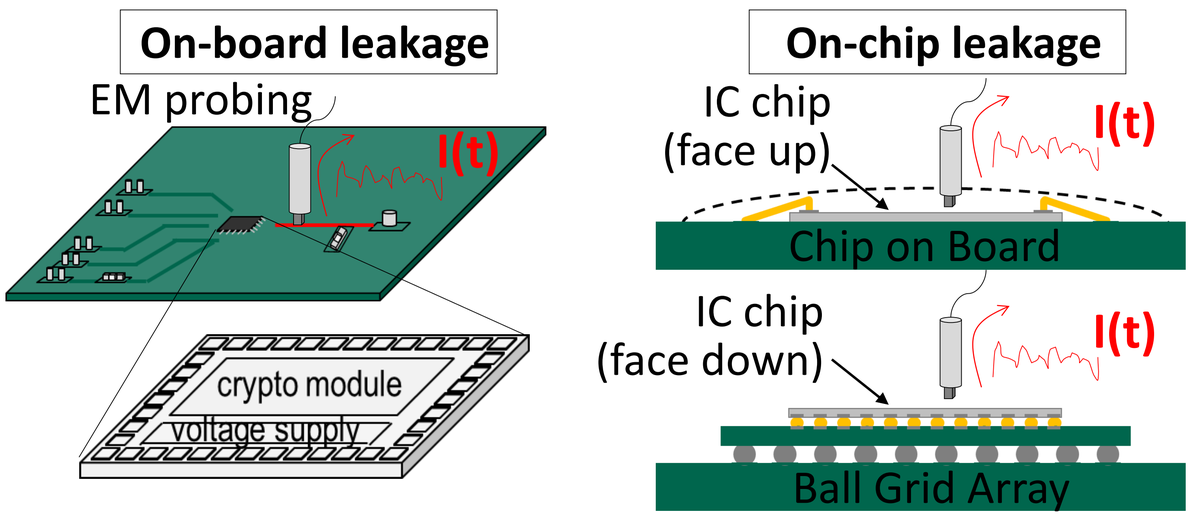
A Full System Simulation Technique of Power-Noise Side Channel Leakage in Cryptographic Integrated Circuits

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

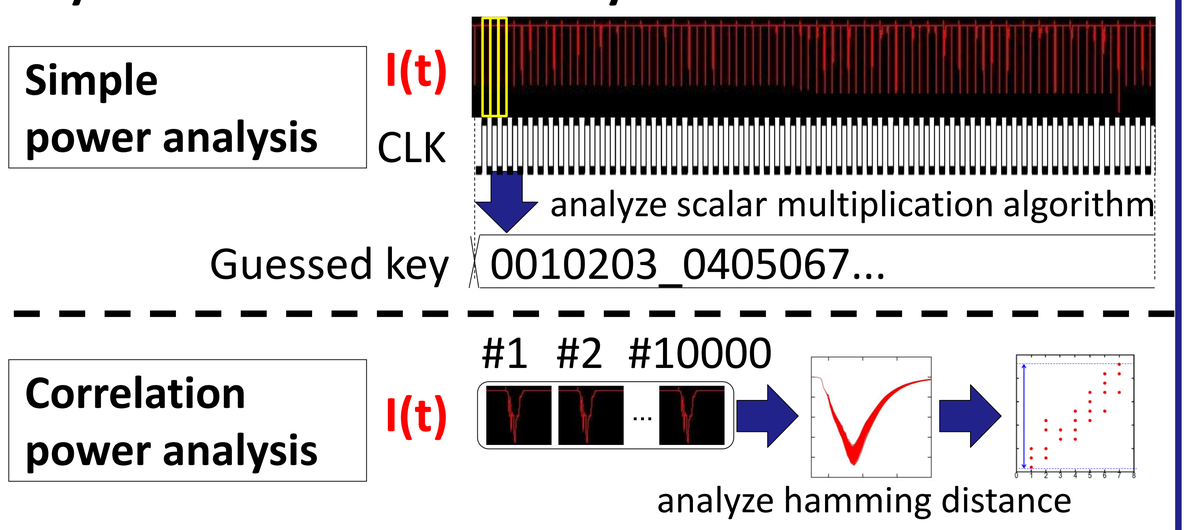
► Introduction (serious threats and vulnerabilities to modern security hardware)

<Power-noise side channel leakage>



Power consumption currents cause "noise" universally existing around IC chip, package and system board, through PDN, EM wave, Silicon substrate noise.

<Analysis to extract a secret key>

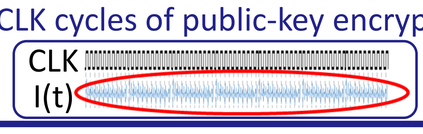


Cryptographic ICs in operation exhibit physical variables strongly correlated with internal information like a secret key

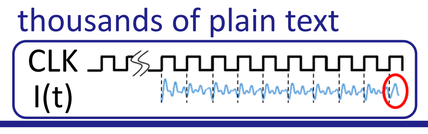
► Challenges

(1) Chip Package System(CPS) board-level power-noise SC leakage modeling and simulation
(2) Analysis (attacks) by simulation to derive a secret key from IC chip level power noise waveforms
⇒very long time power noise simulation or very large set of power noise simulation is required.

