Sharing Randomness Between Masked Multipliers

Advisor: **Roderick Bloem**

Motivation

Masking protects hardware against power side-channel attacks by splitting every secret into $d+1$ random shares. The price is randomness: every masked multiplier consumes fresh random bits, and in a masked AES S-box this dominates the cost. Several multipliers operating on a *common* input may safely share part of their randomness, which saves roughly a fifth of the random bits of a masked inverter.

We have a compiler that turns an ordinary circuit into a masked one, together with a mechanised proof in the Lean 4 proof assistant that its output is secure. It currently gives every multiplier its own fresh randomness and therefore cannot claim this saving. Your task is to teach it to share — and to prove that what it emits still computes the right thing.

Goals and Tasks

- Learn the basics of masking and of Lean 4 (no prior knowledge assumed)
- Add a batched multiplication $z_1 \dots z_n := \mathrm{mul}(a, b_1 \dots b_n)$ to the compiler's input language
- Emit n gadgets that share their blinding randomness and keep the rest per instance
- Prove in Lean that the batched construct is functionally correct
- Machine-check its security for small n and d, and measure how far that scales

Literature

- V. Hadzic and R. Bloem
  Efficient and Composable Masked AES S-Box Designs Using Optimized Inverters
  IACR TCHES 2025(1) 2025
  https://doi.org/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. Information Forensics and Security 2020
  https://eprint.iacr.org/2018/438

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Functional programming; Lean can be learned on the job
- Enjoys proofs; no background in side channels required