Proceedings of the 2023 International Conference on Mathematical Physics and Computational Simulation
DOI: 10.54254/2753-8818/10/20230327

General analysis on essential mathematical principles of elliptic curve cryptography

Huangwei Wu

Nantong High School, Nantong, Jiangsu Province, 226000, PRC

wuhuangwei123@163.com

Abstract: Prevalent is the practical application of Elliptic Curve Cryptography (ECC) in the modern public-key cryptosystem, especially the implementation of ECC algorithm in Bitcoin source code. With the thorough introduction of discrete logarithm and Diffie-Hellman key exchange, ECC has gradually progressed to be sophisticated and efficient simultaneously. Therefore, it currently has been widely regarded as the successor of RSA algorithm in terms of inheritance for its shorter lengths of keys, faster speed and higher safety under the same encryption strength. Due to the potential safety and complexity of Elliptic Curve Cryptosystem, it is apparently noticed that there is included a large volume of Maths principles related to the establishment of ECC algorithm. As a consequence, this paper will mainly focus on qualitative research and exemplary analysis to specifically elucidate the general knowledge on essential mathematical principles of ECC, including the Law of Addition, the Elliptic Curve Discrete Logarithm Problems (ECDLP) and the Elliptic Curve ElGamal (EC ElGamal), together with the corresponding applications combined with their deprivation processes.

Keywords: mathematics, Elliptic Curve Cryptography, discrete logarithm, elgamal, law of addition.

1. Introduction

In the digital era aiming to simplify the communications among users of electronic devices, the penetration rate of heterogeneous network has witnessed a dramatic increase in the past decades [1]. Correspondingly, due to the constructive demand of security and privacy maintenance amid the public internet users, in 1985 Neal Koblitz and Victor Miller independently developed a brand new public key cryptosystem named Elliptic Curve Cryptography (ECC), which is the most typical algorithm allowing the complexity of ECDLP to guarantee the high information security [1-3]. Since the complicated cryptosystem involves a wide range of functions including error detection, image decode, small grid establishment and so on [3-5], the sophisticated ECC algorithm is consisted of divergent principles worth further explorations and illustrations.

As a result, the Elliptic Curve Cryptography is applied in both software and hardware, which has successfully overcome the shortcoming in current cryptographic methods revealed by Mathematical cryptanalysis [3], will be the topic on which this paper consistently focuses to generally analyze its fundamental principles beneficial for a better understanding about the foundation of ECC. Based on the relevance sequence, the main body of the article will be divided into four sections: (1) the elliptic curve cryptography, in which the origin and definition of ECC will be identified; (2) the law of

DOI: 10.54254/2753-8818/10/20230327

addition, which is different from the calculation law of Euclidean space; (3) ECDLP, a Mathematical problem widely regarded as the security root of ECC encryption [3]; and (4) EC ElGamal, a typical transplant of the elliptic curves practically used in modern cryptosystem.

After a comprehensive illustration using qualitative research and exemplary analysis, the research will possibly assist the readers in better understanding Mathematical principles of the Elliptic Curve Cryptography, and stimulate the further development of ECC to obtain a more reliable cryptosystem by which the network communications through plaintext and ciphertext will become by far safer.

2. Elliptic curve cryptography

ECC, an algorithm based on elliptic curve mathematics for establishing public-key cryptography, entered wide use from 2004 to 2005 after it had been initially proposed by Neal and Victor in 1985 [6].

2.1. Elliptic curve origination

Elliptic curve, which dominates no physical resemblance with an ellipse, is a descendant term originating from the close association with the cubic algebra elliptic equation describing the perimeter of an ellipse [7]. In detail, the perimeter formula of an ellipse can be written in the form below:

$$L = 4a\int_0^{\frac{\pi}{2}}\sqrt{1-e^2\sin^2\theta}\,d\theta = 4aE\left(e,\frac{\pi}{2}\right) \quad (1)$$

the polynomial $E(e,\frac{\pi}{2})$ is named the Second Complete Elliptic Integral, guaranteeing the existence of an equation in the form of $y^2 + aty + by = t^3 + ct^2 + dt + e$, which satisfies:

$$f(x) = \int_c^x R\left|t,\sqrt{t^3+ct^2+dt+e}\right|dt \quad (2)$$

Therefore, the common elliptic curve used in cryptography is witnessed: $y^2 = x^3 + Ax + B$, which vividly elucidates the reasons for the name “Elliptic Curve” [8].

