\mathbb{F}}_{q^n})} n_p P$, $n_p \in \mathbb{Z}$ be a divisor of $C/\mathbb{F}_{q^n}$. Assume that D is stable under the action of Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^n}/\mathbb{F}_{q^n})$. Put $\deg(D) := \sum_{P \in C(\overline{\mathbb{F}}_{q^n})} n_p$, and $L(D) := \{f \in \mathbb{F}_{q^n}(C) \,|\, (f) + D \geq 0\} \cup \{0\}$. From the Riemann-Roch theorem (cf [9] 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 this Lemma, $dimL((ng)\infty - D_0) = dimL((ng+g)\infty - \sum_{i=1}^{g} Q_i) = ng - g$ Put $\{f_1(x,y), f_2(x,y), ..., f_{ng-g}(x,y)\}$ by a base of $L((ng)\infty - D_0))$. From Hess [8], we have the following lemma.

Lemma 2. *A base of $L((ng)\infty - D_0)$ is computable within Poly(q) time.*

From this lemma, since ∞ and D_0 is stable under the action of galois group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^n}/\mathbb{F}_{q^n})$, we have the following lemma directly.

Lemma 3. *An element $h \in L((ng)\infty - D_0)$ is written by*

$$a_1 f_1(x,y) + a_2 f_2(x,y) + ... + a_{ng-g} f_{ng-g}(x,y)$$

where a_i are values in $\mathbb{F}_{q^n}$.

Let

$$h(x,y) := A_1 f_1(x,y) + A_2 f_2(x,y) + ... + A_{ng-g} f_{ng-g}(x,y) \tag{3}$$

be a multivariable polynomial in $\mathbb{F}_{q^n}[A_1, ..., A_{ng-g}, x, y]$. For

$$\boldsymbol{a} = (a_1, ..., a_{ng-g}) \in \mathbb{A}^{ng-g}(\mathbb{F}_{q^n})$$

and some polynomial $p(x) \in \mathbb{F}_{q^n}[A_1, ..., A_{ng-g}, x]$, let $p_{\boldsymbol{a}}(x)$ be the polynomial obtained from $p(x)$ by substituting a_i for A_i. Now, we compute the intersections of $h_{\boldsymbol{a}}(x,y) = 0$ on C. Remember that the equation of C_a is $f(x,y) = 0$. Put $S(x) := \mathrm{Resultant}_y(f(x,y), h(x,y))$. From this construction, we then have the following lemma.

Lemma 4. *1) $S(x)$ is a multivariable polynomial in $\mathbb{F}_{q^n}[A_1, .., A_{ng-g}, x]$.*
2) $deg_x S(x) = ng + g$.
3) $\phi_1(x) \mid S(x)$.

Proof. 1) is trivial. For any $\boldsymbol{a} = (a_1, ..., a_{ng-g}) \in \mathbb{A}^{ng-g}(\mathbb{F}_{q^n})$, since $h_{\boldsymbol{a}}(x,y))$ has only poles $(ng+g)\infty$ on points at infinity, we have 2) and since $h_{\boldsymbol{a}}(x,y))$ have zeros at each Q_i's, we have 3).

Put $g(x) := S(x)/\phi(x)$. Since $\phi(x) \in \mathbb{F}_{q^n}[x]$, $g(x)$ is also a multivariable polynomial in $\mathbb{F}_{q^n}[A_1, .., A_{ng-g}, x]$. Thus, $g(x)$ is written in the form

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

where each $C_i \in \mathbb{F}_{q^n}[A_1, .., A_{ng-g}]$. Note that if the indeterminates A_i are replaced by values a_i, then one obtains a polynomial $g_{\boldsymbol{a}}(x)$ in $\mathbb{F}_{q^n}[x]$. The solutions of $g_{\boldsymbol{a}}(x) = 0$ mean the x-coordinates of the intersections $h_{\boldsymbol{a}}(x,y) = 0$ on C except $Q_1, ..., Q_g$. So, we have the following lemma.

Lemma 5. *The condition that D_0 is potentially decomposed is equivalent to the following: There is some $\boldsymbol{a} = (a_1, ..., a_{ng-g}) \in \mathbb{A}^{ng-g}(\mathbb{F}_{q^n})$ such that monic$(g_{\boldsymbol{a}}(x)) \in \mathbb{F}_q[x]$ and monic$(g_{\boldsymbol{a}}(x)) \in \mathbb{F}_q[x]$ factors completely in $\mathbb{F}_q[x]$.*

