South East Asian J. of Mathematics and Mathematical Sciences
Vol. 19, No. 2 (2023), pp. 53-64

DOI: 10.56827/SEAJMMS.2023.1902.4 **ISSN (Online): 2582-0850**

ISSN (Print): 0972-7752

ON THE ARITHMETIC OF ENDOMORPHISM RING End$(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ AND ITS RSA VARIANTS

Ning Jauharotul Farida and Irawati

Algebra Research Group,
Faculty of Mathematics and Natural Sciences,
Institut Teknologi Bandung, Jalan Ganesha No 10,
Bandung, Jawa Barat, 40132, INDONESIA

E-mail : ningjfarida@itb.ac.id

(**Received:** *Apr. 04, 2023* **Accepted:** *Jul. 12, 2023* **Published:** *Aug. 30, 2023)*

Abstract: Bergman (1974) found that for any prime number p, the endomorphism ring End$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a semilocal ring which has p^5 elements and can not be embedded in matrices over any commutative ring. Later on, Climent et al. (2011) found that each element of endomorphism ring End$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ can be identified as a two by two matrix of E_p where the first and the second row entries belong to $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ respectively. By this characterization, Long D.T., Thu D. T., and Thuc D. N. constructed a new RSA variant based on End$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ (2013). In this paper, we state the characteristic of the endomorphism ring End $(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ and the RSA analogue cryptosystem based on it.

Keywords and Phrases: Endomorphism ring, RSA, monoid, cryptosystem, non-commutative ring.

2020 Mathematics Subject Classification: 16S50.

1. Introduction

Let p be a prime number. The set $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ is an additive group under component-wise addition with p^3 elements. The set of all group homomorphism of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ is a ring under addition and composition, denoted by End$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. George M. Bergman (1974) stated that End$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a semilocal ring with p^5 elements which can not be embedded in matrices over any commutative ring [2]. In

2011, Climent et al. conducted a research about the characteristic of End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$). They found that each element of End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$) can be identified as a two-by-two matrix which its first row and second row entries belong to $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ respectively [3].

Cryptosystems is the heart of the communication system. It guarantees data confidentiality, data integrity, authentication and non-repudiation in transferring data from one to others. One of the cryptosystems is River-Shamir-Adleman (RSA) cryptosystem. It was introduced by three researchers from Massachussets Institute of Technology (MIT), Rivest, Shamir, and Adleman on 1978. It becomes popular since it is widely used today. RSA is still seen in a range of web browsers, email, VPNs, chat and other communication channels. Since its popularity, many researchers have been trying to develop the variants of RSA cryptosystem till now. Some of them are RSA variant on platform $\mathbb{Z}_n$ ([5] and [7]), RSA variant on Gaussian integers ring [1], and elliptic curve group [4]. In 2013, Tran D. Long et al. conducted research to construct an RSA variant on a monoid which its multiplication was defined similarly to multiplication on Bergman ring [6]. This research enriched the number of new RSA variants.

This paper describes a new algebraic structure, endomorphism ring End($\mathbb{Z}_{p^2} \times \mathbb{Z}_p$) for any prime number p which is different with endomorphism ring End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$). It also explains a set $E_{p^2,p}$, set of two-by-two matrices which is isomorphic to End($\mathbb{Z}_{p^2} \times \mathbb{Z}_p$). Later, we construct an RSA variant based on End($\mathbb{Z}_{p^2} \times \mathbb{Z}_p$) by constructing a monoid $E_{n^2,n}$ where n is the product of two different prime numbers.

2. The Characterization of End ($\mathbb{Z}_{p^2} \times \mathbb{Z}_p$)

Let p be a prime number. The set $\mathbb{Z}_{p^2} \times \mathbb{Z}_p = \{(x, y)| \; x \in \mathbb{Z}_{p^2}, y \in \mathbb{Z}_p\}$ is an additive group under the component-wise addition

$$(x_1, y_1) + (x_2, y_2) = ((x_1 + x_2) \bmod p^2, (y_1 + y_2) \bmod p).$$

The set of all group endomorphism of $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ under the usual addition and composition function forms an endomorphism ring, denoted by End($\mathbb{Z}_{p^2} \times \mathbb{Z}_p$).

Theorem 1. *Let p be a prime number.*
The endomorphism ring End($\mathbb{Z}_{p^2} \times \mathbb{Z}_p$) can be described as follow:

$$End(\mathbb{Z}_{p^2} \times \mathbb{Z}_p) = \big\{\alpha \; \big| \alpha(1_{p^2}, 0) = (pa + b, d), \alpha(0, 1_p) = (pc, e)\big\}$$

where $a, b, c, d, e \in \mathbb{Z}_p$, 1_p and 1_{p^2} are multiplicative identity in $\mathbb{Z}_p$ dan $\mathbb{Z}_{p^2}$.