2.2. Elliptic curve in cryptography

As the article mentioned before, the Elliptic Curves Cryptography uses the curve equations in the form of $y^2 = x^3 + Ax + B$ (A, B are the constant) most frequently, which is known as Weierstrass equation where the elliptic curve is required to be non-singular (i.e., no tip, no self-intersection, no isolated point) [2]. Thus, this condition is equivalent to [1]:

$$4a^3 + 27b^2 \neq 0.$$

In addition, since the cryptographic operation on elliptic curves are done over finite field through coordinate points on elliptic curve, the equation can be transformed into [2, 4]:

$$y^2 = \{x^3 + ax + b\} \bmod\{p\}.$$

So we can use point set Ep (a,b) to represent the elliptic curve:

$$\{(x,y)|0 \le x \le p, 0 \le y \le p, \text{and } x, y \text{ are both integers}\}\sqcup 0$$

This process empowers the geometric elliptic curves to be shifted into algebra set located in finite field, which makes it possible to be combined with number theory [1, 2, 9].

3. Law of addition

3.1. Four operations in fields

Following are the four Operations in Fields. Addition and Multiplication: the same as the four operations for Euclidean space. Subtraction: require modulo operations for negative numbers: based on definition. Division: require modulo operations for fractions: based on inverse of fraction.

Example:

Find the value of a, in which $(-\frac{1}{2})^2 - 3 - 9 = 4^{-1} + (-12) = 6 + (-12) \equiv a \bmod 23$

Modulo of negative numbers: As (-6) = 23×(-1) + 17, getting $(-6) \equiv 17 \bmod 23$ according to definition;

Modulo of fractions: As $(4 \times 6) \bmod 23 = 1$, getting 4-1 = 6, 6 is the inverse of 4 under modulo 23;

DOI: 10.54254/2753-8818/10/20230327

Hence it is easy to obtain: $(-\frac{1}{2})^2 - 3 - 9 = 4^{-1} + (-12) = 6 + (-12) \equiv 17 \bmod 23$;
Thus, the value of a is 17, easy to be calculated [1, 10].

3.2. Point addition

3.2.1. Definition 1. If P, Q ∈ Ep (k, m), then
M + O = M
If M = (a, b), (a, b) + (a, -b) = O, that is, (a, -b) is the inverse of M under addition, denoted -M
If M = (a1, b1), N = (a2, b2), M ≠ N, then M + N = (a3, b3)

3.2.2. Formula. As the paper has mentioned in 3.2.1., the two point M = (a1, b1) and N = (a2, b2), M + N = (a3, b3) can be precisely calculated by the regular formula below:

$$a_3 = \{\mu^2 - a_1 - a_2\} \bmod p$$
$$b_3 = \{\mu(a_1 - a_3) - b_1\} \bmod p$$

In which:

$$\mu = \frac{b_2 - b_1}{a_2 - a_1} \bmod p$$

3.3. Point doubling

3.3.1. Algebra formula. Similar with *3.2.2.*, the two points, which have the same coordinates, M = (a1, b1) and N = (a1, b1), M + N = (a3, b3) is defined by the following calculation:

$$a_3 = \{\mu^2 - 2a_1\} \bmod p$$
$$b_3 = \{\mu(a_1 - a_3) - b_1\} \bmod p$$

In which:

$$\mu = \frac{3a_1^2 + k}{2b_1} \bmod p$$

Geometric Example [11]: Question: $y^2 = x^3 + 3x + 5;\ P = (-1,1)$, calculate 2P

