Complexity of ECDLP under the First Fall Degree Assumption (Draft)

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

Faculty of Science and Engineering, Kanto Gakuin Univ.,

Abstract. Semaev [14] shows that under the first fall degree assumption, the complexity of ECDLP over $\mathbb{F}_{2^n}$, where n is the input size, is $O(2^{n^{1/2+o(1)}})$. In his manuscript, the cost for solving equations system is $O((nm)^{4w})$, where m $(2 \leq m \leq n)$ is the number of decomposition and $w \sim 2.7$ is the linear algebra constant. It is remarkable that the cost for solving equations system under the first fall degree assumption, is poly in input size n. He uses normal factor base and the revalance of "Probability that the decomposition success" and "size of factor base" is done.
Here, using disjoint factor base to his method, "Probability that the decomposition success becomes ~ 1 and taking the very small size factor base is useful for complexity point of view. Thus we have the result that states
"Under the first fall degree assumption, the cost of ECDLP over $\mathbb{F}_{2^n}$, where n is the input size, is $O(n^{8w+1})$."
Moreover, using the authors results in [11], in the case of the field characteristic ≥ 3, the first fall degree of desired equation system is estimated by $\leq 3p+1$. (In $p = 2$ case, Semaev shows it is ≤ 4. But it is exceptional.) So we have similar result that states
"Under the first fall degree assumption, the cost of ECDLP over $\mathbb{F}_{p^n}$, where n is the input size and (small) p is a constant, is $O(n^{(6p+2)w+1})$. "

1 Notation

Let p be a prime and

$$E/\mathbb{F}_{p^n} : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

be an elliptic curve. Here, we discuss the complexity of ECDLP considering extension degree n being input size.

Problem 1 ((ECDLP)) *Let $P, Q \in E(\mathbb{F}_q)$ such that $< P > \ni Q$. ECDLP is the problem finding integer N satisfying $Q = NP$.*

Petit et al. [12] shows that when $p = 2$ under the first fall degree assumption, it is in $O(n^{2/3+o(1)})$. The author [11] shows this result can be generalized in the case $p \geq 3$. Recently, many researchers [6] [14] propose the method using 3 terms Semaev's formula. In [14], Semaev shows that when $p = 2$ under the first fall degree assumption, it is in $O(n^{1/2+o(1)})$.

Throughout this paper, we fix $\{\alpha_1, ..., \alpha_n\}$ $(\alpha_i \in \mathbb{F}_{p^n})$ by the base of vector space $\mathbb{F}_{p^n}/\mathbb{F}_p$ and put

$$V = V(k) := \{\sum_{i=1}^{k} x_i\alpha_i \,|\, x_i \in \mathbb{F}_p\}$$

by k dimension vector space in $\mathbb{F}_{p^n}$.

2 Semaev's formula

Here, we define the Semaev formula [13] and show its property.

Definition 1. *In the case $p = 2$. Let*

$$E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + Ax^2 + B \qquad (A, B \in \mathbb{F}_{2^n}).$$

Put

$$S_2(x_1, x_2) := x_1 - x_2,$$
$$S_3(x_1, x_2, x_3) := (x_1x_2 + x_1x_3 + x_2x_3)^2 + x_1x_2x_3 + B, \textit{ and}$$
$$S_m(x_1, ., x_m) := Res_x(S_{m-j}(x_1, ..., x_{m-j-1}, x), S_j(x_{m-j}, ..., x_m, x)) \qquad \textit{recursively.}$$

In the case $p \geq 3$. Let

$$E/\mathbb{F}_{p^n} : y^2 = x^3 + A_4x + A_6 \qquad (A_4, A_6 \in \mathbb{F}_{p^n}).$$

Put

$$S_2(x_1, x_2) := x_1 - x_2,$$
$$S_3(x_1, x_2, x_3) := (x_1-x_2)^2x_3^2-2((x_1+x_2)(x_1x_2+A_4)+2A_6)x_3+(x_1x_2-A_4)^2-4A_6x_1x_2, \textit{ and}$$
$$S_m(x_1, ., x_m) := Res_x(S_{m-j}(x_1, ..., x_{m-j-1}, x), S_j(x_{m-j}, ..., x_m, x)) \qquad \textit{recursively.}$$

Proposition 1 (Semaev [13]). *The following two conditions are equivalent;*
1) There exists some $P_1, ..., P_m \in E(\mathbb{F}_{p^n})\backslash\{\infty\}$ such that $P_1 + ... + P_m = 0$.
2) $S_m(x(P_1), ..., x(P_m)) = 0$.

