Quantitative Assessment of Power Side-channel Vulnerability at Pre-silicon Stages

Md Kawser Bepary, Dipayan Saha, Sukanta Dey, Fahim Rahman, Farimah Farahmandi, Mark Tehranipoor

Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611

Email: {mdkawser.bepary, dsaha, sukanta.dey} @ufl.edu, {fahimrahman, farimah, tehranipoor} @ece.ufl.edu

Background

- Power side-channel (PSC) analysis is a powerful technique to extract the secret key from hardware implementations.
- Utilizes silicon power traces of a device when the crypto engine is operational
- Threat model assumes the attacker has physical access to the device and knowledge of the algorithm

Motivation

Traditional power side-channel vulnerability assessment frameworks-

- Rely on post-silicon traces, too late to make design changes
- Information leakage is a black box for designers
- Lacks quantifiable metric for side-channel vulnerability analysis
- Lack of design flexibility, and high cost/time of applying countermeasures

RTL-PAT

Objective:

- Evaluate the PSC vulnerability of a design at the register-transfer level (RTL)
- Intended to help designers find vulnerable designs and leaky submodules with ease
- Model power consumption in early design stage i.e., RTL
- Develop proper metrics to quantify side-channel vulnerability

OVERVIEW OF THE FRAMEWORK

- RTL design is simulated for two sets of input vectors
  - Key1 vs Key2 (Max HD) with fixed random plaintext set
- Estimated power trace is computed as the hamming weight or switching activity of the registers for each clock cycle and submodule
- Two kinds of metric is used in a conformance-style
  - Test vector leakage assessment (TVLA)
  - Kullback-Leibler (KL) Divergence

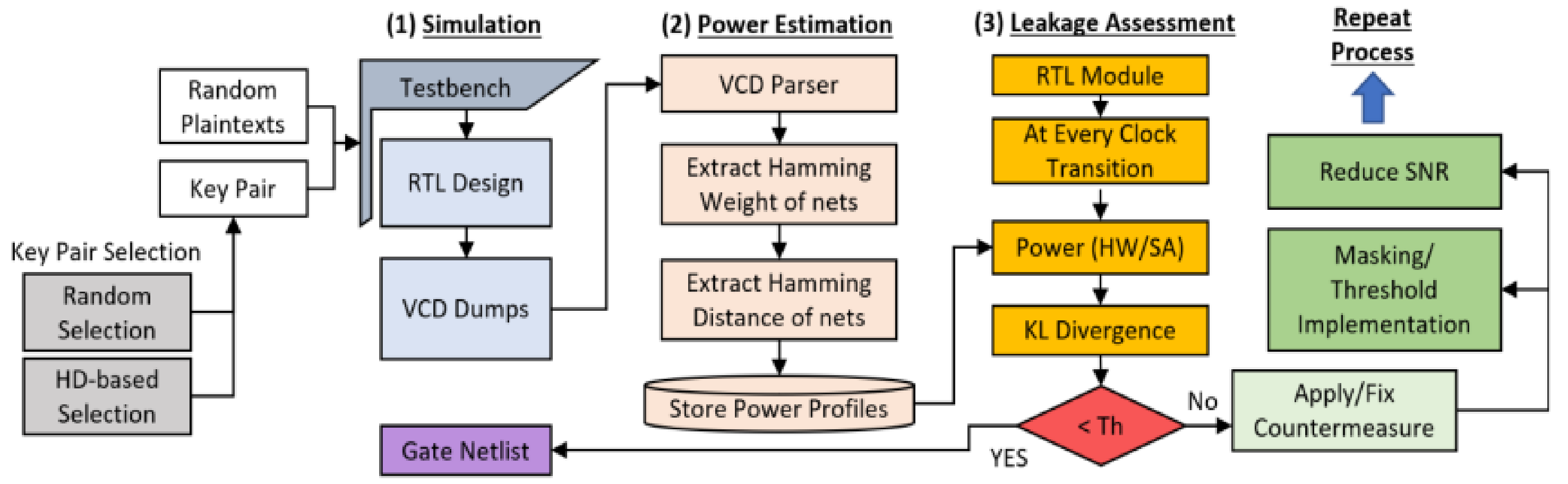


Figure 1: PSC Leakage assessment framework (RTL-PAT) workflow [1]