Now, we find such a_i's. Let $[\alpha_0(=1), \alpha_1, .., \alpha_{n-1}]$ be a base of $\mathbb{F}_{q^n}/\mathbb{F}_q$. We fix this base. Let $A_{i,j}$ $(1 \leq i \leq ng, 0 \leq j \leq n-1)$ be new indeterminates over $\mathbb{F}_q$, and let us consider the polynomials obtained by substituting A_i by $\sum_{j=0}^{n-1} A_{i,j}\alpha_j$ in $g(x)$. Let us denote the coefficients obtained in this way again by C_i. Then the coefficients can be written in the form

$$C_i = \sum_{j=0}^{n-1} C_{i,j}\alpha_j, \quad C_{i,j} \in \mathbb{F}_q[\cup_{1 \leq I \leq ng,\, 0 \leq J \leq n-1}\{A_{I,J}\}].$$

The condition of monic$(g_{\boldsymbol{a}}(x)) \in \mathbb{F}_q[x]$ is equivalent to the condition that the system of the equations

$$C_{i,j} = t_i C_{ng,j} \qquad (0 \leq i \leq ng-1, 0 \leq j \leq n-1) \tag{4}$$

of $(n^2+n)g$ indeterminates $\cup\{A_{i,j}\}$ and $t_0, ..., t_{ng-1}$ defined over $\mathbb{F}_q$ has some solutions in $\mathbb{F}_q$. So, the monic$(g_{\boldsymbol{a}}(x))$ is directly computed from the solution of (4) and we have shown the following lemma under the Assumption 2.

Theorem 1. *The test whether D_0 is potentially decomposed and the computation of the decomposed factor is essentially reduced to solving the system of the equations (4).*

In the next section, we will investigate the case of the hyperelliptic curve. In this case, there is a concrete representation of the Riemann-Roch space, and so we have a more concrete system of equations.

3 Decomposed attack for the Jacobian of a hyperelliptic curve

Now, we discuss the special case of Jacobians of hyperelliptic curves. In this case, there are concrete representations of the Riemann-Roch space and some techniques that $g(x)$ can be taken as a monic polynomial, and from this, a simple system of equations is derived. Let C be a hyperelliptic curve (including an 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 the characteristic of $\mathbb{F}_q$ is not 2 and $n \geq 2$. Put ∞ by the unique point at infinity on C. Let D_0 be a reduced divisor (i.e.,$\mathbb{F}_{q^n}$-rational point of the Jacobian) of C. To represent D_0, we use the so-called Mumford representation:

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

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 $f(x) - \phi_2(x)^2 \equiv 0 \bmod \phi_1(x)$. In the following, we will assume $\deg(\phi_1(x)) = g$. Note that there are $Q_1, .., Q_g \in C(\overline{\mathbb{F}}_{q^n})\backslash\{\infty\}$ satisfying the equation (1) and the multiset $\{Q_1, .., Q_g\}$ is stable under the action of Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^n}/\mathbb{F}_{q^n})$.

Similarly, put $B_0 := \{P \in C \,|\, P = (x, y) \in C(\mathbb{F}_{q^n}),\, x \in \mathbb{F}_q\}$ as a external elements. Then, from the (heuristic) Assumption 1, we can see easily that the probability, that there are some $P_1, P_2, .., P_{ng} \in B_0$ (exactly ng elements, $P_i = P_j$ for some $i \neq j$ being allowed) satisfying the equation (2), is approximately $1/(gn)!$, when $q \gg ng$.

In the following, we fix a reduced divisor D_0. So, $\phi_1(x)$, $\phi_2(x)$, and $Q_1, ..., Q_g$, which are depended on D_0, are also fixed.

In this work, we show the following proposition.

Proposition 1. *Let $V_1, V_2, ..., V_{(n^2-n)g}$ be indeterminates and let D_0 be a reduced divisor of $C/\mathbb{F}_{q^n}$. Then there are some computable 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 decomposed is equivalent to the following 1) and 2):
1) The system of equations $\{C_{i,j} = 0 \,|\, 0 \leq i \leq ng-1,\, 1 \leq j \leq n-1\}$ has some solution $\boldsymbol{v} = (v_1, .., v_{(n^2-n)g}) \in \mathbb{A}^{(n^2-n)g}(\mathbb{F}_q)$.
2) Put $c_i = C_{i,0}(v_1, .., v_{(n^2-n)g})$ for $0 \leq i \leq ng-1$. Then $G(x) = x^{ng} + c_{ng-1}x^{ng-1} + ... + c_0 \in \mathbb{F}_q[x]$ factors completely.
Moreover, if D_0 is potentially decomposed, the x-coordinates of the decomposed factor are the solutions of $G(x) = 0$.

From this proposition, the following theorem is directly obtained.