3 Index Calculus of ECDLP

Here, we remember the Index Calculus algorithm of ECDLP [1]. Recall

$$V = \{\sum_{i=1}^{k} x_i\alpha_i \,|\, x_i \in \mathbb{F}_p\}$$

is k dimension vector space in $\mathbb{F}_{p^n}$ and put factor base Fb by

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

In the index calculus, random element $R(\in E(\mathbb{F}_{p^n}))$ is decomposed into m elements in Fb, i.e,. R is decomposed by $R = P_1 + ..., +P_m$ for some $P_i \in Fb$. This process reduces to solving some equations system and if we take parameter k, m as $km \sim n$, the probability that the decomposition success is $1/m!$.

4 Decomposition using S_3

Here, we describe the method for the Decomposition using S_3 ([6], [14]), which decompose $R \in E(\mathbb{F}p^n)$ into m elements $P_1, ..., P_m \in Fb$.

Definition 2 (EQS1). *$EQS1_{(m,R)}$ consists of the $m - 1$ equations*

$$S_3(X_1, X_2, U_1) = 0, S_3(U_1, X_3, U_2) = 0, ..., S_3(U_{m-3}, X_{m-1}, U_{m-2}) = 0, S_3(U_{m-2}, X_m, x(R)) = 0,$$

where variables X_i moves in V and U_i in $\mathbb{F}_{p^n}$.

Algorithm 1 Index Calculus algorithm of ECDLP [1]

Input: $E/\mathbb{F}_{p^n}$ elliptic curve, $P, Q \in E(\mathbb{F}_q)$ st. $< P > \ni Q$
Output: Integer N satisfying $NP = Q$
Set parameter k, m satisfying $km \sim n$
Put $V = \{\sum_{i=1}^{k} x_i\alpha_i \,|\, x_i \in \mathbb{F}_p\}$
Put $Fb := \{P \in E(\mathbb{F}_{p^n}) \,|\, x(P) \in V\}$
Decompose step:$i := 0, \{P_{B1}, ..., P_{B\#Fb}\} := Fb$
while $i \leq \#Fb$ **do**
  $n_1, n_2 \leftarrow$ random integer, Put $R := n_1P + n_2Q$
  if R is written by the sum of m elements in Fb,
  i.e., $R = \sum_{j=1}^{\#Fb} a_jP_{Bj}$ ($a_j = 0$ or $1, \#\{j|a_j = 1\} = m$) **then**
    $i + +$,Put $n_{i,1} := n_1$, $n_{i,2} := n_2$, $a_{i,j} := a_j$ $(j = 1, .., \#Fb)$
Linear algebra step:
for all $i = 1, ..., \#Fb + 1$ **do**
  Put $\overrightarrow{p}_i := (a_{i,1}, ..., a_{i,\#Fb})$
Find $b_1, ..., b_{\#Fb+1} \in \mathbb{Z}/\#E(\mathbb{F}_{p^n})\mathbb{Z}$ st.$\sum_{i=1}^{\#Fb+1} b_i\overrightarrow{p_i} \equiv \overrightarrow{0} \bmod \#E(\mathbb{F}_{p^n})$
Computation of ECDLP:
Return $-\sum_{i=1}^{\#Fb+1} b_in_{i,1} / \sum_{i=1}^{\#Fb+1} b_in_{i,2} \bmod \#E(\mathbb{F}_{p^n})$

In order for solving $EQS1$, we consider its Weil descent. So, for a while, we describe the definition of Weil descent.

