Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 1, pp. 75–93
DOI : 10.47974/JDMSC-1573

A new public key cryptosystem based on the non-commutative ring R

Bilel Selikh *
Department of Mathematics
Laboratory of Pure and Applied Mathematics
Mohamed Boudiaf University of M'sila
P. O. Box 166 Ichbilia
M'sila 28000
Algeria

Abdelhakim Chillali †
Department of Mathematics, Physics & Computer Science
Polydisciplinary Faculty
Laboratory of Engineering Sciences
Sidi Mohamed Ben Abdellah University
Taza
Morocco

Douadi Mihoubi §
Nacer Ghadbane ‡
Department of Mathematics
Laboratory of Pure and Applied Mathematics
Mohamed Boudiaf University of M'sila
P. O. Box 166 Ichbilia
M'sila 28000
Algeria

Abstract

In this paper, we present a new public cryptosystem based on one of the most problems (word problem, solving a non-linear system problem, integer factorization problem and discrete logarithm problem,...) is the conjugal classical problem (CCP) over a

* *E-mail:* **bilel.selikh@univ-msila.dz (Corresponding Author)**
† *E-mail:* **abdelhakim.chillali@usmba.ac.ma**
§ *E-mail:* **douadi.mihoubi@univ-msila.dz**
‡ *E-mail:* **nasser.ghedbane@univ-msila.dz**

non commutative ring. In generally this cryptosystem is very difficult to solve for decipher. Firstly, by using the elliptic curve over the finite ring $\mathbb{F}_q[\varepsilon]$, where $\varepsilon^4 = \varepsilon^3$, with $q = p^d$ and p is prime number greater than or equal to 5, $d \in \mathbb{N}^*$ [12] we define the non-commutative ring *R*. Secondly, by using the protocol of Diffie-Hellman [4] we have proposed a novel encryption scheme on *R* and we study the problem CCP over it. Precisely, we will make a new fully homomorphic encryption scheme over the ring *R* based on the two difficult problems; conjugal classical problem and discrete logarithm problem.

Subject Classification: *[2010] 14H52, 16S50, 11T55, 94A60, 11T71.*

Keywords: *Elliptic curve, Non commutative ring, Matrix, Cryptography, Conjugal problem, Fully homomorphic cryptosystem.*

1. Introduction

Information security, is the science that works to protect the information and equipment used to store, process and transmit it from theft, intrusion, natural disasters or all of them. It works to keep it available to authorized individuals and the inability to obtain information, except by persons authorized to do so. In computer science, cryptography is a way of protect information and communications between parties by using codes, so that only the parties targeted by the information can read and process it. This is done through the use of specific algorithms (which is a set of mathematical calculations) and a private key.

In cryptography, to transform messages in ways that are hard to decipher, these deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and protect confidential transactions such as credit card and debit card transactions and email (see [6, 7]).

In 1976, public key algorithms came in public sphere when Whitfield Diffie and Martin Hellman published their article entitled by “New Directions in Cryptography “ (see[4]). This is known as the D-H key exchange, its roots go back to the 1970s. The D-H key exchange was one of the most important developments in a public key cryptography and it is still frequently implemented in a range of today is different security protocols.

Naturally, strong and secure encryption system have emerged in the past few decades, one way to achieve confidentiality in applications, such as secure your connection to a website, electronic voting, sending encrypted emails and online banking etc are homomorphic and especially fully homomorphic cryptographic schemes. Originally the notion of fully homomorphic encryption (FHE) scheme is called a privacy homomorphism, were introduced by R. L. Rivest, L. Adleman and M. L. Dertouzos in their article in 1978 (see [9]). In particular, FHE scheme is one of the main pillars to exploit the complete advantages of cloud computing. Homomorphic encryption scheme provides a mechanism to perform operations on encrypted data without decrypting it. Moreover, fully homomorphic encryption scheme allows arbitrary operations on encrypted data, hence it is considered as the holy grail of cryptography (see [3, 10]). The aim of these whole homomorphic systems is data integrity in communication, non repudiation, confidentiality and storage processes, such as the ability to perform computations to untrusted persons.

C. Meshram and X. Li in [8], have introduced a new efficient authentication protocol for discrete logarithm define over multiplicative group based cryptosystem.

P. Sundarayya and G. Vara Prasad in [13], have proposed to develop a public key cryptosystem using affine Hill's cipher.

A. Boulbot et al. in [1], have presented a new method of cryptography based on problem of conjugal on the non commutative ring R, by using elliptic curve over the ring $\mathbb{F}_q[e] := \mathbb{F}_q[X]/(X^2 - X)$, where $e^2 = e$.

The main motivation of our paper is to design efficient cryptographic protocol on a non commutative ring. Where data is already fully homomorphic encryption so that any arbitrary operations are possible on encrypted data as and when required in the cloud.

Firstly, we will show the commutative ring $\mathbb{F}_q[X]/(X^4 - X^3)$ and elliptic curve over it, this section is preliminaries from the article [12].

In section 3, we define the ring $(R, +, *)$, who is not commutative for the law $"*"$. In section 4, we describe a new method of cryptography on this ring R based on the two difficult problems are discrete logarithm problem and conjugal classical problem. Finally, we conclude this paper with a cryptographic example.

2. Preliminaries

Let $\mathbb{F}_q[\varepsilon] = \mathbb{F}_q[X]/(X^4 - X^3)$, where $\varepsilon^4 = \varepsilon^3$, with $q = p^d$ and p is prime number $\geqslant 5$, $d \in \mathbb{N}^*$. The arithmetic operations in $\mathbb{F}_q[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3 \text{and}$$

$$\begin{aligned} X \cdot Y = {} & (x_0 y_0) + (x_0 y_1 + x_1 y_0)\varepsilon + (x_0 y_2 + x_1 y_1 + x_2 y_0)\varepsilon^2 \\ & + ((x_0 + x_1 + x_2 + x_3) y_3 + (x_1 + x_2 + x_3) y_2 + (x_2 + x_3) y_1 + x_3 y_0)\varepsilon^3, \end{aligned}$$

where $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$.

- The ring $\mathbb{F}_q[\varepsilon]$ is a vector space over $\mathbb{F}_q$ of dimension 4, and have $\{1,\varepsilon,\varepsilon^2,\varepsilon^3\}$ as basis, we write: $\mathbb{F}_q[\varepsilon] = \mathbb{F}_q + \mathbb{F}_q\varepsilon + \mathbb{F}_q\varepsilon^2 + \mathbb{F}_q\varepsilon^3$, and it is a finite non local commutative ring.
- An elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$, as a defined in the projective space $\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$, which is given by the homogeneous equation of Weierstrass, $Y^2Z = X^3 + aXZ^2 + bZ^3$, where $(a,b) \in (\mathbb{F}_q[\varepsilon])^2$ such that the discriminant $\Delta := 4a^3 + 27b^2$ is invertible in $\mathbb{F}_q[\varepsilon]$.

