Pre-Silicon Power Side-channel Security Verification For Crypto IPs

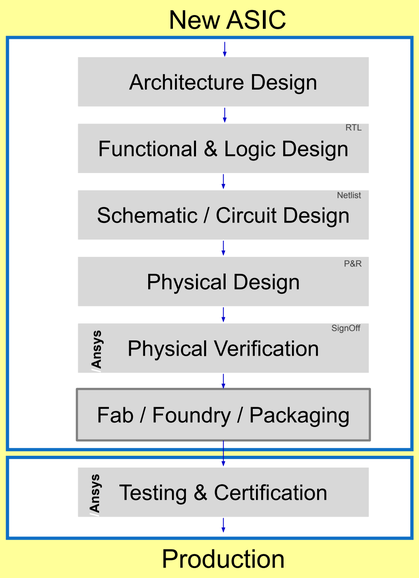
Amitabh Das*, Emrah Karagoz*, Geethu Sathees Babu and Sreeja Chowdhury****

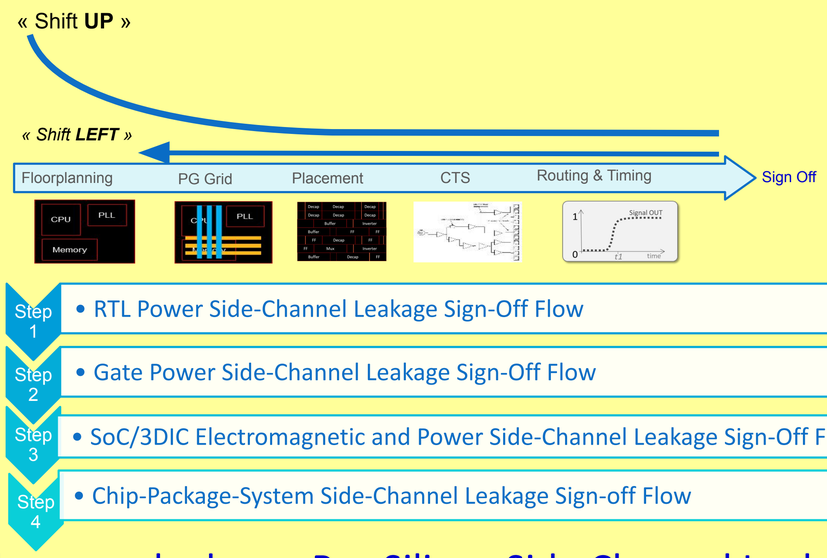
**** AMD (USA) and **Ansys (USA)***

(Amitabh.Das@amd.com, Sreeja.Chowdhury@ansys.com)

Crypto IPs are important for emerging technologies. They contain sensitive information which needs to be protected
Side-channel leakage from implementation vulnerabilities in crypto IPs needs to be evaluated.

Post-Silicon vs Pre-Silicon simulation





- Shift-left mindset for early security verification
- Designers want to perform power-performance analysis (PPA) + Security optimization at RTL, gate netlist and layout stages

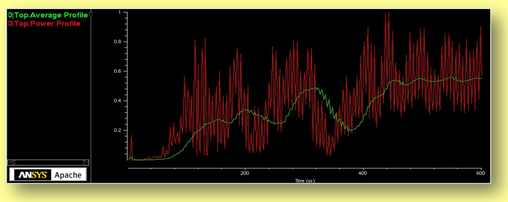
A Pre-Silicon Security Verification workflow is needed!

We have worked on a Pre-Silicon Side Channel Leakage (SCLA) Verification flow targeting the RTL level

PRE-SILICON RTL SIDE-CHANNEL LEAKAGE VERIFICATION FLOW

Ansys Power Artist™

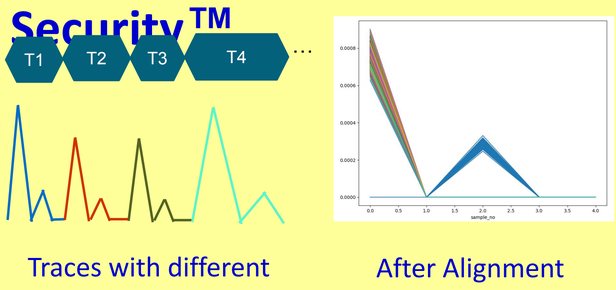
Fast Power Profile



Generation

- Cycle-accurate RTL/gate power profiling to get power side-channel traces of million crypto transactions

