

Elliptic curve matrices over group ring to improve elliptic curve–discrete logarithm cryptosystems

Qasim Mohsin Luhaib *

Ruma Kareem K. Ajeena †

Department of Mathematics

College of Education for Pure Sciences

University of Babylon

Babil

Iraq

Abstract

An elliptic curve matrix (ECM) is created randomly based on an elliptic curve group to modify the elliptic curve-discrete logarithm (EC-DL) cryptosystems, which are elliptic Diffie-Hellman key exchange (DHKE) and elliptic ElGamal public key cryptosystem (EPPKC), and to increase the security level in comparison with the original EC-DL schemes. In proposed schemes, the keys and ciphertext are computed using the ECMs. The security of trust schemes depended on the difficulty of solving the elliptic curve discrete logarithm problem (ECM-DLP). New experimental results on proposed schemes are discussed. The ECM-DL schemes consider new insights for more secure communications.

Subject Classification: 14G50, 11Gxx, 16U60.

Keywords: Elliptic curve cryptography, ECMs, DHKE, EPPKC, Security.

1. Introduction

The EC-DL protocols which are elliptic curve Diffie-Hellman key exchange (ECDHKE) and elliptic ElGamal public key cryptosystem (EPPKC) are the generalization of DHKE [1] and EPPKC [2]. Many studies are proposed to modify these protocols. In 2018, Saba Inam and Rashid Ali, introduced an ElGamal-like public key cryptosystem in a new form based

* E-mail: qasimmohsinluhaib@gmail.com (Corresponding Author)

† E-mail: pure.rume.k@uobabylon.edu.iq

on the matrices over a group ring [3]. In 2020, Bora, Ravi Kumar et. al. [4] developed the ElGamal encryption scheme based on golden matrices over the elliptic curves. In 2021, Ruma Ajeena [5] presented the soft graphic ISD (SG-ISD) method for elliptic scalar multiplication algorithms. Also, in 2021, Karrar Aljamaly and Ruma Ajeena [6,7] first study proposed a new graph based on elliptic scalar multiplication to create a new version of an asymmetric encryption technique. The KR-elliptic curve public key cryptosystem was proposed by the second. In this work, an ECM is created and considered as the main point to propose new versions of EC-DL protocols. The security of these protocols depended on the hard mathematical problem which is ECMDLP.

2. The Elliptic Curve Matrix Over Group Ring

In this section, some new concepts are defined as main points related to this as follows:

Definition 2.1: (Group Ring (RG)). A RG [3] of a group G over a ring R is the set of all formal sums $\sum_{i=1}^n \alpha_i g_i$, with $\alpha_i \in R$ and $g_i \in G$.

Definition 2.2: (Elliptic Curve Matrix (ECM)). An ECM is a $m \times n$ matrix, its elements are elliptic curve points that are chosen randomly from elliptic curve group $E(F_p)$ defined over a prime field F_p . This matrix is denoted by $M_{EC} = [P_{ij}]$, where P_{ij} is a point in $E(F_p)$. To put it another way,

$$M_{EC} = \begin{pmatrix} P_{11} & \dots & P_{1n} \\ \vdots & \ddots & \vdots \\ P_{m1} & \dots & P_{mn} \end{pmatrix}.$$

Definition 2.3: (Scalar Elliptic Curve Matrix (ECM)). Let E be an elliptic curve defined over a prime field F_p . The elliptic curve points form an abelian group $(E(F_p), +_E)$ with elliptic curve addition operation $+_E$. Suppose k is a scalar in a ring R . An elliptic scalar multiplication matrix is defined by

$$M_{ESM} = k \begin{pmatrix} P_{11} & \dots & P_{1n} \\ \vdots & \ddots & \vdots \\ P_{m1} & \dots & P_{mn} \end{pmatrix} = \begin{pmatrix} kP_{11} & \dots & kP_{1n} \\ \vdots & \ddots & \vdots \\ kP_{m1} & \dots & kP_{mn} \end{pmatrix} \pmod{p}, \quad (1)$$

where $k \in R$ and $P_{ij} \in E(F_p)$, for $i=1, \dots, m$ and $j=1, \dots, n$.

Definition 2.4: (Elliptic Curve Matrix Discrete Logarithm Problem (ECMDLP)). Let E be an elliptic curve defined over a prime field F_p . Suppose k is a scalar in a ring of integers Z . Then, finding the value of k that satisfies the relation which is defined in Equation (1) is solving to ECMDLP to the base M_{EC} .

