

ABSTRACT

A Hardware-Assisted Integrity Protection Mechanism For Fully Homomorphic Encryption In Keystone

By

Muhammad Alfi Ramadhan

Fully Homomorphic Encryption (FHE) enables computations on encrypted data but suffers from double encryption overhead when deployed in Trusted Execution Environments (TEEs) like Intel SGX, where hardware memory encryption redundantly encrypts already-encrypted FHE data. This research implements a hardware-assisted integrity protection mechanism for FHE computations in Keystone Enclave using Bonsai Merkle Trees (BMT) to eliminate unnecessary encryption while maintaining security guarantees. The study develops a BMT integrity verification system integrated into gem5's memory controller, constructing an authentication tree over counter blocks rather than individual data blocks for improved storage efficiency. Performance evaluation using T2 FHE benchmarks compares three scenarios: unprotected Keystone execution, BMT-only protection, and full memory protection with both encryption and integrity verification.

Baseline analysis reveals that FHE computations generate substantial memory traffic due to large ciphertext structures. A 4×4 matrix multiplication produces 2.35 million DRAM reads and 1.19 million writes as the memory requirements significantly exceed the 1 MB L2 cache capacity in a single-core system, causing frequent evictions and reloads. Further results demonstrate that BMT-only protection introduces modest overhead of 2.28% for 4×4 matrices and 4.67% for 8×8 matrices. Adding memory encryption increases total overhead to only 2.46% and 4.99% respectively, with encryption contributing minimal additional cost (0.17% and 0.30%). BMT operations consume only 2.2% and 4.5% of total execution time, with the vast majority (95.5-97.8%) dedicated to core FHE computations. This work demonstrates that hardware-assisted BMT integrity protection provides efficient security for FHE computations without additional encryption penalties.

Keywords: Fully Homomorphic Encryption, Trusted Execution Environments, Bonsai Merkle Tree