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 2, July 2024

Optimizing Number Theoretic Transform Techniques for Enhanced Lattice-Based Cryptography

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: *Conventional public key cryptography will be broken by a massive quantum computer. An alternative for safeguarding communications in the age of quantum computing is lattice-based cryptography. One appealing method for effectively handling polynomial multiplication is the Number Theory Transform (NTT).For many systems, including battery-operated devices and Internet of Things (IoT) gadgets, low power consumption is essential. However, further study is needed to develop NTTs that are low power and efficient. The suggested design may be implemented using inexpensive single-port RAM and only requires n log (n) clock cycles*

Keywords: Number Theoretic Transform (NTT), Modular Arithmetic, Polynomial Multiplication

DOI: 10.48175/568