We denote it by:

$$E_{a,b}(\mathbb{F}_q[\varepsilon]) = \{[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon]) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

3. The ring R

$E_{a,b}(\mathbb{F}_q[\varepsilon])$ is an elliptic curve over $\mathbb{F}_q[\varepsilon]$, P is a point of order l and G is the subgroup generated by P. We consider the set:

$$R = \left\{ \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \mid (x_i)_{1\leqslant i\leqslant 3} \in \{0,1,2,\ldots,l-1\} \text{ and } S,L,T \in G \right\}.$$

Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ and $Y = \begin{bmatrix} x_1' & S' & L' \\ 0 & x_2' & T' \\ 0 & 0 & x_3' \end{bmatrix}$ be two elements in R, on which two binary operations are defined, called addition $(+)$ and start $(*)$ and denoted by:

$$X + Y = \begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix},$$

$$X * Y = \begin{bmatrix} x_1x_1' & x_1S'+x_2'S & x_1L'+x_3'L \\ 0 & x_2x_2' & x_2T'+x_3'T \\ 0 & 0 & x_3x_3' \end{bmatrix}.$$

Lemma 3.1 : $(R,+,*)$ *is a non commutative ring with identity*

$$1_R = \begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix}.$$

Proof: Let $X=\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$, $Y=\begin{bmatrix} x_1' & S' & L' \\ 0 & x_2' & T' \\ 0 & 0 & x_3' \end{bmatrix}$ and $Z=\begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix}$ be three elements in R.

- Associative laws: $\forall X, Y, Z \in R.$

  For addition law

$$(X+Y)+Z=\begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix}+\begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix}$$

$$=\begin{bmatrix} x_1+x_1'+x_1'' & S+S'+S'' & L+L'+L'' \\ 0 & x_2+x_2'+x_2'' & T+T'+T'' \\ 0 & 0 & x_3+x_3'+x_3'' \end{bmatrix}$$

$$=X+(Y+Z).$$

  For start law

$$(X*Y)*Z=\begin{bmatrix} x_1x_1' & x_1S'+x_2'S & x_1L'+x_3'L \\ 0 & x_2x_2' & x_2T'+x_3'T \\ 0 & 0 & x_3x_3' \end{bmatrix}*\begin{bmatrix} x_1'' & S'' & L'' \\ 0 & x_2'' & T'' \\ 0 & 0 & x_3'' \end{bmatrix}$$

$$=\begin{bmatrix} x_1x_1'x_1'' & x_1x_1'S''+x_2''(x_1S'+x_2'S) & x_1x_1'L''+x_3''(x_1L'+x_3'L) \\ 0 & x_2x_2'x_2'' & x_2x_2'T''+x_3''(x_2T'+x_3'T) \\ 0 & 0 & x_3x_3'x_3'' \end{bmatrix}$$

$$=\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}*\begin{bmatrix} x_1'x_1'' & x_1'S''+x_2''S' & x_1'L''+x_3''L' \\ 0 & x_2'x_2'' & x_2'T''+x_3''T' \\ 0 & 0 & x_3'x_3'' \end{bmatrix}=X*(Y*Z).$$

- Commutative law: $\forall X, Y \in R,$

$$X+Y=\begin{bmatrix} x_1+x_1' & S+S' & L+L' \\ 0 & x_2+x_2' & T+T' \\ 0 & 0 & x_3+x_3' \end{bmatrix}=\begin{bmatrix} x_1'+x_1 & S'+S & L'+L \\ 0 & x_2'+x_2 & T'+T \\ 0 & 0 & x_3'+x_3 \end{bmatrix}=Y+X.$$

  So, + is commutative.

- A non commutative law: assume that G is the subgroup generated by P of order 30.

$$\exists X=\begin{bmatrix} 2 & 2P & 4P \\ 0 & 4 & 3P \\ 0 & 0 & 1 \end{bmatrix}, Y=\begin{bmatrix} 1 & 4P & 2P \\ 0 & 2 & 5P \\ 0 & 0 & 3 \end{bmatrix}\in R \text{ such that}$$

$$X*Y=\begin{bmatrix} 2 & 12P & 16P \\ 0 & 8 & 29P \\ 0 & 0 & 3 \end{bmatrix}\neq\begin{bmatrix} 2 & 18P & 6P \\ 0 & 8 & 11P \\ 0 & 0 & 3 \end{bmatrix}=Y*X.$$

  So, $*$ is not commutative.

- Distributive laws: $\forall X, Y, Z \in R,$

$$(X+Y)*Z=\begin{bmatrix} x_1+x'_1 & S+S' & L+L' \\ 0 & x_2+x'_2 & T+T' \\ 0 & 0 & x_3+x'_3 \end{bmatrix}*\begin{bmatrix} x''_1 & S'' & L'' \\ 0 & x''_2 & T'' \\ 0 & 0 & x''_3 \end{bmatrix}$$

$$=\begin{bmatrix} (x_1+x'_1)x''_1 & (x_1+x'_1)S''+x''_2(S+S') & (x_1+x'_1)L''+x''_3(L+L') \\ 0 & (x_2+x'_2)x''_2 & (x_2+x'_2)T''+x''_3(T+T') \\ 0 & 0 & (x_3+x'_3)x''_3 \end{bmatrix}$$

$$=\begin{bmatrix} x_1x''_1 & x_1S''+x''_2S & x_1L''+x''_3L \\ 0 & x_2x''_2 & x_2T''+x''_3T \\ 0 & 0 & x_3x''_3 \end{bmatrix}+\begin{bmatrix} x'_1x''_1 & x'_1S''+x''_2S' & x'_1L''+x''_3L' \\ 0 & x'_2x''_2 & x'_2T''+x''_3T' \\ 0 & 0 & x'_3x''_3 \end{bmatrix}$$

$$=X*Z+Y*Z.$$

$$Z*(X+Y)=\begin{bmatrix} x''_1 & S'' & L'' \\ 0 & x''_2 & T'' \\ 0 & 0 & x''_3 \end{bmatrix}*\begin{bmatrix} x_1+x'_1 & S+S' & L+L' \\ 0 & x_2+x'_2 & T+T' \\ 0 & 0 & x_3+x'_3 \end{bmatrix}$$

$$=\begin{bmatrix} x''_1(x_1+x'_1) & x''_1(S+S')+(x_2+x'_2)S'' & x''_1(L+L')+(x_3+x'_3)L'' \\ 0 & x''_2(x_2+x'_2) & x''_2(T+T')+(x_3+x'_3)T'' \\ 0 & 0 & x''_3(x_3+x'_3) \end{bmatrix}$$

$$=\begin{bmatrix} x''_1x_1 & x''_1S+x_2S'' & x''_1L+x_3L'' \\ 0 & x''_2x_2 & x''_2T+x_3T'' \\ 0 & 0 & x''_3x_3 \end{bmatrix}+\begin{bmatrix} x''_1x'_1 & x''_1S'+x'_2S'' & x''_1L'+x'_3L'' \\ 0 & x''_2x'_2 & x''_2T'+x'_3T'' \\ 0 & 0 & x''_3x'_3 \end{bmatrix}$$

$$=Z*X+Z*Y.$$

So, $*$ is distributive with respect to +.