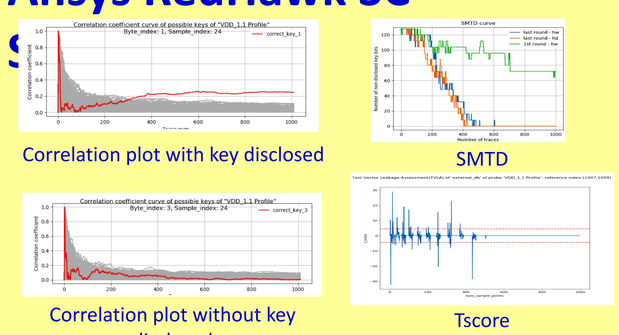
Ansys RedHawk SC Security™



Alignment

- Align the starting time of each transaction with the same operating cycle

Ansys RedHawk SC S…



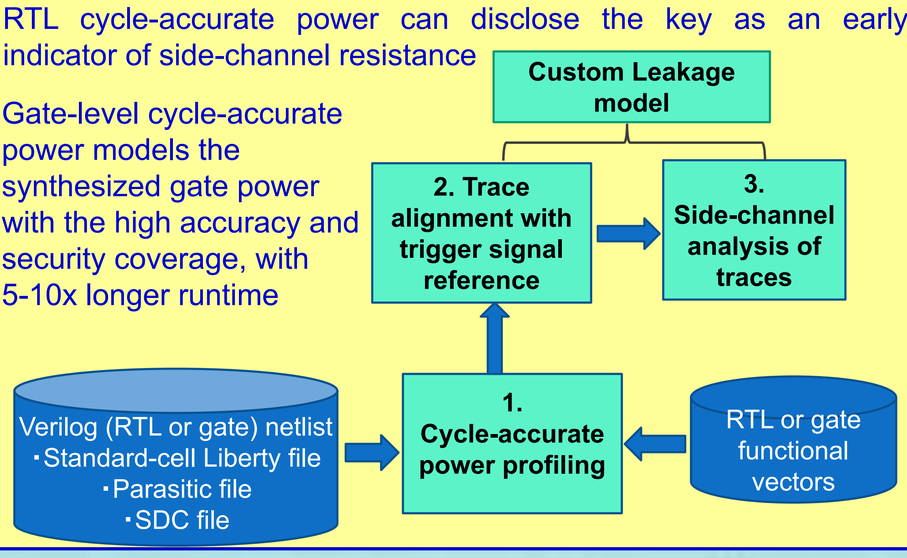
Analytics

- Apply custom leakage model to deal with different functions of crypto IPs (symmetric, asymmetric, post-quantum cryptosystems…)

EVIDENCE: KEY DISCLOSURE AND RUNTIME STATS

Flow Chart

- Custom leakage model can target different crypto function to cover all possible side-channel leakage
- RTL cycle-accurate power can disclose the key as an early indicator of side-channel resistance
- Gate-level cycle-accurate power models the synthesized gate power with the high accuracy and security coverage, with 5-10x longer runtime



Key Disclosure Data

- The leakage model targeting last round of **open-source** AES can disclose 128 bits of AES key with 3989 traces
- Flow is completely scalable with CPUs due to parallel trace processing and side-channel analytics
- Linear runtime increase with # traces and # leakage models
- Total runtime can be controlled under half day for a quick TAT

# of profile power traces	# of leakage models	Runtime	Peak memory (GB)	CPUs
10000	1	10 min	1.6	10
1M	1	40 min	3.8	40
10000	16	4 hr 30 min	6.75	10

	Custom leakage model	RTL activity	RTL Profile Power	Gate power
Hamming Weight	1st round of AES	No disclosure	No disclosure	7 bytes
	1st round of add_round_key	No disclosure	No disclosure	9 bytes
	last round of AES	No disclosure	No disclosure	16 bytes in 403 traces
	Last round of add_round_key	No disclosure	No disclosure	No disclosure
Hamming Distance	1st round of AES	No disclosure	No disclosure	No disclosure
	1st round of add_round_key	No disclosure	No disclosure	No disclosure
	last round of AES	No disclosure	16 byte in 3989 traces	16 bytes in 982 traces
	Last round of add_round_key	No disclosure	No disclosure	No disclosure

SUMMARY & FUTURE WORKS

- Pre-silicon security verification flow is essential for semiconductor industry
- Proposal of EDA flow for side-channel trace generation, alignment and analytics
- Scalable performance and comprehensive coverage of leakage to mitigate power side-channel vulnerabilities