Palestine Journal of Mathematics

Vol 14(3)(2025) , 1061–1071

CERTAIN NEW RESULTS FOR ELLIPTIC CURVE CRYPTOGRAPHY

Zakariae Cheddour, Abdelhakim Chillali and Ali Mouhib

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 11G05; Secondary 11G30, 14H40.

Keywords and phrases: Group ring, elliptic curves, public key cryptography, Diffie-Hellman, key exchange protocol.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Corresponding Author: Z. CHEDDOUR

Abstract In this paper, we present a new platform for elliptic curve cryptography whose security is based on the difficulty of solving both the factorization problem and the elliptic curve discrete logarithm problem.

1 Introduction

For encrypted communication between two or more parties to be secure, it is necessary to exchange keys securely, for example, a list of keys on paper issued by a trusted authority. Achieving this secure communication was a difficult problem. In 1976, the first key exchange protocol was proposed by Diffie and Hellman (DH) [8] whose security is based on the Discrete Logarithm Problem. This key exchange protocol uses $\mathbb{F}_p^*$ as a platform. Since then, many key exchange protocols have been based on the Discrete Logarithm Problem and (IFP) [17, 19]. As in the case of the Diffie-Hellman key exchange protocol, the platform group of these protocols generally has an abelian structure.
All these systems are based on the difficulty of number theory problems. Moreover, they are widely used but have a disadvantage, which is the advancement of quantum computing [22]. Algorithms based on Shor's algorithm and its variants can be used to efficiently solve the (IFP) and the Discrete Logarithm Problem as well as the elliptic curve discrete logarithm problem on quantum computers [21]. Therefore, these public-key systems like ElGamal [11], Elliptic Curve Cryptosystems (ECC) [4, 5], and RSA [7] will not be secure after a sufficiently powerful quantum computer is built. It is therefore extremely important to build faster and more secure cryptosystems and key exchange protocols that do not rely on number theory. To develop cryptosystems, many attempts have been made to develop an alternative public key cryptography (PKC) that relies on various types of problems, including:

- (DP) the decomposition problem [24],
- (CP) the conjugacy search problem [25],
- (DLP) the Discrete Logarithm Problem on groups of invertible matrices [20],
- (WP) word problem for groups and semigroups [13], etc...

R. Odoni et al., proposed a non-commutative group as a platform for the Diffie-Hellman protocol in [8], which was subsequently analyzed using eigenvalues and the Jordan form in [18, 23]. As a result, the application of non-commutative groups and rings in public-key cryptography and coding theory has received considerable attention [1, 3, 6, 9, 12, 26].
In our prior work [2], we introduced a matrix group defined over an elliptic curve, along with its corresponding diagonal in $\mathbb{Z}/n\mathbb{Z}$, utilizing a novel matrix multiplication operation. This

transformation shifts the focus from solving the Discrete Logarithm Problem to the elliptic curve discrete logarithm problem, which serves as a cornerstone in elliptic curve cryptography and matching-based cryptography. This transition effectively thwarts attempts to reduce the DLP on the group of invertible matrices to either the DLP on finite fields or a straightforward factorization problem, thanks to certain matrix properties such as the Cayley-Hamilton theorem, eigenvalues, and determinant, as discussed in [10, 14, 15, 16].
In this article, we introduce a new problem (FECDLP) based on the factorization with the elliptic curve discrete logarithm problem over a non-commutative semigroup $M_2(\mathbb{Z}/n\mathbb{Z}[M])$, where M is a set of square matrices based on an elliptic curve so that the attacks mentioned above are no longer applicable. We then propose a key exchange protocol based on the factorization with the elliptic curve discrete logarithm problem. Furthermore, we present an analysis of the security and complexity of this key exchange protocol. The remainder of this document is structured as follows: In Section 2, we introduce the group ring, while Section 3 discusses the factorization with the elliptic curve discrete logarithm problem and its complexity. In Section 4, we propose a key exchange protocol based on factorization with the elliptic curve discrete logarithm problem and analyze its complexity and security.

