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

(3s.) **v. 2023 (41)** : 1–12.
ISSN-0037-8712 in press
doi:10.5269/bspm.62377

The "Elliptic" Matrices and a New Kind of Cryptography

Zakariae Cheddour, Abdelhakim Chillali and Ali Mouhib

abstract: In their article titled "Cryptography Based on the Matrices", A. Chillali et al. introduce a new cryptographic method based on matrices over a finite field $\mathbb{F}_{p^n}$, where p is a prime number. In this paper, we will generate this method in a new group of square block matrices based on an elliptic curve, called "elliptic" matrices.

Key Words: Cryptosystem, elliptic curves, fully homomorphic encryption, matrices, discrete logarithm problem.

Contents

1 Introduction **1**

2 Ring of "elliptic" matrices **2**
2.1 The Ring $\aleph$ . . . 2
2.2 The "elliptic" matrices . . . 6

3 Encryption Schemes using the "elliptic" matrices **7**
3.1 Cryptographic Protocols . . . 7
3.2 Security of this protocol . . . 8
3.3 Encryption of message . . . 9
3.4 Decryption of message . . . 9

4 Numerical example **10**

5 Conclusion **11**

1. Introduction

In the paper [14], Varadharajan proposed a noncommutative group as a platform group for DH-key exchange, which was later cryptographically analyzed using eigenvalues and Jordan form in the paper [12]. Subsequently, the use of non-commutative groups and rings in public-key cryptography has attracted much attention [4], [5], [6], [15], [17].

In [17], A. Chillali et al. introduce a new cryptographic method based on a non-commutative group matrix over a finite field $\mathbb{F}_{p^n}$, where p is a prime number. As described in [7], [8], [11], [12], [13], some properties of matrices such as determinant, eigenvalues, and Cayley-Hamilton theorem can be used to develop attacks against this protocol. Such attacks reduce DLP on the group of invertible matrices to DLP on finite fields or to a simple factorization problem. To avoid this reduction of DLP on the matrix group to that on finite fields, we will introduce a matrix group over an elliptic curve and its diagonal in $\mathbb{Z}_n$, under a new matrix multiplication operation, and consequently, go from DLP to ($ECDLP$) which is the fundamental factor of elliptic curve cryptography and matching-based cryptography. It has been a major investigation area in number theory and cryptography for many decades [1], [2], [3], [9], [10], [16]. Hence, the main idea of this work is the design of some public key exchange protocols over a noncommutative ring, in particular over the ring of "elliptic" matrix, whose security is based on $ECDLP$. In other words, we propose a new key exchange protocol based on matrices with the following form $M(B_1, B_2, B_3) = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$ called "elliptic" matrices, where $B_1,\ B_2,\ B_3$ are three-dimensional

2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted February 05, 2022. Published April 14, 2022

matrices constructed over an elliptic curve whose diagonal elements are in $\mathbb{Z}_n$. In addition, we investigate the complexity and security of the key exchange protocol.

The rest of the paper is organized as follows. In Sec. 2, we define the non-commutative ring of elliptic matrices and give an example of matrix multiplication on this ring. In Sec. 3, a key exchange protocol is explained and the security and complexity of the protocol are provided. In Sec. 4, we propose a numerical Example.

2. Ring of "elliptic" matrices

Let E be an elliptic curve over a finite field K, P is a point of higher-order n and G is the group generated by P. In this section, we present the theoretical concept for our encryption scheme by using the matrix-ring $\aleph$, with the following form, $\aleph = \left\{ \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \mid a_i \in \mathbb{Z}_n,\ Q_i, P_i \in G,\ i \in \{1,2,3\} \right\}$.

2.1. The Ring $\aleph$

In this subsection, we will define on $\aleph$ two internal laws called addition $+$ and multiplication $\star$ as follows, let $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}$ and $Y = \begin{pmatrix} b_1 & P'_1 & P'_2 \\ Q'_3 & b_2 & P'_3 \\ Q'_2 & Q'_1 & b_3 \end{pmatrix}$ be two elements in $\aleph$, then

$$X + Y = \begin{pmatrix} a_1 + b_1 & P_1 + P'_1 & P_2 + P'_2 \\ Q_3 + Q'_3 & a_2 + b_2 & P_3 + P'_3 \\ Q_2 + Q'_2 & Q_1 + Q'_1 & a_3 + b_3 \end{pmatrix},$$

$$X \star Y = \begin{pmatrix} a_1 b_1 & b_2 P_1 + a_1 P'_1 & b_3 P_2 + a_1 P_2 \\ b_1 Q_3 + a_2 Q'_3 & a_2 b_2 & b_3 P_3 + a_2 P_3 \\ b_1 Q_2 + a_3 Q'_2 & b_2 Q_1 + a_3 Q'_1 & a_3 b_3 \end{pmatrix}.$$

Lemma 2.1. *The set $\aleph$ together with addition "$+$" and multiplication "$\star$" is a unitary noncommutative ring with identities,*

$$1_\aleph = \begin{pmatrix} 1 & [0:1:0] & [0:1:0] \\ [0:1:0] & 1 & [0:1:0] \\ [0:1:0] & [0:1:0] & 1 \end{pmatrix} \text{ and } 0_\aleph = \begin{pmatrix} 0 & [0:1:0] & [0:1:0] \\ [0:1:0] & 0 & [0:1:0] \\ [0:1:0] & [0:1:0] & 0 \end{pmatrix}.$$

