Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 5, pp. 2035–2040
DOI : 10.47974/JDMSC-2673

Cryptosystems based on the Edward curve scalar multiplication matrix function

Karrar Taher R. Aljamaly *
Zainab Flaih Hassan †
Sadeq Hamdallah Naji §
Department of Mathematics
Open Educational College
Najaf Study Center
Najaf
Iraq

Abstract

The key point in this paper is the definition of new mathematical concepts based on point doubling and addition on the Edward curve group and matrix power functions. The basic idea is known as the Edward scalar multiplication matrix function (E_dSMMF). Also proposed is a modification to the Diffie-Hellman and ElGamal schemes in the Edward curve cryptosystem, which is more secure than the original because the discrete logarithm problem is computationally infeasible to solve.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Edward curve cryptography, Scalar multiplication matrix function, Diffie – hellman key exchange, ElGamal public key cryptosystem.*

1. Introduction

Several mathematicians have studied elliptic curves for over a hundred years, and they play an important role in algebra and topology; see [1-5]. They met to solve a wide variety of mathematical problems.

Edwards's curve is a collection of elliptic curves that uses a cryptographic scheme. In 2007, Edwards [6] proposed a novel normal form for elliptic curves and gave the addition laws for a point on it. Bernstein and Lange [7] generalized the Edwards curve to a twisted Edwards curve, which defines the curve more precisely over a finite field. Author introduced Edwards curves, point-counting methods, and the supersingular Edwards and Montgomery

* *E-mail:* karrar.taher@ec.edu.iq (Corresponding Author)
† *E-mail:* Zainab.flaih@ec.edu.iq
§ *E-mail:* alhsynawysadq278@gmail.com

curves. These methods count the number of elements of a given order on Edwards curves over finite fields [8].

2. Edwards curves on prime fields

This section presents basic definitions of Edwards curve defined on prime fields and a sum formula for two points lying on Edwards's curve.

Definition 1.2: [9] An Edwards curve on K, together with $char(K) \neq 2$ be the curve given by $x^2 + y^2 = 1 + dx^2y^2$ where $d \in K\backslash\{0,1\}$.

Definition 2.2: [6] The addition laws of any two points $P = (x_1, y_1)$ & $Q = (x_2, y_2)$ in $E_d(F_p)$ is defined by

$$P + Q = \left(\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$$

3. The Edward Scalar Multiplication Matrix Function (E_dSMMF).

New mathematical concepts, such as points doubling and addition on the Edward curve group, and matrices, power functions are defined as the key points in this work. The essential concept is called the Edward scalar multiplication matrix function (E_dSMMF). The E_dSMMF is the square matrix; its elements are the Edward curves' points. The discussion of these concepts is done as follows.

Definition 3.1: (Left-side Edward scalar multiplications matrix function (E_dSMMF).

Let $*_L: M_n(F_p) \times E_dM_n(F_p) \to E_dM_n(F_p)$ be a map. Then, for all $L \in M_n(F_p)$ and $A \in E_dM_n(F_p)$ there exists $B \in E_dM_n(F_p)$ such that $*_L(A) = L * A = B$. The elements that form an L-ESMMF are computed by $B_{ij} = \sum_{k=1}^{n} l_{ik}A_{kj}$.

Definition 3.2: (Right-side elliptic scalar multiplication matrix function (R-E_dSMMF). Let $*_R: E_dM_n(F_p) \times M_n(F_p) \to E_dM_n(F_p)$ be a map. Then, for all $R \in M_n(F_p)$ and $A \in E_dM_n(F_p)$ there exists $C \in E_dM_n(F_p)$ such that $*_R(A) = A * R = C$, the elements which form an R-E_dSMMF is computed by $C_{ij} = \sum_{t=1}^{n} r_{tj}A_{it}$.

Theorem 3.3: (Properties on the L^R-E_dSMMF).

1. *The L^R-E_dSMMF is an association. This means that* $(L * A) * R = L * (A * R)$
2. $L_1 * (L_2 * A) = (L_1 \cdot L_2) * A$ *and* $(A * R_1) * R_2 = A * (R_1 \cdot R_2)$
3. $L^{-1} * (L * A) = A$*and* $(A * R) * R^{-1} = A$
4. $L_2 * (L_1 * A * R_1) * R_2 = (L_2 \cdot L_1) * A * (R_1 \cdot R_2)$

4. The Edward scalar multiplication matrix function cryptosystems

In this section, the alternative versions of the Edward curve discrete logarithm problem (E_dCDLP) are proposed. This extension is proposed based on the E_dSMMF is applied to satisfy the DLP as explained in the following definitions.