Proof. Since $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ is a module over $\mathbb{Z}_{p^2}$, then it can be expressed as

$$\mathbb{Z}_{p^2} \times \mathbb{Z}_p = \mathbb{Z}_{p^2}(1_{p^2}, 0) \oplus \mathbb{Z}_p(0, 1_p).$$

Thus, every (x, y) in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ can be written uniquely as $x(1_{p^2}, 0) + y(0, 1_p)$ where $x \in \mathbb{Z}_{p^2}$ and $y \in \mathbb{Z}_p$. Let $\alpha \in \mathrm{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ and (x, y) in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, then

$$\begin{aligned}\alpha(x, y) &= \alpha(x(1_{p^2}, 0)) + \alpha(y(0, 1_p)) \\ &= x\alpha(1_{p^2}, 0) + y\alpha(0, 1_p).\end{aligned}$$

From the latter expression, it can be seen that every α in $\mathrm{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ can be uniquely determined by $\alpha(1_{p^2}, 0)$ and $\alpha(0, 1_p)$ in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$. Now, suppose that $\alpha(1_{p^2}, 0) = (x_1, d)$ and $\alpha(0, 1_p) = (x_2, e)$ where $x_1, x_2 \in \mathbb{Z}_{p^2}, d, e \in \mathbb{Z}_p$.
Note that

$$(px_2, 0) = p(x_2, e) = p\alpha(0, 1_p) = \alpha(p(0, 1_p)) = \alpha(0, 0) = (0, 0).$$

Thus, $px_2 = 0$. Since $x_1, x_2 \in \mathbb{Z}_{p^2}$, then $x_2 = pc$ for $c \in \mathbb{Z}_p$ and $x_1 = pa + b$ for $a, b \in \mathbb{Z}_p$. Finally, each $\alpha \in \mathrm{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ is uniquely determined by $\alpha(1_{p^2}, 0) = (pa + b, d)$ and $\alpha(0, 1_p) = (pc, e)$ where $a, b, c, d, e \in \mathbb{Z}_p$.

Remark 2. *The number of elements of the endomorphism ring End*$(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ *is* p^5.

Later, we introduce the new set E_p for any prime number p.

$$E_{p^2,p} = \left\{ \begin{bmatrix} pa + b & pc \\ d & e \end{bmatrix} \text{ where } a, b, c, d, e \in \mathbb{Z}_p \right\}.$$

Let $A_1 = \begin{bmatrix} pa_1 + b_1 & pc_1 \\ d_1 & e_1 \end{bmatrix}, A_2 \begin{bmatrix} pa_2 + b_2 & pc_2 \\ d_2 & e_2 \end{bmatrix}$ be elements in $E_{p^2,p}$. Define addition and multiplication on $E_{p^2,p}$ as follow.

$$A_1 + A_2 = \begin{bmatrix} (p(a_1 + a_2) + (b_1 + b_2)) \bmod p^2 & (p(c_1 + c_2)) \bmod p^2 \\ (d_1 + d_2) \bmod p & (e_1 + e_2) \bmod p \end{bmatrix}$$

$$A_1A_2 = \begin{bmatrix} (p(a_1b_2 + b_1a_2 + c_1d_2) + (b_1b_2)) \bmod p^2 & (p(b_1c_2 + c_1e_2)) \bmod p^2 \\ (d_1b_2 + e_1d_2) \bmod p & (e_1e_2) \bmod p \end{bmatrix}$$

Theorem 3. *Let p be a prime number. The set $E_{p^2,p}$ that is described as above is a noncommutative unitary ring under the previous addition and multiplication. The identity element in $E_{p^2,p}$ is* $I = \begin{bmatrix} 1_{p^2} & 0 \\ 0 & 1_p \end{bmatrix}$.

Proof. The proof is straightforward.

Remark 4. *The number of elements of $E_{p^2,p}$ is p^5.*

On the next theorem, we will show that the endomorphism ring $\mathrm{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ is isomorphic to $E_{p^2,p}$.

