Implementation analysis of index calculus method on elliptic curves over prime finite fields

Abstract—**In 2016,Petit et al. first studied the implementation of the index calculus method on elliptic curves in prime finite fields, and in 2018, Momonari and Kudo et al. improved algorithm of Petit et al. This paper analyzes the research results of Petit, Momonari and Kudo, and points out the existing problems of the algorithm. Therefore, with the help of sum polynomial function and index calculus, a pseudo-index calculus algorithm for elliptic curves discrete logarithm problem over prime finite fields is proposed, and its correctness is analyzed and verified. It is pointed out that there is no subexponential time method for solving discrete logarithms on elliptic curves in the finite fields of prime numbers, or at least in the present research background, there is no method for solving discrete logarithms in subexponential time.**

Keywords—discrete logarithm, decomposition base,smooth boundary, factorization, prime finite fields

I. INTRODUCTION

In public key cryptosystems, the elliptic curve discrete logarithm problem (ECDLP) is one of the most difficult mathematical problems to solve [1].The index calculus (IC) method solves the integer decomposition and discrete logarithm problem On finite fields in subexponential time or even polynomial time [2-8], and has been favored because it is not restricted by the group structure. However, on cryptosystems based on elliptic curve prime finite fields, even with smaller key spaces (except for super singular, distorted and anomalous curves) [9, 10], they have not been subjected to great security attacks, although scholars have proposed many similar attacks on finite fields, such as baby-step giant-step algorithm algorithms, Pohlig-Hellman evolution class algorithms, Pollard-Á probabilistic class algorithms, and IC probability class algorithms [10], but with little success.

In 2004, Semaev [11] introduced the summation polynomial S associated with elliptic curves and gave a method to collect ECDLP relations by constructing a system of S equations. Based on this method, scholars have achieved great success in finite domains, especially binary domains [12-17].In 2016, Petit [1] et al. for the first time extended the IC method on binary curves to elliptic curves in prime finite domains, i.e., the IC method was used to solve the problem of discrete logarithms of elliptic curves on base-p prime domains.In 2016. Galbraith [18] et al. reviewed the progress of elliptic curve discrete logarithm solving.In 2018, Amadori [19] et al. proposed a new IC variant for solving any real example of ECDLP, and in the same year, Kudo [20] et al. improved the work of Amadori et al. However, neither Petit's nor Amadori et al.'s work gave concrete examples and the algorithms could not be implemented efficiently. To this end, we analyze the limitations of the IC method for attacking elliptic curve cryptosystems over prime finite fields, show that the IC method cannot pose a threat to elliptic curve cryptosystems over prime finite fields, and verify the validity of the conclusions with examples.

The rest of the paper is organized as follows. Section 2 describes the concepts of elliptic curve cryptosystems. Section 3 presents the work of Petit and Amadori et al. Section 4 analyzes the limitations of the IC method to attack elliptic curve cryptosystems over prime finite fields. Section 5, proposes a pseudo-IC method for attacking elliptic curve discrete logarithms over prime finite fields, and verifies the correctness of the method with concrete examples. Section 6 summarizes our results and gives an outlook on the possible paths of attacking elliptic curve cryptosystems using the pseudo-IC method over prime finite fields.

II. RELATED CONCEPTS AND PROPERTIES

A. Elliptic Curve over a Prime Finite Fields

Let $p > 3$ be a large prime number, F_p represents a prime finite fields, and the elliptic curve E is an equation of the form $y^2 = x^3 + Ax + B$, where $A, B \in F_p$ and $\Delta = 16(4A^3 + 27B^2) \neq 0$, and the points $(x, y) \in F_p \times F_p$ is a solution of the equation $y^2 = x^3 + Ax + B$. On $E(F_p)$ represents the set of points on the elliptic curve *E* that satisfy the solution of the equation $y^2 = x^3 + Ax + B$, including the point *O* at infinity. The "+" operation on the curve *E* is defined as follows:

$$(x, y) + O = O + (x, y) = (x, y) \tag{1}$$

$$(x, y) + (x, -y) = O \tag{2}$$

If $y \neq 0$,Let $\lambda = \dfrac{3x^2 + A}{2y}$, then $(x_3, y_3) = 2(x, y)$

Where

$$x_3 = \lambda^2 - 2x, y_3 = \lambda(x - x_3) - y \tag{3}$$

If $x_1 \neq x_2$,Let $\mu = \dfrac{y_2 - y_1}{x_2 - x_1}$, then $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$