- Additive identity: $\forall X \in R$,

$$X+0_R=\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}+\begin{bmatrix} 0 & [0:1:0] & [0:1:0] \\ 0 & 0 & [0:1:0] \\ 0 & 0 & 0 \end{bmatrix}=\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$$

$$=\begin{bmatrix} 0 & [0:1:0] & [0:1:0] \\ 0 & 0 & [0:1:0] \\ 0 & 0 & 0 \end{bmatrix}+\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}=0_R+X=X.$$

So, $0_R=\begin{bmatrix} 0 & [0:1:0] & [0:1:0] \\ 0 & 0 & [0:1:0] \\ 0 & 0 & 0 \end{bmatrix}$ is called the additive identity element of R.

- Start identity: $\forall X \in R$,

$$X*1_R=\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}*\begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix}=\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$$

$$=\begin{bmatrix} 1 & [0:1:0] & [0:1:0] \\ 0 & 1 & [0:1:0] \\ 0 & 0 & 1 \end{bmatrix}*\begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}=1_R*X=X.$$

So, $1_R = \begin{bmatrix} 1 & [0{:}1{:}0] & [0{:}1{:}0] \\ 0 & 1 & [0{:}1{:}0] \\ 0 & 0 & 1 \end{bmatrix}$ is called the start identity element of R.

- Additive inverses: $\forall X \in R$,

$$X + (-X) = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} + \begin{bmatrix} -x_1 & -S & -L \\ 0 & -x_2 & -T \\ 0 & 0 & -x_3 \end{bmatrix} = \begin{bmatrix} 0 & [0{:}1{:}0] & [0{:}1{:}0] \\ 0 & 0 & [0{:}1{:}0] \\ 0 & 0 & 0 \end{bmatrix} = 0_R.$$

So, $-X = \begin{bmatrix} -x_1 & -S & -L \\ 0 & -x_2 & -T \\ 0 & 0 & -x_3 \end{bmatrix}$ is called the additive inverse of X.

□

Lemma 3.2 : *Let* $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \in R$, *the element* X *is invertible if and only if* $\gcd(x_i, l) = 1$, *for* $1 \leqslant i \leqslant 3$, *in this case we have:*

$$X^{-1^*} = \begin{bmatrix} x_1^{-1} & -x_1^{-1}x_2^{-1}S & -x_1^{-1}x_3^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_3^{-1}T \\ 0 & 0 & x_3^{-1} \end{bmatrix}.$$

Proof: Let $Y = \begin{bmatrix} x_1' & S' & L' \\ 0 & x_2' & T' \\ 0 & 0 & x_3' \end{bmatrix}$ the inverse of X we have: $X * Y = Y * X = 1_R$.
So,

$$X * Y = \begin{bmatrix} x_1x_1' & x_1S'+x_2'S & x_1L'+x_3'L \\ 0 & x_2x_2' & x_2T'+x_3'T \\ 0 & 0 & x_3x_3' \end{bmatrix} = \begin{bmatrix} 1 & [0{:}1{:}0] & [0{:}1{:}0] \\ 0 & 1 & [0{:}1{:}0] \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$Y * X = \begin{bmatrix} x_1x_1' & x_1'S+x_2S' & x_1'L+x_3L' \\ 0 & x_2x_2' & x_2'T+x_3T' \\ 0 & 0 & x_3x_3' \end{bmatrix} = \begin{bmatrix} 1 & [0{:}1{:}0] & [0{:}1{:}0] \\ 0 & 1 & [0{:}1{:}0] \\ 0 & 0 & 1 \end{bmatrix}$$

$$x_i x_i' \equiv 1[l], \text{for } 1 \leqslant i \leqslant 3$$

thus

$$\begin{cases} x_1S'+x_2'S=[0{:}1{:}0] \\ x_1'S+x_2S'=[0{:}1{:}0] \end{cases} \Rightarrow S' = -x_1^{-1}x_2'S = -x_2^{-1}x_1'S = -x_1^{-1}x_2^{-1}S$$

$$\begin{cases} x_1L'+x_3'L=[0{:}1{:}0] \\ x_1'L+x_3L'=[0{:}1{:}0] \end{cases} \Rightarrow L' = -x_1^{-1}x_3'L = -x_3^{-1}x_1'L = -x_1^{-1}x_3^{-1}L$$

$$\begin{cases} x_2T'+x_3'T=[0{:}1{:}0] \\ x_2'T+x_3T'=[0{:}1{:}0] \end{cases} \Rightarrow T' = -x_2^{-1}x_3'T = -x_3^{-1}x_2'T = -x_2^{-1}x_3^{-1}T$$

Therefore, the element X is invertible if and only if $\gcd(x_i, l) = 1$, for $1 \leqslant i \leqslant 3$, in this case we have:

$$X^{-1^*} = \begin{bmatrix} x_1^{-1} & -x_1^{-1}x_2^{-1}S & -x_1^{-1}x_3^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_3^{-1}T \\ 0 & 0 & x_3^{-1} \end{bmatrix}.$$

□

Lemma 3.3 : *Let k be a strictly positive integer.*

Then if $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ *is any element of R. The k-power of X can be given by*

$$X^k = \begin{bmatrix} x_1^k & \alpha_k S & \beta_k L \\ 0 & x_2^k & \gamma_k T \\ 0 & 0 & x_3^k \end{bmatrix} \text{ where : } \begin{cases} \alpha_k = \sum_{i+j=k-1} x_1^i x_2^j; \\ \beta_k = \sum_{i+j=k-1} x_1^i x_3^j; \\ \gamma_k = \sum_{i+j=k-1} x_2^i x_3^j. \end{cases}$$