Theorem 2. *The test, whether D_0 is potentially decomposed and the computation of the decomposed factor (if possible), is essentially reduced to solving the system of the equations $\{C_{i,j} = 0 \,|\, 0 \leq i \leq ng-1,\, 1 \leq j \leq n-1\}$.*

In the following, we construct such multivariable polynomials $\{C_{i,j}\}$ and show Proposition 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 6. *1) $N_1 + N_2 = ng - 1$.*
2) $N_2 + g - 1 < N_1$.

Proof. Trivial.

Lemma 7. *$\{1, x, x^2, .., x^{N_1}, y, xy, ...x^{N_2}y\}$ 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 the hyperelliptic curve. Thus, since the number of the elements of the list $N_1 + N_2 + 2 = ng + 1$ is the same as the dim $L((ng+g)\infty)$ (from Lemma 1), we finish the proof.

Lemma 8. *$\{\phi_1(x), \phi_1(x)x, ..., \phi_1(x)x^{N_1-g}, (y-\phi_2(x)), (y-\phi_2(x))x, ..., (y-\phi_2(x))x^{N_2}\}$ 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 element in the list has a 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 6), each element in the list has at most $(ng+g)$ poles at ∞. Then

they are in $L((ng)\infty - D_0)$. Now, we show the independence. Assume they are not independent, and there are some non zero $f_1(x), f_2(x) \in \mathbb{F}_{q^n}[x]$ 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 $yf_2(x) \in \mathbb{F}_{q^n}[x]$ and $f_1(x) = f_2(x) = 0$. As this is a contradiction, they are independent. On the other hand, the number of the elements in the list is $N_1 + N_2 + 1 - g = ng - g$ from Lemma 6, which is the same as the $\dim L((ng)\infty - D_0)$. So we finish the proof.

From Lemma 8, an element $h \in L((ng)\infty - D_0)$ is written by

$$h(x,y) = \phi_1(x)(a_0 + a_1x + ... + a_{N_1-g}x^{N_1-g}) + (y - \phi_2(x))(b_0 + b_1x + ... + b_{N_2}x^{N_2}) \tag{5}$$

where a_i,b_i are values in $\mathbb{F}_{q^n}$.

Lemma 9. *Let $h(x,y) \in L((ng)\infty - D_0)$. Assume div(h(x,y)) is written in the form $P_1 + P_2 + ... + P_{ng} + \sum_{i=1}^{g} Q_i - (ng + g)\infty$ for $P_i \in C(\mathbb{F}_{q^n})\backslash\{\infty\}$. Then we have the following:*
1) $a_{N_1-g} \neq 0$ when $ng + g$ is even.
2) $b_{N_2} \neq 0$ when $ng + g$ is odd.

Proof. When $ng + g$ is even, assume $a_{N_1-g} = 0$, thus we have the order of the zero of $h(x,y)$ being truly less than $ng + g$ and $\mathrm{div}(h(x,y))$ is not written by the form of (2). Similarly, when $ng + g$ is odd, assume $b_{N_2} = 0$. Thus we have the order of the zero of $h(x,y)$ being truly less than $ng + g$ and $\mathrm{div}(h(x,y))$ is not written by the form of (2). So, we can assume that $a_{N_1-g} \neq 0$, if $ng + g$ is even, and $b_{N_2} \neq 0$, if $ng + g$ is odd.

Now, we compute the intersections of $h(x,y) = 0$ on C. For this purpose, y must be eliminated. Note that the point (x,y) fulfills $h(x,y) = 0$, if and only if the equation

$$y = \frac{-\phi_1(x)(a_0 + a_1x + ... + a_{N_1-g}x^{N_1-g}) + \phi_2(x)(b_0 + b_1x + ... + b_{N_2}x^{N_2})}{b_0 + b_1x + ... + b_{N_2}x^{N_2}}. \tag{6}$$

holds. By this y's representation, the number of the parameters must be decreased. So, put $a_{N_1-g} = 1$ when $ng + g$ is even and put $b_{N_2} = 1$ when $ng + g$ is odd (this can be done from the above lemma). Also put $M_1 = \begin{cases} N_1 - g - 1 \text{ when } ng + g \text{ is even} \\ N_1 - g \quad\quad \text{when } ng + g \text{ is odd} \end{cases}$, and $M_2 = \begin{cases} N_2 \quad\quad \text{when } ng + g \text{ is even} \\ N_2 - 1 \text{ when } ng + g \text{ is odd} \end{cases}$.
Note that $M_1 + M_2 = ng - g - 2$ from Lemma 6.