Where

$$x_3 = \mu^2 - x_1 - x_2, y_3 = \mu(x_1 - x_3) - y_1 \quad (4)$$

Thus, $(E(F_p), +)$ represents an Abelian group with the unit *O* at infinity. Suppose $N = \#E(F_p)$ is the order of an elliptic curve *E*,by the Hasse theorem known $|p+1-N| \le 2\sqrt{p}$, $N = p+1-t$, t is elliptic curve *E* trace, $|t| \le 2\sqrt{p}$. When $p \mid t$, the elliptic curve *E* is called a hypersingular curve. When $t = 1$, the elliptic curve *E* is called a deformed elliptic curve or an abnormal elliptic curve. When $t = 2$, the elliptic curve *E* is also unsafe[10].

Assuming that $P, Q \in E(F_p)$, $Q = kP \in < P >$,that is, Q is generated by P , and solving *k* is called solving the discrete logarithm of an elliptic curve *E*.

The points on the elliptic curve *E* have symmetry, that is, both the points on the elliptic curve E and its inverses are on the elliptic curve *E*, and the points and their inverses are symmetric with the *x* axis. Whether the point addition operation or the multiplication operation on the elliptic curve *E*, the result is a point, that is, we can only see the value of the horizontal and vertical coordinates of the point, and can not see the relationship between the operation method before the point and the point from the coordinate value of the point. Also, as in finite fields, elements can not be decomposed into products of prime powers. Therefore, for elliptic curves, the multiples of any point and generator cannot be obtained by decomposition, but only by forward operations (point addition or multiplication).

B. Semae Sum Polynomial

The sum polynomial S_r associated with the elliptic curve *E* is defined as[20] :

$$S_2(x_1, x_2) = x_1 - x_2 .$$

$$S_3(x_1, x_2, x_3) = ((x_1 - x_2)x_3)^2 - 2[(x_1 + x_2)(x_1 x_2 + A) + 2B]x_3 + [(x_1 x_2 - A)^2 - 4B(x_1 + x_2)] .$$

For $r \ge 4$, the r th sum polynomial S_r is defined as:

$$Res_x(S_{r-j}(x_1, x_2, \cdots, x_{r-j-1}, x), S_{j+2}(x_{r-j}, x_{r-j-1}, \cdots, x_r, x))$$

For $1 \le j \le r-3$, Res_x represents a result about the variable x .

For any $r \ge 3$, and the sum polynomial S_r is symmetric, and the degree of each variable x_i is 2^{r-2} .Furthermore, the sum polynomial S_r are absolutely irreducible.

The essence of the sum polynomial S_r is to construct (or select) R-order points through the transverse values of points on the elliptic curve *E*. The assumption $P_1 = (x_1, y_1) \in E(F_p)$, $P_2 = (x_2, y_2) \in E(F_p)$, to $P_r = (x_r, y_r) \in E(F_p)$, then $P_1 + P_2 + \cdots + P_r = O$. When $r = 2$, the sum polynomial S_2 consists of the abscissa of any element and its inverse, $x_1 = x_2$;When $r = 3$, the sum polynomial S_3 consists of the sum of any two elements and the horizontal coordinate of the inverse of their sum. Construct sum polynomial S_r by analogy. Obviously, it is correct to construct sum polynomial functions in terms of order.