Proof. Let $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}, Y = \begin{pmatrix} b_1 & P'_1 & P'_2 \\ Q'_3 & b_2 & P'_3 \\ Q'_2 & Q'_1 & b_3 \end{pmatrix}$ *and* $Z = \begin{pmatrix} c_1 & P"_1 & P"_2 \\ Q"_3 & c_2 & P"_3 \\ Q"_2 & Q"_1 & c_3 \end{pmatrix}$ be elements in $\aleph$, then

- Associativity:

  We start with the product law "$\star$",

$$(X \star Y) \star Z = \begin{pmatrix} a_1 b_1 & b_2 P_1 + a_1 P'_1 & b_3 P_2 + a_1 P'_2 \\ b_1 Q_3 + a_2 Q'_3 & a_2 b_2 & b_3 P_3 + a_2 P'_3 \\ b_1 Q_2 + a_3 Q'_2 & b_2 Q_1 + a_3 Q'_1 & a_3 b_3 \end{pmatrix} \star \begin{pmatrix} c_1 & P"_1 & P"_2 \\ Q"_3 & c_2 & P"_3 \\ Q"_2 & Q"_1 & c_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 b_1 c_1 & b_2 c_2 P_1 + a_1 c_2 P'_1 + a_1 b_1 P"_1 & b_3 c_3 P_2 + a_1 c_3 P'_2 + a_1 b_1 P"_2 \\ b_1 c_1 Q_3 + a_2 c_1 Q'_3 + a_2 b_2 Q"_3 & a_2 b_2 c_2 & b_3 c_3 P_3 + a_2 c_3 P'_3 + a_2 b_2 P"_3 \\ b_1 c_1 Q_2 + a_3 c_1 Q'_2 + a_3 b_3 Q"_2 & b_2 c_2 Q_1 + a_3 c_2 Q'_1 + a_3 b_3 Q"_1 & a_3 b_3 c_3 \end{pmatrix}$$

and,

$$X \star (Y \star Z) = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \star \begin{pmatrix} b_1 c_1 & c_2 P'_1 + b_1 P"_1 & c_3 P'_2 + b_1 P'_2 \\ c_1 Q'_3 + b_2 Q"_3 & b_2 c_2 & c_3 P'_3 + b_2 P'_3 \\ c_1 Q'_2 + b_3 Q"_2 & c_2 Q'_1 + b_3 Q"_1 & b_3 c_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1b_1c_1 & b_2c_2P_1 + a_1c_2P'_1 + a_1b_1P"_1 & b_3c_3P_2 + a_1c_3P'_2 + a_1b_1P"_2 \\ b_1c_1Q_3 + a_2c_1Q'_3 + a_2b_2Q"_3 & a_2b_2c_2 & b_3c_3P_3 + a_2c_3P'_3 + a_2b_2P"_3 \\ b_1c_1Q_2 + a_3c_1Q'_2 + a_3b_3Q"_2 & b_2c_2Q_1 + a_3c_2Q'_1 + a_3b_3Q"_1 & a_3b_3c_3 \end{pmatrix}$$

Hence, $(X \star Y) \star Z = X \star (Y \star Z)$.
On the other hand, in the same way, we find that $(X + Y) + Z = X + (Y + Z)$.

- Commutativity:
  Generally, it's clear that: $(X \star Y) \neq (Y \star X)$. So, $\star$ is not commutative, but $+$ is commutative law.

- Distributivity:
  We shall prove that $(X + Y) \star Z = X \star Z + Y \star Z$ and $Z \star (X + Y) = Z \star X + Z \star Y$.
  So, for the first equality $(X + Y) \star Z = X \star Z + Y \star Z$, we have

$$(X + Y) \star Z = \begin{pmatrix} a_1 + b_1 & P_1 + P'_1 & P_2 + P'_2 \\ Q_3 + Q'_3 & a_2 + b_2 & P_3 + P'_3 \\ Q_2 + Q'_2 & Q_1 + Q'_1 & a_3 + b_3 \end{pmatrix} \star \begin{pmatrix} c_1 & P"_1 & P"_2 \\ Q"_3 & c_2 & P"_3 \\ Q"_2 & Q"_1 & c_3 \end{pmatrix}$$

$$= \begin{pmatrix} (a_1 + b_1)c_1 & c_2(P_1 + P'_1) + (a_1 + b_1)P"_1 & c_3(P_2 + P'_2) + (a_1 + b_1)P"_2 \\ c_1(Q_3 + Q'_3) + (a_2 + b_2)Q"_3 & (a_2 + b_2)c_2 & c_3(P_3 + P'_3) + (a_2 + b_2)P"_3 \\ c_1(Q_2 + Q'_2) + (a_3 + b_3)Q"_2 & c_2(Q_1 + Q'_1) + (a_3 + b_3)Q"_1 & (a_3 + b_3)c_3 \end{pmatrix},$$

and, $X \star Z + Y \star Z =$

$$\begin{pmatrix} a_1c_1 + b_1c_1 & c_2P_1 + c_2P'_1 + (a_1 + b_1)P"_1 & c_3P_2 + c_3P'_2 + (a_1 + b_1)P"_2 \\ c_1Q_3 + c_1Q'_3 + (a_2 + b_2)Q"_3 & a_2c_2 + b_2c_2 & c_3P_3 + c_3P'_3 + (a_2 + b_2)P"_3 \\ c_1Q_2 + c_1Q'_2 + (a_3 + b_3)Q"_2 & c_2Q_1 + c_2Q'_1 + (a_3 + b_3)Q"_1 & a_3c_3 + b_3c_3 \end{pmatrix}.$$

Hence, $(X + Y) \star Z = X \star Z + Y \star Z$.
Similarly for the second equality.