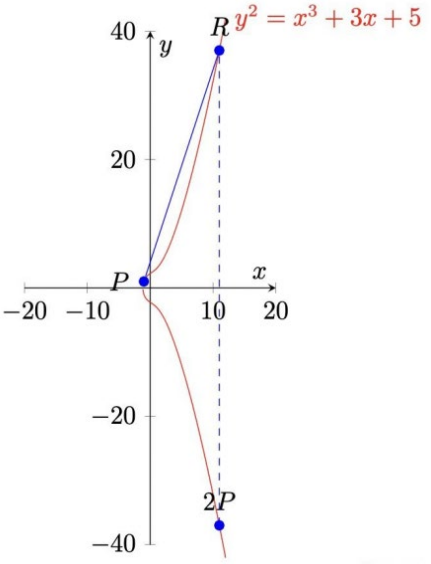

Figure 1. The geometric example.

The common steps of the calculation is as follows:
Find the tangent over point P by derivation : y' = 3x2 + 3;
Find another intersection of the tangent and elliptic curves;
Find the point Q, which satisfies: Q and R are symmetric with respect to the x-axis;

DOI: 10.54254/2753-8818/10/20230327

Therefore, according to the law of addition, Q = 2P.

These are the corresponding Process:

Derivation: $f'(-1) = 3 \times (-1)^2 + 3 = 6$

Get the tangent equation: PR: $y = 6x + 12$

System of simultaneous equations :

$$\begin{cases} y = 6x + 12 \\ y^2 = x^3 + 3x + 5 \end{cases}$$

Calculate the result: $x = x_{2p}$, $y = -y_{2p}$

3.4. Point multiplication

Point multiplication can be a function based on Point Addition: If M is a point on an elliptic curve, the multiplication over M is calculated by the repeated addition [2]:

$$nM = M + M + M + \cdots + n \text{ times}$$

4. Elliptic curve discrete logarithm problem

4.1. Discrete logarithm problem (DLP)

4.1.1. Discrete logarithm. If there exists a random integer p being relatively prime to q, while n is a primitive root of q, exactly a number μ among the sequence 0, 1, 2, ...,$\Phi(n) - 1$, in which $\Phi(n)$ is named as a totient function, can be recognized to satisfy that $p \equiv n^{\mu}(mod\ q)$. Thereby, the number μ is then defined as the discrete logarithm of p with respect to the base n modulo q, denoted $\mu = ind_n p(mod\ q)$ [12].

4.1.2. Mathematical principles of discrete logarithm encryption. Given positive integers x, y, p > 1, to find the positive integer k > 1, satisfying: $y \equiv x^k(mod\ p)$.

x is the base; k is the private key; y is the public key:

If we know the value of x , k (private key), it is easy to find y (public key), decrypted.

If we know the value of x , y (public key), it is complex to find k (private key), hard to crack [1].

4.2. Elliptic curve discrete logarithm problem (ECDLP)

4.2.1. Definition 2. & encryption principles. ECDLP, which is regarded as the essential mathematical principle of elliptic curve encryption, can be reflected in the form: P, Q are the points on the elliptic curve; k is an integer, satisfying : Q = kP, in which P is the base point, k is the private key, and Q is the public key.

Given k and P, according to the addition laws, it is easy to find Q.

Given P and Q, it is hard to find k (the p in ECC is too large to exhaustively cite k by hand).

4.2.2. Isomorphism attack (IA). Isomorphism Attack can be divided into Prime-field-anomalous Attack, WTP attack, Gaudry, Hess and Smart Weil Descent Attack, while all of them together synchronously aim to simplify ECDLP [1].

If there exist two elliptic curves which are simultaneously defined over K, such as:

$$E_1: y^2 + a_1xy + a_3y = x^3 + a_2x^3 + a_4x + a_6$$

$$E_2: y^2 + \bar{a_1}xy + \bar{a_3}y = x^3 + \bar{a_2}x^3 + \bar{a_4}x + \bar{a_6}$$

E1 and E2 are called isomorphic over K [1].

