An in-hardware cycle-accurate benchmarking tool for security critical operations

Julian Pritzi
Advisors: Prof. Pramod Bhatotia,
Harshavardhan Unnibhavi
Chair of Decentralized Systems Engineering
https://dse.in.tum.de/

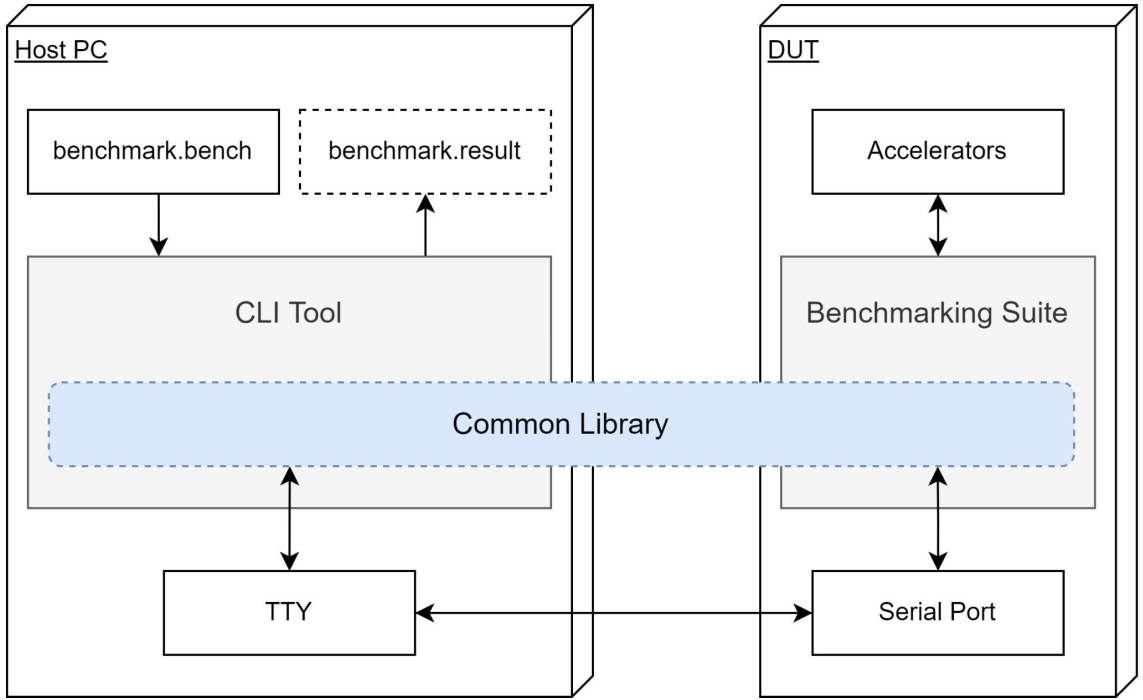
15.04.2022 – 15.08.2022

Introduction

- Opentitan: Open source silicon root of trust
- Composition of components to create new platforms
- Performance analysis: simulation vs in hardware

Benchmarking Tool for a general 32bit RISC-V platform.

Design


Host PC
benchmark.bench
benchmark.result
CLI Tool
Common Library
TTY
DUT
Accelerators
Benchmarking Suite
Serial Port

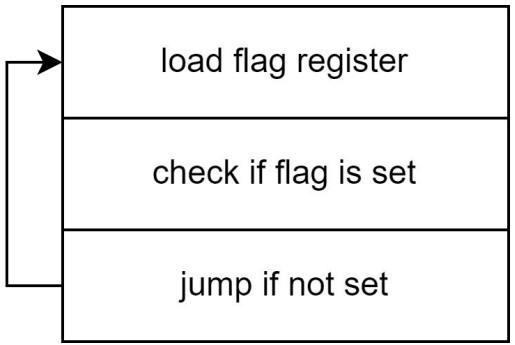
Opentitan - Earl Grey

- RISC-V 32bit Ibex CPU
- earlgrey_silver_v5

Hardware IP Core	Functionality
HMAC	SHA2 Hashing
KMAC	SHA3 Hashing
CSRNG	Random Number Generation
AES	AES Encryption

