IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, August 2023

Performance Evaluation of Tensor Based Light Weight Fully Homomorphic Encryption Scheme

Vinay Kumar Devara[1], Dr. Anshul Mishra[2], Dr. D. Ramesh [3]
Research Scholar Department of Computer Science[1]
Research Supervisor Department of Computer Science and Engineering[2]
NIILM University, Kaithal, Haryana, India[1,2]
Research Co-Supervisor Department of Computer Science[3]
Kakatiya University, Warangal-TG, India[3]

Abstract*: FHE is an outstanding research field on cryptography which facilitates to perform computation on encrypted data. In this research, an effective, simple, secure, and lightweight homomorphic encryption structure is introduced for SHE structure which depends on the integers and utilized matrix. Then employ the coppersmith matrix multiplication method to perform matrix multiplication at the encryption and decryption step to make the scheme more secure. Additionally, a new algorithm is introduced to generate a key and refreshed it for every computation with a stipulated time interval. In the future, this proposed system can be used for asymmetric cryptosystem with two keys, one for encryption, and other for decryption which is more scalable and reliable with high-security measures.*

Keywords: Homomorphic Encryption, Keygen (), Enc () And Dec () Schemes

DOI: 10.48175/568