Proof: Using a proof is by induction on k
for $k = 1$: we have $\alpha_1 = 1, \beta_1 = 1$ and $\gamma_1 = 1$
for $k \geqslant 1$ assume that,

$$\begin{cases} \alpha_k = \sum_{i+j=k-1} x_1^i x_2^j; \\ \beta_k = \sum_{i+j=k-1} x_1^i x_3^j; \\ \gamma_k = \sum_{i+j=k-1} x_2^i x_3^j. \end{cases}$$

and proof that:

$$\begin{cases} \alpha_{k+1} = \sum_{i+j=k} x_1^i x_2^j; \\ \beta_{k+1} = \sum_{i+j=k} x_1^i x_3^j; \\ \gamma_{k+1} = \sum_{i+j=k} x_2^i x_3^j. \end{cases}$$

We have:

$$X^{k+1} = \begin{bmatrix} x_1^k & \alpha_k S & \beta_k L \\ 0 & x_2^k & \gamma_k T \\ 0 & 0 & x_3^k \end{bmatrix} * \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} = \begin{bmatrix} x_1^{k+1} & x_1^k S + x_2 \alpha_k S & x_1^k L + x_3 \beta_k L \\ 0 & x_2^{k+1} & x_2^k T + x_3 \gamma_k T \\ 0 & 0 & x_3^{k+1} \end{bmatrix}$$

$$\text{thus, } \begin{cases} \alpha_{k+1} = x_1^k + x_2 \alpha_k = x_1^k + x_2 \sum_{i+j=k-1} x_1^i x_2^j = \sum_{i+j=k} x_1^i x_2^j; \\ \beta_{k+1} = x_1^k + x_3 \beta_k = x_1^k + x_3 \sum_{i+j=k-1} x_1^i x_3^j = \sum_{i+j=k} x_1^i x_3^j; \\ \gamma_{k+1} = x_2^k + x_3 \gamma_k = x_2^k + x_3 \sum_{i+j=k-1} x_2^i x_3^j = \sum_{i+j=k} x_2^i x_3^j. \end{cases}$$

we conclude that, $\forall k \geqslant 1, \begin{cases} \alpha_k = \Sigma_{i+j=k-1} x_1^i x_2^j; \\ \beta_k = \Sigma_{i+j=k-1} x_1^i x_3^j; \\ \gamma_k = \Sigma_{i+j=k-1} x_2^i x_3^j. \end{cases}$

Definition 3.1 : Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \in R.$ We define the tilde of X; $\tilde{X}$ which is written as follows: $\tilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}.$

Lemma 3.4 : *Let X be an element in the ring R. Then:* $\tilde{\tilde{X}} = X.$

Proof: We have: $\tilde{\tilde{X}} = \widetilde{\begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}} = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} = X.$ □

Lemma 3.5 : *Let* $(X,Y) \in R^2$. *Then:* $\widetilde{X+Y} = \widetilde{X} + \widetilde{Y}.$

Proof: Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ and $Y = \begin{bmatrix} x'_1 & S' & L' \\ 0 & x'_2 & T' \\ 0 & 0 & x'_3 \end{bmatrix}$ be two elements in R.

$$\widetilde{X+Y} = \widetilde{\begin{bmatrix} x_1+x'_1 & S+S' & L+L' \\ 0 & x_2+x'_2 & T+T' \\ 0 & 0 & x_3+x'_3 \end{bmatrix}} = \begin{bmatrix} x_3+x'_3 & T+T' & L+L' \\ 0 & x_2+x'_2 & S+S' \\ 0 & 0 & x_1+x'_1 \end{bmatrix}$$

$$= \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix} + \begin{bmatrix} x'_3 & T' & L' \\ 0 & x'_2 & S' \\ 0 & 0 & x'_1 \end{bmatrix} = \widetilde{X} + \widetilde{Y}.$$

□

Proposition 3.1 : *Let* X, Y *be two elements in the ring* R. *Then:*

$$\widetilde{X * Y} = \widetilde{Y} * \widetilde{X}.$$

Proof: Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix}$ and $Y = \begin{bmatrix} x'_1 & S' & L' \\ 0 & x'_2 & T' \\ 0 & 0 & x'_3 \end{bmatrix}$ be two elements in R.

$$X * Y = \begin{bmatrix} x_1x'_1 & x_1S'+x'_2S & x_1L'+x'_3L \\ 0 & x_2x'_2 & x_2T'+x'_3T \\ 0 & 0 & x_3x'_3 \end{bmatrix}$$

$$\widetilde{X * Y} = \begin{bmatrix} x_3x'_3 & x_2T'+x'_3T & x_1L'+x'_3L \\ 0 & x_2x'_2 & x_1S'+x'_2S \\ 0 & 0 & x_1x'_1 \end{bmatrix} = \begin{bmatrix} x'_3 & T' & L' \\ 0 & x'_2 & S' \\ 0 & 0 & x'_1 \end{bmatrix} * \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix} = \widetilde{Y} * \widetilde{X}.$$

□

Lemma 3.6 : *If the element X is invertible in the ring R. Then $\widetilde{X}$ is invertible and we have:*

$$(\widetilde{X})^{-1^*} = \widetilde{X^{-1^*}}.$$

Proof: Let $X = \begin{bmatrix} x_1 & S & L \\ 0 & x_2 & T \\ 0 & 0 & x_3 \end{bmatrix} \in R,$ the tilde of X is $\widetilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$ then:

$$(\widetilde{X})^{-1^*} = \begin{bmatrix} x_3^{-1} & -x_3^{-1}x_2^{-1}T & -x_3^{-1}x_1^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_1^{-1}S \\ 0 & 0 & x_1^{-1} \end{bmatrix} = \overline{\begin{bmatrix} x_1^{-1} & -x_1^{-1}x_2^{-1}S & -x_1^{-1}x_3^{-1}L \\ 0 & x_2^{-1} & -x_2^{-1}x_3^{-1}T \\ 0 & 0 & x_3^{-1} \end{bmatrix}} = \widetilde{X^{-1*}}.$$

□

Using the Lemma 3.3, we deduce the following corollary.

Corollary 3.1 : *Let $k \in \mathbb{N}^*$. Then if $\widetilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$ is any element of R, the k-power of $\widetilde{X}$ can be given by:*

$$(\widetilde{X})^k = \begin{bmatrix} x_3^k & \gamma_k T & \beta_k L \\ 0 & x_2^k & \alpha_k S \\ 0 & 0 & x_1^k \end{bmatrix}, \textit{ where}: \begin{cases} \alpha_k = \Sigma_{i+j=k-1} x_1^i x_2^j; \\ \beta_k = \Sigma_{i+j=k-1} x_1^i x_3^j; \\ \gamma_k = \Sigma_{i+j=k-1} x_2^i x_3^j. \end{cases}$$

Corollary 3.2 : *Let $k \in \mathbb{N}^*$, the k power of $\widetilde{X} = \begin{bmatrix} x_3 & T & L \\ 0 & x_2 & S \\ 0 & 0 & x_1 \end{bmatrix}$ given by: $(\widetilde{X})^k = \widetilde{X^k}$.*

The center of a ring R, denoted as $Z(R)$ is the subring consisting of the elements X such that $X * Y = Y * X$ for all element Y in R.

