Composing Masked Gadgets in the Presence of Transitions

Advisor: **Roderick Bloem**

Motivation

Masked circuits are built from gadgets that are secure in isolation and composed without further analysis. That is what PINI buys. We have a masking compiler with a mechanised PINI proof in Lean 4, in the glitch-extended probing model. Transitions — a register leaking a function of its old and new contents — break trivial composition, and repairing it takes a stronger notion, O-PINI, together with its own composition theorem.

This thesis supplies both, machine-checked: the definition, the theorem that O-PINI gadgets compose under transitions, and at least one gadget of the development shown to satisfy it. The result extends the compiler's guarantee from one physical defect to two.

Goals and Tasks

- Understand PINI, the robust probing model and the existing composition proof
- Define O-PINI and transition-robustness in the development's framework
- Prove the composition theorem for O-PINI gadgets, generic in *d*
- Show a gadget of the library O-PINI, and see what the compiler must emit
- Stretch: relate the notion to couplings, the third physical defect

Literature

- G. Cassiers and F.-X. Standaert
  Composing Masked Gadgets with Probe Isolating Non-Interference
  IEEE Trans. Inf. Forensics Security 2020
  doi:10.1109/TIFS.2020.2971153
- G. Cassiers and F.-X. Standaert
  Provably Secure Hardware Masking in the Transition- and Glitch-Robust Probing Model: Better Safe than Sorry
  IACR TCHES 2021(2) 2021
  doi:10.46586/tches.v2021.i2.136-158

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