Radboud University

Plan your defense: A comparative analysis of leakage detection methods on RISC-V cores

Konstantina Miteloudi Asmita Adhikary Niels van Drueten Lejla Batina Ileana Buhan

July 3, 2024

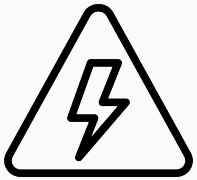
Introduction

- Microprocessors are vital in modern digital systems.
  - From consumer electronics to critical infrastructure.
- Their security is crucial to protect against various forms of attacks.
  - We focus on side-channel attacks.
- First step to enhance the security of RISC-V cores.
  - Assess the leakage:
    - Side-channel Vulnerability Factor (SVF)
    - Test Vector Leakage Assessment (TVLA)
- Our contribution:
  - A comparative analysis of SVF and TVLA
    - on SHAKTI and Ibex RISC-V cores running AES and SHA-3.

Side-Channel Analysis (SCA)

Most common side channel resources:

Power

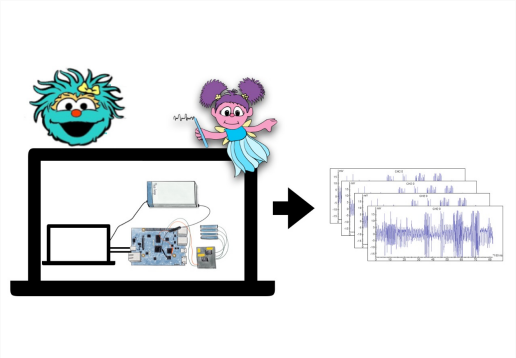


Timing

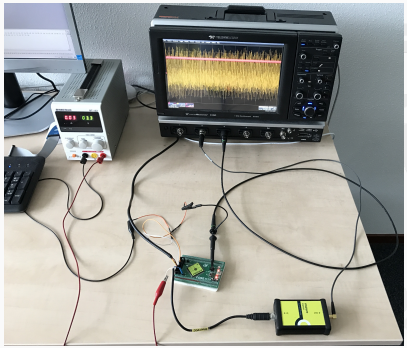
EM emissions

Simulation versus Real measurements

- Simulation
  - pre-silicon analysis
  - reduced cost, very time demanding



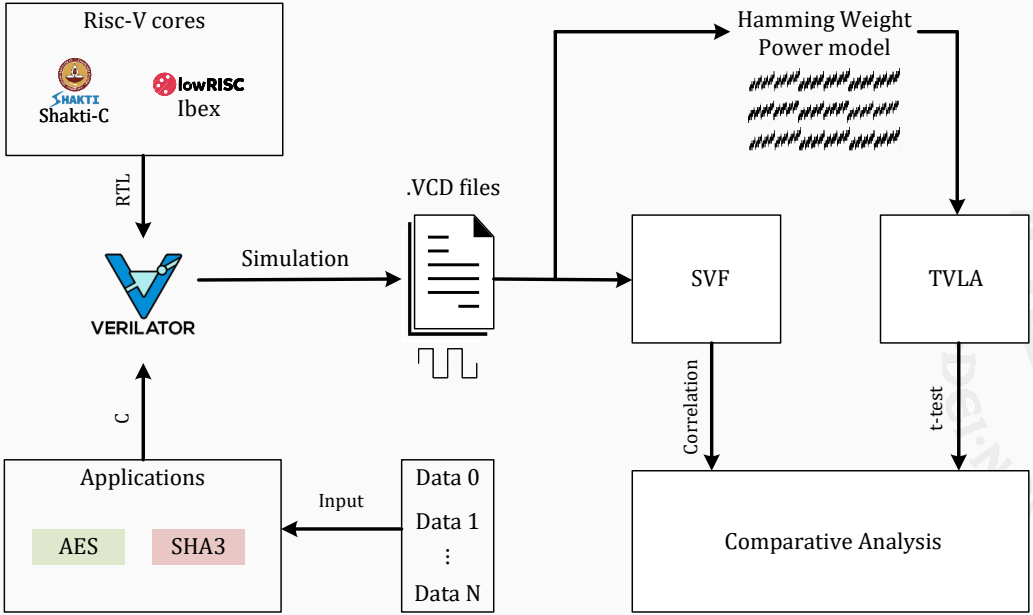
- Measurements
  - post-silicon analysis
  - dedicate equipment, real behavior