Theorem 5. *Let p be any prime number. Define a map as follow:*

$$\psi : End(\mathbb{Z}_{p^2} \times \mathbb{Z}_p) \to E_{p^2,p}$$

$$\alpha \mapsto \begin{bmatrix} pa+b & pc \\ d & e \end{bmatrix}$$

where $\alpha(1_{p^2}, 0) = (pa+b, d), \alpha(0, 1_p) = (pc, e) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_p$ *and* $a, b, c, d, e \in \mathbb{Z}_p$. *Then,* ψ *is a ring isomorphism.*

Proof. It is clear that ψ is well-defined. Let $\alpha_1, \alpha_2 \in \text{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ where

$$\alpha_1(1_{p^2}, 0) = (pa_1 + b_1, d_1), \alpha_1(0, 1_p) = (pc_1, e_1),$$

$$\alpha_2(1_{p^2}, 0) = (pa_2 + b_2, d_2), \alpha_2(0, 1_p) = (pc_2, e_2)$$

where $a_i, b_i, c_i, d_i, e_i \in \mathbb{Z}_p$ for $i = 1, 2$. Note that

$$\begin{aligned}(\alpha_1 + \alpha_2)(1_{p^2}, 0) &= \alpha_1(1_{p^2}, 0) + \alpha_2(1_{p^2}, 0) \\ &= (pa_1 + b_1, d_1) + (pa_2 + b_2, d_2) \\ &= ((p(a_1 + a_2) + b_1 + b_2) \text{ mod } p^2, (d_1 + d_2) \text{ mod } p)\end{aligned}$$

and

$$\begin{aligned}(\alpha_1 + \alpha_2)(0, 1_p) &= \alpha_1(0, 1_p) + \alpha_2(0, 1_p) \\ &= (pc_1, e_1) + (pc_2, e_2) \\ &= ((p(c_1 + c_2)) \text{ mod } p^2, (e_1 + e_2) \text{ mod } p)\end{aligned}$$

Thus,

$$\begin{aligned}\psi(\alpha_1 + \alpha_2) &= \begin{bmatrix} (p(a_1 + a_2) + b_1 + b_2) \text{ mod } p^2 & (p(c_1 + c_2)) \text{ mod } p^2 \\ (d_1 + d_2) \text{ mod } p & (e_1 + e_2) \text{ mod } p \end{bmatrix} \\ &= \psi(\alpha_1) + \psi(\alpha_2).\end{aligned}$$

Note also that

$$\begin{aligned}(\alpha_1\alpha_2)(1_{p^2}, 0) &= \alpha_1(\alpha_2(1_{p^2}, 0) \\ &= \alpha_1(pa_2 + b_2, d_2) \\ &= (pa_2 + b_2)\alpha_1(1_{p^2}, 0) + d_2\alpha_1(0, 1_p) \\ &= (pa_2 + b_2)(pa_1 + b_1, d_1) + d_2(pc_1, e_1) \\ &= (p(a_1b_2 + b_1a_2 + c_1d_2) + b_1b_2) \text{ mod } p^2, (d_1b_2 + e_1d_2) \text{ mod } p)\end{aligned}$$

and

$$\begin{aligned}(\alpha_1\alpha_2)(0,1_p) &= \alpha_1(\alpha_2(0,1_p)) \\ &= \alpha_1(pc_2, e_2) \\ &= pc_2\alpha_1(1_{p^2},0) + e_2\alpha_1(0,1_p) \\ &= pc_2(pa_1+b_1,d_1) + e_2(pc_1,e_1) \\ &= (p(b_1c_2+c_1e_2) \bmod p^2, (e_1e_2) \bmod p)\end{aligned}$$

So that,

$$\begin{aligned}\psi(\alpha_1\alpha_2) &= \begin{bmatrix}(p(a_1b_2+b_1a_2+c_1d_2)+b_1b_2) \bmod p^2 & p(b_1c_2+c_1e_2) \bmod p^2 \\ (d_1b_2+e_1d_2) \bmod p & (e_1e_2) \bmod p\end{bmatrix} \\ &= \psi(\alpha_1)\psi(\alpha_2).\end{aligned}$$

Next, we will prove that ψ is injective.
Let $\alpha_1, \alpha_2 \in$ End$(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ where $\psi(\alpha_1) = \psi(\alpha_2)$. Suppose that

$$\alpha_1(1_{p^2},0) = (pa_1+b_1,d_1), \alpha_1(0,1_p) = (pc_1,e_1)$$

$$\alpha_2(1_{p^2},0) = (pa_2+b_2,d_2), \alpha_2(0,1_p) = (pc_2,e_2)$$

where $a_i, b_i, c_i, d_i, e_i \in \mathbb{Z}_p$ for $i = 1,2$.
Since $\psi(\alpha_1) = \psi(\alpha_2)$ then $a_1 = a_2,\ b_1 = b_2,\ c_1 = c_2,\ d_1 = d_2$, and $e_1 = e_2$.
Let (x,y) be any element of $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, thus

$$\begin{aligned}\alpha_1(x,y) &= x\alpha_1(1_{p^2},0) + y\alpha_1(0,1_p) \\ &= x(pa_1+b_1,d_1) + y(pc_1,e_1) \\ &= x(pa_2+b_2,d_2) + y(pc_2,e_2) \\ &= \alpha_2(x,y).\end{aligned}$$

So, ψ is injective. Since ψ is surjective since $|(\text{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p))| = |E_{p^2,p}|$ then psi is surjective. So, ψ is a ring isomoprhism. Based on this theorem, every element of End$(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ can be identified as a two by two matrix in E_p.

