Analysis Of Attack Methods Based on Elliptic Curve Discrete Logarithm Problem

Xiao Ni

Mathematics, University of Wisconsin-Madison, United States

xni27@wisc.edu

Abstract. With growing public concern about information security issues, cryptography is becoming increasingly essential not only in the military sector, but also in daily life. Numerous cryptographic techniques have been invented during past hundreds of years. Elliptic Curve Cryptography (ECC) is one of the most modern and efficient cryptography methods. Therefore, research on exploring advantages and disadvantages is necessary in order to make the best use of ECC. This paper aims to briefly introduce Elliptic Curve (EC) and how it can be applied to ECC. Moreover, this paper indicates the mathematical principle Elliptic Curve Discrete Logarithm Problem (ECDLP) behind Elliptic Curve cryptography: how it is different from traditional Discrete Logarithm Problem (DLP) and the difficulty to solve ECDLP which protects ECDLP from various attacks. Most importantly, several potential attacks against ECC such as Exhaustive Search and Pollard's Rho algorithm are listed and discussed, which lead to reflections on the security issues of ECC and prospects for possible developments in the future.

Keywords: elliptic curve cryptography, elliptic curve, discrete logarithm Problem, elliptic curve discrete logarithm problem.

1. Introduction

In modern world, cryptography plays an important role in helping to protect both personal information and networks. Among all kinds of cryptographic techniques, Elliptic Curve Cryptography (ECC) is an advanced and strong one [1]. There are several advantages offered by ECC. For instance, it can achieve the same level of security using smaller keys. Therefore, less power consumption is required to do encryption or create a digital signature.

Before trying to explore more deeply into attacks on ECDLP, a brief overview of what ECC is and how ECC works to encrypt and decrypt messages is necessary.

Elliptic curve cryptography applies to curve points (x, y) where x and y satisfies formulas

$$y^2 \equiv x^3 + ax + b \ (mod\ p) \tag{1}$$

$$4a^3 + 27b^2 \neq 0 \tag{2}$$

and p is a prime number. The security of ECC is ensured by ECDLP, which states that knowing the private key k and a random base point P on a given elliptic curve, it is easy to compute the public key Q using the formula

$$\mathrm{Q} = k \cdot p \tag{3}$$

However, it is much harder to calculate k knowing P and Q, especially when p is a large prime number, so attempts to attack ECC are difficult to achieve.

The following is a simplified example of using point addition and point doubling to encrypt and decrypt messages. Actual implementations can be much more complicated. To use ECC, one should share the public key Q, the elliptic curve used--values of $a, b, p,$ and the base point P openly. At the same time, one should keep the private key k in secret. With all information except the private key, one can perform computations on curve points using point addition and point doubling. They help to do operations between curve points. Point addition applies to two different points. For two curve points $M = (x_1, y_1)$, $N = (x_2, y_2)$, the gradient of the line connecting M and N is

$$m = \frac{y_2 - y_1}{x_2 - x_1} \ (mod\ p) \tag{4}$$

Point doubling applies to two same points. For $H = (x_1, y_1)$,

$$m = \frac{\partial y}{\partial x} = \frac{3{x_1}^2 + a}{2y_1} \ (mod\ p) \tag{5}$$

The result of $M + N$ or $2H$ is (x_3, y_3), where

$$x_3 = m^2 - x_1 - x_2 \ (mod\ p) \tag{6}$$

$$y_3 = m(x_1 - x_3) - y_1 \ (mod\ p) \tag{7}$$

Combining these two algorithms, one can compute operations between curve points and do direct encryption and decryption. To make these operations well-defined, the curve must be non-singular.

With the help of point addition and point doubling, the public key can be generated, and encryption and decryption can be done. To generate a public key, one can simply apply formula 2.

To encrypt a message, one firstly maps the message to a specific point on the curve. Then, one picks an arbitrary natural number a sends (C_1, C_2), where

$$C_1 = a \cdot P \ , C_2 = M + a \cdot Q \tag{8}$$

as cyphertext. To decrypt a message, one computes

$$M = M + a \cdot k \cdot P - a \cdot k \cdot P = C_2 - k \cdot C_1 \tag{9}$$

The security level of ECC almost entirely ensured by the difficulty of solving ECDLP. Consequently, an analysis of the attack methods to solve ECDLP is essential for practical cryptographic applications. Specifically, analysis on attack methods such as Exhaustive Search, Baby-Step Giant-Step (BSGS) algorithm, and Pollard's Rho algorithm establishes a base level of security and helps to determine the minimum size of private keys required for a given security level.