III. PETIT AND MOMONARI , KUDO ET AL.'S STUDY

A. Petit et al. 's Approach

Let $M = \{P_1, P_2, \cdots, P_r\}$, which is called the factor basis, obviously $M \subseteq E(F_p)$.The IC algorithm on elliptic curves is divided into three stages.In the first stage, parameters satisfying the condition of $a_i P + b_i Q + \sum e_{ij} P_j = O$ are collected and saved. In the second stage, linear algebraic operations are performed on the relation found in the first stage, that is, solving the linear equation, and a relation of the form $aP + bQ = O$ is derived, from which the discrete logarithm $k = -\frac{a}{b} (\mathrm{mod}\, N)$ can be easily derived.

They define the sum polynomial functions S_r such as equation (5) or equation (6).

$$\begin{cases} S_{r+1}(x_{1,1}, x_{2,1}, \cdots, x_{r,1}, x) \\ x_{i,j} = x_{i,j-1}^q, i = 1,2,\cdots,r; j = 2,3,\cdots,n' \\ \sum_{j=0}^{n'} c_i x_{i,j} = 0, i = 1,2,\cdots,r \end{cases} \quad (5)$$

Or

$$\begin{cases} S_{r+1}(x_{1,1}, x_{2,1}, \cdots, x_{r,1}, x) \\ x_{i,j} = x_{i,j-1}^q - \alpha_{j-1} x_{i,j}, i = 1,2,\cdots,r; j = 2,3,\cdots,n' \\ 0 = x_{i,n'}^q - \alpha_{n'} x_{i,n'}, i = 1,2,\cdots,r \end{cases} \quad (6)$$

On equation (5) or equation (6),the working finite fields is F_{q^n} , where *n* is the embedding degree of the finite fields F_q . $n' \approx \left[\frac{n}{m}\right]$. $L(x) = \prod (x - v) = \sum_{n'} C_j x^{q^j}$, $C_j \in F_{q^n}$,

$v \in V$ .V is the vector space of a point on the horizontal coordinate of an elliptic curve *E*. See Algorithm 1 for IC implementation of the elliptic curves over finite fields of prime numbers.

Algorithm 1.IC algorithm for elliptic curves over finite fields of prime numbers

Input : E, p, P, Q

Output: k

1.Fix *r*.

2.Find a suitable mapping *L* and its decomposition $L = O_{j=1}^{n'} L_j$.

3.Define a factor base $M = \{(x, y) \in E(F_p) \mid L(x) = 0\}$.

4.The relationship between calculation degree $L+\Delta$ is as follows:

a. Randomly select $a, b \in F_p$ and calculate $(x, y) = aP + bQ$.

b. Construct and solve the system

$$\begin{cases} S_{r+1}(x_{1,1}, x_{2,1}, \cdots, x_{r,1}, x) \\ x_{i,j+1} = L_j(x_{i,j}), i = 1,2,\cdots,r; j = 2,3,\cdots,n'\text{-}1 \\ 0 = L_{n'}(x_{i,n'}), i = 1,2,\cdots,r \end{cases}$$

(If L is a relational map, put their denominators on the left-hand side to get a polynomial system)

c.For any solution found (modular symmetry, i.e., permutation of $x_{i,1}$), this relationship is saved if $P_i = (x_i, y_i) \in M$ exists such that $\sum P_i = O$.

5. Using linear algebra to solve discrete logarithm, output k.

B. Momonari, Kudo et al. 's Approach

The research of Momonari, Kudo et al. is based on the research of Petit et al., and only optimizes the construction of the sum polynomial function S_r. The idea and structure of the algorithm are the same as that of algorithm 1. Let's look at their optimized and polynomial function S_r.