Some approaches in the literature

- Pre-silicon and simulation:
  - A V Lakshmy, Chester Rebeiro, and Swarup Bhunia. **"FORTIFY: Analytical Pre-Silicon Side-Channel Characterization of Digital Designs".** In: *ASP-DAC*. 2022, pp. 660–665. DOI: 10.1109/ASP-DAC52403.2022.9712551
- Side channel metrics based on measurements:
  - Kostas Papagiannopoulos et al. **"The Side-channel Metrics Cheat Sheet".** In: *ACM Comput. Surv.* 55.10 (2023). DOI: 10.1145/3565571
- Hybrid approach use information from pre-silicon to model better the post- assessment:
  - Dillibabu Shanmugam and Patrick Schaumont. **"Improving Side-channel Leakage Assessment Using Pre-silicon Leakage Models".** In: *Constructive Side-Channel Analysis and Secure Design*. Springer Nature Switzerland, 2023, pp. 105–124. DOI: 10.1007/978-3-031-29497-6_6

Framework


Risc-V cores
Shakti-C
lowRISC
Ibex
RTL
VERILATOR
Simulation
.VCD files
Hamming Weight
Power model
SVF
TVLA
Correlation
t-test
C
Applications
AES
SHA3
Input
Data 0
Data 1
⋮
Data N
Comparative Analysis

TVLA

TVLA computation

- Fixed versus random test
- Simulated executions
- Hypothetical power consumption model:
  - Hamming Weight (HW)
- Calculation of traces:
  - HW for every timestamp
- Size of random set:
  - N = 128 for SHAKTI
  - N = 256 for Ibex

.

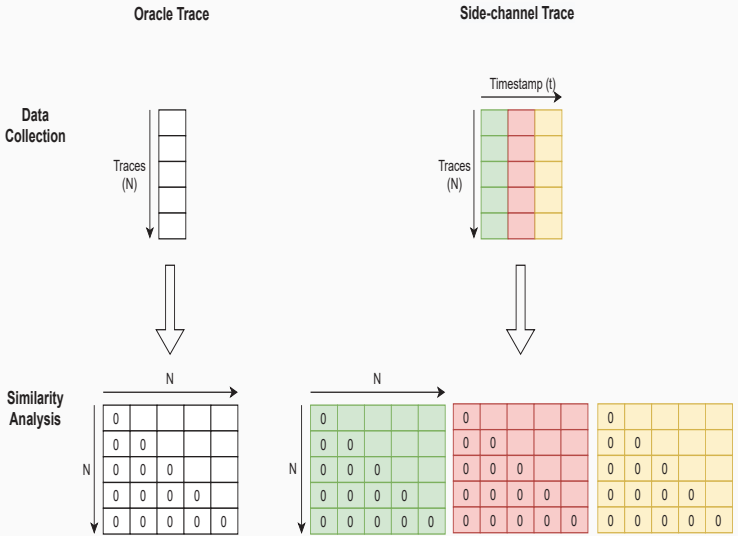
The t-test statistic is computed as follows:

$$\frac{\mu_A - \mu_B}{\sqrt{\frac{\sigma_A^2}{N_A} + \frac{\sigma_B^2}{N_B}}}$$

where:

- μ the average of the traces,
- σ the standard deviation, and
- N the number of traces.

