



# Fuzzing a Verified Compiler's Blind Spot

Advisor: **Roderick Bloem**

## Motivation

We have a compiler that protects circuits against power side-channel attacks, and a mechanised proof in Lean 4 that its output is secure. The proof is about data structures inside the compiler. What the compiler hands you is a text file — and the claim that this text describes the circuit the proof is about is trusted, not proven.

That is where the bugs live. Three were found by hand in a single week: wire names decoded arithmetically instead of looked up, every unrecognised gate silently resolving to the same one, and share names concatenated so that two different wires ended up with the same name. Each of them parsed cleanly, ran fine, and computed the wrong function. Nobody is testing this layer. You will.

## Goals and Tasks

- ✂ Write your own evaluator for the circuit format, in the language you are fastest in
- ✂ Generate random circuits and push them through the pipeline: mask, print, read back
- 💡 Compare both sides, shrink every disagreement to a small example, and report the bugs
- 💡 Stretch: simulate power traces of the emitted circuit and run a first-order leakage test

## Literature

- > [X. Yang et al.](#)  
Finding and Understanding Bugs in C Compilers  
PLDI 2011  
[doi:10.1145/1993498.1993532](https://doi.org/10.1145/1993498.1993532)
- > [K. Claessen and J. Hughes](#)  
QuickCheck: A Lightweight Tool for Random Testing of Haskell Programs  
ICFP 2000  
[doi:10.1145/351240.351266](https://doi.org/10.1145/351240.351266)

## 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

- > A strong programmer, in any language
- > No proofs, no Lean, no side-channel background needed

## Advisor Contact

[roderick.bloem@tugraz.at](mailto:roderick.bloem@tugraz.at)