Equations System coming from Weil descent and subexponential attack for algebraic curve cryptosystem (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.))

Revise 9/8 Lemma 9 of the first version of this manuscript is false and I delete the content of §4 and related footnote. In §4 of the first version, we only showed the existence of many trivial relations, and please note that this revise does not influence our theorems, which state the subexponential complexity of ECDLP/JACDLP under first fall degree assumption.

Abstract. In [2], Faugére et al. shows that the decomposition problem of a point of elliptic curve over binary field $\mathbb{F}_{2^n}$ reduces to solving low degree equations system over $\mathbb{F}_2$ coming from Weil descent. Using this method, the discrete logarithm problem of elliptic curve over $\mathbb{F}_{2^n}$ reduces to linear constrains, i.e., solving equations system using linear algebra of monomial modulo field equations, and its complexity is expected to be subexponential of input size n. However, it is pity that at least using linear constrains, it is exponential. In [7], Petit et al. shows that assuming first fall degree assumption, from which the complexity of solving low degree equations system using Gröbner basis computation is subexponential, its total complexity is heuristically subexponential. On the other hands, the author [6] shows that the decomposition problem of Jacobian of plane curve over $\mathbb{F}_{p^n}$ also essentially reduces to solving low degree equations system over $\mathbb{F}_p$ coming from Weil descent. In this paper, we revise (precise estimation of first fall degree) the results of Petit et al. and show that the discrete logarithm problem of elliptic curve over small characteristic field $\mathbb{F}_{p^n}$ is subexponential of input size n, and the discrete logarithm problem of Jacobian of small genus curve over small characteristic field $\mathbb{F}_{p^n}$ is also subexponential of input size n, under first fall degree assumption.

Keywords Decomposition Attack, ECDLP, first fall degree

1 Notations and Results

Through out of this paper, let p be a small prime number(or power of prime number), n, n', d, $(d, n' \leq n)$, $N = n'd$ be positive integers [1] , $\{w_i\}_{i=1,...,n}$ be a fixed base of $\mathbb{F}_{p^n}/\mathbb{F}_p$, and

$$B := \{\sum_{i=1}^{n'} x_i w_i \,|\, x_i \in \mathbb{F}_p\} (\subset \mathbb{F}_{p^n}).$$

Let $\overrightarrow{X_i}$ $(i = 1, .., d)$ be variables which move in extension field $\mathbb{F}_{p^n}$. $\overrightarrow{X_i}$ are called global variables and a polynomial $\overrightarrow{F} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ is called global polynomial. Let $\{X_{i,j}\}_{i=1,...,d, j=1,...,n'}$ be variables which moves in base field $\mathbb{F}_p$. $\{X_{i,j}\}$ are called local variables and a polynomial $F \in \mathbb{F}_p[\{X_{i,j}\}]$ is called local polynomial. (We sometimes write $\{X_{i,j}\}$ by $\{X_1, ..., X_N\}$ where $N = dn'$ for simplicity.) Since $X_{i,j}$'s are the variables, whose values are in $\mathbb{F}_p$, there is a set of equations

$$S_{fe} := \{X_{i,j}^p - X_{i,j} \,|\, 1 \leq i \leq d, 1 \leq j \leq n'\}$$

called field equations.

[1] In elliptic curve case $N > n$, and in Jacobian case $N > ng$, where g is the genus of the curve, is needed.

For global polynomial $\overrightarrow{F} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$, let $wd(\overrightarrow{F})(\in \mathbb{F}_{p^n}[\{X_{i,j}\}])$ be the polynomial obtained by substituting $\overrightarrow{X_i} := \sum_{j=1}^{n'} X_{i,j} w_j$ $(i = 1, ..., d)$ and decreasing the degrees of $X_{i,j}$'s taking modulo field equations S_{fe} [2] i.e.,

$$wd(\overrightarrow{F}) := \overrightarrow{F}|_{\overrightarrow{X_i} := \sum_{j=1}^{n'} X_{i,j} w_j} \bmod S_{fe}.$$

Let $[\overrightarrow{F}]_k^{\downarrow} (\in \mathbb{F}_p[\{X_{i,j}\}])$ $(k = 1, ..., n)$ be the local polynomials such that

$$wd(\overrightarrow{F}) = \sum_{k=1}^{n} [\overrightarrow{F}]_k^{\downarrow} w_k.$$

We will call $wd(\overrightarrow{F})$, $[\overrightarrow{F}]_k^{\downarrow}$ by Weil descent of $\overrightarrow{F}$.

Let $E/\mathbb{F}_{p^n} : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ be an elliptic curve. From technical reason, we assume that E has no $\mathbb{F}_{p^n}$ rational point at $x = 0$, i.e., the equation $f(0, y) = 0$ has no solution in $\mathbb{F}_{p^n}$, which does not lose the generality. Put decomposed factor

