Highly Parallelized Implementation of MiMC and Related Designs

Advisor(s): Sebastian Ramacher and Markus Schofnegger

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Lightweight block ciphers find many interesting applications in advanced cryptographic schemes and protocols. Recently, the lightweight cipher MiMC [1] and various designs based on the same ideas have been used to build post-quantum signatures.
In particular, the zero-knowledge proof system ZKB++ [2] benefits from ciphers using a comparatively small number of multiplications. Additionally, the protocol requires subsequent evaluations of a block cipher with varying key material. However, for certain instances of MiMC and related designs, the size of the computations is well below the word size of the processor, hence "wasting" part of the instructions.
In the current implementation of ZKB++, there is no parallelism in the evaluations of the block cipher. Your task is to investigate which operations can be executed in parallel, and how these operations can be implemented in order to increase the amount of parallelism and – possibly – reduce the total runtime of the protocol.

Goals and Tasks

- Get familiar with MiMC and ZKB++
- Study existing implementations and parallelization techniques
- Develop and implement a highly parallelized version of MiMC and related designs

Literature

- M. R. Albrecht et al.
  MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity
  ASIACRYPT (1)
- M. Chase et al.
  Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives
  CCS

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Interest in cryptography
- Programming (C/C++, Python)

Advisor / Contact

markus.schofnegger@iaik.tugraz.at