

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

Julian Pritzi

Advisor: Harshavardhan Unnibhavi

Chair of Decentralized Systems Engineering

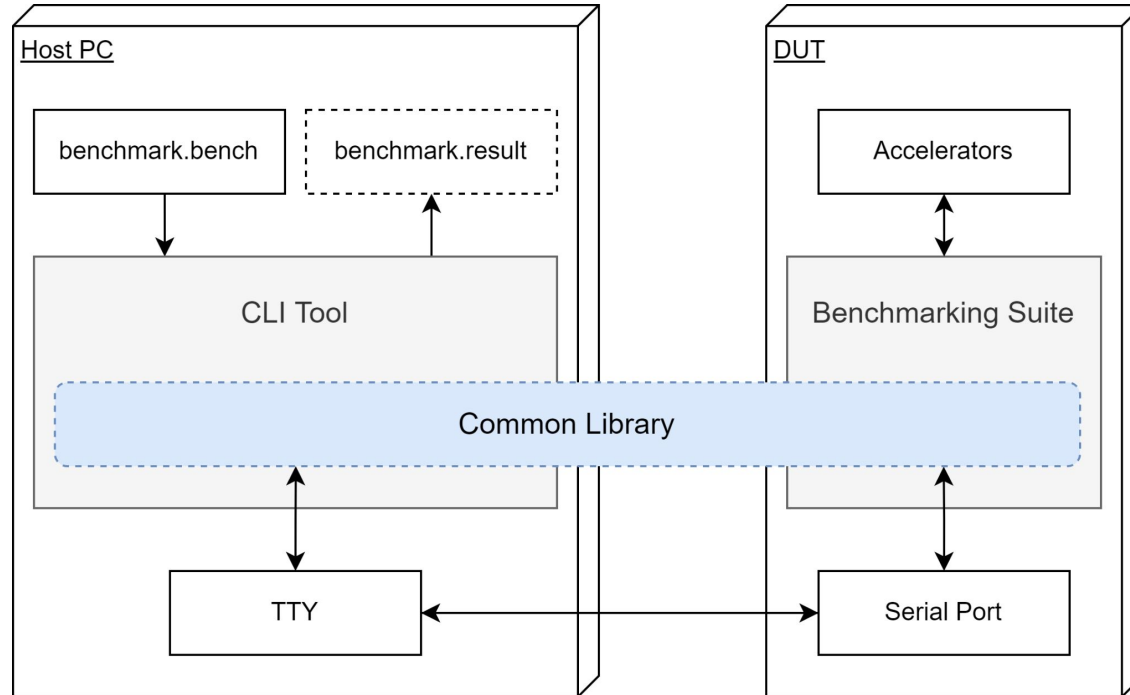
<https://dse.in.tum.de/>



15.04.2022 – 15.08.2022

- 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.

