Side Channel Attacks

Makoto Nagata
Graduate School of Science, Technology and Innovation
Kobe University
1-1 Rokkodai, Nada, Kobe, Japan
nagata@cs.kobe-u.ac.jp

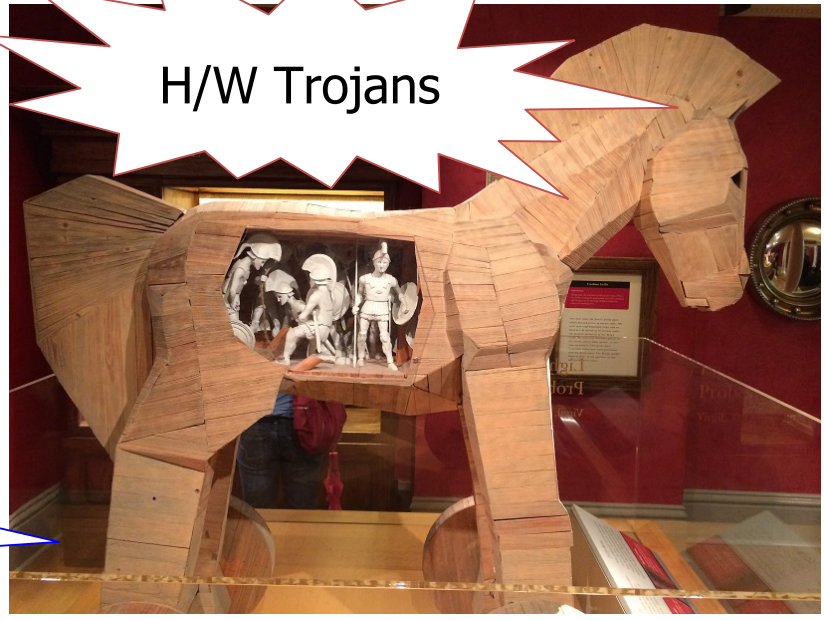
Outline

- Physical attacks
- On-chip security sensor circuits
- Simulation technique of side-channel leakage
- Conclusions

