Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 1, pp. 343–348
DOI : 10.47974/JDMSC-2600

A novel public key cryptosystem considering elliptic curve principles

Pauly J. *
Saju M I †
Antony John E F §
Renjith Varghese ‡
Department of Mathematics
St. Thomas College (Autonomous)
Affiliated to University of Calicut
Thrissur 680001
Kerala
India

Abstract

The unique public key cryptosystem presented in this work is built on the fundamental concepts of elliptic curves. The proposed method aims to offer a versatile and efficient Public Key Cryptography (PKC) solution by utilizing the inherent properties of elliptic curves. The mathematical foundations of elliptic curves are reviewed, with particular emphasis on their suitability for cryptography applications. This work improves the study of elliptic curve principles in the design of public key cryptosystems by providing a fresh perspective on generating efficient cryptographic solutions without compromising security.

Subject Classification: *11G07, 94A60, 15A09.*

Keywords: *Elliptic curves, Elliptic curve discrete logarithm problem (ECDLP), Public key-cryptography (PKC), Rectangular matrix.*

1. Introduction

Securing data is of utmost importance today, where constant surveillance leaves virtually every spoken sentence susceptible to interception. Consequently, maintaining confidential communication becomes an exceedingly challenging

* *ORCID-ID:* `0000-0003-1647-1029`

* *E-mail:* `jincy.pauly@gmail.com (Corresponding Author)`
† *E-mail:* `sajumambilly@gmail.com`
§ *E-mail:* `antonyjohnef@gmail.com`
‡ *E-mail:* `renjithvarghese8@gmail.com`

© Taru Publications

task. In such scenarios, the implementation of encryption becomes imperative. Currently, there are various cryptosystems in existence, broadly classified into two types: "private-key cryptosystem" and "public-key cryptosystem."

Private key encryption, within the realm of cryptosystems, offers several advantageous features. Notably, its resistance against brute-force and dictionary attacks is heightened by greater entropy, or randomness, and the utilization of longer private keys.

Despite the benefits, symmetric key cryptosystems present a drawback in the challenge of managing keys, as each user necessitates a unique key. PKC was introduced by Diffie and Hellman as a solution to this problem in their landmark work [1], and a great deal of study was done in this field thereafter [2]–[6] .

In terms of computational efficiency, symmetric-key encryption, with its public-private key pairings, surpasses asymmetric encryption in speed. Many cryptographic operations employ private key encryption for securing data transfers. Additionally, the secure exchange of secret keys is often facilitated using a public key technique.

One disadvantage of PKC is the larger key size. Current research efforts are focused on finding solutions to the primary size-related problems to get around this restriction. In 1985 Koblitz [7] and Miller [8] independently proposed the use of elliptic curves for cryptography. Because of its reduced key size, elliptic curve encryption is becoming more popular. ECC provides the same level of security as traditional PKC methods but with reduced key sizes. ECC should also be given more consideration because of its quick speed, low power consumption, and little storage needs. The discrete logarithm issue on an elliptic curve serves as the security assumption for systems based on elliptic curves. Numerous researchers created ECDLP-based systems [9]– [12].

In order to strengthen public key cryptosystems, recent research has investigated strong algebraic and elliptic structures. To improve security, Mittal et al. [15] combined the NTRU technique with group ring algebra to create new challenging issues including inverse computation in group rings and discrete logarithm. Küsmüş and Hanoymak [16] created a Bass cyclic unit-based cryptosystem that combines elements of RSA and ElGamal. To increase key security and efficiency, they used non-commutative operations in dihedral group rings. Using the elliptic curve matrix discrete logarithm problem (ECM-DLP), Luhaib and Ajeena [17] extended these concepts by including elliptic curve matrices (ECMs) to strengthen EC–DL–based systems and achieve more robustness. Collectively, these elements show how elliptic curve and group ring integrations can be used to create cryptographic frameworks that are more resilient and robust.

Rectangular matrices, their pseudo-inverse, and modular operations over prime fields are used by Pauly et al. in [6] to ensure security. As a result, authors are encouraged to create systems with non-commutative structures to ECC. The goal of this work is to create a public key cryptosystem based on elliptic curves over a finite field while addressing the discrete logarithm problem's difficulties.

