EM Side-Channel Leakage Modeling and Security Assessment at Pre-Silicon Stages

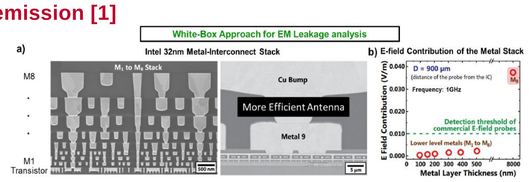
Md Kawser Bepary, Tanvir Rahman, Hasan Al-Shaikh, Jungmin Park, Fahim Rahman, Mark Tehranipoor,
Florida Institute of Cybersecurity (FICS) Research, Department of ECE, University of Florida

INTRODUCTION

Electromagnetic (EM) side-channel analysis is a powerful technique to extract secret keys and assets from electronic hardware.

- EM emanation occurs due to data-dependent current flowing through the metal layers of an IC
- Higher metal layers contribute the most to the detectable EM side-channel.

Figure 1: Contribution of each metal layers for EM emission [1]



APPLICATION

Analyze cryptographic hardware designs and secure operation against EMSC-based attacks

- Model EM leakage at pre-silicon stage – easy to assess, identify, fix, and iterate.
- Establish easy-to-quantify EMSC metrics.
- Scalable and automated CAD framework for vulnerability analysis with ease
- Designer require no/minimal knowledge – Black-box information leakage model

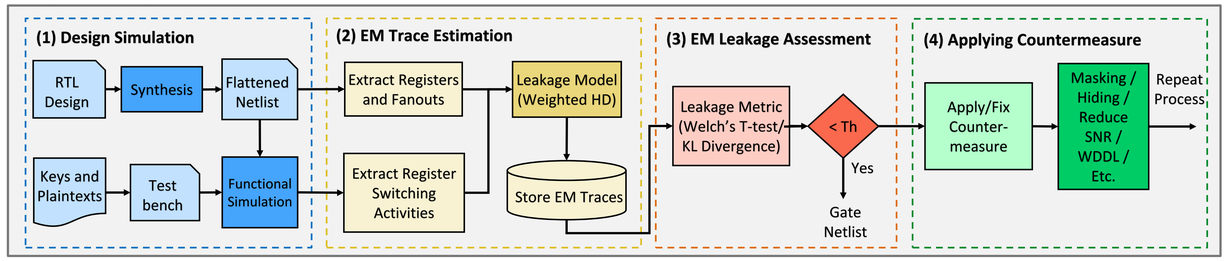
Traditional EM/Power side-channel vulnerability assessment rely on post-silicon traces -- Too late to make design improvements for countermeasure.

INNOVATION

A complete framework at RT- and gate-level for EM side-channel assessment

- Provides fast quantitative detection of EM side-channel vulnerability at RT/Gate Level
- Offer improved EM leakage model with physical design-guided parameters for higher accuracy and scalability
- Establish side-channel metrics (TVLA and KL Divergence) for assessment and validation

Figure 2: High-level overview of pre-silicon EM side-channel assessment framework



Proposed Framework

- Registers and their driving fanouts are extracted → input to the leakage model.
- Functional simulation is performed for inputs --
  - Fixed key, random vs random plaintext
  - Fixed key, random vs semifixed plaintext
  - Chosen key pair, fixed random plaintext
  - Random key pair, fixed random plaintext
- Simulated EM leakage trace is computed as the weighted switching activity of the registers
- Vulnerability assessed against metrics TVLA and KL Divergence
- WIP: Physical design guided weight is assigned to account for higher metal layers' EM emission

Figure 3: Physical layout guided weight assignment in the leakage model

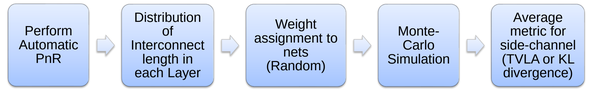


Figure 4: Layout-level EM analysis flow using RedHawk

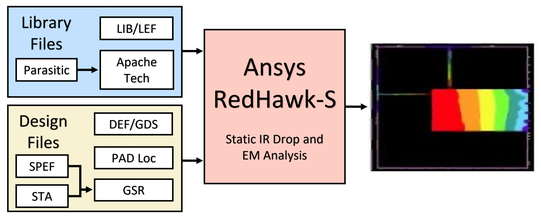


Figure 5: Simulated EM traces of example AES design for random and semifixed plaintext sets