Security Metrics

- **TVLA:** $|t - value| \geq 4.5 \rightarrow Leaky\ Design$
Only Pass/Fail Test
- **KL Divergence:** Correlated to adversary's *failure probability*
→ Probability of incorrect inference based on PSC attack

EXPERIMENTAL RESULTS

- Module and submodule level leakage analysis of AES designs with KL divergence and TVLA metric

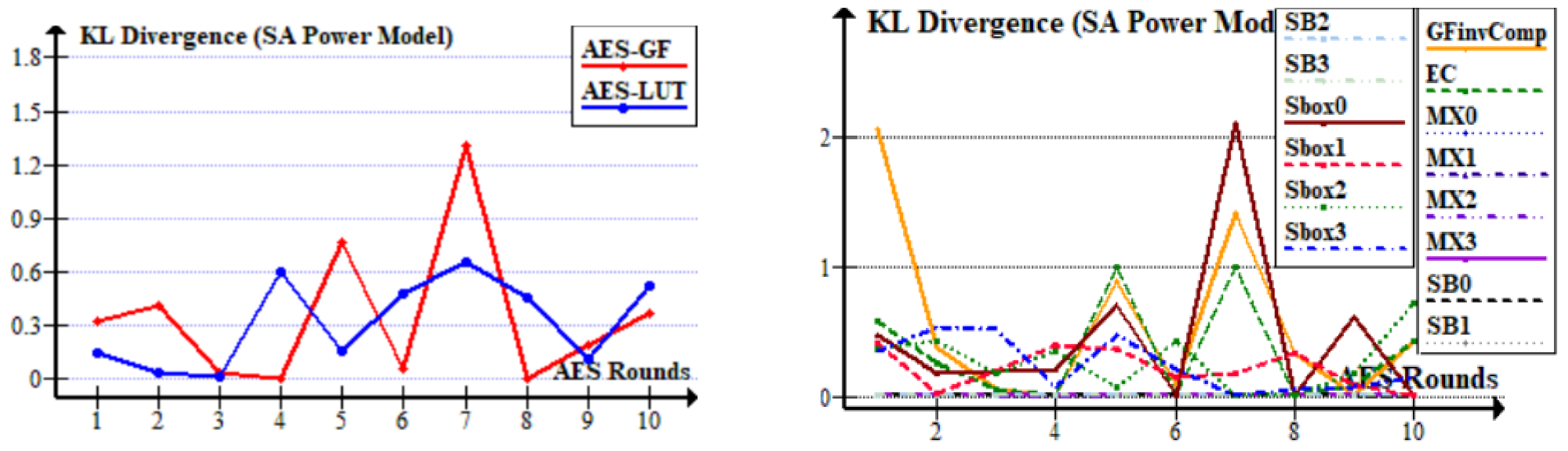


Figure 2: (a) Module level KL divergence for AES-GF and AES-LUT designs, (b) Submodule level KL divergence for AES-GF

