Decomposition formula of the Jacobian group of plane curve (Draft)

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

Fac. of Engineering, Kanto Gakuin Univ.,

Joint-work with Kazuto Matsuo(Kanagawa Univ.,) and Tsuyoshi Takagi(Kyushu Univ.))

Abstract. In this article, we give an algorithm for decomposing given element of Jacobian gruop into the sum of the decomposed factor, which consists of certain subset of the points of curve.

Keywords Decomposition Attack, ECDLP

1 Introduction

In this article, we give an algorithm for decomposing given element of Jacobian gruop into the sum of the decomposed factor, which consists of the points of curve. This is the generalization of the Semaev's formula [8] and by leading this formuls, we use the Riemann-Roch space technique similar as [5]. Recently, French researchers [2], [7], propose the algorithm for solving ECDLP over binary extension field by subexponential complexities of extension degree n. This algorithm uses the fact that the system of the equations obtained by decomposing given element of elliptic curve into decomposed fatcor contains many hidden equations and the complexity for decomposing a point of elliptic curve into $d = n^c$ ($0 < c < 1/2$ is a constant [1]) elements of decomposed factor, is subexponential. These arguments seems to have some gaps, but, any way, there is some posibility that ECDLP is subexponential. By using thier argument to the Jacobian of plane curve, we similarly get that the DLP of the Jacobian of plane curve of small genus over binaly extension field /or its generalization to small characterristic field also subexponential.

2 Notations

In this article, let $C : f(x, y) = 0$ be a plane curve of small genus g over $\mathbb{F}_{p^n}$, ∞ be a fixed point at infinity, $D_0 = Q_1 + Q_2 + ... + Q_g - g\infty$ be a fixed element of $\mathbf{Jac}(C/\mathbb{F}_{p^n})$. We also put $d_y := \deg_y f(x, y)$ and $\phi_1(x) := \prod_{i=1}^{g} x - x(Q_i)$.

3 Riemann-Roch Space

Proposition 1 (Riemann-Roch). *Let D be a divisor such that $\deg D \geq 2g - 1$. Then $dimL(D) = \deg D - g + 1$.*

Let d be an integer such that $d > 2g-1$. Put $D := d\infty - D_0 = (d+g)\infty - Q_1 - Q_2 - ... - Q_g$. Then form Riemann-Roch theorem(Proposition 1), there are independent elements of function field $f_i(x, y) \in \mathbb{F}_{p^n}(C)$ ($i = 0, 1, .., d - g$) such that $f_i(x, y) = 0$ at all $Q_1, .., Q_g$, $f_i(x, y)$ does not has a pole except ∞, $\mathrm{ord}_\infty f_i(x, y) < -d-g$ for $i = 1, 2, .., d-g$ and $\mathrm{ord}_\infty f_0(x, y) = -d-g$. Moreover, form Riemann-Roch Theorem, the element $h(x, y)$ of function field $F_{p^n}(C)$ such that $h(x, y) = 0$ at all $Q_1, .., Q_g$, $h(x, y)$ does not has a pole except ∞, and $\mathrm{ord}_\infty h(x, y) = -d-g$, is written by $h(x, y) = f_0(x, y)+a_1 f_1(x, y)+....+a_n f_n(x, y)$ ($a_i \in \mathbb{F}_{p^n}$) up to constant multiplication.

[1] Taking $d = O(n^{1/3})$ is best possible for the complexity

Let us denote

$$H(x,y) := f_0(x,y) + A_1 f_1(x,y) + ... + A_n f_n(x,y)$$

where A_i are variables and let $S(x) := \text{resultant}_y(f(x,y), H(x,y))$.

Lemma 1. *1.* $\deg_x S(x) = d + g$.
2. $\phi_1(x) \mid S(x)$
3. Put $g(x) := S(x)/\phi_1(x)$ *and we have* $\deg_x g(x) = d$.
4. Put C_i *be the i-th coefficients of* $g(x)$ *(i.e.* $g(x) = \sum_{i=0}^{d} C_i x^i$*). Then we have* C_i *is a polynomial of* $A_1, ..., A_{d-g}$ *with total degree* $\leq d_y$.

