Abstract: Fully Homomorphic Encryption (FHE) is a technique that allows arbitrary computations to be performed on encrypted data without the need for decryption, making it ideal for securing many emerging applications. However, FHE computation is significantly slower than computation on plain data due to the increase in data size after encryption. Processing In-Memory (PIM) is a promising technology that can accelerate data-intensive workloads with extensive parallelism. However, FHE is challenging for PIM acceleration due to the long-bitwidth multiplications and complex data movements involved. We propose a PIM-based FHE accelerator, FHEmem, which exploits a novel processing in-memory architecture to achieve high-throughput and efficient acceleration for FHE. We propose an optimized end-to-end processing flow, from low-level hardware processing to high-level application mapping, that fully exploits the high throughput of FHEmem hardware. Our evaluation shows FHEmem achieves significant speedup and efficiency improvement over state-of-the-art FHE accelerators.

@misc{zhou2023fhemem, title={FHEmem: A Processing In-Memory Accelerator for Fully Homomorphic Encryption}, author={Minxuan Zhou and Yujin Nam and Pranav Gangwar and Weihong Xu and Arpan Dutta and Kartikeyan Subramanyam and Chris Wilkerson and Rosario Cammarota and Saransh Gupta and Tajana Rosing}, year={2023}, eprint={2311.16293}, archivePrefix={arXiv}, primaryClass={cs.AR} }

FHEmem: A Processing In-Memory Accelerator for Fully Homomorphic Encryption

Fully Homomorphic Encryption (FHE) is a technique that allows arbitrary computations to be performed on encrypted data without the need for decryption, making it ideal for securing many emerging applications. However, FHE computation is significantly...