

# 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 group into the sum of the decomposed factor, which consists of certain subset of the points of curve.

**Keywords** Decomposition Attack, ECDLP

**revise 6 Nov** First version of this manuscript, we use Weil descent like technique and the decomposition problem of Jacobian reduces to solving exact  $g$  number equations system. However, Proposition 3 is not true and this technique can not be used. So, we re-write §4 and show that the decomposition problem of Jacobian reduces to solving some equations system (however, the number of the equations is quite large).

## 1 Introduction

In this article, we give an algorithm for decomposing given element of Jacobian group into the sum of the decomposed factor, which consists of the points of curve. This is the generalization of the Semaev's formula [9] and by leading this formula, we use the Riemann-Roch space technique similar as [6]. Recently, French researchers [3], [8], 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 factor 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<sup>1</sup>) elements of decomposed factor, is subexponential. These arguments seems to have some gaps, but, any way, there is some possibility that ECDLP is subexponential. By using their argument to the Jacobian of plane curve, we similarly get that the DLP of the Jacobian of plane curve of small genus over binary extension field /or its generalization to small characteristic field also subexponential.

## 2 Notations

In this article, let  $C : f(x, y) = 0$  be a plane curve of small genus  $g$  over  $\mathbb{F}_{p^n}$ ,  $\infty$  be a fixed point at infinity,  $D_0 = Q_1 + Q_2 + \dots + Q_g - g\infty$  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  $\dim L(D) = \deg D - g + 1$ .*

Let  $d$  be an integer such that  $d > 2g - 1$ . Put  $D := d\infty - D_0 = (d + g)\infty - Q_1 - Q_2 - \dots - Q_g$ . Then from Riemann-Roch theorem(Proposition 1), there are independent elements of function field  $f_i(x, y) \in \mathbb{F}_{p^n}(C)$  ( $i = 0, 1, \dots, d - g$ ) such that  $f_i(x, y) = 0$  at all  $Q_1, \dots, Q_g$ ,  $f_i(x, y)$  does

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

not has a pole except  $\infty$ ,  $\text{ord}_\infty f_i(x, y) < -d-g$  for  $i = 1, 2, \dots, d-g$  and  $\text{ord}_\infty f_0(x, y) = -d-g$ . Moreover, from Riemann-Roch Theorem, the element  $h(x, y)$  of function field  $F_{p^n}(C)$  such that  $h(x, y) = 0$  at all  $Q_1, \dots, Q_g$ ,  $h(x, y)$  does not has a pole except  $\infty$ , and  $\text{ord}_\infty h(x, y) = -d-g$ , is written by  $h(x, y) = f_0(x, y) + a_1 f_1(x, y) + \dots + a_{d-g} f_{d-g}(x, y)$  ( $a_i \in \mathbb{F}_{p^n}$ ) up to constant multiplication.

Let us denote

$$H(x, y) := f_0(x, y) + A_1 f_1(x, y) + \dots + A_{d-g} f_{d-g}(x, y)$$

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  $A_1, \dots, A_{d-g}$  with total degree  $\leq d_y$ .

## 4 System of equations

From the discussion of §3, we have the following lemma;

**Lemma 2.** Let  $P_i = (x_i, y_i) \in C(\overline{\mathbb{F}_p})$  ( $i = 1, 2, \dots, d$ ) and Put  $s_i$  by the  $x^i$  coefficient of the polynomial  $\prod_{i=1}^d (x - x_i)$ . When  $D_0 + P_1 + \dots + P_d - d\infty \sim 0$ , there are some  $a_i \in \overline{\mathbb{F}_p}$  ( $i = 1, 2, \dots, d-g$ ) satisfying the following:

1.  $h(x, y) = \text{Constant} \times H(x, y)|_{A_i=a_i}$ ,

2.  $s_i \cdot C_d|_{A_i=a_i} = C_i|_{A_i=a_i}$  ( $i = 0, 1, \dots, d-1$ ).

