A Machine-Checked Proof of Randomness Reuse in Masked Circuits

Advisor: **Roderick Bloem**

Motivation

Masking protects hardware against power side-channel attacks by splitting secrets into $d+1$ shares, and randomness is what it costs. Hadzic and Bloem show that several HPC3.1 multipliers sharing one input sharing may also share their blinding randomness without losing d-probe-isolating non-interference, glitches included. That saves about a fifth of the random bits of a masked AES inverter, but it is stated for concrete netlists at a fixed order and proved as a sketch.

We have a compiler in the Lean 4 proof assistant that masks circuits and proves the result PINI; HPC3.1 and its security proof are fully formalised in it. This thesis turns the sketch into a machine-checked theorem, generic in the protection order and in the field, so that the compiler can claim the saving with a proof behind it.

Goals and Tasks

- Understand PINI and the existing HPC3.1 security proof
- State the n-fold composition with shared randomness, generic in d and the field
- Machine-check that it is d-PINI, and prove the shared-input side condition necessary
- Certify the compiler's randomness saving end to end
- Stretch: extend the argument to the HPC3.2 gadget

Literature

- V. Hadzic and R. Bloem
  Efficient and Composable Masked AES S-Box Designs
  IACR TCHES 2025(1) 2025
  doi:10.46586/tches.v2025.i1.656-683
- G. Cassiers and F.-X. Standaert
  Trivially and Efficiently Composing Masked Gadgets with Probe Isolating Non-Interference
  IEEE Trans. Inf. Forensics Security 2020
  doi:10.1109/TIFS.2020.2971153

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 ☑ SEM

Prerequisites

- Probability and quantifiers
- Interest in theorem proving; Lean can be learned on the job

Advisor Contact

roderick.bloem@tugraz.at