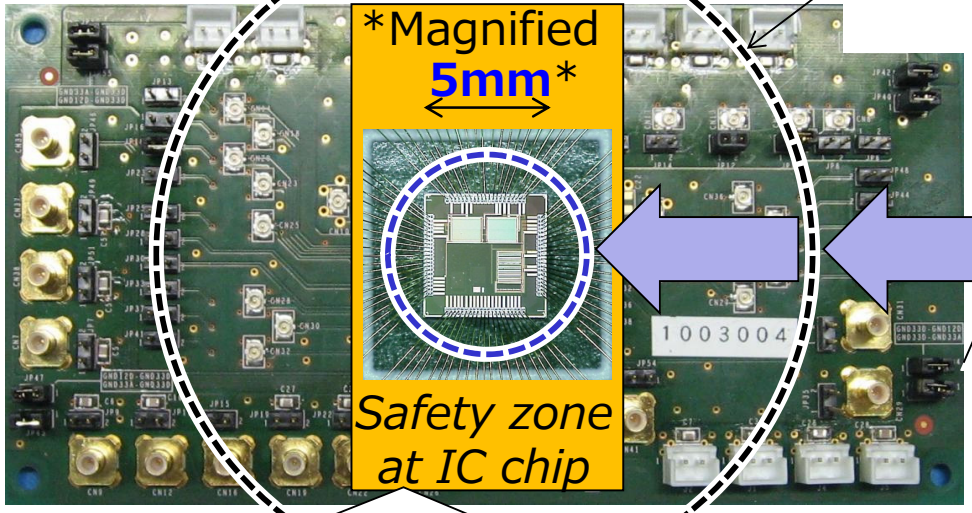
Advent of Adversary among IC Chips

Crypto attacks

H/W Trojans



Physical Attacks in Dimensions

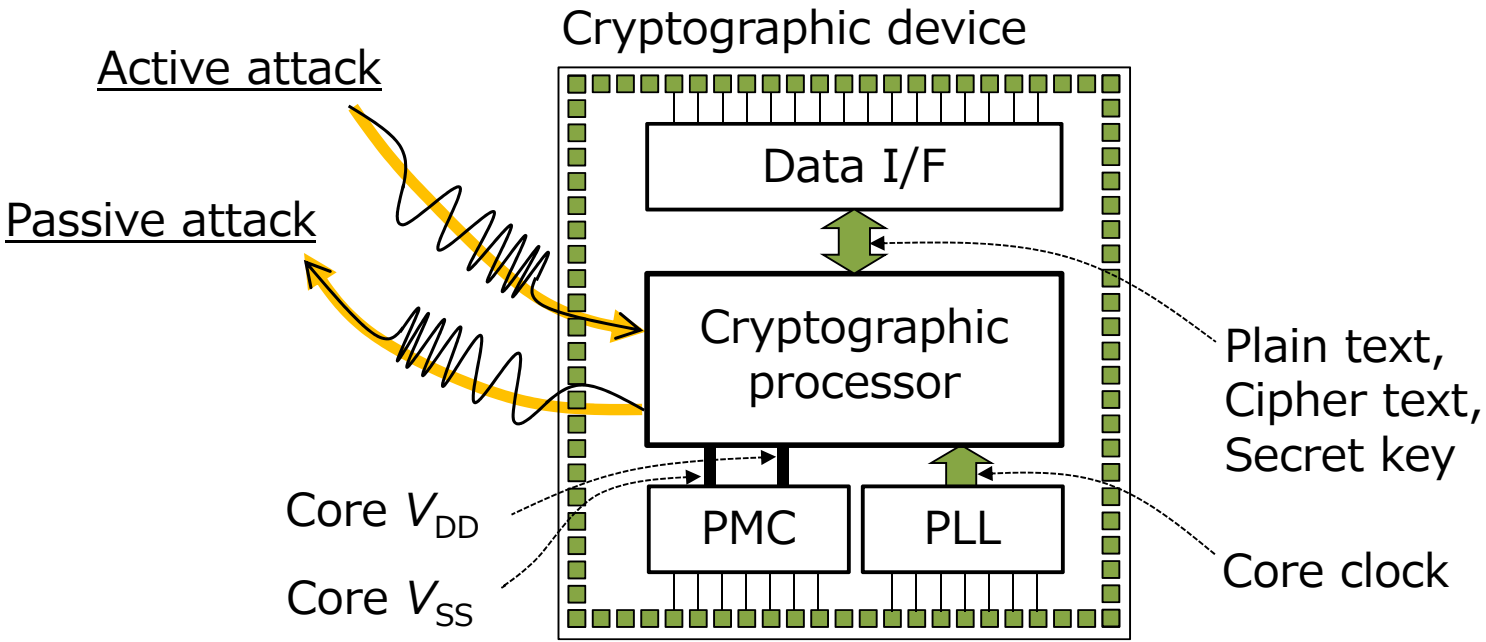


Leakage observed on PCB
~100mm

Leakage through far
EM emanation
1m~

Objective: Securing crypto-engines in the areas of ICs

Physical Attack Isolation Walls at Chip Level



Passive Attack -- Power Noise Analysis

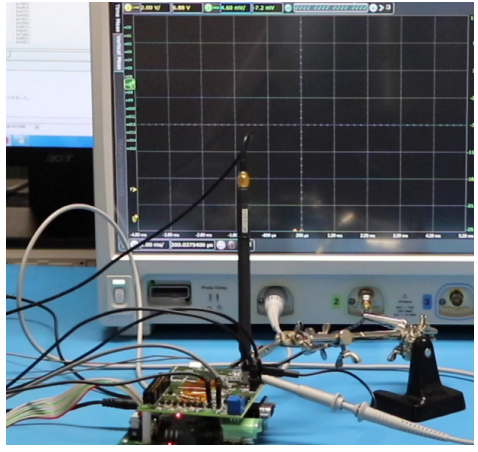
μEM probe
(Attacker)

Analysis models (Attacker)
- Simple power analysis (SPA)
- Differential power analysis (DPA)
- Correlation power analysis (CPA)
- Local EM analysis (LEMA)