Further let  $X_i$  ( $i = 1, \dots, d$ ) be variables and put  $S_i = S_i(X_1, \dots, X_d) \in \mathbb{F}_{p^n}[X_1, \dots, X_d]$  by  $x^i$ -th coefficient of  $\prod_{i=1}^d (X - X_i)$ . Put

$$g_i(A_1, \dots, A_{d-g}; X_1, \dots, X_d) := S_i(X_1, \dots, X_d) C_d(A_1, \dots, A_{d-g}) - C_i(A_1, \dots, A_{d-g}), \quad (i = 0, \dots, d-1)$$

and consider the equation system

$$EQS_1 : \{g_i(A_1, \dots, A_{d-g}; X_1, \dots, X_d) = 0 \mid i = 0, \dots, d-1\}.$$

**Lemma 3.** When  $EQS_1$  has a solution  $(a_1, \dots, a_{d-g}; x_1, \dots, x_d) \in \mathbb{A}^{2d-g}(\overline{\mathbb{F}_p})$ , there are some  $P_i \in C(\overline{\mathbb{F}_p})$  ( $i = 1, \dots, d$ ) such that  $D_0 + P_1 + \dots + P_d - d\infty \sim 0$  and  $x(P_i) = x_i$  ( $i = 1, \dots, d$ ).

*Proof.* Put  $h(x, y) = f_0(x, y) + \sum_{i=1}^{d-g} a_i f_i(x, y)$ , and let  $P_i$ 's be the points on  $C(\overline{\mathbb{F}_p})$  which meet  $h(x, y) = 0$  except  $Q_1, \dots, Q_g$ . So, we have  $\{x(P_i) \mid i = 1, \dots, d\} = \{x_1, \dots, x_d\}$  and finish the proof.

From Lemma 2, and Lemma 3, we have the following;

**Proposition 2.** The following (1) (2) are equivalent;

1)  $EQS_1$  has solution  $(a_1, \dots, a_{d-g}; x_1, \dots, x_d) \in \mathbb{A}^{2d-g}(\overline{\mathbb{F}_p})$

2) There are some  $P_i \in C(\overline{\mathbb{F}_p})$  ( $i = 1, \dots, d$ ) satisfying  $x(P_i) = x_i$  ( $i = 1, \dots, d$ ) and  $D_0 + P_1 + \dots + P_d \sim 0$ .

Let  $T_1, \dots, T_g$  be new variables and put

$$h_i(A_1, \dots, A_{d-g}; X_1, \dots, X_d; T_1, \dots, T_g) := g_i(A_1, \dots, A_{d-g}; X_1, \dots, X_d), \quad (i = 0, \dots, d-g-1),$$

$h_{d-g}(A_1, \dots, A_{d-g}; X_1, \dots, X_d; T_1, \dots, T_g) := \sum_{i=1}^g T_i \cdot g_{i+d-g-1}(A_1, \dots, A_{d-g}; X_1, \dots, X_d)$ , and consider the equation system

$$EQS_2 : \{h_i(A_1, \dots, A_{d-g}; X_1, \dots, X_d; T_1, \dots, T_g) = 0 \mid i = 0, \dots, d-g\}.$$

## 5 Absolute resultant

In this section, we study the absolute resultant of  $EQS_2$  (cf [1] §3). Here, we consider  $\{A_i\}$  as variables and  $\{X_i\} \cup \{T_i\}$  as constants and eliminate  $\{A_i\}$  from  $EQS_2$ . For the precise discussion, we must use the homogenous polynomial system. However, it is complicated and we continue the discussion using non-homogenous polynomial system.

