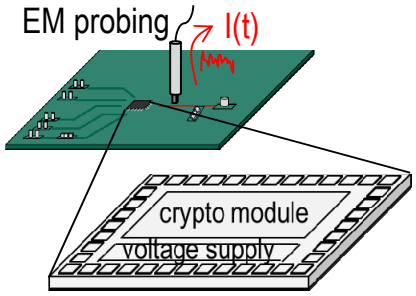
A Full System Simulation Technique of Power-Noise Side Channel Leakage in Cryptographic Integrated Circuits

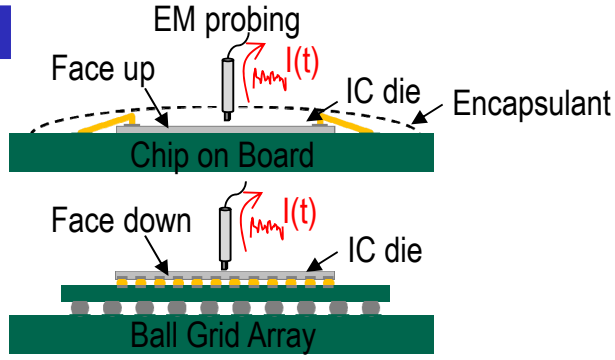
Akihiro Tsukioka(1), Makoto Nagata(1)
Karthik Srinivasan(2), Shan Wan(2), Lang Lin(2), Ying-Shiun Li(2), Norman Chang(2)
Kobe University(1), ANSYS Corporation(2)

Motivation & Problem Statement (1/2)