This paper provides an overview and analysis of these attack methods on ECDLP. By collecting and analyzing both advantages and disadvantages of these attack methods, this paper aims to serve as a reference for other researchers interested in this topic.

2. Mathematical Foundation of ECC

2.1. Definition of EC

As its name suggests, Elliptic curve cryptography relies on an elliptic curve to do encryption and decryption. The general Weierstrass equation over a field can be written is $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ [2]. It also has a simplified form $y^2 = x^3 + ax + b$ [3].

Elliptic curve is useful in many tools in cryptography, such as ECC and Elliptic Curve Digital Signature Algorithm (ECDSA) [3][4].

2.2. Discrete Logarithm Problem and Elliptic Curve Discrete Logarithm Problem

2.2.1 Discrete Logarithm Problem (DLP)

The Discrete Logarithm Problem (DLP) is a fundamental problem in cryptography. It is defined within the context of finite cyclic groups. Given a generator g and an element h, the DLP aims to look for an integer x such that

$$g^x \equiv h \ (mod\ p) \tag{10}$$

The computational difficulty of finding such x is the base of many public-key schemes.

2.2.2 Elliptic Curve Discrete Algorithm Problem (ECDLP)

The Elliptic Curve Discrete Algorithm Problem (ECDLP) is an analogue of the DLP on elliptic curves. Given an elliptic curve E over a finite field, a base point P, and another point Q on E, the ECDLP asks for an integer k which satisfies formula 2.

Just like the point addition and point doubling, which can be regarded as a special case of point addition, explained in the previous section, the scalar multiplication in the ECDLP plays the same role as the modular exponentiation in the DLP.

It is believed that for similar key sizes, solving the ECDLP is significantly harder than solving the DLP [5]. Therefore, the ECC achieves similar security level with much smaller parameters, making it more efficient in practice.

2.3. Difficulty of Solving the ECDLP

Since elliptic points addition has no straightforward inverse formula that expresses the integer k in terms of P and Q, the relation between k and Q is non-linear.

Unlike the classical DLP, the coordinates of points are defined by solutions to the Weierstrass equation

$$y^2 \equiv x^3 + ax + b \ (mod\ p) \tag{11}$$

and the group operation depends on functions of these coordinates. In particular, the operation of point addition on an elliptic curve involves computing slopes, modular inverses, and rational functions, which mixes the coordinates x and y so that one cannot simplify the equation to find a linear relationship between k and Q. This non-linear structure makes it difficult to solve the ECDLP.

In addition, the search space is extremely large. The order of the base point P can be chosen close to the size of the field, which can reach 2^{256} for modern cryptographic system [6]. According to Hasse's Theorem, the number of points on an elliptic curve over a finite field is bound around the field size, allowing the base point P to generate a subgroup that has a very large prime order [7]. It enforces attackers to consider the entire group order instead of breaking it into small factors. In order to determine k, an exponentially large number of possibilities must be worked with. There is no known mathematical relation that is able to significantly reduce the huge workload [8].

As a result, the ECDLP is thought to be more resistant to attacks than the DLP, which makes ECC more secure for the same key size.

3. Attack Methods on ECC

The most straightforward attack method to any cryptographic technique is by Exhaustive Search, also known by brute force search. By using exhaustive search, one tests every possible k by computing successive multiples of the base point P until the result matches with Q.

A more efficient method is the Baby-Step Giant-Step (BSGS) algorithm [9]. It is based on the idea that splitting k in the range $[0, n-1]$ into two parts:

$$k = i \cdot m + j \tag{12}$$

where i is the baby step index, j is the giant step index, and

$$m = \lceil \sqrt{n} \rceil \tag{13}$$

The first step is to compute and record values of jp for $j = 0, 1, 2, \cdots, m-1$. The second step is to compute $Q - i \cdot mp$ for $i = 0, 1, 2, \cdots, m-1$ and check if the result matches one of the results gained in baby steps. When a match is found, k can be calculated using formula 12.

For example, for an elliptic curve group of order $n = 13$,

$$m = \lceil \sqrt{n} \rceil = 4 \tag{14}$$

Baby steps are to compute $0P, 1P, 2P, 3P$, and giant steps are to compute $Q - 0 \cdot 6P, Q - 1 \cdot 6P, Q - 2 \cdot 6P, Q - 3 \cdot 6P$. As a result, one of these in giant steps will match a baby step, so k is determined.

Pollard's Rho algorithm is considered as the most practical attack against the ECDLP [10]. It has similar mathematical principles to the birthday paradox, which are about estimating the likelihood of collisions among a large space of values [11]. The first step is to define a partition of the elliptic curve group into subsets, where each subset has a rule. Then, starting from an initial point, a sequence of points can be made through iterations. By the birthday paradox, after a certain number of steps, a collision is very likely to occur. By setting up an equation between colliding points and rearranging their terms, one can solve for k.