3. EC-DL Cryptosystem

This section proposes new versions of EC- DL cryptosystem using the ECM as follows.

3.1 The ECM for Diffie–Hellman Key Exchange

Alice and Bob agreed to use an elliptic curve group $EC(F_p)$ and an ECM M_{EC} . Alice and Bob choose her and his secret keys $n_a, n_b \in Z$ respectively. They compute $Q_{ECMa} = n_a M_{EC}$ and $Q_{ECMb} = n_b M_{EC}$ exchange these values. Alice then computes $n_a Q_{ECMb}$ and Bob similarly computes $n_b Q_{ECMa}$. A shared secret key is computed as an ECM by

$$k = n_a Q_b = n_a n_b M = (n_a n_b) M = n_b Q_a$$

3.2 The ECM for Elliptic ElGamal Public Key Cryptosystem

Assume E is an elliptic curve with a prime field F_p . The elliptic curve group $E(F_p)$ and Z is a ring of integers. Alice chooses her private key k as a scalar from a ring Z . She computes her public key Q_{ESM} as a scalar multiplication matrix by

$$Q_{ESM} \equiv k A_{ECM} \pmod{p},$$

where A_{ECM} is a matrix of elliptic curve points that are chosen randomly from the elliptic curve group $E(F_p)$. Bob chooses his plaintext M_{ECM} as an elliptic curve matrix. He uses Alice's public key Q_{ESM} to encrypt the M_{ECM} . Randomly, he selected his ephemeral key t as an element from a ring Z . He computes the ciphertext (C_{ESM1}, C_{ESM2}) as two elliptic curve matrices, where

$$C_{ESM1} \equiv t A_{ECM} \pmod{p} \text{ and } C_{ESM2} \equiv M_{ECM} + t Q_{ESM} \pmod{p}.$$

Upon Alice receiving the ciphertext (C_{ESM1}, C_{ESM2}) , she wants to decrypt it and recover an original plaintext M_{ECM} . The decryption process is done by computing

$$C_{ESM2} - n C_{ESM1} \equiv M_{ECM} \pmod{p}.$$

4. Study Cases of EC–DL Cryptosystem

Two study cases are discussed as new computational results to explain the proposed EC–DL Cryptosystem as follows:

4.1 Study Case of DHKE Based on ECM

Let $p = 111217$ be a prime as a public parameter. Suppose $E: y^2 = x^3 + 3x + 29$ is an elliptic curve defined over a prime field F_{111217} . The $E(F_{111217}) = \{(3, 46578), (3, 64639), (5, 13), (5, 111204), (7, 48895), (7, 62322), \dots, (111216, 111212), (111216, 5), O_E\}$. Suppose k is an element in a ring of integers Z . Let M_{EC} be ECM is chosen randomly

$$M_{EC} = \begin{pmatrix} (15962, 32969) & (97437, 30779) \\ (73013, 80897) & (3, 46578) \end{pmatrix}.$$

Alice chooses her secret integer $n_a = 2471 \in Z$ and she computes her public key as an ECM by

$$Q_a = 2471 \begin{pmatrix} (18129, 47152) & (61967, 96875) \\ (33116, 44697) & (61733, 32895) \end{pmatrix} = \begin{pmatrix} (18129, 47152) & (61967, 96875) \\ (33116, 44697) & (61733, 32895) \end{pmatrix}.$$

Bob chooses a secret integer $n_b = 7219 \in Z$ and he computes his public key as an ECM by

$$Q_b = 7219 \begin{pmatrix} (15962, 32969) & (97437, 30779) \\ (73013, 80897) & (3, 46578) \end{pmatrix} = \begin{pmatrix} (75820, 23114) & (30526, 28346) \\ (14453, 98828) & (84143, 28520) \end{pmatrix}.$$

Alice sends Q_a to Bob and Bob sends Q_b to Alice. Finally, they compute

$$n_b Q_a = \begin{pmatrix} (28529, 105061) & (17566, 95093) \\ (101522, 3107) & (98289, 18184) \end{pmatrix} \text{ and } n_a Q_b = \begin{pmatrix} (28529, 105061) & (17566, 95093) \\ (101522, 3107) & (98289, 18184) \end{pmatrix}.$$

So, a shared secret key is

$$n_b Q_{ECMa} = \begin{pmatrix} (28529, 105061) & (17566, 95093) \\ (101522, 3107) & (98289, 18184) \end{pmatrix} = n_a Q_{ECMb}.$$

4.2 Study Case of EEPKC Based on ECM

Let $p = 317$ be a prime. Suppose $E: y^2 = x^3 + x + 5$ is an elliptic curve defined over a prime field F_{317} . The set $E(F_{317}) = \{(1, 18), (1, 299), (2, 40), (1, 277), \dots, (314, 64), (314, 253), O_E\}$. Let $A_{ECM} = \begin{pmatrix} (283, 64) & (188, 202) \\ (197, 304) & (163, 239) \end{pmatrix}$.

