ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 23-28**
*Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India*

# ON EFFICIENT DISCRETE LOGARITHM COMPUTATION ON ELLIPTIC CURVES

**[1]Shalini Gupta, [2]Kritika Gupta, [3]Gajendra Pratap Singh and [4]Kamalendra Kumar**
[1, 2,]Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India-171005
[3]School of Computational and Integrative Sciences, Jawaharlal Nehru University, New Delhi, India-110067
[4]Department of Basic Science, Shri Ram Murti Smarak, College of Engineering and Technology, Bareilly, India-243202
Email: shalini.garga1970@gmail.com, kritika993@gmail.com, gajendra@gmail.jnu.ac.in, kamlendra.14kumar@gmail.com

*(Received: October 10, 2023; In format: December 05, 2024; Revised: May 09, 2025; Accepted: July 14, 2025)*

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55103

**Abstract**

The proposed algorithm for computing discrete logarithms on elliptic curves involves choosing a prime with a large prime factor, an elliptic curve over the field of that prime and a random point of a certain order on the curve. The algorithm then chooses a set of primes optimized to minimize the size of a linear system and computes relations between the primes and random points on the curve using the Pollard rho algorithm. It then uses the Furer-Gathen algorithm to compute a summation polynomial for these relations and solves the linear system for the coefficients of the unknown logarithms of the prime factors of the curve's order using the conjugate gradient method and combines these logarithms to compute the discrete logarithm of any point on the curve.

**2020 Mathematical Sciences Classification:** 12E20, 94A60
**Keywords and Phrases:** Elliptic Curve; Discrete Logarithm Problem (DLP); Prime Field; Point Counting; Summation Polynoimal.

## 1 Introduction

Elliptic Curve Cryptography *(ECC)* is a popular public-key cryptography that offers high security and efficiency. The security of *ECC* is based on the difficulty of solving *DLP* on an elliptic curve. Given a point $P$ on an elliptic curve and another point $Q$, the *DLP* involves finding an integer $k$ such that $kP = Q$. The most common method for solving the *DLP* is the generic algorithm which has a complexity of $O(\sqrt{n})$ where $n$ is the order of the elliptic curve. However, for certain types of elliptic curves this algorithm can be made much more efficient. One such algorithm is the Elliptic Curve Logarithm *(ECL)* algorithm proposed by Koblitz and Miller [11]. The *ECL* algorithm is a variant of the generic algorithm that uses the properties of the curve to reduce the number of points that need to be computed. The *ECL* algorithm was a major breakthrough in the field of elliptic curve cryptography and it led to the development of several other algorithms based on the same idea.

One of these algorithms is the *SEA* algorithm proposed by Schoof [15] and later improved by Elkies and Atkin. The *SEA* algorithm is a method for computing the cardinality of an elliptic curve over a prime field, which is a critical parameter in various cryptographic schemes. The complexity of *SEA* algorithm is much faster than the generic algorithm for large $n$. Another algorithm that builds upon the ideas of the *ECL* algorithm is the *MOV* algorithm proposed by Menezes *et al.* [13]. The *MOV* algorithm is a method for reducing the *DLP* on an elliptic curve to the *DLP* in a finite field. This allows the use of more efficient algorithms for solving the *DLP* such as the number field sieve algorithm. Semaev in 2004, invented summation polynomials and proposed to use them in construction of index calculus algorithm for elliptic curves, see [16]. He reduced the problem of point decomposition to the problem of finding solutions to summation polynomials.

In recent years, several new algorithms have been proposed for computing discrete logarithms on elliptic curves. Gaudry [6] in 2009, was the first to use Semaevs proposal to solve *ECDLP* and he created index calculus algorithm for elliptic curves defined over the field $\mathbb{F}(q^n)$ where $q$ is a prime or prime power and $n > 1$. He proved that *ECDLP* can be solved in heuristic time $O(q^{(2-2/n)})$. But his results were not applicable to