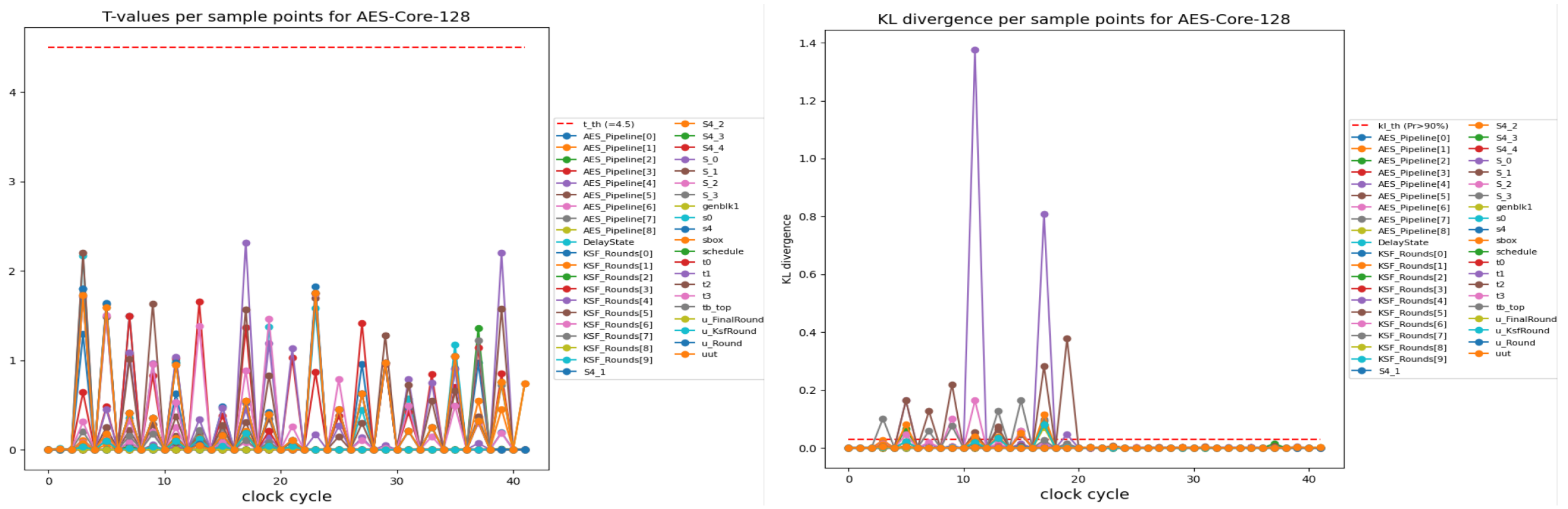


Figure 3: Submodule level (a) T-values and (b) KL divergence for a custom AES-128 design

SoC-PAT

Objective:

- Evaluate the PSC vulnerability of an SoC design with AES engine at RTL
- Quantify the impact (additional noise) of integration parameters (parallel activity, shared power distribution network, etc.) on security metrics.