On-Board Leakage

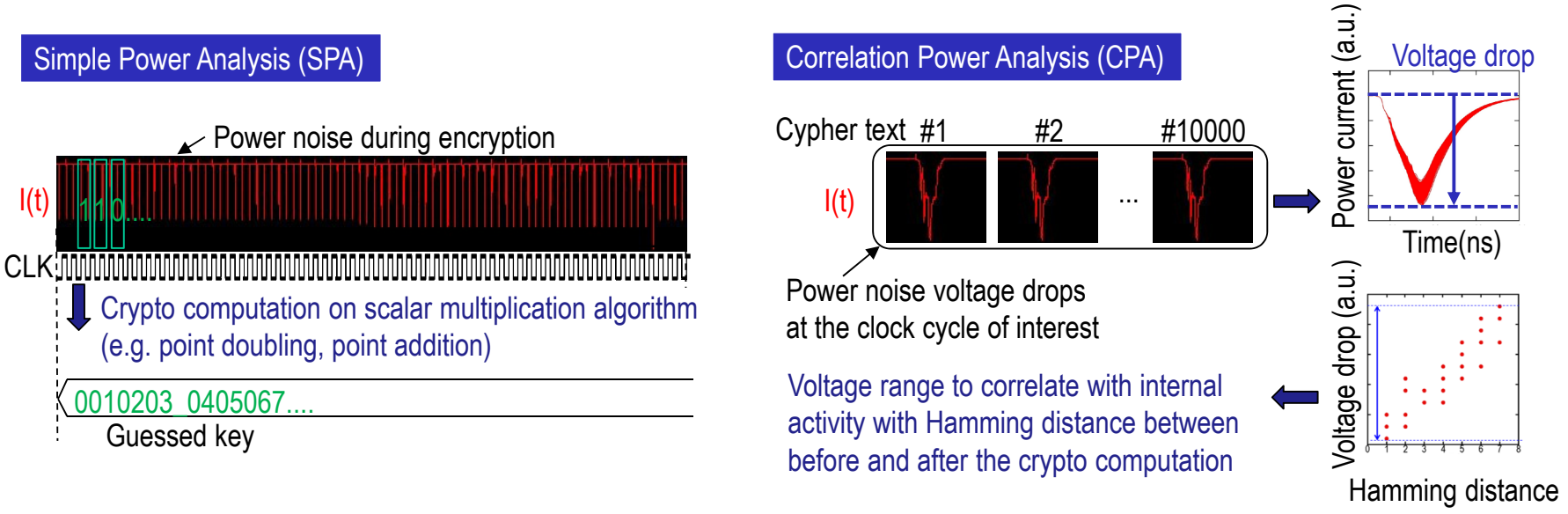


On-Chip Leakage



- Side-channel information leakage -- as serious threats and vulnerabilities to modern security hardware
  - ✓ Cryptographic ICs in operation exhibit physical variables much correlated with internal information like a secret key.
- Power-noise side channel (SC) leakage
  - ✓ Power consumption currents cause “noise” universally existing around IC chip, package and system board, through PDN, EM wave, Silicon substrate noise.

Motivation & Problem Statement (2/2)



- Analysis (or attacks in a malicious case) to extract a secret key from power-noise waveforms
- Simulation technique to evaluate security risks in design against diversified leakage models

Previous Research

- Countermeasure design styles against SCA (e.g.)
  - ✓ Wave Dynamic Differential Logic (WDDL) [1]
  - ✓ Masked And Operation (MAO) [2]
  - ✓ Masked Dual-Rail Pre-charge Logic (MDPL) [3]
  - ✓ Threshold Implementation (TI) [4]