Let  $D_i := \deg_{\{X_i\}} h_i (\leq d_y)$  ( $i = 0, \dots, d-g$ ) and  $D = \sum_{i=0}^{d-g} D_i - (d-g) (\leq (d-g)d_y)$ . Let  $M_{all}$  be the set of monomials of  $A_1, \dots, A_{d-g}$  of degree  $\leq D$ . The number of such monomial  $\#M_{all}$  is estimated by  $\binom{d-g+D}{d-g} \leq \binom{(d-g)(d_y-1)}{d-g}$  and from Stirling formula, which

states  $N! \sim \sqrt{2\pi N} N^N \exp(-N)$ , we have  $\#M_{all} \leq \sqrt{\frac{d_y+1}{2\pi(d-g)d_y}} \left\{ \frac{(d_y+1)^{d_y+1}}{d_y^{d_y}} \right\}^{d-g}$ . Let

$$S_0 := \{m \in M_{all} \mid \deg_{\{A_i\}} m \leq D - D_0\},$$

$$S_1 := \{m \in M_{all} \mid \deg_{\{A_i\}} m > D - D_0, A_1^{D_1} \mid m\},$$

$$S_2 := \{m \in M_{all} \mid \deg_{\{A_i\}} m > D - D_0, A_1^{D_1} \nmid m, A_2^{D_2} \mid m\},$$

.....

$$S_{d-g} := \{m \in M_{all} \mid \deg_{\{A_i\}} m > D - D_0, A_1^{D_1} \nmid m, \dots, A_{d-g-1}^{D_{d-g-1}} \nmid m, A_{d-g}^{D_{d-g}} \mid m\},$$

Note that it is well known that  $\#S_{d-g} = D_0 D_1 \dots D_{d-g-1}$  and  $M_{all} = \cup_{i=0}^{d-g} S_i$  (disjoint division of  $M_{all}$ ).

Put  $M_{all} = \{\vec{M}_1, \dots, \vec{M}_{\#M_{all}}\}$  and  $\cup_{i=0}^{d-g} \{h_i m \mid m \in S_i\} = \{G_1, \dots, G_{\#M_{all}}\}$ . Let  $G_{ij} \in \mathbb{F}_p[\{X_i\} \cup \{T_i\}]$  be the polynomials such that  $G_i = \sum_{j=1}^{\#M_{all}} G_{ij} \vec{M}_j$  and

$$Res(X_1, \dots, X_d; T_1, \dots, T_g) = \text{determinant of the matrix } [G_{ij}]_{1 \leq i, j \leq \#M_{all}} \in \mathbb{F}_p[\{X_i\} \cup \{T_i\}].$$

$Res$  is known as absolute resultant and we have the following;<sup>2</sup>

**Lemma 4.** Let  $(x_1, \dots, x_d) \in \mathbb{A}^d(\overline{\mathbb{F}}_p)$ . The following (1) (2) are (essentially) equivalent;

1)  $Res(x_1, \dots, x_d; T_1, \dots, T_g) = 0$  ( $T_i$ 's are still variables).

2) There are some  $(a_1, \dots, a_{d-g}) \in \mathbb{A}^{d-g}(\overline{\mathbb{F}}_p)$  satisfying  $(a_1, \dots, a_{d-g}; x_1, \dots, x_d)$  is a solution of  $EQS_1$ .

**Lemma 5.** 1)  $\deg_{\{T_i\}} Res(X_1, \dots, X_d; T_1, \dots, T_g) \leq d_y^{d-g}$ .

2)  $\deg_{\{X_i\}} Res(X_1, \dots, X_d; T_1, \dots, T_g) \leq d \cdot \#M_{all} \leq d \cdot \sqrt{\frac{d_y+1}{2\pi(d-g)d_y}} \left\{ \frac{(d_y+1)^{d_y+1}}{d_y^{d_y}} \right\}^{d-g}$ .

*Proof.* The number of the row that  $T_i$  appears equals to  $\#S_{d-g} = D_0 D_1 \dots D_{d-g-1} \leq d_y^{d-g}$  and the degree of  $\{T_i\}$  of each element of the the matrix is 1. So, we have 1). The degree of  $\{X_i\}$  of each element of the the matrix is  $\leq d$  and the size of the matrix is  $\#M_{all}$ . So, we have 2).

