South East Asian J. of Mathematics and Mathematical Sciences
Vol. 17, No. 3 (2021), pp. 01-16

ISSN (Online): 2582-0850

ISSN (Print): 0972-7752

CRYPTANALYSIS OF RSA-LIKE CRYPTOSYSTEM WITH MODULUS $N = pq$ AND $ed \equiv 1(\text{mod } (p^2+p+1)(q^2+q+1))$

L. Jyotsna and L. Praveen Kumar

Department of Mathematical and Computational Sciences,
Sri Sathya Sai University for Human Excellence,
Kalaburagi - 585313, Karnataka, INDIA

E-mail : jyotsna.l@sssuhe.ac.in, praveen.l@sssuhe.ac.in

(**Received:** *Apr. 12, 2021* **Accepted:** *Oct. 28, 2021* **Published:** *Dec. 30, 2021)*

Abstract: In 2018, N. Murru and F. M. Saettone proposed a novel RSA-like cryptosystem with modulus $N = pq$ and $ed \equiv 1(\text{ mod } (p^2+p+1)(q^2+q+1))$ based on a generalization of the Rédei Rational functions. In this paper, we give some bounds on the deciphering exponent $d = N^\delta$, in which this RSA-like cryptosystem is insecure. For the enciphering exponent $e = N^\alpha$ and $p + q + 1 = N^\beta$, the attack bound on d is $\delta < \frac{2-(\alpha+\beta)}{3}$ in the case of $\alpha < 1$ and $\delta < \frac{\alpha-2\beta}{2}$ when $\alpha > 1$. Furthermore, we describe the magnitude of the bounds in all cases of α and β.

Keywords and Phrases: RSA-like cryptosystem, Cryptanalysis, LLL algorithm, Coppersmith's method.

2020 Mathematics Subject Classification: 11T71.

1. Introduction

RSA Cryptosystem [8] is the first public-key cryptosystem invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977 and is widely used for secure data transmission. RSA involves a public key and a private key. The public key (enciphering exponent) can be shared with everyone, whereas the private key (deciphering exponent) must be kept secret. The keys for the RSA algorithm are generated in the following way:

- Choose two distinct prime numbers p, q, and compute $N = pq$, the RSA modulus.