Improving Cheon-Kim-Kim-Song (CKKS) Performance with Vector Computation and GPU Acceleration

Authors : Smaran Manchala

Abstract : Homomorphic Encryption (HE) enables computations on encrypted data without requiring decryption, mitigating data vulnerability during processing. Usable Fully Homomorphic Encryption (FHE) could revolutionize secure data operations across cloud computing, AI training, and healthcare, providing both privacy and functionality, however, the computational inefficiency of schemes like Cheon-Kim-Kim-Song (CKKS) hinders their widespread practical use. This study focuses on optimizing CKKS for faster matrix operations through the implementation of vector computation parallelization and GPU acceleration. The variable effects of vector parallelization on GPUs were explored, recognizing that while parallelization typically accelerates operations, it could introduce overhead that results in slower runtimes, especially in smaller, less computationally demanding operations. To assess performance, two neural network models, MLPN and CNN—were tested on the MNIST dataset using both ARM and x86-64 architectures, with CNN chosen for its higher computational demands. Each test was repeated 1,000 times, and outliers were removed via Z-score analysis to measure the effect of vector parallelization on CKKS performance. Model accuracy was also evaluated under CKKS encryption to ensure optimizations did not compromise results. According to the results of the trail runs, applying vector parallelization had a 2.63X efficiency increase overall with a 1.83X performance increase for x86-64 over ARM architecture. Overall, these results suggest that the application of vector parallelization in tandem with GPU acceleration significantly improves the efficiency of CKKS even while accounting for vector parallelization overhead, providing impact in future zero trust operations.

Keywords : CKKS scheme, runtime efficiency, fully homomorphic encryption (FHE), GPU acceleration, vector parallelization

Conference Title : ICECECE 2024 : International Conference on Electrical, Computer, Electronics and Communication Engineering

Conference Location : New York, United States

Conference Dates : December 09-10, 2024

Open Science Index, Electrical and Computer Engineering Vol:18, No:12, 2024 publications.waset.org/abstracts/192456.pdf