Definition 4.1: If E_d is the Edward curve on prime fields F_p & A , B are matrices in the $E_dM_n(F_p)$. A left-side Edward discrete logarithms matrix function (L- E_dDLMF) problem is to find a matrix $L \in M_n(F_p)$ such that $L * A = B$. The left matrix L is called the L-E_dMF-DLP problem of B to the matrix A.

Definition 4.2: If E_d is the Edward curve on the prime fields F_p & A, Bbe matrices in the $E_dM_n(F_p)$. A right-side Edward discrete logarithms matrix function (R- E_dDLMF) problem is to find a matrix $R \in M_n(F_p)$ such that $A * R = B$. The right matrix R is called the R- E_dDLMF-DLP problem of B to the matrix A.

Now, the alternative version of the encryption schemes based on the newly proposed problems, as defined in Definitions (4.1) and (4.2), is discussed as follows.

4.1 *The ECDLMF-Diffie – Hellman Key Exchange*

In 2007, The authors [1], proposed the Edward curve Diffie-Hellman (E_dCDH key exchange protocol, which depends on the difficulty of the ECDLP. On an alternative version of the Edward curve Diffie-Hellman key exchange, which is named E_dCDLMF-Diffie–Hellman key exchange. The following Algorithm used to obtain a result of a revised E_dCDLMF-DH key exchanges.

Algorithm (1): The E_dCMF-DH Key Exchange

Input: A set $E_d(F_p)$ of Edward points & the matrices $D \in E_dM_n(F_p)$.

Output: A shared key K, when $K \in E_dM_n(F_p)$.

Alice

1. She chooses $L \in M_n(F_p)$ as her a private key.
2. She computes $A = L * D$.
3. The keys Alice's (L, A).

Bob:

1. He chooses $R \in M_n(F_p)$ is a private key.
2. He computes his public key $B = D * R$.
3. Bob keys are (R, B).

Alice and Bob are compute a shared secret key$K = L * D * R$ by

$$K = A^{\bullet} = L * B = L * (D * R) = (L * D) * R = A * R = B^{\bullet}.$$

4.2 *The E_dCDLMF-ElGamal Public Key Cryptosystem*

In 2013, The authors [10], proposed (E_dCEPKC) defined on a prime field F_p. The E_dCEPKC is close to E_dCDH key exchange.

The Edward ElGamal public key cryptosystem takes alternative versions based over a MF-E_dCDLP. According to Algorithms (2), (3), and (4).

Algorithm (2): The E_dCMF-EPKC: Keys Generation.

Input: A set $E_d(F_p)$ of Edward points & the matrix $D \in E_d M_n(F_p)$.

Output: A public key A, when $A \in E_d M_n(F_p)$.

1. Alice chooses her private key randomly as a left matrix $L \in M_n(F_p)$.
2. She computes $A = L * D$.
3. Alice's keys are (L, A).

Algorithm (3): The E_dCMF-EPKC: Encryption.

Input: A set $E_d(F_p)$ of Edward points, a matrix $D \in E_d M_n(F_p)$ & the public keys A.

Output: A public key A, where $A \in E_d M_n(F_p)$.

1. Bob chooses his key as a right matrix R, where $R \in M_n(F_p)$.
2. He chooses a plaintext $M \in E_d M_n(F_p)$.
3. He computes a cipher text by a computation for the two matrices $C_1 = D * R$and $C_2 = M + A * R$.
4. Bob sends a cipher text pair (C_1, C_2) to Alice.

Algorithm (4): An E_dCMF-EPKC: Decryption.

Input: A set $E_d(F_p)$ of Edward points and a ciphertext pair (C_1, C_2).

Output: The plaintext M.

1. Alice uses her secret keys L for computed$-L * C_1$.
2. She computes a matrix $\boldsymbol{C_2 - L * C_1}$which is equal to the original message M.