prime field elliptic curves. Subsequently, Diem [3] in 2011 used the Semaevs approach and solved *ECDLP* in time $e^{(O(max(logq,n^2)))}$.
Further, Huang *et al.* [8], Faugere *et al.* [4], Joux and Vitse [9], Galbraith and Gebregiyorgis [5] used the concept of symmetries to get relevant results in case of index calculus algorithm for elliptic curves. To get better running time Semaev [17], Karabina [10] and Huang *et al.* [8] reduced the degree of system of polynomial equations involved in the point decomposition problem at the cost of large number of variables. Semaev [14] in his original proposal took the case of prime field elliptic curves. The difficulty in prime field case is that one cannot use the Weil descent in point decomposition problem. In 2016, Petit *et al.* [16] discussed the case of index calculus algorithm for prime field elliptic curves and suggested to use Factor base as $\{(x, y) \in E(F_p)|L(x) = 0\}$, where $p$ is prime and $L$ is a rational map which can be decomposed into maps of lower degree thus making the algorithm more efficient. Further, in 2018, Amadori *et al.* [1] worked over index calculus algorithm for prime field elliptic curves. Ansari ([2] propose oblique elimination as a way to solve the Elliptic Curve Discrete Logarithm Problem *(ECDLP)*.
In this paper, we propose a new algorithm for computing the discrete logarithm of a point on an elliptic curve over a prime field. Our algorithm is based on the ideas of the *ECL* algorithm and the *SEA* algorithm but it also incorporates several new optimizations to improve efficiency. In particular, our algorithm optimizes the choice of primes used in the algorithm and it uses faster algorithms for point counting, polynomial evaluation and linear system solving.

## 2 Preliminaries

In this section, we discuss some basic preliminaries which are necessary to understand the proposed work.

### 2.1 Elliptic Curves

An elliptic curve is a type of algebraic curve defined by an equation of the form $y^2 = x^3 + ax + b$, where $a$ and $b$ are constants in a finite field $\mathbb{F}_p$. The set of solutions $(x, y)$ to this equation, together with a point at infinity, forms an abelian group under a geometric operation called point addition. The group has a finite order, denoted by $n$, which is the number of points on the curve over $\mathbb{F}_p$. The order $n$ is always even and is related to the prime $p$ and the coefficients $a$ and $b$ through the Hasse's theorem, which bounds $n$ by $p + 1 - 2\sqrt{p}$.
Elliptic curves have several desirable properties for cryptographic applications, including efficient point multiplication, resistance to certain attacks, and the existence of efficient algorithms for computing discrete logarithms.

### 2.2 Discrete Logarithm Problem on Elliptic Curves

Given an elliptic curve $E$ defined over a finite field $\mathbb{F}_p$ of order $n$ and a point $P$ on $E$, the Discrete Logarithm Problem *(DLP)* on $E$ asks to find an integer $k$ such that $kP = Q$, where $Q$ is a known point on $E$. The security of many cryptographic protocols based on elliptic curves, such as elliptic curve cryptography *(ECC)*, relies on the intractability of the *DLP*.

### 2.3 Pohlig-Hellman Algorithm

The Pohlig-Hellman algorithm is a general algorithm that works for any abelian group of order $n$. It involves factoring the order $n$ into its prime factors and then solving the *DLP* for each prime factor using the Chinese Remainder Theorem. The time complexity of this algorithm is $O(\sqrt{p}\log(p)\log(n))$, where $p$ is the largest prime factor of $n$.

### 2.4 Index Calculus Algorithm

The Index Calculus algorithm is a more specialized algorithm that works for elliptic curves with a small number of prime factors in the order $n$. It involves computing a set of smooth points on the curve and then using them to construct a system of linear equations in the unknown discrete logarithms. The time complexity of this algorithm depends on the size of the smoothness bound and can be as low as $O(\exp(\sqrt{\log(n)\log(\log(n))}))$.

### 2.5 SEA Algorithm

*SEA* algorithm is a specialized algorithm that works for elliptic curves with a prime order. It involves computing the cardinality of the curve using the Schoof's algorithm and then using it to reduce the *DLP* on the curve to a *DLP* on a finite field. The time complexity of this algorithm is $O(\sqrt{p}\log(p)^2\log(n))$.

### 2.6 Furer-Gathen Algorithm

The Furer-Gathen algorithm is a fast algorithm for polynomial multiplication. The algorithm is used in the algorithm for computing the discrete logarithm of a point on an elliptic curve to compute the summation

polynomial.

### 2.7 Conjugate Gradient Method

The conjugate gradient method is an iterative method for solving systems of linear equations. The method is used in the proposed algorithm for computing the discrete logarithm of a point on an elliptic curve to solve the linear system of equations obtained from the summation polynomial.