First construct a function $f(x) = \prod (x - v) \in F_p[x]$, $V \subseteq F_p$, $x \in V$. Secondly, the sum polynomial S_r is defined, and the specific definition is shown in equations (7) and (8).

$$\begin{cases} S_r(x_1, x_2, \cdots, x_r) \\ f(x_1) = 0 \\ f(x_2) = 0 \\ \vdots \\ f(x_r) = 0 \end{cases} \tag{7}$$

$$\begin{cases} S_r'(t_1, t_2, z) = (t_1^2 - 4t_2)z^2 - 2(t_1 t_2 + At_1 + \\ 2B)z + (t_2 - A)^2 - 4Bt_1 = 0 \\ g_+(t_1, t_2) = f(x_1) + f(x_2) = \prod_{v \in V} (x_1 - v) + \\ \prod_{v \in V} (x_2 - v) = x_1^t + x_2^t - \sum_{v \in V} (x_1^{t-1} + x_2^{t-1}) + \\ \cdots = 0 \\ g_\times(t_1, t_2) = f(x_1, x_2) = \prod_{v \in V} (x_1 - v)(x_2 - v) = 0 \end{cases} \tag{8}$$

Where $t_1 = x_1 + x_2$, $t_2 = x_1 x_2$, $t = |V|$.

They analyze and optimize the sum polynomial function S_r . But they do not give how to construct the sum polynomial function when the number of variables is greater than 3

IV. ALGORITHM ANALYSIS

A. Algorithm 1 Analysis

From the implementation steps of algorithm 1, the set $M = \{P_1, P_2, \cdots, P_r\}$ is known, but the set *M* on the finite fields needs to be constructed, that is, *r+d* relations need to be selected, so as to find The value of the discrete logarithm of the first r prime numbers in *M*. In addition, there are a large number of smooth numbers on the finite fields (that is, all the prime factors of the decomposition product of these numbers are in *M*), this feature is the premise of IC algorithm implementation, and it has not been found on the finite fields of elliptic curve prime numbers with similar characteristics, therefore, algorithm 1 is clearly not a real application of the IC method to solve discrete logarithms on elliptic curves *E*. Furthermore, if *M* is known, it is not easy to randomly select two integers $a_i, b_i \in Z$ to satisfy the relationship of the equation $a_i P + b_i Q + \sum e_{ij} P_j = O$ .If we can easily find a relationship such as $a_i P + b_i Q + \sum e_{ij} P_j = O$, then algorithm 1 is meaningless. Because if we obtain the relation $a_i P + b_i Q + \sum e_{ij} P_j = O$, then $k = -\left(\sum_{P_j} e_{ij} + a_i \right) / b_i \pmod N$, that is, k can be solved directly without solving a system of linear equations.

In addition, the reference [1] limited domain for F_{q^n}, $n' \approx \lceil n/m \rceil$. Assuming that if $n=1$, $m \geq 1$, then $n'=1$, $j=1$, in *algorithm 1* 4.b), *j* is 2, 3,...,n', suggesting that the conditions of the algorithm 1 is not correct. If allowed to $j=1$,then $L_1(x_{i,1}) = C_0 x_{i,1} + C_1 x_{i,1}^q = 0$, $x_{i,2} = L_1(x_{i,1})$, now watch *m* = 3,

$$L_1(x_{1,1}) = C_0 x_{1,1} + C_1 x_{1,1}^q = 0,$$

$$L_1(x_{2,1}) = C_0 x_{2,1} + C_1 x_{2,1}^q = 0,$$

$$L_1(x_{3,1}) = C_0 x_{3,1} + C_1 x_{3,1}^q = 0,$$

thus $x_{1,2} = x_{2,2} = x_{3,2} = 0$,

so $S_4(x_{1,1}, x_{2,1}, x_{3,1}, x) = 0$, $x_{2,1}$ and $x_{3,1}$ do not exist in the calculation before *L(x)*, which means that $x_{2,1}$ and $x_{3,1}$ are unknown, and *x* cannot be determined. If reference [1] reverses the variable sign of the polynomial S_r, i.e., $S_4(x_{1,1}, x_{1,2}, x_{1,3}, x) = 0$, then $x_{1,3}$ is not included in the preceding calculation, so there is no way to determine *x*. If $x_{i,j+1}$ signs are also reversed, then $x_{2,1} = x_{2,2} = x_{2,3} = 0$, the conclusion is also incorrect.