For instance, for an elliptic curve group of order $n = 13$, define three subsets: if the x-coordinate $x \equiv 0\ (mod\ 3)$, add P; if $x \equiv 1\ (mod\ 3)$, add Q; if $x \equiv 2\ (mod\ 3)$, double the point.

Begin with an arbitrary point, for example, $X_0 = P$. By applying the above rules, a sequence of points $X_0, X_1, X_2, \cdots$ can be created. A collision between points in this sequence is likely to occur after about $\sqrt{n} \approx 4$ steps. Both points can be expressed in terms of P and Q, and an equation in the form of

$$a_s P + b_s Q = a_t P + b_t Q \tag{15}$$

$$(a_s - a_t)P = (b_t - b_s)Q \tag{16}$$

can be yielded. Therefore, k can be solved [12].

4. Analysis of Attack Methods on ECC

Elliptic curve cryptography can provide high security with relatively small key sizes. The security of ECC depends on the difficulty of computing the ECDLP. Over years, various methods have been developed to solve the ECDLP. Thus, analyzing the strength and weakness of each attack method is crucial for improving the resistance of ECC to attacks. The three attack methods discussed are Exhaustive Search, the BSGS algorithm, and Pollard's Rho algorithm. Each method has different advantages and disadvantages in terms of time and space complexity, which determines whether they are practical depending on the available computational resources.

Exhaustive Search is the simplest and the least feasible attack method, because its linear time complexity implies that the number of steps required scales with the order of the elliptic curve group [13]. For Exhaustive Search, the attacker tests each integer $k \in [1, n-1]$ until the formula $Q = kP$ is found. The number of operations required (time complexity) is

$$T_{ES} = n - 1 \approx O(n) \tag{17}$$

and the memory usage (space complexity) is

$$S_{ES} = O(1) \tag{18}$$

since only the current multiple of P needs to be stored. In modern cryptography, the order of the elliptic curve group often exceeds 2^{256} [6]. Even though there are some advancements in parallel processing [14], the number of required operations grows exponentially so that only using Exhaustive Search remains impractical. Furthermore, while Exhaustive Search needs minimal memory for storing points which are computed, it is negligible compared to the overwhelming computational demand [15]. Consequently, Exhaustive Search is unlikely to be a realistic threat to ECC.

The BSGS method achieves sub-linear growth in operations with respect to the group order. For the BSGS algorithm, the time complexity is

$$T_{BSGS} = O(\sqrt{n}) \tag{19}$$

and the space complexity is

$$S_{BSGS} = O(\sqrt{n}) \tag{20}$$

since $2m$ numbers of points in total need to be recorded where $m = \lceil \sqrt{n} \rceil$. While this method reduces the expected number of computations to the square root of the group order, the memory requirement grows in the same way. This requirement can become expensive for complicated elliptic curves, which limits the feasibility of using the BSGS against high security ECC systems in situations where storage ability is limited [16].

Pollard's Rho algorithm provides a balance of relatively low time complexity and low space complexity. By utilizing collision detection, it also achieves sub-linear expected time complexity while requiring negligible memory. The time complexity of Pollard's Rho algorithm is

$$T_{Rho} = O(\sqrt{n}) \tag{21}$$

and the space complexity is

$$S_{Rho} = O(1) \tag{22}$$

because, like Exhaustive Search, one only needs to store the current result of iterations and compare it with the initial point. The low memory requirement makes this algorithm feasible on resource-constrained hardware, unlike BSGS, and maintaining competitive runtime efficiency at the same time. However, despite its advantages, Pollard's Rho algorithm still cannot avoid the exponential growth in operations as the order of the elliptic curve increases, which means that sufficiently large curves remain resistant to attack [16].

Comparing these three attack strategies highlights the effective security provided by ECC. Exhaustive Search is computationally prohibitive for modern curve sizes, the BSGS method is limited by memory restrictions, and Pollard's Rho algorithm, while both efficient and scalable, is still constrained by exponential growth in group order. These limitations of attack methods collectively illustrate why ECC maintains a high level of security for commonly used key sizes of 256 bits or higher. Moreover, understanding these constraints informs the selection of curve parameters, balancing efficiency and security while mitigating potential vulnerabilities from attacks.