Let  $\{m_1, \dots, m_N\}$  be the set of monomial of  $\{T_1, \dots, T_g\}$  which divide some monomial of  $Res(X_1, \dots, X_d; T_1, \dots, T_g)$  and put

$Res(X_1, \dots, X_d; T_1, \dots, T_g) = \sum_{i=1}^N H_i(X_1, \dots, X_d) \cdot m_i$ . From Lemma 5, we have  $\deg_{\{T_i\}} Res \leq d_y^{d-g}$  and  $N = \binom{\deg_{\{T_i\}} Res + g}{g} \leq \frac{(d_y^{d-g} + g)^g}{g!}$ . From Lemma 5,

we also have  $\deg_{\{X_i\}} H_i(X_1, \dots, X_d) \leq d \sqrt{\frac{d_y+1}{2\pi(d-g)d_y}} \left\{ \frac{(d_y+1)^{d_y+1}}{d_y^{d_y}} \right\}^{d-g}$  ( $i = 1, \dots, N$ ).

From Lemma 4 and Proposition 2, we have the following;

**Proposition 3.** Let  $(x_1, \dots, x_d) \in \mathbb{A}^d(\overline{\mathbb{F}}_p)$ . The following (1) (2) are (essentially) equivalent;

1)  $H_i(x_1, \dots, x_d) = 0$  ( $i = 1, \dots, N$ ).

2) There are some  $P_i \in C(\overline{\mathbb{F}}_p)$  ( $i = 1, \dots, d$ ) satisfying  $x(P_i) = x_i$  ( $i = 1, \dots, d$ ) and  $D_0 + P_1 + \dots + P_d \sim 0$ .

<sup>2</sup> We do not use homogenous polynomial system and projective variety. So, there is some gap. However, it seems to negligible and continue the discussion.

Thus, the decomposition problem of Jacobian of a plane curve reduced to solve some the equations system.

## 6 Hyper elliptic curve case

In this section, we consider the hyper elliptic curve case. Let  $C : f(x, y) = y^2 + b_1xy + \dots - x^{2g+1} - b_{2g}x^{2g} - \dots - a_0 = 0$  be a hyper elliptic curve of small genus  $g$  over  $\mathbb{F}_{p^n}$ ,  $\infty$  be a unique point at infinity,  $D_0 = Q_1 + Q_2 + \dots + Q_g - g\infty$  be a fixed element of  $\mathbf{Jac}(C/\mathbb{F}_{p^n})$ . From Mumford 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  $D := d\infty - D_0 = (d+g)\infty - Q_1 - Q_2 - \dots - Q_g$ . Then from Riemann-Roch theorem (Proposition 1), the base of the vector space  $L(D) := \{h \in C(\mathbb{F}_{p^n}) | h \text{ has zero at all } Q_1, \dots, Q_g \text{ and has pole only at } \infty, \text{ord}_\infty h \leq -d - g\}$  is written by

$$\{\phi_1(x), \phi_1(x)x, \dots, \phi_1(x)x^{M_1}, (y - \phi_2(x)), (y - \phi_2(x))x, \dots, (y - \phi_2(x))x^{M_2}\}$$

where  $M_1 = \lfloor (d-g)/2 \rfloor$  and  $M_2 = \lfloor (d-g-1)/2 \rfloor$ . Note that when  $2|(d-g)$ ,  $\text{ord}_\infty \phi_1(x)x^{M_1} = g + d$  and when  $2 \nmid (d-g)$ ,  $\text{ord}_\infty (y - \phi_2(x))x^{M_2} = g + d$ .