$$DF := \{P \in E(\mathbb{F}_{p^n}) \,|\, x(P) \in B\},$$

where $x(P)$ is the x-coordinate of P, and consider the decomposition problem which states that for arbitrary $P_0 \in E(\mathbb{F}_{p^n})$ finding $P_1, ..., P_d \in DF$ satisfying $P_0 + P_1 + ... + P_d = 0$. From Semaev [8], there is a global polynomial $\overrightarrow{Sem}_{P0}(\overrightarrow{X_1}, ..., \overrightarrow{X_d})$ of degree $< 2^d$ such that $P_0 + P_1 + ... + P_d = 0$ is equivalent to $\overrightarrow{Sem}_{P0}(x(P_1), ..., x(P_d)) = 0$. So the problem reduces to solving local equations system consisting $[\overrightarrow{Sem}_{P_0}]_k^{\downarrow} = 0$ $(k = 1, ..., n)$ and field equations $X_{i,j}^p - X_{i,j} = 0$ $(i = 1, ..., d, j = 1, ..., n')$. From the assumption that E has no $\mathbb{F}_{p^n}$ rational points at $x = 0$, this problem also reduces to solve $[c \cdot \overrightarrow{m} \cdot \overrightarrow{Sem}_{P_0}]_k^{\downarrow} = 0$ $(k = 1, ..., n)$ and field equations $X_{i,j}^p - X_{i,j} = 0$, where c is arbitrary element of $\mathbb{F}_{p^n}^{\times}$ and $\overrightarrow{m} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e_i}$ is arbitrary monomial of $\{\overrightarrow{X_i}\}$ [3]. In this paper, we show that taking $n' = O(n^{2/3})$, $d = O(n^{1/3})$ and the complexity of computing $[\overrightarrow{m_0} \cdot \overrightarrow{Sem}_{P_0}]_k^{\downarrow}$ is $O(exp(n^{2/3+o(1)}))$, where $o(1) \to 0$ when $n \to \infty$. Moreover, if we assume the first fall degree assumption of [7], the complexity of solving local equations system is also $O(exp(n^{2/3+o(1)}))$. So the total cost of solving discrete logarithm of $E(\mathbb{F}_{p^n})$ which consists of DF times decomposition of a point of $E(\mathbb{F}_{p^n})$ and linear algebra computation of $\#DF \times \#DF$ size matrix, is also $O(exp(n^{2/3+o(1)}))$.

Let $C/\mathbb{F}_{p^n} : f(x, y) = 0$ be a plane curve of small constant genus g. Fix $\infty \in C(\mathbb{F}_{p^n})$ be some point of C at $x = \infty$. From technical reason, we assume that C has no $\mathbb{F}_{p^n}$ rational point at $x = 0$, i.e., the equation $f(0, y) = 0$ has no solution in $\mathbb{F}_{p^n}$, which does not lose the generality. [4] Put decomposed factor

$$DF := \{P - \infty \,|P \in C(\mathbb{F}_{p^n}),\, x(P) \in B\}$$

and consider the decomposition problem which states that for arbitrary divisor $D_0 \in Jac(C/\mathbb{F}_{p^n})$ finding $D_1, ..., D_d \in DF$ satisfying $D_0 + D_1 + ... + D_d \sim 0$. From the author [6], there is a set of g global polynomials $\overrightarrow{F_{(D_0)1}}, ..., \overrightarrow{F_{(D_0)g}}$ of degree $< C^d$ (C is some constant)such that this problem reduces to solving local equations system consisting $[\overrightarrow{F_{(D_0)i}}]_j^{\downarrow} = 0$ $(i = 1, ..., g,\ j = 1, ..., n)$ and field equations $X_{i,j}^p - X_{i,j} = 0$ $(i = 1, ..., d, j = 1, ..., n')$. From the assumption that C

[2] For each i, j, $\deg_{X_{i,j}} wd(\overrightarrow{F}) \leq p - 1$.

[3] In order for solving ECDLP in subexponential complexity, we will take $\deg \overrightarrow{m} = O(exp(n^{1/3+o(1)}))$.

[4] From this assumption, solving equations system $[c \cdot \overrightarrow{m} \cdot \overrightarrow{Sem}_{P_0}]_k^{\downarrow} = 0$ $(k = 1, ..., n)$ and field equations, is equivalent condition of finding $P_1, ..., P_d$. Note that if this assumption does not hold, it is only a necessary condition.

has no $\mathbb{F}_{p^n}$ rational points at $x=0$, this problem also reduced to solve $[c\cdot\overrightarrow{m}\cdot\overrightarrow{F_{(D_0)i}}]_j^{\downarrow}=0$ $(i=1,...,g,\ j=1,...,n)$ and field equations $X_{i,j}^p-X_{i,j}=0$, where c is arbitrary element of $\mathbb{F}_{p^n}^{\times}$ and $\overrightarrow{m}=\prod_{i=1}^d\overrightarrow{X_i}^{e_i}$ is arbitrary monomial of $\{\overrightarrow{X_i}\}$. In this paper, we show that taking $n'=O(n^{2/3})$, $d=O(gn^{1/3})=O(n^{1/3})$ and the complexity of computing $[c\cdot\overrightarrow{m}\cdot\overrightarrow{F_{(D_0)i}}]_j^{\downarrow}$ is $O(exp(n^{2/3+o(1)}))$, where $o(1)\to 0$ when $n\to\infty$. Moreover, if we assume first fall degree assumption of [7], the complexity of solving local equations system is also $O(exp(n^{2/3+o(1)}))$. So the total cost of solving discrete logarithm of $Jac(C/\mathbb{F}_{p^n})$ which consists of DF times decomposition of a divisor in $Jac(C/\mathbb{F}_{p^n})$ and linear algebra computation of $\#DF\times\#DF$ size matrix, is also $O(exp(n^{2/3+o(1)}))$.

It must be noted that although its complexity is subexponential, the practical computation, especially in cases of $p>2$ or $g\geq 2$, is difficult and it is only a result of the complexity.

