Highly Parallelized Implementation of LowMC

Advisor(s): Daniel Kales and Sebastian Ramacher

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 LowMC has been used to build post-quantum signatures and variants such as ring signatures and double-authentication preventing signatures.
Those applications benefit from highly efficient implementations of LowMC, as they require multiple evaluations of the cipher with varying key material. However, LowMC has an expansive linear layer involving large matrix multiplications. Recent work has significantly reduced the costs of the linear layer, but the involved matrices have dimensions that no longer match word boundaries and SIMD instruction sizes. Thus we want to look into alternative implementation techniques for matrix-vector implementations, that can still benefit from speedups provided by SIMD instruction sets. One option could be to compute the matrix-vector in parallel for multiple vectors in a bit-sliced manner.
Your task is to investigate, design and implement a highly parallelized LowMC variant, that is suitable for use in its applications.

Goals and Tasks

- Get familiar with LowMC
- Study existing implementations and parallelization techniques
- Develop and implement highly parallelized version of LowMC

Literature

- D. Kales et al.
  Improvements to the Linear Layer of LowMC: A Faster Picnic
  IACR Cryptology ePrint Archive 2017
  https://eprint.iacr.org/2017/1148
- I. Dinur
  Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC
  IACR Cryptology ePrint Archive 2018
  https://eprint.iacr.org/2018/772

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

daniel.kales@iaik.tugraz.at