Definition 3 (Weil descent). *Let $F = F(X_1, ..., X_N) \in \mathbb{F}_{p^n}[X_1, ..., X_N]$, $\overrightarrow{v} = (v_1, ..., v_N) \in \mathbb{A}^N(\mathbb{F}_{p^n})$ [1] and $j_1, ..., j_N$ be some integers $\leq n$. [2] We describe the set of new variables X_{ij} $(1 \leq i \leq N, 1 \leq j \leq j_i)$. Put the set of field equations by*

$$S_{fe} := \{X_{ij}^p - X_{ij} \,|\, 1 \leq i \leq N, 1 \leq j \leq j_i\}.$$

The polynomials $F_j^{\downarrow} = F_{\overrightarrow{v},j}^{\downarrow}$ $(\in \mathbb{F}_p[\{X_{ij}\}]$, $1 \leq j \leq n)$ is defined as follows; [3]

$$\sum_{j=1}^{n} F_{\overrightarrow{v},j}^{\downarrow} \times \alpha_j = F(v_1 + \sum_{j=1}^{j_1} x_{1j}\alpha_j, ..., v_N + \sum_{j=N}^{j_N} x_{Nj}\alpha_j) \bmod S_{fe}.$$

Definition 4 (EQS2). *$EQS2_{(m,R)}$ is the equations system obtained by Weil descent (taking $v_1 = ... = v_N = 0$) from each equations of $EQS1_{(m,R)}$ and field equations.*
i,e., $EQS2_{(m,R)} := \{F_{\overrightarrow{0},j}^{\downarrow} \,|\, 1 \leq j \leq n,\ F \in EQS1_{(m,R)}\} \cup S_{fe}$.

Remark that $EQS2_{(m,R)}$ consists of $n(m-1)$ variables, $n(m-1)$ degree 4 polynomials (when $p = 2$ degree 3 polynomials can be taken) coming from the Weil descent of S_3 and $n(m-1)$ degree p field equations.

Let $P_1, ..., P_m \in Fb$ such that $P_1 + ... + P_m = R$. Then we see easily $EQS1_{m,R}$ have solution

$$(X_1, ..., U_1, ...) = (x_1, ...u_1, ...) \in \mathbb{A}^{2m-2}(\mathbb{F}_{p^n})$$

such that $x_i = x(P_i)$ $(i = 1, ..., m)$.

[1] Here, we take $\overrightarrow{v} = \overrightarrow{0}$. Latter we will consider disjoint factor base and at this time, the values $v_1, ..., v_N$ must be needed.

[2] Here, $j_1 = ... = j_N = \dim_{\mathbb{F}_p} V = k$.

[3] Strictly saying, we must define $F_j^{\downarrow} = F_{\overrightarrow{v},\overrightarrow{J},j}^{\downarrow}$, where $\overrightarrow{J} = (j_1, ..., J_N)$, since not only $v_1, ..., v_N$, $j_1, ..., j_N$ must be needed in the definition of Weil descent. However, in this paper, $j_1 = ... = j_N = \dim_{\mathbb{F}_p} V = k$ and it is fixed. So we simply omit this term in the definition.

Lemma 1 (Semaev [14]). *Let $x_1, ..., x_m \in V$ and $u_1, ..., u_{m-2} \in \mathbb{F}_{p^n}$. Suppose*

$$(X_1, ..., U_1, ...) = (x_1, ...u_1, ...) \in \mathbb{A}^{2m-2}(\mathbb{F}_{p^n})$$

is a solution of $EQS1_{(m,R)}$. Then we have the following;
1) There exists $P_1, ..., P_m \in E(\mathbb{F}_{2n})$ such that

$$P_1 + .. + P_m = R, x(P_1) = x_1, ..., x(P_m) = x_m.$$

2) Such $P_1, .., P_m$ can be recovered from the solution of $EQS1_{(m,R)}$.
3) Put $S := \{P \mid P \in \{P_1, ..., P_m\} \cap E(\mathbb{F}_{p^n})\}$. So, there exists some 2-torsion $T \in E(\mathbb{F}_{p^n})[2]$ satisfying $\sum_{P \in S} P + T = R$.
(Note $\#S \leq m$. From 1), $T = \infty$ when $\#S = m$.)

From this Lemma, the decomposition of R reduces to solving $EQS1_{(m,R)}$ and solving $EQS2_{(m,R)}$.

