Bit Coincidence Mining Algorithm II (Draft)

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

Fac. of Science and Engineering, Kanto Gakuin Univ.,

Abstract. In [14], Petit et al. shows that under the algebraic geometrical assumption named "First Fall degree Assumption", the complexity of ECDLP over binary extension field $\mathbb{F}_{2^n}$ is in $O(exp(n^{2/3+o(1)}))$ where $\lim_{n\to\infty} o(1) = 0$ and there are many generalizations and improvements for the complexity of ECDLP under this assumption [10], [11], [5], [16]. In [13], the author proposes the bit coincidence mining algorithm, which states that under the heuristic assumption of the complexity of xL algorithm, the complexity of ECDLP $E/\mathbb{F}_q$ over arbitrary finite field including prime field, is in $O(exp(n^{1/2+o(1)}))$ where $n \sim \log_2 \# E(\mathbb{F}_q) \sim \log_2 q$. It is the first (heuristic) algorithm for solving ECDLP over prime field in subexponential complexity. In both researches, ECDLP reduces to solving large equations system and from each assumption, the complexity for solving reduced equations system is subexponential (or polynomial) complexity. However, the obtained equations system is too large for solving in practical time and space, they are only the results for the complexity.
xL algorithm [2], is the algorithm for solving quadratic equations system, which consists of n variables and m equations. Here, n and m are considered as parameters. Put $D = D(n, m)$ by the maximal degree of the polynomials, which appears in the computation of solving equations system by xL. Courtois et al. observe and assume the following assumption;
1) There are small integer C_0, such that $D(n, n + C_0)$ is usually in $O(\sqrt{n})$, and the cost for solving equations system is in $O(exp(n^{1/2+0(1)}))$.
However, this observation is optimistic and it must have the following assumption
2) The equations system have small number of the solutions over algebraic closure. [1]
(In this draft we assume the number of the solutions is 0 or 1)
In the previous version's bit coincidence mining algorithm [13], the number of the solutions of the desired equations system over algebraic closure is small and it can be probabilistically controlled to be 1 and the assumption 2) is indirectly true. For my sense, the reason that xL algorithm, which is the beautiful heuristic, is not widely used is that the general equations system over finite field does not satisfy the assumption 2) (there are many solutions over algebraic closure) and is complexity is much larger.
In the previous draft [13], I show that the ECDLP of $E(\mathbb{F}_q)$ reduces to solving equations system consists of $d - 1$ variables and $d + C_0 - 1$ equations where C_0 is an arbitrary positive integer and $d \sim C_0 \times \log_2 q$. So, the complexity for solving ECDLP is in subexponential under the following assumption
a) There are some positive integer C_0 independent from n, such that solving quadratic equations system consists of n variables and $m = n + C_0$ equations (and we must assume the assumption 2)) by xL algorithm, the maximum degree of the polynomials $D = D(n, m)$, appears in this routine is in $O(\sqrt{n})$ in high probability.
Here, we propose the new algorithm that ECDLP of $E(\mathbb{F}_q)$ is essentially reducing to solving equations system consists of $d - 1$ variables and $\frac{b_0}{2}d$ equations where $b_0(\geq 2)$ is an arbitrary positive integer named block size and $d \sim (b_0 - 1)\log_{b_0} q$. Here, we mainly treat the case block size $b_0 = 3$. In this case, ECDLP is essentially reducing to

[1] Generally, the number of the equations m is much larger than the number of the variables n, the number of the solutions seems to be true. However it is not true and the assumption 2) must be needed. For example considering the equations system consists of the union of random quadratic equations

$$p_1(\overrightarrow{X}) = ... = p_{n/2}(\overrightarrow{X}) = 0, \qquad p_i \in \mathbb{F}_2[x_1, ..., x_n]$$

and field equations

$$x_1^2 - x_1 = ... = x_n^2 - x_n = 0$$

where n is even number and $\overrightarrow{X} = (x_1, .., x_n)$. From the probabilistic discussion, the average number of the solution of this equations system is $2^{n/2}$, although the number of the equations is much larger than the number of the variables.

solving equations system consists of about $2\log_3 q$ variables and $3\log_3 q$ equations. So that the desired assumption 1) is always true. Moreover, the number of the solutions (over algebraic closure) of this equations system can be probabilistically controlled to be 1 and the desired assumption 2) is also true.
In the former part of this manuscript, the author states the algorithm for the construction of equations system that ECDLP is reduced and in the latter part of this manuscript, the author state the ideas and devices in order for increasing the number of the equations, which means the obtained equations system is easily solved by xL algorithm.

1 Notation

Let q be a power of prime including prime number and

$$E/\mathbb{F}_q : y^2 + \tilde{a_1}xy + \tilde{a_3}y - x^3 - \tilde{a_2}x^2 - \tilde{a_4}x - \tilde{a_6} = 0$$

be an elliptic curve. We mainly consider the case q being large prime.

For simplicity, we will assume $\#E(\mathbb{F}_q)$ is prime number.

Problem 1 ((ECDLP)) *Let $P, Q \in E(\mathbb{F}_q)$ such that $< P > \ni Q$. ECDLP is the problem finding integer n satisfying $0 = Q + nP$.*

Here, we propose an improved algorithm for solving ECDLP. In this algorithm, for an arbitrary positive integer $b_0 (\geq 2)$, ECDLP of $E(\mathbb{F}_q)$ is, in about $O(1)$ probability, reducing to solving quadratic equations system consists of $(b_0 - 1)l - 1$ variable and $\frac{b_0(b_0-1)}{2}l$ equations, where $l := \lfloor \log_{b_0} \#E(\mathbb{F}_q) \rfloor$. From the heuristics of xL algorithm, the cost for solving this kind of equations system is $O(exp(\#E(\mathbb{F}_q)^{1/2+o(1)}))$ and it is subexponential complexity.

2 $L((d+1)\infty - P_0)$

Let $P_0, P_1, .., P_d$ be the $d+1$ point in $E(\mathbb{F}_q)\backslash\{\infty\}$. In this section, we further fix P_0. Put $(x_i, y_i) := P_i$. Then the space of function field $L((d+1)\infty - P_0)$, which means the set of the elements of function field that has pole only at ∞, the order of the pole at ∞ is $\leq d+1$ and has zero at P_0, is spanned by

$$(x - x_0), (x - x)x, ..., (x - x_0)x^{\lfloor (d-1)/2 \rfloor}, (y - y_0), (y - y_0)x, ..., (y - y_0)x^{\lfloor (d-2)/2 \rfloor}.$$

Then an element of $L((d+1)\infty - P_0)$, whose order of the pole at ∞ is exactly $d+1$, is written by the following;
1) In the case d is odd,

$$\phi_{\overrightarrow{A}}(x, y) := (y - y_0) \sum_{i=1}^{(d-1)/2} A_i x^{i-1} + (x - x_0)(\sum_{i=(d+1)/2}^{d-1} A_i x^{i-(d+1)/2} + x^{(d-1)/2})$$

2) In the case d is even,

$$\phi_{\overrightarrow{A}}(x, y) := (x - x_0) \sum_{i=1}^{d/2} A_i x^{i-1} + (y - y_0)(\sum_{i=d/2+1}^{d-1} A_i x^{i-d/2-1} + x^{d/2-1}).$$

Here, $A_1, ..., A_{d-1}$ are considered as parameter and $\phi_{\overrightarrow{A}}(x, y)$ is considered as an element of $\mathbb{F}_q[A_1, ..., A_{d-1}, x, y]$.

Remember that we here treat the ECDLP of $E(\mathbb{F}_q)$ and find the unknown integer n such that $0 = Q + nP$ for given $P, Q \in E(\mathbb{F}_q)$.