"SPA" with thousands of CLK cycles of public-key encrypt

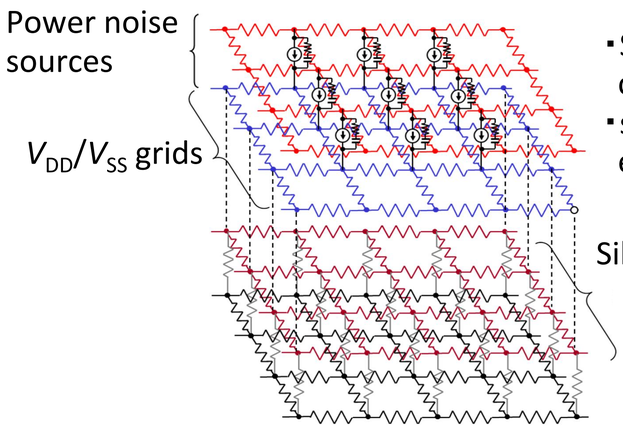


"CPA" with one CLK cycle for thousands of plain text



► Solution to draw efficient power-noise side channel (SC) leakage models of crypto engines

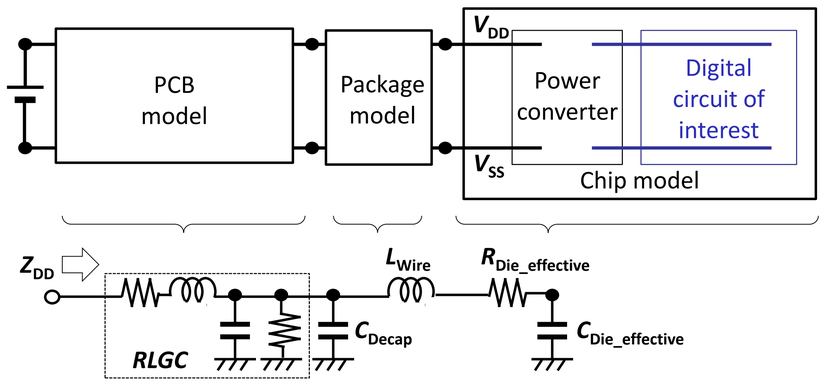
<Chip Power Model (CPM)>



- SPICE compatible compact chip model
- simulated with external off chip models

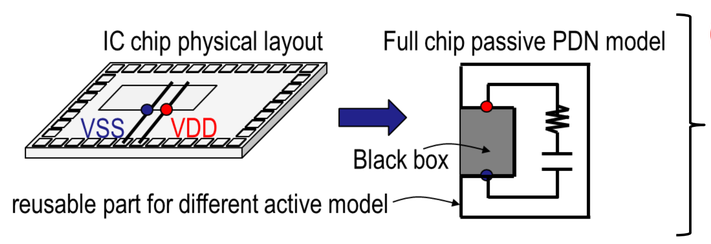
A whole chip CPM inclusive of silicon substrate network