2 Group Ring

This section focuses on defining the group ring on an elliptic curve and evaluating the effectiveness of matrix multiplication in this particular group ring. First, we define the multiplicative group denoted by M, on which we will construct the group ring.
Let's consider Θ as a point of order n on an elliptic curve E defined over $\mathbb{F}_q$, and let $G =< \Theta >$. We define the following set:

$$M = \left\{ \begin{pmatrix} u_1 & T \\ S & u_2 \end{pmatrix} \mid u_1, u_2 \in \mathbb{Z}/n\mathbb{Z},\ S, T \in G \right\}.$$

Let $U = \begin{pmatrix} u_1 & T \\ S & u_2 \end{pmatrix}$ and $V = \begin{pmatrix} v_1 & T' \\ S' & v_2 \end{pmatrix}$ be two elements in M. So,

$$U + V = \begin{pmatrix} u_1 + v_1 & T + T' \\ S + S' & u_2 + v_2 \end{pmatrix},$$

$$U \star V = \begin{pmatrix} u_1 v_1 & v_2 T + u_1 T' \\ v_1 S + u_2 S' & u_2 v_2 \end{pmatrix}.$$

Throughout this article, we will use the symbol m to indicate the order of M.

Remark 1. Throughout this article, multiplication by a scalar is defined and noted as follows: for $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ we take $\bar{a}T = aT$ for a representation $0 \leq a < n$ of $\bar{a}$.

Proposition 2.1. The set $(M, +, \star)$ is a unitary non-commutative ring. Moreover,

$$1_M = \begin{pmatrix} 1 & (0:1:0) \\ (0:1:0) & 1 \end{pmatrix} \text{ and } 0_M = \begin{pmatrix} 0 & (0:1:0) \\ (0:1:0) & 0 \end{pmatrix}.$$

The subsequent proposition offers a description of invertible elements within M.

Proposition 2.2. Let $U = \begin{pmatrix} u_1 & T \\ S & u_2 \end{pmatrix} \in M$, U is invertible iff $gcd(u_i, n) = 1$ for $i = 1, 2$, and then we have,

$$U^{\star(-1)} = \begin{pmatrix} u_1^{-1} & -u_1^{-1}u_2^{-1}T \\ -u_1^{-1}u_2^{-1}S & u_2^{-1} \end{pmatrix} \in M.$$

Proof. Let $V = \begin{pmatrix} v_1 & T' \\ S' & v_2 \end{pmatrix}$ the inverse of U, we have:

$$U \star V = V \star U = 1_M$$

So,

$$U \star V = \begin{pmatrix} u_1 v_1 & v_2 T + u_1 T' \\ v_1 S + u_2 S' & u_2 v_2 \end{pmatrix} = \begin{pmatrix} 1 & (0:1:0) \\ (0:1:0) & 1 \end{pmatrix},$$

and

$$V \star U = \begin{pmatrix} u_1 v_1 & v_1 T + u_2 T' \\ v_2 S + u_1 S' & u_2 v_2 \end{pmatrix} = \begin{pmatrix} 1 & (0:1:0) \\ (0:1:0) & 1 \end{pmatrix}.$$

Thus, $u_i v_i \equiv 1 \pmod{n}$ for $i = 1, 2$ and

$$\begin{aligned} v_2 T + u_1 T' &= (0:1:0), \\ v_1 T + u_2 T' &= (0:1:0), \\ v_1 S + u_2 S' &= (0:1:0), \\ v_2 S + u_1 S' &= (0:1:0). \end{aligned}$$

Therefore, U is invertible iff $gcd(u_i, n) = 1$ for $i = 1, 2$, and then we have, $v_i = u_i^{-1}$ for $i = 1, 2$ and

$$\begin{aligned} T' &= -u_1^{-1} u_2^{-1} T, \\ S' &= -u_2^{-1} u_1^{-1} S. \end{aligned}$$

So,

$$U^{\star(-1)} = \begin{pmatrix} u_1^{-1} & -u_1^{-1} u_2^{-1} T \\ -u_1^{-1} u_2^{-1} S & u_2^{-1} \end{pmatrix} \in M.$$

□

Lemma 1. The c-power of an element $U = \begin{pmatrix} u_1 & T \\ S & u_2 \end{pmatrix} \in M$ and c a positive integer, is given by $U^{\star c} = \begin{pmatrix} u_1^c & \lambda_c T \\ \lambda_c S & u_2^c \end{pmatrix}$, where

$$\lambda_c = \sum_{i+j=c-1} u_1^i u_2^j.$$

Proof. First, for $c = 1$, we obtain that $\lambda_1 = 1$, so $U^{\star 1} = U$. Thus, assuming that $\lambda_c = \sum_{i+j=c-1} u_1^i u_2^j$ for $c \geq 1$, we still need to prove that,

$$\lambda_{c+1} = \sum_{i+j=c} u_1^i u_2^j.$$

Thus,

$$U^{\star(c+1)} = \begin{pmatrix} u_1^c & \lambda_{1,c} T \\ \lambda_c S & u_2^c \end{pmatrix} \star \begin{pmatrix} u_1 & T \\ S & u_2 \end{pmatrix}.$$