By this theorem, we can identify each element in End$(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ as a two by two matrix in $E_{p^2,p}$.

3. The Arithmetic of Ring $E_{p^2,p}$

As the consequence of theorem 5, the arithmetic of End$(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ can be identified same as the arithmetic of $E_{p^2,p}$. So, we will observe the arithmetic in $E_{p^2,p}$. In this section, we will regard $\mathbb{Z}_p$ as a subset of $\mathbb{Z}_{p^2}$ even $\mathbb{Z}_p$ is not subring of $\mathbb{Z}_{p^2}$.

Theorem 6. *Let p be a prime number,*

$A_1 = \begin{bmatrix} pa_1 + b_1 & pc_1 \\ d_1 & e_1 \end{bmatrix}$, $A_2 = \begin{bmatrix} pa_2 + b_2 & pc_2 \\ d_2 & e_2 \end{bmatrix}$ *be elements of* $E_{p^2,p}$, *then*

$$A_1 + A_2 = \begin{bmatrix} p\left(a_1 + a_2 + \left\lfloor \frac{b_1 + b_2}{p} \right\rfloor\right) \ mod\ p + (b_1 + b_2)\ mod\ p & p((c_1 + c_2)\ mod\ p) \\ (d_1 + d_2)\ mod\ p & (e_1 + e_2)\ mod\ p \end{bmatrix}.$$

Proof. Based on the definition of addition in $E_{p^2,p}$,

$$A_1 + A_2 = \begin{bmatrix} (p(a_1 + a_2) + b_1 + b_2) \text{ mod } p^2 & (p(c_1 + c_2)) \text{ mod } p^2 \\ (d_1 + d_2) \text{ mod } p & (e_1 + e_2) \text{ mod } p \end{bmatrix}.$$

By using Lemma 1 from Climent [3],
$((pa_1+b_1)+(pa_2+b_2)) \text{ mod } p^2 \equiv p\left(\left(a_1+a_2+\left\lfloor \frac{b_1 + b_2}{p} \right\rfloor\right) \text{ mod } p\right)+(b_1+b_2) \text{ mod } p$
and $(pc_1 + pc_2) \text{ mod } p^2 \equiv p(c_1 + c_2) \text{ mod } p$.
So,

$$A_1+A_2 = \begin{bmatrix} p\left(a_1 + a_2 + \left\lfloor \frac{b_1 + b_2}{p} \right\rfloor\right) \text{ mod } p + (b_1 + b_2) \text{ mod } p & p((c_1 + c_2) \text{ mod } p) \\ (d_1 + d_2) \text{ mod } p & (e_1 + e_2) \text{ mod } p \end{bmatrix}.$$

Hence, the proof is completed.

Theorem 7. *Let p be a prime number,* $A_1 = \begin{bmatrix} pa_1 + b_1 & pc_1 \\ d_1 & e_1 \end{bmatrix}, A_2 = \begin{bmatrix} pa_2 + b_2 & pc_2 \\ d_2 & e_2 \end{bmatrix}$ *be elements in* $E_{p^2,p}$, *then*

$$A_1A_2 = \begin{bmatrix} p\left(a_1b_2 + b_1a_2 + c_1d_2 + \left\lfloor \frac{b_1b_2}{p} \right\rfloor\right) \ mod\ p + (b_1b_2)\ mod\ p & p((b_1c_2 + c_1e_2)\ mod\ p) \\ (d_1b_2 + e_1d_2)\ mod\ p & (e_1e_2)\ mod\ p \end{bmatrix}$$

Proof. We use the similar argument of proof in Lemma 2 in Climent et al. [3].