Based on the above analysis, we believe that the algorithm in reference [1] is not an effective algorithm, and the experiment cannot effectively verify the theoretical design.

B. Analysis of Momonari, Kudo et al. 's Improvement Methods

Momonari, Kudo et al. did not give a specific algorithm, but improved on Semaev's sum polynomial functions. In terms of type (8), the conclusion is correct, because the assumption $(t_1, t_2) \in F_p^2$ is a solution of type (8), for the arbitrary point $(\alpha, \beta) \in F_p^2$, $t_1 = \alpha + \beta$, $t_2 = \alpha\beta$, $f(\alpha) + f(\beta) = g_+(t_1, t_2) = 0$, $f(\alpha) f(\beta) = g_\times(t_1, t_2) = 0$, $f(\alpha) = f(\beta) = 0$, namely the $S_3(\alpha, \beta, z) = S_3'(t_1, t_2, z) = 0$. But they don't tell us how the number of variables greater than 3 will be constructed.

Since they are the optimization of algorithm 1, we analyzed the inefficiency of algorithm 1 in Section 3.1, so it is not known whether the improved algorithm of Momonari and Kudo has improved the operation efficiency.

C. Pseudo-IC Method

We propose an IC method to mimic the discrete logarithmic solution of elliptic curves over a prime finite fields by assisting the idea of sum function proposed by Semaev, and we call it the *pseudo-IC method* because there is no notion of smooth boundaries and smooth numbers. The implementation method borrows the idea of the IC method and converts the method of solving the discrete logarithm of the prime factors of the smooth boundary by using a system of linear equations into a multiplicative construction, not only because of the high efficiency of multiplication, but also because it is not possible to solve the discrete logarithm of each prime factor of the smooth boundary by a system of linear equations. In addition, for a point to be solved, a multiplicative alternative to decomposition is used, i.e., whether or not the factor of the decomposition is in the base table is converted to whether or not the multiplicative factor is in the base table.

Since the prime factor multiple points on the elliptic curve cannot be obtained by multiplication, the base table selection is the same as that of classical IC, that is, the multiple points of the initial r prime factors (including generator P) are selected. Assuming the discrete logarithm of the initial r prime factor multiple points is known, then the composition of the set M is $\{P_1, P_2, \cdots, P_r, -(P_1 + P_2 + \cdots + P_r)\}$, apparently $P_1 + P_2 + \cdots + P_r + (-(P_1 + P_2 + \cdots + P_r)) = O$, including $P_1 = P = (x_1, y_1)$, $P_2 = 2P = (x_2, y_2)$,..., $P_r = rP = (x_r, y_r)$. Let $-M$ be the set of symmetric elements of *M*, then $U = (-M) \bigcup M \bigcup \{O\}$ .Let $\lambda \leq N$ is a prime number close to *N*. If $\lambda Q \in U$,and suppose $\lambda Q = k_i P$,then $k = \lambda^{-1} k_i \pmod N$,else $s = \lambda$, $R = sP$,and find next prime number close to λ ,until $\lambda Q = k_i P$ or $R + \lambda Q \in M$ or $R + \lambda Q = O$,corresponding, there are $k = \lambda^{-1} k_i \pmod N$,or $k = \lambda^{-1}(k_i - s) \pmod N$,or $k = -\lambda^{-1} s \pmod N$.

Now, the value of *r* follows the method of discrete logarithms over a finite fields, i.e., take $r = \left| \exp\{\sqrt{\ln p}\} \right|$[21]. From the above construction of *M*,it is clear that $S_r(x_1, x_2, \cdots, x_r) = 0$. See *Algorithm 2* for the specific implementation of the above described process.

Algorithm 2.IC algorithms for elliptic curves over prime finite fields

Input : E, p, P, Q

Output: k

1.Let $r = \lceil \log_2 p \rceil, R = O$.