Then,

$$U^{\star(c+1)} = \begin{pmatrix} u_1^{c+1} & (u_1^c + u_2 \lambda_{1,c}) T \\ (u_2^c + u_1 \lambda_{1,c}) S & u_2^{c+1} \end{pmatrix}.$$

therefore,

$$\lambda_{c+1} = u_1^c + u_2 \lambda_c = u_1^c + u_2 \sum_{i+j=c-1} u_1^i u_2^j.$$

Thus, for all $c \geq 1$,

$$\lambda_c = \sum_{i+j=c-1} u_1^i u_2^j.$$

Therefore, we can conclude the result. □

As the $\star$-operation is not commutative, we aim to characterize the subset of matrices in M that demonstrate commutativity with the given matrix: $U = \begin{pmatrix} u_1 & sT \\ kT & u_2 \end{pmatrix}$. This characterization involves defining the centralizer of the matrix U on M, denoted as follows.

$$\mathrm{C}_M(U) = \{V \in M \mid U \star V = V \star U\}.$$

Proposition 2.3. With the same notation as above, we have $V = \begin{pmatrix} v_1 & eT \\ fT & v_2 \end{pmatrix} \in \mathrm{C}_M(U)$ iff

$$\begin{cases} v_1 \equiv v_2 \pmod{n}, & if\ u_1 \equiv u_2 \pmod{n}, \\ sf \equiv ke \pmod{n}, & if\ u_1 - u_2 \neq 0 \pmod{n}. \end{cases}$$

Proof. Since,

$$U \star V = \begin{pmatrix} u_1 v_1 & v_2 sT + u_1 eT \\ v_1 kT + u_2 fT & u_2 v_2 \end{pmatrix},$$

and

$$V \star U = \begin{pmatrix} u_1 v_1 & v_1 sT + u_2 eT \\ v_2 kT + u_1 fT & u_2 v_2 \end{pmatrix}.$$

So, we have the result with comparative calculations. □

Next, we'll define the group ring. Suppose that A is a ring and consider the multiplicative group $(M, \star)$. The group ring $A[M]$ is a free module given by

$$\{\sum_{g \in M} \alpha_g g \mid \alpha_g \in A\}.$$

Let $a = \sum_{g \in M} \beta_g g$, $b = \sum_{h \in M} \gamma_g g$ and $c = \sum_{h \in M} \alpha_h h$ be elements of $A[M]$, then

$$a + b = \left(\sum_{g \in M} \beta_g g\right) + \left(\sum_{g \in M} \gamma_g g\right) = \sum_{g \in M} (\beta_g + \gamma_g)\, g$$

and

$$ac = \left(\sum_{g \in M} \beta_g g\right)\left(\sum_{h \in M} \alpha_h h\right) = \sum_{g,h \in M} \beta_g \alpha_h (g \star h) = \sum_{e \in M} \eta_e e$$

where $e = g \star h$ and

$$\eta_e = \sum_{gh=e} \beta_g \alpha_h = \sum_{g} \beta_g \alpha_{g^{-1}e} = \sum_{h} \beta_{eh^{-1}} \alpha_h$$

Example 2.1. (Matrices over the group ring $\mathbb{Z}/n\mathbb{Z}([M])$). Let $p = 107099$ and consider the point $T = (32999, 14634)$ of order $n = 107263$ on $E : y^2 = x^3 + 2x + 10[107099]$. Let $x, y \in \mathbb{Z}/107263\mathbb{Z}([M])$, and "e" denotes its multiplication identity element, such that

$$x = 3A_1 + 2A_2,$$
$$y = 4B_1 + 2A_1 + A_2 \star B_2.$$

Where,

$$A_1 = \begin{pmatrix} 1 & (32999, 14634) \\ (99196, 25036) & 2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & (32999, 14634) \\ (17936, 26766) & 2 \end{pmatrix}$$

$$B_1 = \begin{pmatrix} 5 & (99196, 25036) \\ (99196, 25036) & 2 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & (32999, 14634) \\ (32999, 14634) & 4 \end{pmatrix}$$

Then from the above definition,

$$\begin{aligned} x^2 &= 9A_1^{\star 2} + 6A_1 \star A_2 + 6A_2 \star A_1 + 4A_2^{\star 2}, \\ &= \begin{pmatrix} 25 & (54542, 25619) \\ (56261, 90874) & 100 \end{pmatrix}, \\ y + x &= 4B_1 + 5A_1 + 2A_2 + A_2 \star B_2, \\ &= \begin{pmatrix} 30 & (44357, 10955) \\ (104303, 73225) & 30 \end{pmatrix}. \end{aligned}$$

Similarly, we can calculate xy and yx.