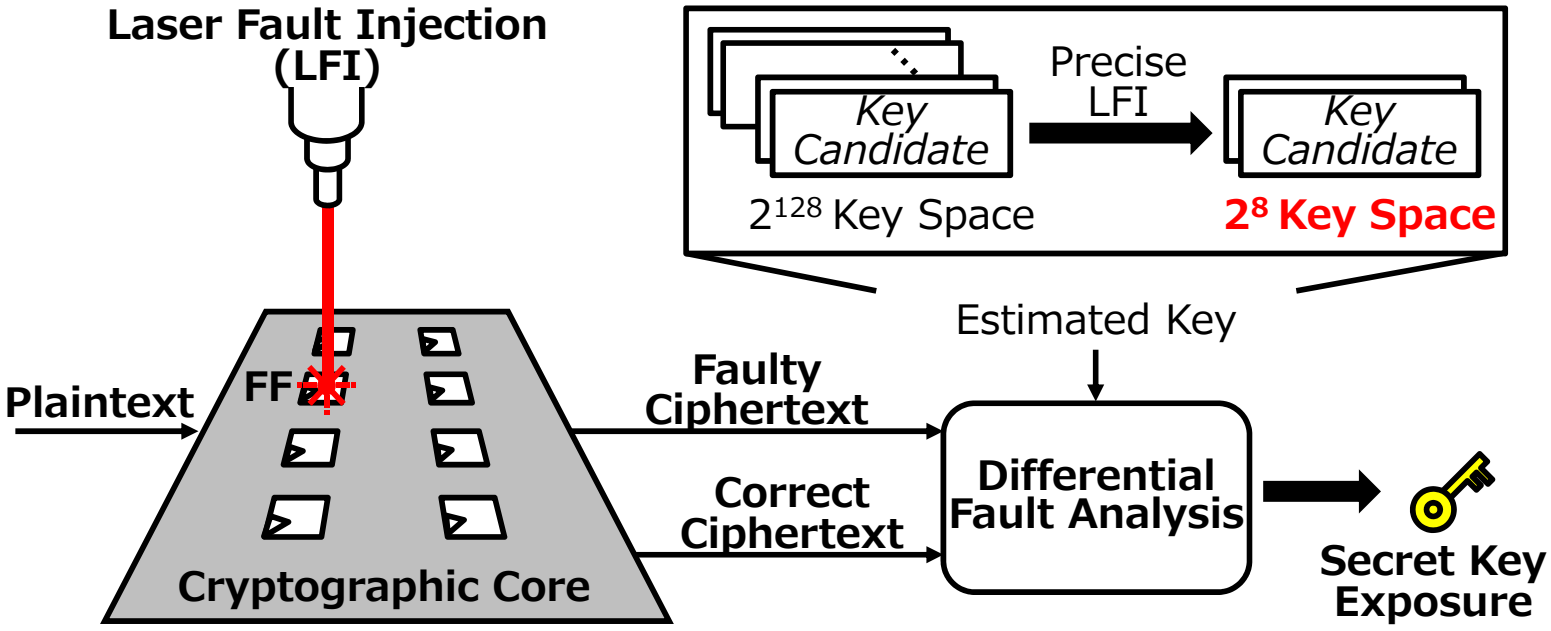
IC chip with
crypto engine

EM emanation

Package and PCB

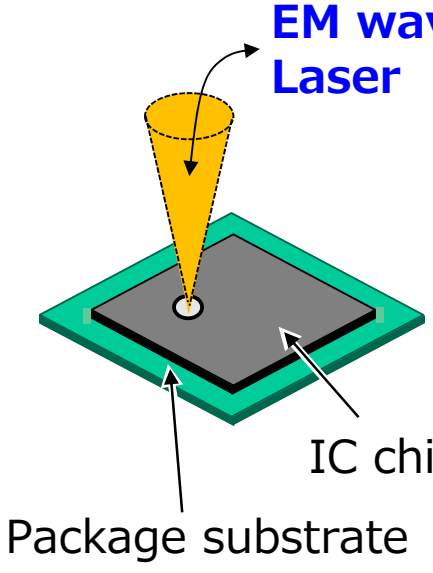


Active Attack -- Laser Fault Injection



- High resolution fault injection both in time and space, 1-bit fault potentially leads to leakage of 121-bit key (@AES-128)

Attack Measures and Packaging Structures



Physical media

Passive attacks	Side channel attack (SCA)	EM, Photon, Volt., Current
Active attacks	Fault attack (FA)	EM, Laser, ESD, Glitch

Assembly structure

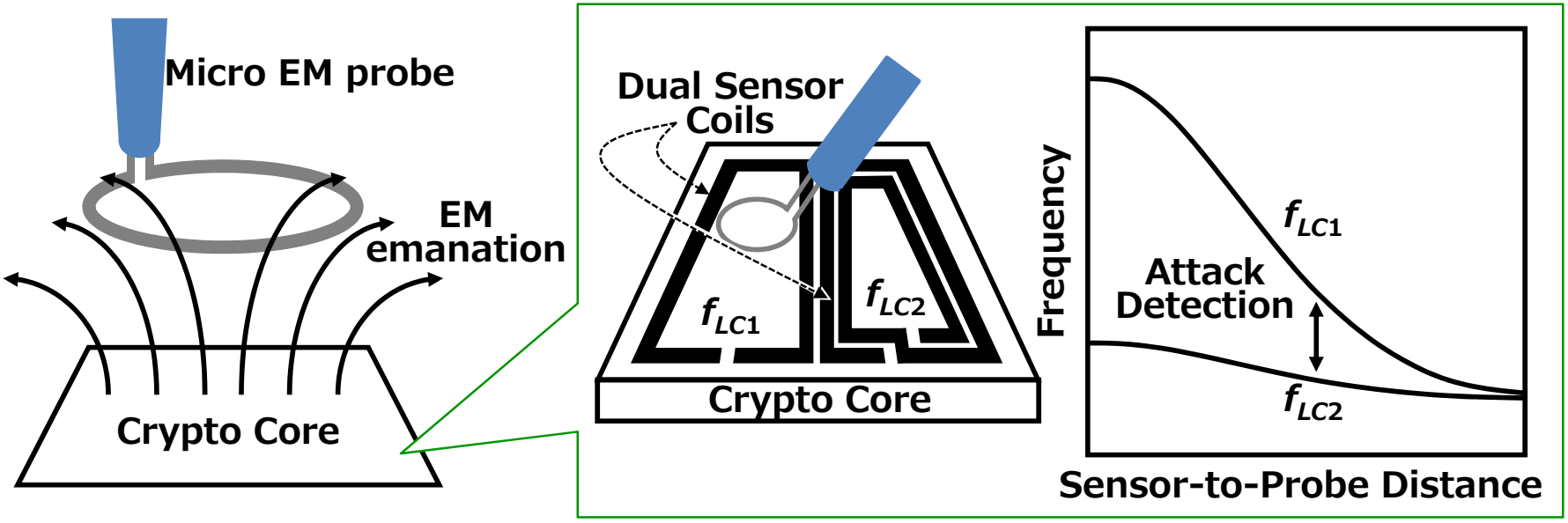
ASIC	Wire bonding, Flip chip	Plastic mold, CoB, etc.
FPGA	3D stacking, Fan out	Si interposer, MCM, etc.