2.Construct the set *M*

a. $i = 2$

b.Calculate $iP, R = R + iP$,save i , iP , $(N-i)P$

c. $i = i + 1$, if i is prime, go to b, else loop at step c

3. Find *k*

a.Select λ , λ is a prime number from 2 to *N*

b.if $\lambda Q \in U$ then $k = \lambda^{-1} k_i \pmod N$,goto 4

c. $s = \lambda$, $R = sP$

d.repeat finding next prime number close to λ ,until $\lambda Q = k_i P$ or $R + \lambda Q \in M$ or $R + \lambda Q = O$ or $\lambda Q = \sum_{i=1}^{r} k_i P_i$

e.If $\lambda Q = k_i P$ then $k = \lambda^{-1} k_i \pmod N$

f.If $R + \lambda Q \in M$ then $k = \lambda^{-1}(k_i - s) \pmod N$

g.If $R + \lambda Q = O$ then $k = -\lambda^{-1} s \pmod N$

h.If $\lambda Q = \sum_{i=1}^{r} k_i P_i$ then $k = \lambda^{-1}\left(\sum_{i=1}^{r} k_i P_i\right) \pmod N$

4. output *k*

V. PSEUDO-IC METHOD ANALYSIS

A. Case Verification

Algorithm 2 presented in Section IV.C is now verified. Choose a prime number from 2 to $N-1$ and do a multiplication of point Q. Compare the result with the value in *U,*otherwise *slelct next a* prime number. If the point is in *U*, the algorithm is solved correctly according to the algorithm and outputs the discrete logarithmic value, otherwise it fails.

Example 1. Suppose the elliptic curve $E: y^2 = x^3 + x + 1$ definition over prime finite fields F_{23} , results show *N*=28, take point *P*=(0, 1) for the generator of elliptic curve *E*, the other 27 points as follows:2*P*=(2,19),3*P*=(3,13),4*P*=(13,16),5*P*=(18,3),6*P*=(7,11),7*P*=(11,13),8*P*=(5,19),9*P*=(19,18),10*P*=(12,4),11*P*=(1,16),12*P*=(17,20),13*P*=(9,16),14*P*=(4,0),15*P*=(9,7),16*P*=(17,3),17*P*=(1,7),18*P*=(12,19),19*P*=(19,5),20*P*=(5,4),21*P*=(11,20),22*P*=(7,12),23*P*=(18,20),24*P*=(13,7),25*P*=(3,10),26*P*=(6, 4),27*P*=(0,22),28*P*=O.

Because $r = \left| \sqrt{\log_2 23} \right| = 3$, so *M*={*P*,2*P*,3*P*,5*P*,18*P*}, *U*={*P*,2*P*,3*P*,5*P*,18*P*,25*P*,26*P*,*O*}.

Now calculate the discrete logarithm of *Q*=4*P*. select $\lambda = 23$ .Since $R = 23Q = 92P = 8P \notin U$.*Next* select $l = 19$, $19Q = 76P = 20P \notin U$, $R = R + 19P = 28P = O$ .So $k = 23^{-1}(-19) \pmod N = 4$. After 2 searches, the discrete logarithm of *Q* is obtained.

Let's calculate the discrete logarithm of *Q*=11*P*. select $\lambda = 23$ .Since $R = 23Q = 253P = P \in U$ .So $k = 23^{-1} \pmod N = 11$. After 1 searches, the discrete logarithm of *Q* is obtained.

Example 2. Suppose that the elliptic curve $E: y^2 = x^3 + 373x + 837$ is defined on the prime finite fields F_{1019} , we can see that *N*=1019, and take the point *P*=(293, 914) as the generator of the elliptic curve *E*, now solve *Q*=(794, 329).

Since $r = \left| \sqrt{\log_2 1019} \right| = 4$, *M*={*P*,2*P*,3*P*,5*P*,7*P*,1002*P*}, – *M*={17*P*,1012*P*,1014*P*,1016*P*,1017*P*},*U*={*P*,2*P*,3*P*,5*P*,7*P*, 17*P*,1002*P*,1012*P*,1014*P*,1016*P*,1017*P*,*O*}.