2 First fall degree assumption

Definition 1 (First fall degree [7]). *Let K be a field and let $f_1,...,f_l\in K[X_1,...,X_N]$. first fall degree D_{ff} is the (minimal) positive integer satisfying the following;*
There exists $g_i\in K[X_1,...,X_N]$ $(i=1,...,l)$ such that
1) $\max_{1\leq i\leq l}\deg(g_if_i)=D_{ff}$, 2) $\sum_{i=1}^l g_if_i\neq 0$, 3) $\deg(\sum_{i=1}^l g_if_i)<D_{ff}$, 4) $\deg(f_i)\leq D_{ff}$.

Petit et al. [7] assume the following assumption show the subexponentiality of the discrete logarithm problem of elliptic curve over binary field.

Assumption 1 (First fall degree Assumption) *Upper bound of the degree of the polynomial for computing Gröbner basis of $f_1,...,f_l$ of F4 algorithm is $D_{ff}+O(1)$.*

This assumption has some counter examples and Petit et al. assume that the polynomials $f_1,...,f_l$ are general polynomials. However, if $f_1,...,f_l$ are randomly chosen, the value of D_{ff} seems to be very large. In our situation, we treat only the cases that $D_{ff}\sim\max_i\deg f_i$ and so, $f_1,...,f_l$ cannot be randomly chosen.

For my opinion, if there are many l-ple $(g_1,...,g_l)\in\mathbb{A}^l(K[X_1,...,X_N])$ satisfying the definition of first fall degree, assumption seems to be true. For example, for any $l\times l$ size invertible matrix M, put $\begin{pmatrix}f_1^{(N)}\\ \vdots\\ f_l^{(M)}\end{pmatrix}:=M\begin{pmatrix}f_1\\ \vdots\\ f_l\end{pmatrix}$. Define $D_{ff}(M)$ by minimal integer satisfying the following;
There exists $g_i^{(M)}\in K[X_1,...,X_N]$ $(i=1,...,l)$ such that
1) $\max_{1\leq i\leq l}\deg(g_i^{(M)}f_i^{(M)})=D_{ff}(M)$, 2) $\sum_{i=1}^l g_i^{(M)}f_i^{(M)}\neq 0$, 3) $\deg(\sum_{i=1}^l g_i^{(M)}f_i^{(M)})<D_{ff}$, 4) $\deg(f_i^{(M)})\leq D_{ff}(M)$. Put first fall degree $D_{ff}:=\max_M D_{ff}(M)$. However, by using this new assumption, I can not prove that the equations system coming from Weil descent have low first fall degree in strict way and it remains a future work.

Lemma 1. *Under the Assumption 1, the complexity of computing Gröbner basis of $f_1,...,f_l$ by F4 algorithm is estimated by $\leq O(N^{D_{ff}\cdot C+O(1)})$, when $N\gg D_{ff}$ and where C is some constant ~ 3.*

Proof. The number of the monomials of degree $\leq D_{ff}+O(1)$ is $\begin{pmatrix}D_{ff}+O(1)+N-1\\ D_{ff}+O(1)\end{pmatrix}<N^{D_{ff}+O(1)}$. So, in order to compute Gröbner basis of $f_1,...,f_l$, it is sufficient to compute linear algebra of the matrix of size $N^{D_{ff}+O(1)}\times N^{D_{ff}+O(1)}$. So its complexity is estimated by $\leq O(N^{D_{ff}\cdot C+O(1)})$, where C is linear algebra constant.

In the discussion of [7], the decomposition of arbitrary $\mathbb{F}_{p^n}$ rational point of elliptic curve into d-elements of decomposed factor DF (they treat only binary field $\mathbb{F}_{2^n}$ case and we make

its generalization here), reduces to solving equations system
$[\overrightarrow{f}]_k^{\downarrow} = 0$, $(k = 1, ..., n)$ and field equations $X_{i,j}^p - X_{i,j} = 0$, where $\overrightarrow{f} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ is some global polynomial and $N = dn'$ is an integer $> n$. Moreover they show that there exists heuristically some local polynomials $g, g_1, ..., g_n \in \mathbb{F}_p[\{X_{i,j}\}]$ such that
1) $g \equiv \sum_{i=1}^n g_i [\overrightarrow{f}]_i^{\downarrow} \bmod S_{fe}$,
2) $\deg g_i \leq 1$ $(i = 1, , ..., n)$, and 3) $\deg g \leq \max_i \deg [\overrightarrow{f}]_i^{\downarrow}$.

So, from the definition of first fall degree, the first fall degree of equations system $\{[\overrightarrow{f}]_k^{\downarrow} \in \mathbb{F}_p[\{X_{i,j}\}]_{1 \leq i \leq d, 1 \leq j \leq n'} \,|\, k = 1, ..., n\}$ seems to be $1 + \max_i \deg [\overrightarrow{f}]_i^{\downarrow}$. However, g is only equivalent to $\sum_{i=1}^n g_i [\overrightarrow{f}]_i^{\downarrow}$ modulo field equations. So. it seems to include some gap. However, from the following lemma, we see that it is not a gap and the equations system $\{[\overrightarrow{f}]_k^{\downarrow} \in \mathbb{F}_p[\{X_{i,j}\}]_{1 \leq i \leq d, 1 \leq j \leq n'} \,|\, k = 1, ..., n\} \cup S_{fe}$ heuristically has low first fall degree $\leq 1 + \max_i \deg [\overrightarrow{f}]_i^{\downarrow}$.