Outline

Physical attacks

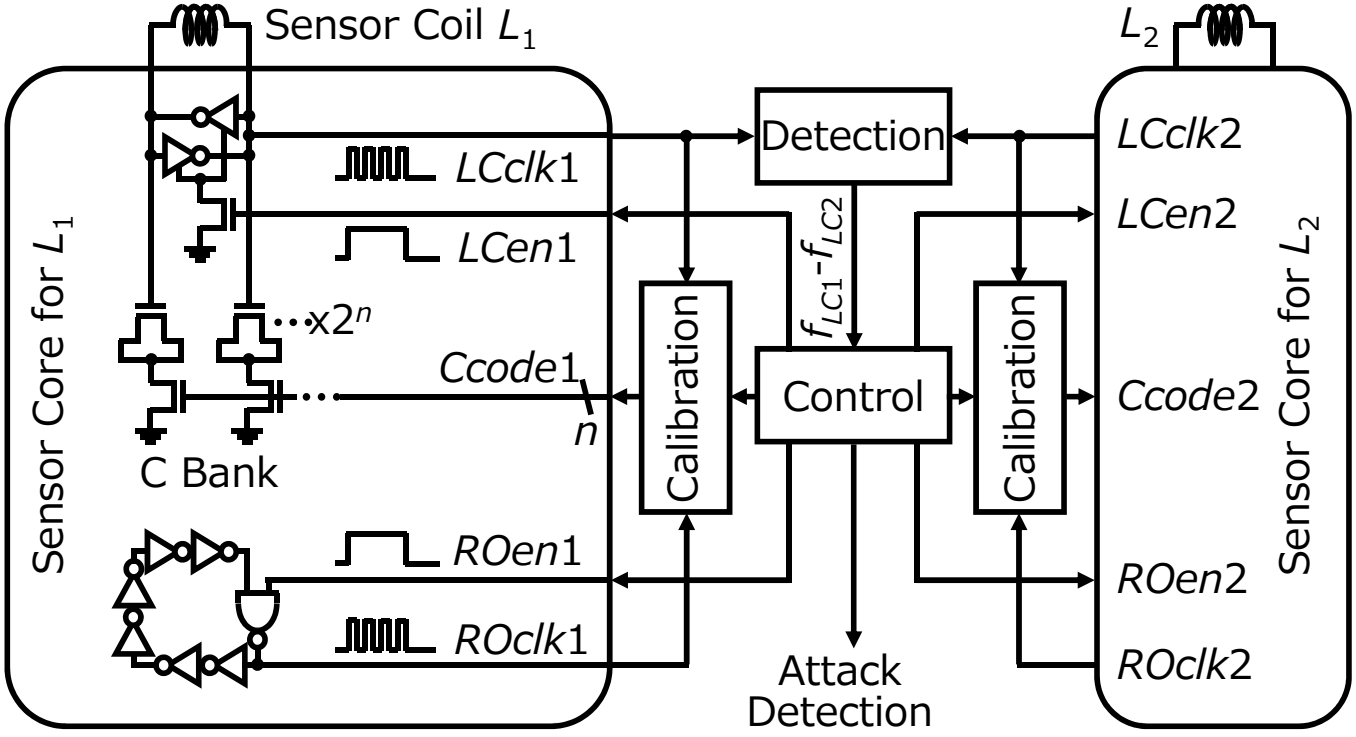
- On-chip security sensor circuits
- Simulation technique of side-channel leakage
- Conclusions

LEMA Attack Sensor



- EM observation impossible w/o disturbance to fields -- "*invasive attack*" is not true