Let $b_0 (\geq 2)$ be a natural number (we mainly concern the case $b_0 = 3$) and put

$$l := \lfloor \log_{b_0} \#(\mathbb{F}_q) \rfloor \sim \log_{b_0} q, \ d := (b_0 - 1)l.$$

Let $r_i \ (i = 1, ..., b_o l)$be random integers and put

$$P_0 := Q, \ P_j := r_j P \ (j = 1, ..., b_0 l).$$

We assume all $P_0, ..., P_{b_0 l}$ are distinct points in $E(\mathbb{F}_q) \backslash \{\infty\}$, otherwise, take another random numbers. Here, we call the sequence of the points

$$\{P_{b_0 k+1}, ..., P_{b_0 k+b_0}\}$$

k-th block where k moves $0 \leq k \leq l-1$. Note that all points $P_1, ..., P_{b_0 l}$ are the disjoint union of the k-th blocks.

Definition 1 (Normal decomposition) *If there exists $l_j \in \{0, 1\}$, $(1 \leq j \leq b_0 l)$ such that for $\forall k \ (0 \leq k \leq l-1)$*

$$\#\{i \,|\, l_{kb_0+i} = 1, 1 \leq i \leq b_0\} = b_0 - 1$$

and P_0 is expressed by the form

$$0 = P_0 + \sum_{j=1}^{b_0 l} l_j P_j,$$

we call P_0 has normal decomposition into $P_1, ..., P_{b_0 l}$.

It means that $-P_0$ is written by the sum of the element of $P_1, ..., P_{b_0 l}$ and from each block, $b_0 - 1$ points are used in this sum. Since the number of the selection of $b_0 - 1$ elements from each block is b_0, the number of the expression

$$\sum_{j=1}^{b_0 l} l_j P_j, \ l_j = \{0, 1\}, \ \#\{i \,|\, l_{kb_0+i} = 1, 1 \leq i \leq b_0\} = b_0 - 1$$

is

$$b_0^l \sim \#E(\mathbb{F}_q).$$

So, we have the following

Lemma 1. *The average number of the normal decomposition and the probability that normal decomposition success is around $O(1)$.*

Put $x_j := x(P_j), y_j := y(P_j) \ (j = 0, ..., b_0 l)$.

Definition 2 (Equations system) *Put*

$$\psi_i := \psi_{i, \overrightarrow{A}} = \phi_{\overrightarrow{A}}(x_i, y_i) (\in \mathbb{F}_q[A_1, ..., A_{d-1}]) \ (i = 1, ..., b_0 l),$$

and consider the equations system

$$EQS1 := \{\psi_{kb_0+i}\psi_{kb_0+j} = 0 \,|\, 0 \leq k \leq l-1, 1 \leq i < j \leq b_0\}$$

We will call ψ_i by the polynomial of point P_i and $EQS1$ consist of the product of two polynomials of the points including the same block. Note that $EQS1$ consists of $\frac{b_0(b_0-1)}{2} l$ quadratic equations.

Suppose that P_0 has normal decomposition. Then there is some element $f(x, y)$ in $L((d+1)\infty - P_0)$ satisfying

$$\text{zero of } f = \{P_0\} \cup \{P_j \,|\, l_j = 1\}.$$

Since P_i's are distinct points, we have

$$\mathrm{div} f = P_0 + \sum_{j=1}^{b_0 l} l_j P_j - (d+1)\infty.$$

Then, we see that there are some $\overrightarrow{a} \in \mathbb{A}^{d-1}(\mathbb{F}_q)$ such that

$$\mathrm{div}\phi_{\overrightarrow{a}}(x,y) = P_0 + \sum_{j=1}^{b_0 l} l_j P_j - (d+1)\infty.$$

For each k-th block $(0 \le k \le l-1)$, the number of the points $P_{b_0 k+i}$ $(1 \le i \le b_0)$ that are zero of $\phi_{\overrightarrow{a}}(x,y)$ is exactly $b_0 - 1$. So, we have

$$\psi_{kb_0+i,\overrightarrow{a}}\psi_{kb_0+j,\overrightarrow{a}} = 0 \, (0 \le k \le l-1, 1 \le i < j \le b_0)$$

and $\overrightarrow{A} = \overrightarrow{a}$ is a solution of $EQS1$.

Conversely, suppose that $EQS1$ has some solution $\overrightarrow{A} = \overrightarrow{a} \in \mathbb{A}^{d-1}(\overline{\mathbb{F}_q})$ over algebraic closure.

Lemma 2. *Let* a_i $(i = 1, ..., b_0)$ *be the number,satisfying* $a_i a_j = 0 (1 \le i < j \le b_0)$. *Then* $\#\{i \,|\, a_i = 0\} \ge b_0 - 1$.

From this lemma, we see that for each k $(0 \le k \le l-1)$,

$$\#\{i \,|\, \psi_{kb_0+i}|_{\overrightarrow{A}=\overrightarrow{a}} = 0\} \ge b_0 - 1.$$

It means that $\phi_{\overrightarrow{a}}(x,y)$ has zero at more than $b_0 - 1$ points in every k-th blocks. Since k varies from 0 to $l-1$, $\phi_{\overrightarrow{a}}(x,y)$ has zero at more than $(b_0-1)l$ points in $P_1, ..., P_{b_0 l}$. However, from the construction of $\phi_{\overrightarrow{A}}(x,y)$ and $P_0, ..., P_{b_0 l}$ being distinct points, $\phi_{\overrightarrow{a}}(x,y)$ has zero at only $(b_0-1)l$ points in $P_1, ..., P_{b_0 l}$ and the zeros of $\phi_{\overrightarrow{a}}(x,y)$ is P_0 and the union of the zeros of the k-th block.

So, put

$$l_i := \begin{cases} 1 & \phi_{\overrightarrow{a}}(x(P_i), y(P_i)) = 0 \\ 0 & \text{otherwise} \end{cases},$$

and from $\phi_{\overrightarrow{a}}(x(P_i), y(P_i)) = \psi_i|_{\overrightarrow{A}=\overrightarrow{a}}$, we have

$$\mathrm{div}\ \phi_{\overrightarrow{a}}(x,y) = P_0 + \sum_{j=1}^{b_0 l} l_j P_j - (d+1)\infty.$$

Moreover, since $P_0, ..., P_{b_0 l}$ are in $E(\mathbb{F}_q)$, we have $\phi_{\overrightarrow{a}}(x,y) \in \mathbb{F}_q[x,y]$ and $\overrightarrow{a} \in \mathbb{A}^{d-1}(\mathbb{F}_q)$. Summarizing this, we have the following theorem

Theorem 1. *1. The following two statements are equivalent:*
a) $EQS1$ *has some solution* $\overrightarrow{a} \in \mathbb{A}^{d-1}(\overline{\mathbb{F}_q})$,
b) P_0 *has normal decomposition.*
2. If $EQS1$ *has a solution* $\overrightarrow{a} \in \mathbb{A}^{d-1}(\overline{\mathbb{F}_q})$, *then* $\overrightarrow{a} \in \mathbb{A}^{d-1}(\mathbb{F}_q)$.

3 Toy example

Here, we compute toy example. Let $E/\mathbb{F}_{727} : y^2 = x^3 + x + 1$. We have $\#E(\mathbb{F}_{727}) = 691$ and it is prime order. Let $P = (5, 191), Q = (100, 161) \in E(\mathbb{F}_{727})$ and we will compute discrete

logarithm n i.e, the integer n such that $0 = nP + Q$.
Let $b_0 = 3$,$l = 6$,$d = 12$ and put $P0 = Q = (100, 161)$,
$P1 = 2P = (5, 191), P2 = 2^2P = (334, 383), P3 = 2^3P = (431, 228)$,
$P4 = 2^4P = (607, 76), P5 = 2^5P = (156, 130), P6 = 2^6P = (525, 55), P7 = 2^7P = (613, 305)$,
$P8 = 2^8P = (647, 58), P9 = 2^9P = (101, 309), P10 = 2^{10}P = (533, 482)$,
$P11 = 2^{11}P = (698, 632), P12 = 2^{12}P = (422, 186), P13 = 2^{13}P = (380, 343)$,
$P14 = 2^{14}P = (391, 200), P15 = 2^{15}P = (489, 219), P16 = 2^{16}P = (233, 692)$,
$P17 = 2^{17}P = (632, 149), P18 = 2^{18}P = (32, 61)$.