Proposition 3.2 : The mapping φ given by:

$$\begin{array}{ccc} \varphi : Z(R) & \rightarrow & Z(R) \\ X & \mapsto & \widetilde{X} \end{array}$$

is an isomorphism.

Proof: For all $X, Y \in Z(R)$

1. φ is a ring morphism:
   - $\varphi(X+Y) = \widetilde{X+Y} = \widetilde{X} + \widetilde{Y} = \varphi(X) + \varphi(Y)$.
   - $\varphi(X * Y) = \widetilde{X * Y} = \widetilde{Y} * \widetilde{X} = \widetilde{X} * \widetilde{Y} = \varphi(X) * \varphi(Y)$.
   - $\varphi(1_{Z(R)}) = \tilde{1}_{Z(R)} = 1_{Z(R)}$.

2. φ is a injective:

$$\varphi(X) = \varphi(Y) \Leftrightarrow \widetilde{X} = \widetilde{Y} \Leftrightarrow \widetilde{\widetilde{X}} = \widetilde{\widetilde{Y}} \Leftrightarrow X = Y.$$

3. φ is a surjective:
   $\forall\, Y \in Z(R),\ \ \exists X = \widetilde{Y} \in Z(R)$ such that $\varphi(X) = \varphi(\widetilde{Y}) = \widetilde{\widetilde{Y}} = Y.$

Finally, by (1),(2) and (3) the mapping φ is an isomorphism. □

4. Crytpographic protocol

In this section we describe, fully homomorphic encryption scheme, exchange of secret key and we provide to construct a new encryption scheme using the non-commutative ring R.

Definition 4.1 (see [2]) **:** A public key cryptosystem is a triplet $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ such that:

- $\mathcal{K}$ is a finite set called space of the keys.
- $\mathcal{E}$ is a finite set of the plaintext space.
- $\mathcal{D}$ is a finite set of the ciphertext space.
- For all outputs $(pk, sk) \in \mathcal{K},$ there is an encryption function $Encpk$ and a decryption function $Decsk$ such that:
  1. For any plaintext $m \in \mathcal{E},$ the ciphertext is: $c = Encpk(m, pk) \in \mathcal{D}.$
  2. For any ciphertext $c \in \mathcal{D},$ the plaintext is: $m = Decsk(c, sk) \in \mathcal{E}.$
  3. For any plaintext m: $Decsk(Encpk(m, pk), sk) = m.$

Definition 4.2 (see [1, 3, 5]) : *A public key encryption scheme* $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ *is homomorphic if for all outputs* $(pk, sk) \in \mathcal{K},$ *it is possible to define groups* $(\mathcal{M}, \star),$ $(\mathcal{C}, \circledcirc)$ *so that:*

- The plaintext space $\mathcal{M},$ and all ciphertexts output by $Encpk$ are elements of $\mathcal{C}.$
- For any $\mathfrak{m}_1, \mathfrak{m}_2 \in \mathcal{M}$ and $\mathfrak{c}_1, \mathfrak{c}_2 \in \mathcal{C}$ with $\mathfrak{m}_1 = Decsk(\mathfrak{c}_1, sk)$ and $\mathfrak{m}_2 = Decsk(\mathfrak{c}_2, sk)$ holds that:

$$Decsk(\mathfrak{c}_1 \circledcirc \mathfrak{c}_1, sk) = \mathfrak{m}_1 \star \mathfrak{m}_2.$$

A fully homomorphic encryption scheme can be defined as a tuple of three algorithms $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ for which the message space is a ring $(R, \ominus, \circledast)$ and the ciphertext space is also a ring $(R', \oplus, \odot)$ such that for all messages $\mathfrak{m}_1, \mathfrak{m}_2 \in R,$ and all outputs $(pk, sk) \in \mathcal{K}$ we have:

$$\mathfrak{m}_1 \ominus \mathfrak{m}_2 = Decsk(Encpk(\mathfrak{m}_1, pk) \oplus Encpk(\mathfrak{m}_2, pk), sk),$$

$$\mathfrak{m}_1 \circledast \mathfrak{m}_2 = Decsk(Encpk(\mathfrak{m}_1, pk) \odot Encpk(\mathfrak{m}_2, pk), sk).$$

If $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric fully homomorphic encryption scheme, we will have a single key for encryption and decryption, so the role of pk will be played by sk.

A scheme is supposed to be somewhat homomorphic if it permits only a limited number of additions and multiplications.

4.1 *Exchange of secret keys*

Diffie-Hellman key exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network (see [4]).

For a secure encrypted message exchange between two entities Alice and Bob requires an exchange of keys first by using protocol Diffie-Hellman. This key can be used to encrypt and decrypt messages transmitted between them.

The Diffie-Hellman protocol given by the following diagram:

1. Alice and Bob agree on a prime number p, a point P generating subgroup G of order l of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$, where $(a,b) \in (\mathbb{F}_q[\varepsilon])^2$.
2. (x_1, x_2, x_3) in $(\{0,1,2,\ldots,l-1\})^3$ is a public and $\gcd(x_i, l) = 1$, for $1 \le i \le 3$.
3. Alice chooses three private positive random integers are all different $a_i < ord(P)$, and sends a_iP to Bob, for $1 \le i \le 3$.
4. Bob chooses three private positive random integers are all different $b_i < ord(P)$, and sends by the order b_iP to Alice, for $1 \le i \le 3$.
5. Alice build the following table:

Private keys Message sent by Bob	a_1	a_2	a_3	Sum
b_1P	a_1b_1P	a_2b_1P	a_3b_1P	K_1
b_2P	a_1b_2P	a_2b_2P	a_3b_2P	K_2
b_3P	a_1b_3P	a_2b_3P	a_3b_3P	K_3

6. Bob build the following table:

Private keys Message sent by Alice	b_1	b_2	b_3
a_1P	b_1a_1P	b_2a_1P	b_3a_1P
a_2P	b_1a_2P	b_2a_2P	b_3a_2P
a_3P	b_1a_3P	b_2a_3P	b_3a_3P
Sum	K_1	K_2	K_3

7. The secret key between Alice and Bob is $K = \begin{bmatrix} x_1 & K_1 & K_2 \\ 0 & x_2 & K_3 \\ 0 & 0 & x_3 \end{bmatrix}$, K is $*$ invertible in R.