<Chip-Package-System board model diagram>

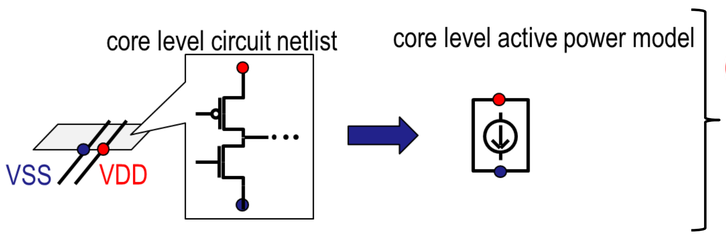


Full-system level simulation of power noise SC leakage

<Proposed CPM modeling for SC leakage simulation>

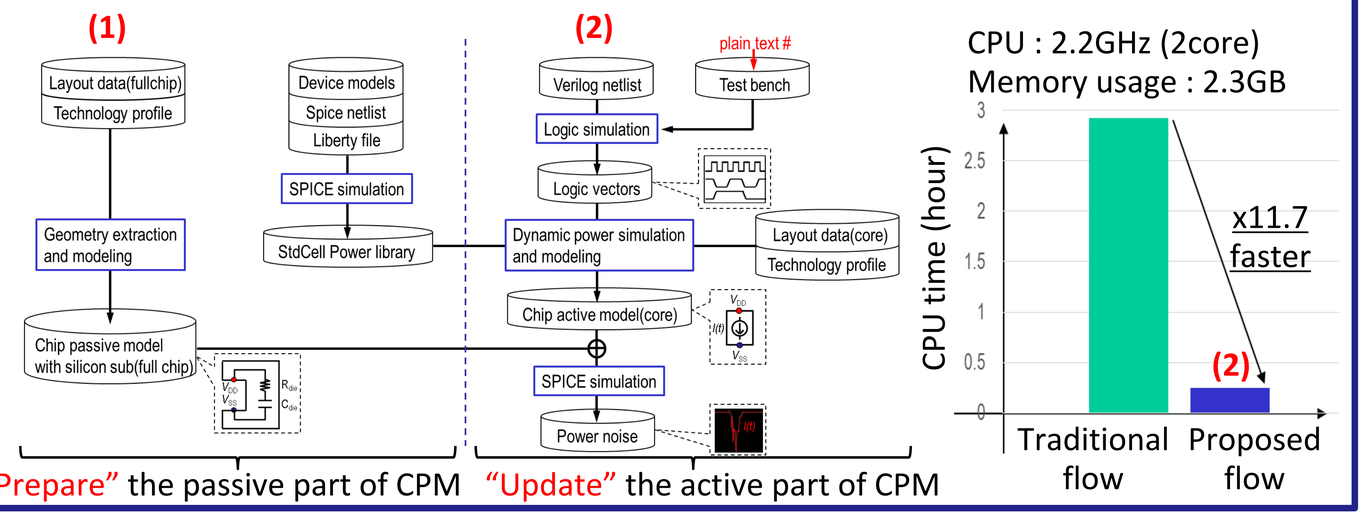


(1) Full chip-level power delivery network (PDN) modeling
- ✓create noise paths (reusable part)
- ✓include silicon substrate
- ✓noise source can be replaced



(2) Core level power modeling
- ✓create noise source
- ✓without full chip PDN, substrate extraction

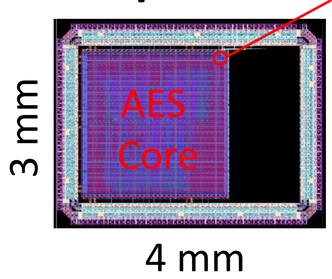
<Proposed CPM modeling flow>



CPU : 2.2GHz (2core)
Memory usage : 2.3GB

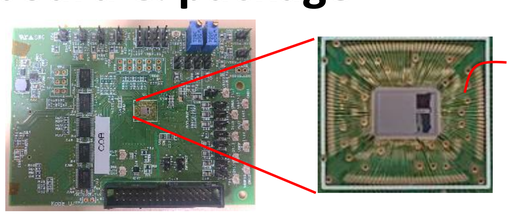
► Results: examples of power-noise SC leakage simulation

<Test chip>



-Private key cryptographic (AES)
-130 nm CMOS process
-Single power domain

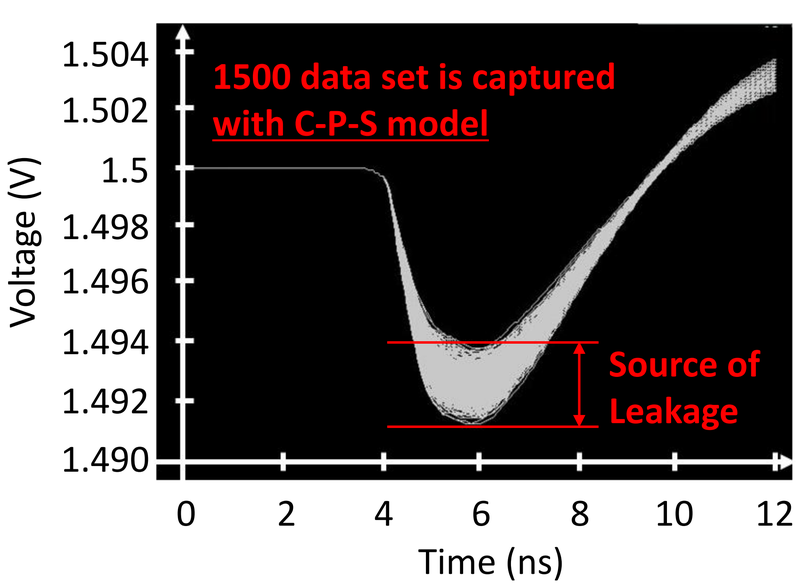
<Test board & package>



Au wire (5 mm)

Chip on Board (CoB) Assembly

<Simulated power noise waveforms>



<Simulation cost evaluation>

		Memory	Threads	Wall time
Reuse part	PDN modeling	2726MB	8	2hrs 56mins
Update part	Power noise modeling	2348MB	8	8mins 37sec
Update part	Power noise simulation	229MB	1	2.8sec

server: Intel Xeon CPU ES-2699 v4 (2.2GHz)

The modeling cost for a single waveform including pre- and post-computation

► Conclusions

- Power-noise side-channel leakage simulation technique was established and applicable to general cryptographic IC chips.
- Advanced CPM flow – the whole system-level CPM is created one time, and then the models of active power current is updated for different inputs/time segments.
- Power-noise side-channel analysis will be performed on the set of power-noise simulated waveforms, and shed light on leakage mechanisms at physical level.