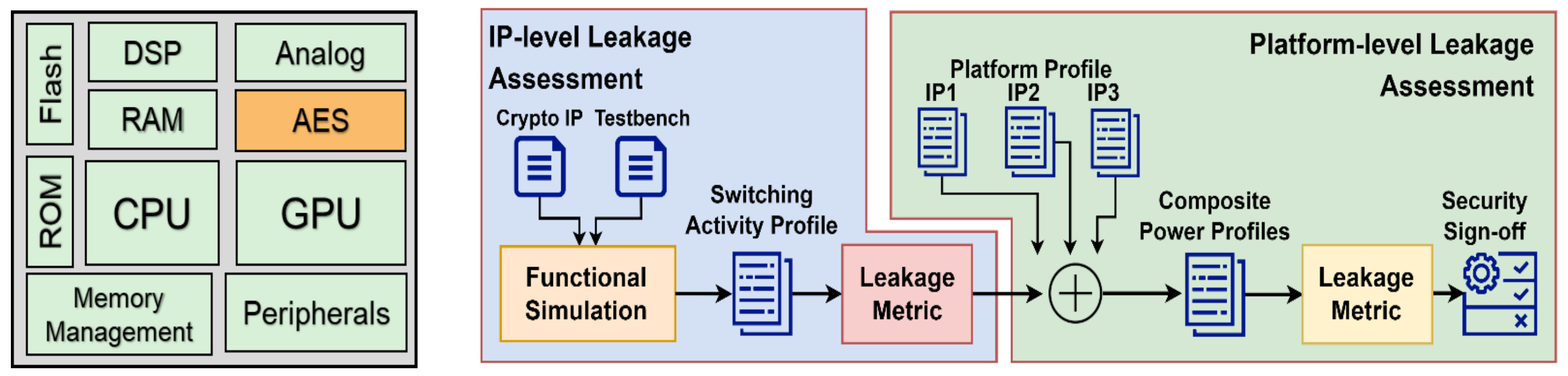


Figure 4: Platform-level PSC leakage assessment (SoC-PAT) in RTL

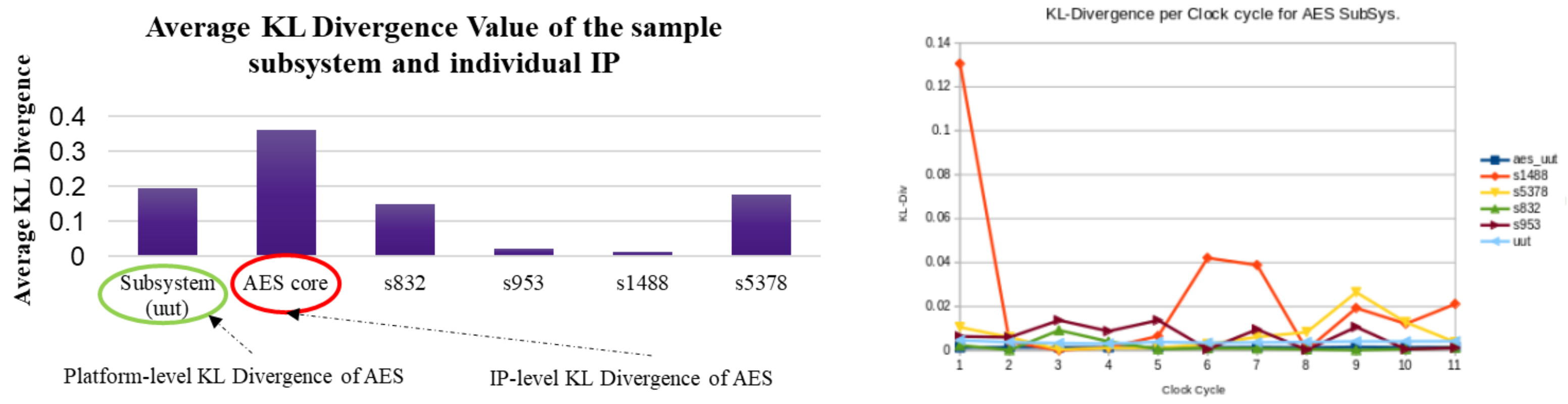


Figure 5: Subsystem level PSC metric for example designs

PD-PAT

Objective:

- Develop a fast and efficient physical design level PSC assessment framework with the help of deep learning
- Reduce the execution time for PSC assessment at the layout level
- Model power signature at the layout level by considering different physical layout features and switching activity

OVERVIEW OF THE FRAMEWORK

- The flow of the PD-PSC framework starts with the formation of a database of multiple physical layouts.
- The framework analyzes synthesized netlist, VCD file, and layout design files (DEF, SPEF, and SDF) to extract the relevant and potential features.
- The extracted features are applied to a GNN architecture to map the physical layout level dynamic power signature.