4.2 *Encryption and decryption functions*

The scheme is constructed using the non commutative ring $(R,+,*)$. To encrypt a message $m \in R,$ we compute the ciphertext $E_{nc}(m)$ such that:

$$c = E_{nc}(m) = \widetilde{K * m * K^{-1*}}.$$

To decrypt a ciphertext $c \in R,$ we compute:

$$m = D_{ec}(c) = K^{-1*} * \tilde{c} * K.$$

- Encryption function: $\forall K \in R^{\times}$,

$$\begin{array}{rcl} E_{nc} : R & \to & R \\ m & \mapsto & \widetilde{K * m * K^{-1*}} \end{array}$$

- Decryption function: $\forall K \in R^{\times}$,

$$\begin{array}{rcl} D_{ec} : R & \to & R \\ c & \mapsto & K^{-1*} * \tilde{c} * K \end{array}$$

We have:

$$D_{ec}(E_{nc}(m)) = m, \forall m \in R.$$

Lemma 4.1 : *Let* m_1, m_2 *be two messages in R. Then:*

$$E_{nc}(m_1 + m_2) = E_{nc}(m_1) + E_{nc}(m_2).$$

Proof: By the encryption function we have:

$$\begin{aligned} E_{nc}(m_1 + m_2) &= \overline{K * (m_1 + m_2) * K^{-1^*}} \\ &= \overline{K * m_1 * K^{-1^*} + K * m_2 * K^{-1^*}} \\ &= \overline{K * m_1 * K^{-1^*}} + \overline{K * m_2 * K^{-1^*}} \\ &= E_{nc}(m_1) + E_{nc}(m_2). \end{aligned}$$

□

Lemma 4.2 : *For all* $m_1, m_2 \in R.$ *If* $m_1 * m_2 = m_2 * m_1$ *then:*

$$E_{nc}(m_1 * m_2) = E_{nc}(m_1) * E_{nc}(m_2).$$

Proof: By the encryption function we have:

$$E_{nc}(m_1 * m_2) = \overline{K * (m_1 * m_2) * K^{-1^*}}$$

Using the Proposition 3.1, if $m_1 * m_2 = m_2 * m_1$ then:

$$\begin{aligned} E_{nc}(m_1 * m_2) &= \overline{K * (m_2 * m_1) * K^{-1^*}} \\ &= \overline{K * m_2 * K^{-1^*} * K * m_1 * K^{-1^*}} \\ &= \overline{K * m_1 * K^{-1^*}} * \overline{K * m_2 * K^{-1^*}} \\ &= E_{nc}(m_1) * E_{nc}(m_2). \end{aligned}$$

Thus, the lemma is proved. □

Remark 4.1 : Fully homomorphic cryptosystem based on the ring R:

- Space of lights: $E = Z(R)$.
- Space of quantified: $F = Z(R)$.
- Space of keys: $R^{\times} - \{Z(R)\}$.
- Encryption function: $\forall K \in R^{\times} - \{Z(R)\}$,

$$\begin{array}{rcl} E_{nc} : E & \rightarrow & F \\ m & \mapsto & \overline{K * m * K^{-1^*}} \end{array}$$

- Decryption function: $\forall K \in R^{\times} - \{Z(R)\}$,

$$\begin{array}{rcl} D_{ec} : F & \to & E \\ c & \mapsto & K^{-1^*} * \tilde{c} * K \end{array}$$

5. Security of protocol

Due to the development of quantum computation, which has become a major threat to asymmetric cipher systems, which made many researchers they focus on creating new encryption algorithms that allow public and private keys and be resistant to quantum computers. In this work, we designed an encryption scheme that is one of the alternatives to resist quantum attacks, it depends on the two difficult problems are problem of discerte logarithm (DLP) (see [8, 11]) and problem of conjugal on a non commutative ring (CCP).

The security of our cryptosystem over the non commutative ring R is very strong and secure, because it based on the two problems DLP and CCP which are very difficult to solve.

If another person wants to compute the secret key K, it must solve the following problem $K_i = \sum_{j=1}^{3} b_i a_j P = \sum_{j=1}^{3} a_j b_i P$ for $1 \leq i \leq 3$, this problem is very hard to solve and if he wants to compute a message m, it must solve the conjugal problem.

6. Numerical example of cryptography

Alice and Bob agree on a prime number $p = 7$ and a point $P = [3\varepsilon^2 + 5\varepsilon + 6 : 1 : 3\varepsilon^3 + 5\varepsilon^2 + 3\varepsilon + 3]$ generating the subgroup G of order $l = 35$ of elliptic curve $E_{a,b}(\mathbb{F}_7[\varepsilon])$, where $a = 2\varepsilon^3 + 1, b = 2\varepsilon^3 + 3\varepsilon^2 + \varepsilon + 1$ in $\mathbb{F}_7[\varepsilon]$. The subgroup of $G =< P >$ is shown as follows:

n	nP	n	nP
1	$[3\varepsilon^2 + 5\varepsilon + 6 : 1 : 3\varepsilon^3 + 5\varepsilon^2 + 3\varepsilon + 3]$	19	$[4\varepsilon^3 + 6\varepsilon^2 + 3\varepsilon + 1 : 1 : 4\varepsilon^3 + 4\varepsilon^2 + 2\varepsilon + 4]$
2	$[5\varepsilon^3 + 3\varepsilon^2 + 6\varepsilon : 1 : \varepsilon^3 + 6\varepsilon^2 + \varepsilon + 6]$	20	$[5\varepsilon^3 + \varepsilon^2 + \varepsilon : 1 : 0]$
3	$[5\varepsilon^3 + 5\varepsilon^2 + 4\varepsilon : 1 : 2\varepsilon^3 + 3\varepsilon^2 + \varepsilon + 1]$	21	$[6\varepsilon^3 + 3\varepsilon^2 + 6\varepsilon + 6 : 1 : 3\varepsilon^2 + \varepsilon + 3]$
4	$[6\varepsilon^3 + 3\varepsilon^2 + 4\varepsilon + 1 : 1 : 3\varepsilon^2 + 4]$	22	$[3\varepsilon^2 + 4\varepsilon : 1 : 2\varepsilon^3 + 4\varepsilon^2 + 2\varepsilon + 6]$
5	$[3\varepsilon^3 + 2\varepsilon^2 + 2\varepsilon : 1 : 0]$	23	$[6\varepsilon^3 + 6\varepsilon^2 + 2\varepsilon : 1 : 4\varepsilon^3 + 2\varepsilon + 1]$
6	$[\varepsilon^2 + 6 : 1 : \varepsilon^3 + 4\varepsilon^2 + 6\varepsilon + 3]$	24	$[6\varepsilon^3 + 2\varepsilon^2 + 5\varepsilon + 1 : 1 : 6\varepsilon^3 + 6\varepsilon^2 + 5\varepsilon + 4]$
7	$[5\varepsilon^2 + 2\varepsilon : 1 : 5\varepsilon^3 + 3\varepsilon + 6]$	25	$[\varepsilon^3 + 3\varepsilon^2 + 3\varepsilon : 1 : 0]$
8	$[2\varepsilon^3 + 5\varepsilon^2 : 1 : 4\varepsilon^3 + 6\varepsilon^2 + 3\varepsilon + 1]$	26	$[3\varepsilon^3 + 4\varepsilon^2 + \varepsilon + 6 : 1 : 6\varepsilon^3 + \varepsilon^2 + 4\varepsilon + 3]$

Contd...

