An SMT Model of the OTBN Instruction Set

Advisor: **Roderick Bloem**

Motivation

OpenTitan's ECC and RSA implementations are written in assembly for OTBN, a RISC-V core with 256-bit integer instructions. We want tools that reason about such code automatically — for instance to find places where a secret becomes visible in a power trace. Any such tool needs one thing first: a description of what each OTBN instruction does, written as logical formulas a solver can work with.

Your job is to write that description and, more importantly, to show that it is right. Wide arithmetic, carry flags and the two register files leave plenty of room for a model that looks plausible and quietly disagrees with the hardware.

Goals and Tasks

- Get to know the OTBN instruction set and bit-vector reasoning with a solver
- Translate straight-line OTBN assembly into SMT formulas, instruction by instruction
- Build a test harness: run a block on the simulator, evaluate the formula, compare
- Report which instructions are modelled, which are validated, and what is abstracted

Literature

- L. de Moura and N. Bjørner
  Z3: An Efficient SMT Solver
  TACAS 2008
  doi:10.1007/978-3-540-78800-3_24
- lowRISC
  OpenTitan Big Number Accelerator (OTBN)
  https://opentitan.org/book/hw/ip/otbn/

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

- Solid Python, some assembly
- Care for detail; no background in verification needed

Advisor Contact

roderick.bloem@tugraz.at