Build a DOM Circuit Compiler

Advisor: **Vedad Hadžić**

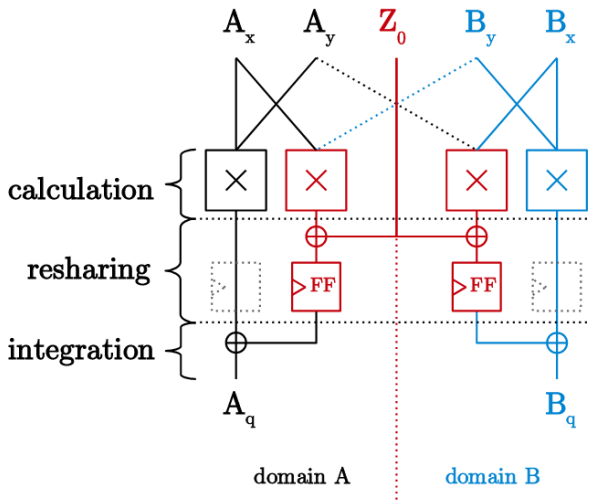
Motivation

Power analysis side-channel attacks are a serious threat to embedded devices. An attacker could monitor the power consumption during cryptographic operations and recover the keys. A popular strategy to mitigate these issues is to make the computations independent from the secret data through masking.

Traditionally, masking schemes are manually implemented by a hardware designer. We have developed a tool that can check whether the produced circuits are secure. We want to have an automatic circuit compiler that takes a simple circuit, applies a known masking scheme like DOM or TI, and produces the masked circuit. Additionally, our tool could then be used for optimizations of the generated circuits.

Goals and Tasks

- Become familiar with TI and DOM
- Parse Verilog or VHDL circuits with Yosys
- Apply a masking scheme to the netlist
- Convert netlist back to Verilog or VHDL
- Check the security of the circuit using Rebecca



Literature

- H. Groß, S. Mangard, and T. Korak
  Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order
- S. Nikova, C. Rechberger, and V. Rijmen
  Threshold Implementations Against Side-Channel Attacks and Glitches
- R. Bloem et al.
  Formal Verification of Masked Hardware Implementations in the Presence of Glitches

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

- Good knowledge of Python, Verilog
- Understanding of graphs and logic circuits

Advisor / Contact

vedad.hadzic@iaik.tugraz.at