Project VE-HEP, poster presented at: Tag der vertrauenswürdigen Elektronik 2023, May 2023

Evaluating an Open-Source EDA Toolchain

GOALS

- Open Source Hardware Security Module
  (HSRM, SIT, IHP)
- Semi-automated hardening against power side-channel attacks
  (RUB)
- Formally verified RISC-V core and security extension
  (DFKI)
- Hardware weak spots, e.g., scan chain
  (TUB)
- Automotive demonstrator (IAV, EB)

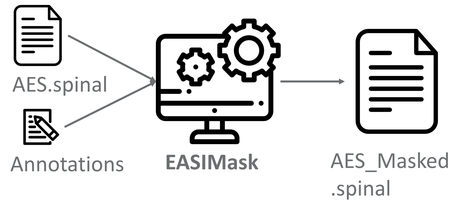
Tool-Chain

- Spinal HDL
- OpenRoad
- KLayout
- Interoperability with Cadence tool chain works perfectly
- Scan chain insertion done with Cadence
- DRC & LVS done in Cadence
- First try no LVS errors
- Two tapeouts done

Verification

- $State\_(N+1)=FS(State\_N, Input)$
- $Output=FO\ (State\_N, Input)$
- 16 Cycles – 9 Startup/7 Instruction (75h)
- Find illegal instructions
- 37 Base-instructions
- Correct arithmetic of ALU
- Read and write of registers
- Correct functioning of PC
- Correct interaction with memory

Security extension



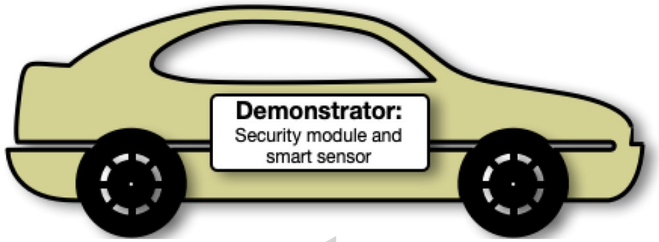
- AES words with 32 bits (plaintext + key)
- Round-based implementation
- FPGA implementation: 1st order secure

OUTLOOK

- IHP Open Source PDK to fill European open source flow gap
- Electrical functionality evaluation (waiting for silicon)
- Demonstrator setup partly started
- Evaluate risk of found weak spots in the scan chain
- Develop open IHP PDK-based SRAM cell

Hochschule RheinMain
University of Applied Sciences
Wiesbaden Rüsselsheim Geisenheim

Fraunhofer SIT



Elektrobit

automotive engineering iav

… to IHP fab.

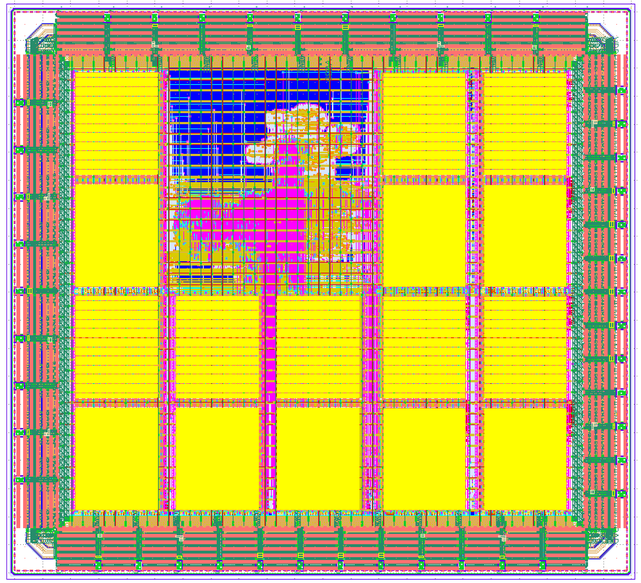
… via OpenRoad …

From SpinalHDL …

berlin

RUB

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH



Förderungsnummer:
16KIS1339K
Slide edited Sept. 2023

SPONSORED BY THE
Federal Ministry of Education and Research

Leibniz Association