9	$[4\varepsilon^3+3\varepsilon^2+6\varepsilon+1:1:\varepsilon^3+6\varepsilon^2+3\varepsilon+4]$	27	$[5\varepsilon^3+2\varepsilon^2:1:3\varepsilon^3+\varepsilon^2+4\varepsilon+6]$
10	$[6\varepsilon^3+4\varepsilon^2+4\varepsilon:1:0]$	28	$[2\varepsilon^2+5\varepsilon:1:2\varepsilon^3+4\varepsilon+1]$
11	$[\varepsilon^3+5\varepsilon^2+2\varepsilon+6:1:\varepsilon^3+\varepsilon^2+2\varepsilon+3]$	29	$[6\varepsilon^2+1:1:6\varepsilon^3+3\varepsilon^2+\varepsilon+4]$
12	$[\varepsilon^3+\varepsilon^2+5\varepsilon:1:3\varepsilon^3+5\varepsilon+6]$	30	$[4\varepsilon^3+5\varepsilon^2+5\varepsilon:1:0]$
13	$[4\varepsilon^2+3\varepsilon:1:5\varepsilon^3+3\varepsilon^2+5\varepsilon+1]$	31	$[\varepsilon^3+4\varepsilon^2+3\varepsilon+6:1:4\varepsilon^2+3]$
14	$[\varepsilon^3+4\varepsilon^2+\varepsilon+1:1:4\varepsilon^2+6\varepsilon+4]$	32	$[2\varepsilon^3+2\varepsilon^2+3\varepsilon:1:5\varepsilon^3+4\varepsilon^2+6\varepsilon+6]$
15	$[2\varepsilon^3+6\varepsilon^2+6\varepsilon:1:0]$	33	$[2\varepsilon^3+4\varepsilon^2+\varepsilon,1,6\varepsilon^3+\varepsilon^2+6\varepsilon+1]$
16	$[3\varepsilon^3+\varepsilon^2+4\varepsilon+6:1:3\varepsilon^3+3\varepsilon^2+5\varepsilon+3]$	34	$[4\varepsilon^2+2\varepsilon+1:1:4\varepsilon^3+2\varepsilon^2+4\varepsilon+4]$
17	$[\varepsilon^3+5\varepsilon^2+\varepsilon:1:2\varepsilon^3+6\varepsilon^2+6]$	35	$[0:1:0]=\infty$
18	$[6\varepsilon^3+2\varepsilon^2+6\varepsilon:1:5\varepsilon^3+\varepsilon^2+1]$		

- $(x_1,x_2,x_3)=(2,6,3)\in(\{0,1,\ldots,34\})^3$ is a public and $\gcd(x_i,35)=1,$ for $1\leqslant i\leqslant 3$.
- Alice chooses three private random positive integers are all different less than $ord(P)$:

$$\begin{cases} a_1=5 \\ a_2=7 \\ a_3=10 \end{cases} \xrightarrow{\text{and sends}} \begin{cases} 5P \\ 7P \\ 10P \end{cases} \text{to Bob.}$$

- Bob chooses three private random positive integers are all different less than $ord(P)$:

$$\begin{cases} b_1=4 \\ b_2=9 \\ b_3=13 \end{cases} \xrightarrow{\text{and sends by the order}} \begin{cases} 4P \\ 9P \\ 13P \end{cases} \text{to Alice.}$$

- Alice calculates:

$$K_1=5\times 4P+7\times 4P+10\times 4P=18P=[6\varepsilon^3+2\varepsilon^2+6\varepsilon:1:5\varepsilon^3+\varepsilon^2+1],$$
$$K_2=5\times 9P+7\times 9P+10\times 9P=23P=[6\varepsilon^3+6\varepsilon^2+2\varepsilon:1:4\varepsilon^3+2\varepsilon+1],$$
$$K_3=5\times 13P+7\times 13P+10\times 13P=6P=[\varepsilon^2+6:1:\varepsilon^3+4\varepsilon^2+6\varepsilon+3].$$

- Bob calculates:

$$K_1=4\times 5P+4\times 7P+4\times 10P=18P=[6\varepsilon^3+2\varepsilon^2+6\varepsilon:1:5\varepsilon^3+\varepsilon^2+1],$$
$$K_2=9\times 5P+9\times 7P+9\times 10P=23P=[6\varepsilon^3+6\varepsilon^2+2\varepsilon:1:4\varepsilon^3+2\varepsilon+1],$$
$$K_3=13\times 5P+13\times 7P+13\times 10P=6P=[\varepsilon^2+6:1:\varepsilon^3+4\varepsilon^2+6\varepsilon+3].$$

- The secret key between Alice and Bob is $K=\begin{bmatrix}2 & K_1 & K_2\\ 0 & 6 & K_3\\ 0 & 0 & 3\end{bmatrix}$. The inverse of K is:

$$K^{-1^*}=\begin{bmatrix}2^{-1} & -2^{-1}6^{-1}K_1 & -2^{-1}3^{-1}K_2\\ 0 & 6^{-1} & -6^{-1}3^{-1}K_3\\ 0 & 0 & 3^{-1}\end{bmatrix}=\begin{bmatrix}18 & 32K_1 & 29K_2\\ 0 & 6 & 33K_3\\ 0 & 0 & 12\end{bmatrix}=\begin{bmatrix}18 & S_1 & S_2\\ 0 & 6 & S_3\\ 0 & 0 & 12\end{bmatrix}, \text{ where :}$$

$$S_1=32K_1=32\times 18P=16P=[3\varepsilon^3+\varepsilon^2+4\varepsilon+6:1:3\varepsilon^3+3\varepsilon^2+5\varepsilon+3],$$
$$S_2=29K_2=29\times 23P=2P=[5\varepsilon^3+3\varepsilon^2+6\varepsilon:1:\varepsilon^3+6\varepsilon^2+\varepsilon+6],$$
$$S_3=33K_3=33\times 6P=23P=[6\varepsilon^3+6\varepsilon^2+2\varepsilon:1:4\varepsilon^3+2\varepsilon+1].$$