We have
$\phi_{\overrightarrow{A}}(X, Y) = 726 * A1 * X + 100 * A1 + 726 * A2 * X^2 + 100 * A2 * X + 726 * A3 * X^3 + 100 * A3 * X^2 + 726 * A4 * X^4 + 100 * A4 * X^3 + 726 * A5 * X^5 + 100 * A5 * X^4 + 726 * A6 * X^6 + 100 * A6 * X^5 + A7 * Y + 566 * A7 + A8 * X * Y + 566 * A8 * X + A9 * X^2 * Y + 566 * A9 * X^2 + A10 * X^3 * Y + 566 * A10 * X^3 + A11 * X^4 * Y + 566 * A11 * X^4 + X^5 * Y + 566 * X^5$
and
$\psi_1 = 95 * A1 + 475 * A2 + 194 * A3 + 243 * A4 + 488 * A5 + 259 * A6 + 30 * A7 + 150 * A8 + 23 * A9 + 115 * A10 + 575 * A11 + 694$
$\psi_2 = 493 * A1 + 360 * A2 + 285 * A3 + 680 * A4 + 296 * A5 + 719 * A6 + 222 * A7 + 721 * A8 + 177 * A9 + 231 * A10 + 92 * A11 + 194$
$\psi_3 = 396 * A1 + 558 * A2 + 588 * A3 + 432 * A4 + 80 * A5 + 311 * A6 + 67 * A7 + 524 * A8 + 474 * A9 + 7 * A10 + 109 * A11 + 451$
$\psi_4 = 220 * A1 + 499 * A2 + 461 * A3 + 659 * A4 + 163 * A5 + 69 * A6 + 642 * A7 + 22 * A8 + 268 * A9 + 555 * A10 + 284 * A11 + 89$
$\psi_5 = 671 * A1 + 715 * A2 + 309 * A3 + 222 * A4 + 463 * A5 + 255 * A6 + 696 * A7 + 253 * A8 + 210 * A9 + 45 * A10 + 477 * A11 + 258$
$\psi_6 = 302 * A1 + 64 * A2 + 158 * A3 + 72 * A4 + 723 * A5 + 81 * A6 + 621 * A7 + 329 * A8 + 426 * A9 + 461 * A10 + 661 * A11 + 246$
$\psi_7 = 214 * A1 + 322 * A2 + 369 * A3 + 100 * A4 + 232 * A5 + 451 * A6 + 144 * A7 + 305 * A8 + 126 * A9 + 176 * A10 + 292 * A11 + 154$
$psi_8 = 180 * A1 + 140 * A2 + 432 * A3 + 336 * A4 + 19 * A5 + 661 * A6 + 624 * A7 + 243 * A8 + 189 * A9 + 147 * A10 + 599 * A11 + 62$
$\psi_9 = 726 * A1 + 626 * A2 + 704 * A3 + 585 * A4 + 198 * A5 + 369 * A6 + 148 * A7 + 408 * A8 + 496 * A9 + 660 * A10 + 503 * A11 + 640$
$\psi_{10} = 294 * A1 + 397 * A2 + 44 * A3 + 188 * A4 + 605 * A5 + 404 * A6 + 321 * A7 + 248 * A8 + 597 * A9 + 502 * A10 + 30 * A11 + 723$
$\psi_{11} = 129 * A1 + 621 * A2 + 166 * A3 + 275 * A4 + 22 * A5 + 89 * A6 + 471 * A7 + 154 * A8 + 623 * A9 + 108 * A10 + 503 * A11 + 680$
$\psi_{12} = 405 * A1 + 65 * A2 + 531 * A3 + 166 * A4 + 260 * A5 + 670 * A6 + 25 * A7 + 372 * A8 + 679 * A9 + 100 * A10 + 34 * A11 + 535$
$\psi_{13} = 447 * A1 + 469 * A2 + 105 * A3 + 642 * A4 + 415 * A5 + 668 * A6 + 182 * A7 + 95 * A8 + 477 * A9 + 237 * A10 + 639 * A11 + 2$
$\psi_{14} = 436 * A1 + 358 * A2 + 394 * A3 + 657 * A4 + 256 * A5 + 497 * A6 + 39 * A7 + 709 * A8 + 232 * A9 + 564 * A10 + 243 * A11 + 503$
$\psi_{15} = 338 * A1 + 253 * A2 + 127 * A3 + 308 * A4 + 123 * A5 + 533 * A6 + 58 * A7 + 9 * A8 + 39 * A9 + 169 * A10 + 490 * A11 + 427$
$\psi_{16} = 594 * A1 + 272 * A2 + 127 * A3 + 511 * A4 + 562 * A5 + 86 * A6 + 531 * A7 + 133 * A8 + 455 * A9 + 600 * A10 + 216 * A11 + 165$
$\psi_{17} = 195 * A1 + 377 * A2 + 535 * A3 + 65 * A4 + 368 * A5 + 663 * A6 + 715 * A7 + 413 * A8 + 23 * A9 + 723 * A10 + 380 * A11 + 250$
$\psi_{18} = 68 * A1 + 722 * A2 + 567 * A3 + 696 * A4 + 462 * A5 + 244 * A6 + 627 * A7 + 435 * A8 + 107 * A9 + 516 * A10 + 518 * A11 + 582$.

$EQS1 = \{\psi_1\psi_2 = 0, \psi_1\psi_3 = 0, \psi_2\psi_3 = 0, \psi_4\psi_5 = 0, \psi_4\psi_6 = 0, \psi_5\psi_6 = 0, \psi_7\psi_8 = 0, \psi_7\psi_9 = 0, \psi_8\psi_9 = 0, \psi_{10}\psi_{11} = 0, \psi_{10}\psi_{12} = 0, \psi_{11}\psi_{12} = 0, \psi_{13}\psi_{14} = 0, \psi_{13}\psi_{15} = 0, \psi_{14}\psi_{15} = 0, \psi_{16}\psi_{17} = 0, \psi_{16}\psi_{18} = 0, \psi_{17}\psi_{18} = 0\}$
has a solution
$(A1, ..., A11) = (378, 2, 521, 58, 79, 503, 526, 681, 302, 82, 535) \in \mathbb{A}^{11}(\mathbb{F}_{727})$
and we can recover
$(l_1, ..., l_{11}) = (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$.
Put

$n := \sum_{i=1}^{11} l_i 2^i \bmod 691 = 234$ and we can check $234P = (100, 566) = -Q$ and discrete logarithm is computed.

4 xL algorithm

First, we try to estimate the complexity for solving this equations system by xL algorithm [2]. In [2], Courtois et al. treat the only case that the equations are of the form "homogeneous quadratic polynomial=constant", but, one can obtain similar results if general quadratic equations are used.