5. Conclusion

This paper has introduced what ECC is, the mathematical foundation of ECC, and the difficulty to solve ECDLP. Moreover, this study focuses on analyzing three attacks methods on ECDLP: exhaustive search, BSGS algorithm, and Pollards' Rho algorithm. This paper makes contributions on comparing these attack methods with respect to computational complexity.

Based on the preceding analysis, the following conclusions can be made: The security of ECC is ensured by the computational complexity of solving ECDLP. The analysis indicates that exhaustive search is impractical in real world due to its linear time complexity. Although the BSGS algorithm can reduce the time complexity, there is still an enormous space complexity requirement, which leads to prohibitive memory demand if someone wants to attack ECDLP. Finally, Pollard's Rho algorithm is confirmed as the most efficient attack method. Nevertheless, a certain parameter of ECC, such as the order of the elliptic subgroup, can be selected to protect ECC from Pollard's Rho algorithm such that it cannot be solved within a reasonable time period.

The primary impact of this paper is its role in connecting between the hardness of solving ECDLP and practical requirements for cryptographic design. By analyzing these attack methods, this paper provides a reference for other researchers. Furthermore, this study helps to dispel misconceptions about ECC by doing objective evaluations, emphasizing that its security is not absolute.

This paper also has some limitations, primarily on lacking enough practical analysis on specific elliptic curve models and other attack methods. In the future, research can focus more on other attack methods such as the MOV attack using pairings. Moreover, the emergence of quantum computing can somewhat threaten the security of ECC.

References

[1] Adeniyi, A. E., Jimoh, R. G., Awotunde, J. (2024). A review on elliptic curve cryptography algorithm for Internet of Things: Categorization, application areas, and security. Application Areas, and Security.

[2] Ahlswede, R. (2016). Elliptic Curve Cryptosystems. In: Ahlswede, A., Althöfer, I., Deppe, C., Tamm, U. (eds) Hiding Data - Selected Topics. Foundations in Signal Processing, Communications and Networking, vol 12. Springer, Cham.

[3] Yan, Y. (2022, December). The overview of elliptic curve cryptography (ECC). In Journal of Physics: Conference Series (Vol. 2386, No. 1, p. 012019). IOP Publishing.

[4] Hankerson, D., Menezes, A. (2025). Elliptic curve cryptography. In Encyclopedia of Cryptography, Security and Privacy (pp. 783-784). Cham: Springer Nature Switzerland.

[5] Miller, V. S., Koblitz, N. (1985). As cited in Discrete Logarithm Problem – Cryptographic Pairings Efficiency: DLP Security.

[6] Smith-Tone, D. (2023). NIST Special Publication 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. National Institute of Standards and Technology.

[7] Silverman, J. H. (2009). The arithmetic of elliptic curves (Vol. 106, pp. xx+-513). New York: Springer.

[8] Galbraith, S. D., Gaudry, P. (2015). Recent progress on the elliptic curve discrete logarithm problem. IACR Cryptology ePrint Archive, Paper 2015/1022.

[9] Jindal, A., Jatain, A., Bajaj, S. B. (2023, October). Method for Solving the ECDLP. In Proceedings of International Conference on Paradigms of Communication, Computing and Data Analytics: PCCDA 2023 (p. 275). Springer Nature.

[10] Sadkhan, S. B. (2021, February). A Proposed Developments of Pollards Rho Method for Attacking the ECDLP. In 2021 7th International Engineering Conference “Research & Innovation amid Global Pandemic"(IEC) (pp. 151-155). IEEE.

[11] Josodipuro, M. J., Saputra, K. V. I., Lukas, S. (2022, September). Statistical Analysis of Pollard's Rho Attack on Elliptic Curve Cryptography. In 2022 1st International Conference on Technology Innovation and Its Applications (ICTIIA) (pp. 1-6). IEEE.

[12] Nickerson, D. (2020). Collision detection and Pollard's rho.

[13] Lv, M., Sun, H., Xin, J., Zheng, N. (2020). Efficient repair analysis algorithm exploration for memory with redundancy and in-memory ECC. IEEE Transactions on Computers, 70(5), 775-788.

[14] Kang, M., Park, D. (2021). Lightweight Microcontroller with Parallelized ECC-Based Code Memory Protection Unit for Robust Instruction Execution in Smart Sensors. Sensors, 21(16), 5508.

[15] Dossou-Yovo, V., Nitaj, A., Togbé, A. (2022, October). Finding Points on Elliptic Curves with Coppersmith’s Method. In International Conference on Algebraic Informatics (pp. 69-80). Cham: Springer International Publishing.

[16] Katti, J. (2015). Attacks on Elliptic Curve Cryptography Discrete Logarithm Problem (EC-DLP). International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 3(4), 1–5.