SVF similarity phase



Similarity matrix $M^{\mathcal{O}}_{\text{input}}$ for the Oracle:

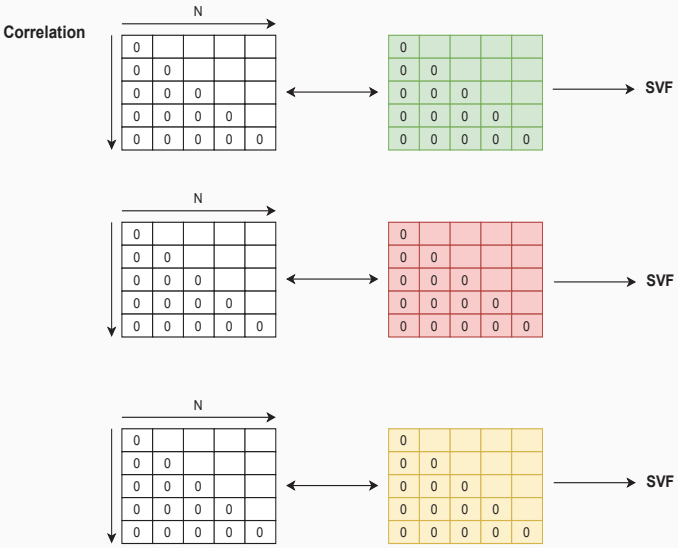
$$M^{\mathcal{O}}_{\text{input}}(o^i_t, o^j_t) = \begin{cases} \tilde{D}(o^i_t; o^j_t), & \text{if } i < j \\ 0, & \text{if not.} \end{cases}$$

and similarity matrix $M^{\mathcal{S}}_{\text{input}}$ for every simulated trace:

$$M^{\mathcal{S}}_{\text{input}}(s^i_t, s^j_t) = \begin{cases} \bar{D}(s^i_t, s^j_t), & \text{if } i < j \\ 0, & \text{if not.} \end{cases}$$

where $\bar{D}$ is the Hamming distance and zeros are omitted.

SVF correlation phase



For every pair of traces Oracle and Side-channel, the Pearson correlation coefficient is calculated in absolute terms:

$$SVF_t = \mid \rho(\tilde{D}_o, \bar{D}_{s,t}) \mid$$

and if we want SVF for the module:

$$SVF_{\text{module}} = \max(SVF)$$

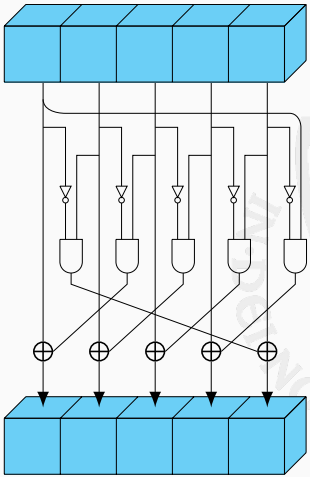
Four classes of leakage:

- 0.0 - 0.1: No leakage.
- 0.1 - 0.3: Mild leakage.
- 0.3 - 0.6: Medium leakage.
- 0.6 - 1.0: Severe leakage.

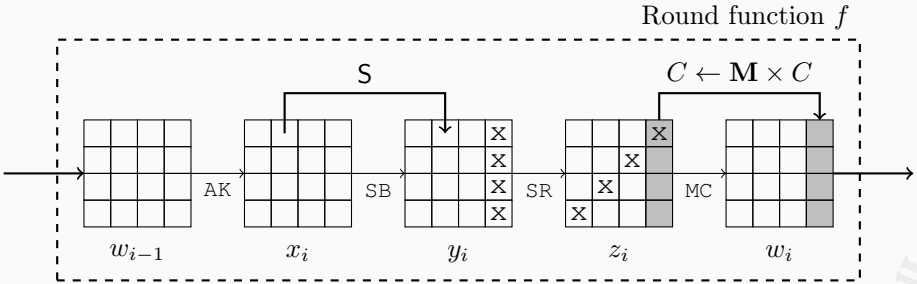
SHA3(Keccak-f) intermediate values

- For SHA-3 we target the operations:
  - In the non-linear χ step:
    - *xor* operation
    - *not* operation
  - and *bc*, implementation-specific operation
    - $bc[i] = st[j + i]$, where $i = 0$ and $j = 0$.