Algorithm 1 xL algorithm [2]

```
  Notation: $K$ field, $X_1, ..., X_n$ variables, $\overrightarrow{X} := (X_1, ..., X_n)$
  $p_i(\overrightarrow{X}) \in K[X_1, ..., X_n]$ $(i = 1, ..., m)$ quadratic polynomials
  $\mathcal{M}_d := \{$All monomials of $X_1, ..., X_n$ degree $\leq d\}$
  Assumption: $n \leq m$
Input: $p_i(\overrightarrow{X})$ $(i = 1, ..., m)$
Output: $\overrightarrow{x} = (x_1, ..., x_n) \in \mathbb{A}^n(K)$ satisfying $p_i(\overrightarrow{x}) = 0$ $(i = 1, ..., m)$
  Set parameter $D = D(n, m)$
  Multiply:
  for all $m(\overrightarrow{X}) \in \mathcal{M}_{D-2},\ p(\overrightarrow{X}) \in \{p_1(\overrightarrow{X}), ..., p_m(\overrightarrow{X})\}$ do
    Genera all products $m(\overrightarrow{X})p(\overrightarrow{X})$
  Linearize: Consider each monomial in $\mathcal{M}_D$ as new variable and perform Gaussian elimination
  on the equations obtained in "Multiply". The ordering on the monomial must be such that all the
  terms containing 1 variable (say $X_1$) are eliminated last
  Solve: Assume that Linearize step yields at least one univariate equation in the powers of $X_1$,
  Solve this equation.
  Repeat: Simplify the equations and repeat the process to find the values of the other variables.
```

In [2], Courtois et al. observed as follows;

When $D = O(\sqrt{n})$ and $m \geq n$, the number of the equations obtained by "Multiply Step" is bigger than $\#\mathcal{M}_D$ and so, xL algorithm seems to be work. However, in the case $m = n$, simulation(maybe computer experiments) shows the D that xL algorithm works well must be 2^n. (Reason is clear, since the equations system have generally 2^n solutions in $\overline{K}$. From this observation, xL algorithm is useful only in the case that "the equations system has only small number of the solutions over algebraic closure".) In the case $m = n + 1$, simulation(maybe computer experiments) shows the D that xL algorithm works well must be n (in stead of $\sqrt{n}$, Reason is not clear). In the case $m = n + C_0$ (C_0 some small value), D that xL algorithm works well can be taken $O(\sqrt{n})$.

In his observation, C_0 is only small number and so, it is hard to formulate. So, we formulate the weaker assumption, which means the number of the equations is much larger than that of variables, by the following Assumption 1;

Assumption 1 *Suppose the given equations system has only small number of solutions over algebraic closure and m is written by $m = \alpha n$ for some constant $\alpha > 1$ which does not depend on n. Then there is positive constant β (which does not depend on n) satisfying the following: Put $D := \beta\sqrt{n}$, and xL algorithm returns the solution(in high probability).*

Assume Assumption 1 and $D := \beta\sqrt{n}$. we have $\#\mathcal{M}_D = \binom{n+D}{D} \preceq n^{\beta\sqrt{n}} = O(exp(n^{1/2+o(1)}))$. (Many terms are absorbed into $o(1)$ term. Then $o(1)$ is Huge, although $\lim_{n\to\infty} o(1) = 0$.) In order for performing xL algorithm, the dominant part is Gaussian elimination of the matrix whose size is about $\#\mathcal{M}_D \times \#\mathcal{M}_D$. Its cost is $(\#\mathcal{M}_D)^w$ where $w \sim 2.7$ is the linear algebra constant and it is also written by $O(exp(n^{1/2+o(1)}))$. Thus we have

Lemma 3. *Assume Assumption 1, the complexity of xL algorithm is estimated by $O(exp(n^{1/2+o(1)}))$.*

Our equations system $EQS1$ has $d-1=(b_0-1)l-1$ variables and $\frac{b_0(b_0-1)}{2}l$ equations. So, when $b_0 \geq 3$, the ratio $m/n > \frac{b_0}{2} \geq 1.5$. Moreover, for all $\alpha(>1, \in \mathbb{R})$, put $b_0 := \lceil 2\alpha \rceil$, the ratio $m/n > \frac{b_0}{2} \geq \alpha$. Also, from Lemma 1 and Theorem 1, we see that the number of the solutions over algebraic closure is small. So, EQS1 satisfies Assumption 1 and we have the following:

Theorem 2. *Under the Assumption 1, the complexity of ECDLP is estimated by* $O(exp((\log \#E(\mathbb{F}_q))^{1/2+o(1)}))$.

5 Rigid algorithm

From the algorithm shown in §2, the following "Restricted ECDLP" can not reduced to the suitable equations system. We will construct the equations system for sloving the "Restricted ECDLP" below. We also assume $\#E(\mathbb{F}_q)$ be prime number for simplicity.

Problem 2 ((Restricted ECDLP)) *Let $P, Q \in E(\mathbb{F}_q)$ such that $< P > \ni Q$ and N be a positive integer. Assume that there is (unknown) unique integer n such that $0 = Q + nP$ and $0 \leq n < N$. Restricted ECDLP is the problem finding integer n satisfying $0 = Q + nP$.*

Remark that if one takes $N = \#E(\mathbb{F}_q)$, it it normal ECDLP.

Also fix $b_0(\geq 2)$ be a positive integer and put $l := \lfloor \log_{b_0} \#E(\mathbb{F}_q) \rfloor$. The restricted ECDLP is divided by the following small restricted ECDLP

$$0 = (Q + i(b_0^l)P) + [n \bmod b_0^l]P \qquad (0 \leq i \leq \lceil \frac{N}{b_0^l} \rceil - 1)$$

and there exists unique I $(0 \leq I \leq \lceil \frac{N}{b_0^l} \rceil - 1)$, such that $0 = (Q + I\lfloor \frac{N}{b_0^l} \rfloor (b_0^l)P) + nP$ $(0 \leq n < b_0^l)$have a solution or both of $0 = Q + nP$ and $0 = (Q + i(b_0^l)P) + nP$ $(0 \leq n < b_0^l)$have solutions.

Exchanging $Q + ib_0^lP$ by Q, we only consider the following ECDLP

Problem 3 ((Restricted ECDLP 2)) *Let $P, Q \in E(\mathbb{F}_q)$ such that $< P > \ni Q$ and b_0, l be a positive integer. Assume that there is (unknown) unique integer n such that $0 = Q + nP$ and $0 \leq n < b_0^l$. Restricted ECDLP is the problem finding integer n satisfying $0 = Q + nP$.*

Here, we consider the b_0-adic expansion of unknown discrete logarithm n.

Definition 1 *Let $\epsilon_{(n)}^{(k)}$ $(0 \leq \epsilon_{(n)}^{(k)} \leq b_0 - 1)$ be the integer satisfying*

$$n = \sum_{k=0}^{l-1} \epsilon_{(n)}^{(k)} b_0^k.$$

For arbitrary k, i $(0 \leq k \leq l-1, 1 \leq i \leq b_0)$, put

$$l_{b_0k+i}^{(n)} := \begin{cases} 1 & \epsilon_{(n)}^{(k)} = i-1 \\ 0 & otherwise \end{cases}.$$

Definition 2 *For arbitrary k, i $(0 \leq k \leq l-1, 1 \leq i \leq b_0)$, put*

$$n_{b_0k+i}^{(1)} := (i-1)b_0^k, \text{ and } P_{b_0k+i}^{(1)} := n_{b_0k+i}^{(1)}P.$$

From the definition, we have the following:

Lemma 4.

$$n = \sum_{j=1}^{b_0 l} l_j^{(n)} n_j^{(1)}.$$

These notations are hard to understand. So, we show small exmple. In the case $b_0 = 3, l = 3$, $n_j^{(1)}$ are written by the following:

$$n_1^{(1)} = 0, n_2^{(1)} = 1, n_3^{(1)} = 2, \text{(0-th block)},$$

$$n_4^{(1)} = 0, n_5^{(1)} = 3, n_6^{(1)} = 6, \text{(1st block)},$$

$$n_7^{(1)} = 0, n_8^{(1)} = 9, n_9^{(1)} = 18, \text{(2nd block)}.$$

If the discrete logarithm $n = 19$, it is written by

$$n = 19 = 1 + 0 * 3 + 2 * 3^2,$$

and

$$\epsilon_{(19)}^{(0)} = 1, \epsilon_{(19)}^{(1)} = 0, \epsilon_{(19)}^{(2)} = 2.$$

Then we have

$$l_1^{(19)} = 0, l_2^{(19)} = 1, l_3^{(19)} = 0, \text{(0-th block)},$$

$$l_4^{(19)} = 1, l_5^{(19)} = 0, l_6^{(19)} = 0, \text{(1st block)},$$

$$l_7^{(19)} = 0, l_8^{(19)} = 0, l_9^{(19)} = 1 \text{(2nd block)}.$$

Thus we have

$$19 = 1 + 0 + 18 = \sum_{j=1}^{9} l_j^{(19)} n_j^{(1)}.$$

Here, we define the decomposition using $P_1^{(1)}, ..., P_{b_0 l}^{(1)}$.