LEMA Sensor Circuit Details



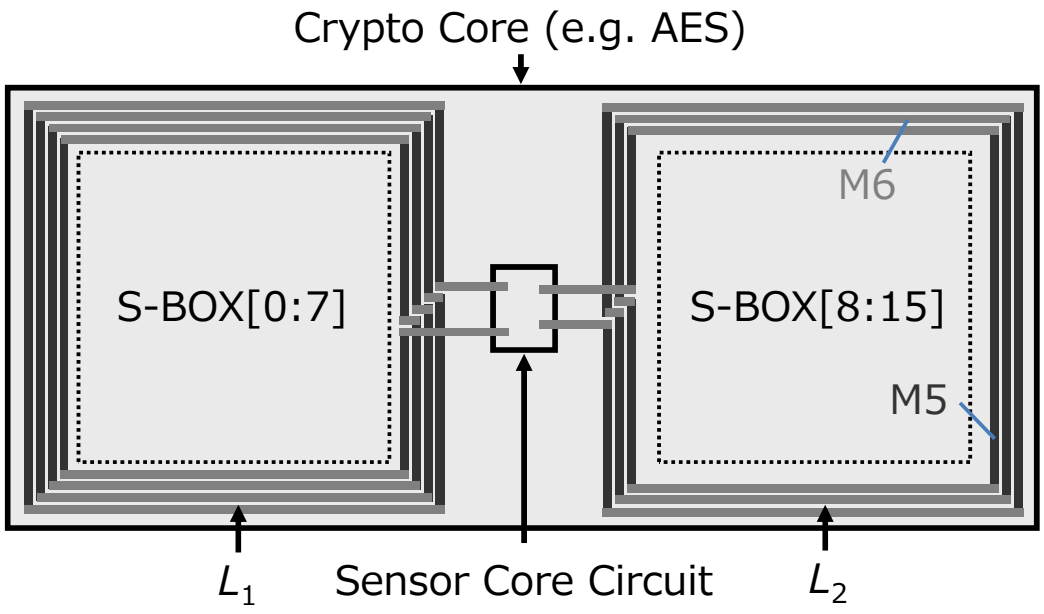
LEMA Sensor Features

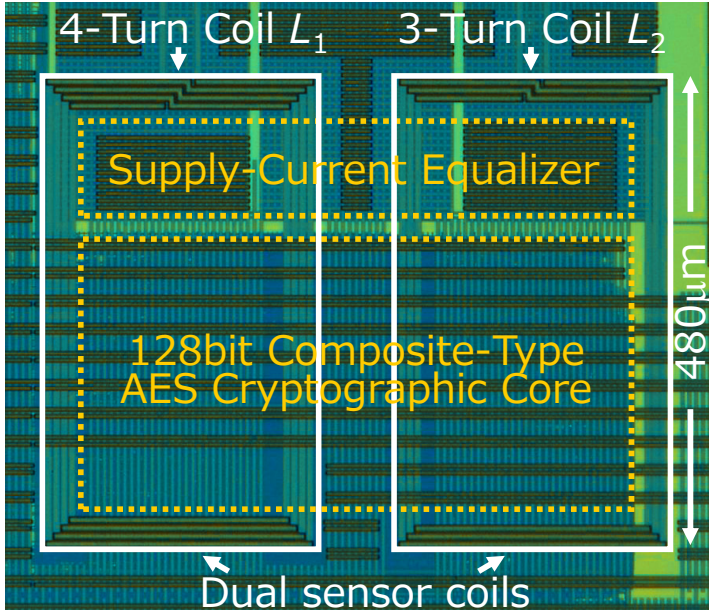
- **No frequency reference needed**
  - ✓ Robust and yet low-cost countermeasure
  - ✓ Different coil shapes further enhance robustness
  - ✓ Dual EM-probe attack almost impossible

- **Fully-digital oscillator-based sensor circuit**
  - ✓ Detection: 2 Racing Digital Counters (2RDC)
  - ✓ Calibration: Ring Oscillator (RO) + 2RDC

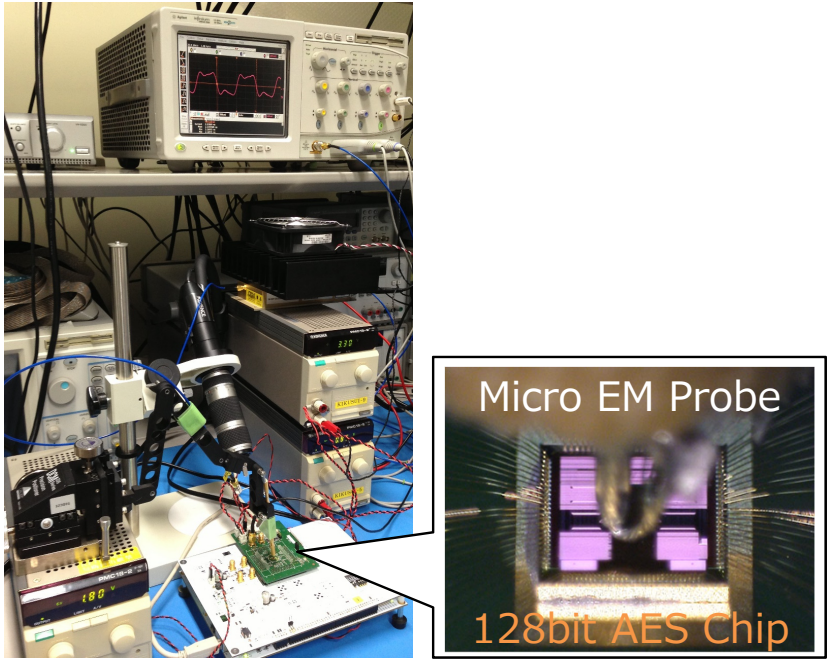
N. Homma *et al*., “Design Methodology and Validity Verification for a Reactive Countermeasure Against EM Attacks," IACR Journal of Cryptology, Dec. 2015.