Put

$$s(x) := \begin{cases} -(\text{denominator of (6)})^2 f(x) + (\text{numerator of (6)})^2, \text{ if } ng + g \text{ is even} \\ (\text{denominator of (6)})^2 f(x) - (\text{numerator of (6)})^2, \quad \text{if } ng + g \text{ is odd} \end{cases}.$$

and let $S(x)$ be the multivariable polynomial obtained from the definition of $s(x)$ replacing the values a_i and b_i by the indeterminates A_i and B_i. From the construction, $S(x)$ is a monic polynomial of the 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 a monic polynomial in $\mathbb{F}_{q^n}[x]$, $g(x)$ is

also a 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.,

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

Similarly, for

$$\boldsymbol{v} = (a_0, ...a_{M_1}, b_0, ..., b_{M_2}) \in \mathbb{A}^{M_1+M_2+2}(\mathbb{F}_{q^n})$$

and some polynomial $p(x)$ in $\mathbb{F}_{q^n}[A_0, ..., A_{M_1}, B_{M_0}, ..., B_{M_2}, x]$, let $p_{\boldsymbol{v}}(x)$ be the polynomial obtained from $p(x)$ by substituting a_i and b_i for A_i and B_i. Then, the zeros of $g_{\boldsymbol{v}}(x) = 0$ are the x-coordinate of the intersections of $h(x, y) = 0$ on C except $Q_1, ..., Q_g$. Thus, we have the following lemma.

Lemma 10. *The condition that D_0 is a potentially decomposed reduced divisor is equivalent to the following:*
There is some $\boldsymbol{v} = (a_0, .., a_{M_1}, b_0, ...b_{M_2}) \in \mathbb{A}^{M_1+M_2+2}(\mathbb{F}_{q^n})$ such that $g_{\boldsymbol{v}}(x) \in \mathbb{F}_q[x]$ and $g_{\boldsymbol{v}}(x) \in \mathbb{F}_q[x]$ factors completely in $\mathbb{F}_q[x]$.

We now show how to find a_i in $\mathbb{F}_{q^n}$ $(0 \le i \le M_1)$ and b_i in $\mathbb{F}_q^n$ $(0 \le i \le M_2)$ such that $g_{\boldsymbol{v}}(x)$ in $\mathbb{F}_q[x]$.

Let $[\alpha_0(= 1), \alpha_1, .., \alpha_{n-1}]$ be a base of $\mathbb{F}_{q^n}/\mathbb{F}_q$ and fix this base. Let $A_{i,j}$ $(0 \le i \le M_1, 0 \le j \le n-1)$ and $B_{i,j}$ $(0 \le i \le M_2, 0 \le j \le n-1)$ be new indeterminates over $\mathbb{F}_q$. Note that the number of the indeterminates $\{A_{i,j}\} \cup \{B_{i,j}\}$ is

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

For simplicity, substitute the variables $A_{i,j}$ $(0 \le i \le M_1, 0 \le j \le n-1)$ and $B_{i,j}$ $(0 \le i \le M_2, 0 \le j \le n-1)$ by $\{V_1, V_2, ..., V_{(n^2-n)g}\}$. Let us consider the polynomials obtained by substituting A_i by $\sum_{j=0}^{n-1} A_{i,j}\alpha_j$ and B_i by $\sum_{j=0}^{n-1} B_{i,j}\alpha_j$ in $g(x)$. Also let us denote the coefficients obtained in this way again by C_i. Then the coefficients can be written in the form

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

Thus from Lemma 10, the condition $g_{\boldsymbol{v}}(x) \in \mathbb{F}_q[x]$ is equivalent to the condition that there are some $v_1, v_2, ..., v_{(n^2-n)g} \in \mathbb{F}_q$ such that

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

Moreover, when $g_{\boldsymbol{v}}(x) \in \mathbb{F}_q[x]$, $g(x) = x^{ng} + C_{ng-1,0}x^{ng-1} + ... + C_{0,0}$. The condition that $g_{\boldsymbol{v}}(x)$ 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 $c_i = C_{i,0}(v_1, v_2, ..., v_{(n^2-n)g})$. In this case, the solutions of $G(x) = 0$ are the x-coordinates of the decomposed factor. Then, we finish the proof of proposition 1 and construct the equation system $\{C_{i,j} = 0\}$.

4 Example

In this section, we examine three computational experiments of the decomposed factors of Jacobian. The computations are done by using the computer algebra system magma on a Windows XP preinstalled PC (CPU:Pentium M 2GHz, RAM:1GB). (In order to solve equation system, the function "variety" prepared in magma is used.) We compute three cases 1) $(g,n)=(1,3)$, 2) $(g,n)=(2,2)$, and 3) $(g,n)=(3,2)$ where g and n are the genus and the extension degree of the definition field of the chosen hyperelliptic/elliptic curve, respectively. In all cases, one trial, which means the judge as to whether a given element of Jacobian is decomposed or not and compute its decomposed factor, if it is decomposed, is done within 1 second. Since the probability that an element of Jacobian is decomposed is approximately $1/(gn)!$, the amount of the time for obtaining one potentially decomposed reduced divisor is within 6 sec, 24 sec, and 720 sec, respectively. Further, we will give the following three examples.