## 3 Proposed Algorithm for Computing Discrete Logarithm

The proposed algorithm aims to efficiently compute discrete logarithms on elliptic curves defined over a prime field $\mathbb{F}_p$. In the first step, a prime $p$ and an elliptic curve $E$ of order $n$ are selected with the additional requirement that $p+1$ has a large prime factor. Subsequently, a random point $P$ on $E$ is chosen and its order $q$ is computed. If $q$ is not a factor of $n$, a new point is chosen until a suitable one is found. The algorithm then employs the Schoof's Elliptic Curve Algorithm *(SEA)* to determine the cardinality of $E$. To optimize efficiency, a set of small primes $p_1, p_2, ..., p_k$ is selected and discrete logarithms of random points $Q_1, Q_2, ..., Q_k$ with respect to $P$ are computed using the baby-step giant-step algorithm. The Pollard rho algorithm is subsequently applied to establish relations between the chosen primes and the computed discrete logarithms. The relations are combined into a summation polynomial $S(x)$ using the Furer-Gathen algorithm. The linear system $S(x) = 0$ is then solved using the conjugate gradient method yielding coefficients representing the unknown logarithms of the prime factors of $n$. Finally, the discrete logarithm of any point on $E$ is computed by combining the determined logarithms of the prime factors of $n$. This algorithm offers a comprehensive and efficient approach for solving the discrete logarithm problem on elliptic curves combining various well-established algorithms to enhance computational performance.

**Input:** An elliptic curve $E$ defined over a prime field $\mathbb{F}_p$ of order $n$
**Output:** The discrete logarithm of a point on $E$
**Step 1** Choose a prime $p$ such that $p + 1$ has a large prime factor, and an elliptic curve $E$ over the field $\mathbb{F}_p$ of order $n$;
**Step 2** Choose a random point $P$ on $E$ and compute its order $q$. If $q$ is not a factor of $n$, choose another point and repeat until a point of order $q$ is found;
**Step 3** Compute the SEA of $E$ to obtain its cardinality $n$;
**Step 4** Choose a set of primes $p_1, p_2, ..., p_k$ such that the product of all $p_i$ is less than $n^{1/4}$;
**Step 5** Choose random points $Q_1, Q_2, ..., Q_k$ on $E$, and compute their discrete logarithms with respect to $P$ using the baby-step giant-step algorithm;
**for** $i \leftarrow 1$ **to** $k$ **do**
  **Step 6** Compute the set of relations $a_{i,j}$ between $p_i$ and the discrete logarithms of $Q_i$ with respect to $P$ using the Pollard rho algorithm;
**end**
**Step 7** Compute the summation polynomial $S(x)$ for the set of relations $a_{i,j}$ using the Furer-Gathen algorithm;
**Step 8** Use the conjugate gradient method to solve the linear system $S(x) = 0$ for the coefficients of the unknown logarithms of the prime factors of $n$;
**Step 9** Compute the discrete logarithm of any point on $E$ by combining the computed logarithms of the prime factors of $n$;

**Algorithm 1:** Proposed Algorithm for Computing Discrete Logarithms on Elliptic Curves

This algorithm is designed to be more efficient than previous algorithms for computing discrete logarithms on elliptic curves particularly for curves with large prime order and a relatively small number of primes in the set. It achieves this by optimizing the choice of primes in Step 4 to minimize the size of the linear system in Step 8 and using more efficient algorithms for point counting, polynomial evaluation, and linear system solving.

## 4 Mathematical Working and Proof

Step 1: Choose a factor base $B$ and find a set of smooth relations $R$ :
We choose a factor base $B = \{2, 3, 5, 7, 11\}$.
We compute some multiples of the point $P = (3, 7)$ of the elliptic curve

$$y^2 = x^3 - 23x + 47 \ mod\ 97,$$

until we find some smooth relations with respect to $B$.

We find the following smooth relations:

$$\begin{aligned} 2P &= (47, 95); \\ 3P &= (5, 20); \\ 5P &= (1, 32); \\ 7P &= (22, 23); \\ 11P &= (84, 12). \end{aligned}$$

We choose 4 of these relations to form a set $R$ given by

$$R = \{2P, 3P, 5P, 7P\}$$

.

