Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–5.
ISSN-0037-8712
doi:10.5269/bspm.75787

A Modification of the Elliptic Curve Massey-Omura Cryptosystem

Ammar Ali Neamah* and Hiba Hilal Hadi

ABSTRACT: Several advancements have been made to the Massey-Omura cryptographic system due to its significance in secure communication. These improvements aim to improve security and efficiency, ensuring the system remains robust against evolving technological challenges in data exchange. This paper presents a modification of the elliptic curve analogue of the Massey-Omura cryptosystem by incorporating a matrix-based structure. Compared to the original system, this novel approach offers enhanced security, as an attacker must solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) multiple times, depending on the size of the secret matrices chosen by the users. This significantly strengthens the system's resilience against cryptanalysis and increases its potential for use in modern secure communication protocols.

Key Words: Massey-Omura Cryptosystem, ECDLP, Matrix-based Encryption.

Contents

1. Introduction

The science and study of cryptography focus on preventing unauthorized disclosure and manipulation of data in computer networks and communications [1]. Cryptographic systems are broadly categorized into two types: secret-key (symmetric) and public-key (asymmetric) cryptosystems. Both types rely on complex mathematical calculations and are implemented using algorithmic processes. The Massey-Omura cryptosystem, introduced in the mid-1980s by Massey and Omura [2], can be considered a hybrid of private and public-key cryptography. One of its most notable features is that users can generate their private keys, similar to public-key cryptography. However, unlike traditional public key systems, the encryption and decryption keys in the Massey-Omura system remain confidential among all participants in the communication.

In this scheme, a user releases a public encryption key, which anyone can use to send encrypted messages to them. In contrast, the user retains a private decryption key, known only to him, which is used to decrypt the received ciphertexts. Although public-key cryptosystems may seem vulnerable due to the public availability of certain data, their security relies on mathematical problems that are computationally hard to solve. For instance, the security of many public-key systems is based on the difficulty of solving problems like the Discrete Logarithm Problem (DLP) or the Elliptic Curve Discrete Logarithm Problem (ECDLP).

In the mid-1980s, Miller [3] and Koblitz [4] introduced elliptic curve-based public-key cryptographic systems, which have since been extensively studied by researchers (see, for example, [5], [11]). Early

* Corresponding author

Submitted February 18, 2025. Published July 11, 2025
2010 *Mathematics Subject Classification:* 14H52, 94A60, 15A24.

proposals for elliptic curve (EC) cryptosystems were adaptations of existing systems, such as the Massey-Omura [2] and ElGamal [5] cryptosystems. Over the years, several developments and applications of the Massey-Omura scheme have been proposed. For example, Manjunatha et al. [9] combined the Massey-Omura seed exchange protocol with the Vernam cipher and vulgar fractions to generate a complex key. Furthermore, Al Saffar et al. [10] utilized the Massey-Omura cryptosystem for grayscale image encryption, demonstrating how the three-pass protocol can securely manage keys during encryption and decryption.

This paper introduces a novel development of the elliptic curve (EC) analogue of the Massey-Omura cryptosystem, incorporating a matrix-based structure. This approach is inspired by the block matrix concept, as Hadi and Neamah introduced in [11]. The proposed system leverages the Elliptic Curve Discrete Logarithm Problem (ECDLP) to enhance security compared to the original Massey-Omura cryptosystem. Specifically, if users employ 4×4 secret matrices, a cryptanalyst would need to solve the ECDLP sixteen times for each matrix entry, instead of solving it once, as required in the original system. This multiplicative increase in complexity significantly strengthens the system's resistance to attacks.

2. Elliptic Curve Function

Let $p > 2$ be a prime. An elliptic curve E over a prime finite field F_p, is a graph of the equation

$$E : y^2 = x^3 + ax + b \,(mod\, p), \tag{2.1}$$

where $a, b \in F_p$ and satisfy the condition $(4a^3 + 27b^2)\, mod\, p \neq 0$. The group of elliptic curve points $E(F_p)$ is the set of all solutions (x, y) to Equation (2.1) together with the point at infinity O_∞ [1].