Let $M_{2\times 2}\left(\mathbb{Z}/107263\mathbb{Z}\left([M]\right)\right)$ be the semigroup of 2×2 matrices over the group ring $\mathbb{Z}/107263\mathbb{Z}\left([M]\right)$. Let $U_1, U_2 \in M_{2\times 2}\left(\mathbb{Z}/107263\mathbb{Z}\left([M]\right)\right)$ where

$$U_1 = \begin{pmatrix} 0 & y \\ \mathbf{e} & x \end{pmatrix}, \quad U_2 = \begin{pmatrix} y & \mathbf{e} \\ \mathbf{e} & x \end{pmatrix}$$

then

$$U_1U_2 = \begin{pmatrix} y & yx \\ y + x & \mathbf{e} + x^2 \end{pmatrix},$$

$$U_2U_1 = \begin{pmatrix} \mathbf{e} & y^2 + x \\ x & y + x^2 \end{pmatrix}.$$

Remark 2. All computations presented in this article were performed using the Magma calculator.

3 Factorization with the elliptic curve discrete logarithm problem

This section defines the new factorization with the elliptic curve discrete logarithm problem and discusses its Brute complexity.
First, we will define the elliptic curve discrete logarithm problem.

Definition 3.1. Let $E/\mathbb{F}_q$ be an elliptic curve, and let $T \in E\left(\mathbb{F}_q\right)$ be a point of order k. Given $S \in \langle T\rangle$, the elliptic curve discrete logarithm problem aims to determine the integer n, $0 \leq n \leq k-1$, verifying $S = nT$.

This problem is a specific instance of the Discrete Logarithm Problem, where the cyclic group is represented by the subgroup $\langle T\rangle$ comprised of points on an elliptic curve. The ECDLP holds significant cryptographic relevance due to its perceived computational complexity, serving as the foundation for the security of elliptic curve cryptography.
Next, in the following definition, we will define the factorization search problem, denoted (FP)

Definition 3.2. Let x be an element of M and T, E subgroups of M. The (FP) therefore consists of finding two elements $t \in T$ and $e \in E$ verifying $t.e = x$.

Therefore, we introduce a new factorization with the elliptic curve discrete logarithm problem from the two previous issues.

Definition 3.3. (FECDLP). Consider $a, b \in \mathcal{M}$ where $(\mathcal{M}, \cdot)$ is a finite non-abelian semigroup. So find $s \in \mathbb{Z}$ and $r \in \mathcal{M}$ such that $a = b^s r$. Note that in our case, we have $\mathcal{M} = M_{2\times 2}(\mathbb{Z}/n\mathbb{Z}[M])$.

3.1 Brute force complexity of the Factorization with the elliptic curve discrete logarithm problem

Consider the non-commutative semigroup $\mathcal{M} = M_{2\times 2}(\mathbb{Z}/n\mathbb{Z}[M]) = \{c_1, c_2, \ldots, c_{m^4}\}$ with m is the order of $\mathbb{Z}/n\mathbb{Z}[M]$. Let $r \in \mathcal{M}$ and $s \in \{0, 1, ..., n-1\}$ such that for given $a, b \in \mathcal{M}$, $a = b^s r$. Since $a, b, r \in \mathcal{M}$, they can be expressed as $a = c_i, b = c_j, r = c_k$ with $k, j, i \in \{1, \ldots, m^4\}$. On the other hand, we have m^4 and n possibilities for r and s, respectively. Therefore, the brute force attack to solve the factorization with the elliptic curve discrete logarithm problem requires $O(m^4 n)$ steps, which grows exponentially in the bit size of $m^4 n$, i.e.,

$$m^4 n = e^{\log_e m^4 n} = e^{\log_e 2 \cdot \log_2 m^4 n} = e^{\text{d.size}\,(m^4 n)} \ where\ d = \log_e 2.$$

We will show in the following example that even by using small values of m and n, the size of $\mathcal{M} = M_{2\times 2}(\mathbb{Z}/n\mathbb{Z}[M])$ grows reasonably fast.

Examples 1. Consider the group ring $\mathbb{Z}/5\mathbb{Z}[M]$ of order $m = 25$ and let $x \in \mathbb{Z}/5\mathbb{Z}\,[M]$. So,

$$x = \sum_{i=1}^{5} u_i v_i,$$

where $u_i \in \mathbb{Z}/5\mathbb{Z}$ and $v_i \in M$. Hence, the semigroup $\mathcal{M} = M_{2\times 2}\,(\mathbb{Z}/5\mathbb{Z}\,[M])$ of 2×2 matrices has $(25)^4 = 390625$ elements.