- Additive inverses, $\forall X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \in \aleph$, we have $X + (-X) = 0_{\aleph}$, with

$$(-X) = \begin{pmatrix} -a_1 & -P_1 & -P_2 \\ -Q_3 & -a_2 & -P_3 \\ -Q_2 & -Q_1 & -a_3 \end{pmatrix}$$

  is called the additive inverse of X.

□

The next proposition characterize the set of invertible elements in $\aleph$.

Proposition 2.2. *Let* $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \in \aleph$, *$X$ is invertible if only if $a_i \wedge n = 1$ for all $i \in \{1, 2, 3\}$, in this case we have,*

$$X^{\star(-1)} = \begin{pmatrix} a_1^{-1} & -a_1^{-1}a_2^{-1}P_1 & -a_1^{-1}a_3^{-1}P_2 \\ -a_1^{-1}a_2^{-1}Q_3 & a_2^{-1} & -a_2^{-1}a_3^{-1}P_3 \\ -a_1^{-1}a_3^{-1}Q_2 & -a_2^{-1}a_3^{-1}Q_1 & a_3^{-1} \end{pmatrix} \in \aleph.$$

Proof. Let $Y = \begin{pmatrix} b_1 & P'_1 & P'_2 \\ Q'_3 & b_2 & P'_3 \\ Q'_2 & Q'_1 & b_3 \end{pmatrix}$ the inverse of X, we have: $X \star Y = Y \star X = 1_{\aleph}$.

So,

$$X \star Y = \begin{pmatrix} a_1b_1 & b_2P_1 + a_1P'_1 & b_3P_2 + a_1P'_2 \\ b_1Q_3 + a_2Q'_3 & a_2b_2 & b_3P_3 + a_2P'_3 \\ b_1Q_2 + a_3Q'_2 & b_2Q_1 + a_3Q'_1 & a_3b_3 \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] & [0:1:0] \\ [0:1:0] & 1 & [0:1:0] \\ [0:1:0] & [0:1:0] & 1 \end{pmatrix},$$

and

$$Y \star X = \begin{pmatrix} a_1b_1 & b_1P_1 + a_2P'_1 & b_1P_2 + a_3P'_2 \\ b_2Q_3 + a_1Q'_3 & a_2b_2 & b_2P_3 + a_3P'_3 \\ b_3Q_2 + a_1Q'_2 & b_3Q_1 + a_2Q'_1 & a_3b_3 \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] & [0:1:0] \\ [0:1:0] & 1 & [0:1:0] \\ [0:1:0] & [0:1:0] & 1 \end{pmatrix}.$$

Thus, $a_ib_i \equiv 1[n]$ for all $i \in \{1,2,3\}$ and

$$\begin{aligned} b_2P_1 + a_1P'_1 &= [0:1:0], \\ b_3P_2 + a_1P'_2 &= [0:1:0], \\ b_3P_3 + a_2P'_3 &= [0:1:0], \\ b_2Q_1 + a_3Q'_1 &= [0:1:0], \\ b_1Q_2 + a_3Q'_2 &= [0:1:0], \\ b_1Q_3 + a_2Q'_3 &= [0:1:0]. \end{aligned}$$

Therefore, X is invertible if only if $a_i \wedge n = 1$ for all $i \in \{1,2,3\}$, in this case we have, $b_i = a_i^{-1}$ for all $i \in \{1,2,3\}$ and

$$\begin{aligned} P'_1 &= -a_1^{-1}a_2^{-1}P_1, \\ P'_2 &= -a_1^{-1}a_3^{-1}P_2, \\ P'_3 &= -a_2^{-1}a_3^{-1}P_3, \\ Q'_1 &= -a_3^{-1}a_2^{-1}Q_1, \\ Q'_2 &= -a_3^{-1}a_1^{-1}Q_2, \\ Q'_3 &= -a_2^{-1}a_1^{-1}Q_3. \end{aligned}$$

So,

$$X^{\star(-1)} = \begin{pmatrix} a_1^{-1} & -a_1^{-1}a_2^{-1}P_1 & -a_1^{-1}a_3^{-1}P_2 \\ -a_1^{-1}a_2^{-1}Q_3 & a_2^{-1} & -a_2^{-1}a_3^{-1}P_3 \\ -a_1^{-1}a_3^{-1}Q_2 & -a_2^{-1}a_3^{-1}Q_1 & a_3^{-1} \end{pmatrix} \in \aleph.$$

