



Where Masking Proofs Stop: Transitions

Advisor: **Roderick Bloem**

Motivation

Masking protects hardware against power side-channel attacks by splitting every secret into $d + 1$ shares. Its great convenience is composition: build gadgets that are secure on their own, wire them together, and the whole circuit is secure — no further analysis needed. That guarantee holds in a model of the hardware that accounts for glitches.

Real hardware also leaks on *transitions*: a register that goes from one value to another leaks something about both. We have a compiler that masks circuits automatically, together with a mechanised proof in Lean 4 that its output is secure — but only against glitches. Why it stops there is currently a sentence of prose. Your job is to turn that sentence into a theorem: two gadgets, each secure by itself, whose composition leaks as soon as an attacker sees transitions.

Goals and Tasks

-  Learn the probing model and the composition notion the development uses
-  Formalise the transition-extended attacker and the stronger security notion (O-PINI)
-  Build a small, concrete counterexample and machine-check that it leaks
-  Report what the counterexample shows and what it does not

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

- ☒ **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

- > Likes definitions and counterexamples
- > Lean can be learned on the job; no side-channel background needed

Advisor Contact

roderick.bloem@tugraz.at