We show the size of $M_{2\times 2}\,(\mathbb{Z}/n\mathbb{Z}\,[M])$ for different values of m in the following table.

$m = 16$	$m = 32$	$m = 81$	$m = 243$
$(16)^4 = 65536$	$(32)^4 = 1048576$	$(81)^4 = 43046721$	$(243)^4 = 3486784401$

Thus, even for small sizes of m, the complexity of the factorization with the elliptic curve discrete logarithm problem over $M_{2\times 2}\,(\mathbb{Z}/n\mathbb{Z}\,[M])$ is significantly high.

4 Key exchange protocol based on the factorization with the elliptic curve discrete logarithm problem

This section presents a key exchange protocol based on factorization with the elliptic curve discrete logarithm problem and provides an interesting numerical example and an analysis of its security and complexity.

4.1 Key exchange protocol

Let $\mathcal{H} = \left\{ A \in \mathcal{M}\ where\ A = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ be a subsemigroup of the finite non-commutative semigroup $\mathcal{M} = M_{2\times 2}\,(\mathbb{Z}/n\mathbb{Z}\,[M])$.
Let q be a power of a prime number p and $E/\mathbb{F}_q$ be an elliptic curve. The following paragraphs describe a key agreement protocol between **Alice** and **Bob**. They own the public data (p, T, B), where $B \in M$ and $T \in E(\mathbb{F}_q)$ has order n.

First **Alice** selects a matrix $A_1 \in M \setminus \mathrm{C}_M(B)$ and publishes $\mathrm{C}_M(A_1)$, similarly, **Bob** selects a matrix $B_2 \in M \setminus \mathrm{C}_M(B)$ and publishes $\mathrm{C}_M(B_2)$.

Alice selects private keys, $c \in \mathbb{N}^*$ and $T = \begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix}$ such that $A_2 \in \mathrm{C}_M(B_2) \setminus \mathrm{C}_M(B)$, and transmits the matrix $T_c = \sum_{j=0}^{c-1} A_1^{c-1-j}(B) A_2^j$ to **Bob**.

Bob selects private keys, $t \in \mathbb{N}^*$ and $E = \begin{pmatrix} B_1 & B \\ 0 & B_2 \end{pmatrix}$ such that $B_1 \in \mathrm{C}_M(A_1) \setminus \mathrm{C}_M(B)$, and transmits the matrix $E_t = \sum_{i=0}^{t-1} B_1^{t-1-i}(B)B_2^i$ to **Alice**.

Next, **Alice** and **Bob** separately calculate the matrices:

$$\textbf{Alice}: E_{t,c} = \sum_{j=0}^{c-1} A_1^{c-j-1} E_t A_2^j \tag{4.1}$$

$$\textbf{Bob}: T_{c,t} = \sum_{i=0}^{t-1} B_1^{t-i-1} T_c B_2^i \tag{4.2}$$

We have, $B_1 \in \mathrm{C}_M(A_1)$ and $A_2 \in \mathrm{C}_M(B_2)$, then

$$\begin{aligned} T_{c,t} &= \sum_{i=0}^{t-1} B_1^{t-i-1} T_c B_2^i = \sum_{i=0}^{t-1} B_1^{t-i-1} \left(\sum_{j=0}^{c-1} A_1^{c-1-j}(B) A_2^j \right) B_2^i \\ &= \sum_{i=0}^{t-1} \sum_{j=0}^{c-1} B_1^{t-i-1} A_1^{c-1-j}(B) A_2^j B_2^i = \sum_{j=0}^{c-1} \sum_{i=0}^{t-1} A_1^{c-j-1} B_1^{t-1-i}(B) B_2^i A_2^j \\ &= \sum_{j=0}^{c-1} A_1^{c-j-1} \left(\sum_{i=0}^{t-1} B_1^{t-1-i}(B) B_2^i \right) A_2^j = \sum_{j=0}^{c-1} A_1^{c-j-1} E_t A_2^j = E_{t,c}. \end{aligned}$$

Thus, both Alice and Bob compute the same shared secret, $\phi = T_{c,t} = E_{t,c}$.

4.2 Numerical example

Alice and **Bob** select a prime number $p = 107099$ and a point $T = (5896, 6763)$ over the elliptic curve $E : y^2 = x^3 + 2x + 10[107099]$ of order $n = 107263$.
First **Alice** selects two matrices from M,

$$A = \begin{pmatrix} 1 & (5896, 6763) \\ (101629, 69640) & 2 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & (5896, 6763) \\ (22874, 70293) & 2 \end{pmatrix}$$

and proceeds to publishes the pair $(A, \mathrm{C}_M(A_1))$, similarly, **Bob** selects two matrices from M,

$$B = \begin{pmatrix} 5 & (101629, 69640) \\ (101629, 69640) & 2 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & (5896, 6763) \\ (5896, 6763) & 4 \end{pmatrix}$$

and proceeds to publishes the pair $(B, \mathrm{C}_M(B_2))$.