Semaev treats the case $km \sim n$ and we will suppose $km \sim n$. Note that $\#FB \sim \#V = p^k$ and the Probability that the element in $E(\mathbb{F}_{p^n})$ is written by the form $P_1 + ... + P_m$ ($P_i \in Fb$) is estimated by

$$\frac{(\#Fb)^m}{m!} \cdot \frac{1}{\#E(\mathbb{F}_{p^n})} \sim \frac{(p^k)^m}{(m!) \cdot p^n} \sim \frac{1}{m!}.$$

On the other hands, Probability that the element in $E(\mathbb{F}_{p^n})$ is written by the form $P_1 + ... + P_t + T$ ($P_i \in Fb$, $t < m$, $T \in E(\mathbb{F}_{p^n})[2] \backslash \{\infty\}$) is estimated by

$$3\frac{(\#Fb)^t}{t!} \cdot \frac{1}{\#E(\mathbb{F}_{p^n})} \sim 3\frac{(p^k)^t}{(t!) \cdot p^n} \sim 3\frac{1}{p^{k(m-t)}t!} \ll \frac{1}{m!}.$$

So the probability that R is written by $R = P_1 + ... + P_t + T$ for some $t (< m)$ and $T \in E(\mathbb{F}_{p^n})[2] \backslash \{\infty\}$ is very small and negligible. Thus, further, we assume that R is written by $R = P_1 + ... + P_m$ ($P_i \in Fb$) and exceed the discussion.

5 First fall degree assumption

Definition 5 (First fall degree). *Let K be a field and $f_1, ..., f_M \in K[X_1, ..., X_N]$. First fall degree of $\{f_1, ..., f_M\}$ is the minimal integer d_F satisfying the following.*
There exists $g_1, ..., g_M \in K[X_1, ..., X_N]$ such that
1) $\max_i\{\deg g_i f_i\} \geq d_F$,
2) $\deg(\sum_{i=1}^{M} g_i f_i) < d_F$,
3) $\sum_{i=1}^{M} g_i f_i \neq 0$.

Under the following assumption, the algorithm for solving ECDLP in sub-exponential complexity are proposed [12], [11], [14].

Assumption 1 *$\{f_1, ..., f_M\}$ Degree of the polynomial appears in the Gröbner basis computation (by F4 algorithm) of $\{f_1, ..., f_M\}$ is $\leq d_F$.*

From this assumption, the number of the monomial appears in the Gröbner basis computation is $\leq O(N^{d_F})$ So, we have the following;

Lemma 2. *The complexity of Gröbner basis computation (by F4 algorithm) of $\{f_1, ..., f_M\}$ is $\leq O(N^{d_F w})$, where $w \sim 2.7$ is the linear algebra constant.*

Many researchers misunderstand the definition of first fall degree and use this assumption and estimation of the complexity using the following FAKE version.

Definition 6 (Fake first fall degree). *Let $f_1, ..., f_M \in \mathbb{F}_p[X_1, ..., X_N]$ and let $S_{fe} := \{X_i^p - X_i \,|\, 1 \le i \le N\}$ be the set of field equations Fake first fall degree of $\{f_1, ..., f_M\} \cup S_{fe}$ is the minimal integer d'_F satisfying the following.*
There exists $g_1, ..., g_M \in K[X_1, ..., X_N]$ such that
1) $\max_i\{\deg g_i f_i \bmod S_{fe}\} \ge d_F$,
2) $\deg(\sum_{i=1}^{M} g_i f_i \bmod S_{fe}) < d_F$,
3) $\sum_{i=1}^{M} g_i f_i \not\equiv 0 \bmod S_{fe}$.

In [14], Semaev says from the equation $S_3(x, u, R_X) = 0$, where $x = \sum_{i=1}^{k} x_i\alpha_i$ $u = \sum_{i=1}^{n} u_i\alpha_i$ and $R_X \in \mathbb{F}_{p^n}$, the relations of low first degree do not appears. Considering $xuS_3(x, u, R_X)$, one can easily have the relation that its Fake first fall degree $d'_F \le 4$. He uses the true definition of first fall degree.

In [11], the author shows the following lemma and it has no problem to use Fake first fall degree instead of use true first fall degree.