4 System of equations

Assume that there are d elements $P_i = (x_i, y_i) \in C(\bar{\mathbb{F}}_p)$ $(i = 1, 2, .., d)$ such that the relation $D_0 + P_1 + ... + P_d - d\infty \sim 0$ holds. From the definition of linear equivalence, there is an element $h(x,y) \in C(\bar{\mathbb{F}}_p)$ such that div $h(x,y) = D_0 + P_1 + ... + P_d - d\infty$. Put s_i by the x^i coefficient of the polynomial $\prod_{i=1}^{d}(x - x_i)$.

Lemma 2. *There are some* $a_i \in \bar{\mathbb{F}}_p$ $(i = 1, 2, .., d - g)$ *satisfying the following:*
1. $h(x,y) = Constant \times H(x,y)|_{A_i = a_i}$,
2. $s_i \cdot C_d|_{A_i=a_i} = C_i|_{A_i=a_i}$ $(i = 0, 1, .., d - 1)$.

Further let X_i $(i = 1, 2, .., d)$ be variables and put $S_i = S_i(X_1, .., X_d)$ by the X^i coefficient of the polynomial $\prod_{i=1}^{d}(X - X_i)$.

Consider the system of the equations

$$S_i(X_1, ..., X_d) \cdot C_d(A_1, .., A_{d-g}) = C_i(A_1, .., A_{d-g}) \quad (i = 0, 1, .., d - 1). \tag{1}$$

Note that the equations system consists of d equations of $d - g$ variables of A_i and d variables of X_i with total degree associated with $\{A_i' s\}$ being $\leq d_y$.

Proposition 2. *The condition that there are some* $P_i = (x_i, y_i)$ $(i = 1, 2, .., d)$ *such that* $D_0 + P_1 + ... + P_d - d\infty \sim 0$ *is equivalent to the condition that the equations system 1 of the variables*$\{A_i\}$ *and* $\{X_i\}$ *has some solution satisfying* $X_i = x_i$.

We want to eliminate the value of $\{A_i\}$. Fundamentaly, by eliminating $d - g$ variables form d equations, we must obtain (at least) g equations of $X_1, .., X_d$. However, only eliminating $\{A_i\}$, we does not get the sufficient condition that $\{X_i' s\}$ is the x-coordinate of decomposed factor, we use very techniqual method.

Let $[\theta_1, \theta_2, ..., \theta_g]$ be a (fixed) base of $\mathbb{F}_{p^{gn}}/\mathbb{F}_{p^n}$ and consider the equations

$$\text{The equations of (1) and } T = X_{d-g+1}\theta_1 + X_{d-g+2}\theta_2 + ... + X_d\theta_g \tag{2}$$

Note that the equations system consists of $d + 1$ equations of $d - g$ variables of A_i and d variables of X_i ,and one variable T with total degree associated with $\{A_i' s\}$ being $\leq d_y$ and with $\{X_i' s\}$ being $\leq d$.

Let $F(X_1, .., X_{d-g}, T)$ be the polynomial $\in \mathbb{F}_{p^{gn}}[X_1, ..., X_d, T]$ obtained from equation 2 by eliminating $A_1, ..., A_{d-g}$ and $X_{d-g+1}, ..., X_d$.

Proposition 3. *Assume* $P_i = (x_i, y_i) \in C(\mathbb{F}_{p^n})$ $(i - 1, 2, .., d)$ *and put* $t := x_{d-g+1}\theta_1 + x_{d-g+2}\theta_2 + ... + x_d\theta_g$. *The condition* $D_0 + P_1 + ... + P_d - d\infty \sim 0$ *is equivalent to the condition* $F(x_1, ..., x_{d-g}, t) = 0$.