Alice's private key is $n = 13$. Alice's public key is

$$Q \equiv 13A_{ECM} \equiv \begin{pmatrix} (137,292) & (123,34) \\ (30,224) & (27,78) \end{pmatrix} (\text{mod } p).$$

Bob chooses a plaintext as an elliptic curve matrix

$M_{ECM} = \begin{pmatrix} (88,277) & (102,114) \\ (47,97) & (201,79) \end{pmatrix}$. Suppose $t=103$. So the ciphertext (C_{ESM1}, C_{ESM2}) is computed by

$$C_{ESM1} \equiv 103A_{ECM} \equiv \begin{pmatrix} (283,64) & (16,89) \\ (197,304) & (285,217) \end{pmatrix} (\text{mod } p) \text{ and}$$

$$\begin{aligned} C_{ESM2} &\equiv \begin{pmatrix} (88,277) & (102,114) \\ (47,97) & (201,79) \end{pmatrix} + 103 \begin{pmatrix} (137,292) & (123,34) \\ (30,224) & (27,78) \end{pmatrix} (\text{mod } p) \\ &\equiv \begin{pmatrix} (196,311) & (232,211) \\ (264,51) & (266,206) \end{pmatrix} (\text{mod } p). \end{aligned}$$

For the decryption process and recovering the original plaintext M_{ECM} , Alice computes

$$\begin{aligned} C_{ESM2} - nC_{ESM1} &\equiv \begin{pmatrix} (196,311) & (232,211) \\ (264,51) & (266,206) \end{pmatrix} - 13 \begin{pmatrix} (283,64) & (16,89) \\ (197,304) & (285,217) \end{pmatrix} (\text{mod } p) \\ &\equiv \begin{pmatrix} (88,277) & (102,114) \\ (47,97) & (201,79) \end{pmatrix} (\text{mod } p) \equiv M_{ECM}. \end{aligned}$$

5. Security Considerations of EEPKC Based on ECM

The security considerations of the proposed EEPKC based on ECM is determined through the difficulty to solve the ECMDLP and determine a value of a scalar k that is used to compute the ciphertext (C_{ESM1}, C_{ESM2}) .

6. Conclusions

This work proposed new versions of the EC-DL protocol, which are DHKE and EEPKC, by using ECMs. On ECM-DHKE and ECM-EEPCK, the keys and ciphertext in (ECM-EEPCK) are computed as the ECMs. The computations are performed simultaneously to save time. The proposed version depended on the hardness computations of ECMDLP that are needed to recover the original plaintext. From a security point of view, the proposed protocols seem to be more reliable and secure in comparison with the original ones.

References

- [1] Diffie, W., and M. E. Hellman. "New Directions in Cryptography" *IEEE Transactions on Information Theory*, v. IT-22, n. 6 (1976).
- [2] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." *IEEE Transactions on Information Theory* 31.4, 469-472 (1985).
- [3] Inam, Saba, and Rashid Ali. "A new ElGamal-like cryptosystem based on matrices over groupring." *Neural Computing and Applications* 29.11, 1279-1283 (2018).
- [4] Bora, Ravi Kumar, Ashok Kumar, and N. Surendra. "A Study of Elgamal Encryption Scheme of Elliptic Curves Using Golden Matrices." (2020).
- [5] Ajeena, Ruma Kareem K. "The soft graphic integer sub-decomposition method for elliptic scalar multiplication." *Journal of Discrete Mathematical Sciences and Cryptography* 24.6, 1751-1765 (2021).
- [6] Aljamaly, Karrar Taher R., and Ruma Kareem K. Ajeena. "The elliptic scalar multiplication graph and its application in elliptic curve cryptography." *Journal of Discrete Mathematical Sciences and Cryptography* 24.6, 1793-1807 (2021).
- [7] Aljamaly, Karrar Taher R., and Ruma Kareem K. Ajeena. "The kr-elliptic curve public key cryptosystem." *Journal of Physics: Conference Series*, IOP Publishing, Vol. 1879. No. 3 (2021).

Received March, 2022

Revised April, 2022