Case 1. Let $q=1073741789$(prime number), $\mathbb{F}_{q^3}:=\mathbb{F}_q[t]/(t^3+456725524t^2+251245663t+746495860)$, and let $E/\mathbb{F}_{q^3}$ be an elliptic curve defined by $y^2=x^3+(1073741788t^2+t)x+(126t+3969)$ 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.)

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

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

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

and let

$$\begin{aligned}
D_0 := (&x^2+1073741787tx+327245929t+867501600,\\
&(1023168391t+350252228)x+658555356t+446913597)
\end{aligned}$$

be a reduced divisor of C. We investigate whether $nD_0 : n = 1, 2, ..100$ are decomposed and find the following 9 decompositions. ($71D_0$ is written by 2 forms.)

$6D_0 \sim (1025731975, 776505688t + 911495013) + (728060789, 648475468t + 1067025179)$
$+ (341799975, 145077925t + 187604034) + (61964999, 227570631t + 639782700) - 4\infty$
$19D_0 \sim (1039361498, 15180988t + 396695374) + (828360115, 179412594t + 719919461)$
$+ (483171045, 677645208t + 604714840) + (34566209, 753841024t + 14375633) - 4\infty$
$33D_0 \sim (970690833, 608141084t + 889165804) + (260086243, 894605411t + 261264640)$
$+ (208957980, 43330622t + 581461318) + (190782894, 124873649t + 510328990) - 4\infty$
$35D_0 \sim (699447787, 267523741t + 562899544) + (559470007, 197827114t + 99971197)$
$+ (472594781, 579187919t + 266558458) + (453661772, 449424806t + 977318920) - 4\infty$
$48D_0 \sim (1009979214, 959734525t + 990871450) + (995813251, 44186049t + 288496638)$
$+ (521299995, 556594200t + 468424666) + (17946008, 977064852t + 1071618742) - 4\infty$
$71D_0 \sim (1019155056, 573896856t + 103042116) + (944470217, 829781939t + 184620624)$
$+ (727156004, 462612591t + 582877732) + (281900623, 553507533t + 42660552) - 4\infty$
$\sim (502979299, 412632304t + 1036827718) + (74527656, 927651409t + 452588110)$
$+ (50078888, 801072540t + 888737005) + (2986754, 556402789t + 236723678) - 4\infty$
$73D_0 \sim (843747137, 682161676t + 600252618) + (829302257, 145878028t + 853397395)$
$+ (290487906, 645896278t + 279001181) + (184873704, 567002729t + 620354511) - 4\infty$
$80D_0 \sim (907811987, 216534804t + 936839244) + (808513243, 873487475t + 273845273)$
$+ (520893378, 757248670t + 381150138) + (486203744, 494475019t + 791571132) - 4\infty$

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

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

and let

$$D_0 := (x^2 + 1073741787tx + 327245929t + 867501600, \\ (473621736t + 256126568)x + 145989647t + 687383736)$$

be a reduced divisor of C. We investigate whether $nD_0 : n = 1, 2, ..3000$ are decomposed and find the following 6 decompositions.

$414D_0 \sim (1001437837, 752632260t + 700158497) + (747112084, 656073918t + 400137619)$
$+ (620249588, 127943213t + 635474623) + (614180498, 206297635t + 445250468)$
$+ (515769009, 607297126t + 554290493) + (488549466, 627952783t + 854182612) - 6\infty$
$657D_0 \sim (939617127, 695261735t + 239531611) + (933351280, 935312661t + 961494096)$
$+ (799612924, 341923983t + 677495100) + (294787599, 279723229t + 760003067)$
$+ (273118782053704103t + 577497766) + (153381525, 983211238t + 517037777) - 6\infty$
$921D_0 \sim (1034634787, 400751409t + 829801342) + (763888873, 757155774t + 829936954)$
$+ (619620874, 800641683t + 200272230) + (603032615, 115219564t + 655011145)$
$+ (436423191, 285214454t + 450812747) + (125198811, 884750621t + 123305741) - 6\infty$
$1026D_0 \sim (1024020017, 267457905t + 41452942) + (794174628, 615676821t + 723336407)$
$+ (738567269, 433647609t + 128304659) + (629287731, 465842490t + 789390318)$
$+ (435082408, 878213106t + 603353206) + (79621979, 479459622t + 672937516) - 6\infty$
$1121D_0 \sim (764081031, 812350603t + 347878564) + (673426715, 687737442t + 381588704)$
$+ (6102522082007139t + 99219637) + (467560104, 619342780t + 228756808)$
$+ (179787786, 333322906t + 75482151) + (59221667, 860686653t + 625301206) - 6\infty$
$2289D_0 \sim (729358563, 482925408t + 170057124) + (529840657, 42328987t + 857983002)$
$+ (514618236, 436901100t + 416530686) + (350106356, 183495333t + 950710579)$

$$+(175898979, 411808870t + 427518366) + (96240558, 703780413t + 461022225) - 6\infty$$