- Simulation methodology of SCA (e.g.)
  - ✓ Power consumption model [5]
  - ✓ Capacitor charging model [6]
  - ✓ Computational platforms / Gate and transistor-level simulation [7]

[1] K. Tiri, *et al.*, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," DATE'04, vol.1, pp.10246-10251, 2004.

[2] E. Trichina, "Combinational Logic Design for AES SubByte Transformation On Masked Data," Cryptology ePrint Archive, 2003/236, 2003.

[3] T.pop, *et al.*, "Masked Dual-Rail Precharge Logic : DPA-Resistance Without Routing Constrain," CHES2005, LNCS3659, pp.172-186, Springer-Verlag, 2005.

[4] S.Nikova, *et al.*, "Threshold Implementations Against Side-Channel Attacks and Glitches," The 8th Internal Conference on Information and Communications Security (ICICS 2006), LNCS4307, pp. 529-545, Springer-Verlag, Dec. 2006.

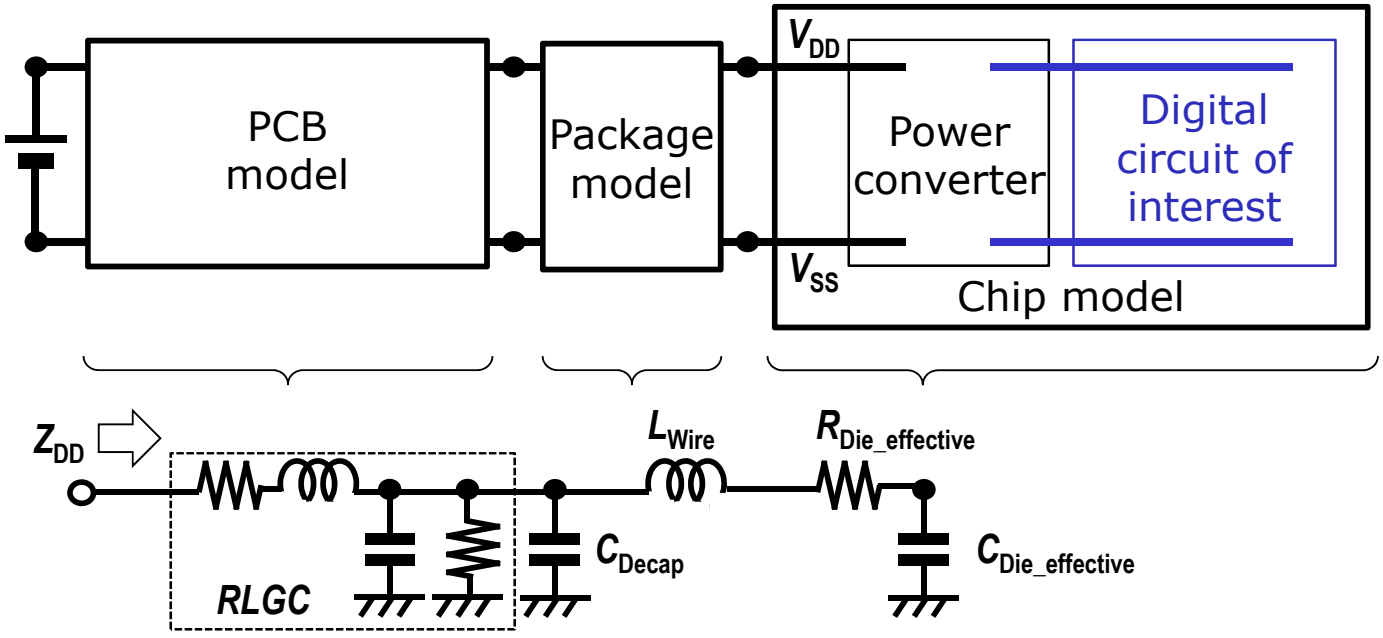
[5] K. Tiri, *et al.*, Simulation Models for Side-Channel Information Leaks," The proceedings of DAC 05, pp. 228-233, Dan Diego, CA, USA, June. 2005.