Definition 3 (Reverse decomposition) *If there exists $l_j \in \{0, 1\}$, $(1 \le j \le b_0 l)$ such that for $\forall k$ $(0 \le k \le l - 1)$*

$$\#\{i \,|\, l_{kb_0+i} = 1, 1 \le i \le b_0\} = 1$$

and Q is expressed by the form

$$0 = Q + \sum_{j=1}^{b_0 l} l_j P_j^{(1)},$$

we call Q has reverse decomposition into $P_1^{(1)}, ..., P_{b_0 l}^{(1)}$.

Note this definition is different to the previous manuscript. In the previous manuscript, $\#\{i \,|\, l_{kb_0+i} = 1, 1 \le i \le b_0\}$ is $b_0 - 1$,which is called normal decomposition. But here it is 1.

Remember n $(0 \le n < b_0^l)$ be the discrete logarithm. We have

$$0 = Q + nP = Q + \sum_{k=0}^{l-1} \epsilon_{(n)}^{(k)} b_0^k P = Q + \sum_{k=0}^{l-1} P_{b_0 k + \epsilon_{(k)}^{(n)} + 1}^{(1)} = Q + \sum_{j=1}^{b_0 l} l_j^{(n)} P_j^{(1)}$$

and Q has reverse decomposition into $P_1^{(1)}, ..., P_{b_0 l}^{(1)}$.

Conversely, suppose Q has reverse decomposition $0 = Q + \sum_{j=1}^{b_0 l} l_j P_j^{(1)}$ into $P_1^{(1)}, ..., P_{b_0 l}^{(1)},$. Put $n = \sum_{j=1}^{b_0 l} l_j^{(n)} n_j^{(1)}$ and we have $0 \le n < b_0^l$ and $0 = Q + nP$. Then we have the following:

Lemma 5. *1. The following two statements are equivalent:*
a) There is an integer n satisfying $0 = Q + nP$ and $0 \le n < b_0^l$,
b) Q has reverse decomposition into $P_1^{(1)}, ..., P_{b_0 l}^{(1)}$.

Definition 4 *For arbitrary k, i $(0 \le k \le l-1, 1 \le i \le b_0)$, put*

$$n_{b_0k+i}^{(2)} := n_{b_0k+i}^{(1)} + b_0^k = ib_0^k, P_{b_0k+i}^{(2)} := n_{b_0k+i}^{(2)} P,$$

$$n_{b_0k+i}^{(3)} := n_{b_0k+i}^{(2)} + \begin{cases} 1 & k\text{:}odd \\ 0 & k\text{:}even \end{cases} = ib_0^k + \begin{cases} 1 & k\text{:}odd \\ 0 & k\text{:}even \end{cases}, \text{ and } P_{b_0k+i}^{(3)} := n_{b_0k+i}^{(3)} P.$$

Her, the difference $n_{b_0k+i}^{(2)} - n_{b_0k+i}^{(1)} = b_0^k$ is called 1st jamming term and the difference $n_{b_0k+i}^{(3)} - n_{b_0k+i}^{(2)} = \begin{cases} 1 & k\text{:}odd \\ 0 & k\text{:}even \end{cases}$ is called 2nd jamming term.

Lemma 6. *$\{n_j^{(3)} \,|\, 1 \le j \le b_0 l\}$ are distinct.*

Further, we will assume the following:

Assumption 2 *$\{P_j^{(3)} \,|\, 1 \le j \le b_0 l\}$ are distinct.*

From above Lemma, it is almost true.
Remark We can continue the discussion if we take

$$n_{b_0k+i}^{(3)} := n_{b_0k+i}^{(2)} + n(k)$$

where $n(k)$ is some integer dependent on k. In this manuscript, we simply take $n(k) := \begin{cases} 1 & k\text{:odd} \\ 0 & k\text{:even} \end{cases}$. Generally, 2nd jamming term can be taken by this $n(k)$.

From this Remark, if there are some $0 \le k_1 < k_2 \le l-1$ and $1 \le i_1, i_2 \le b_0$ satisfying $P_{b_0k_1+i_1}^{(3)} = P_{b_0k_2+i_2}^{(3)}$ exchanging 2nd jamming term, and the Assumption2 holds. Otherwise in the case, if there are some $0 \le k_1 \le l-1$ and $1 \le i_1 < i_2 \le b_0$ satisfying $P_{b_0k_1+i_1}^{(3)} = P_{b_0k_1+i_2}^{(3)}$ and $P_{b_0k_1+i_1}^{(2)} = P_{b_0k_1+i_2}^{(2)}$. So we have $(b_0^{k_1})(i_2 - i_1)P = 0$. In this case ECDLP is very special and one can easily solve ECDLP.

Definition 5 *Put*

$$J_1 := \sum_{k=0}^{l-1} b_0^k = \frac{b_0^l - 1}{b_0 - 1}$$

by the $\frac{1}{b_0}$ times of the total sum of 1st jamming term and put

$$J_2 := (b_0 - 1)\lfloor \frac{l}{2} \rfloor$$

by the $\frac{b_0 - 1}{b_0}$ times of the total sum of 2nd jamming term. Also put

$$M_1 := \sum_{k=0}^{l-1} \sum_{i=1}^{b_0} ib_0^k = \frac{(b_0^l - 1)b_0(b_0 + 1)}{2(b_0 - 1)}$$

by the total sum of $n_{b_0k+i}^{(3)}$.

Suppose Q has normal decomposition $0 = Q + \sum_{j=1}^{b_0 l} l_j P_j^{(1)}$. Then we have

$$0 = Q + \sum_{j=1}^{b_0 l} l_j P_j^{(1)} = Q - J_1 P + \sum_{j=1}^{b_0 l} l_j P_j^{(2)} = Q - J_1 P + M_1 P + \sum_{j=1}^{b_0 l} (l_j - 1) P_j^{(2)}.$$

Put

$$l'_j = 1 - l_j \in \{0, 1\}$$

and we have each k $(0 \leq k \leq l-1)$ block, we have

$$\#\{i \,|\, l'_{b_0 k+i} = 1, 1 \leq i \leq b_0\} = b_0 - 1 \text{ and} \#\{i \,|\, l'_{b_0 k+i} = 0, 1 \leq i \leq b_0\} = 1.$$

Return to the formulation of the formula, we have

$$0 = -Q + J_1 P - M_1 P + \sum_{j=1}^{b_0 l} (1 - l_j) P_j^{(2)} = -Q + J_1 P - M_1 P - J_2 P + \sum_{j=1}^{b_0 l} (1 - l_j) P_j^{(3)}$$

$$= -Q + (J_1 - J_2 - M_1) P + \sum_{j=1}^{b_0 l} l'_j P_j^{(3)}.$$

So, put

$$P_0 := -Q(J_1 - J_2 - M_1) P, r_j := n_j^{(3)}, P_j := P_j^{(3)} \quad (j = 1, ..., b_0 l),$$

the algorithm in §2 is available. i.e., P_0 has normal decomposition into $P_1, ..., P_{b_0 l}$. Put

$$\psi_i := \psi_{i, \overrightarrow{A}} = \phi_{\overrightarrow{A}}(x(P_i), y(P_i)) (\in \mathbb{F}_q[A_1, ..., A_{d-1}]) \ (i = 1, ..., b_0 l),$$

and consider the equations system

$$EQS1 := \{\psi_{kb_0+i} \psi_{kb_0+j} = 0 \,|\, 0 \leq k \leq l-1, 1 \leq i < j \leq b_0\}.$$