2.1. Elliptic Curve Operations

One of the core operations in elliptic curve cryptography (ECC) is elliptic curve scalar multiplication (ECSM), the most computationally intensive component of encryption and decryption processes. ECSM is performed using two fundamental operations: point addition and point doubling, which are repeatedly applied to compute scalar multiplication efficiently [12].

2.1.1. Point addition and doubling. Let $P, Q \in E(F_p)$ such that $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.

1. If $Q = O_\infty$, then $P \oplus Q = P$.
2. If $x_1 = x_2$ and $y_1 = -y_2$, then $P \oplus Q = O_\infty$.
3. Otherwise, define λ by

$$\lambda := \begin{cases} \frac{3x_1^2 + a}{2y_2} & \text{if } P = Q, \\ \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q, \end{cases} \tag{2.2}$$

and let

$$x_3 = \lambda^2 - x_1 - x_2 \text{ and } y_3 = \lambda(x_1 - x_3) - y_1.$$

Then $P \oplus Q = (x_3, y_3)$.

2.1.2. Scalar Multiplication. Let P be a point that lies on $E(F_p)$. Then the scalar multiplication operation over P, which can be described by the repeated addition of the point P to itself k times, is written as

$$kP = \underbrace{P \oplus P \oplus \ldots \oplus P}_{k \text{ copies}} \tag{2.3}$$

2.2. Elliptic Curve Discrete Logarithm Problem

Assume that E is the elliptic curve over F_p, where p is a prime number. Given a point Q and a point P on $E(F_p)$, the discrete logarithm problem on elliptic curves (ECDLP) is described as finding $k \in \mathbb{Z}$, if it exists, such that $Q = kP$. Here, k represents the private key and Q represents the public key [1].

Definition 2.1 *Let K be a matrix all of whose entries are integers; (i.e., $k_{ij} \in \mathbb{Z}$ for $i = 1, \ldots, m, j = 1, \ldots, n.$) and let $P \in E(F_p)$. Then $K \otimes P$ can be defined by multiplying each element of K by P as follows:*

$$K \otimes P = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mn} \end{bmatrix} \otimes P = \begin{bmatrix} k_{11}P & k_{12}P & \cdots & k_{1n}P \\ k_{21}P & k_{22}P & \cdots & k_{2n}P \\ \vdots & \vdots & & \vdots \\ k_{m1}P & k_{m2}P & \cdots & k_{mn}P \end{bmatrix}$$

3. Modified Massey-Omura Cryptosystem

The Massey-Omura cryptosystem is a three-pass protocol that enables secure message transmission between Party A and Party B without requiring key exchange or distribution. This scheme can be enhanced through a matrix-based modification, where the communicating parties utilize square invertible matrices as specified in the following implementation.

Initialization:

The parties A and B publicly select E over F_p, and we further assume that $N = \#E(F_p)$ (the number of points on $E(F_p)$) is also publicly known.

Key generation:

- Party A selects a private square matrix η_A whose elements are integers and the determinant of the matrix η_A is ± 1. Then he calculates its inverse $\delta_A = \eta_A^{-1} mod\, N$.
- Party B selects a private square matrix η_B whose elements are integers and the determinant of the matrix η_B is ± 1. Then he calculates its inverse $\delta_B = \eta_B^{-1} mod\, N$.
- Keep $\eta_A, \delta_A, \eta_B,$ and δ_B secret.

Transmission procedure:

Party A sends the message M to Party B as follows:

- Party A computes $\eta_A \otimes M$ and sends it to Party B.
- Party B computes $\eta_B \eta_A \otimes M$ and sends it to Party A.
- Party A computes $(\eta_B \eta_A \otimes M)\delta_A$ and sends it to Party B.
- Party B recovers the original message M by computing the following: $(\eta_B \eta_A \otimes M)\delta_A \delta_B = M \otimes I = M$, where I is the identity matrix.