Theorem 8. *Let p be a prime number and* $X = \begin{bmatrix} pa + b & pc \\ d & e \end{bmatrix}$ *be an element of* $E_{p^2,p}$. *Then X is invertible in* $E_{p^2,p}$ *if and only if* $e \neq 0$ *and* $b \neq 0$. *Let* X^{-1} *be the inverse of X then*

$$X^{-1} = \begin{bmatrix} pa' + b' & pc' \\ d' & e' \end{bmatrix}$$

where

$$a' = \left((b^{-1})^2 e^{-1} cd - a(b^{-1})^2 - \lfloor \frac{bb^{-1}}{p} \rfloor b^{-1}\right)\ mod\ p,$$
$$b' = (b^{-1})\ mod\ p, \qquad e' = (e^{-1})\ mod\ p,$$
$$c' = (-b^{-1}ce^{-1})\ mod\ p,\ dan$$
$$d' = (-e^{-1}b^{-1}d)\ mod\ p.$$

Proof. $(\Rightarrow)$ Let $X = \begin{bmatrix} pa+b & pc \\ d & e \end{bmatrix}$ be an invertible element in $E_{p^2,p}$. Then there is $Y = \begin{bmatrix} pa'+b' & pc' \\ d' & e' \end{bmatrix}$ in $E_{p^2,p}$ such that $XY = YX = \begin{bmatrix} 1_{p^2} & 0 \\ 0 & 1_p \end{bmatrix}$. Hence, $bb‘ = 1 \bmod p$ and $ee' = 1 \bmod p$. So that, both b and e must not be zero.
$(\Leftarrow)$ By the hypothesis, there exist b^{-1}, e^{-1} in $\mathbb{Z}_p$ such that $bb^{-1} = 1_p = ee^{-1}$. Let Y be an element of $E_{p^2,p}$ which its entries are the same as the entries of X^{-1} in this theorem. Then,

$$\begin{aligned}
XY &= \begin{bmatrix} pa+b & pc \\ d & e \end{bmatrix} \begin{bmatrix} pa'+b' & pc' \\ d' & e' \end{bmatrix} \\
&= \begin{bmatrix} p\left(ab' + ba' + cd' + \left\lfloor \dfrac{bb'}{p} \right\rfloor\right) \bmod p + (bb') \bmod p & p((bc' + ce') \bmod p) \\ (db' + ed') \bmod p & (ee') \bmod p \end{bmatrix} \\
&= \begin{bmatrix} 1_{p^2} & 0 \\ 0 & 1_p \end{bmatrix} \\
&= YX.
\end{aligned}$$

Hence, X is invertible in $E_{p^2,p}$. Thus, the proof is completed.

Example 8.1. In this example, we show how to use theorem 8 to find the inverse of invertible elements in $E_{p^2,p}$.
Let $A = \begin{bmatrix} 37 & 28 \\ 3 & 6 \end{bmatrix}$ be an element of $E_{49,7}$.
Let $a = 5, b = 2 \neq 0, c = 4, d = 3$, and $e = 6 \neq 0$, then $A = \begin{bmatrix} 7 \cdot 5 + 2 & 7 \cdot 4 \\ 3 & 6 \end{bmatrix}$.
Based on Theorem 8 A is invertible in $E_{49,7}$.
By theorem 8, we get
$a' = \left(4^2 \cdot 6 \cdot 4 \cdot 3 - 5 \cdot 4^2 - \lfloor \dfrac{2 \cdot 4}{7} \rfloor \cdot 4\right) \bmod 7 = 1548 \bmod 7 = 1 \bmod 7$
$b' = 4 \bmod 7$
$c' = (-4 \cdot 4 \cdot 6) \bmod 7 = -96 \bmod 7 = 2 \bmod 7$
$d' = (-6 \cdot 4 \cdot 3) \bmod 7 = -72 \bmod 7 = 5 \bmod 7$
$e' = 6 \bmod 7.$
Thus, $A^{-1} = \begin{bmatrix} 7 \cdot 1 + 4 & 7 \cdot 2 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 11 & 14 \\ 5 & 6 \end{bmatrix}$

Remark 9. *Let p be a prime number and $E^*_{p^2,p}$ is the set of all invertible elements of $E_{p^2,p}$. Then, $E^*_{p^2,p}$ is a multiplicative group and the order of $E^*_{p^2,p}$ is $p^3(p-1)^2$.*

4. The New RSA Variant

Before constructing the RSA analogue cryptosystem on the endomorphism ring

End($\mathbb{Z}_{p^2} \times \mathbb{Z}_p$), we state some sets and maps as follow.