- step χ



AES intermediate values

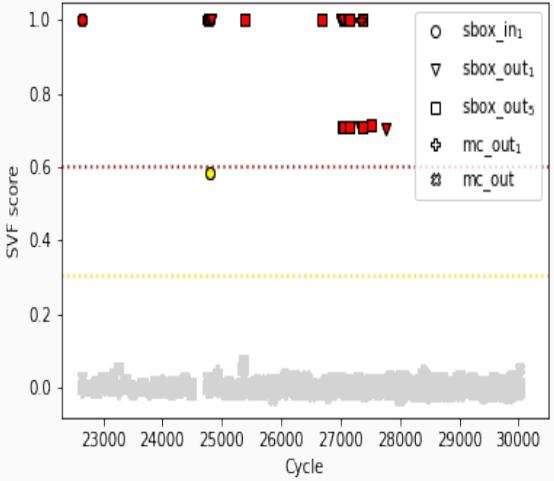


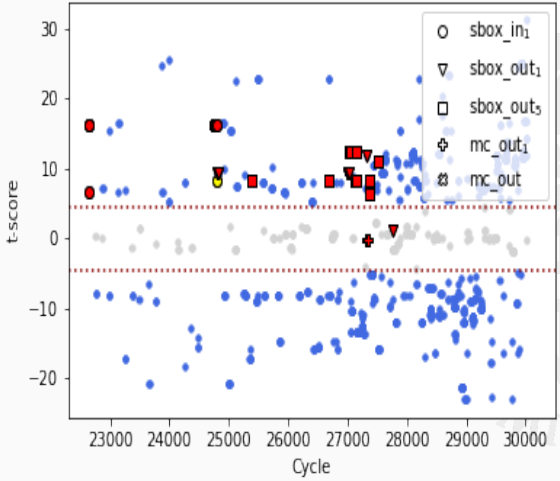
- For AES we target:
  - the first byte of the S-box output,
  - the full round output,
  - the first byte of the round output.

- AES byte ordering

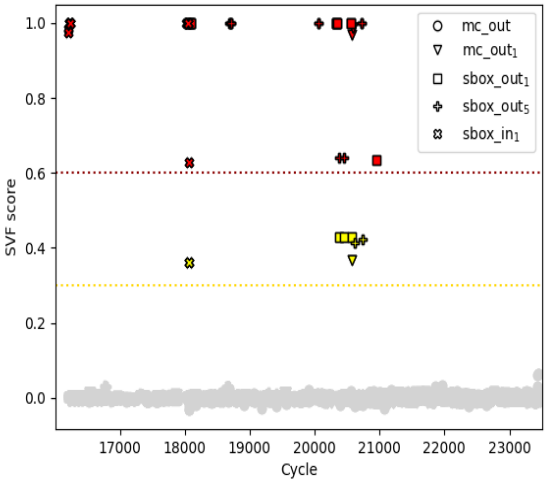
0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