Lemma 3 ([11]). *Let $F = F(X_1, ..., X_N)$ be a polynomial in $\mathbb{F}_p[X_1, .., X_N]$ such that $F \equiv 0 \bmod S_{fe}$. i.e., There are $f_1, ..., f_M \in \mathbb{F}_p[X_1, .., X_N]$ such that $F := \sum_{i=1}^{N} f_i \cdot (X_i^p - X_i)$. So, there are some polynomials $f_1^{new}, ..., f_M^{new} \in \mathbb{F}_p[X_1, .., X_N]$ satisfying $F := \sum_{i=1}^{N} f_i^{new} \cdot (X_i^p - X_i)$ and $\deg f_i^{new} \le \deg F - p$ $(i = 1, ..., N)$.*

Example 1 *Let X, Y, Z are variables moves in $\mathbb{F}_2$. Note that the set of field equations is written by $S_{fe} = \{X^2 + X, Y^2 + Y, Z^2 + Z\}$.*
Let $F = (X^2 + X)(Y^2 + Y) + (X^2 + X)(Y^2 + Z) \in \mathbb{F}_2[X, Y, Z]$. From its construction, $F \equiv 0 \bmod S_{fe}$ and expanding the formula, we have $F = X^2Y + Y^2Z + YZ + X^2Z + XY^2 + XZ$ and $\deg F = 3$.
F can be transformed by $F = (X^2 + X)(Y^2 + Y) + (X^2 + X)(Y^2 + Z)$
$= (X^2 + X)(Y^2 + Y) + (X^2 + X)(Y^2 + Y) + (X^2 + X)(Y^2 + Y) + (X^2 + X)(Y^2 + Z)$
$= (X + Z)(Y^2 + Y) + (X^2 + X)(Y + Z)$, and F can be written by the sum of smaller degree polynomials, which are divided by a certain field equation.

Proof of this Lemma is complicated and not constructive.
From this lemma, we have the following:

Lemma 4. *Let $f_1, ..., f_M \in \mathbb{F}_p[X_1, ..., X_N]$. Put d_F by the first fall degree of $\{f_1, ..., f_M\}$ and put d'_F by the Fake first fall degree of $\{f_1, ..., f_M\} \cup S_{fe}$. Then $d_F \le d'_F$.*

Now, we will estimate the first fall degree of $EQS2_{(m,R)}$ in case of $p \ge 3$. For this purpose, we prepare the following

Lemma 5 (Also the author 's result in [11]). *Let $F = F(X_1, ..., X_N)$ be a polynomial in $\mathbb{F}_p[X_1, .., X_N]$ and let $m = m(X_1, ..., X_N)$ be a monomial in $\mathbb{F}_p[X_1, .., X_N]$. Then we have*

$$[m \cdot F]_j^{\downarrow} \equiv \sum_{i=1}^{n} [\alpha_i \cdot m]_j^{\downarrow} \, [F]_i^{\downarrow} \bmod S_{fe} \qquad (j = 1, ..., n).$$

Lemma 6. *Let $F = F(X_1, ..., X_n)$ be a polynomial in $\mathbb{F}_{p^n}[X_1, .., X_n]$. The first fall degree of the equations system $\{F_j^{\downarrow}(\in \mathbb{F}_p[\{X_{ij}\}]) \,|\, 1 \le j \le n\} \cup S_{fe}$ is heuristically $\le (p-1)n + \deg F$.*

Proof. Put $m = m(X_1, ..., X_n) = X_1^{p-1} \cdots X_n^{p-1}$. From Lemma 5, we have

$$[m \cdot F]_j^{\downarrow} \bmod S_{fe} \equiv \sum_{i=1}^{n} [\alpha_i \cdot m]_j^{\downarrow} \, [F]_i^{\downarrow} \bmod S_{fe} \qquad (j = 1, ..., n).$$

From field equation, $\deg([m \cdot F]_j^{\downarrow} \bmod S_{fe})$ is $\le (p-1)n + \deg F - 1$. On the other hands, $\deg[\alpha_i \cdot m]_j^{\downarrow}$ is heuristically $= (p-1)n$ and $\deg[F]_i^{\downarrow}$ is also heuristically $= \deg F$. [4] Thus the

[4] We use heuristic argument only here.