Definition 1. *Let $n = p \cdot q$ where p, q be two different prime numbers. Denote $E_{n^2,n}$ as*

$$E_{n^2,n} = \left\{ \begin{bmatrix} a & nc \\ b & d \end{bmatrix} \middle| \, a \in \mathbb{Z}_{n^2}, b, c, d \in \mathbb{Z}_n \right\}.$$

Let $X = \begin{bmatrix} a_1 & nc_1 \\ b_1 & d_1 \end{bmatrix}, Y = \begin{bmatrix} a_2 & nc_2 \\ b_2 & d_2 \end{bmatrix} \in E_{n^2,n}$. Define

$$XY = \begin{bmatrix} a_1 & nc_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & nc_2 \\ b_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1a_2 + nc_1b_2) \ mod \ p^2 & n(a_1c_2 + c_1d_2) \ mod \ p^2 \\ (b_1a_2 + d_1b_2) \ mod \ p & (d_1d_2) \ mod \ p \end{bmatrix}.$$

*This multiplication is an associative binary operation on $E_{n^2,n}$. Thus, $E_{n^2,n}$ is a **monoid**.*

Define two maps θ_1 and θ_2 as follows:

$$\theta_1 : E_{n^2,n} \to E_{p^2,p} \text{ where}$$

$$\begin{bmatrix} a & nc \\ b & d \end{bmatrix} \longmapsto \begin{bmatrix} a \text{ mod } p^2 & p(qc\text{mod } p) \\ b \text{ mod } p & d \text{ mod } p \end{bmatrix} \text{ and}$$

$$\theta_2 : E_{n^2,n} \to E_{q^2,q} \text{ where}$$

$$\begin{bmatrix} a & nc \\ b & d \end{bmatrix} \longmapsto \begin{bmatrix} a \text{ mod } q^2 & q(pc\text{mod } q) \\ b \text{ mod } q & d \text{ mod } q \end{bmatrix}.$$

It is easily seen that θ_1 and θ_2 are well defined.

Theorem 10. *θ_1 and θ_2 defined above are monoid-homomorphisms.*

Proof. Let $X = \begin{bmatrix} a_1 & nc_1 \\ b_1 & d_1 \end{bmatrix}, Y = \begin{bmatrix} a_2 & nc_2 \\ b_2 & d_2 \end{bmatrix}$ be elements of $E_{n^2,n}$. Note that

$$\theta_1(X) = \begin{bmatrix} a_1 \text{ mod } p^2 & p(qc_1 \text{ mod } p) \\ b_1 \text{ mod } p & d_1 \text{ mod } p \end{bmatrix} \text{ and } \theta_1(Y) = \begin{bmatrix} a_2 \text{ mod } p^2 & p(qc_2 \text{ mod } p) \\ b_2 \text{ mod } p & d_2 \text{ mod } p \end{bmatrix}.$$

Hence,

$$\begin{aligned} \theta_1(XY) &= \theta_1\left(\begin{bmatrix} (a_1a_2 + nc_1b_2) \text{ mod } n^2 & n(a_1c_2 + c_1d_2) \text{ mod } n^2 \\ (b_1a_2 + d_1b_2) \text{ mod } n & (d_1d_2) \text{ mod } n \end{bmatrix} \right) \\ &= \begin{bmatrix} (a_1a_2 + nc_1b_2) \text{ mod } p^2 & p\big(q(a_1c_2 + c_1d_2) \text{ mod } p\big) \\ (b_1a_2 + d_1b_2) \text{ mod } p & (d_1d_2) \text{ mod } p \end{bmatrix} \\ &= \theta_1(X)\theta_1(Y). \end{aligned}$$

So that, θ_1 is a monoid-homomorphism. The similar argument can be used to prove that θ_2 is also a monoid-homomorphism.

Theorem 11. *Define a map* $\gamma : E_{n^2,n} \to E_{p^2,p} \times E_{q^2,q}$ *where*
$A \mapsto \big(\theta_1(A), \theta_2(A)\big)$
Then, γ *is injective.*

Proof. Let $A_1 = \begin{bmatrix} a_1 & nc_1 \\ b_1 & d_1 \end{bmatrix}$, $A_2 = \begin{bmatrix} a_2 & nc_2 \\ b_2 & d_2 \end{bmatrix}$ be elements of $E_{n^2,n}$ such that $\gamma(A_1) = \gamma(A_2)$. Hence,

$$\theta_1(A_1) = \theta_1(A_2)$$
$$\begin{bmatrix} a_1 \bmod p^2 & p(qc_1 \bmod p) \\ b_1 \bmod p & d_1 \bmod p \end{bmatrix} = \begin{bmatrix} a_2 \bmod p^2 & p(qc_2 \bmod p) \\ b_2 \bmod p & d_2 \bmod p \end{bmatrix}$$

and

$$\theta_2(A_1) = \theta_2(A_2)$$
$$\begin{bmatrix} a_1 \bmod q^2 & q(pc_1 \bmod q) \\ b_1 \bmod q & d_1 \bmod q \end{bmatrix} = \begin{bmatrix} a_2 \bmod q^2 & q(pc_2 \bmod q) \\ b_2 \bmod q & d_2 \bmod q \end{bmatrix}$$