□

Lemma 2.3. *Let k be a positive integer. Then if $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}$ is an element of $\aleph$, the k-power of X can be given by $X^{\star k} = \begin{pmatrix} a_1^k & \lambda_{1,k}P_1 & \lambda_{2,k}P_2 \\ \lambda_{1,k}Q_3 & a_2^k & \lambda_{3,k}P_3 \\ \lambda_{2,k}Q_2 & \lambda_{3,k}Q_1 & a_3^k \end{pmatrix}$, where*

$$\lambda_{1,k} = \sum_{i+j=k-1} a_1^i a_2^j \tag{2.1}$$

$$\lambda_{2,k} = \sum_{i+j=k-1} a_1^i a_3^j \tag{2.2}$$

$$\lambda_{3,k} = \sum_{i+j=k-1} a_2^i a_3^j \tag{2.3}$$

Proof. Using a proof by induction on k. For $k = 1$, we have $\lambda_{i,1} = 1$ for all $i \in \{1, 2, 3\}$, then $X^{\star 1} = X$ Let $k \geq 1$. Assume the induction hypothesis, for a given value $k \geq 1$, the single case

$$\lambda_{1,k} = \sum_{i+j=k-1} a_1^i a_2^j \tag{2.4}$$

$$\lambda_{2,k} = \sum_{i+j=k-1} a_1^i a_3^j \tag{2.5}$$

$$\lambda_{3,k} = \sum_{i+j=k-1} a_2^i a_3^j \tag{2.6}$$

is true, and proof that we have,

$$\lambda_{1,k+1} = \sum_{i+j=k} a_1^i a_2^j \tag{2.7}$$

$$\lambda_{2,k+1} = \sum_{i+j=k} a_1^i a_3^j \tag{2.8}$$

$$\lambda_{3,k+1} = \sum_{i+j=k} a_2^i a_3^j \tag{2.9}$$

so, we have

$$X^{\star(k+1)} = \begin{pmatrix} a_1^k & \lambda_{1,k} P_1 & \lambda_{2,k} P_2 \\ \lambda_{1,k} Q_3 & a_2^k & \lambda_{3,k} P_3 \\ \lambda_{2,k} Q_2 & \lambda_{3,k} Q_1 & a_3^k \end{pmatrix} \star \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}.$$

Then,

$$X^{\star(k+1)} = \begin{pmatrix} a_1^{k+1} & (a_1^k + a_2 \lambda_{1,k}) P_1 & (a_1^k + a_3 \lambda_{2,k}) P_2 \\ (a_2^k + a_1 \lambda_{1,k}) Q_3 & a_2^{k+1} & (a_2^k + a_3 \lambda_{3,k}) P_3 \\ (a_3^k + a_1 \lambda_{2,k}) Q_2 & (a_3^k + a_2 \lambda_{3,k}) Q_1 & a_3^{k+1} \end{pmatrix}.$$

Thus,

$$\begin{aligned} \lambda_{1,k+1} &= a_1^k + a_2 \lambda_{1,k} = a_1^k + a_2 \sum_{i+j=k-1} a_1^i a_2^j \\ &= \sum_{i+j=k} a_1^i a_2^j, \\ \lambda_{2,k+1} &= a_1^k + a_3 \lambda_{2,k} = a_1^k + a_3 \sum_{i+j=k-1} a_1^i a_3^j \\ &= \sum_{i+j=k} a_1^i a_3^j, \\ \lambda_{3,k+1} &= a_2^k + a_3 \lambda_{3,k} = a_2^k + a_3 \sum_{i+j=k-1} a_2^i a_3^j \\ &= \sum_{i+j=k} a_2^i a_3^j. \end{aligned}$$

We conclude that, $\forall k \geq 1$,

$$\begin{aligned} \lambda_{1,k} &= \sum_{i+j=k-1} a_1^i a_2^j, \\ \lambda_{2,k} &= \sum_{i+j=k-1} a_1^i a_3^j, \\ \lambda_{3,k} &= \sum_{i+j=k-1} a_2^i a_3^j, \end{aligned}$$

hence the result. □

We have $\star$ is a noncommutative law, so in the following proposition we will characterize the set of matrices in $\aleph$ that commute with such a matrix $X = \begin{pmatrix} a_1 & n_1P & n_2P \\ m_3P & a_2 & n_3P \\ m_2P & m_1P & a_3 \end{pmatrix}$.

Definition 2.4. *The centralizer of the matrix X over $\aleph$ is defined as follows*

$$\mathrm{C}_{\aleph}(X) = \{Y \in \aleph \mid X \star Y = Y \star X\}.$$

Proposition 2.5. *With the same notation as above, we have $Y = \begin{pmatrix} b_1 & e_1P & e_2P \\ f_3P & b_2 & e_3P \\ f_2P & f_1P & b_3 \end{pmatrix} \in \mathrm{C}_{\aleph}(X)$ if and only if*

$$\begin{cases} b_1 = b_2\ ,\ n_2f_2 = m_2e_2 \text{ and } n_3f_1 = m_1e_3, & if\ a_1 = a_2 \text{ and } a_2 - a_3 \neq 0; \\ b_i = b_j\ for\ i \neq j, & if\ a_i = a_j\ for\ i \neq j; \\ n_1f_3 = m_3e_1,\ n_2f_2 = m_2e_2 \text{ and } n_3f_1 = m_1e_3, & if\ a_i - a_j \neq 0\ for\ i \neq j. \end{cases}$$