Section 2 of the article explains the requirements needed to understand this topic. The suggested method is explained in Section 3, 4, and 5. The suggested system is illustrated in the sixth section. The security of the proposed system has been covered in section 7. Finally, this theoretical investigation is summarized and concluded in section 8.

2. Preliminaries

2.1. *Elliptic curves* [13]

Weierstrass equations are commonly used to represent elliptic curves. Let F be a field such that $y^2 = x^3 + ax + b$, where $a, b \in F$. If the curve is non-singular and the field is not characteristic 2 or 3. The desired geometric qualities of not having cusps or self-crossings are provided by non-singularity, which implies algebraically that the discriminant $\Delta = -16(4a^3 + 27b^2)$ must not be zero.

2.2. *Elliptic curves over finite field* [13]

Elliptic curves over finite fields give finite abelian groups.

For instance, the curve $y^2 = x^3 + 2x + 3$ over F_{11} is {∞, (0, 5), (0, 6), (2, 2), (2, 9), (3, 5), (3, 6), (4, 3), (4, 8), (6, 0), (8, 5), (8, 6), (10, 0)}

2.3. *ECDLP* [13]

An elliptic curve is E over F_q. The ECDLP finds a solution m to the equation $kG = S$ for given points $G, S \in E$. Despite intense investigation since the mid-1980s, collision algorithms with $O(\sqrt{q})$ steps are the fastest known algorithms for solving the ECDLP on generic curves. Consequently, the best algorithms for solving the ECDLP in E have running times that are exponential in $\log q$. This property is the primary advantage of using elliptic curves in encryption.

Example: Consider the elliptic curve discribed in 2.2, the ECDLP of $(4, 3)$ under the base $(4, 8)$ will be 8.

3. Crafting public and private key pairs

First and foremost, the two participants in the conversation—Sandie and Jessiya—need to fix the prime number, elliptic curve $(E_p(a, b))$, and code table [14] they want to utilize. It is anticipated that the user Sandie, who desires to receive the message, will generate the public and private key pairs. For that Sandie Choose a $m \times 1$ matrix K_{pub} so that its left inverse K_{pri} exists modulo the number of points on the elliptic curve $(\#(E_p(a, b)))$, with its entries being integers less than or equal to $(\#(E_p(a, b)))$. This is going to be a public key. Additionally, choose a random integer s that is less than or equal to $(\#(E_p(a, b)))$. Next, locate point sG on the curve, where G is the curve's generator. Subsequently the public key will be (K_{pub}, sG, G) and private key will be (K_{pri}, s).

4. Encryption

Let's say Jessiya has to talk to Sandie. To achieve this, Jessiya must randomly choose an integer j that is either less than or equal to $(\#(E_p(a,b)))$. For the very next, Jessiya uses a code table to translate the meaningful message into points on an elliptic curve. Sandie's K_{pub} has order $m \times 1$, thus Jessiya must divide the translated message into m blocks and use the following equations to encrypt each block individually.

For one block M,

$$C_1 = code\ equalalnce\ of\ (K_{pub}.M + (jG)^{-1}.J_m) \tag{1}$$

where J_m be $m \times m$ matrix of all entries 1.

$$C_2 = sG + jG \tag{2}$$

Then the cipher text will be $C = (C_1, C_2)$.

5. Decryption

Sandie needs to do the following actions to decode the message $C = (C_1, C_2)$:

First find

$$C_2' = C_2 + (sG)^{-1} \tag{3}$$

$$C_1' = C_1 + C_2'.J_m \tag{4}$$

Then $M = K_{pri}.C_1'$, using code table the communicated message can be retrieved.

6. Illustration

Jessiya wants to send the message "LOVE" to Sandie using the public-key $\left((9\ 4\ 5\ 3)^T, (22,19), (27,41)\right)$ published by Sandie. For that Jessiya use prime of $p = 43$, an elliptic curve $E_{43}(5,9)$ as well as a code table that they agree prior to conversation.

For the encryption process Jessiya convert message using code table and make matrix $M = ((0,40)\ (40,28)\ (7,0)\ (34,3))$ then select $j = 20$.