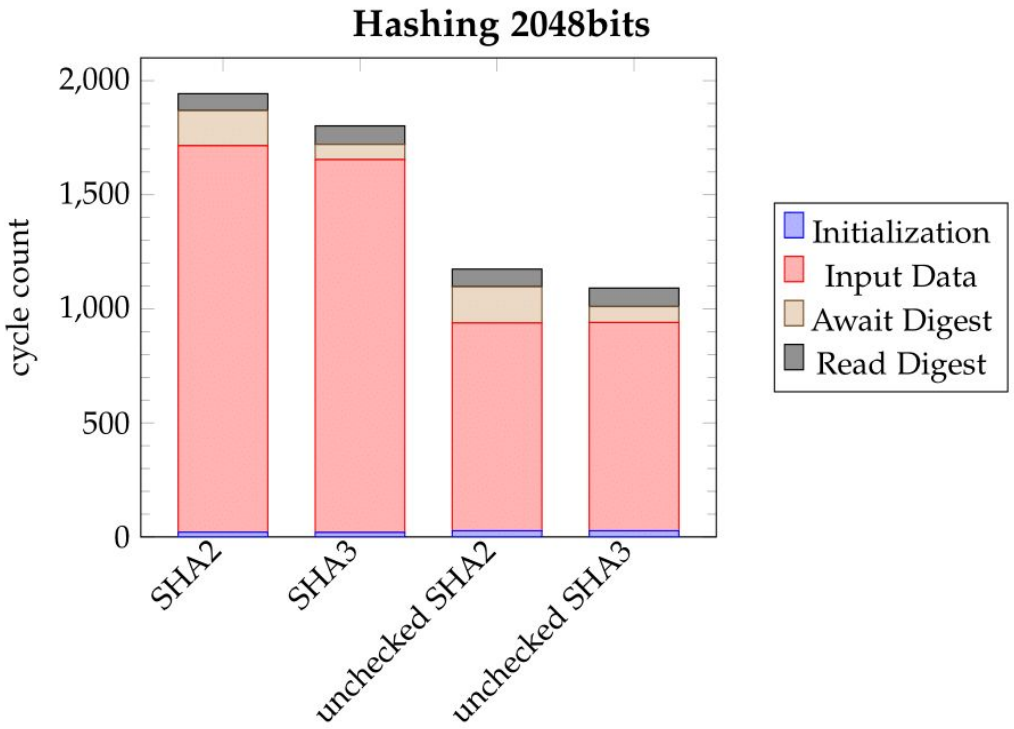
Hashing - Implementation

1. Initialize Accelerator
2. For each 32bit block:
    a. **Wait for** input queue
    b. Insert Block
3. **Wait for** completion
4. Read Digest