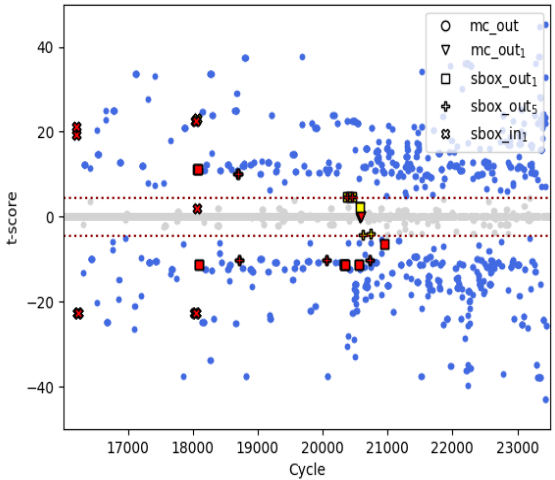
Results AES/ALU/Shakti



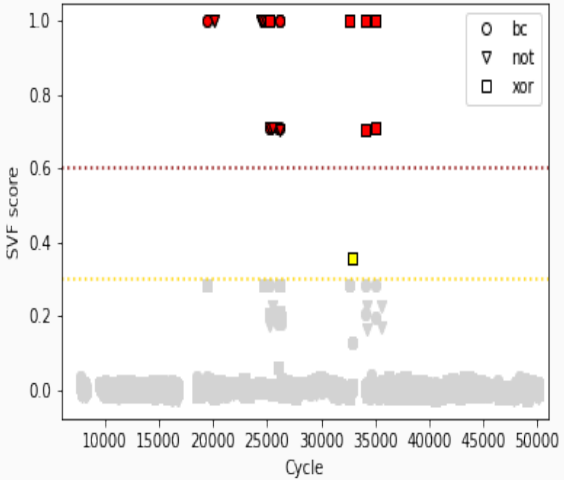


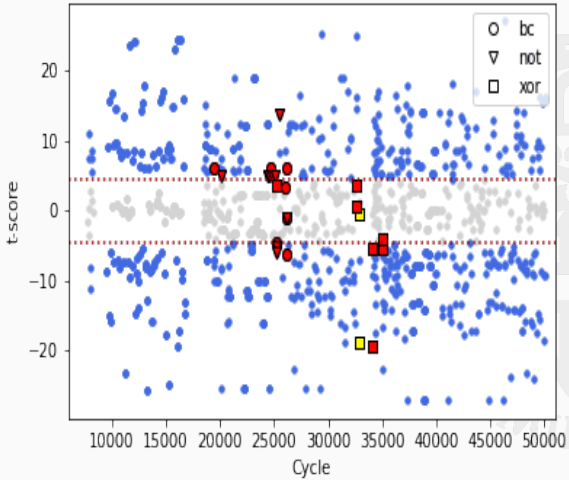
Results AES/ALU/Ibex



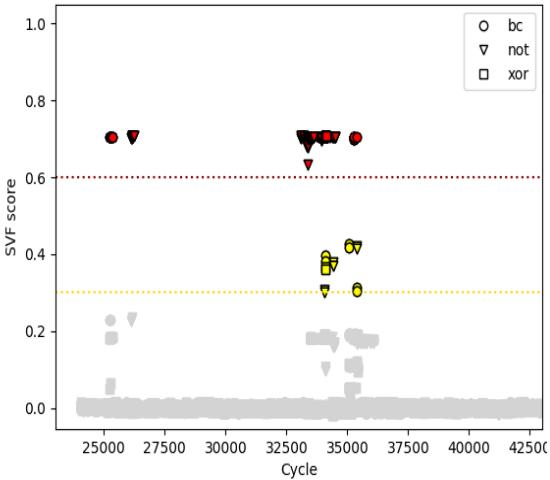


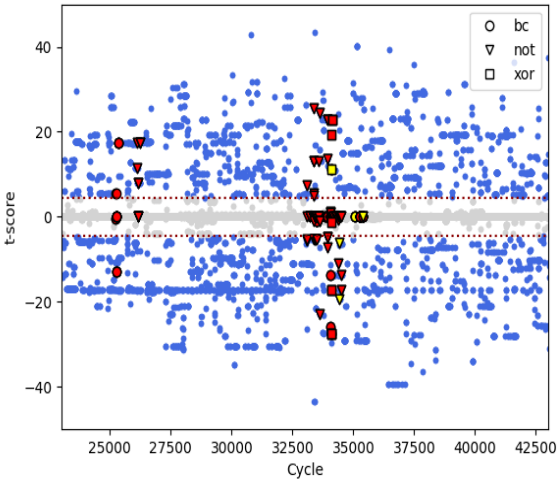
Results SHA3/ALU/Shakti





Results SHA3/ALU/Ibex





Thank you!