[6] D. Fujimoto, *et al.*, "A Fast Power Current Simulation of Cryptographic VLSI Circuits for Side Channel Attack Evaluation," IEICE Transactions on Fundamentals, Vol.E96-A, No.12, pp.2533-2541, Dec. 2013.

[7] A. Kumar, *et al.*, "Efficient simulation of em side-channel attack resilience," IEEE/ACM Int. Conf. Comp. Aided Design (ICCAD), pp. 123-130, Nov. 2017.

CPS* Model for Diagnosis and Analysis

*Chip-Package-System board



- Full-system level simulation of power-noise SC leakage

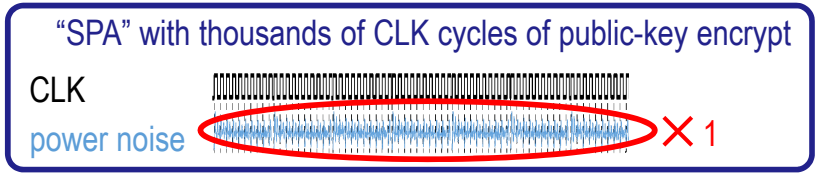
Challenges

- Challenge1: Chip Package System(CPS) board-level power-noise SC leakage modeling and simulation

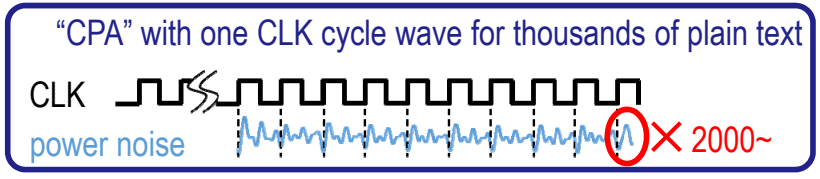
✓ Side-channel leakage is assessed on countermeasure crypto ICs in a design phase.

- Challenge2: Analysis (attacks) by simulation to derive a secret key from IC chip level power noise waveforms

✓ Public-key cryptography –
Simple Power Analysis ("SPA"), a single power-noise waveform over thousands of CLK cycles, very long time power noise simulation is required.



✓ Private-key cryptography –
Correlation Power Analysis ("CPA"), power-noise waveforms for thousands of different plain texts, very large set of power noise simulation is required.