Since $F(X_1, .., X_{d-g}, T) \in \mathbb{F}_{p^{gn}}[X_1, .., X_{d-g}, T]$, there are polynomials $F_j(X_1, ..., X_d) \in \mathbb{F}_{p^n}[X_1, , , .X_d]$ $(j = 1, 2, ..., g)$ such that

$$F(X_1, .., X_{d-g}, X_{d-g+1}\theta_1 + X_{d-g+2}\theta_2 + ... + X_d\theta_g) = \sum_{j=1}^{g} F_j(X_1, ..., X_d)\theta_j.$$

Proposition 4. *Assume $P_i = (x_i, y_i) \in C(\mathbb{F}_{p^n})$ $(i = 1, 2, .., d)$. The condition $D_0 + P_1 + ... + P_d - d\infty \sim 0$ is equivalent to the condition $F_j(x_1, ..., x_d) = 0$ $(j = 1, 2, ..., g)$.*

In order for estimating the total degree of $F_j(X_1, .., X_d)$, we use the Macaulay matrix [3]. Let Res be the multipolynomial resutant of the system of the equations (2) considering $A_1, ..., A_{d-g}, X_{d-g+1}, ..., X_d$ as variables and $X_1, ..., X_{d-g}, T$ as constants. Form its meaning, Res is one representation of $F(X_1, ..., X_{d-g}, T)$. Since each equation of (2) has degree $\leq d_y + g$, the maximam degree of the multipolynomial, which is represented by some row of Res is $\leq \sum_{i=1}^{d}(d_y + g - 1) = d(d_y + g - 1)$. So we have the upper bound of the size of the matrix Res is $\leq \binom{d(d_y+g)}{d}$, since the number of the monomials of n variables and degree $\leq m$ is $\binom{m+n}{n}$. From Stirling formula, which state $N! \approx \sqrt{2\pi N}N^N \exp(-N)$, it is estimated by

$$\sqrt{\frac{d_y + g}{2\pi(d_y + g - 1)d}} \times (\frac{(d_y + g)^{(d_y+g)}}{(d_y + g - 1)^{(d_y+g-1)}})^d.$$

Moreover, we see that an element of the matrix Res is degree 1 polynomial of $S_i = S_i(X_1, ..., X_d)$ and T (thus also we see degree atmost $d - g$ polynomial of $\{X_i\}$ and T), we have the following:

Proposition 5. *The upper bound of the total degree of the multipolinomial $F(X_1, ..., X_{d-g}, T)$ and $F_j(X_1, ..., X_d)$ $(j = 1, 2, ..., g)$ are estimated by $(d-g) \times \sqrt{\frac{d_y+g}{2\pi(d_y+g-1)d}} \times (\frac{(d_y+g)^{(d_y+g)}}{(d_y+g-1)^{(d_y+g-1)}})^d$.*

5 Hyper elliptic curve case

In this section, we consider the hyper elliptic curve case. Let $C : f(x, y) = y^2 + b'_1 xy + .. - x^{2g+1} - b_{2g}x^{2g} - ... - a_0 = 0$ be a hyper elliptic curve of small genus g over $\mathbb{F}_{p^n}$, ∞ be a unique point at infinity, $D_0 = Q_1 + Q_2 + ... + Q_g - g\infty$ be a fixed element of $\mathbf{Jac}(C/\mathbb{F}_{p^n})$. From Munford representation, D_0 is also represented by using two polynomials $\phi_1(x) := \prod_{i=1}^{g} x - x(Q_i)$ and $\phi_2(x)$ which has the properties $\deg \phi_2(x) \leq g - 1$ and $y(Q_i) = \phi_2(x(Q_i))$.

Let d be an integer such that $d > 2g-1$. Put $D := d\infty - D_0 = (d+g)\infty - Q_1 - Q_2 - ... - Q_g$. Then form Riemann-Roch theorem(Proposition 1), the base of the vector space
$L(D) := \{h \in C(\mathbb{F}_{p^n}) | h$ has zero at all $Q_1, .., Q_g$ and has pole only at ∞, $\mathrm{ord}_\infty h \leq -d - g\}$ is written by

$$\{\phi_1(x), \phi_1(x)x, ..., \phi_1(x)x^{M_1}, (y - \phi_2(x)), (y - \phi_2(x))x, ..., (y - \phi_2(x))x^{M^2}\}$$