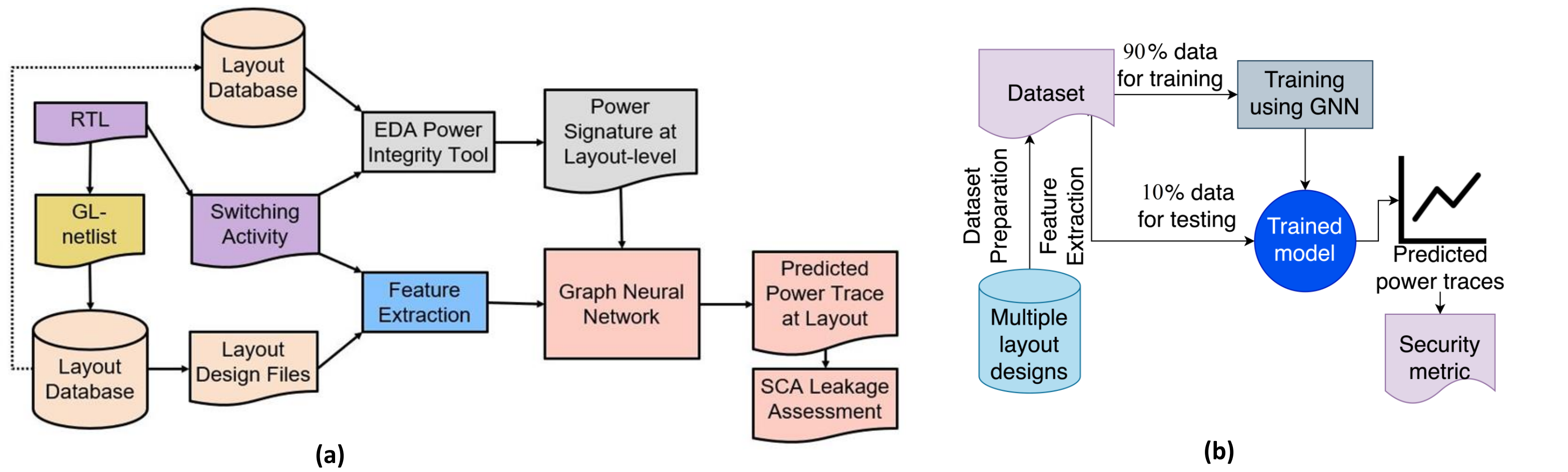


Figure 6: Proposed (a) PD-PAT framework and (b) overall approach for power side channel assessment at the physical design level