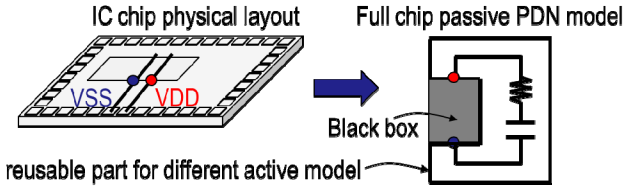


Chip Power Model of Crypto Engines

► Noise paths and noise sources

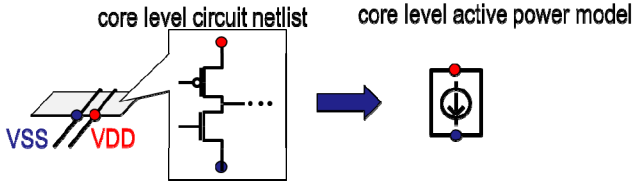
(1) Full chip PDN modeling

- ✓ include silicon substrate
- ✓ w/o dynamic power simulation



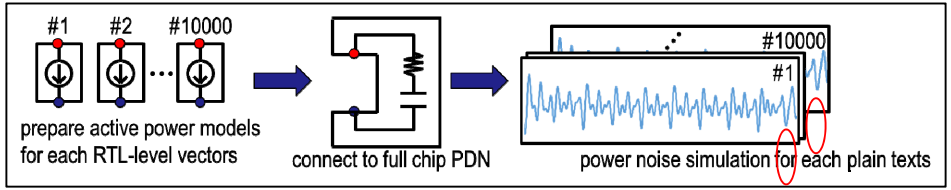
(2) Core level power modeling

- ✓ w/o full chip Si sub. and PDN extraction

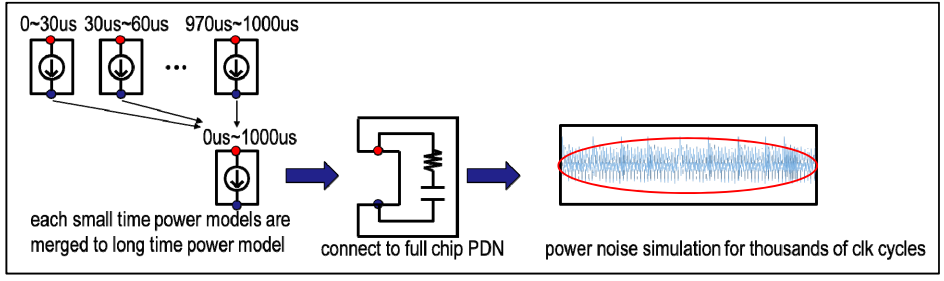


► Power-noise SC leakage simulation

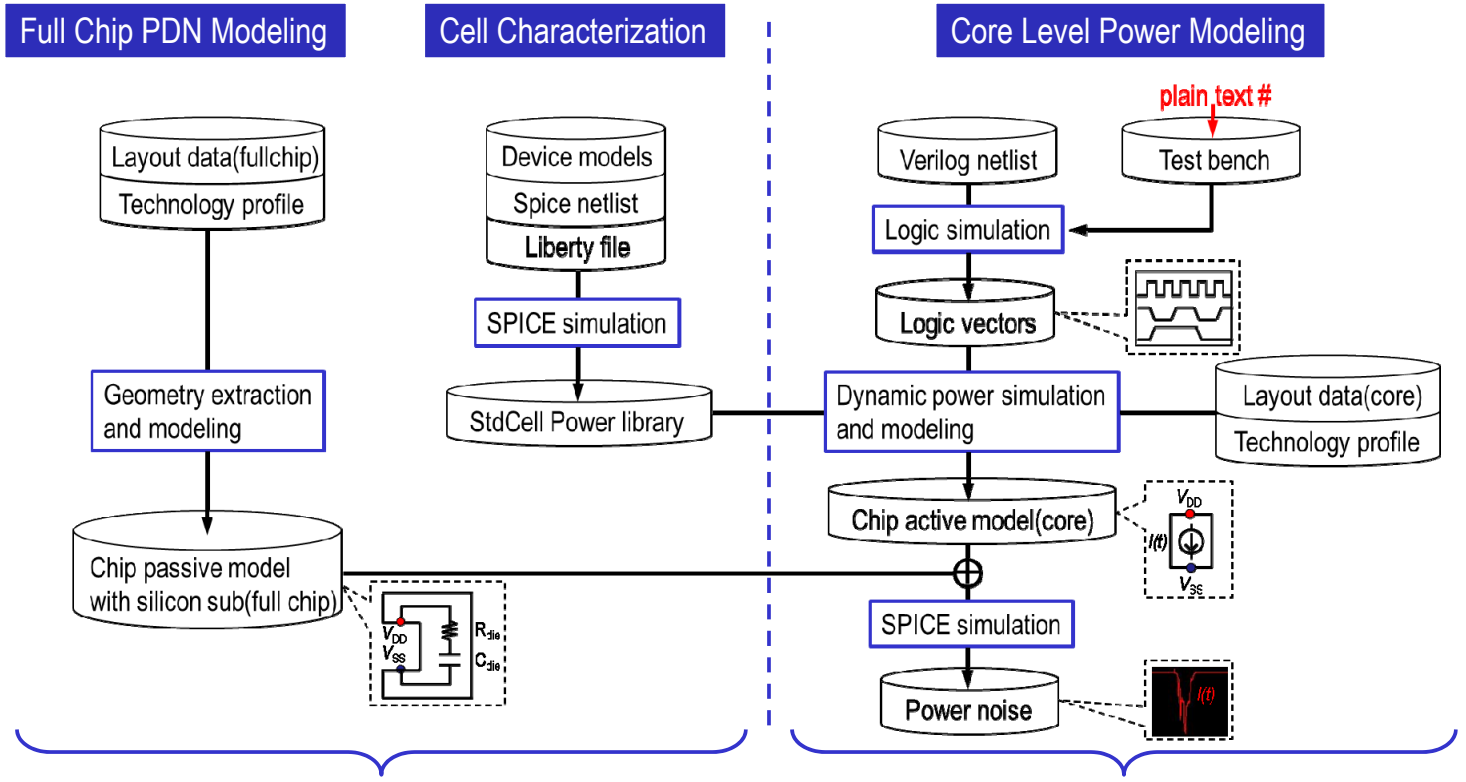
Case1: Private-key (e.g. AES) – power-noise waveforms for thousands of plain texts (#1~#10000) (different test vectors for short CLK cycles)



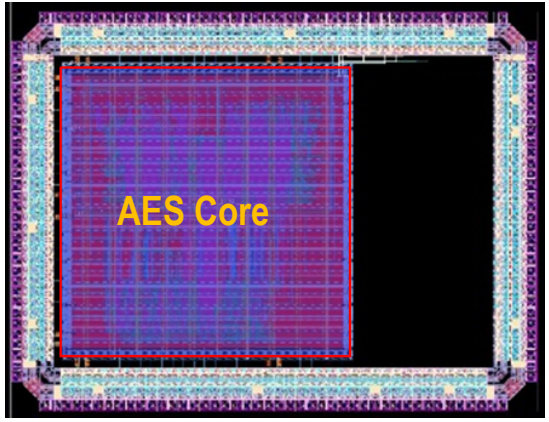
Case2: Public-key (e.g. RSA, DSA, ECDSA) -- a single power-noise waveform of several thousand CLK cycles