Note that $EQS1$ consists of $\frac{b_0(b_0-1)}{2} l$ quadratic equations and $(b_0 - 1)l - 1$ variables and the restricted ECDLP is reducing to solving this equations system. Also put

$$l'_i := \begin{cases} 1 & \phi_{\overrightarrow{a}}(x(P_i), y(P_i)) = 0 \\ 0 & \text{otherwise} \end{cases},$$

then we have a normal decomposition

$$0 = P_0 + \sum_{j=1}^{b_0 l} l'_j P_j,$$

and ECDLP is recovered by

$$n = \sum_{0 \leq k \leq l-1, 1 \leq i \leq b_0} (1 - l'_{kb_0+i}) \{(i-1) b_0^k\}.$$

Similarly we have the following

Theorem 3. *Under the assumption 1, the complexity of solving restricted ECDLP is*

$$exp((\log N)^{1/2+o(1)}).$$

6 Toy example

Here, we compute toy example. Let $E/\mathbb{F}_{1073741789} : y^2 = x^3+x+109$. We have $\#E(\mathbb{F}_{1073741789}) = 1073734999$ and it is prime order. Let $P = (1, 143901150), Q = -700P = (647703549, 245552865) \in E(\mathbb{F}_{1073741789})$ and we will recover discrete logarithm $n = 700$ i.e, $0 = 700P + Q$.
Let $b_0 = 3$,$l = 6$,$d = 12$ and put $P0 := -Q - (2184 + 6 - 364) * P = (226088430, 436478206)$
$P1 := P = (1, 143901150)$
$P2 := 2 * P = (299873831, 928636621)$
$P3 := 3 * P = (503128344, 969239414)$
$P4 := 4 * P = (767039651, 913339816)$
$P5 := 7 * P = (1002246095, 733782485)$
$P6 := 10 * P = (733179341, 52798551$
$P7 := 9 * P = (901739418, 109858882)$
$P8 := 18 * P = (73367306, 298975683)$
$P9 := 27 * P = (866076745, 131780578)$
$P10 := 18 * P = (978711160, 864620715)$
$P11 := 55 * P = (923735979, 1039609632)$
$P12 := 82 * P = (279349632, 577287516)$
$P13 := 81 * P = (480576973, 493449251)$
$P14 := 162 * P = (418886202, 729929637)$
$P15 := 243 * P = (570168111, 424873673)$
$P16 := 244 * P = (1019714204, 50723728)$
$P17 := 487 * P = (241092407, 504678284)$
$P18 := 730 * P = (333788268, 386257268)$

We have
$\phi_{\overrightarrow{A}}(X, Y) == 1073741788 * A1 * XX + 226088430 * A1 + 1073741788 * A2 * XX^2 + 226088430 * A2 * XX + 1073741788 * A3 * XX^3 + 226088430 * A3 * XX^2 + 1073741788 * A4 * XX^4 + 226088430 * A4 * XX^3 + 1073741788 * A5 * XX^5 + 226088430 * A5 * XX^4 + 1073741788 * A6 * XX^6 + 226088430 * A6 * XX^5 + A7 * YY + 637263583 * A7 + A8 * XX * YY + 637263583 * A8 * XX + A9 * XX^2 * YY + 637263583 * A9 * XX^2 + A10 * XX^3 * YY + 637263583 * A10 * XX^3 + A11 * XX^4 * YY + 637263583 * A11 * XX^4 + XX^5 * YY + 637263583 * XX^5$
and
$\psi_1 = 226088429 * A1 + 226088429 * A2 + 226088429 * A3 + 226088429 * A4 + 226088429 * A5 + 226088429 * A6 + 781164733 * A7 + 781164733 * A8 + 781164733 * A9 + 781164733 * A10 + 781164733 * A11 + 781164733$
$\psi_2 = 999956388 * A1 + 560865895 * A2 + 968576376 * A3 + 477394866 * A4 + 252235669 * A5 + 413913084 * A6 + 492158415 * A7 + 571481171 * A8 + 551121029 * A9 + 823268001 * A10 + 501594843 * A11 + 349808028$
$\psi_3 = 796701875 * A1 + 766405831 * A2 + 1027132502 * A3 + 716438354 * A4 + 447015914 * A5 + 521745128 * A6 + 532761208 * A7 + 505005988 * A8 + 870485541 * A9 + 269259172 * A10 + 708628250 * A11 + 533404740$
$\psi_4 = 532790568 * A1 + 953692135 * A2 + 208625061 * A3 + 573614824 * A4 + 177893183 * A5 + 203868720 * A6 + 476861610 * A7 + 63004931 * A8 + 608571849 * A9 + 313556486 * A10 + 667535215 * A11 + 1036244402$
$\psi_5 = 297584124 * A1 + 700624089 * A2 + 537562339 * A3 + 841317366 * A4 + 460515561 * A5 + 357738131 * A6 + 297304279 * A7 + 308615293 * A8 + 141226927 * A9 + 586580448 * A10 + 797428242 * A11 + 163126219$
$\psi_6 = 566650878 * A1 + 233980350 * A2 + 2349552 * A3 + 380208128 * A4 + 1015854050 * A5 + 156987499 * A6 + 690062134 * A7 + 477240871 * A8 + 676367821 * A9 + 766705898 * A10 + 92471318 * A11 + 906744953$
$\psi_7 = 398090801 * A1 + 557621334 * A2 + 966407363 * A3 + 102032405 * A4 + 41149805 * A5 + 254997820 * A6 + 747122465 * A7 + 313058754 * A8 + 319254209 * A9 + 260839876 * A10 + 538121333 * A11 + 146610434$
$\psi_8 = 152721124 * A1 + 277054419 * A2 + 39055253 * A3 + 1023309119 * A4 + 777639824 * A5 + 247204648 * A6 + 936239266 * A7 + 973986002 * A8 + 736020831 * A9 + 465924531 * A10 + 150306321 * A11 + 81608701$
$\psi_9 = 433753474 * A1 + 985435165 * A2 + 241055825 * A3 + 195248984 * A4 + 548549445 * A5 + 589380119 * A6 + 769044161 * A7 + 1045275912 * A8 + 291960878 * A9 + 637760874 * A10 +$

$201328562 * A11 + 1048602103$
$\psi_{10} = 321119059 * A1 + 283376342 * A2 + 232981203 * A3 + 338231614 * A4 + 790848784 * A5 + 474139666 * A6 + 428142509 * A7 + 359853650 * A8 + 346610100 * A9 + 818740049 * A10 + 107537958 * A11 + 1037457469$
$\psi_{11} = 376094240 * A1 + 926778644 * A2 + 75958860 * A3 + 518509838 * A4 + 426098264 * A5 + 653389532 * A6 + 603131426 * A7 + 907074846 * A8 + 601153885 * A9 + 902541026 * A10 + 483429797 * A11 + 525478439$
$\psi_{12} = 1020480587 * A1 + 267964645 * A2 + 975226971 * A3 + 132890043 * A4 + 499781944 * A5 + 30456621 * A6 + 140809310 * A7 + 655421731 * A8 + 166756042 * A9 + 496439397 * A10 + 574421574 * A11 + 563373482$
$\psi_{13} = 819253246 * A1 + 371332294 * A2 + 168284383 * A3 + 271746380 * A4 + 751211904 * A5 + 349890385 * A6 + 56971045 * A7 + 917952990 * A8 + 803045277 * A9 + 31302661 * A10 + 857977353 * A11 + 49709379$
$\psi_{14} = 880944017 * A1 + 403877358 * A2 + 444527849 * A3 + 363063687 * A4 + 4095602 * A5 + 895956652 * A6 + 293451431 * A7 + 829411202 * A8 + 990876149 * A9 + 651368586 * A10 + 36129035 * A11 + 750028193$
$\psi_{15} = 729662108 * A1 + 660951032 * A2 + 215502507 * A3 + 328959790 * A4 + 273153836 * A5 + 521132947 * A6 + 1062137256 * A7 + 756861618 * A8 + 721088906 * A9 + 816140550 * A10 + 56542021 * A11 + 41073575$
$\psi_{16} = 280116015 * A1 + 347477506 * A2 + 741089275 * A3 + 578494533 * A4 + 271590481 * A5 + 607687676 * A6 + 687987311 * A7 + 1037696180 * A8 + 983997075 * A9 + 809799124 * A10 + 457325577 * A11 + 92657733$
$\psi_{17} = 1058737812 * A1 + 963328085 * A2 + 122041552 * A3 + 548247200 * A4 + 82872780 * A5 + 847566113 * A6 + 68200078 * A7 + 488790147 * A8 + 71164651 * A9 + 307239508 * A10 + 107966160 * A11 + 67581091$
$\psi_{18} = 966041951 * A1 + 351552123 * A2 + 831558009 * A3 + 1041096055 * A4 + 309522466 * A5 + 1047068892 * A6 + 1023520851 * A7 + 260751606 * A8 + 82001771 * A9 + 430269312 * A10 + 42277896 * A11 + 543975617$