where $M_1 = \lfloor (d-g)/2 \rfloor$ and $M_2 \lfloor (d-g-1)/2 \rfloor$. Note that when $2|(d-g)$, $\mathrm{ord}_\infty \phi_1(x)x^{M_1} = g+d$ and when $2 \not| (d - g)$, $\mathrm{ord}_\infty (y - \phi_2(x))x^{M_2} = g + d$.
So put $f_0(x, y) := \begin{cases} \phi_1(x)x^{M_1} & 2|(d-g) \\ (y - \phi_2(x))x^{M_2} & 2 \not| (d-g) \end{cases}$ and put$f_i(x, y)$ $(1 \leq i \leq d - g)$ by other bases of $L(D)$ and exceeds the simailar argument of Section 2. Let us denote

$$H(x, y) := f_0(x, y) + A_1 f_1(x, y) + ... + A_n f_n(x, y)$$

where A_i are variables and let $S(x) := \pm\mathrm{resultant}_y(f(x, y), H(x, y))$.

Lemma 3. *1. $S(x)$ is monic polynomial of x and $\deg_x S(x) = d + g$.*
2. $\phi_1(x) \,|\, S(x)$
3. Put $g(x) := S(x)/\phi_1(x)$. $g(x)$ is a monic polynomial of x and $\deg_x g(x) = d$.
4. Put C_i be the i-th coefficients of $g(x)$ (i.e. $g(x) = x^d + \sum_{i=0}^{d-1} C_i x^i$). Then we have C_i is a polynomial of $A_1, ..., A_{d-g}$ with total degree 2. (Note that $C_d = 1$ form $g(x)$ being monic.)

Similarly let X_i $(i = 1, 2, .., d)$ be variables and put $S_i = S_i(X_1, .., X_d)$ by the X^i coefficient of the polynomial $\prod_{i=1}^{d}(X - X_i)$.

Consider the system of the equations

$$S_i(X_1, ..., X_d) = C_i(A_1, .., A_{d-g}) \quad (i = 0, 1, .., d-1). \tag{3}$$

Proposition 6. *The condition that there are some $P_i = (x_i, y_i)$ $(i = 1, 2, .., d)$ such that $D_0 + P_1 + ... + P_d - d\infty \sim 0$ is equivalent to the condition that the equations system 3 of the variables$\{A_i\}$ and $\{X_i\}$ has some solution satisfying $X_i = x_i$.*

6 Decomposed factor

In 2009, Diem [1] proposes the way of taking decomposed factor, called Diem-variant, and shows ECDLP of elliptic curves over $\mathbb{F}_{p^n}$ satisfying $\log p = O(n^2)$ has subexponential complexity when input size $n \log p$ goes to infinity. In 2005 or 2006, soon after the Semaev's formula is discoverd, Matsuo also found the simmilar and more general way of taking decomposed factor (for exapmle distinct or non-equal size decomposed factor). Matsuo tries to decompose an element of elliptic curve over around 120-bit size binary field, but, huge memory workstation does not returns the reply and it it not presented and only the researchers around him knows this.

Here, we propose the way of taking decomposed factor of Jacobian of the curve, which is the generalization of Matsuo's decomposed factor. Fix $[w_1, ..., w_n]$ be the base of $\mathbb{F}_{p^n}/\mathbb{F}_p$. Let $n_1, ..n_d$ be the positive integers satisfying $n_1 + ... + n_d \approx ng$. Put

$$B'_i := \{\sum_{j=1}^{n_j} x_{i,j} w_j | x_{i,j} \in \mathbb{F}_p\} \quad (i = 1, 2, ..., d).$$

Let $r_1, ..., r_d$ be elements of $\mathbb{F}_{p^n}$ [2] and take decomposed factor B_i by

$$B_i := \{P - \infty \in \mathbf{Jac}(C/\mathbb{F}_{p^n}) | P \in C(\mathbb{F}_{p^n}),\ \exists x \in B'_i \text{ such that } x(P) = x + r_i\} \quad (i = 1, 2, ..., d),$$

and consider the decomposition (of D_0)

$$D_0 + \sum_{i=1}^{d}(P_i - \infty) = 0 \qquad (P_i - \infty) \in B_i$$

in Jacobian group.