Therefore, we will get the following equations:

(i) $a_1 \bmod p^2 = a_2 \bmod p^2$ dan $a_1 \bmod q^2 = a_2 \bmod q^2$

(ii) $b_1 \bmod p = b_2 \bmod p$ dan $b_1 \bmod q = b_2 \bmod q$

(iii) $c_1 \bmod p = c_2 \bmod p$ dan $c_1 \bmod q = c_2 \bmod q$

(iv) $d_1 \bmod p = d_2 \bmod p$ dan $d_1 \bmod q = d_2 \bmod q$

Since $p^2, q^2 \in \mathbb{Z}_p$, $\gcd(p^2, q^2) = 1$, $0 \le a_1, a_2 < p^2$, $0 \le a_1, a_2 < q^2$, then $a_1 = a_2$. The similar argument can be applied to prove that $b_1 = b_2, c_1 = c_2$, and $d_1 = d_2$. Hence, $A_1 = A_2$ and γ is an injective map. So that, the proof is completed.

The next theorem shows the requirement for elements in $E_{n^2,n}$ such that their maps under θ_1 and θ_2 is invertible in $E_{p^2,p}$ and $E_{q^2,q}$ respectively.

Theorem 12. *Let* $A = \begin{bmatrix} nu + v & nc \\ b & d \end{bmatrix} \in E_{n^2,n}$ *where* $u, v, b, c, d \in \mathbb{Z}_p$*, then* $\theta_1(A) \in E^*_{p^2,p}$ *and* $\theta_2(A) \in E^*_{q^2,q}$ *if and only if* $gcd(d, n) = 1$ *dan* $gcd(v, n) = 1$.

Proof. Based on the definition of θ_1 dan θ_2,

$$\theta_1(A) = \begin{bmatrix} p\left(\left\lfloor \dfrac{nu + v}{p} \right\rfloor \bmod p\right) + v \bmod p & p(qc \bmod p) \\ b \bmod p & d \bmod p \end{bmatrix}$$

and

$$\theta_2(A) = \begin{bmatrix} q\left(\left\lfloor \dfrac{nu+v}{q} \right\rfloor \bmod q\right) + v \bmod q & q(pc \bmod q) \\ b \bmod q & d \bmod q \end{bmatrix}.$$

By Theorem 8, $\theta_1(A) \in E^*_{p^2,p}$ if and only if

$$v \bmod p \neq 0 \text{ and } d \bmod p \neq 0.$$

Hence, $\gcd(v, p) = 1$ and $\gcd(d, p) = 1$. Since q is also a prime number, then $\theta_2(A) \in E^*_{q^2,q}$ if and only if

$$v \bmod q \neq 0 \text{ and } d \bmod q \neq 0.$$

By this result, we also get that $\gcd(v, q) = 1$ and $\gcd(d, q) = 1$.
Since $n = p \cdot q$, then $\gcd(v, n) = 1$ and $\gcd(d, n) = 1$. Hence, the proof is completed.

The most important step in constructing RSA cryptosystem is finding positive integers r, s such that $A^{rs} = A$ where A is an element in $E_{n^2,n}$. In the next theorem, we state these numbers.

Theorem 13. *Let A be an element of $E_{n^2,n}$ such that $\theta_1(A) \in E^*_{p^2,p}$ and $\theta_2(A) \in E^*_{q^2,q}$. Then $A^{rs} = A$ where r, s are natural numbers such that $rs \equiv 1$ mod L where*

$$L = lcm(p^3(p-1)^2, q^3(q-1)^2).$$

Proof. Since θ_1 and θ_2 are monoid-homomorphism, then $\theta_1(A^{rs}) = \big(\theta_1(A)\big)^{rs}$ and $\theta_2(A^{rs}) = \big(\theta_2(A)\big)^{rs}$. By the hypothesis, $\theta_1(A) \in E^*_{p^2,p}$ and $\theta_2(A) \in E^*_{q^2,q}$ which their order is $p^3(p-1)^2$ and $q^3(q-1)^2$ respectively. Thus,

$$\theta_1(A^{rs}) = \big(\theta_1(A)\big)^{rs} = \big(\theta_1(A)\big)^{1 \bmod L} = \theta_1(A) \text{ and}$$

$$\theta_2(A^{rs}) = \big(\theta_2(A)\big)^{rs} = \big(\theta_2(A)\big)^{1 \bmod L} = \theta_2(A).$$

