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