Multiply *Q* by randomly selecting a number from the prime numbers 2 to 1018, and find that 613*Q*=1012*P* belongs to *U*. Now we know the discrete logarithm of Q is 123.Because $Q = \left[1012 * 613^{-1} \pmod N\right] P = 123P$. If you look at the primes from 2 to 1018, it takes 112 times to find the discrete logarithm of *Q*, which means that it is very difficult to find the discrete logarithm of a point exactly. Of course, as a probability solution, it works.

Step d of algorithm 2 can also be used as $\lambda Q = \sum_{i=1}^{r} k_i P_i$ (where $P_i \in U, k_i \in Z$), if the equation is full, then $m = \lambda^{-1}\left(\sum_{i=1}^{r} k_i P_i\right) \pmod N$, but this kind of search process is also very difficult. For example, $5Q = 5P_1 + 5P_2 + 200P_3 = 615P$ (Of course, there are many other forms of combination, as long as the value of the sum polynomial can reach $615P$), then $m = 5^{-1} \times 615 \pmod{1019} = 123$. But it is not easy to combine several elements from the set U to double the operation exactly $615P$, because $615P$ is unknown.

B. Algorithm 2 Analysis

Algorithm 2 is correct in terms of the construction and examples of sum polynomial functions. However, the efficiency of *Algorithm 2* is extremely low, because arbitrarily choosing an integer to multiply a point, the probability that the result falls into *U* is only $2r / N \approx 2\left|\exp\{\sqrt{\ln p}\}\right| / p$, and when $p \to \infty$, the probability is very small, so *Algorithm 2* is extremely inefficient. Because a point of the factor base on the elliptic curve needs to store three values, which are the multiplicity of the point, the horizontal coordinate, and the vertical coordinate, it needs *O(6r)* space complexity for the factor base *U* . If the multiplicative point search for prime numbers according to *Algorithm 2* is successful, the complexity of the search in the worst case is $O(p / \ln p)$, in which case the probability is $\sqrt{\ln p} / \ln p$. In the best case, the discrete logarithm is obtained only once, but such a case can be ignored. Therefore, under the condition of prime finite fields, there exists no method of subexponential discrete logarithm solution on elliptic curves, or at least in the present

research context, no method of subexponential discrete logarithm solution has been found.

VI. SUM POLYNOMIAL IN II.B CORRECTNESS ANALYSIS

Using the data in Example 1 to verify, it is found that the expression of sum polynomial S_3 is not correct in II.B.Such as $2P+3P+23P=O$,wherer $x_1=2, x_2=3, x_3=18$,but $S_3=5\neq 0$ .This shows that the expression for the sum polynomial S_3 is incorrect.

According to the derivation process in literature [11], $x_4-x_3=0$. Because x_3 and x_4 are the horizontal coordinates of two symmetric points on elliptic curves.However, Semaev constructs the expression of sum polynomial S_3 by taking x_3 and x_4 as the relationship between the roots and coefficients of the quadratic equation with one variable, and it is obvious that the expression of S_3 may not satisfy the points on the elliptic curve.

VII. CLOSING REMARKS

Since 1985,Miller and Koblitz independently proposed that elliptic curves can be applied in public-key cryptosystems,scholars have carried out a lot of research on the problem of discrete logarithmic solution on elliptic curves.They have achieved greater success on finite fields with small features,but it is more difficult on prime finite fields,especially when the order of elliptic curves contains large prime factors.In 2016. Petit et al. tried to realize the operation of IC method on finite fields by using algebraic methods.Our analysis concludes that the algorithm did not achieve the expected results, and their experimental results are yet to be further confirmed due to the flaws in their theoretical design.In addition, the expression of sum polynomial fails to satisfy the points on elliptic curves. Our proposed algorithm only imitates the implementation of the IC method on finite fields, but the algorithm is not subexponential time. Therefore, we believe that it is impossible to obtain the effect of solving discrete logarithms on finite fields using the IC method as far as the existing research is concerned.

