Karna: A Security Aware EDA Flow for Improved Side-Channel Attack Protection

Contact: Patanjali SLPSK slpskp@cse.iitm.ac.in , Prasanna Karthik Vairam pkarthik@cse.iitm.ac.in , Chester Rebeiro chester@iitm.ac.in , Kamakoti V kama@cse.iitm.ac.in

RISE group, Department of Computer Science and Engineering, IIT Madras

The Problem

Can we incorporate security constraints into backend VLSI design?

1. Introduction

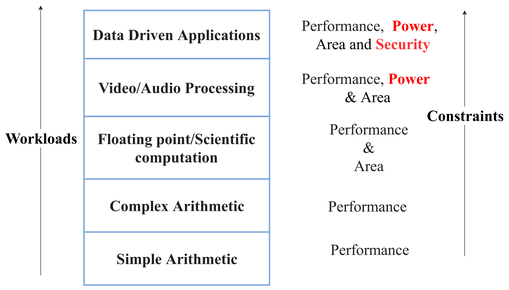
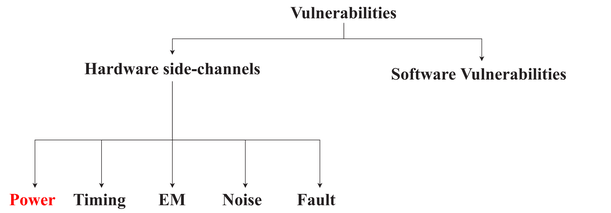


Figure: With increasing workloads the constraints that are placed on the device also increases.

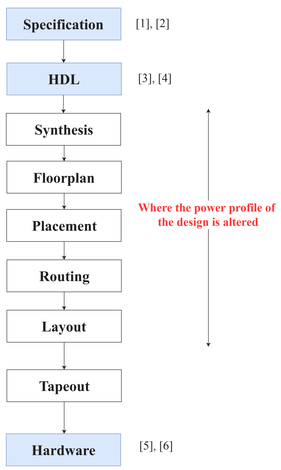
2. Overview



3. Goals

- Can try and identify the reason for the information leakage via power side-channel?
- Can we come up with a solution to minimize/eliminate the same while designing a device?**Bonus:** Can we keep the overheads down?

4. Prior Work



5. Motivation

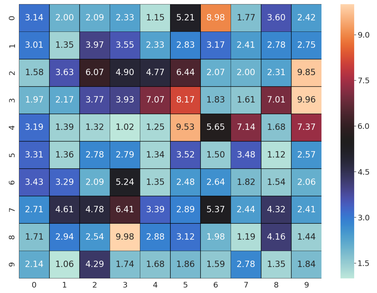


Figure: The TVLA profile of the AES-128 design, with the design divided into a 10 × 10 grid before Karna optimization.

Not all areas in the design are equally vulnerable !

6. Observation I:

Can we adjust gate parameters to reduce the power consumption of the gates in these vulnerable areas?

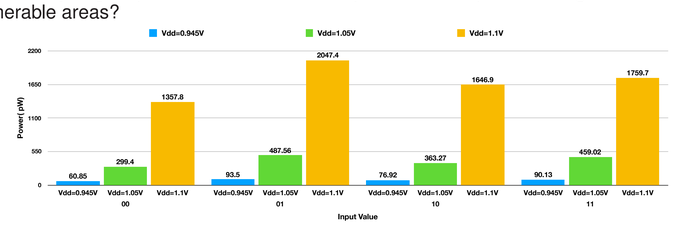


Figure: Variation of power with V_{dd} for a AND gate.

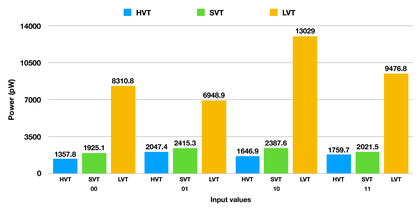
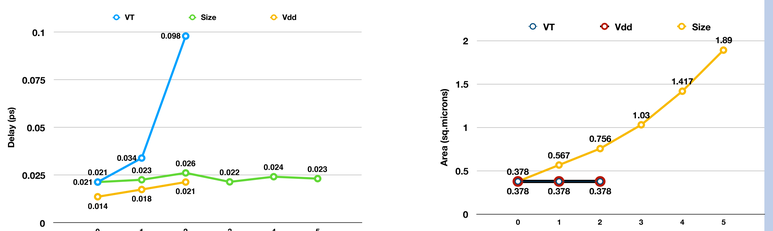


Figure: Variation of power with V_t for a AND gate.

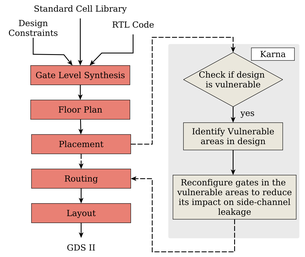
Varying the gate parameters carefully might reduce the power consumed by each gate!

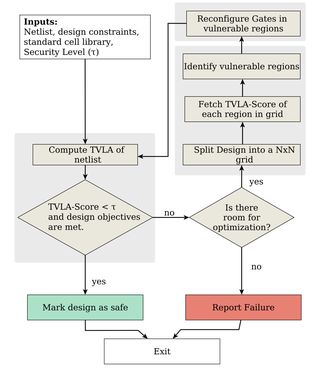
7. Observation II:



Changing the gate parameters might affect the other design goals like delay and area.

8. Solution:Karna





Results

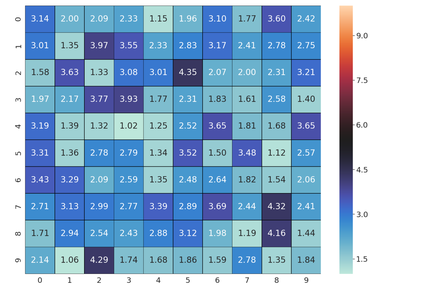


Figure: The TVLA profile of the AES-128 design, with the design divided into a 10 × 10 grid after Karna optimization.

9. Results

Table: Design delay, area and power numbers with and without Karna for achieving a security (τ) of 4.5.

	AES		PRESENT		Simon	
	Without Karna	With Karna	Without Karna	With Karna	Without Karna	With Karna
Delay (ns)	0.5	0.5	0.3	0.3	1.12	1.12
Leakage Power(μW)	492.4	236.65	5.62	0.418	3.70	0.16
#Gates	149943	149943	1520	1520	622	622
TVLA	8.22	3.7	12.28	4.06	20.799	4.48

- Power reduction of 80.05% on average.
- Karna meets security & delay objectives.

10. Future Work

- Can be extended to target fault attacks, EM attacks.
- Can be extended to incorporate more constraints (e.g. Routing).

References

1. Canright et.al. "A very compact "perfectly masked" s-box for AES (corrected)." CHES 2009.
2. Akkar et.al. " An implementation of DES and aes, secure against some attacks." CHES 2001.
3. Tiri et.al. " A vlsi design flow for secure side-channel attack resistant ics." DATE 2005.
4. A. G. Bayrak et al. An eda-friendly protection scheme against side-channel attacks. DATE 2013.
5. Arvind Singh, et.al. "Exploring power attack protection of resource constrained encryption engines using integrated low-drop-out regulators." ISLPED 2015.
6. Sanu Mathew, et.al. "Ultra-low energy circuit building blocks for security technologies." DATE 2018.