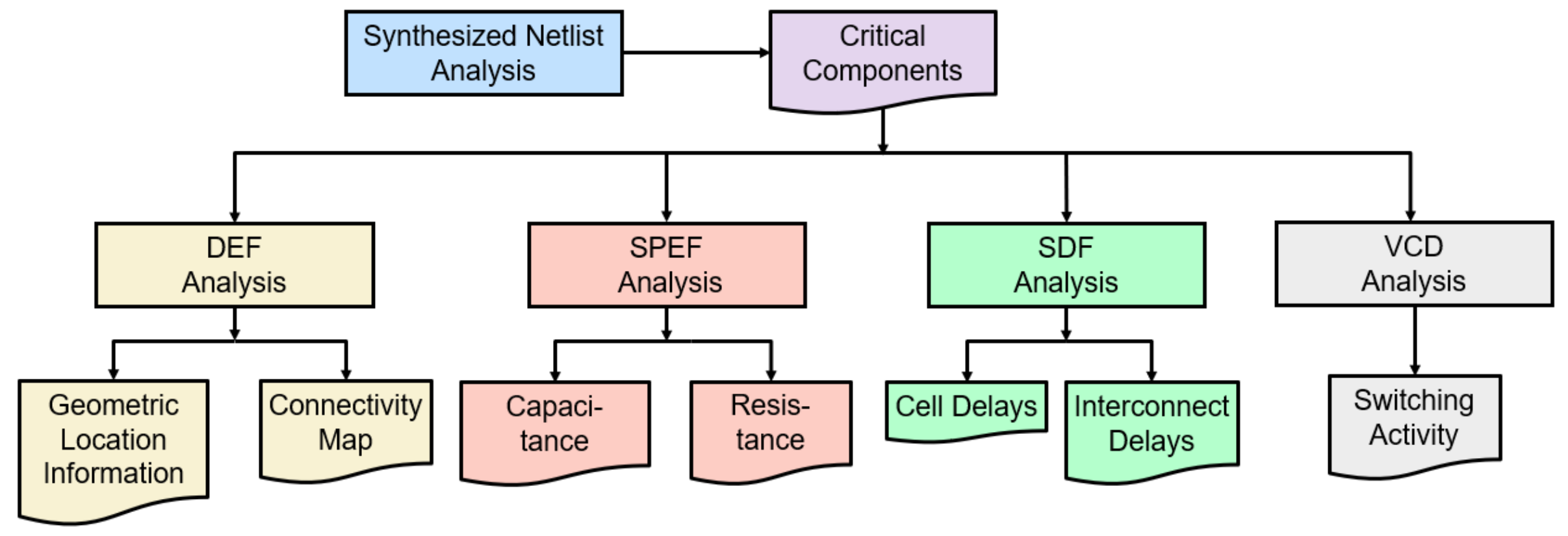


Figure 7: Feature Extraction for PD-PAT framework

EXPERIMENTAL RESULTS

- A dataset with 200k power traces collected at the layout level from 100 different physical design of AES-GF
- PD-PAT can significantly reduce the execution time compared to the traditional approach with a speedup of 100× - 200× (approx.) depending on the design size
- PD-PAT obtains a mean absolute variation of 3.35 in terms of KL divergence from the golden layout-level leakage assessment.

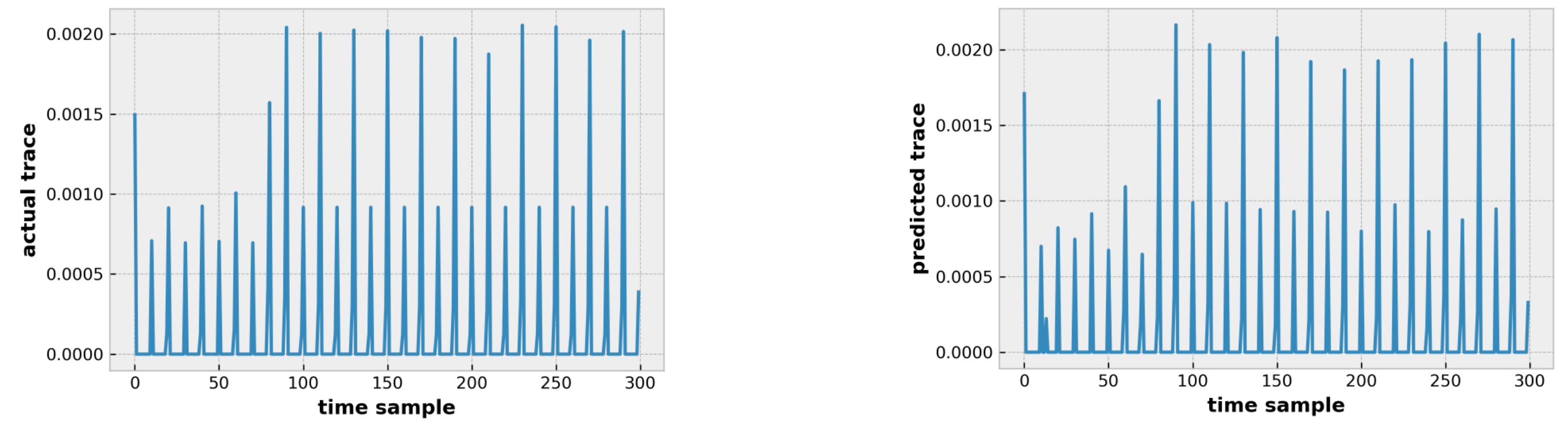
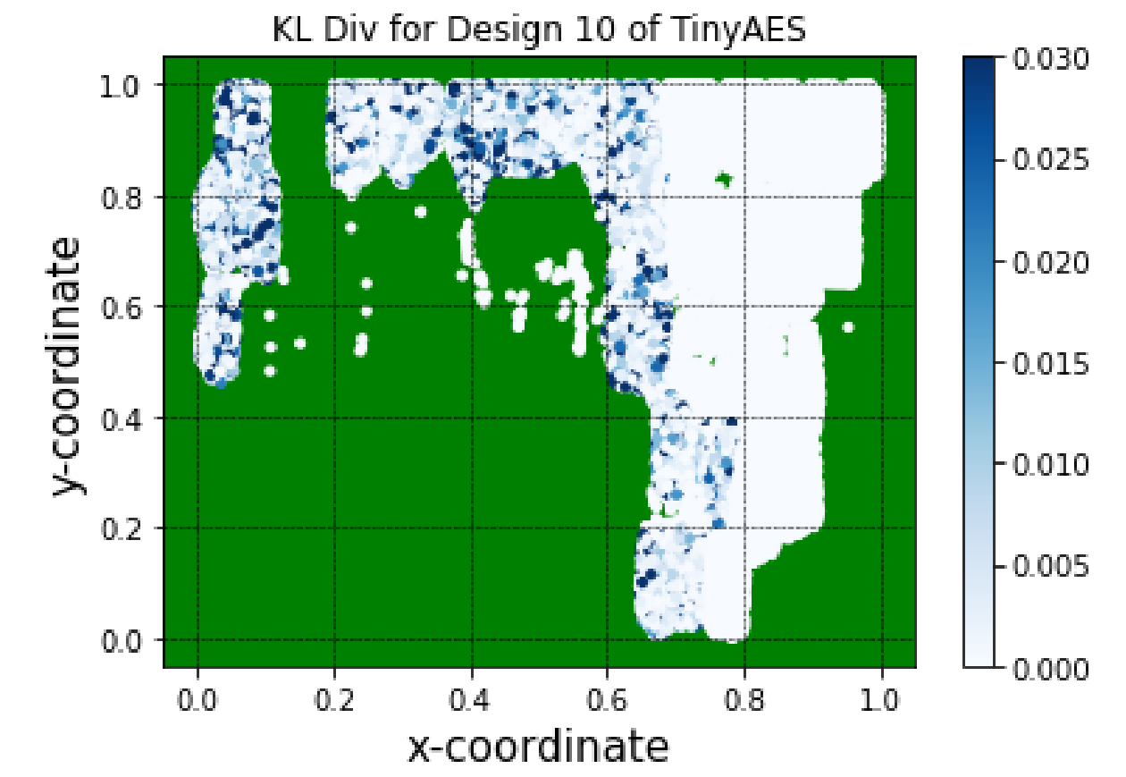