Proof. Since,

$$X \star Y = \begin{pmatrix} a_1b_1 & b_2n_1P + a_1e_1P & b_3n_2P + a_1e_2P \\ b_1m_3P + a_2f_3P & a_2b_2 & b_3n_3P + a_2e_3P \\ b_1m_2P + a_3f_2P & b_2m_1P + a_3f_1P & a_3b_3 \end{pmatrix},$$

and

$$Y \star X = \begin{pmatrix} a_1b_1 & b_1n_1P + a_2e_1P & b_1n_2P + a_3e_2P \\ b_2m_3P + a_1f_3P & a_2b_2 & b_2n_3P + a_3e_3P \\ b_3m_2P + a_1f_2P & b_3m_1P + a_2f_1P & a_3b_3 \end{pmatrix}.$$

And with comparative calculations we find the result. □

2.2. The "elliptic" matrices

In the following, we present the theoretical concept for our encryption scheme by using the elliptic matrix $M(B_1, B_2, B_3) = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$ where $B_i \in \aleph$ for all $i \in \{1, 2, 3\}$.

Lemma 2.6. *With the same notations as above, we have the k-power of an elliptic matrix as follows,*

$$M(B_1, B_2, B_3)^{\star k} = \begin{pmatrix} B_1^{\star k} & T_k \\ 0 & B_3^{\star k} \end{pmatrix}\ for\ all\ \ k \in \mathbb{N}^*$$

with $T_k = \sum_{i=0}^{k-1} B_1^{\star(k-1-i)} B_2 B_3^{\star i}$.

Proof. Fix an arbitrary matrices B_1, B_2 and B_3 in $\aleph$, and let $M(B_1, B_2, B_3)^k$ be the statement. We give the proof by induction on k, we have

$$\begin{aligned} M(B_1, B_2, B_3)^{\star 1} &= \begin{pmatrix} B_1^{\star 1} & T_1 \\ 0 & B_3^{\star 1} \end{pmatrix} \\ &= \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \\ &= M(B_1, B_2, B_3) \end{aligned}$$

then our Lemma is true for $k = 1$.

We assume the recurrence hypothesis, $M(B_1,B_2,B_3)^{\star k} = \begin{pmatrix} B_1^{\star k} & T_k \\ 0 & B_3^{\star k} \end{pmatrix}$ for certain k. So, We have

$$\begin{aligned}
M(B_1,B_2,B_3)^{\star(k+1)} &= (M(B_1,B_2,B_3))^{\star k} \star M(B_1,B_2,B_3) \\
&= \begin{pmatrix} B_1^{\star k} & T_k \\ 0 & B_3^{\star k} \end{pmatrix} \star \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star k} \star B_1 & B_1^k B_2 + T_k \star B_3 \\ 0 & B_3^{\star k} \star B_3 \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & B_1^k B_2 + (\sum_{i=0}^{k-1} B_1^{\star(k-1-i)} B_2 B_3^{\star i}) \star B_3 \\ 0 & B_3^{\star(k+1)} \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & B_1^k B_2 + \sum_{i=0}^{k-1} B_1^{\star(k-1-i)} B_2 B_3^{\star(i+1)} \\ 0 & B_3^{\star(k+1)} \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
&= \begin{pmatrix} B_1^{\star(k+1)} & B_1^k B_2 + \sum_{j=1}^{k} B_1^{\star(k-j)} B_2 B_3^{\star j} \\ 0 & B_3^{\star(k+1)} \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & \sum_{j=0}^{k} B_1^{\star(k-j)} B_2 B_3^{\star j} \\ 0 & B_3^{\star(k+1)} \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & T_{k+1} \\ 0 & B_3^{\star(k+1)} \end{pmatrix}.
\end{aligned}$$

Hence the result. □

3. Encryption Schemes using the "elliptic" matrices

In this section we will construct an encryption scheme using the matrix $M(B_1, B_2, B_3)$.

3.1. Cryptographic Protocols

This sub-section describes some public-key encryption and key establishment schemes. Surveys the state-of-the-art in algorithms for solving the following classical problem(ECDLP) find an integer a, if it exists, such that $Q = aP$, with P and Q being well-defined points of this elliptic curve, whose intractability is necessary for the security of our cryptographic schemes.

- **Key exchange protocol**
  Alice and **Bob** agree on public prime number p and a point P over an elliptic curve $E(\mathbb{F}_q)$ of order n, where q is a power of p.
  First **Alice** chooses two matrices $(A, A_1) \in \aleph$ and publish the pair $(A, \mathrm{C}_\aleph(A_1))$, in the same way, **Bob** chooses two matrices $(B, B_2) \in \aleph$ and publish the pair $(B, \mathrm{C}_\aleph(B_2))$.
  Alice chooses private keys: $k \in \mathbb{N}^*$ and $A_2 \in \mathrm{C}_\aleph(B_2)$. She calculated the matrix

$$(M(A_1, A+B, A_2))^{\star k} = \begin{pmatrix} A_1^{\star k} & T_k \\ 0 & A_2^{\star k} \end{pmatrix}$$

  and send T_k to **Bob**.
  In turn, **Bob** chooses private keys, $t \in \mathbb{N}^*$ and $B_1 \in \mathrm{C}_\aleph(A_1)$. He calculated the matrix

$$(M(B_1, A+B, B_2))^{\star t} = \begin{pmatrix} B_1^{\star t} & E_t \\ 0 & B_2^{\star t} \end{pmatrix}$$

and send E_t to **Alice**.
With their private keys k and t, **Alice** and **Bob** calculate separately the matrices:

$$\textbf{Alice} : M(A_1, E_t, A_2)^{\star k} = \begin{pmatrix} A_1^{\star k} & E_{t,k} \\ 0 & A_2^{\star k} \end{pmatrix} \tag{3.1}$$

$$\textbf{Bob} : M(B_1, T_k, B_2)^{\star t} = \begin{pmatrix} B_1^{\star t} & T_{k,t} \\ 0 & B_2^{\star t} \end{pmatrix} \tag{3.2}$$