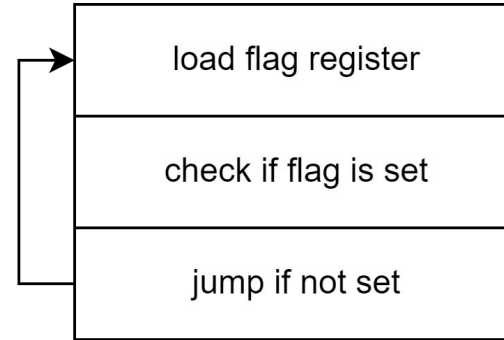


- RISC-V 32bit Ibex CPU
- earlgrey_silver_v5

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

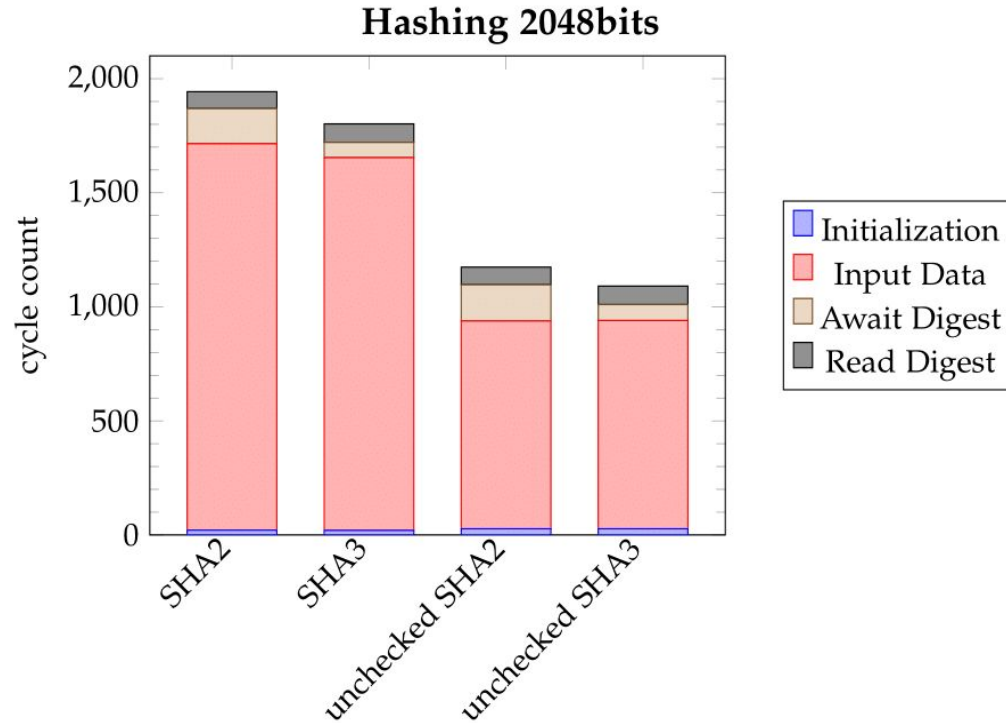
Hashing - Implementation

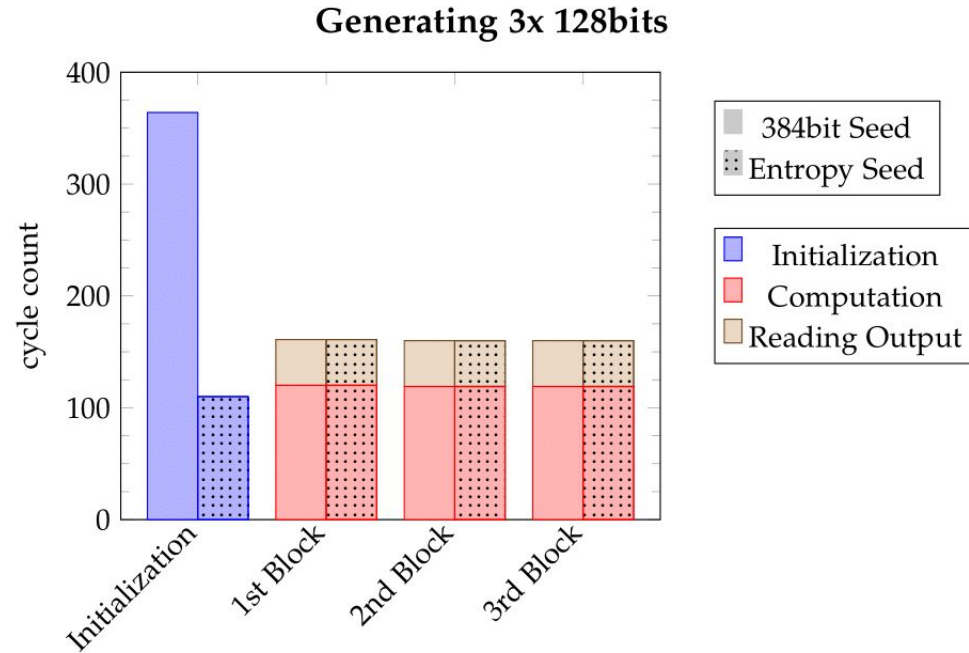
1. Initialize Accelerator
2. For each 32bit block:
 - a. **Wait for** input queue
 - b. Insert Block
3. **Wait for** completion
4. Read Digest