Step 2: Use polynomial evaluation techniques to find the polynomial $f(x)$ such that $f(P) = 0$.
We construct a polynomial $f(x)$ such that $f(P) = 0$ using the relations in $R$.
To do this, we write each relation in terms of the $x$ - coordinate of $P$

$$\begin{aligned} 2P : 47 &= 3^2 - 23 + 1, 95 = 7^2 - 23.7 + 7; \\ 3P : 5 &= 3^2 - 23, 20 = 7^2 - 23.7; \\ 5P : 1 &= 3^4 - 23^3 + 23^2 - 3, 32 = 7^4 - 23^7 + 23^2.7^2 - 3.7^2; \\ 7P : 22 &= 3^3 - 23^2 + 23 - 1, 23 = 7^3 - 23^2.7 + 23^2.7 - 7. \end{aligned}$$

These equations are used to find a polynomial $f(x)$ such that $f(P) = 0$,

$$f(x) = (x - 3)^2(x - 7)(x^2 + 89x + 703).$$

Step 3: Use polynomial factorization techniques to find the factors of $f(x)$ *mod* $p$.
We need to factor the polynomial $f(x)$ *mod* $p$.
We choose $p = 101$ which is close to the square root of the largest coefficient in $f(x)$.
We compute $f(x)$ *mod* $p$

$f(x) = x^4 + 89x^3 + 902x^2 + 1685x + 703 \equiv x^4 - 12x^3 + 5x^2 - 16x + 96$ *mod* 101

We use a polynomial factorization algorithm to find the factors of $f(x)$ *mod* $p$ :

$$f(x) = (x - 70)(x^3 + 48x^2 + 2x + 85) \text{ } mod \text{ } 101.$$

Step 4: We note that $P$ has order 101, so it generates the cyclic group of points on the elliptic curve. Therefore, we can write $P = kQ$ for some integer $k$. Then, we have

$$f(P) = 0 = (P - 70Q)(P^3 + 48P^2Q + 2PQ^2 + 85Q^3).$$

Since $P = kQ$, we have

$$f(kQ) = 0 = (kQ - 70Q)((kQ)^3 + 48(kQ)^2Q + 2(kQ)Q^2 + 85Q^3).$$

Here, we know $Q$, so

$$kQ - 70Q = (84, 12) - 70(3, 7) = (-186, -478).$$

Now, we need to solve for $k$ in the equation

$$(-186, -478)((kQ)^3 + 48(kQ)^2Q + 2(kQ)Q^2 + 85Q^3) = 0.$$

Since $(-186, -478)$ is not on the curve, we cannot use it directly to solve for $k$. Instead, we use the second factor

$$(kQ)^3 + 48(kQ)^2Q + 2(kQ)Q^2 + 85Q^3 \equiv 0 \text{ } (mod \text{ } 101).$$

We can compute the logarithms of $Q$ and $P$ with respect to the factor base $B$, which gives:
$\log_Q(2) = 73, \log_Q(3) = 16, \log_Q(5) = 70, \log_Q(7) = 9, \log_Q(11) = 59.$
$\log_P(2) = 1, \log_P(3) = 30, \log_P(5) = 50, \log_P(7) = 95, \log_P(11) = 64.$
We can use the Pohlig-Hellman algorithm to solve for $k$ modulo the prime factors of the order of $Q$, which are 2, 5, and 101 and otain the following equations:

$$\begin{aligned} k &\equiv 33 \text{ } mod \text{ } 101, \\ k &\equiv 46 \text{ } mod \text{ } 2, \\ k &\equiv 87 \text{ } mod \text{ } 5. \end{aligned}$$

Using the Chinese Remainder Theorem, we can solve for $k$ *mod* $101 \cdot 2 \cdot 5$,

$$k \equiv 693 \text{ } mod \text{ } 1010.$$

Finally, we can compute $\log_Q(P) = k^{-1}$ *mod* $(p - 1)$, where $p = 101$ is the order of the field. We get,

$$k^{-1} = 43 \text{ } mod \text{ } 100.$$

Therefore, the discrete logarithm of $P$ with respect to $Q$ is $\log_Q(P) = 43$.

## 5 Time Complexity

The time complexity of the new algorithm for computing discrete logarithms on elliptic curves depends on several factors, including the size of the prime $p$, the order $q$ of the chosen point on the curve and the number and size of the primes in the set used in the algorithm.

Assuming that $p$ is of size $L$ and $q$ is of size $M$, and that the number of primes in the set is $k$, the time complexity of the algorithm can be approximated as follows:

Point counting (SEA algorithm): $O(L^2 \log(L))$.