Fake first fall degree of $\{F_j^{\downarrow}(\in \mathbb{F}_p[\{X_{ij}\}]) \,|\, 1 \leq j \leq n\}$ is bounded by $\leq (p-1)n + \deg F$ and from Lemma 4, we have this lemma.

From this proposition, we have the following:

Proposition 2 (Semaev [14] and its generalization to $p \geq 3$). *First fall degree of $EQS2_{(m,R)}$[5] is bounded by*

$$\begin{cases} 4 & (p=2) \\ 3p+1 & (p \geq 3) \end{cases}.$$

From this proposition and Lemma 2, we can estimate the complexity:

Proposition 3 (Semaev [14] and its generalization to $p \geq 3$). *Under the first fall degree assumption, the complexity of solving $EQS2_{(m,R)}$ is bounded by*

$$\begin{cases} O((nm)^{4w}) & (p=2) \\ O((nm)^{(3p+1)w} & (p \geq 3) \end{cases}.$$

6 Complexity estimation by Semaev

Here, we adopt the easy and rough estimation. For this reason, the complexity of input size n is written by the form $O(exp(n^{\alpha+o(1)}))$, where $\lim_{n\to\infty} o(1) = 0$. Many complicated terms are included into the $o(1)$ term and so for normal size input n, $o(1)$ has HUGE value although $\lim_{n\to\infty} o(1) = 0$.

Semaev considers the case $m \sim n^{1/2+o(1)}$ then k is taken $k \sim \frac{n}{m} = n^{1/2+o(1)}$. Then we have

1) $\#Fb \sim p^k = p^{n^{1/2+o(1)}} = O(exp(n^{1/2+o(1)}))$,

2) The probability that decomposition success $= \frac{1}{m!} \sim \frac{1}{O(exp(n^{1/2+o(1)}))}$,

3) The complexity of "Decompose step" $= \frac{\#Fb\times \text{ cost of solving } EQS2}{\text{Probability}} = O(exp(n^{1/2+o(1)}))$

4) The complexity of "linear algebra step" $= (\#FB)^w = O(exp(n^{1/2+o(1)}))$ ($w \sim 2.7$ linear algebra constant).

Thus we have the following;

Proposition 4 (Semaev [14] and its generalization to $p \geq 3$). *Under the first fall degree assumption, the complexity of solving ECDLP for an elliptic curve $E/\mathbb{F}_{p^n}$ is estimated by $O(exp(n^{1/2+o(1)}))$.*

7 Disjoint factor base

The idea of using disjoint factor base is known by [10] and recently re-discovered by [5].

Recall $V = \{\sum_{i=1}^{k} x_i\alpha_i \,|\, x_i \in \mathbb{F}_p\}$ be a dimension k vector space in $\mathbb{F}_{p^n}$ and m, k be the parameter $mk \sim n$.

Let $v_1, ..., v_m$ be elements in $\mathbb{F}_{p^n}$ such that all $V + v_i$ $(i = 1, ..., m)$ are disjoint. Put

$$V_i := V + v_i \qquad (i = 1, ..., m),$$

$$Fb_i := \{P(\in E(\mathbb{F}_{p^n})) \,| x(P) \in V_i\} \qquad (i = 1, ..., m),$$

$$Fb := \cup_{i=1}^{m} FB_i, \text{and}$$

consider the decomposition of $R(\in E(\mathbb{F}_{p^n}))$ by

$$R = P_1 + ... + P_m \qquad (P_i \in Fb_i)$$

and the index calculus whose factor base is Fb.

Note that $\#Fb_i \sim \#V_i = \#V \sim p^k$, $\#Fb \sim m \cdot p^k$.

Using the similar argument in §2, the decomposition reduces to solving the following equations system

[5] Assume $S_{fe} \subseteq EQS2_{(m,R)}$

Definition 7 (EQS3). *$EQS3_{(m,R)}$ consists of the $m-1$ equations*

$$S_3(X_1, X_2, U_1) = 0, S_3(U_1, X_3, U_2) = 0, ..., S_3(U_{m-3}, X_{m-1}, U_{m-2}) = 0, S_3(U_{m-2}, X_m, x(R)) = 0,$$

where variables X_i moves in V_i and U_i in $\mathbb{F}_{p^n}$.