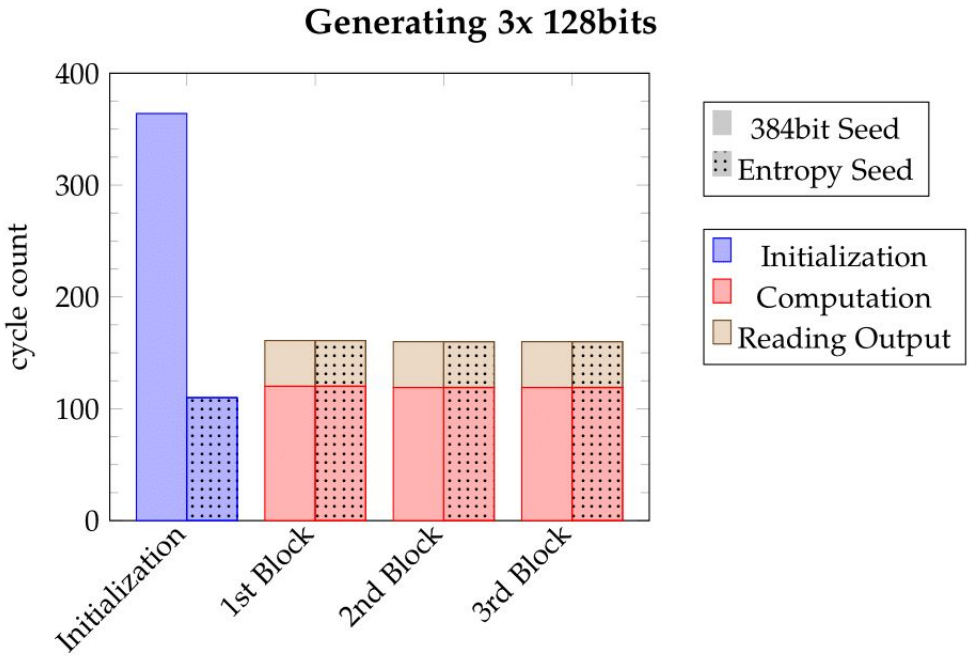


“Wait for”-Logic, ≥6 cycles on Ibex

Hashing - Evaluation

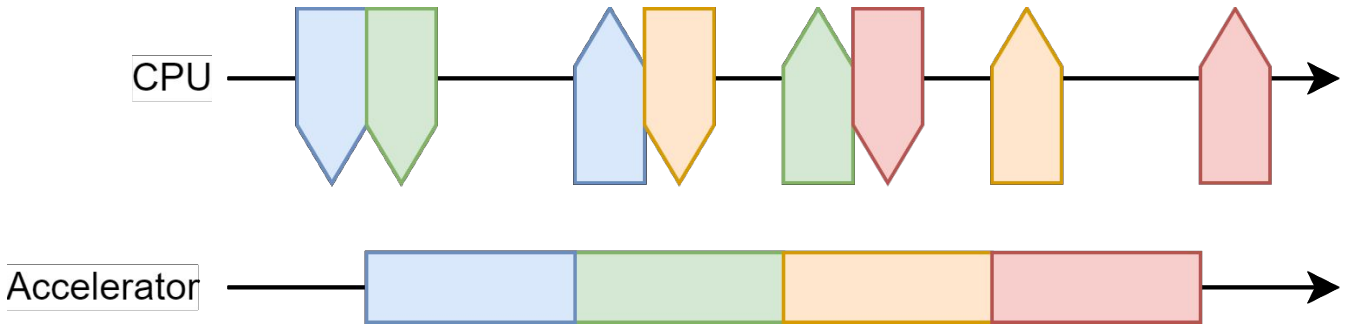


RNG - Evaluation

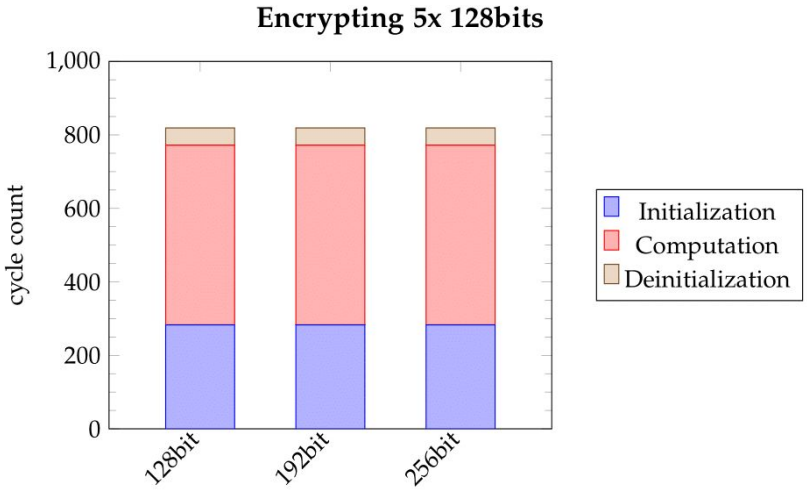


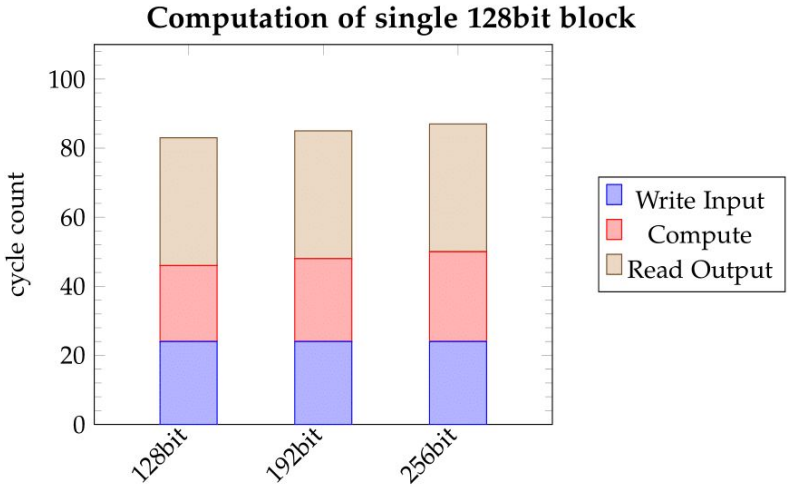
AES - Implementation

- Initialization configures mode, operation, key, …
- Blockwise encryption:

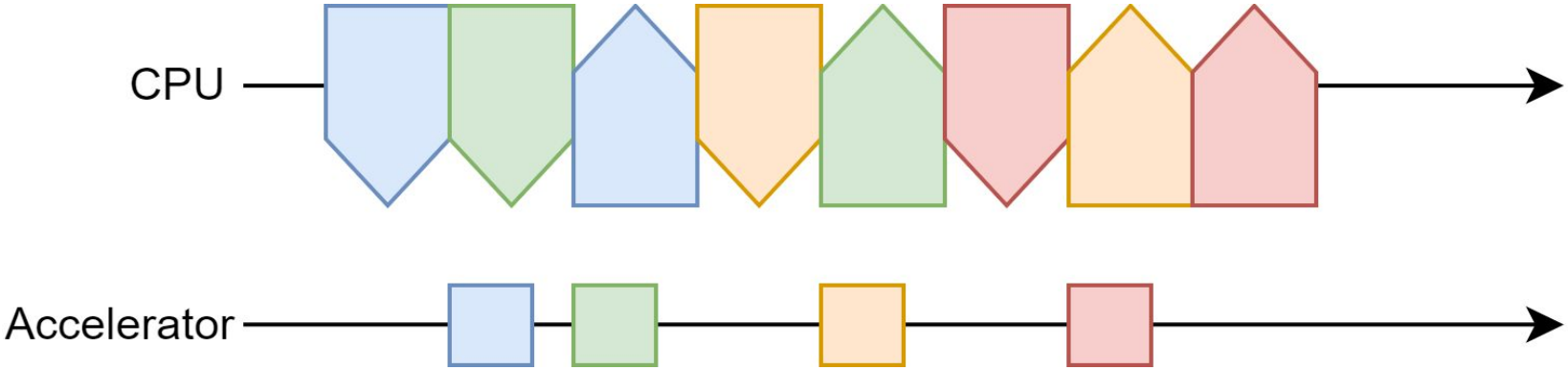


AES - Evaluation





AES - Evaluation



Conclusion

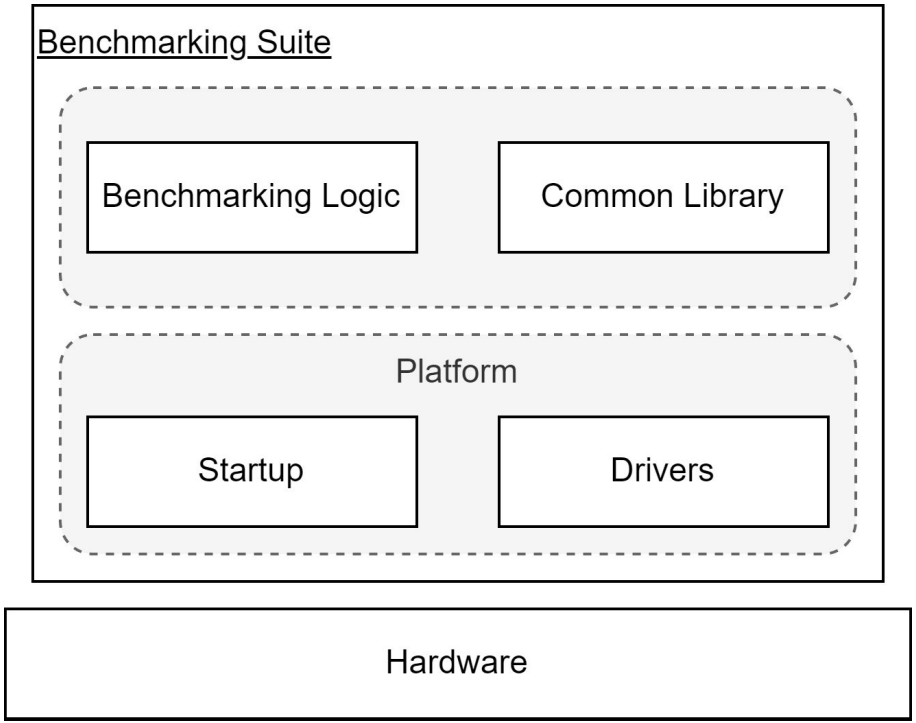
CPU read/writes and “Wait for” loops significantly impact performance.

Future Work

- Opentitan Big Number Accelerator
- Masked vs. Unmasked
- Newest Opentitan Version

Backup

Design - Benchmarking Suite



Ibex Core - Changes