5 Conclusion

In this manuscript, we have proposed an algorithm which checks whether a reduced divisor is potentially decomposed or not, and we have computed the decomposed factor, if it is potentially decomposed. From this algorithm, 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 the Institute of Information Security for useful comments and fruitful discussions and Professor Lisa Bond in Kanto Gakuin University for English writing.

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. D. G. Cantor, Computing in the Jacobian of hyperelliptic curve, Math. Comp., 48,1987,. pp.95-101.
3. C. Diem, An Index Calculus Algorithm for Plane Curves of Small Degree, Algorithmic Number Theory - ANTS VII, LNCS 4076, 2006
4. A. Enge, P. Gaudry, A general framework for subexponential discrete logarithm algorithms, *Acta Arith.,* **102**, no. 1, 2002, pp. 83–103.
5. P.Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, *Eurocrypt 2000*, LNCS 1807, Springer-Verlag, 2000, pp. 19–34.
6. P. Gaudry, E. Thomé, Thériault, C. Diem, A double large prime variation for small genus hyperelliptic decomposed attack, Math. Comp. 76, 2007, pp.475–492. (Preprint version is available on `http://eprint.iacr.org/2004/153/`)
7. P. Gaudry, Index calculus for abelian varieties and the elliptic curve discrete logarithm problem, preprint, 2004. `http://eprint.iacr.org/2004/073`
8. F. Hess, Computing Riemann-Roch spaces in algebraic function fields and related topics, *J. Symb. Comp.* **11**, 2001, pp. 1–22.
9. M. Hindry, J. H. Silverman, Diophantine Geometry An introduction, Graduate Texts in Math. 201, Springer, 2000.
10. R. Granger, F. Vercauteren, On the Discrete Logarithm Problem on Algebraic Tori, Advances in Cryptology, CRYPTO 2005, LNCS 3621, Springer-Verlag, 2005, pp. 66-85.
11. B. A. LaMacchia, A. M. Odlyzko, Solving large sparse linear systems over finite fields, *Crypto '90*, LNCS 537, Springer-Verlag, 1990, pp. 109–133.
12. K. Nagao, Index calculus for Jacobian of hyperelliptic curve of small genus using two large primes, Japan Journal of Industrial and Applied Mathematics, **24**, no.3, 2007. (Preprint version entitled by "Improvement of Thériault Algorithm of decomposed attack for Jacobian of Hyperelliptic Curves of Small Genus" is available on `http://eprint.iacr.org/2004/161`)

13. I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Preprint, 2004.
14. N. Thériault, Index calculus for hyperelliptic curves of small genus, ASIACRYPT2003, LNCS 2894, Springer-Verlag, 2003, pp. 75–92.
15. D. H. Wiedemann, Solving sparse linear equations over finite fields, *IEEE Trans. Inform. Theory*, **IT-32**, no.1, 1986, pp.54–62.

6 Appendix

In the appendix, we estimate the complexity of the decomposed attack, associated with input size q, for fixed g, n (i.e., g, n are considered as constants) under the Assumption 1. Here, we apply the ideas of the "The Rebalanced method" [4],"One external element method" [14], and "Two external elements method" [12] [6], which are the techniques of solving discrete logarithm of the Jacobian of a hyperelliptic curve over a general finite field, to our cost estimation for the case of an extension field. These techniques are very complicated, and we only give the outline of the algorithm and estimation of the complexity.

In this estimation, since n, g are fixed, the cost for solving the system of the equations is considered as Poly(q). For simplicity, the terms of Poly(q)-part of the complexity is omitted. For this purpose, we denote the symbol $\tilde{O}$ where the complexity $\tilde{O}(N(q))$ is estimated by

$$\tilde{O}(N(q)) < x(\log q)^y N(q) \quad \text{for some constants } x, y \in \mathbb{R}_{>0},$$

and the symbol $\approx$ that the relation $N_1(q) \approx N_2(q)$ is defined by

$$\frac{N_2(q)}{x_1(\log q)^{y_1}} < N_1(q) < x_2(\log q)^{y_2} N_2(q) \quad \text{for some constants } x_1, x_2, y_1, y_2 \in \mathbb{R}_{>0},$$

where $N(q), N_1(q) and N_2(q)$ are functions of input size q.

