Attacks on Elliptic Curve Discrete Logarithm Problem

Vishnu Prasad V
Department of Computer Science and Engineering
Adhiyamaan College of Engineering
Hosur, India
vishnuprasadyy@gmail.com

***Abstract*—This paper presents an examination of the Elliptic Curve Discrete Logarithm Problem and techniques in attacking cryptosystems dependent on the ECDLP and briefly discusses how to generate cryptographically strong elliptic curves.**

Keywords—Elliptic Curve, Cryptography, Groups and Fields, Discrete logarithm problem, Attacks.

I. Introduction

In 1976, Diffie and Hellman published "New Directions in Cryptography" which introduced the discrete logarithm problem in finite fields as a one-way function. The discrete logarithm problem for $\mathbb{F}p$ is defined as *Let g be generator of the group $\mathbb{F}_q^*$. For some integer a, $0 \leq a < q - 1$, let $h = g^a \in \mathbb{F}_q^*$. The discrete logarithm problem (DLP) for $\mathbb{F}_q$ is defined to the problem of finding the number a given g and h. An attack on the DL is defined to be a method or algorithm which attempts to solve the DLP.* For an elliptic curve discrete logarithm problem over the finite field $\mathbb{F}p$ and generator point G and point p on the curve, such that $P = kG$, find the integer k.

II. Elliptic Curves

Elliptic Curve is the set of all solutions to a specific kind of polynomial equation in two real variables xy over a field f:

The equation of the form: $y^2 = x^3 + ax + b$

The general form of an elliptic curve is called the generalized Weierstrass equation and is given by the following equation:

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.where $a1, \ldots., a6$ are constants. The definition of elliptic curve requires that the curve is non-singular and an abelian variety; it has a group law defined algebraically.

III. The Group Law

A. Point Addition

Suppose now that $P1$ and $P2$ are two points in $E(Fp)$ and we want to add the points $P1$ and $P2$ of an elliptic curve E to produce a new, third point $P3$ $(x\,3,\ y\,3)$. This construction will be denoted as the addition of two points of the elliptic curve and represented by $P1 + P2 = P3$

B. Point Multiplication

Computing a point multiplication is through repeated addition. However the double-and-add algorithm is essentially a fast way to compute multiple of a point.

Let n be a positive integer and let P be a point on an elliptic curve. The following computes nP in a faster way.

1. *Start with $a = n$, $B = \infty$, $C = P$*
2. *If a is even, let $a = a/2$ and let $B = B$, $C = 2C$*
3. *If a is odd, let $a = a - 1$ and let $B = B + C, C = C$*
4. *If $a \neq 0$, go to step 2*
5. *Output B*

The output B is nP.

IV. Elliptic Curve Cryptography

Elliptic Curve Cryptography is an approach to public key cryptography. It is based on the algebraic structure of EC over finite fields. The principal attraction of ECC over non-ECC, is that it appears to offer equal security for a far smaller key size. The key exchange in ECC is described in *figure 1*.

If we have two secret numbers a and b (two private keys, belonging to Alice and Bob) an ECC with generator point G, we can exchange over an insecure channel the values $[a]G$ and $[b]G$ (the public keys of Alice and Bob) from there we can derive a shared secret $[a][b]G = [b][a]G$.

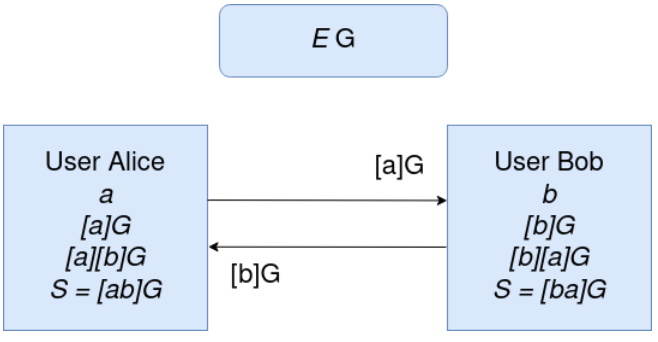

Figure 1: Key exchange in ECC.

V. Elliptic Curve Discrete Logarithm Problem

The classical discrete logarithm problem is to find k, satisfying the following condition $ak \equiv b\ (mod\ p)$. Let p be a prime number and let a and b be integers that are nonzero $(mod\ p)$.

The elliptic curve E, defined over the finite field $\mathbb{F}$p and let P and Q be points in $E(\mathbb{F}p)$. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem of finding an integer n such that $Q = nP$. By analogy with the discrete logarithm problem for $\mathbb{F}$*p we denote this integer n by $n = log\ P\ (Q)$ and we call n the elliptic discrete logarithm of Q with respect to P.