3.1. Implemented Example

Suppose that parties A and B agree upon an $E(F_{1109})$ with parameters $a = 1, b = 911$ where $4a^3 + 27b^2\, mod\, 1109 \neq 0$ and $\#E(F_{1109}) = 1109$. If Party A wishes to send the message $M = (115, 411)$ to Party B using the modified Massey-Omura system, what should they do?

Solution: Key generation

- Party A selects a private matrix $\eta_A = \begin{bmatrix} 11 & 3 \\ 7 & 2 \end{bmatrix}$, and calculates $\delta_A = \eta_A^{-1} = \begin{bmatrix} 2 & -3 \\ -7 & 11 \end{bmatrix} \ mod\, 1109 = \begin{bmatrix} 2 & 1106 \\ 1102 & 11 \end{bmatrix}$.
- Party B selects a private matrix $\eta_B = \begin{bmatrix} 53 & 2 \\ 79 & 3 \end{bmatrix}$, and calculates $\delta_B = \eta_B^{-1} = \begin{bmatrix} 3 & -2 \\ -79 & 53 \end{bmatrix} \ mod\, 1109 = \begin{bmatrix} 3 & 1107 \\ 1030 & 53 \end{bmatrix}$.
- Keep $\eta_A, \delta_A, \eta_B,$ and δ_B secret.

Transmission procedure:

Party A sends the message $M = (115, 411)$ to Party B as follows:

- Party A calculates, $\eta_A \otimes M = \begin{bmatrix} 11 & 3 \\ 7 & 2 \end{bmatrix} \otimes M = \begin{bmatrix} 11(115,411) & 3(115,411) \\ 7(115,411) & 2(115,411) \end{bmatrix}$
  $= \begin{bmatrix} (396,778) & (397,786) \\ (498,17) & (888,799) \end{bmatrix}$ and sends it to Party B.
- Party B calculates, $\eta_B\eta_A \otimes M = \begin{bmatrix} 53 & 2 \\ 79 & 3 \end{bmatrix} \otimes \begin{bmatrix} (396,778) & (397,786) \\ (498,17) & (888,799) \end{bmatrix}$
  $= \begin{bmatrix} 53 & 2 \\ 79 & 3 \end{bmatrix} \otimes \begin{bmatrix} 53(396,778) \oplus 2(498,17) & 53(397,786) \oplus 2(888,799) \\ 79(396,778) \oplus 3(498,17) & 79(397,786) \oplus 3(888,799) \end{bmatrix}$
  $= \begin{bmatrix} (898,755) \oplus (380,459) & (502,1039) \oplus (317,335) \\ (440,444) \oplus (829,377) & (496,566) \oplus (983,495) \end{bmatrix} = \begin{bmatrix} (714,776) & (874,195) \\ (842,452) & (608,762) \end{bmatrix}$, and sends it to Party A.
- Party A calculates, $(\eta_B\eta_A \otimes M)\delta_A = \begin{bmatrix} (714,776) & (874,195) \\ (842,452) & (608,762) \end{bmatrix} \begin{bmatrix} 2 & 1106 \\ 1102 & 11 \end{bmatrix}$
  $= \begin{bmatrix} 2(714,776) \oplus 1102(874,195) & 1106(714,776) \oplus 11(874,195) \\ 2(842,778) \oplus 1102(608,762) & 1106(842,452) \oplus 11(608,762) \end{bmatrix}$
  $= \begin{bmatrix} (1055,303) \oplus (732,997) & (444,757) \oplus (681,406) \\ (906,139) \oplus (913,667) & (707,783) \oplus (770,161) \end{bmatrix} = \begin{bmatrix} (288,758) & (888,799) \\ (634,574) & (397,786) \end{bmatrix}$ and sends it to Party B.
- Party B recovers the message M by computing the following:
  $(\eta_B\eta_A \otimes M)\delta_A\delta_B = \begin{bmatrix} (288,758) & (888,799) \\ (634,574) & (397,786) \end{bmatrix} \begin{bmatrix} 3 & 1107 \\ 1030 & 53 \end{bmatrix}$
  $= \begin{bmatrix} 3(288,758) \oplus 1030(888,799) & 1107(288,758) \oplus 53(888,799) \\ 3(634,574) \oplus 1030(397,786) & 1107(634,574) \oplus 53(397,786) \end{bmatrix}$
  $= \begin{bmatrix} (502,1039) \oplus (1064,792) & (315,614) \oplus (315,495) \\ (496,566) \oplus (496,543) & (1064,792) \oplus (502,1039) \end{bmatrix}$
  $= \begin{bmatrix} (115,411) & O_\infty \\ O_\infty & (115,411) \end{bmatrix} = (115,411) \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = M \otimes I = M.$