Lemma 2. *Let $G_1, ..., G_N \in \mathbb{F}_p[X_1, .., X_N]$ be local polynomials and put $F := \sum_{i=1}^N G_i \cdot (X_i^p - X_i)$ and $D := \deg F$. So, there are some local polynomials $G'_1, ..., G'_N \in \mathbb{F}_p[X_1, .., X_N]$ satisfying $F := \sum_{i=1}^N G'_i \cdot (X_i^p - X_i)$ and $\deg G'_i \leq D - p$ $(i = 1, ..., N)$.*

Proof. Fix some monomial order $>$ satisfying $\prod X_i^{e_i} > \prod X_i^{f_i}$ when $\sum e_i > \sum f_i$. For a local polynomial $H \in \mathbb{F}_p[X_1, ..., X_d]$, let $LM(H)$ (resp. $LM(H)$) be the leading term (resp. leading monomial) of H associated with monomial order $>$. Put

$$\mathcal{G} := \{(G_1, ..., G_N) \in \mathbb{A}^N(\mathbb{F}_p[X_1, ..., X_d]) \,|\, F = \sum_{i=1}^N G_i(X_i^p - X_i)\}.$$

For $G = (G_1, ..., G_N) \in \mathcal{G}$, let $\psi(G)$ be the maximal monomial i.e.,
$\psi(G) \in \{LM(G_1 X_1^p), ..., LM(G_N X_N^p)\}$ and $\psi(G) \geq LM(G_i X_i^p)$ for all $i = 1, ..., N$. Put

$$IND(G) := \{i \,|\, \psi(G) = LM(G_i X_i^p)\}, \quad NUM(G) := \#IND(G).$$

For $G = (G_1, ..., G_N) \in \mathcal{G}$, if $NUM(G) = 1$, there is some $I (\leq N)$ such that $\psi(G) = LM(G_I X_I^p)$ and $\psi(G) > LM(G_i X_i^p)$ for $i \neq I$. So, we have $D = \deg F = \deg \psi(G) \geq p + \deg LM(G_i)$ and $\deg G_i \leq D - p$ $(i = 1, ..., N)$.

Assume $NUM(G) > 1$ and $\deg \psi(G) > D$, and we will construct $G^{new} \in \mathcal{G}$ such that $\psi(G^{new}) < \psi(G)$ and from the induction of $\psi(G)$, we will prove this lemma.

Let $\{I_1, .., I_k\} = IND(G)$. ($k = NUM(G) > 1$ is assumed.) We have easily
1) $X_{I_1}^p | G_{I_i}$ $(2 \leq i \leq k)$,
2) $\sum_{i=1}^k LT(G_{I_i} X_{I_i}^p) = \sum_{i=1}^k LT(G_{I_i} X_{I_i}^p) = 0$ and
3) $(X_{I_i}^p - X_{I_i}) G_{I_i} = (X_{I_i}^p - X_{I_i})(G_{I_i} - LT(G_{I_i}) + \frac{LT(G_{I_i})}{X_{I_1}^{p-1}})$
$$+ \frac{LT(G_{I_i})}{X_{I_1}^p}(X_{I_1}^p - X_{I_1})(X_{I_i}^p - X_{I_i}) \ (i = 1, ..., k).$$

So, put
$G_{I_1}^{new} := G_{I_1} + \sum_{i=2}^k \frac{LT(G_{I_i})}{X_{I_1}^p}(X_{I_i}^p - X_{I_i})$
$G_{I_i}^{new} := G_{I_i} - LT(G_{I_i}) + \frac{LT(G_{I_i})}{X_{I_1}^{p-1}}$ for$(2 \leq i \leq k)$ and
$G_i^{new} := G_i$ for $i \notin IND(G)$.
Then we have
$G^{new} = (G_1^{new}, ..., G_N^{new}) \in \mathcal{G}$ and $LM(G_i^{new}) < \psi(G)$ $(i = 1, ..., N)$. Here, we prove $LM(G_i^{new}) < \psi(G)$ only in the case $i = I_1$. (In other cases, proofs are easy.)

From the definition of $G_{I_1}^{new}$, we have
$G_{I_1}^{new} X_{I_1}^p = G_{I_1} X_{I_1}^p + \sum_{i=2}^k LT(G_{I_i})(X_{I_i}^p - X_{I_i}) = \sum_{i=1}^k LT(G_{I_i}) X_{I_i}^p = 0$. So the term of

the monomial $\psi(G)$ cancels and we have $LT(G_{I_1}^{new}) < LT(G_{I_1}) = \psi(G)$. Similarly we have $LT(G_i^{new}) < \psi(G)$ for all $i = 1, ..., N$. This means $\psi(G^{new}) < \psi(G)$ and the proof is finished.

