UNIVERSITY OF MINNESOTA
Driven to Discover℠

Reduced complexity modular polynomial multiplication for R-LWE cryptosystems

A method for integrating modular reduction into Karatsuba polynomial multiplication, used to optimize performance of R-LWR-based ciphers and other cryptographic systems.

IP Status: US Patent Issued; Patent No. 11,750,366

Applications

- Post-quantum cryptography
- Homomorphic encryption
- Secure cloud computing

Technology Overview

In post-quantum cryptography, ring-learning with errors (R-LWR) is a computational problem utilized to build new cryptographic ciphers that resist quantum-computing attacks. Modular multiplication of long polynomials with large coefficients is the most critical operation in these ciphers, and the complexity of these operations drives significant energy consumption.

Researchers at the University of Minnesota have developed a new method for integrating modular reduction into Karatsuba polynomial multiplication. Using this complexity reduction method, modular reduction is applied to intermediate segment products instead of the final product. As a result, additional sub-structure sharing is enabled, and the number of coefficient additions needed for assembling the segment products to get the final result is substantially reduced. For polynomial multiplications with decomposition factors 2, 3, and 4, this method reduces the number of additions by 13-17%. This innovative method optimizes the performance of R-LWR-based ciphers and other cryptographic systems reliant on polynomial multiplication. By integrating modular reduction into Karatsuba polynomial multiplication, this method achieves significant efficiency gains while ensuring continued security and resilience of these encryption techniques in the face of quantum computing threats.

Phase of Development

TRL: 3-4
The researchers have tested this method to validate analytical predictions. For polynomial multiplications with decomposition factors 2, 3, and 4, this method reduces the number of additions by 13-17%.

Desired Partnerships

This technology is now available for:

- License
- Sponsored research
- Co-development

Please contact our office to share your business' needs and learn more.

Technology ID
2021-250

Category
Software & IT/Algorithms
Software & IT/Cloud Computing
Software & IT/Cyber Security
Software & IT/Data Mining
Software & IT/Databases
Software & IT/Health IT

Learn more

Researchers

- **Keshab Parhi, PhD** Distinguished McKnight University Professor, Department of Electrical and Computer Engineering

References

1. Xinmiao Zhang; Keshab K. Parhi(13 May 2021) , https://doi.org/10.1109/ICASSP39728.2021.9414005, https://ieeexplore.ieee.org/document/9414005
2. Zhang, X., Huai, Z. & Parhi, K.K.(2022) , https://doi.org/10.1007/s11265-022-01746-7, https://link.springer.com/article/10.1007/s11265-022-01746-7, 94, 799–809