So put  $f_0(x, y) := \begin{cases} \phi_1(x)x^{M_1} & 2|(d-g) \\ (y - \phi_2(x))x^{M_2} & 2 \nmid (d-g) \end{cases}$  and put  $f_i(x, y)$  ( $1 \leq i \leq d-g$ ) by other bases of  $L(D)$  and exceeds the simillar argument of Section 2. Let us denote

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

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

**Lemma 6.** 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  $A_1, \dots, A_{d-g}$  with total degree 2. (Note that  $C_d = 1$  form  $g(x)$  being monic.)

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

Consider the system of the equations

$$EQS_3 : \{S_i(X_1, \dots, X_d) = C_i(A_1, \dots, A_{d-g}) \mid i = 0, 1, \dots, d-1\} \quad (1)$$

**Proposition 4.** Let  $(x_1, \dots, x_d) \in \mathbb{A}^d(\overline{\mathbb{F}_p})$ . The condition that there are some  $P_i = (x_i, y_i)$  ( $i = 1, 2, \dots, d$ ) such that  $D_0 + P_1 + \dots + P_d - d\infty \sim 0$  and  $x(P_i) = x_i$  ( $i = 1, \dots, d$ ) is equivalent to the condition that the equations system  $EQS_3$  of the variables  $\{A_i\}$  and  $\{X_i\}$  has some solution satisfying  $X_i = x_i$ .

Note that the variables  $\{A_i\}$  can be eliminated by the technique of previous section.

## 7 Decomposed factor

In 2009, Diem [2] 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 discovered, Matsuo also found the simillar 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 return the reply and it is not presented and only the researchers around him know 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  $[w_1, \dots, w_n]$  be the base of  $\mathbb{F}_{p^n}/\mathbb{F}_p$ . Let  $n_1, \dots, n_d$  be the positive integers satisfying  $n_1 + \dots + n_d \approx ng$ . Put

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

Let  $r_1, \dots, r_d$  be elements of  $\mathbb{F}_{p^n}$ <sup>3</sup> and take decomposed factor  $B_i$  by

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

and consider the decomposition (of  $D_0$ )

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

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  $O(p^{n_1 + \dots + n_d - ng}) \approx 1$ . 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 5.** *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  $d = ng$ ,  $n_1 = n_2 = \dots = n_d = 1$  and compute the decomposition of given divisor  $D_0$ . 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 ??, in order to find such  $\{x_{i,1}\}$ , it is sufficient to solve the  $2ng$  equations  $F_{j,k} \in \mathbb{F}_p[\{x_{i,1}\}]$  obtained by Weil descent from  $F_j(x_{1,1} w_1 + r_1, \dots, x_{ng,1} w_1 + r_{ng}) = 0$  ( $j = 1, 2, \dots, g$ ). (Note that put  $F_{j,k}$  be the polynomials obtained by  $F_j(x_{1,1} w_1 + r_1, \dots, x_{ng,1} w_1 + r_{ng}) = \sum_{k=1}^n F_{j,k}(x_{1,1}, \dots, x_{ng,1}) w_k$  ). From Proposition ??, 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  $(\text{Const}_1^{ng})^{ng \times \text{Const}_2} = \exp(\text{Const}_3 n^2 g^2) = \exp(N^{2/3+o(1)})$ . 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. D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Springer, 1997.
2. C. Diem, On the discrete logarithm problem in class groups II, preprint, 2011.
3. J-C. Faugère, 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.
4. F.S. Macaulay, The algebraic Theory of modular systems, 1916, Cambridge.
5. 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.
6. 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.

<sup>3</sup> Take  $r_{i+1} \in \mathbb{F}_{p^n} \setminus \cup_{j=1}^i B'_j$  and disjoint decomposed factor is constructed

7. K. Nagao, Equations System coming from Weil descent and subexponential attack for algebraic curve cryptosystem, draft, 2013.
8. C. Petit and J-J. Quisquater. On Polynomial Systems Arising from a Weil Descent, Asiacrypt 2012, Springer LNCS **7658**, Springer, pp.451-466.
9. I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Preprint, 2004.