The relation between isomorphism and elliptic curves is an equivalent relation defined over K, If there exist two isomorphic elliptic curves (E1 and E2) exist, subsequently their groups E1(K) and E2(K) of K-rational points must be also isomorphic [1, 3].

DOI: 10.54254/2753-8818/10/20230327

Through Isomorphism Attack, ECDLP can be simplified to the corresponding DLP, while these attacks are unique in producing ECDLP solvers which are better than Pollard's rho algorithm for certain elliptic curves [1, 3, 10].

5. EC ElGamal

5.1. Diffie-hellman-merkle key exchange (DHM)

With the help of the secure DHM protocol, two parties can generate a key via an unsecure channel without knowing anything about one another beforehand. In subsequent communications, this key may be used as a symmetric key to encrypt the communication's content [1].

The process is as exemplified as below [2]:

Alice and Bob decide a prime number p and choose a Q on the curve, making p and Q public:

$$E_p: y^2 = x^3 + Ax + B(\mathrm{mod}\ p)$$

Alice and Bob randomly select an integer NA and NB respectively, and keep them not disclosed.

Alice calculates QA=NA·Q (NA·Q refers to N times Q, same way as finding 2P), send it to Bob.

Bob calculates QB=NB·Q, and sends it to Alice.

Bob calculates NA·QB; Alice calculates NB·QA

Therefore, Alice and Bob get the public key:

$$N_A Q_B = N_A(N_B Q) = (N_A N_B)Q = (N_B N_A)Q = N_B(N_A Q) = N_B Q_A$$

5.2. ElGamal

ElGamal encryption algorithm is an asymmetric encryption algorithm based on the Difi-Hermann (DHM) key exchange. In 1985, Taher Elgamal proposed the ElGamal algorithm in his paper "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"[2].

The safety of ElGamal depends on discrete logarithm problem (DLP) on G, which is an Abelian group of prime order p and g is a generator of G, while ElGamal is consisted of 3 parts, including key generation, encryption and decryption [1].

5.3. EC ElGamal

Elliptic Curve ElGamal is one form of ECC, in which the ElGamal is transplanted to an elliptic curve [1]. Specifically, the concept of EC ElGamal was initially proposed by Neal Koblitz in his paper "Elliptic Curve Cryptosystems" in 1997 [2].

The safety of EC ElGamal depends on the elliptic curve discrete logarithm (ECDLP) on G, while it can be similarly divided into key generation, encryption and decryption as well [4].

5.3.1. Key generation process. Select a elliptic curve to obtain Ep(a, b), embed the plaintext information m into the point Pm on the curve, and then perform an encryption transformation on the point Pm. Take a generator G of Ep(a, b), Ep(a, b) and G as the public parameters, and User A selects: nA as the private key; PA = nAG as the public key [2].

5.3.2. Encryption process. User B firstly sends a message Pm to User A, selects a random positive integer, and generates the following points as ciphertext [4]:

$$C_m = \{kG, P_m + kP_A\}$$

5.3.3. Decryption process. Subtract the multiplication of the first point with the private key from the second point in the ciphertext point pair, then it is easy to obtain:

$$P_m + kP_A - n_A kG = P_m + k(n_A G) - n_A kG = P_m$$

As the definition emphasized, here multiplied does not equal to simple multiplication in algebra; instead, it should be restricted by the point multiplication mentioned in 3.4., based on point addition.