Substituting $X_i = v_i + \sum_{j=1}^{k} X_{ij}\alpha_j$ and $U_i = \sum_{j=1}^{n} X_{(m+i)j}\alpha_j$ to the equations in $EQS3_{(m,R)}$ and the equations in $\mathbb{F}_p[\{X_{ij}\}]$ are obtained from Weil descent process.

Definition 8 (EQS4). *$EQS4_{(m,R)}$ is the equations system obtained by Weil descent from each equations in $EQS3_{(m,R)}$ and field equations.*
i,e., $EQS4_{(m,R)} := \{F^{\downarrow}_{\overrightarrow{v},j} \,|\, 1 \le j \le n,\, F \in EQS3_{(m,R)}\} \cup S_{fe}$ where $\overrightarrow{v} = (v_1, .., v_N)$.

Similarly, solving $EQS3$ reduces to solving $EQS4$ and its complexity is estimated as follows; [6]

Proposition 5. *First fall degree of $EQS4_{(m,R)}$ is bounded by*

$$\begin{cases} 4 & (p=2) \\ 3p+1 & (p \ge 3) \end{cases}.$$

Proposition 6. *Under the first fall degree assumption, the complexity of solving $EQS4_{(m,R)}$ is bounded by*

$$\begin{cases} O((nm)^{4w}) & (p=2) \\ O((nm)^{(3p+1)w}) & (p \ge 3) \end{cases}.$$

The difference between using normal factor base and disjoint factor base is the probability that decomposition success. The number of the elements in $E(\mathbb{F}_{p^n})$ written by the form $P_1 + ... + P_m$ ($P_i \in Fb_i$) is $\prod_{i=1}^{m} \#Fb_i \sim (p^k)^m \sim p^k \sim \#E(\mathbb{F}_{p^n})$. So, the probability that decomposition success, is $O(1)$. On the other hands, the size of all factor base $\cup Fb_i$ became m times large. However, it is not heavy problem.

Now fix $k = C_0$ be a small natural number and put the parameter $m \sim \frac{n}{k} = \frac{n}{C_0}$. Then we have $\prod_{i=1}^{m} \#Fb_i \sim (p^k)^m \sim p^n$. (Note: if one takes $k=1$, it sometimes happens $\#Fb_i = \emptyset$ for some i. To avoid such case and confirm the relation $\prod_{i=1}^{m} \#Fb_i \sim p^n$, we choose suitable constant C_0.) From $m \sim \frac{n}{C_0}$, one has $\#Fb \sim m \cdot p^k = \frac{p^{C_0}}{C_0} \cdot n = O(n)$. So from Lemma 6, since we must collect $\#Fb + 1$ decompositions, the cost of "decompose step" is estimated by

$$\begin{cases} (nm)^{4w} \cdot \frac{p_0^C}{C_0} n = (n\frac{n}{C_0})^{4w} \cdot \frac{p_0^C}{C_0} n = O(n^{8w+1}) & (p=2) \\ (nm)^{(3p+1)w} \cdot \frac{p_0^C}{C_0} n = (n\frac{n}{C_0})^{(3p+1)w} \cdot \frac{p_0^C}{C_0} n = O(n^{(6p+2)w+1}) & (p \ge 3) \end{cases}.$$

The complexity of linear algebra step is $(\#Fb)^w \sim (n \cdot \frac{p^{C_0}}{C_0})^w = O(n^w)$ and very very small. Thus we have the following theorem:

Theorem 1. *Under the first fall degree assumption, the complexity of solving ECDLP for an elliptic curve $E/\mathbb{F}_{p^n}$ is estimated by*

$$\begin{cases} O(n^{8w+1}) & (p=2) \\ O(n^{(6p+2)w+1}) & (p \ge 3) \end{cases}.$$

Acknowledgement I would like to have great thanks to Professor Kazuto Matsuo in Kanagawa University for useful advices and coments.

[6] The situation is the same as the Semaev's case. So, we omit the proof.