Now, let G be a general finite group and we consider the general decomposed attack over G. In the following, we also assume that
i) G has a prime order.
It is not an essential assumption, but it needs for the simplicity.

Definition 2 *1) An element of $g \in G$ written by $g = g_1 + .. + g_N$ for $g_1, ...g_N \in B_0$ is called potentially decomposed.*
2) The multiset $\{g_1, ..., g_N\}$ is called decomposed factor.

Take $B_0 \subset G$ as the external elements. For some positive integer N(Constant), we assume the following ii),iii),iv), and v):
ii) The probability that $g \in G$ is potentially decomposed is $O(1)$.
iii) For a $g \in G$, the cost for checking whether g is potentially decomposed or not is $\tilde{O}(1)$.
iv) For the potentially decomposed $g \in G$ the cost of computing decomposed factor $\{g_1, ..., g_N\}$ from g is $\tilde{O}(1)$. (If there are plural decoposed factors, the computation of all decomposed factors is needed.)
v) $|B_0|^2 \ll |G|$.

Note that $o(|G|) < |B_0|^N$ from ii) and $|B_0|^N < \tilde{O}(|G|)$ from iv). (Otherwise, the expected number of decomposed factors is bigger than $\tilde{O}(q^{\varepsilon})$ for some $\varepsilon > 0$ and iv) does not hold.) In the normal index calculus, the number of the factor basis which are used for the decomposition is basically large (i.e.,$N >> 1$). So, the randomly chossen element is basically written by some linear sum of factor basis in many many ways. However, it is difficult to compute such linear sums, so, by the use of the lifting to integer or number field ring and by the use of the sieving method, one can find some decomposition of randomly choosen element. So, remark carefully that the prerequisite condition of the normal index calculus and that of the decomposed attack is quite different.

In our case (i.e., G being the Jacobian of a hyperelliptic curve of genus g over extension field $\mathbb{F}_{q^n}$, B_0 being the set of $\mathbb{F}_{q^n}$-rational point of the curve whose x-coordinate lie in $\mathbb{F}_q$, $N = ng$), ii) is from (heuristic) Assumption 1, iii) and iv) are from Theorem 2, and v) is from the notations.

Take $B \subset B_0$ as a restricted external elements.

Definition 3 *1) An element of $g \in G$ written by $g = g_1 + .. + g_N$ for $g_1, ...g_N \in B$ is called decomposed.*
2) An element of $g \in G$ written by $g = g_1 + .. + g_N$ for one $g_i \in B_0 \backslash B$, and the other $g_j \in B$ $(1 \leq j \leq N, j \neq i)$ is called almost decomposed.
3) An element of $g \in G$ written by $g = g_1 + .. + g_N$ for two $g_{i1}, g_{i2} \in B_0 \backslash B$, and the other $g_j \in B$ $(1 \leq j \leq N, j \neq i_1, i_2)$is called 2-almost decomposed.
4)In every case, the multiset $\{g_1, ..., g_N\}$ is also called decomposed factor.

Now, we give the outlines of the algorithms, which are the variant of the decomposed attack [4], [14], [12], and [6], by Algorithm 1 and Algorithm 2.

Algorithm 1 The outline of the Rebalanced method

Input: $a, b \in G$ s.t. $a = nb$ for some unknown $n \in \mathbb{Z}/|G|\mathbb{Z}$.
Output: find n.
1: Initializing the list of the relations $L = \{\}$
2: **while** $|L| >$ suitable number N_0 **do**
3: For a pair of random numbers (r_1, r_2), computing $r_1 a + r_2 b$.
4: **if** $r_1 a + r_2 b$ being decomposed **then**
5: adding the informations of (r_1, r_2) and the decomposed factor to L.
6: (If there are plural decoposed factors, choosing one decomposed factor randomly.)
7: Solving the linear algebraic computation of roughly $|B| \times |B|$ size, modulo $|G|$
8: Computing n

Note that Algorithm 1 and Algorithm 2 are probabilistic, since they need random numbers. Also note that the probability that $r_1 a + r_2 b$ is potentially decomposed is $O(1)$, since $|G|$ is a prime number and $r_1 a + r_2 b$ can be considered as a random element of G. From the ideas of [4], [14], [12], and [6], we can obtain the following lemma.