From this lemma, the first fall degree of the equations system, which consists of the following $n + N$ number equations $\{[\overrightarrow{f}]_k^{\downarrow} \in \mathbb{F}_p[\{X_{i,j}\}]_{1\leq i\leq d, 1\leq j\leq n'} \mid k = 1, ..., n\} \cup S_{fe}$, is heuristically $1 + \max_{1\leq i\leq n} \deg[\overrightarrow{f}]_i^{\downarrow}$. We also remark that when $\deg \overrightarrow{f} \sim exp(n^{1/3+O(1)})$, which is used for solving ECDLP, computation of such G_i' is very difficult and its complexity (using direct computation) seems to be exponential of n, although computation of $wd(\overrightarrow{f})$ is subexponential. [5]

3 Weight Theory and precise estimation of first fall degree

Here, we compute the precise values of the degree of the polynomial $\deg wd(\overrightarrow{F})$ and $[\overrightarrow{F}]_i^{\downarrow}$ $(i = 1, ..., n)$ of a global polynomial $\overrightarrow{F} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ satisfying $\deg \overrightarrow{F} \ll p^{n'-1}$, and show that the equations system coming from Weil descent have strictly low first fall degree. In order to develop the strict argument, instead of computing $wd(\overrightarrow{F})$, we compute $wd(\overrightarrow{m_1}\,\overrightarrow{m_0}\,\overrightarrow{F})$ where $\overrightarrow{m_0}$, $\overrightarrow{m_1}$ are some global monomials such that $\deg(\overrightarrow{m_0}\,\overrightarrow{F})$ is written by the form $p^\alpha - 1$ [6].

Definition 2. *Let $e = \sum_{k=0}^{\lfloor \log_p e\rfloor} e_k p^k$ $(0 \leq e_k \leq p-1)$ be a positive integer $\leq p^{n'-1}$. Put its weight by $wt(e) := \sum_{k=0}^{\lfloor \log_p e\rfloor} e_k$.*
For a global variable $\overrightarrow{X}$ and positive integer e $(\leq p^{n'-1})$, put $wt(\overrightarrow{X}^e) := wt(e)$ and for a global monomial $\overrightarrow{m} = \prod_{i=1}^d \overrightarrow{X_i}^{e_i}$ satisfying $0 \leq e_i \leq p^{n'-1}$, put $wt(\overrightarrow{m}) := \sum_{i=1}^d wt(e_i)$.

Further we assume the following assumption of the choice of the base $\{w_i\}$ of $\mathbb{F}_{p^n}/\mathbb{F}_p$, which does not lose the generality;

Assumption 2 (choice of the base) *$n' \times n'$ size matrix $M := (w_j^{p^{i-1}})_{1\leq i,j\leq n'}$ is invertible.*

Lemma 3. *For a monomial $\overrightarrow{m} = \prod_{i=1}^d \overrightarrow{X_i}^{e_i}$ satisfying $0 \leq e_i \leq p^{n'-1}$, $\deg(wd(\overrightarrow{m})) = \sum_{i=1}^d wt(e_i)$.*

Proof. It is sufficient to show $\deg(wd(\overrightarrow{X_l}^{e_l})) = wt(e_l)$. Let $e_l = \sum_{k=0}^{\lfloor \log_p e_l\rfloor} e_{l,k} p^k$ $(0 \leq e_{l,k} \leq p-1)$ and $\begin{pmatrix} Y_1 \\ \vdots \\ Y_{n'} \end{pmatrix} := M \begin{pmatrix} X_{l,1} \\ \vdots \\ X_{l,n'} \end{pmatrix}$. From $\overrightarrow{X_l} = \sum_{j=1}^{n'} X_{l,j} w_j$, we have $\overrightarrow{X_l}^{p^{i-1}} \equiv \sum_{j=1}^{n'} X_{l,j} w_j^{p^{i-1}} \mod S_{fe} = Y_i$ and $wd(\overrightarrow{X_l}^{e_l}) \equiv \prod_{i=0}^{\lfloor \log_p e_l\rfloor} Y_{i+1}^{e_{l,i}} \mod S_{fe}$. (Here we use the condition $e_l \leq p^{n'-1}$ which is equivalent to $\log_p e_l \leq n'-1$.) So, we have $\deg_{Y_1,...,Y_{n'}} wd(\overrightarrow{X_l}^{e_l}) = wt(e_l)$ and from the invertibility of M, we also get $\deg wd(\overrightarrow{X_l}^{e_l}) = \deg_{X_{l,1},...,X_{l,n'}} wd(\overrightarrow{X_l}^{e_l}) = wt(e_l)$. (Note that assume $wt(e_l) > \deg wd(\overrightarrow{X_l}^{e_l}) = \deg_{X_{l,1},...,X_{l,n'}} wd(\overrightarrow{X_l}^{e_l})$, substituting $X_{l,i} := \sum_{j=1}^{n'} M_{i,j}^{-1} Y_j$ to $wd(\overrightarrow{X_l}^{e_l})$ and we obtains $\deg_{Y_1,...,Y_{n'}} wd(\overrightarrow{X_l}^{e_l}) < wt(e_l)$, which is a contradiction.)

Lemma 4. *For a monomial $\overrightarrow{m} = \prod_{i=1}^d \overrightarrow{X_i}^{e_i}$ satisfying $0 \leq e_i \leq p^{n'-1}$, there is some $c \in \mathbb{F}_{p^n}^\times$ such that $\deg[c\overrightarrow{m}]_j^{\downarrow} = wt(\overrightarrow{m})$ for arbitrary $j = 1, ..., n$.*

[5] G_i' seems to be able to recover using Gröbner basis computation and under the first fall degree assumption, complexity of the computation is subexponential.

[6] Note that if the constant term of $\overrightarrow{F}$ is not zero, solution(s) of $\overrightarrow{m}\,\overrightarrow{F} = 0$ equals to the solution(s) of $\overrightarrow{F} = 0$ and $\overrightarrow{m}\,\overrightarrow{F}$ can be used instead of $\overrightarrow{F}$.

Proof. Let $c_0 \cdot m$ ($c_0 \in \mathbb{F}_{p^n}^{\times}$, $m \in Mon(\{X_{i,j}\})$) be a certain term of $wd(\overrightarrow{m})$ whose degree equals to $\deg wd(\overrightarrow{m})$. Take $c := c_0^{-1} \cdot \sum_{i=1}^{n} w_i$, we have a desired result.