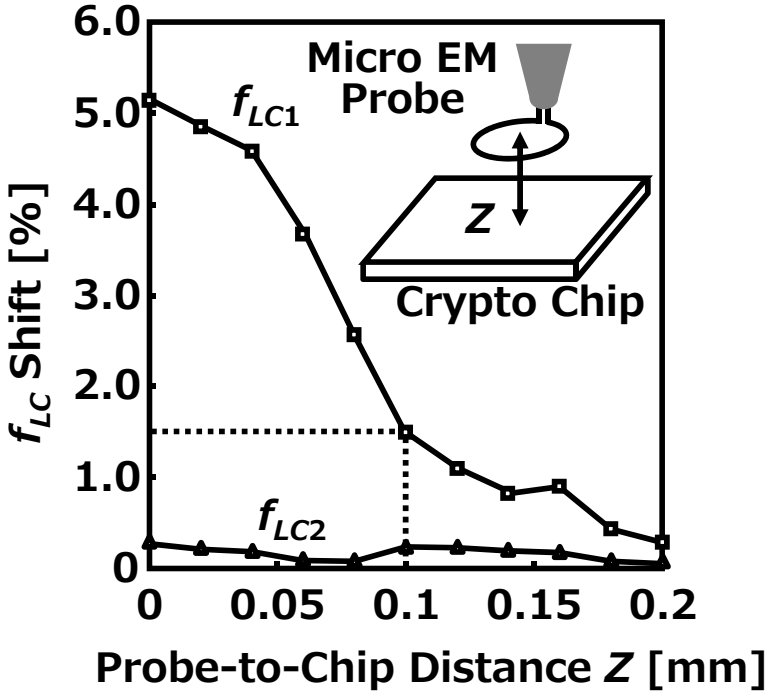
Design Example



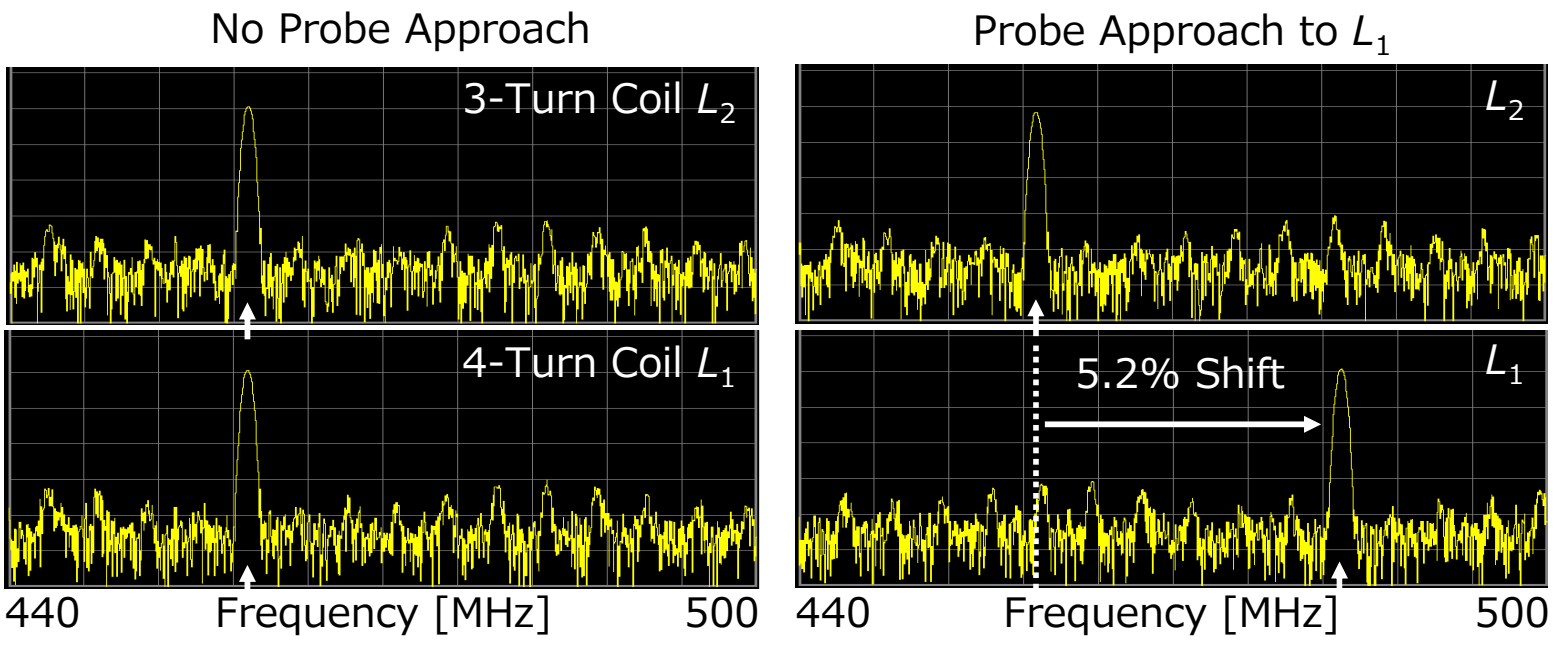


Detection Range Measurements



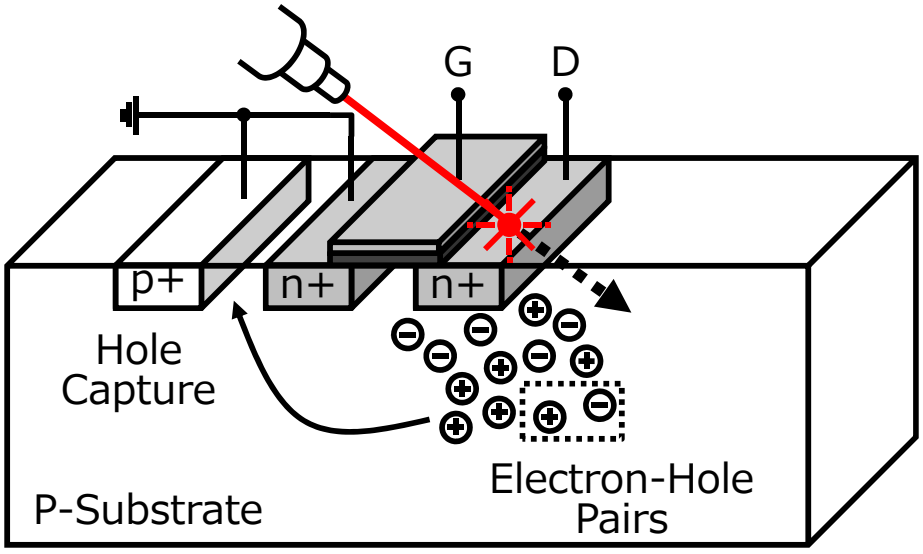


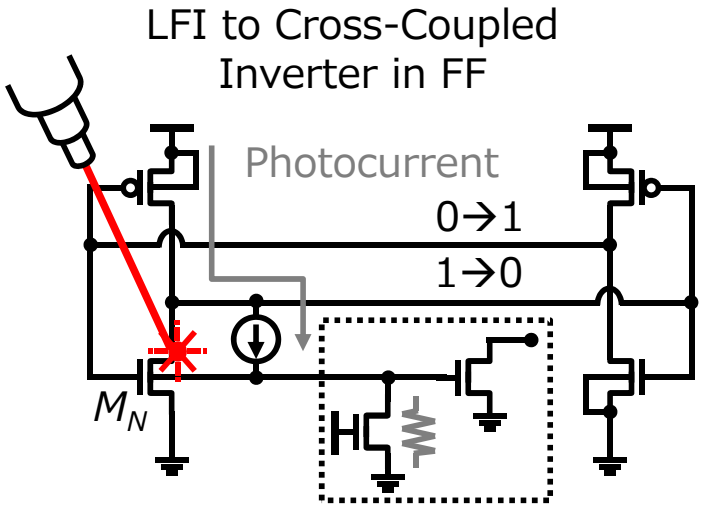
Demonstration of EM Probe Detection