Alice selects a private key, $r = 56$ and

$$A_2 = \begin{pmatrix} 2 & (5896, 6763) \\ (5896, 6763) & 3 \end{pmatrix} \in \mathrm{C}_M(B_2).$$

She calculated

$$T_{56} = \sum_{i=0}^{56-1} A_1^{\star(56-1-i)} (A + B) A_2^{\star i} \tag{4.3}$$

$$= \begin{pmatrix} 4323455642275676 10 & (59708, 42145) \\ (21745, 77289) & 209339053182121177270233434 0 \end{pmatrix} \tag{4.4}$$

$$= \begin{pmatrix} 7666 & (59708, 42145) \\ (21745, 77289) & 12558 \end{pmatrix} \tag{4.5}$$

and sends it to **Bob**.
In turn, **Bob** selects a private key, $t = 34$ and

$$B_1 = \begin{pmatrix} 1 & (101629, 69640) \\ (77210, 79507) & 3 \end{pmatrix} \in \mathrm{C}_M(A_1).$$

He calculated

$$E_{34} = \sum_{i=0}^{34-1} B_1^{\star(34-1-i)}(A+B)B_2^{\star i} \tag{4.6}$$

$$= \begin{pmatrix} 50031545098999704 & (99786, 64341) \\ (91468, 81265) & 1180524911990612637148 \end{pmatrix} \tag{4.7}$$

$$= \begin{pmatrix} 64291 & (99786, 64341) \\ (91468, 81265) & 19173 \end{pmatrix} \tag{4.8}$$

and sends it to **Alice**.

Next,
Alice calculates the matrix:

$$E_{34,56} = \begin{pmatrix} u_1 & (69853, 39203) \\ (106326, 69275) & u_2 \end{pmatrix}$$

with,

$$u_1 = 4632654778292424869085 \equiv 14764 \pmod{107263},$$
$$u_2 = 10034144166652023329505464075205 \equiv 72722 \pmod{107263},$$

Bob calculates the matrix:

$$T_{56,34} = \begin{pmatrix} v_1 & (69853, 39203) \\ (106326, 69275) & v_2 \end{pmatrix}$$

with,

$$v_1 = 63923637454821955144 \equiv 14764 \pmod{107263},$$
$$v_2 = 37062579611945283743261 46 \equiv 72722 \pmod{107263}.$$

Hence, $E_{34,56} = T_{56,34}$. So,

$$\phi = \begin{pmatrix} 14764 & (69853, 39203) \\ (106326, 69275) & 72722 \end{pmatrix}. \tag{4.9}$$

4.3 Complexity and Security

Addressing both spatial and temporal complexities is crucial in our cryptographic protocol. While spatial complexity relates to handling a substantial private centralizer, temporal complexity primarily affects the protocol's speed and efficiency.

The centralizer, encompassing elements interacting with the private element, may expand considerably based on the cryptographic operations and algorithms utilized. Dealing with a large centralizer poses significant challenges in spatial complexity, entailing the storage and manipulation of numerous elements throughout protocol execution.

Increasing the number of exchanged elements strengthens security by making decryption more difficult for adversaries. This increased protection proves beneficial in scenarios where robust safety is a priority, even at the cost of increased spatial complexity.

However, in the subsequent discussion, we estimate the computation time required for running the factorization with the elliptic curve discrete logarithm problem.

- Suppose we have $\epsilon-$operations for the elliptic curve law, and δ is a natural number. Therefore, $\delta\epsilon$ operations are required to multiply two matrices of order 2.
- Computing A^t involves $\delta\epsilon\log(n)$ bit operations.
- Determining $T_c = \sum_{j=0}^{c-1} A_1^{c-1-j} B A_2^j$ thus necessitates $2c\delta\epsilon(\log(n)+1)$ operations.
- Consequently, calculating $T_{c,t} = \sum_{i=0}^{t-1} B_1^{t-i-1} T_c B_2^i$ requires $2\delta\epsilon t(c+1)(\log(n)+1)$ operations.
- Therefore, to compute ϕ we need $\mathrm{O}\left(2\delta\epsilon t(c+1)(\log(n)+1)\right)$ bit-operations, which is proportional to $\mathrm{O}\left(2\delta\epsilon t(c+1)\log(n)\right)$.