Lemma 5. *Let α be a positive integer. Then $wt(p^\alpha - 1) = (p-1)\alpha$ and for any $x \leq 2p^\alpha - p^{\alpha-1} - 2$ except $x = p^\alpha - 1$, $wt(x) < (p-1)\alpha$.*

Proof. trivial.

Let $\overrightarrow{F} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ be a global polynomial satisfying $\deg \overrightarrow{F} \ll p^{n'-1}$. We fix $\overrightarrow{M}_{max} = \prod_{i=1}^{d} \overrightarrow{X_i}^{E_i} \in Mon(\overrightarrow{F})$ such that $\deg \overrightarrow{M}_{max} \geq \deg \overrightarrow{M}$ for any $M \in Mon(\overrightarrow{F})$. Let $\alpha = \alpha(\overrightarrow{F})$ be a positive integer satisfying $p^\alpha - 1 + \deg \overrightarrow{F} < 2p^\alpha - p^{\alpha-1} - 2 \leq p^{n'-1}$.
From $\deg \overrightarrow{F} \ll p^{n'-1}$, such α can be take in $O(\log_p \deg \overrightarrow{F})$.
Put $H := p^\alpha - p^{\alpha-1} - \deg \overrightarrow{F} - 1 (> 0)$, $D := \sum_{i=1}^{d} E_i$, and $\overrightarrow{m_0} := \prod_{i=1}^{d} \overrightarrow{X_i}^{p^\alpha - 1 - E_i}$.
So from Lemma 3, we have $wt(\overrightarrow{m_0} \cdot \overrightarrow{M}_{max}) = wt(\prod_{i=1}^{d} \overrightarrow{X_i}^{p^\alpha - 1}) = (p-1)d\alpha$. Also let $\overrightarrow{M} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e_i} \in Mon(\overrightarrow{F}) \setminus \{\overrightarrow{M}_{max}\}$, we have $wt(\overrightarrow{m_0} \cdot \overrightarrow{M}) = wt(\prod_{i=1}^{d} \overrightarrow{X_i}^{p^\alpha - 1 + (e_i - E_i)})$ and since
$0 < p^\alpha - 1 + (e_i - E_i) < p^\alpha - 1 + \deg \overrightarrow{F} \leq 2p^\alpha - p^{\alpha-1} - 1$, we have $wt(\overrightarrow{m_0} \cdot \overrightarrow{M}) < (p-1)d\alpha$ form Lemma 5. Thus, from Lemma 4, we obtain the following;

Lemma 6. *Assume $\deg \overrightarrow{F} \ll p^{n'-1}$ and let α be a positive integer satisfying $p^\alpha - 1 + \deg \overrightarrow{F} < 2p^\alpha - p^{\alpha-1} - 2 \leq p^{n'-1}$. Then we have*
1) $\deg wd(\overrightarrow{m_0} \cdot \overrightarrow{F}) = (p-1)d\alpha$.
2) There is some $c_0 \in \mathbb{F}_{p^n}^{\times}$ such that $\deg[c_0 \overrightarrow{m_0} \cdot \overrightarrow{F}]_j^{\downarrow} = (p-1)d\alpha$ for any $j = 1, ..., n$.

Also put $\overrightarrow{m_1} := \prod_{i=1}^{d} \overrightarrow{X_i}^{f_i}$ ($0 \leq f_i \leq H$). let $\overrightarrow{M} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e_i} \in Mon(\overrightarrow{F})\}$, we have $wt(\overrightarrow{m_1}\overrightarrow{m_0} \cdot \overrightarrow{M}) = wt(\prod_{i=1}^{d} \overrightarrow{X_i}^{p^\alpha - 1 + f_i + (e_i - E_i)})$ and since
$0 < p^\alpha - 1 + f_i + (e_i - E_i) \leq p^\alpha - 1 + \deg \overrightarrow{F} + N \leq 2p^\alpha - p^{\alpha-1} - 1$, we have $wt(\overrightarrow{m_1}\overrightarrow{m_0} \cdot \overrightarrow{M}) \leq (p-1)d\alpha$ form Lemma 5. Thus, from Lemma 4, we obtain the following;

Lemma 7. *Assume $\deg \overrightarrow{F} \ll p^{n'-1}$ and let α be a positive integer satisfying $p^\alpha - 1 + \deg \overrightarrow{F} < 2p^\alpha - p^{\alpha-1} - 2 \leq p^{n'-1}$. Then we have*
1) $\deg wd(\overrightarrow{m_1} \cdot \overrightarrow{m_0} \cdot \overrightarrow{F}) \leq (p-1)d\alpha$.
2) For all $c \in \mathbb{F}_{p^n}^{\times}$, $\deg[c \cdot \overrightarrow{m_1} \cdot \overrightarrow{m_0} \cdot \overrightarrow{F}]_j^{\downarrow} \leq (p-1)d\alpha$ for any $j = 1, ..., n$.

Further put $\overrightarrow{F_0} := c_0 \cdot \overrightarrow{m}_0 \cdot \overrightarrow{F}$ and $a_{i,j,k} \in \mathbb{F}_p$ by $w_i w_j = \sum_{k=1}^{n} a_{i,j,k} w_k$.