$EQS1 = \{\psi_1\psi_2 = 0, \psi_1\psi_3 = 0, \psi_2\psi_3 = 0, \psi_4\psi_5 = 0, \psi_4\psi_6 = 0, \psi_5\psi_6 = 0, \psi_7\psi_8 = 0, \psi_7\psi_9 = 0, \psi_8\psi_9 = 0, \psi_{10}\psi_{11} = 0, \psi_{10}\psi_{12} = 0, \psi_{11}\psi_{12} = 0, \psi_{13}\psi_{14} = 0, \psi_{13}\psi_{15} = 0, \psi_{14}\psi_{15} = 0, \psi_{16}\psi_{17} = 0, \psi_{16}\psi_{18} = 0, \psi_{17}\psi_{18} = 0\}$
has a solution

$(A1, ..., A11) = (1052610325, 1027299158, 204711428, 665478999, 576105216, 887736260, 977723279, 634207409, 151915098, 706654193, 1065506101)$
and we can recover

$(l'_1, ..., l'_{18}) = (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0).$
Put [2]

$$n := \sum_{j=1}^{18}(1 - l'_j)n_j^{(1)} = \sum_{k=0}^{5}\sum_{i=1}^{3}(1 - l'_{3k+i})(i - 1)b_0^k = \sum_{k=0}^{5}\sum_{i=2}^{3}(1 - l'_{3k+i})(i - 1)b_0^k$$

$= (1 - l'_2) * 1 + (1 - l'_3) * 2 + (1 - l'_5) * 3 + (1 - l'_6) * 6 + (1 - l'_8) * 9 + (1 - l'_9) * 18 + (1 - l'_{11}) * 27 + (1 - l'_{12}) * 54 + (1 - l'_{14}) * 81 + (1 - l'_{15}) * 162 + (1 - l'_{17}) * 243 + (1 - l'_{18}) * 486 = 700.$
and we can check $-700P = Q$ and discrete logarithm is computed.

7 Loss of the equation

Here, we show the following theorem:

Theorem 4. *Let $EQS1$ is the equations system of the ECDLP of $E(\mathbb{F}_q)$. Remember that $b_0(\geq 2)$, $l \sim \log_{b_0} \#E(\mathbb{F}_q)$, $d := (b_0 - 1)l$ be fixed integers and $P_0, ..., P_{b_0 l}$ are some points in $E(\mathbb{F}_q)$. Also remember that the polynomials $\psi_i(\in \mathbb{F}_q[A_1, ..., A_{d-1}], i = 1, ..., b_0 l)$ are defined and the equations system $EQS1$ is defined by*

$$\{\psi_{kb_0+i}\psi_{kb_0+j} = 0 \,|\, 0 \leq k \leq l - 1, 1 \leq i < j \leq b_0\}.$$

[2] From the term $(i - 1)$, the term of $i = 1$ is erasing

Here, let

$$EQS1' := EQS1 \backslash \{\psi_1\psi_2 = 0\}.$$

Then, $EQS1'$ have more than b_0^{l-1} solutions.

Proof. For arbitrary k-th ($1 \leq k \leq l-1$) block $\{P_{b_0k+i} \,|\, 1 \leq i \leq b_0\}$, , we select $b_0 - 1$ elements $\{P_{b_0k+I_j} \,|\, 1 \leq j \leq b_0 - 1\}$. Note that the number of the selections is b_0^{l-1}. For 0-th block, we select, $b_0 - 2$ elements $P_3, ..., P_{b_0}$.

Put

$$R := -P_0 - \sum_{i=3}^{b_0} P_i - \sum_{1\leq k\leq l-1, 1\leq j\leq b_0-1} P_{b_0k+I_j}.$$

Then there exists some $f(x,y) \in L((d+1)\infty - P_0)$ such that

$$\text{div } f(x,y) = R + P_0 + \sum_{i=3}^{b_0} P_i + \sum_{1\leq k\leq l-1, 1\leq j\leq b_0-1} P_{b_0k+I_j} - (d-1)\infty.$$

Thus, there exists some $\overrightarrow{a} = (a_1, ..., a_{d-1}) \in \mathbb{A}^{d-1}(\mathbb{F}_q)$ such that $f(x,y) = \phi_{\overrightarrow{a}}(x,y)$. On the other hand, $\psi_i = \phi_{\overrightarrow{A}}(x(P_i), y(P_i))$, we have $\psi_i|_{\overrightarrow{A}=\overrightarrow{a}} = f(x(P_i), y(P_i))$. So, from the construction of $EQS1'$, $\overrightarrow{a} = (a_1, ..., a_{d-1}) \in \mathbb{A}^{d-1}(\mathbb{F}_q)$ is a solution of $EQS1'$.

This theorem says that although the average number of the solution of $EQS1$ is controlled to be 1, if one equation is dropped, the number of the solutions is very large. In the following, to avoid this situation, we proposed two devices and ideas and increasing the number of the equations.

8 Inter block equations system

Here, we state the devices to adding some equations to $EQS1$ named "Inter block equations system". This devices is mainly useful in the case $b_0 \geq 3$ and we assume in this section $b_0 \geq 3$. Moreover, we assume that the $EQS1$ has only one solution for simplicity. First, we consider the normal decomposition of P_0

$$0 = P_0 + \sum_{j=1}^{b_0 l} l_j P_j,\ l_j \in \{0,1\},\ \#\{i \,|\, l_{kb_0+i} = 1, 1 \leq i \leq b_0\} = b_0 - 1$$

Let n_0 be positive integer and consider the n_0 equations $f_1 = f_2 = ... = f_{n_0} = 0$ where each f_I is random polynomials of the form

$$\psi_{k_1b_0+i_1}\psi_{k_2b_0+i_2} \quad (0 \leq k_1 < k_2 \leq l-1, 1 \leq i_1, i_2 \leq b_0)$$

and consider the new equations system

$$EQS2 := EQS1 \cup \{f_1 = 0, ..., f_{n_0} = 0\}.$$

Note that $\psi_{k_1b_0+i_1}\psi_{k_2b_0+i_2}$ is the product of two polynomials of the points in the different block. Let $\overrightarrow{a} = (a_1, ..., a_{d-1}) \in \mathbb{A}^{d-1}(\mathbb{F}_q)$ be the unique (unknown) solution of $EQS1$. From the construction, in each k-th ($0 \leq k \leq l-1$) block, there exists some I_k ($1 \leq I_k \leq b_0$) such that

$$\psi_{kb_0+I_k}|_{\overrightarrow{A}=\overrightarrow{a}} \neq 0, \qquad \psi_{kb_0+i}|_{\overrightarrow{A}=\overrightarrow{a}} = 0 \text{ for } i \in \{1, ..., b_0\}\backslash\{I_k\}.$$

Then, for each i ($1 \leq i \leq n_0$), the probability $f_i|_{\overrightarrow{A}=\overrightarrow{a}} = 0$ is $1 - \frac{1}{b_0^2}$ and the probability $f_1|_{\overrightarrow{A}=\overrightarrow{a}} = ...f_{n_0}|_{\overrightarrow{A}=\overrightarrow{a}} = 0$ is $(1 - \frac{1}{b_0^2})^{n_0}$. Since $\lim_{n\to\infty}(1 - \frac{1}{n})^n = \frac{1}{e} \sim 0.367879$ and in the case $n = 9$, $(1 - \frac{1}{9})^9 \sim 0.346439$ and this value is near to $\frac{1}{e}$, we have

$$(1 - \frac{1}{b_0^2})^{n_0} = (1 - \frac{1}{b_0^2})^{b_0^2 \cdot \frac{n_0}{b_0^2}} \sim (\frac{1}{e})^{\frac{n_0}{b_0^2}} \sim (0.367879)^{\frac{n_0}{b_0^2}}.$$

The we have that the probability that $EQS2$ has a solution is around $(0.367879)^{\frac{n_0}{b_0^2}}$.