So that,

$$\begin{aligned} \gamma(A^{rs}) &= (\theta_1(A^{rs}), \theta_2(A^{rs})) \\ &= \Big(\big(\theta_1(A)\big)^{rs}, \big(\theta_2(A)\big)^{rs}\Big) && \text{by Theorem 10} \\ &= (\theta_1(A), \theta_2(A)) && \text{by Theorem 13} \\ &= \gamma(A) && \text{by the definition of } \gamma \end{aligned}$$

Since γ is injective, then $A^{rs} = A$. Hence, the proof is completed.

Now, we are ready to construct RSA analogue cryptosystem by using our theorems above. There are three main activities in RSA analogue cryptosystem: generating key, encryption, and decryption. Here are the algorithm for all of them:

Generating Key Algorithm

Input : Choose p, q different prime numbers.
Process : Calculate $L = \text{lcm}(p^3(p-1)^2, q^3(q-1)^2)$,
: Choose positive integer $0 < r < L$ where $\gcd(L, r) = 1$,
: Calculate $s \equiv r^{-1} \bmod L$,
Output : Publish (n, r) as public key, keep (n, s) as a private key.

Encryption Algorithm

Input : Choose $0 \leq b \leq n-1$ as a plaintext.
Process : Choose $c, d, u, v \in \mathbb{Z}_n$ such that $\gcd(d, n) = 1$, $\gcd(v, n) = 1$.
: Choose positive integer $0 < r < L$ where $\gcd(L, r) = 1$,
: Let $A = \begin{bmatrix} nu+v & nc \\ b & d \end{bmatrix}$.
: Calculate $B = A^r$.
Output : B:= ciphertext.

Decryption Algorithm

Input : Recall B:= ciphertext.
Process : Calculate B^s.
Output : $A = \begin{bmatrix} nu+v & nc \\ b & d \end{bmatrix}$, $b :=$ plaintext.

Example 13.1. Ali will sent a message to Bob, that is "math". Ali will use RSA cryptosystem based on $\text{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ to send it to Bob.
Let $p = 5$ and $q = 7$, then $n = 35$ and $L = 6174000$.
Choose $r = 17$ then we get $s = r^{-1} \bmod L = 726353$. Publish $(35, 17)$ as a public key and keep $(35, 726353)$ as a private key. Bob must keep this key to decrypt ciphertext from Ali.
Let a plaintext "math" is corresponding to $b = 1$ in the first column and second row of a matrix $A = \begin{bmatrix} 35 \cdot 1 + 9 & 35 \cdot 4 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 43 & 140 \\ 1 & 3 \end{bmatrix}$. The message "math" will be encrypted as $B = A^{17}$. Bob must use the private key to decrypt this message by calculating B^{726353}.

5. Conclusion

By this research, the endomorphism ring $\text{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ is isomorphic to $E_{p^2,p}$, a set of two by two matrices where the first and the second row entries belong to $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p$ respectively. It means, each element of $\text{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ can be identified as a two by two matrix in $E_{p^2,p}$. The arithmetic in $\text{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ can also be seen from the arithmetic in $E_{p^2,p}$. This paper also provide the other RSA variant based on the endomorphism ring $\text{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$. For further research, we can observe the structure of $\text{End}(\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})$ where m is different from n. If it is possible, we also can construct the RSA variant based on this ring.

References

[1] Abdul-Nasser El-Kassar, Ramzi Haraty, Yahia Awad, and Narayan Debnath, Modified rsa in the domains of gaussian integers and polynomials over finite fields, 01 (2005), 298–303.

[2] Bergman G. M., Some examples in pi ring theory, Israel J. Math, 18 (1974), 257–277.

[3] Climent J. J., Navarro P. and Tortosa L., On the arithmetic of the endomorphisms ring End $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, AAECC, 22, 03 (2011).

[4] Demytko N., A new elliptic curve based analogue of rsa, In Advances in Cryptology - EUROCRYPT '93, Vol. 765 (1993), 40–49.

[5] Fiat A., Batch rsa, Journal of Cryptology, 10 (1997).

[6] Long D. T., Thu D. T. and Thuc D. N., A bergman ring based cryptosystem analogue of rsa, In 2013 International Conference on IT Convergence and Security (ICITCS), (2013), pages 1–4.

[7] Thomas Collins, Dale Hopkins, Susan Langford, and Michael Sabin. Public key cryptographic apparatus and method. (RE40530), October (2008).