Lemma 8.

$$[\overrightarrow{m_1} \cdot \overrightarrow{F_0}]_k^{\downarrow} \equiv \sum_{i=1}^{n} [w_i \cdot \overrightarrow{m_1}]_k^{\downarrow} [\overrightarrow{F_0}]_i^{\downarrow} \bmod S_{fe} \qquad (k = 1, ..., n).$$

Proof. From $\sum_{k=1}^{n} [w_i \overrightarrow{m_1}]_k^{\downarrow} w_k = wd(w_i \overrightarrow{m_1}) = \sum_{k=1}^{n} w_i [\overrightarrow{m_1}]_k^{\downarrow} w_k = \sum_{j=1}^{n} [\overrightarrow{m_1}]_j^{\downarrow} w_i w_j$
$= \sum_{k=1}^{n} (\sum_{j=1}^{n} a_{i,j,k} [\overrightarrow{m_1}]_j^{\downarrow}) w_k$, we have $[w_i \overrightarrow{m_1}]_k^{\downarrow} = \sum_{j=1}^{n} a_{i,j,k} [\overrightarrow{m_1}]_j^{\downarrow}$.
On the other hands, we have
$wd(\overrightarrow{m_1} \cdot \overrightarrow{F_0}) \equiv wd(\overrightarrow{m_1}) \times wd(\overrightarrow{F_0}) \bmod S_{fe} = wd(\overrightarrow{m_1}) \times wd(\overrightarrow{F_0}) = \sum_{i=1}^{n} \sum_{j=1}^{n} [\overrightarrow{m_1}]_j^{\downarrow} [\overrightarrow{F_0}]_i^{\downarrow} w_i w_j$
$= \sum_k (\sum_i (\sum_j a_{i,j,k} [\overrightarrow{m_1}]_j^{\downarrow}) [\overrightarrow{F_0}]_i^{\downarrow}) w_k = \sum_k (\sum_i [w_i \overrightarrow{m_1}]_k^{\downarrow} [\overrightarrow{F_0}]_i^{\downarrow}) w_k$.

For arbitrary $I \in [1, .., n]$, since $\overrightarrow{m_1}$ is not constant, and $\deg wd(w_I \overrightarrow{m_1}) \geq 1$, there exists some integer $k(I) \in [1, ..., n]$ such that $\deg[w_I \overrightarrow{m_1}]_{k(I)}^{\downarrow} \geq 1$. So consider the formula obtained from Lemma 8, we have

$$[\overrightarrow{m_1} \overrightarrow{F_0}]_{k(I)}^{\downarrow} \equiv \sum_{i=1}^{n} [w_i \overrightarrow{m_1}]_{k(I)}^{\downarrow} [\overrightarrow{F_0}]_i^{\downarrow} \bmod S_{fe}.$$

From Lemma 6 and Lemma 7, we remember $\deg[\overrightarrow{F_0}]_i^{\downarrow} = (p-1)d\alpha$, $1 \leq \deg[\overrightarrow{m_1}\,\overrightarrow{F_0}]_{k(I)}^{\downarrow} \leq (p-1)d\alpha$, and using Lemma 2, we have the precise estimation of first fall degree;

Proposition 1. *first fall degree of the equations system*

$$\{[\overrightarrow{F_0}]_k^{\downarrow} \mid k = 1, ..., n\} \cup S_{fe}$$

is estimated by $\leq (p-1)d\alpha + 1$. [7]

4 Cost for computing Weil descent

In this section, we estimate the upper bound of the cost for computing $wd(\overrightarrow{f})$, where $\overrightarrow{f} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ is a global polynomial with $n', d \ll \deg \overrightarrow{f} \ll p^{n'-1}$.

Lemma 10. *The number of the monomials of N_1 variables with degree $\leq N_2$ (not consider field equations) is* $\binom{N_1+N_2-1}{N_1-1} = \binom{N_1+N_2-1}{N_2}$

Let I_1 be the number of global monomial $\in Mon(\overrightarrow{f})$. From this lemma and $d \ll \deg \overrightarrow{f}$, I_1 is estimated by $I_1 \leq \binom{\deg \overrightarrow{f} + d - 1}{d} < (\deg \overrightarrow{f})^d$.

Lemma 11. *Let $\overrightarrow{M} \in Mon(\overrightarrow{f})$ and let I_2 be the upper bound of the degree of $wd(\overrightarrow{M})$. Then, $I_2 \leq (p-1)\,d\,(\log_p \deg \overrightarrow{f} + 1)$.*

Proof. Put $\overrightarrow{M} = \prod \overrightarrow{X_i}^{e_i}$. Remark that $e_i \leq \deg \overrightarrow{f}$ and $\log_p e_i \leq \log_p \deg \overrightarrow{f}$, we have $wd(\overrightarrow{M}) = \sum_{i=1}^{d} wt(e_i) \leq (p-1)\,d\,\max_i(\lfloor log_p e_i + 1 \rfloor) \leq (p-1)\,d\,(\deg \overrightarrow{f} + 1)$ where $\lfloor log_p e_i + 1 \rfloor$ is the p-adic digits of e_i.

Let I_3 be the number of local monomials $\in \mathbb{F}[\{X_{i,j}\}]$ with degree $\leq I_2$. From Lemma 10, $I_3 = \binom{I_2 + n'd - 1}{I_2}$ and from $\deg \overrightarrow{f} \ll p^{n'-1}$, we have $I_2 \ll n'd$ and $I_3 \leq (n'd)^{I_2}$.