Note that B_i's are essentially disjoint, $|B_i| \approx p^{n_i}$, and the probability that the decomposition success is $O(p^{n_1+...+n_d-ng}) \approx 1$. From the disjointness, it is improved that the term of $1/d!$ in the probability is omitted. (Remark that it is needed to compute gaussian elimination of d-times size matrix in the last step.)

So, we have the following proposition, which is a generalization of Diem's result:

Proposition 7. *DLP of the Jacobian group of a plane curve of small genus g over extension field $\mathbb{F}_{p^n}$ satisfying $\log p = O((ng)^2)$ (since g is constant, it is equivalent to $\log p = O(n^2)$) has subexponential complexity when input size $N = ng \log p$ goes to infinity. .*

Proof. We consider the case $d = ng$, $n_1 = n_2 = ... = n_d = 1$ and compute the decomposition of given divissor D_0. In this case, D_0 is decomposed by the divisor $\sum_{i=1}^{ng}(P_i - \infty)$ such that $x(P_i) = (x_{i,1}w_1 + r_i)$ with $x_{i,1} \in \mathbb{F}_p$. From Proposition 4, in order to find such $\{x_{i,1}\}$, it it sufficient to solve the $2ng$ equations $F_{j,k} \in \mathbb{F}_p[\{x_{i,1}\}]$ obtained by Weil descent from $F_j(x_{1,1}w_1 + r_1, ..., x_{ng,1}w_1 + r_{ng}) = 0$ $(j = 1, 2, ..., g)$. (Note that put $F_{j,k}$ be the polymonials obtained by $F_j(x_{1,1}w_1 + r_1, ..., x_{ng,1}w_1 + r_{ng}) = \sum_{k=1}^{n} F_{j,k}(x_{1,1}, ..., x_{ng,1})w_k$). From

[2] Take $r_{i+1} \in \mathbb{F}_{p^n} \setminus \cup_{j=1}^{i} B'_j$ and disjoint decomposed factor is constracted

Proposition 5,the degree of the equations obtained by Weil descent is $\leq \text{Const}_1^d = \text{Const}_1^{ng}$. So the upper bound of the cost of finding the value of $\{x_{i,1}\}$ by using Gröbner basis is estimated by $(\text{Const}_1^{ng})^{ng\times\text{Const}_2} = exp(\text{Const}_3\, n^2g^2) = exp(N^{2/3+o(1)})$. In order to solve the DLP, we must have obtain $dp = ngp$ decomposition and compute the Gaussian elimination of the $dp = ngp$ size matrix. Since $ngp = exp(\log(ng) + \log p) = exp(N^{2/3+o(1)})$, we also have both of the costs of ngp decomposition and Gaussian elimination are $exp(N^{2/3+o(1)})$.

References

1. C. Diem, On the discrete logarithm problem in class groups II, preprint, 2011.
2. J-C. Faugére, L. Perret, C. Petit, and G. Renault, Improving the complexity of index calculus algorithms in elliptic curves over binary fields, EUROCRYPTO 2012, LNCS **7237**, pp.27-44.
3. F.S. Macaulay, The algebraic Theory of modular systems, 1916, Cambridge.
4. 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.
5. K. Nagao, Decomposition Attack for the Jacobian of a Hyperelliptic Curve over an Extension Field, 9th International Symposium,ANTS-IX., Nancy, France, July 2010, Proceedings LNCS 6197,Springer, pp.285–300, 2010.
6. K. Nagao, Equations System coming from Weil descent and subexponential attack for algebraic curve cryptosystem, draft, 2013.
7. C. Petit and J-J. Quisquater. On Polynomial Systems Arising from a Weil Descent, Asiacrypt 2012, Springer LNCS **7658**, Springer, pp.451-466.
8. I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Preprint, 2004.