

Accelerating Large Integer Modular Multiplication using Vector Instructions

Advisor: **Selim Kirbiyik**

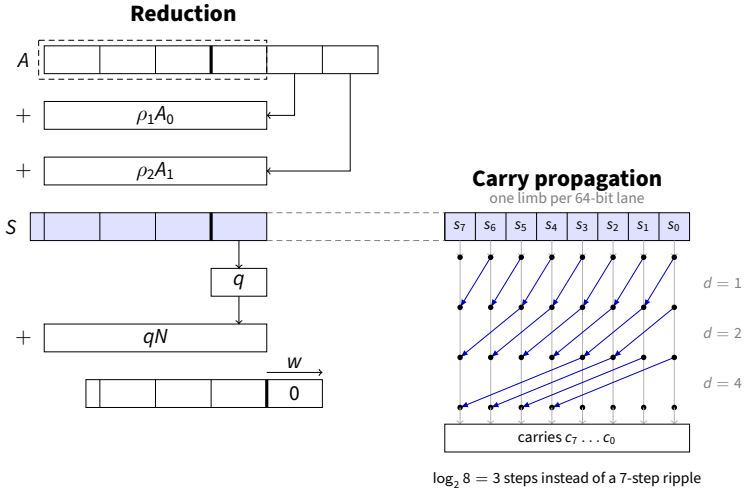
Motivation

Modular multiplication is a key cryptographic operation that dominates cryptographic implementations. Performing modular multiplications at large operand sizes also brings significant challenges. Memory residency and ALU utilization trade-offs offer design choices that require exploration.

In this topic, we want to explore low-latency implementations of large-integer modular multiplication. Newer processors offer vector instructions which allow for low-latency parallel arithmetic. Specifically the IFMA instructions are of interest.

Goals and Tasks

- Understand vectorization friendly modular reduction algorithms
- Explore trade-offs between different scan algorithms for the addition steps
- Improve upon the lowest latency implementations



Parallel reduction with KS as the scan algorithm.

Literature

- S. Kırbıyık et al.
  Efficient Parallelization of Large-Scale Modular Multiplication via Low-Latency LogJumps

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ MATH

Prerequisites

- Interest in fast modular arithmetic
- Programming (x86_64 Assembly, C/C++, Python)

Advisor Contact

selim.kirbiyik@tugraz.at