Lemma 3.1. *With the same notation as above, we have $E_{t,k} = T_{k,t}$.*

Proof. We have,

$$\begin{aligned} T_{k,t} &= \sum_{i=0}^{t-1} B_1^{t-i-1} T_k B_2^i \\ &= \sum_{i=0}^{t-1} B_1^{t-i-1} \left(\sum_{j=0}^{k-1} A_1^{k-1-j}(A+B)A_2^j \right) B_2^i \\ &= \sum_{i=0}^{t-1} \sum_{j=0}^{k-1} B_1^{t-i-1} A_1^{k-1-j}(A+B)A_2^j B_2^i \end{aligned}$$

and

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

or, $B_1 \in C_{\aleph}(A_1)$ and $A_2 \in C_{\aleph}(B_2)$, it follows that $T_{k,t} = E_{t,k}$. □

Corollary 3.2. *The secret key of **Alice** and **Bob** is the matrix $\Phi = E_{t,k} = T_{k,t}$.*

3.2. Security of this protocol

The set $C_{\aleph}(B_2)$, $C_{\aleph}(A_1)$ and the matrices A, B are public. If another person wants to compute the secret key Φ, it must solve the following equation:
$\sum_{i=0}^{k-1} A_1^{k-1-i}(A+B)A_2^i = T_k$ whose unknowns the matrices A_1, A_2 and the natural number k.
In other words, to find the key, it is necessary(not sufficient) to solve the following classical problem, find an integer a, if it exists, such that $Q = aP$.

Proposition 3.3. *The complexity to calculate the key Φ is $\mathcal{O}\left(3^{tk}\right)$.*

Proof. The encryption scheme using a matrix over $\aleph$ of order 3, will use a key Φ of size $O(3)$, as described previously. Since

$$\Phi = \sum_{i=0}^{k-1} \sum_{j=0}^{t-1} A_1^{t-1-j} B_1^{k-1-i}(A+B)B_2^i A_2^j,$$

we have the complexity to calculate the key Φ is $\mathcal{O}\left(3^{tk}\right)$. □

3.3. Encryption of message

Let Φ be a secret key exchanged by **Alice** and **Bob**. If Φ refers to the unit matrix and is invertible, let ∇ be the message that **Alice** wants to send to **Bob**, ∇ is a matrix of the same size as Φ. The encryption message

$$\triangle = e_{\Phi}(\nabla) = \Phi \star \nabla \star \Phi^{-1}$$

otherwise, we return to the key exchange protocol.

Lemma 3.4. *Let ∇_1, ∇_2 be two messages and for all invertible key not equal to unit matrix, Φ, we have:*

$$\begin{aligned} e_{\Phi}(\nabla_1 + \nabla_2) &= e_{\Phi}(\nabla_1) + e_{\Phi}(\nabla_2), \\ e_{\Phi}(\nabla_1 \star \nabla_2) &= e_{\Phi}(\nabla_1) \star e_{\Phi}(\nabla_2). \end{aligned}$$

Proof. We have:

$$\begin{aligned} e_{\Phi}(\nabla_1 + \nabla_2) &= \Phi \star (\nabla_1 + \nabla_2) \star \Phi^{-1} \\ &= (\Phi \star \nabla_1 + \Phi \star \nabla_2) \star \Phi^{-1} \\ &= \Phi \star \nabla_1 \star \Phi^{-1} + \Phi \star \nabla_2 \star \Phi^{-1} \\ &= e_{\Phi}(\nabla_1) + e_{\Phi}(\nabla_2) \end{aligned}$$

and

$$\begin{aligned} e_{\Phi}(\nabla_1 \star \nabla_2) &= \Phi \star (\nabla_1 \star \nabla_2) \star \Phi^{-1} \\ &= \Phi \star \nabla_1 \star \Phi^{-1} \star \Phi \star \nabla_2 \star \Phi^{-1} \\ &= e_{\Phi}(\nabla_1) \star e_{\Phi}(\nabla_2). \end{aligned}$$

□

Remark 3.5. *This encryption message is a fully homomorphic encryption that allows calculations to be performed on the ciphertext, producing an encrypted result that, when decrypted, matches the result of the operations performed on the plaintext.*

3.4. Decryption of message

When **Bob** receives the encrypted message $\triangle$ sent by **Alice**, it uses a decryption function to decrypt it. This function noted d_{Φ} is defined as follows:

$$d_{\Phi}(\triangle) = \Phi^{-1} \star \nabla \star \Phi.$$

Lemma 3.6. *For all message ∇, we have $d_{\Phi} \circ e_{\Phi}(\nabla) = \nabla$.*