Using equations (1) and (2) the cipher text sent to Sandie will be

$$C = (*\ 1by2\&x\ *\ \&kbepyb!, (23,6))$$

Upon the reception of C Sandie do equation (3) and (4) using private key ((3 4 8 2),38) and code table, reads the message "LOVE" without any corruption.

7. Security

The computational difficulties of finding the right left inverse of a row matrix and the ECDLP are the foundations of the suggested system.

In a brute force attack, the attacker looks for the original message by attempting to decrypt the encrypted message through trial and error. The secret key in the suggested technique is obtained by the attacker if they correctly predict the left inverse of the public matrix. As the matrix size increases, it is

harder for the attacker to test every scenario. This guarantees the security of the suggested system against brute force assaults.

Despite the discovery or inference of one or more simple texts, the private key matrix T remains elusive. It will therefore be more difficult to defeat the CPA assault if the suggested strategy is used. The fact that decisions are made randomly also strengthens the system's defense against side channel attacks

8. Conclusion

Mathematical complexity at the foundation determines the cryptographic system's strength exclusively. An innovative and captivating cryptosystem has been developed, based on ECDLP. The encryption technique is simple, but decryption is intricate and challenging to calculate. According to the proposed cryptosystem, the selected public key must be a noninvertible matrix. Prime number and the elliptic curve determine how strong the system is. Increases in the prime and the number of points on the elliptic curve will make the recommended system safer.

Acknowledgment

The corresponding author acknowledges Department of Science & Technology, Government of India for financial support under 'WISE Fellowship for Ph.D.' programme to carry out this work".

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," in Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, pp. 365–390 (2022).

[2] L. R. Celemín, "McEliece Cryptosystem," Citeseer (2011).

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126 (1978).

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472 (1985).

[5] M. I. Saju, R. Varghese, and E. F. A. John, "A design of public key cryptosystem in an algebraic extension field over a finite field using the difficulty of solving DLP," *Malaya Journal of Matematik*, vol. 8, pp. 459–463 (2020).

[6] J. Pauly, M. I. Saju, R. Varghese, and E. F. A. John, "Design of public key cryptosystem based on the underlying mathematical complexity,"

Journal of Discrete Mathematical Sciences and Cryptography, vol. 28, no. 3, pp. 973–984 (2025).

[7] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209 (1987).

[8] V. S. Miller, "Use of elliptic curves in cryptography," in Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Springer, pp. 417–426 (1985).

[9] R. Haakegaard and J. Lang, "The elliptic curve Diffie-Hellman (ECDH)," [Online]. Available: https://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Haakegaard+Lang.pdf, December (2015).

[10] G. Filippone, "On the discrete logarithm problem for elliptic curves over local fields," arXiv preprint arXiv:2304.14150 (2023).

[11] S. Aikins-Bekoe and J. B. Hayfron-Acquah, "Elliptic curve Diffie-Hellman (ECDH) analogy for secured wireless sensor networks," *International Journal of Computer Applications,* vol. 176, no. 10, pp. 1–8 (2020).

[12] M. S. Hijazi, N. Tahat, A. A. Tahat, R. Raft, and E. S. Ismail, "Authenticated encryption scheme based on ECDLP and DLP," *Applied Mathematics and Information Sciences*, vol. 14, no. 3, pp. 425–430 (2020).

[13] J. H. Silverman, "The Arithmetic of Elliptic Curves," 2nd ed., vol. 106, Springer, June (2009).

[14] D. S. Kumar, C. Suneetha, and Chandrasekhar, "Encryption of data using elliptic curve over finite fields," arXiv preprint arXiv:1202.1895, February (2012).

[15] G. Mittal, S. Kumar, and S. Kumar, "Novel public-key cryptosystems based on NTRU and algebraic structure of group rings," *Journal of Information and Optimization Sciences,* vol. 42, no. 7, pp. 1507–1521 (2021).

[16] Ö. Küsmüş and T. Hanoymak, "A novel public-key encryption scheme based on Bass cyclic units in integral group rings," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 2, pp. 579–589 (2022).

[17] Q. M. Luhaib and R. K. K. Ajeena, "Elliptic curve matrices over group rings to improve elliptic curve–discrete logarithm cryptosystems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 6, pp. 1699–1704 (2023).

Received April, 2025