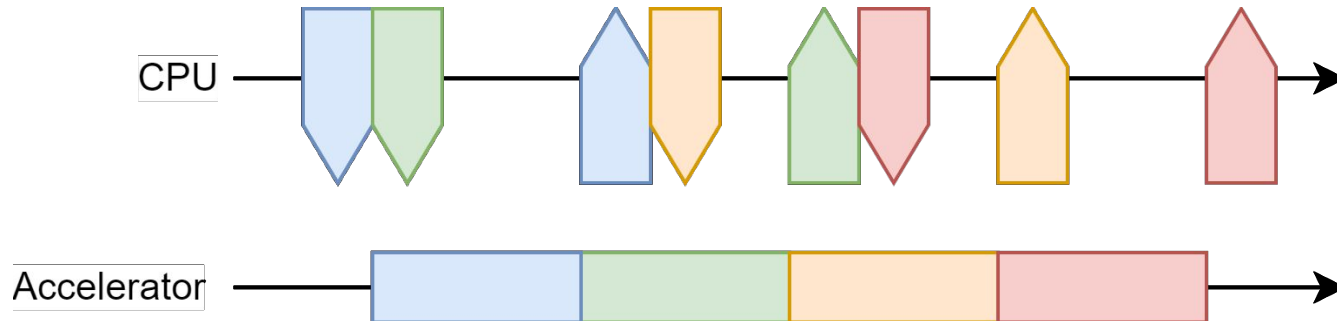
“Wait for”-Logic, ≥ 6 cycles on Ibex

Hashing - Evaluation

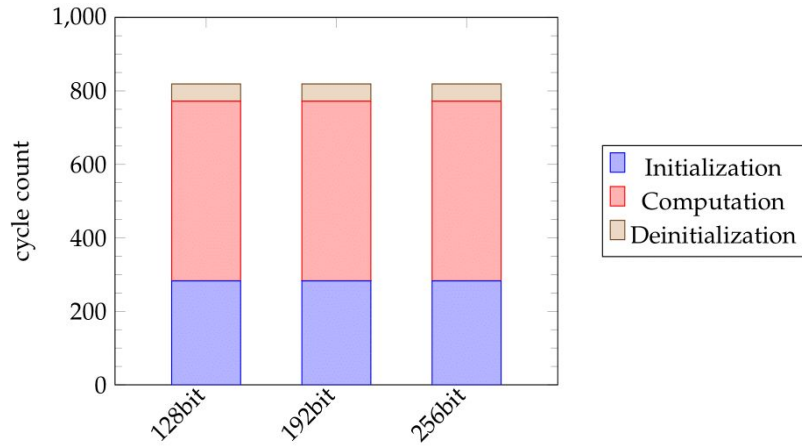




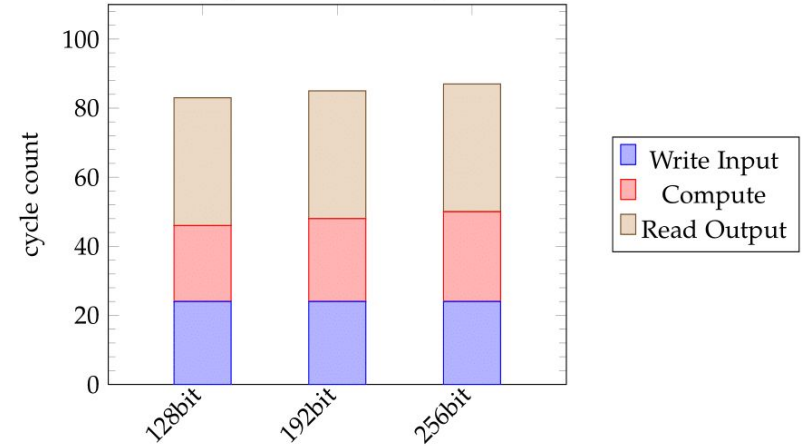
- Initialization configures mode, operation, key, ...
- Blockwise encryption:

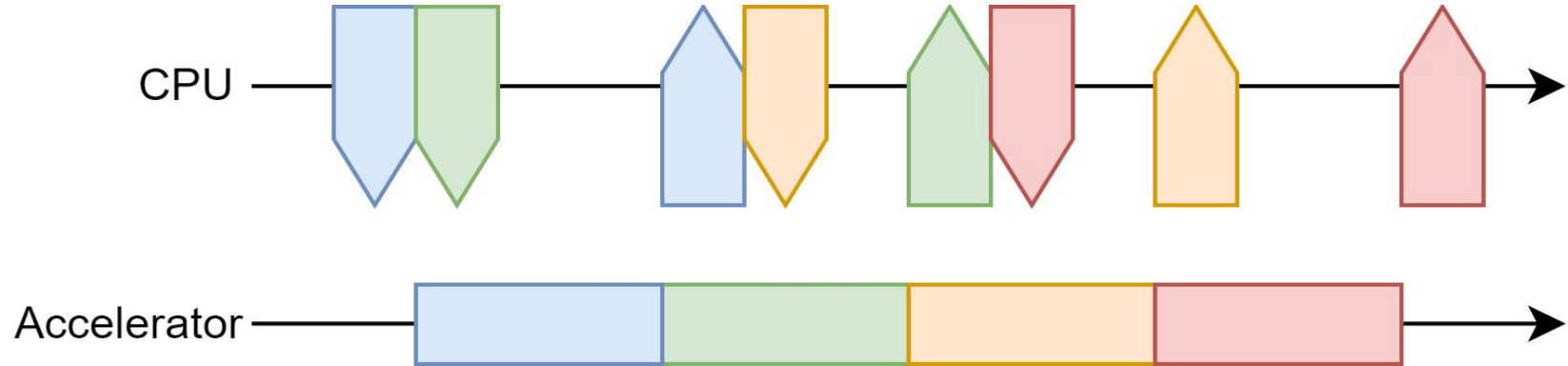


Encrypting 5x 128bits



Computation of single 128bit block

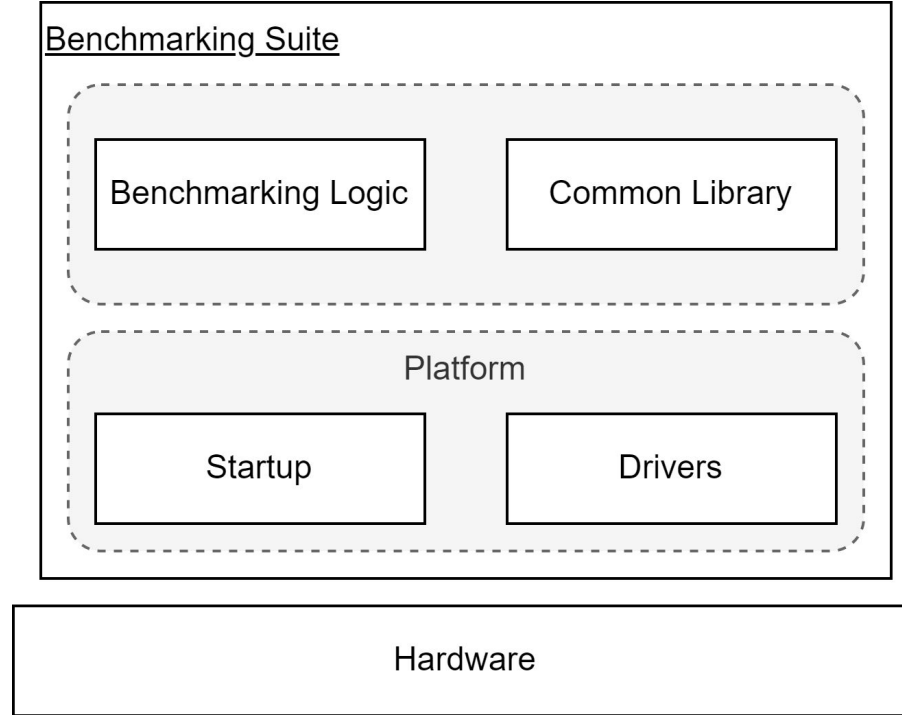




CPU read/writes and “Wait for” loops significantly impact performance.

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

Backup



Ibex Core - Changes