Proof. We have:

$$\begin{aligned} d_{\Phi} \circ e_{\Phi}(\nabla) &= d_{\Phi}(e_{\Phi}(\nabla)) \\ &= \Phi^{-1} \star e_{\Phi}(\nabla) \star \Phi \\ &= \Phi^{-1} \star \Phi \star \nabla \star \Phi^{-1} \star \Phi \\ &= \nabla \end{aligned}$$

□

Remark 3.7. *The security of this cryptosystem is based on,*
- *the difficulty in computing the key Φ whose complexity is $\mathcal{O}\left(3^{tk}\right)$,*
- *the discrete logarithm problem on an elliptic curve.*

4. Numerical example

Alice and **Bob** choose a large prime number p, $r \in \mathbb{N}^*$ and a point P over an elliptic curve $E(\mathbb{F}_{p^r})$ of a large order $n > 10^{32}$.
First **Alice** chooses two matrices in $\aleph$,

$$A = \begin{pmatrix} 1 & P_{1,A} & P_{2,A} \\ Q_{3,A} & 2 & P_{3,A} \\ Q_{2,A} & Q_{1,A} & 3 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & P_{1,A_1} & P_{2,A_1} \\ Q_{3,A_1} & 2 & P_{3,A_1} \\ Q_{2,A_1} & Q_{1,A_1} & 3 \end{pmatrix}$$

and publish the pair $(A, \mathrm{C}_{\aleph}(A_1))$, in the same way, **Bob** chooses two matrices in $\aleph$,

$$B = \begin{pmatrix} 5 & P_{1,B} & P_{2,B} \\ Q_{3,B} & 2 & P_{3,B} \\ Q_{2,B} & Q_{1,B} & 3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & P_{1,B_2} & P_{2,B_2} \\ Q_{3,B_2} & 4 & P_{3,B_2} \\ Q_{2,B_2} & Q_{1,B_2} & 2 \end{pmatrix}$$

and publish the pair $(B, \mathrm{C}_{\aleph}(B_2))$.
To simplify the verification of our method, we will give the points of the matrices A, B, A_1 *and* B_2 as a function of the point P.
So, consider

$$A = \begin{pmatrix} 1 & P & P \\ 2P & 2 & P \\ 2P & 2P & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 2P & P \\ 2P & 2 & O \\ 2P & O & 3 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 1 & P & 2P \\ 3P & 2 & 3P \\ 2P & P & 3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & P & P \\ P & 4 & 2P \\ P & 5P & 2 \end{pmatrix}$$

Alice choose a private keys, $k = 19$, and a matrix

$$A_2 = \begin{pmatrix} 2 & P & P \\ P & 3 & 2P \\ P & 5P & 1 \end{pmatrix} \in \mathrm{C}_{\aleph}(B_2).$$

She calculated the matrix

$$(M(A_1, A+B, A_2))^{\star 19} = \begin{pmatrix} A_1^{\star 19} & T_{19} \\ 0 & A_2^{\star 19} \end{pmatrix}$$

Where

$$T_{19} = \sum_{i=0}^{18} A_1^{\star(18-i)}(A+B)A_2^{\star i} \tag{4.1}$$

$$= \begin{pmatrix} 3145722 & 7549456659P & 3489929930P \\ 4727164798P & 4646948716 & 15096291883P \\ 15097864744P & 141216865400P & 3486784398 \end{pmatrix} \tag{4.2}$$

and send it to **Bob**.

In turn, **Bob** choose a private keys, $t = 28$, and a matrix $B_1 = \begin{pmatrix} 1 & 2P & 4P \\ 6P & 3 & 6P \\ 4P & 2P & 5 \end{pmatrix} \in \mathrm{C}_{\aleph}(A_1)$. He calculated the matrix

$$(M(B_1, A+B, B_2))^{\star 28} = \begin{pmatrix} B_1^{\star 28} & E_{28} \\ 0 & B_2^{\star 28} \end{pmatrix}$$

Where
$E_{28} = \sum_{i=0}^{27} B_1^{\star(27-i)}(A+B)B_2^{\star i}$
$= \begin{pmatrix} 68630377364880 & 408166228667740245P & 745058745963944206 68P \\ 291776278982230708P & 288138868981891900 & 223805076368081713309P \\ 223517166263534710094P & 594245099411470048724P & 745058059687014103 38 \end{pmatrix}$ and send it

to **Alice**.
With their private keys k and t, **Alice** and **Bob** calculate separately the matrices:

$$\textbf{Alice}: M(A_1, E_{28}, A_2)^{\star 19} = \begin{pmatrix} A_1^{\star 19} & E_{28,19} \\ 0 & A_2^{\star 19} \end{pmatrix} \quad (4.3)$$

$$\textbf{Bob}: M(B_1, T_{19}, B_2)^{\star 28} = \begin{pmatrix} B_1^{\star 28} & T_{19,28} \\ 0 & B_2^{\star 28} \end{pmatrix} \quad (4.4)$$

