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: 7.53
Volume 4, Issue 1, August 2024

An Analysis of Lattice Methods in Quantum-Resilient Cryptographic Designs

Gauswami Rohitgiri Mahendragiri[1] and Dr. Rajeev Kumar [2]
Research Scholar, Department of Math[1]
Associate Professor, Department of Math[2]
Sunrise University, Alwar, Rajasthan, India

Abstract: *A secure encryption technique can be produced by applying mathematics to cryptography. In the realm of cryptography, lattices have become a potent mathematical tool with a wide range of uses, from safe multi-party computing to encryption. This study offers a thorough analysis of lattices' function in cryptography, encompassing both its theoretical underpinnings and real-world applications. The fundamental ideas of lattices and their application to cryptographic protocols are covered in the first section of the study. It then examines important cryptographic primitives based on lattice issues, including digital signatures, completely homomorphic encryption, and lattice-based encryption algorithms. A novel lattice-based cryptography technique is also suggested in the study*

Keywords: Lattice-Based Cryptography, Shortest Vector Problem, Learning With Errors, Post-Quantum Cryptography, Quantum Resistance, Cryptographic Primitives, Public Key Encryption, Digital Signatures, Lattice Reduction, Homomorphic Encryption, Security Proofs, Quantum Computing Threats, Cryptanalysis, Code-based Cryptography, Lattices, group theory

DOI: 10.48175/568