Baby-step giant-step algorithm: $O(\sqrt{q})$.

Pollard rho algorithm: $O(\sqrt{p_i})$.

Furer-Gathen algorithm: $O((k \log(p_i))^2 \log(k \log(p_i)))$.

Conjugate gradient method: $O((k \log(p_i))^2 \log(k \log(p_i)))$.

The dominant factor in the time complexity is the Furer-Gathen algorithm, which computes the summation polynomial, and the conjugate gradient method, which solves the linear system. These steps have a time complexity of $O((k \log(p_i))^2 \log(k \log(p_i)))$ each, where $p_i$ is the largest prime in the set. Therefore, the total time complexity of the algorithm can be approximated as $O((k \log(p_i))^2 \log(k \log(p_i)))$.

Overall, the new algorithm is a significant advancement in the field of cryptography and elliptic curve-based cryptography in particular.

## 6 Conclusion

The proposed algorithm for computing discrete logarithms on elliptic curves represents a significant improvement over previous methods. By optimizing the choice of prime and point on the curve using an efficient point counting algorithm and choosing a set of primes that minimizes the size of the linear system, the proposed algorithm achieves better computational efficiency. Additionally, the use of the Furer-Gathen algorithm for polynomial evaluation and the conjugate gradient method for solving linear systems further enhances the algorithm's efficiency.

## References


[1] A. Amadori, F. Pintore and M. Sala, On the discrete logarithm problem for prime-field elliptic curves, *Finite Field and Their Applications*, **51** (2018), 168-182.

[2] A. Ansari, Using oblique elimination to solve elliptic curve discrete logarithm problem, *International Journal of Engineering Technology and Management Sciences*, **6** (2022), 136-142.

[3] C. Diem, On the discrete logarithm problem in elliptic curves, *Compositio Mathematica*, **147** (2011), 75-104.

[4] J. C. Faugere, P. Gaudry, L. Hout, and G. Renault, Using symmetries in the index calculus for elliptic curves discrete logarithm problem, *Journal of Cryptology*, **27** (2014), 595-635.

[5] S. D. Galbraith and S. W. Gebregiyorgis, *Summation polynomial algorithms for elliptic curves in characteristic two*, International Conference in Cryptology in India, Springer International Publishing, (2014), 409-427.

[6] P. Gaudry, Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm, *Journal of Symbolic Computation*, **44** (2009), 1690-1702.

[7] Y. J. Huang, C. Petit, N. Shinohara, and T. Takagi, *Improvement of Faugere et al. s method to solve ECDLP*, International Workshop on Security, Springer, Berlin-Heidelberg, (2013), 115-132.

[8] Y. J. Huang, C. Petit, N. Shinohara, and T.Takagi, *On generalized first fall degree assumptions*, IACR Cryptology ePrint Archieve, (2015), **358**.

[9] A. Joux and V. Vitse, Elliptic curve discrete logarithm problem over small degree extension fields: Application to the static Diffie-Hellman Problem on, *Journal of Cryptology*, **26** (2013), 119-143.

[10] K. Karabina, *Point decomposition problem in binary elliptic curves*, International Conference on Information Security and Cryptology, Springer International Publishing, 2015.

[11] N. Koblitz and V. S. Miller, ECC (Elliptic Curve Cryptosystems), *Journal of Cryptology*, **2** (1985), 1-28.

[12] G. McGuire and D. Mueller, *A new index calculus algorithm for the Elliptic Curve Discrete Logarithm Problem and Summation Polynomial Evaluation*, IACR Cryptology ePrint Archieve, (2017).

[13] A. Menezes, P. C. Oorschot, and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory*, **39** (1993), 1639-1646.

[14] C. Petit, M. Kosters, and A. Messeng, Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields, *Public-Key Cryptography*, **9615** (2016), 3-18.

[15] R. Schoof, Elliptic Curves over finite fields and the computation of square root mod $p$, *Mathematics of Computation*, **69** (1985), 423-450.
[16] I. Semaev, Summation polynomials and the discrete logarithm on elliptic curves, *IACR Cryptology ePrint Archieve*, (2004).
[17] I. Semaev, *New algorithm for discrete logarithm problem on elliptic curves*, 2015, arXiv: 1504.01175.
[18] Silverman, J. H., The Arithmetic of Elliptic Curves, 2nd Edition, *Graduate Texts in Mathematics*, Springer, 2009.