For example, take $n_0 := b_0^2 \times 10$ (resp. $n_0 := b_0^2 \times 5$), the probability is around $\frac{1}{22026}$ (resp. $\frac{1}{148}$ and trying to 22026 (resp. 148) times solving $ESQ2$, we can recover ECDLP. In the case $b_0 = 3$, adding $n_0 = 90$ equations to $EQS1$, we can recover ECDLP in $\frac{1}{22026}$ probability and by 22026 times solving EQS2, ECDLP can be recovered.

9 Mirroring equations system

Here, we state the devices to adding some equations to $EQS1$ named "Mirroring equations system". The new equations system obtained by this devices has n_1 times variables of $EQS1$. However, if many many equations are lost from this equations system, the original solution can be recovered. We also assume that the original equations system $EQS1$ has only one solution for simplicity. First, we consider the normal decomposition of $P_0 = P_0^{(0)}$ into $P_1^{(0)}, ..., P_{b_0 l}^{(0)}$,

$$0 = P_0^{(0)} + \sum_{j=1}^{b_0 l} l_j P_j^{(0)},\ l_j \in \{0, 1\},\ \#\{i \,|\, l_{kb_0+i} = 1, 1 \leq i \leq b_0\} = b_0 - 1$$

and $\psi_i^{(0)} \in \mathbb{F}_q[A_1^{(0)}, ..., A_{d-1}^{(0)}]$ be the polynomial of the point $P_i^{(0)}$. Original equations system $EQS1 = EQS1^{(0)}$ is made by

$$\{\psi_{kb_0+i}^{(0)}, \psi_{kb_0+j}^{(0)} = 0 \,|\, 0 \leq k \leq l-1, 1 \leq i < j \leq b_0\}.$$

Let $n_1 (\geq 2)$ be the positive integer and $\alpha_m (1 \leq m \leq n_1 - 1)$ be the random integers co-prime to $\#E(\mathbb{F}_q)$. Put

$$P_i^{(m)} := \alpha_m P_i \qquad (1 \leq m \leq n_1 - 1, 0 \leq i \leq b_0 l)$$

and consider the normal decomposition named mirroring normal decomposition

$$0 = P_0^{(m)} + \sum_{j=1}^{b_0 l} l_j P_j^{(m)},\ l_j \in \{0, 1\},\ \#\{i \,|\, l_{kb_0+i} = 1, 1 \leq i \leq b_0\} = b_0 - 1$$

and $\psi_i^{(m)} \in \mathbb{F}_q[A_1^{(m)}, ..., A_{d-1}^{(m)}]$ be the polynomial of the point $P_i^{(m)}$. Mirroring equations system $EQS1^{(m)}$ is made by

$$\{\psi_{kb_0+i}^{(m)} \psi_{kb_0+j}^{(m)} = 0 \,|\, 0 \leq k \leq l-1, 1 \leq i < j \leq b_0\}.$$

From the construction and the assumption that $EQS1^{(0)}$ has unique solution, $EQS^{(m)}$ has unique solution. Let $\overrightarrow{a}^{(m)} = (a_0^{(m)}, ..., a_{d-1}^{(0)}) \in \mathbb{A}^{d-1}(\mathbb{F}_q)$ be the unique solution of $EQS1^{(m)}$ and put

$$\overrightarrow{a}_{\text{all}} := (a_0^{(0)}, ..., a_{d-1}^{(n_1-1)}) \in \mathbb{A}^{n_1(d-1)}(\mathbb{F}_q).$$

Lemma 7. *We have the relation that*

$$\psi_i^{(m_1)}|_{\overrightarrow{A}^{(m_1)} = \overrightarrow{a}^{(m_1)}} = 0 \Leftrightarrow \psi_i^{(m_2)}|_{\overrightarrow{A}^{(m_2)} = \overrightarrow{a}^{(m_2)}} = 0$$

for any $0 \leq m_1, m_2, \leq n_1 - 1, 1 \leq i \leq b_0 l$.

Definition 6 (Mirroring equations system) *Put*

$$ESQ3 := \{\psi_{kb_0+i_1}^{(m_1)} \psi_{kb_0+i_2}^{(m_2)} = 0 \,|\, 0 \leq k \leq l-1, 1 \leq i_1 < i_2 \leq b_0, 0 \leq m_1, m_2 \leq n_1 - 1\}.$$

From Lemma 7, we have the following

Lemma 8. *$ESQ3$ has a unique solution $\overrightarrow{a}_{all} \in \mathbb{A}^{d-1}(\mathbb{F}_q)$.*

Also from Lemma 7, we have the following

Lemma 9. *Let M $(0 \leq M \leq n_1 - 1)$ be a integer. Put*

$$ESQ3^{(M)} := \{\psi^{(m_1)}_{kb_0+i_1}\psi^{(M)}_{kb_0+i_2} = 0 \,|\, 0 \leq k \leq l-1, 1 \leq i_1 < i_2 \leq b_0, 0 \leq m_1 \leq n_1 - 1\}.$$

Note that $EQS3^{(M)}$ is a subset of $EQS3$. Although the number of the equations is very smaller, $ESQ3^{(M)}$ has a unique solution $\overrightarrow{a}_{all} \in \mathbb{A}^{d-1}(\mathbb{F}_q)$.

Postscript In this mamuscripts, the author gives the improvements of Bit Coincidence Mining Algorithm, which state that if the xL algorithm works well, the complexity of solving DLP of elliptic curve over arbitrary finite field is sub-exponential. However, from my recent research in this summer vacation, xL algorithm may not works well.

References

1. 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`
2. N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Effcient Algorithms for Solving Overdefined 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.
3. 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.
4. S. Galbraith and S.Gebregiyorgis, Summation polynomial algorithms for elliptic curves in characteristic two, https://eprint.iacr.org/2014/806
5. Y. Huang, C. Petit, N. Shinohara, and T. Takagi, On Generalized First Fall Degree Assumptions, https://eprint.iacr.org/2015/358
6. M. Kosters, S.L. Yeo, NOTES ON SUMMATION POLYNOMIALS, http://arxiv.org/pdf/1503.08001.pdf 2015.
7. 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.
8. 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.
9. K. Nagao, Decomposition formula of the Jacobian group of plane curve, https://eprint.iacr.org/2013/548
10. K. Nagao, Equations System coming from Weil descent and subexponential attack for algebraic curve cryptosystem, https://eprint.iacr.org/2013/549
11. K. Nagao, Complexity of ECDLP under the First Fall Degree Assumption, https://eprint.iacr.org/2015/984
12. K. Nagao, Polynomial time reduction from 3SAT to solving low first fall degree multivariable cubic equations system, https://eprint.iacr.org/2015/985
13. K. Nagao, Bit Coincidence Mining Algorithm, https://eprint.iacr.org/2015/986
14. C. Petit and J-J. Quisquater. On Polynomial Systems Arising from a Weil Descent, Asiacrypt 2012, Springer LNCS **7658**, Springer, pp.451-466.
15. I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. https://eprint.iacr.org/2004/031.pdf
16. I. Semaev, New algorithm for the discrete logarithm problem on elliptic curves, https://eprint.iacr.org/2015/310.pdf