Where, $E_{28,19} = \begin{pmatrix} a_1 & a_2P & a_3P \\ a_4P & a_5 & a_6P \\ a_7P & a_8P & a_9 \end{pmatrix}$ with,
$a_1 = 35982014657500840560$,
$a_2 = 4045330715650548582676534 65$,
$a_3 = 4329761367132924025435382 1864$,
$a_4 = 3347606713335388775284861 48$,
$a_5 = 3347416368112736979889501 00$,
$a_6 = 1302275822909818035206575 26727$,
$a_7 = 3029268330974050766883642 56534$,
$a_8 = 5638865124033116058442340 338994$,
$a_9 = 4329761363534722564785571 7754$,
and, $T_{19,28} = \begin{pmatrix} b_1 & b_2P & b_3P \\ b_4P & b_5 & b_6P \\ b_7P & b_8P & b_9 \end{pmatrix}$ with,
$b_1 = 35982014657500840560$,
$b_2 = 4045330715650548582676534 65$,
$b_3 = 4329761367132924025435382 1864$,
$b_4 = 3347606713335388775284861 48$,
$b_5 = 3347416368112736979889501 00$,
$b_6 = 1302275822909818035206575 26727$,
$b_7 = 3029268330974050766883642 56534$,
$b_8 = 5638865124033116058442340 338994$,
$b_9 = 4329761363534722564785571 7754$.
Hence, $E_{28,19} = T_{19,28}$.

Remark 4.1. *In this example, from small private keys $k = 19$ and $l = 28$, we have constructed a large private key:*

$$\Phi = \begin{pmatrix} a_1 & a_2P & a_3P \\ a_4P & a_5 & a_6P \\ a_7P & a_8P & a_9 \end{pmatrix}.$$

5. Conclusion

In this paper we have shown how noncommutative rings can be used in order to provide protocols that allow a key exchange in a secure manner. More precisely, we give a protocols based on the ring of the "elliptic" matrix, for an elliptic curve over $\mathbb{F}_q$. This protocol improves the matrix-based key exchange protocol. We use a matrix whose coefficients are in an elliptic curve and whose diagonal elements are in $\mathbb{Z}_n$, that are part of each user's private key. Thus, an attacker who wants to recover the shared secret must obtain summation:

$$\sum_{i=0}^{k-1} A_1^{k-1-i}(A+B)A_2^i = T_k \quad (5.1)$$

whose unknowns the matrices A_1, A_2 and the natural number k.
The security of this Cryptosystem is based on,
• the difficulty in computing the key Φ,
• the ECDLP problem; find an integer a, if it exists, such that $Q = aP$, with P and Q being well defined points of elliptic curve.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, Handbook of elliptic and hyperelliptic cryptography. Chapman and Hall/CRC (2006).
2. I. F. Blake, G. Seroussi and N. P. Smart, Elliptic Curves in Cryptography. Cambridge (1999).
3. I. F. Blake, G. Seroussi and N. P. Smart, Advances in Elliptic Curve Cryptography. Cambridge (2005).
4. C. Boyd & A. Mathuria, Protocols for Authentication and Key Establishment, Information Security and Cryptography Series, Springer-Verlag, Heidelberg, (2003).
5. A. Chillali, Cryptography over elliptic curve of the ring $\mathbb{F}_q[e], e^4 = 0$, World Acad. of Sci. Eng. & Technol. 78 (2011) 848-850.
6. J. J. Climent, P. R. Navarro and L. Tortosa, Key exchange protocols over non-commutative rings. The case of End $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$, Int. J. Comput. Math. 89(1314) (2012) 1753-1763.
7. M. Eftekhari, A Diffie-Hellman key exchange protocol using matrices over non-commutative rings, Groups Complex. Cryptol. 4(1) (2012) 167-176.
8. M. Eftekhari, Cryptanalysis of some protocols using matrices over group rings, in Int. Conf. on Cryptology in Africa: Progress in Cryptology - AFRICACRYPT 2017, Lecture Notes in Computer Science, Vol. 10239 (Springer, 2017).
9. S. D. Galbraith, Mathematics of public key cryptography. Cambridge University Press (2012).
10. D. Hankerson, A. Menezes and S. Vanstone, Guide to elliptic curve cryptography. Springer (2004).
11. D. Kahrobaei, C. Koupparis and V. Shpilrain, Public key exchange using matrices over group rings, Groups Complex. Cryptol. 5(1) (2013) 97-115.
12. A. J. Menezes and Y. H. Wu, The discrete logarithm problem in $GL(n, q)$, ARS Combinatoria. 47 (1997) 23-32.
13. G. Micheli, Cryptanalysis of a non-commutative key exchange protocol, Adv. Math. of Comm. 9(2) (2015) 247-253.
14. R. Odoni, V. Varadharajan and P. Sanders, Public key distribution in matrix rings, Electron. Lett. 20(9) (1984) 386-387.
15. A.P. Stakhov, The 'golden' matrices and a new kind of cryptography, Chaos, Solitons and Fractals 32 (2007) 1138-1146.
16. L. C. Washington, Elliptic Curves, Number Theory and Cryptography, 2nd edn. CRC Press (2008).
17. M. Zeriouh, A. Chillali and A. Boua, Cryptography Based on the Matrices, Bol. Soc. Paran. Mat (2019) 75-83.

Zakariae Cheddour,
Department of Mathematics,
University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, LSI Laboratory,
Taza, Morocco.
E-mail address: zakariae.cheddour@usmba.ac.ma

and

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

and

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