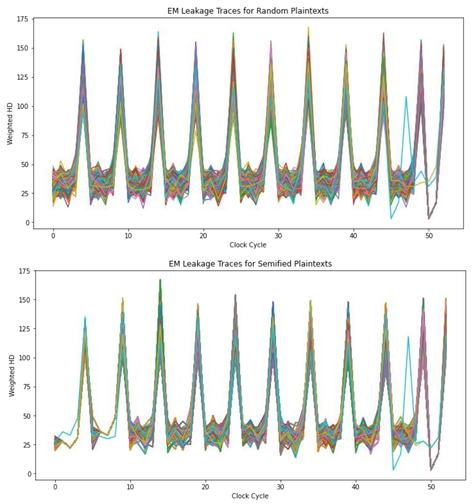


Figure 6: Distribution of weighted switching activities at different sample points

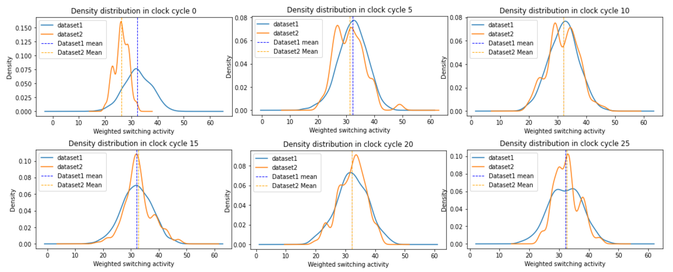


Figure 7: T-test and KL-divergence results of AES module for each sample points

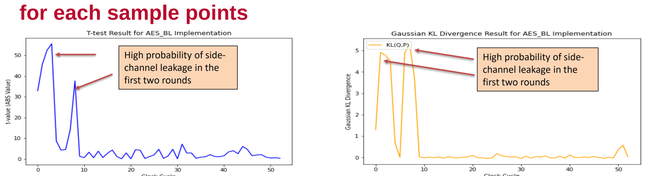


Table 1: Features for Pre-silicon EM/Power Leakage Assessment in Each Abstraction Level

	RTL	Gate-level Netlist	Layout Level
Available information	Switching Activity	Switching Activity	Switching Activity
	Register Counts	# of Fanout (≈ Load Capacitance ≈ C_{gate} + C_{wire} + $C_{diffusion}$)	Load Capacitance (C_{gate} + C_{wire} + $C_{diffusion}$ + $C_{parasitic}$), resistance
	Submodules (hierarchy)	Library Definition	Parasitic Capacitance, Resistance
	Functional Testbench	Functional and Parametric Testbench	Metal layer interconnect
Simulation Granularity	Transition of each node for each clock cycle	n-time samples per clock cycle	Transistor level SPICE simulation
	For each submodule	For each node	For each transistor
Tool	Synopsys VCS (SAIF), Cadence Incisive (VCD)	Synopsys VCS (SAIF), Cadence Incisive (VCD)	Cadence Voltus, Spectre, Synopsys HSPICE
Trace Computa-tion	Hamming Distance (HD), Hamming Weight (HW) Model	Hamming Distance (HD), Hamming Weight (HW) Model	Hamming Distance (HD), Hamming Weight (HW) Model
Leakage Assess-ment Metric	Test Vector Leakage Assessment (TVLA), KL/JS Divergence	Test Vector Leakage Assessment (TVLA), KL/JS Divergence	Test Vector Leakage Assessment (TVLA), KL/JS Divergence

RESULT & WORK-IN-PROGRESS

- Current weighted switching activity model provides insights into each round of operations
- Both T-test and KL-div. agree on vulnerable modules
- Static IR drop analysis identifies hotspot locations
- WIP: A layout level EM simulation with Ansys RedHawk is underway for improved modeling

REFERENCES

[1] Das, D., & Sen, S. (2020). Electromagnetic and power side-channel analysis: Advanced attacks and low overhead generic countermeasures through white-box approach. Cryptography, 4(4), 30.

ACKNOWLEDGEMENTS

We like to thank AFRL for sponsoring this project.