IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

A Right Duo Seminearring based Key Exchange Technique

Senthil S[1], Perumal R[2], and Babu M[3]
Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India[1,3]
Department of Mathematics, College of Engineering and Technology,
SRM Institute of Science and Technology, Kattankulathur, Tamilnadu, India[2]
senthilsports@yahoo.co.in, perumalr@srmist.edu.in, mbabu5689@gmail.com

Abstract: *In this paper, we present a novel symmetric key exchange protocol based on Right duo seminearring. The proposed protocol leverages the unique algebraic properties of Right duo seminearrings to ensure secure key exchange. We provide detailed examples to illustrate the protocol's functionality and practical applicability. The algorithm's structure is elaborated, and its time complexity is analyzed to demonstrate computational efficiency. Furthermore, a comprehensive security analysis is conducted, highlighting the protocol's resilience against common cryptographic attacks. The proposed cryptosystem offers a secure and efficient approach to symmetric key exchange, contributing to the advancement of algebra-based cryptographic protocols.*

Keywords: Key exchange, Semirings, Cryptography 2000 Mathematics subject classification: 16Y60, 94A60, 14G50, 11K70, 11T71

DOI: 10.48175/568