Figure 8: Performance of PD-PAT in power modeling

Performance and Work-in-progress

- RTL-PAT performs AES PSC analysis in 20-40 minutes, compared to 20-30 hours at gate-level and a few days at the physical level
- FPGA TVLA analysis provides qualitative validation of RTL-PAT results
- Submodule-level analysis can identify vulnerable blocks and help designers apply countermeasures accordingly
- PD-PAT performs PSC leakage assessment correctly at the physical design level with a significant speed-up.
- Work-in-Progress:
  - ➢Complete SoC design simulation and PSC leakage assessment => non-trivial, time (~20 hours), and resource intensive
  - ➢Cell-level PSC leakage assessment at the layout level



Summary and Conclusion

Complete automated CAD frameworks at RTL and physical level for power side-channel security sign-off

- RTL-PAT provides fast quantitative detection of power side-channel vulnerability at RTL
- Submodule level analysis provides flexibility and reduces redesign time and cost
- System level PSC metric goes down (resiliency increases) due to additional noise components
- SoC-level PSC vulnerability analysis is required for complete security sign-off at RTL
- Quick estimation of PSC vulnerability with PD-PAT tool is important to ensure secure physical design.

REFERENCES

[1] N. Pundir, J. Park, F. Farahmandi and M. Tehranipoor, "Power Side-Channel Leakage Assessment Framework at Register-Transfer Level," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 9, pp. 1207-1218, Sept. 2022.