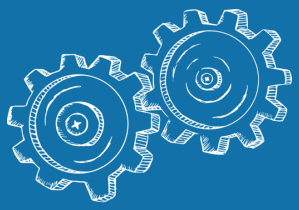

Finding Optimal Attacks on GGM Trees

Advisor: **Robert Primas**

Motivation

A GGM tree is a special cryptographic construction that allows building symmetric cryptographic schemes that are inherently secure against powerful DPA attacks, without that need for implementation-level countermeasures such as masking. With ISAP, we currently have a submission to NIST's standardization project for lightweight cryptography that utilizes a sponge variant of a GGM tree.

When using GGM trees, one can tweak various parameters that result in different trade-offs between DPA protection and performance. In this work, you shall first study the effective DPA protection of ISAP in its current form by (1) performing practical measurements on microprocessors and FPGAs (2) analytically analyzing the maximum amount of key bits an attacker could extract if he is limited to a certain amount of memory/computational complexity. Based on this analysis you shall then define and test more aggressive parameters for ISAP that improve performance but still offer plenty of DPA protection in realistic attacker scenarios.

Goals and Tasks

- Contact us for discussing possible topics and scope.
- Read literature to acquire the necessary background.
- Design/Implement/Attack/Protect/Verify.
- Write/Present your Master project/thesis.

Literature

- NIST
  Lightweight Cryptography - Round 2 Candidates
  https : / / csrc . nist . gov / Projects / lightweight - cryptography / round - 2 - candidates
- C. Dobraunig et al.
  ISAP Lightweight Authenticated Encryption
  https://isap.iaik.tugraz.at/

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, ...
- Writing thesis
- Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Interest in cryptography
- Interest in implementation security

Advisor / Contact

robert.primas@iaik.tugraz.at