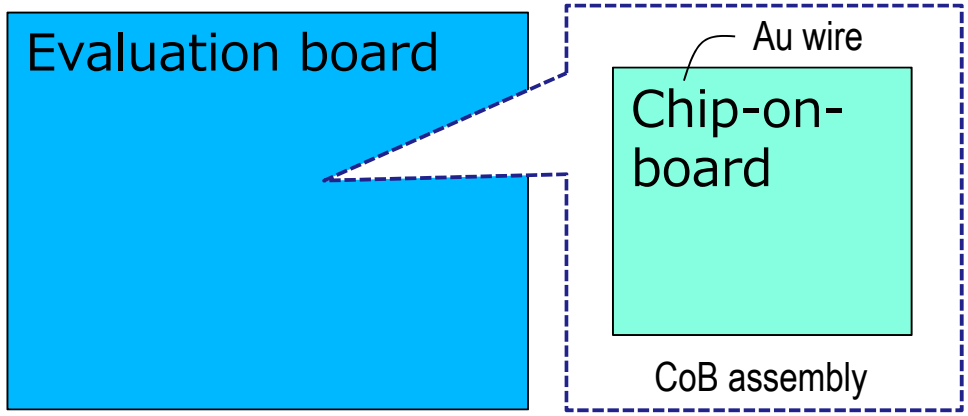


Power-Noise SC Leakage Simulation Flow



Silicon Experiments





- 128bit AES crypto IC chip
  - ✓ 3 mm x 4 mm
  - ✓ 130 nm CMOS process
  - ✓ Private key cryptographic (AES)
  - ✓ Single power domain (1.5V)
- Evaluation board and system
  - ✓ 7.3 cm x 10.0 cm
  - ✓ 4 layers of interconnect
  - ✓ Chip on Board (CoB) assembly
  - ✓ Daughter board to micro controller

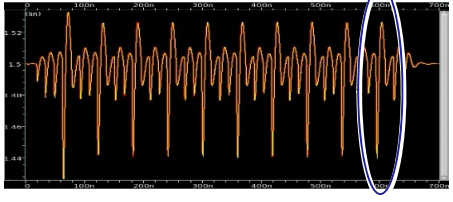
Power-Noise SC Leakage Simulation Results

- Case study: private-key cryptographic IC chip
  - ✓ AES encryption engine
  - ✓ Operation frequency: 34 MHz

	#of cells	# of wires	# of vias
Full IC chip	231036	13674	41265

Active gate count=34K

- Power noise on VDD during crypto operation of last round (12 ns) in C-P-S simulation
  - ✓ # of plain texts: 1500

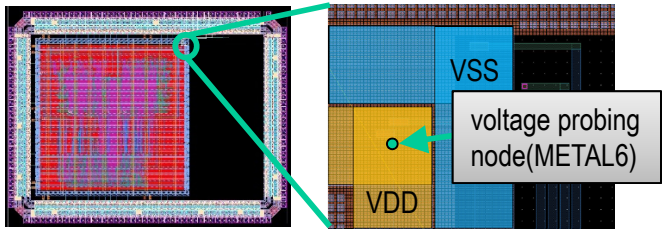


- Simulation cost evaluation
  - ✓ server: Intel Xeon CPU ES-2699 v4 (2.2GHz)

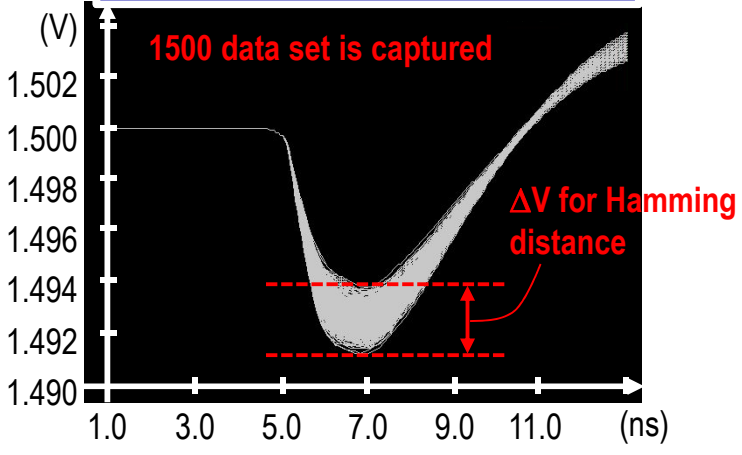
	Memory	Threads	CPU time
PDN modeling	2726MB	8	3.0 hour
power noise modeling	2348MB	8	8.5 min
power noise simulation	229MB	1	2.8 sec