REFERENCES

[1] PETIT C, KOSTERS M, MESSENG A. Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields [M]//CHENG C M, CHUNG K M, PERSIANO G, et al, eds. Public-Key Cryptography – PKC 2016. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 3-18.

[2] ADLEMAN L.A subexponential algorithm for discrete logarithms with applications to cryptography[C].Proc.20th IEEE Found.Comp.Sei.Symp.,IEEE Computer Society, Long Beach,CA,1979,55-60.

[3] ADLEMAN L M, DEMARRAIS J. A subexponential algorithm for discrete logarithms over all finite fields[J]. Mathematics of Computation, 1993, 61(203): 1-15.

[4] ENGE A, GAUDRY P. A general framework for subexponential discrete logarithm algorithms [J]. Acta Arithmetica, 2002, 102(1): 83-103.

[5] PADMAVATHY R, BHAGVATI C. Performance analysis of index calculus method [J]. Journal of Discrete Mathematical Sciences and Cryptography, 2009, 12(3): 353-371.

[6] HU J J, WANG W,LI H J. An improving algorithm of index calculus[J].Journal of Nanchang University(Engineering and Technology Edition), 2016, 38(3):286-289.

[7] HU J J.A method for computing discrete logarithm based on ICA [J]. Engineering Journal of Wuhan University,2021,54(9):874-878.

[8] HU J J. Analysis and optimization of improved index calculus algorithm [J]. Mathematics and Computer Science, 2023, 8(2):57-61.

[9] HU J J, WANG W, LI H J. Solving the discrete logarithm on elliptic curve of trace one[J].Journal of An hui University(Natural Science Edition),2023,47(06):1-6.(in Chinese)

[10] XIAO Y A.Research on elliptic curve cryptosystem [M]. Wuhan: Huazhong University of Science and Technology Press, 2006:56-88.

[11] SEMAEV I. Summation polynomials and the discrete logarithm problem on elliptic curves[J]. Cryptology ePrint Archive, 2004.

[12] GAUDRY P. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem [J]. Journal of Symbolic Computation, 2009, 44(12): 1690-1702.

[13] DIEM C. On the discrete logarithm problem in elliptic curves [J].Compositio Mathematica,2011,147(1):75-104.

[14] FAUGERE J C, PERRET L, PETIT C, et al. Improving the complexity of index calculus algorithms in `elliptic curves over binary fields [M]//Advances in Cryptology – EUROCRYPT 2012. Berlin, Heidelberg:Springer Berlin Heidelberg, 2012: 27-44.

[15] DIEM C. On the discrete logarithm problem in elliptic curves II [J]. Algebra & Number Theory, 2013,7(6): 1281-1323.

[16] SHANTZ M, TESKE E. Solving the elliptic curve discrete logarithm problem using semaev polynomials,Weil descent and gr¨obner basis methods – an experimental study [M]//Lecture Notes in Computer Science.Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 94-107.

[17] SEMAEV I.New algorithm for the discrete logarithm problem on elliptic curves[J]. ar**v preprintar**v:1504.01175, 2015.

[18] GALBRAITH S D, GAUDRY P. Recent progress on the elliptic curve discrete logarithm problem [J].Designs, Codes and Cryptography, 2016, 78(1): 51-72.

[19] AMADORI A, PINTORE F, SALA M. On the discrete logarithm problem for prime-field elliptic curves[J]. Finite Fields and Their Applications, 2018, 51: 168-182.

[20] KUDO M, YOKOTA Y, TAKAHASHI Y, et al. Acceleration of index calculus for solving ECDLP over prime fields and its limitation [M]//CAMENISCH J, PAPADIMITRATOS P, eds. Cryptology and Network Security. Cham: Springer International Publishing, 2018: 377-393.

[21] SILVERMAN J H, SUZUKI J. Elliptic curve discrete logarithms and the index calculus [M]//Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998: 110-125.