HEAX: High-Performance Hardware Architecture for Microsoft SEAL

Sadegh Riazi, Kim Laine, Blake Pelton, Wei Dai
Microsoft Research

Abstract
HEAX is a high-performance hardware architecture for accelerating computation on Homomorphically encrypted data in the cloud. Each component within HEAX is fully pipelined, providing high-throughput computations on cipher texts. Proof-of-concept implementation on FPGA demonstrates more than two orders of magnitude performance improvement that fully saturates the PCIe bus used to transfer data between CPU and FPGA board. Thus, HEAX achieves an optimal hardware acceleration for computing on Homomorphically encrypted data compared to other hardware-based acceleration solutions including any type of FPGAs or GPUs as they should be connected using PCIe bus. From system-view perspective, the bottleneck is the bandwidth of PCIe that is used to transfer data from host CPU to FPGA and vice versa.

High-level System View

FPGA Resource Utilization

Proof-of-concept implementation on FPGA shows more than two orders of magnitude performance improvement that fully saturates the PCIe bus used to transfer data between CPU and FPGA board. Thus, HEAX achieves an optimal hardware acceleration for computing on Homomorphically encrypted data compared to other hardware-based acceleration solutions including any type of FPGAs or GPUs as they should be connected using PCIe bus. From system-view perspective, the bottleneck is the bandwidth of PCIe that is used to transfer data from host CPU to FPGA and vice versa.

Performance Results

NTT Module Pipeline

NTT Module Architecture

KeySwitch Module Pipeline

KeySwitch Module Architecture

Multiplication Module Architecture