} for a single waveform

Test Chip Layout

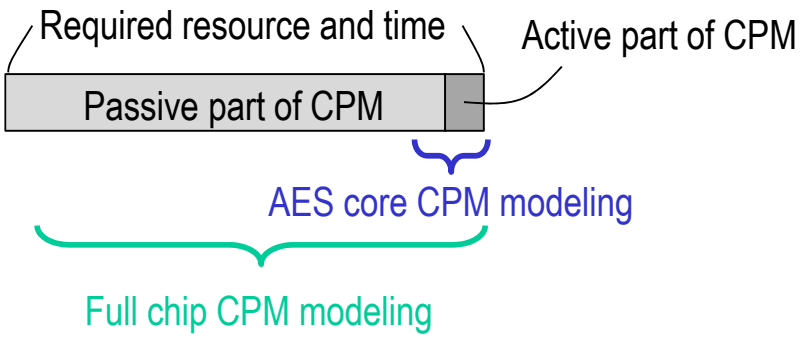


Simulated Power Noise Waveform

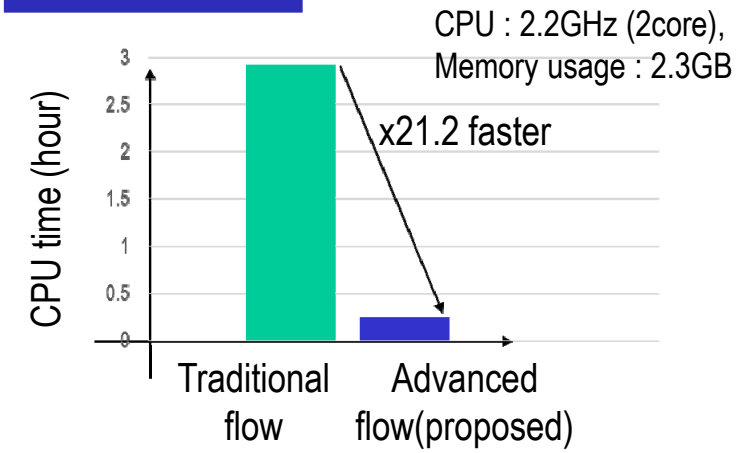


Acceleration of Simulation

Cost of CPM Extraction



Cost of Simulation



- Traditional full-chip level simulation takes longer computation time due to impedance extracted from physical layout of an IC chip in long sim. time.
- Proposed flow iteratively updates the active part of CPM while keeping passive networks (e.g. PDN) and focuses on dynamic power noise data.

Summary

- Power-noise SC leakage simulation technique was established and applicable to general cryptographic ICs
  - ✓ Private- and public-key crypto algorithms with diversified countermeasures at physical design.
- Advanced CPS simulation flow:
  - ✓ Full-chip CPM is created one time, and then the active power current is updated.
  - ✓ Core-level active power modeling is separated from full chip-level passive part modeling.
  - ✓ Whole crypto operation including pre- and post-data processing time
- Silicon examples:
  - ✓ Demonstrated 21.2 times faster modeling/simulation of private-key crypto engine, in the last 2 clock cycles (24 ns) for SC analysis
- Future scopes:
  - ✓ The simulation technique will assess the effect of countermeasure with hiding, masking, even power conditioning technique in the physical design stage.
  - ✓ Power-noise SC analysis will be performed on the set of power-noise simulated waveforms, and shed light on leakage mechanisms at physical level.