4. Conclusion

In this work, we develop an enhanced elliptic curve (EC) Massey-Omura cryptosystem. The proposed modification improves security over the original scheme by requiring an attacker to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) multiple times, specifically, as many times as the number of entries in the user-selected private matrix. For example, with a private matrix of size 4×4, the ECDLP must be solved 16 times, compared to only once in the original system. This modification not only strengthens security but also maintains efficiency while enabling the simultaneous encryption of multiple messages. Future work will investigate the applicability of the proposed cryptosystem to image encryption, adopting a similar approach to that described in [13].

Acknowledgments

The authors are grateful to the referees for their valuable suggestions.

References

1. A. A. Neamah, *New Collisions to Improve Pollard's Rho Method of Solving the Discrete Logarithm Problem on Elliptic Curves*, Journal of Computer Science, **11**, no. 9, 971-975, (2015).
2. J. L. Massey and J.K. Omura, *Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission*, January 28, US Patent 4,567,600, (1986).
3. V. Miller, *Uses of Elliptic Curves in cryptography, In Advances in Cryptology-CRYPTO 85*; Springer: Berlin/Heidelberg, Germany, 417-426, (1986).
4. N. Koblitz, *Elliptic Curve Cryptosystems, Mathematics of Computation*, **48**, no. 77, 203-209, (1987).
5. T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on information theory, **31**, no. 4, 469-472, (1985).
6. R. Winton, *Enhancing the massey–omura cryptosystem*, Journal of Mathematical Sciences and Mathematics Education, **2**, no. 1, 21-29, 2007, (2007).
7. R. Winton, *Combining public and private key cryptography,* Journal of Mathematical Sciences and Mathematics Education, **7**, no. 1, 1-10, (2012).
8. T. Zebua, R. K. Hondro, and E. Ndruru, *Message security on chat app based on massey omura algorithm*, International Journal of Information System and Technology, **1**, no. 2, 16-23, (2018).
9. V. Manjunatha, A. Rao, and A. Khan, *Complex key generation with secured seed exchange for Vernam cipher in security applications*, Materials Today: Proceedings, **35**, part 3, 497-500, (2021).
10. N. F. H. Al Saffar, I. R. Al-Saiq, and R. R. M. Abo Alsabeh, *Asymmetric image encryption scheme based on Massey Omura scheme*, International Journal of Electrical and Computer Engineering, **12**, no. 1, 1040-1047, (2022).
11. H. H. Hadi, and A. A. Neamah, *Diffie-Hellman Key Exchange Based on Block Matrices Combined with Elliptic Curves*, International Journal of Intelligent Systems and Applications in Engineering, **11**, no. 5s, 353-360, (2023).
12. K. T. Aljamaly and R. K. Ajeena, *The elliptic scalar multiplication graph and its application in elliptic curve cryptography*, Journal of Discrete Mathematical Sciences and Cryptography, **24**, no. 6, 1793-1807, (2021).
13. H. H. Hadi, and A. A. Neamah, *An image encryption method based on modified elliptic curve Diffie-Hellman key exchange protocol and Hill Cipher*, Open Engineering, **14**, no. 1, 20220552, (2024).

Ammar Ali Neamah,
Faculty of Computer Science and Mathematics,
University of Kufa,
Najaf, Iraq.
E-mail address: ammara.meamah@uokufa.edu.iq

and

Hiba Hilal Hadi,
Department of Mathematics,
Faculty of Computer Science and Mathematics,
University of Kufa,
Najaf, Iraq.
E-mail address: hebah.alsalamy@uokufa.edu.iq