Let I_4 be the cost of computing $wd(\overrightarrow{f})$. Since $wd(\overrightarrow{f}) = \sum_{\overrightarrow{M} \in Mon(\overrightarrow{f})} wd(\overrightarrow{M})$, $I_4 = I_1 \times$ cost of computing $wd(\overrightarrow{M})$. Since the cost of computing the product of two polynomials with degree $\leq I_2$ is I_3^2 and computation of $wd(\overrightarrow{M})$ which consists of at most I_2 times multiplication of polynomials of degree $\leq I_2$, cost of computing $wd(\overrightarrow{M})$ is estimated by $\leq I_2\, I_3^2$ and the following;

Lemma 12. *Let $\overrightarrow{f} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ be a global polynomial with $n', d \ll \deg \overrightarrow{f} \ll p^{n'-1}$, and let $I_1, ..., I_4$ be the complexities, which appears in the previous sentence. Then $I_4 \leq I_1 \times I_2 \times I_3^2$.*

Further, we estimate the cost of computing discrete logarithm of elliptic curve $E/\mathbb{F}_{p^n}$. In elliptic curve case, we take $d = O(n^{1/3})$, $n' = O(n^{2/3})$ and we try to decompose arbitrary $P_0 \in E(\mathbb{F}_{p^n})$ into d- decomposed factor $\in DF$. So, we must take $\overrightarrow{F} := \overrightarrow{Sem_{P_0}}$ whose degree $< 2^d$. Since $d = O(n^{1/3})$, $\alpha = \alpha(\overrightarrow{F})$ can be taken $\alpha = \log_p 2^d + O(1)$ and $\deg \overrightarrow{F_0} = \deg(c\,\overrightarrow{m_0}\,\overrightarrow{F}) \leq 2p^{\alpha} - p^{\alpha-1} - 2 < 2^{d+O(1)}$ and the condition $n', d \ll \deg \overrightarrow{F_0} \ll p^{n'-1}$ holds. Each complexities are estimated by $I_1 \leq 2^{d^2+O(1)d} = O(exp(n^{2/3+o(1)}))$, $I_2 \leq O(d(d+O(1))) \leq O(n^{2/3+o(1)})$, $I_3 \leq (n'd)^{I_2} = O(exp(n^{2/3+o(1)}))$, and $I_4 \leq I_1 \times I_2 \times I_3^2 = O(exp(n^{2/3+o(1)}))$. On the other hands from Proposition 1, first fall degree of the equation system $\{[\overrightarrow{F_0}]_k^{\downarrow} \mid k = 1, ..., n\} \cup S_{fe}$ is

[7] Note that $\overrightarrow{m_1}$ can be take degree 1 global monomial

$D_{ff} \leq I_2+1$ If we assume the first fall degree assumption 1, from Lemma 1, the cost of solving this equations system also $O(exp(n^{2/3+o(1)}))$. So, the total cost of solving discrete logarithm of $E(\mathbb{F}_{p^n})$, which consists of $\#DF = O(n^{2/3})$ times decompositions and $\#DF \times \#DF$ size linear algebra computations is also $O(exp(n^{2/3+o(1)}))$. Thus we have the following;

Theorem 1. *Under the first fall degree assumption 1, the cost of solving discrete logarithm of $E(\mathbb{F}_{p^n})$ where p is a small prime number (or a power of prime number) is $O(exp(n^{2/3+o(1)}))$ when $n \to \infty$.*

Further, we estimate the cost of computing discrete logarithm of Jacobian of a curve $C/\mathbb{F}_{p^n}$ of small constant genus g. In this case, we also take $d = O(g \cdot n^{1/3}) = O(n^{1/3})$, $n' = O(n^{2/3})$ and we try to decompose arbitrary $D_0 \in Jac(C/\mathbb{F}_{p^n})$ into d- decomposed factor $\in DF$. In the author [6], there is a set of global polynomials $\overrightarrow{F_{D_0,1}}, ..., \overrightarrow{F_{D_0,g}}$ such that $\deg \overrightarrow{F_{D_0,i}} < C^d$ (C:some constant) the decomposition problem reduces to solving equations system $\{[\overrightarrow{F_{D_0,i}}]_j^{\downarrow} | 1 \leq i \leq g, 1 \leq j \leq n\}$ and field equations. By using similar trick, which use $\overrightarrow{m_{i,0}}\,\overrightarrow{F_{D_0,i}}$ instead of $\overrightarrow{F_{D_0,i}}$, there exists some monomials $\overrightarrow{m}_{i,0}$ such that the decomposition problem also reduces to solving equations system $\{[\overrightarrow{m}_{i,0}\,\overrightarrow{F_{D_0,i}}]_j^{\downarrow} | 1 \leq i \leq g, 1 \leq j \leq n\}$ and field equations and its first fall degree can be estimated $\leq O(n^{2/3+O(1)})$. So, we similarly have the following;

Theorem 2. *Under the first fall degree assumption 1, the cost of solving discrete logarithm of $Jac(C/\mathbb{F}_{p^n})$ of small genus g, where p is a small prime number (or a power of prime number), is $O(exp(n^{2/3+o(1)}))$ when $n \to \infty$.*

Acknowledgement The author would like to have great thanks to Professor Kazuto Matsuo in Kanagawa University, to whom the author makes many times fruitful discussions from when the author starts this research and Professor Tsuyoshi Takagi in Kyushu University, who teaches recent trend of researches and points out many mistakes.

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, Decomposition formula of the Jacobian group of plane curve, 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.