In our protocol, keys take the form of 2×2 matrices over $\mathbb{Z}/n\mathbb{Z}[M]$. Deriving the shared key involves multiplying five matrices of this type, resulting in computational complexity for key generation of $\mathrm{O}\left(2^4 t(c+1)\log(n)\right)$. Conversely, the complexity of exhaustive search scales proportionally with $\mathrm{O}(\eta n)$, where η denotes the cardinality of the semigroup $M_{2\times 2}(\mathbb{Z}/n\mathbb{Z}[M])$. On the other hand, the Diffie-Hellman protocol is based on the $\mathbb{F}_q^*$ platform, with the keys residing in $\mathbb{F}_q^*$, and the complexity of the key calculation is $\mathrm{O}\left((\log_2 q)^3\right)$. Also, as outlined in Section 4, the protocol's security hinges on the complexity of a computational problem. Specifically, it assumes the challenge of computing the shared key using the publicly available information B, T_c, and E_t. This computational assumption underpins the protocol's security, with a stronger variant known as the decisional assumption. The decisional assumption posits that discerning ϕ from a random element $M_1 B M_2$ is also a challenging task.

In the subsequent security analysis, we scrutinize the protocol's resilience against various attacks documented in existing literature [9, 10, 18, 23]. First, we delve into, **Elliptic Curve Discrete Logarithm Problem Attacks**. Several techniques exist for solving the elliptic curve discrete logarithm problem, such as Baby-Step Giant-Step, and Pollard Rho methods. However, without altering this protocol, the adversary cannot directly apply these methods because, in such approaches, they possess knowledge of an element T and its power T^t. Contrastingly, in our scenario, A_1^c and A_2^j remain concealed, as exemplified by $T_c = \sum_{j=0}^{c-1} A_1^{c-1-j}(B)A_2^j$.
For the **Attacks by group ring decomposition**, M. Eftekhari [10] proposed an analysis of key exchange protocol using group rings as a platform. This cryptanalysis aims at reducing the Discrete Logarithm Problem on $M_{c\times c}(\mathbb{F}_q[S_n])$ to the Discrete Logarithm Problem on block matrices on $\mathbb{F}_q$.
This attack is not realistic for our protocol since we need to know the public key N, M such as $N = M^l$ in this cryptanalysis, instead, we use the secret parameters t, k, A_1 and A_2 with the existing elliptic curve discrete logarithm problem as in Sec. 4. Therefore, we have no advantage over our protocol for this type of cryptanalysis.
Finally, we have an **Explanation with the Random Oracle Model**. In the framework of the Random Oracle Model, elliptic curve operations are treated as abstract mathematical processes, akin to the behavior of the random oracle itself. Within this model, the computation of S from A^sB is viewed as a straightforward mathematical procedure. However, the challenge posed by the Full Domain elliptic curve discrete logarithm problem arises from the inherent difficulty in efficiently computing s and B given S and A^sB, even when equipped with knowledge of the curve parameters. Here's the underlying reasoning:

- Random Oracle Operation for Multiplication: In this context, the multiplication A^sB can be likened to an interaction with a random oracle that generates points on the elliptic curve. The oracle takes AB and applies a random transformation a certain number of times to produce S. Each invocation of this random oracle yields a matrix within a set M, mirroring the behavior of random value generation in other cryptographic settings.

- Unfeasibility of Oracle Reversal: The difficulty of the FECDLP lies in the impracticality of reversing the oracle to determine s and B. This challenge arises from the inherently random and unpredictable nature of the transformations enacted by the oracle. No efficient algorithm is known to effectively reverse this process, necessitating a brute-force search

through all possible values to find s and B, which becomes computationally unfeasible for large elliptic curves.

5 Conclusion

This article presents a novel factorization with the elliptic curve discrete logarithm problem along with its complexity analysis under different security parameters. Building upon the factorization with the elliptic curve discrete logarithm problem, a Diffie-Hellman key exchange scheme is proposed for $M_{2\times 2}\left(\mathbb{Z}/n\mathbb{Z}[M]\right)$, and the security and complexity of the proposed system are thoroughly examined. These findings contribute to the development of secure key exchange protocols and highlight the importance of analyzing the security and complexity of such systems.

Funding

This research received no external funding.

Data availability

Not applicable.

Conflicts of interest

The authors declare no conflict of interest.

References

[1] M.R. Alimoradi, Decoding of cyclic codes over a class of finite rings, Palestine Journal of Mathematics, 12 (2), pp. 321-328, (2023).