Lemma 11. *Under the assumptions of i),ii),iii), iv) and v), we have the following:*
1) Let N_0 be the number of decomposed elements of G which are required in the

Algorithm 2 The outlines of the One (resp. Two)external element method

Input: $a, b \in G$ s.t. $a = nb$ for some unknown $n \in \mathbb{Z}/|G|\mathbb{Z}$.
Output: find n.

```
Initializing the list of the relations L = {}
while |L| > suitable numberN_1 (resp. N_2) do
    For a pair of random numbers (r_1, r_2), computing r_1 a + r_2 b.
    if r_1 a + r_2 b being almost-decomposed (resp. 2-almost decomposed) then
        adding the informations of (r_1, r_2) and the decomposed factor to L.
        (If there are plural decoposed factors, choosing one decomposed factor randomly.)
Updating L by the elimination of the terms of external elements.
Solving the linear algebraic computation of roughly |B| × |B| size, modulo |G|
Computing n
```

rebalanced method. Then, N_0 is estimated by Const $\times |B|$, i.e., $N_0 = O(|B|)$.
2) Let N_1 be the number of almost decomposed elements of G which are required in the one external element method. Then, $N_1^2/|B_0|$ is estimated by Const $\times |B|$, i.e., $N_1 = O(|B|^{1/2}|B_0|^{1/2})$.
3) Let N_2 be the number of 2-almost decomposed elements of G which are required in the two external element method. Then, N_2 is estimated by Const $\times |B_0|$, i.e., $N_2 = O(|B_0|)$.

Proof. Since $r_1a + r_2b$ is considered as a random element of G, if $r_1a + r_2b$ is potentially decomposed, the decomposed factor is considerd as rondom N-ple of external elements B_0. So, the (heuristic) assumption of the algorithm of [12] is true and the cost estimations are done by similar way of [12].

Thus, we have the following estimations of the complexity.

Lemma 12. *Under the assumptions of i),ii),iii), iv) and v), we have the following:*
1) The complexity of the general decomposed attack taking B as a restricted external elements by the rebalanced method is minimized at $|B| \approx |B_0|^{N/(N-1)}$, and it is estimated by $\tilde{O}(|B_0|^{(2N)/(N+1)})$.
2) The complexity of the general decomposed attack taking B as a restricted external elements and taking $B_0 \backslash B$ as a set of external elements by the one external element method is minimized at $|B| \approx |B_0|^{(2N-1)/(2N+1)}$, and it is estimated by $\tilde{O}(|B_0|^{(4N-2)/(2N+1)})$.
3) The complexity of the general decomposed attack taking B as a restricted external elements and taking $B_0 \backslash B$ as a set of external elements by the two external element method is minimized at $|B| \approx |B_0|^{(N-1)/N}$, and it is estimated by $\tilde{O}(|B_0|^{(2N-2)/N})$.

Proof. (Sketch of the proof) In every case, the cost of the part of linear algebra is $\tilde{O}(|B|^2)$, and for the rebalance, which is needed for minimizing the complexity, it is the same as the cost of the collecting divisors. So, we only need to estimate the optimized size $|B|$.

1)**The rebalanced method.** The probability that $g \in G$ is a decomposed group element is $O(|B/B_0|^N)$. So, the cost to obtain one decomposed group element g is $\tilde{O}(|B_0/B|^N)$. From Lemma 11, 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 decomposed group elements, and the right hand side is the cost for the linear algebra. Thus we have $|B| \approx |B_0|^{(2N)/(N+1)}$.
2) **The one external element method.** The probability that $g \in G$ is an almost decomposed group element is $O(|B/B_0|^{N-1})$. From Lemma 11, we must have $O(|B|^{1/2}|B_0|^{1/2})$ number of such g. Similarly, we have

$$|B_0/B|^{N-1} \cdot |B|^{1/2}|B_0|^{1/2} \approx |B|^2$$

and $|B| \approx |B_0|^{(2N-1)/(2N+1)}$ is obtained.
3) **The two external elements method.** The probability that $g \in G$ is a 2-almost decomposed group element is $O(|B/B_0|^{N-2})$. From Lemma 11, we must have $O(|B_0|)$ number of such g. Similarly, we have

$$|B_0/B|^{N-2} \cdot |B_0| \approx |B|^2$$

and $|B| \approx |B_0|^{(N-1)/N}$ is obtained.

Now, we apply this lemma for the decomposed attack 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 thus, we have the following claim.

Claim 1 *Assuming the (heuristic) Assumption 1 and $Jac(C/\mathbb{F}_{q^n})$ having a prime order, we have the following:*
1) The complexity of the decomposed attack by rebalanced method is estimated by $\tilde{O}(q^{(2ng)/(ng+1)})$.
2) The complexity of the decomposed attack by one external element method is estimated by $\tilde{O}(q^{(4ng-2)/(2ng+1)})$.
3) The complexity of the decomposed attack by two external element method is estimated by $\tilde{O}(q^{(2ng-1)/(ng)})$.