Algorithm 2 Index Calculus algorithm of ECDLP using dis joint factor base

Input: $E/\mathbb{F}_{p^n}$ elliptic curve, $P, Q \in E(\mathbb{F}_q)$ st. $< P >\ni Q$
Output: Integer N satisfying $NP = Q$
  Set parameter k, m satisfying $km \sim n$
  Put $V = \{\sum_{i=1}^{k} x_i\alpha_i \,|\, x_i \in \mathbb{F}_p\}$
  Put $v_1, ..., v_m \in \mathbb{F}_{p^n}$ st. $V + v_i$ are disjoint
  Put $V_i := V + v_i$,
  Put $Fb_i := \{P \in E(\mathbb{F}_{p^n}) \,|\, x(P) \in V\}$
  Put $Fb := \cup_{i=1}^{m} Fb_i$
  Decompose step:$i := 0, \{P_{B1}, ..., P_{B\#Fb}\} := Fb$
  while $i \leq \#Fb$ **do**
    $n_1, n_2 \leftarrow$ random integer, Put $R := n_1P + n_2Q$
    if R is written by the sum $P_1 + ... + P_m$ for $P_i \in Fb_i$, **then**
      Put a_j by $R = \sum_{j=1}^{\#Fb} a_jP_{Bj}$ ($a_j = 0$ or 1,$\#\{j|a_j = 1\} = m$)
      $i++$,Put $n_{i,1} := n_1$, $n_{i,2} := n_2$, $a_{i,j} := a_j$ $(j = 1, .., \#Fb)$
  Linear algebra step:
  for all $i = 1, ..., \#Fb + 1$ **do**
    Put $\overrightarrow{p}_i := (a_{i,1}, ..., a_{i,\#Fb})$
  Find $b_1, ..., b_{\#Fb+1} \in \mathbb{Z}/\#E(\mathbb{F}_{p^n})\mathbb{Z}$ st.$\sum_{i=1}^{\#Fb+1} b_i\overrightarrow{p_i} \equiv \overrightarrow{0} \mod \#E(\mathbb{F}_{p^n})$
  Computation of ECDLP:
  Return $-\sum_{i=1}^{\#Fb+1} b_in_{i,1}/\sum_{i=1}^{\#Fb+1} b_in_{i,2} \mod \#E(\mathbb{F}_{p^n})$

References

1. P.Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, *Eurocrypt 2000*, LNCS 1807, Springer-Verlag, 2000, pp. 19–34.
2. J. Ding, J. Buchmann, M. Mohamed, W. Mohamed and R-P Weinmann, MutantXL, `http://www.academia.edu/2863459/Jintai_Ding_Johannes_Buchmann_Mohamed_Saied_Emam_Mohamed`
3. N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Effcient Algorithms for Solving Over defined Systems of Multivariate Polynomial Equations. In Proceedings of International Conference on the Theory and Application of Cryptographic Tech- niques(EUROCRYPT), volume 1807 of Lecture Notes in Computer Science, pages 392–407, Bruges, Belgium, May 2000. Springer.
4. 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.
5. S. Galbraith and S.Gebregiyorgis, Summation polynomial algorithms for elliptic curves in characteristic two, https://eprint.iacr.org/2014/806
6. Y. Huang, C. Petit, N. Shinohara, and T. Takagi, On Generalized First Fall Degree Assumptions, https://eprint.iacr.org/2015/358
7. M. Kosters, NOTES ON SUMMATION POLYNOMIALS, http://arxiv.org/pdf/1503.08001.pdf 2015.
8. 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.
9. 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.
10. K. Nagao, Decomposition formula of the Jacobian group of plane curve, https://eprint.iacr.org/2013/548
11. K. Nagao, Equations System coming from Weil descent and subexponential attack for algebraic curve cryptosystem, https://eprint.iacr.org/2013/549
12. C. Petit and J-J. Quisquater. On Polynomial Systems Arising from a Weil Descent, Asiacrypt 2012, Springer LNCS **7658**, Springer, pp.451-466.
13. I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. https://eprint.iacr.org/2004/031.pdf
14. I. Semaev, New algorithm for the discrete logarithm problem on elliptic curves, https://eprint.iacr.org/2015/310.pdf