[2] Z. Cheddour, A. Chillali and A. Mouhib, The Elliptic matrices and a new kind of cryptography, Boletim da Sociedade Paranaense de Matemática, 41, (2023).

[3] Z. Cheddour, A. Chillali and A. Mouhib, Elliptic curve and k-Fibonacci-like sequence, Scientific African, (2023).

[4] Z. Cheddour, A. Chillali and A. Mouhib, Elliptic curves over a finite ring, Annals of the University of Craiova, Mathematics and Computer Science Series, 50(2), 313–324, (2023).

[5] Z. Cheddour, A. Chillali and A. Mouhib, Generalized Fibonacci Sequences for Elliptic Curve Cryptography, Mathematics, 11(22), (2023).

[6] J. J. Climent, P. R. Navarro and L. Tortosa, Key exchange protocol over non-commutative rings, the case of $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$, International Journal of Computer Mathematics, 89(13-14), 1753-1763, (2012).

[7] R. Cramer and V. Shoup, Signature Schemes Based on the Strong RSA Assumption, ACM Transactions on Information and System Security, 3(3), 161–185, (2000).

[8] W. Diffie and M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 22(6), 644-654, (1976).

[9] M. Eftekhari, A Diffie-Hellman Key exchange protocol using matrices over non-commutative rings, Groups, Complexity, Cryptology, 4(1), 167-176, (2012).

[10] M. Eftekhari, Cryptanalysis of some protocols using matrices over group rings, International Conference on Cryptology in Africa: Progress in Cryptology - AFRICACRYPT 2017, LNCS 10239, (2017).

[11] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31(4), 469-472, (1985).

[12] N.U. Rehman, M. Azmi, G. Mohammad, Reversible cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{k1}\mathbb{F}_2$, Palestine Journal of Mathematics, 12 (2), pp. 395-407, (2023).

[13] N. Ghadbane, On public key cryptosystem based on the word problem in a group, Journal of Discrete Mathematical Sciences and Cryptography, 25(6), 1563-1568, (2022).

[14] G. Indivar, P. Atul and K. D. Manish, A Key exchange protocol using matrices over group ring, Asian-European Journal of Mathematics, 12(1), (2019).

[15] D. Kahrobaei, C. Koupparis and V. Shpilrain, Public key exchange using matrices over group rings, Groups, Complexity, Cryptology, 5(1), 97-115, (2013).

[16] N. Koblitz, A Course in Number Theory and Cryptography, 2nd edn., Springer, New York, (1994).

[17] A. J. Menezes and Y. H. Wu, The discrete logarithm problem in $GL(n, q)$, Ars Combinatoria, 47, 23-32, (1997).

[18] G. Micheli, Cryptanalysis of a non-commutative Key exchange protocol, Advances in Mathematics of Communications, 9(2), 247-253, (2015).

[19] A. Odlyzko, Discrete logarithms: The past and the future, Designs, Codes, and Cryptography, 19, 129–145, (2000).

[20] R. Odoni, V. Varadharajan and P. Sanders, Public key distribution in matrix rings, Electronics Letters, 20(9), 386-387, (1984).

[21] J. Proos and C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves, Quantum Information and Computation, 3, 317-344, (2003).

[22] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing, 26(5), 1484-1509, (1997).

[23] V. Shpilrain, Cryptanalysis of Stickel's key exchange scheme, Proc. of Computer Science in Russia, LNCS 5010, 283-288, (2008).

[24] V. Shpilrain and A. Ushakow, A new Key exchange protocol based on the decomposition problem, arXiv preprint, arXiv:math.GR/0512140, (2005).

[25] V. Shpilrain and A. Ushakow, The conjugacy search problem in public key cryptography: Unnecessary and insufficient, Applicable Algebra in Engineering, Communications and Computing, 17(3-4), 285-289, (2006).

[26] A. P. Stakhov, The golden matrices and a new kind of cryptography, Chaos, Solitons and Fractals, 32, 1138–1146, (2007).

Author information

Zakariae Cheddour, Department of Mathematics, University Abdelmalek Essaadi, Faculty of Sciences and Technology Al Hoceima, BP 34. Ajdir 32003 Al Hoceima, Morocco.
E-mail: z.cheddour@uae.ac.ma

Abdelhakim Chillali, MATH Department, LSI Laboratory, University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, 1223., Morocco.
E-mail: abdelhakim.chillali@usmba.ac.ma

Ali Mouhib, MATH Department, LSI Laboratory, University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, 1223, Morocco., Morocco.
E-mail: ali.mouhib@usmba.ac.ma

Received: 2024-11-10
Accepted: 2025-03-21