- To encrypt a message $m=\begin{bmatrix}20 & 19P & 14P\\ 0 & 31 & 27P\\ 0 & 0 & 26\end{bmatrix}\in R,$ we compute:

$c=E_{nc}(m)=\widetilde{K*m*K^{-1^*}}$, we have:

$$K*m*K^{-1^*}=\begin{bmatrix}2 & K_1 & K_2\\ 0 & 6 & K_3\\ 0 & 0 & 3\end{bmatrix}*\begin{bmatrix}20 & 19P & 14P\\ 0 & 31 & 27P\\ 0 & 0 & 26\end{bmatrix}*\begin{bmatrix}18 & S_1 & S_2\\ 0 & 6 & S_3\\ 0 & 0 & 12\end{bmatrix}$$
$$=\begin{bmatrix}5 & P & 31P\\ 0 & 11 & 3P\\ 0 & 0 & 8\end{bmatrix}*\begin{bmatrix}18 & S_1 & S_2\\ 0 & 6 & S_3\\ 0 & 0 & 12\end{bmatrix}$$
$$=\begin{bmatrix}5 & P & 31P\\ 0 & 11 & 3P\\ 0 & 0 & 8\end{bmatrix}*\begin{bmatrix}18 & 16P & 2P\\ 0 & 6 & 23P\\ 0 & 0 & 12\end{bmatrix}=\begin{bmatrix}20 & 16P & 32P\\ 0 & 31 & 9P\\ 0 & 0 & 26\end{bmatrix}.$$

Then the ciphertext is: $c=\widetilde{\begin{bmatrix}20 & 16P & 32P\\ 0 & 31 & 9P\\ 0 & 0 & 26\end{bmatrix}}=\begin{bmatrix}26 & 9P & 32P\\ 0 & 31 & 16P\\ 0 & 0 & 20\end{bmatrix}.$

- To decrypt a ciphertext $c=\begin{bmatrix}26 & 9P & 32P\\ 0 & 31 & 16P\\ 0 & 0 & 20\end{bmatrix}\in R,$ we compute:

$$m=K^{-1^*}*\tilde{c}*K=\begin{bmatrix}18 & S_1 & S_2\\ 0 & 6 & S_3\\ 0 & 0 & 12\end{bmatrix}*\begin{bmatrix}20 & 16P & 32P\\ 0 & 31 & 9P\\ 0 & 0 & 26\end{bmatrix}*\begin{bmatrix}2 & K_1 & K_2\\ 0 & 6 & K_3\\ 0 & 0 & 3\end{bmatrix}$$
$$=\begin{bmatrix}10 & 14P & 33P\\ 0 & 11 & 22P\\ 0 & 0 & 32\end{bmatrix}*\begin{bmatrix}2 & 18P & 23P\\ 0 & 6 & 6P\\ 0 & 0 & 3\end{bmatrix}=\begin{bmatrix}20 & 19P & 14P\\ 0 & 31 & 27P\\ 0 & 0 & 26\end{bmatrix}.$$

Then the plaintext is: $m=\begin{bmatrix}20 & 19P & 14P\\ 0 & 31 & 27P\\ 0 & 0 & 26\end{bmatrix}.$

7. Conclusion

In conclusion, we have defined the non commutative ring *R* and have introduced new method of a cryptography over it. This method is based on DLP and the conjugacy search problem for a non commutative ring, and is also a fully homomorphic encryption scheme. We have calculated this cryptographic example with the help of Maple 18.

References

[1] Boulbot A., Chillali A. and Mouhib A., Cryptographic Protocols on the non commutative Ring R, *International Journal of Mathematical and Computational Methods,* 2017, 2, 138-141. DOI: 10.1109/ISACS48493.2019.9068892.

[2] Boyd C. and Mathuria A., Protocols for Authentication and Key Establishment, Information Security and Cryptography Series; Springer-Verlag, Heidelberg, 2003.

[3] Chatterjee A. and Aung K. M. M., Fully Homomorphic Encryption in Real World Applications, Computer Architecture and Design Methodologies, Springer Nature, Singapore, 2019. DOI: 10.1007/978-981-13-6393-1.

[4] Diffie W. and Hellman M., New directions in cryptography, *IEEE Transactions on Information Theory,* 1976, 22(6), 644-654. DOI: 10.1109/TIT.1976.1055638.

[5] Elhassani M., Boulbot A., Cillali A. and Mouhib A., Fully homomorphic encryption scheme on a non-Commutative ring R, International Conference on Intelligent Systems and Advanced Computing Sciences (ISACS), 2019. DOI: 10.1109/ISACS48493.2019.9068892.

[6] Koblitz N., Elliptic curve cryptosystems, Mathematics of Computation, 1987, 48(177), 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5.

[7] Miller V., Use of elliptic curves in cryptography, CRYPTO'85, LNCS 218, Springer, 1986, 417-426. DOI: 10.1007/3-540-39799-X_31.

[8] Meshram C. and Li X. , New efficient key authentication protocol for public key cryptosystem using DL over multiplicative group, *Journal of Information and Optimization Sciences,* 2018, 39(2), 391-400. DOI: 10.1080/02522667.2017.1411013.

[9] Rivest R. L., Adleman L. and Dertouzos M. L., On data banks and privacy homomorphisms, Foundations of Secure Computation 1978, 11(4), 169-180.

[10] Sahmoudi M. and Chillali A., Key exchange over particular algebraic closure ring, Tatra Mountains Mathematical Publications, 2017, 70, 151-162. DOI: 10.1515/tmmp-2017-0024.

[11] Selikh B., Chillali A., Mihoubi D. and Ghadbane N., ECC over the ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = 0$ by using two methods, *Tbilisi Mathematical Journal,* 2021, 14(3), 213-223. DOI: 10.32513/tmj/19322008155.

[12] Selikh B., Mihoubi D. and Ghadbane N., Classification of elements in elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$, *Discussiones Mathematicae General Algebra and Applications,* 2021, 41(2), 283-298. DOI: 10.7151/dmgaa.1371.

[13] Sundarayya P. and Vara Prasad G., A public key cryptosystem using Affine Hill Cipher under modulation of prime number, J*ournal of Information and Optimization Sciences,* 2019, 40(4), 919-930. DOI: 10.1080/02522667.2018.1470751.

Recieved August, 2021