USC Viterbi School of Engineering

Seminar

Ming Hsieh Department of Electrical and Computer Engineering

Code generation for cryptographic kernels using multi-word modular arithmetic

Naifeng Zhang
PhD Candidate, Electrical and Computer Engineering
Carnegie Mellon University

Friday, May 9, 2025 | 11am - 12pm | MCB 102

Abstract: Fully homomorphic encryption (FHE) and zero-knowledge proofs (ZKPs) are emerging as solutions for data security in distributed environments. However, the widespread adoption of these encryption techniques is hindered by their significant computational overhead, primarily resulting from core cryptographic operations that involve large integer arithmetic. This paper presents a formalization of multi-word modular arithmetic (MoMA), which breaks down large bit-width integer arithmetic into operations on machine words. We further develop a rewrite system that implements MoMA through recursive rewriting of data types, designed for compatibility with compiler infrastructures and code generators. We evaluate MoMA by generating cryptographic kernels, including basic linear algebra subprogram (BLAS) operations and the number theoretic transform (NTT), targeting various GPUs. Our MoMA-based BLAS operations outperform state-of-the-art multi-precision libraries by orders of magnitude, and MoMA-based NTTs achieve near-ASIC performance on commodity GPUs.

Bio: Naifeng Zhang is a fourth-year Ph.D. candidate in Electrical and Computer Engineering at Carnegie Mellon University, advised by Professor Franz Franchetti. He received bachelor's degrees in Mathematics and Computer Science from the University of Southern California, advised by Professor Viktor K. Prasanna. His research interests include high-performance code generation, programming languages, compilers, and algorithms. His webpage can be found at https://naifeng.github.io/

Host: Viktor Prasanna, prasanna@usc.edu