Example 4.1: Alice and Bob agreed to use an Edward curve, which is defined by $x^2 + y^2 = 1 + 13x^2y^2$ over F_{19} The points on E_{13} form a set

$E_{13}(F_{19}) = \{(0, \mp 1), (1,0), (18,0), (2, \mp 3), (3, \mp 2), (5, \mp 9), (6, \mp 6), (9, \mp 5), (10, \mp 5), (13, \mp 6), (14, \mp 9), (16, \mp 2), (17, \mp 3)\}$ and a public matrix

$$D = \begin{pmatrix} (3,2) & (13,6) \\ (10,5) & (14,10) \end{pmatrix}$$

Where $D \in E_{13} M_2(F_{19})$,

Keys generation process. Alice performs the following:

1. She chooses her secret key $L = \begin{pmatrix} 6 & 4 \\ 3 & 8 \end{pmatrix}$,

2. computes her public key $A = L * D = \begin{pmatrix}(17,3) & (16,17)\\ (16,2) & (10,14)\end{pmatrix}$.

Encryption process. Bob does the following steps:

1. He chose his plaintext M as a matrix to send Alice the plaintext
$$M = \begin{pmatrix}(5,9) & (18,0)\\ (6,13) & (2,16)\end{pmatrix} \in E_{13}M_2(F_{19})$$
2. He chooses his ephemeral key as a matrix $R = \begin{pmatrix}10 & 5\\ 6 & 12\end{pmatrix}$,
3. He computes $A * R = \begin{pmatrix}(17,16) & (17,3)\\ (3,17) & (3,2)\end{pmatrix}$,
4. He computes his ciphertext $C_1 = D * R = \begin{pmatrix}(16,17) & (16,2)\\ (2,16) & (14,9)\end{pmatrix}$ and
$$C_2 = M + A * R = \begin{pmatrix}(13,13) & (16,17)\\ (10,14) & (6,6)\end{pmatrix}$$
5. He sends his ciphertext (C1, C2) to Alice.

Decryption process. Alice performs the following steps:

1. She uses her private key L, first computes $-L * C_1$.
2. Finally, she computes $\boldsymbol{C_2 - L * C_1}$which is equal to the original plaintext
$$M = \begin{pmatrix}(5,9) & (18,0)\\ (6,13) & (2,16)\end{pmatrix}.$$

5. Conclusions

In this work, the encryption schemes of the Edward curve cryptosystem were developed, following the definition of L/R-DLP. A security for a E_dPKC determines the difficulty of solving L ^ R-ECMF-DLP. To solve this must solve the original $\boldsymbol{E_d}$CDLP in a first step, and this is very hard because every element is obtained by collecting products $\boldsymbol{E_d}$CDLP: we can apply these results to image and character encryption. Also, can be modified over extension Galois fields.

References

[1] Z. H. Abdulqader, R. B. Esmaeel, and N. E. Arif, "L-open set and some related concepts," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 5, pp. 1715–1721 (2024).

[2] H. F. Abbas, H. H. Ebrahim, and A. Al-Fayadh, "Soft P-field and some of its properties," *Journal of Discrete Mathematical Sciences & Cryptography,* vol. 26, no. 7, pp. 1875–1882 (2023).

[3] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO 1985*, Berlin, Heidelberg: Springer, pp. 417–426 (1985).

[4] A. S. Mohammed, I. S. Ahmed, and S. H. Asaad, "Study of the rings in which each element express as the sum of an idempotent and pure," *Int. J. Nonlinear Anal. Appl,* vol. 12, no. 2, pp. 1719-1724 (2021), doi: 10.22075/IJNAA.2021.5311.

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

[6] H. Edwards, "A normal form for elliptic curves," *Bulletin of the American mathematical society,* vol. 44, no. 3, pp. 393–422 (2007).

[7] D. J. Bernstein and T. Lange, "Inverted Edwards coordinates," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes.* Lecture Notes in Computer Science, vol. 4851, S. Boztaş and H. F. Lu, Eds., Berlin, Heidelberg: Springer, pp. 20–27 (2007).

[8] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, "Twisted Edwards curves," in *Cryptology in Africa — AFRICACRYPT 2008*. Lecture Notes in Computer Science, vol. 5023, I. B. Damgard, Ed., Berlin, Heidelberg: Springer, pp. 389–405 (2008).

[9] A. A. Abd El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-International Journal of Electronics and Communications,* vol. 67, no. 2, pp. 136–143 (2013).

[10] S. H. Asaad, I. S. Ahmed, and H. H. Ebrahim, "On Finitely Null-additive and Finitely Weakly Null-additive Relative to the σ–ring," *Baghdad Sci. J,* vol. 19, no. 5, pp. 1148-1154 (2022).

Received November, 2025