

Utilizing Neural Processing Units for Cryptography

Advisor: **Selim Kirbiyik**

Motivation

Modern processing units include integrated low-power AI accelerators called Neural Processing Units (NPUs). One such example is the AMD XDNA NPU, which features a spatial array architecture with low precision optimized for ML workloads. These architectures are specialized for performing efficient matrix-matrix multiplications.

Identifying which of the cryptographic primitives can be expressed as a matrix-matrix multiplication is of interest. Number Theoretic Transform, utilized in lattice-based cryptography, can be viewed as a matrix product and is a suitable candidate.

Goals and Tasks

-  Understand AMD XDNA architecture
-  Explore how well cryptographic primitives map to NPUs
-  Implement efficient techniques to map primitives to NPUs

Literature

- > [S. Santan](#)
AMD NPU - Linux Documentation
docs.kernel.org/accel/amdxdna/amdnpu.html

Courses & Deliverables

☒ Master Project

Project code
Report
Presentation

– OR –

☒ Master's Thesis

Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

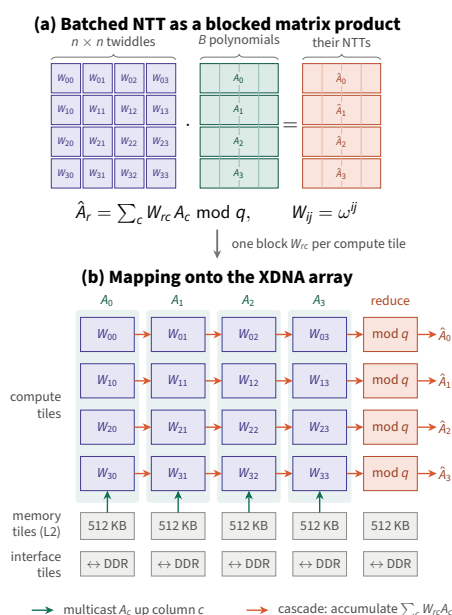
☒ CS ☒ ICE ☒ MATH

Prerequisites

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

Advisor Contact

selim.kirbiyik@tugraz.at



An example usage of NPUs.