VI. Attacking The EC Discrete Logarithm Problem

A. Baby-Step, Giant-Step Algorithm

For every finite cyclic group a Baby-Step, Giant-Step algorithm can be used to solve ECDLP. It makes use of time-space tradeoff to solve discrete logarithm problems in arbitrary groups.

Let $E(\mathbb{F}q)$ be an elliptic curve with generator G. Suppose G has order n and let $Q \in G$, suppose that we want to solve $Q = [k]G$. Set $m = \lceil \sqrt{n} \rceil$ and compute $[m]G$. We now make a list of $[i]G$ for $0 \leq i < m$ and store this list. Now we can compute $Q - [j]([m]G)$ until we have found a match from the list that we have stored.

$iG = Q - j(mG)$ hence, $Q = iG + j(mG)$.

Therefore we have solved the ECDLP since
$k\,i + jm\ mod\ n$.

Hence this attack requires $\sqrt{n}$ operations and $\sqrt{n}$ values to search for collisions in the list and the time complexity of this algorithm is $O(\sqrt{n})$.

B. Pollard's rho

Pollard's rho algorithm is an algorithm for integer factorization. To solve discrete logarithm problem we want to find n where n is an element not higher than the order of the starting point P, such that $Q = [k]P$ and where $Q \in \langle P \rangle$ In this attack we will attempt to find distinct pairs of integers (a, b) at random and check against all previously stored triples until we find a pair (a', b') with $[a']P + [b']Q$ where $(a, b) \neq (a', b')$ thus ECDLP solved when $k \equiv (a - a')(b - b')^{-1}$ mod n. This method requires time complexity of $O(\sqrt{\frac{\pi n}{2}})$, and space complexity of $O(\sqrt{\frac{\pi n}{2}})$ to store triples.

C. The Pohlig-Hellman Method

Pohling-Hellman algorithm is for computing discrete logarithms in finite abelian group and applies to $|G| = p^n$. The worst-case time complexity is $0(\sqrt{n})$ For an elliptic curve $E(\mathbb{F}q)$, a point $P \in E(\mathbb{E}p)$ of order n and $Q \in \langle P \rangle$. To solve for the unique integer k such that $Q = [k]P$. If we assume $\prod_i l_i^{ei}$, where l_i is prime now attempt to solve for k by reducing the problem to solve for values of $k_i \equiv k \bmod l_i^{ei}$ for $0 \leq i \leq r$. The complexity will be:

$$O\left(\sum_i e_i(\log n + \sqrt{p_i})\right)$$

This attack is infeasible when n has a large prime divisor. P is sufficiently large when $p > 2^{160}$. When p is bigger than 2^{160}. The Chinese Remainder Theorem takes too much time to solve.

VII. Specialized Attacks

A. Pairing Attacks

The most common attack is MOV and Frey-Rűck, which uses Weil and Tate pairing. MOV attack attempts to reduce the ECDLP on an elliptic curve $E(\mathbb{F}_q)$ to the DLP in a $\mathbb{F}^{\times}_{Q^m}$ to solve in subexponential-time.

The pairing attacks are inefficient if n does not divide particularly the MOV attack might not be very useful for some cases, because m could still be very large.

VIII. Conclusion

The general attacks on the ECDLP are expected to run in fully exponential time. The feasible attack is the Pohlig-Hellman algorithm. To defend against this attack it is essential to choose an order where it has largest prime factor $p > 2^{160}$. The *table 1* summarizes expected running time of our general attacks.

TABLE I.. **E**XPECTED **T**IME **C**OMPLEXITY

Attack	Expected Time Complexity
Baby-Step, Giant-Step Algorithm	$O(\sqrt{n})$
Pollard's rho	$O(\sqrt{\frac{\pi n}{2}})$
Pohlig-Hellman	$O(\sqrt{n})$

Generating a cryptographically strong elliptic curve that resists all known attacks is simply generating curves at random then running them through a series of test attacks to see if they satisfy certain conditions.

References

[1] Dr. Joachim Rosenthal, “Cryptography”, Winter term 2004/05, University of Zurich.

[2] Peter Novotney, “Weak Curves In Elliptic Curve Cryptography”, 2010.

[3] Nolan Winkler, The Discrete Log Problem And Elliptic Curve Cryptography.

[4] J. Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag, 1986.

[5] “The Discrete Logarithm Problem”, Spring 2021, Faculty of Mathematics MIT.

[6] A.V. Sutherland, “Structure computation and discrete logarithms in finite abelian p groups” Mathematics of Computation 80 (2011), 501–538.

[7] E. Teske, “On random walks for Pollard’s rho method”, Mathematics of Computation 70 (2001), 809-825.

[8] J VenkataGiri, ASR Murty, “Elliptic Curve Cryptography Design Principles”, 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 2021, pp. 889-893, doi:10.1109/RTEICT52294.2021.9573662.