DOI: 10.54254/2753-8818/10/20230327

6. Conclusion

In this paper, basic principles of Elliptic Curve Cryptography have been concisely covered, combining number theory, group theory and elliptic curve together to introduce a frequently-witnessed cryptosystem in modern information world. According to ECC's complexity and efficiency which have outperformed those of RSA, elliptic curve cryptosystem will make the network communication much safer and more private. Consequently, the Mathematical principles, including point addition, ECDLP, EC ElGamal, to name but a few, are basically elucidated in the article from the perspectives of concept, definition, application and so on. This paper is likely to be helpful especially for novices majoring in Cryptography due to the applied qualitative research and exemplary analysis. Additionally, through the horizontal comparison with RSA, it can be clearly noted that the advantages of ECC are predominant, which deserve a more comprehensive research in the next paper.

Acknowledgement:

Sincere thanks for Prof. Paolo Cascini from Imperial College London, who assists the article in fundamentally establishing a basic framework according to the relevant cryptography lemmas and algorithms. Special appreciation for Prof. Zhenyu Guo from Xi'an Jiaotong University, who inspires the paper to focus on elliptic curve cryptosystem through a view of number theory and a strategy of exemplary analysis. Earnest thanks for Miss. Zhiyun Deng, who reinforces the knowledge foundation of the essay by patiently answering the questions after lectures. Particular appreciation for Mr. Ziru Xing, who carefully guides and subsequently checks the structure, grammar and citation of the whole essay, ensuring the article to be academic and normative.

References:

[1] Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review, 47, 100530. https://doi.org/10.1016/j.cosrev.2022. 100530

[2] Singh, L. D., & Singh, K. M. (2015). Implementation of text encryption using elliptic curve cryptography. Procedia Computer Science, 54, 73–82. https://doi.org/10.1016/j.procs. 2015. 06.009

[3] Saudy, N. F., Ali, I. A., & Barkouky, R. A. (2019). Error analysis and detection procedures for elliptic curve cryptography. Ain Shams Engineering Journal, 10(3), 587–597. https://doi. org/10.1016/j.asej.2018.11.007

[4] Singh, L. D., & Singh, K. M. (2015). Image encryption using elliptic curve cryptography. Procedia Computer Science, 54, 472–481. https://doi.org/10.1016/j.procs.2015.06.054

[5] Khan, A. A., Kumar, V., & Ahmad, M. (2022). An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. Journal of King Saud University - Computer and Information Sciences, 34(3), 698–705. https://doi.org/ 10.1016/j.jksuci.2019.04.013

[6] Introduction and overview. (n.d.). Springer Professional Computing, 1–23. https://doi.org/ 10.1007/0-387- 21846-7_1

[7] Unger, D. J. (2022). Yield criteria representable by elliptic curves and weierstrass form. Procedia Structural Integrity, 35, 2–9. https://doi.org/10.1016/j.prostr.2021.12.041

[8] Elliptic curve. from Wolfram MathWorld. (n.d.). Retrieved March 15, 2023, from https://mathworld.wolfram.com/EllipticCurve.html

[9] Tadmori, A., Chillali, A., & Ziane, M. (2015). Cryptography over the elliptic curve ea,b(a3). Journal of Taibah University for Science, 9(3), 326–331. https://doi.org/10.1016 /j.jtusci.2015.02.005

[10] Taqi, S. A., & Jalili, S. (2022). LSPA-SGS: A Lightweight and secure protocol for authentication and key agreement based elliptic curve cryptography in smart grids. Energy Reports, 8, 153–164. https://doi.org/10.1016/j.egyr.2022.06.096

DOI: 10.54254/2753-8818/10/20230327

[11] css-uodor8{border-radius:50%;}.css-1y9jkzv{box-sizing:border-box;margin:0;min-width:0;max-width:100%;height:auto;background-color:#FFFFFF;width:38px;height:38px;border-radius:50%;}zhuoyuechengjiu.css-1cd9gw4{margin-left:.3em;}liuxuegou. (n.d.). elliptic curve cryptography. zhihuzhuanlan. Retrieved March 16, 2023, from https://zhuanlan.zhihu.com/p/443011441

[12] Discrete logarithm. from Wolfram MathWorld. (n.d.). Retrieved March 16, 2023, from https://mathworld.wolfram.com/DiscreteLogarithm.html