1/4 Divided Clock Frequency Spectrum

LFI Attack Sensor

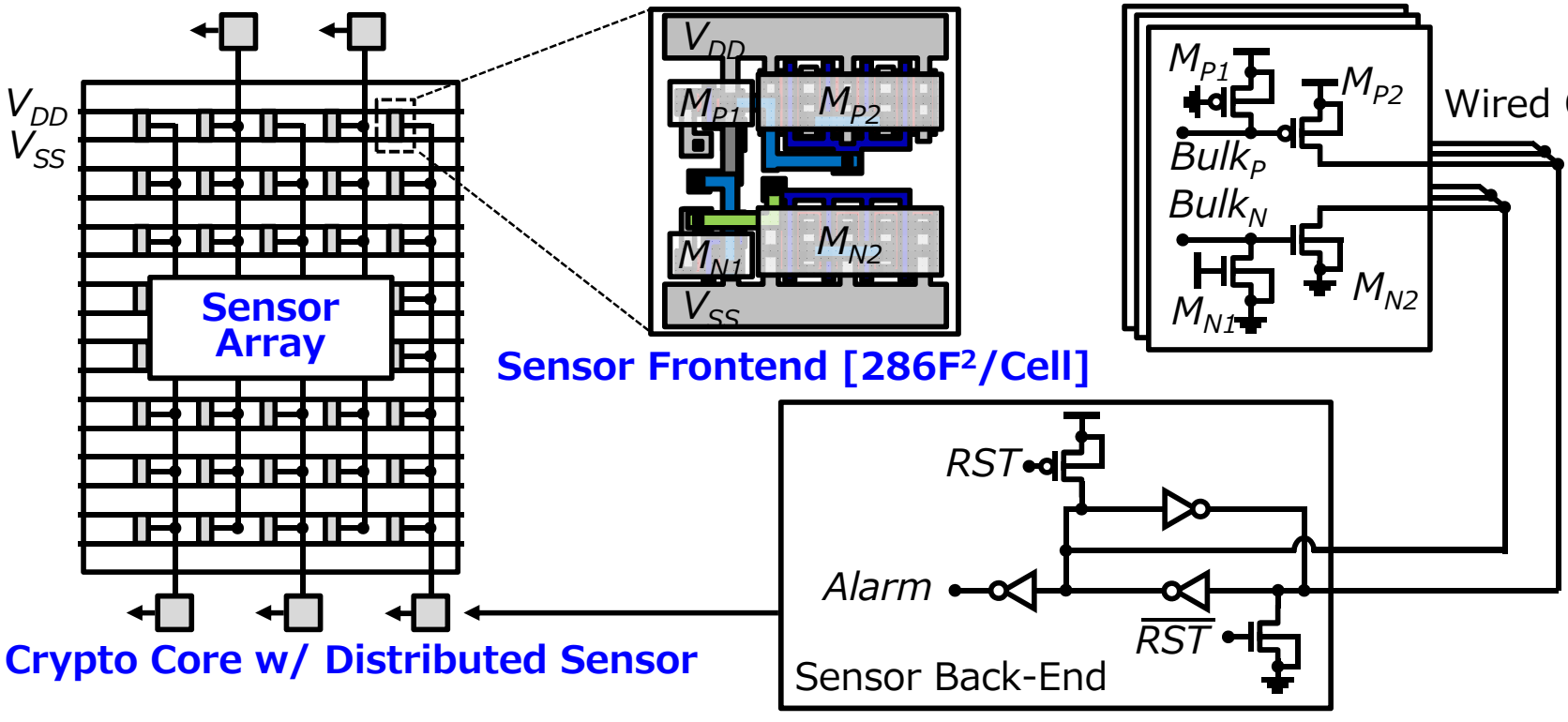




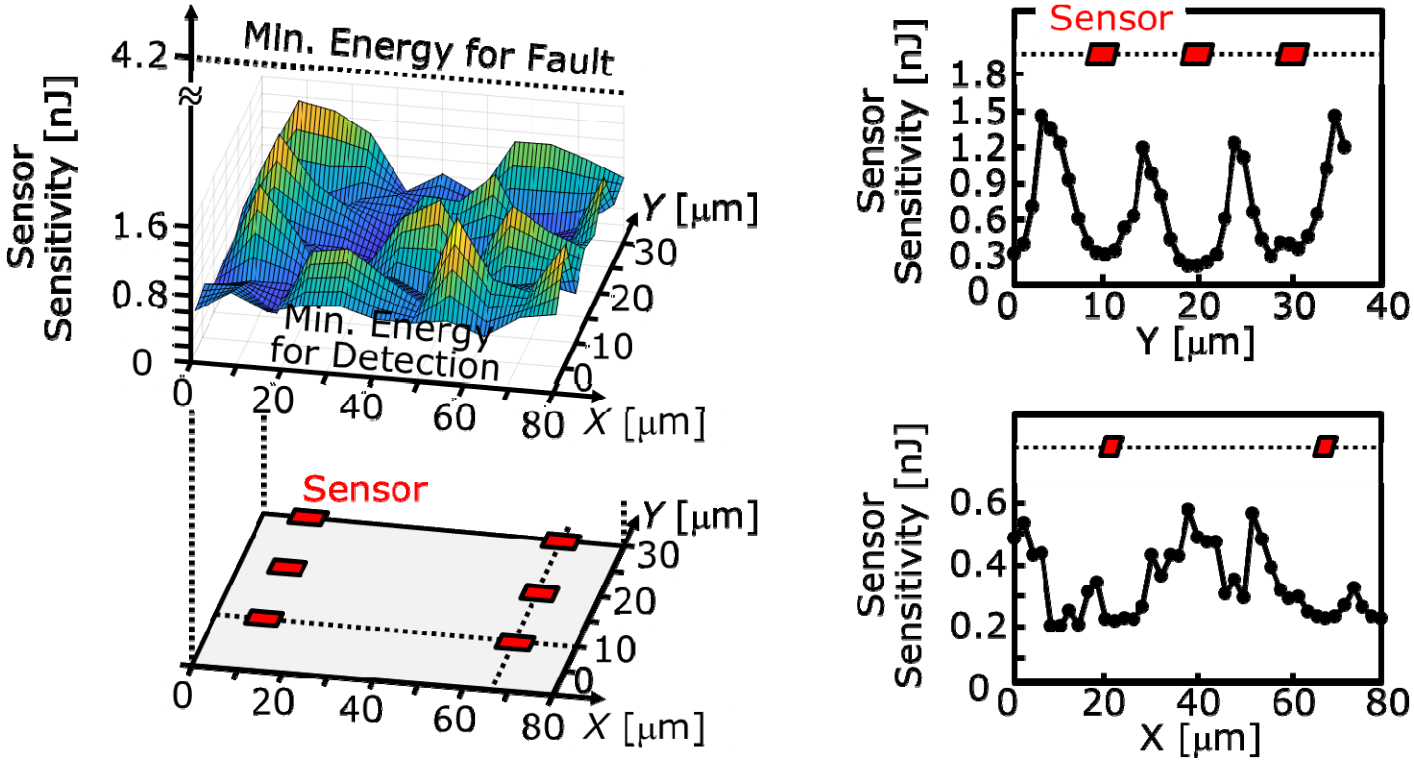
Bulk-Current Sensor*

*E. Neto *et al.*, "Using Bulk Built-in Current Sensors to Detect Soft Errors," IEEE Micro, 2006.

Distributed Bulk-Current Sensor



LFI Detection Measurements



*K. Matsuda *et al*., "A 286 F2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack on Cryptographic Processor," IEEE J. Solid-State Circuits, 2019.

LFI Detection Sensor Demonstration

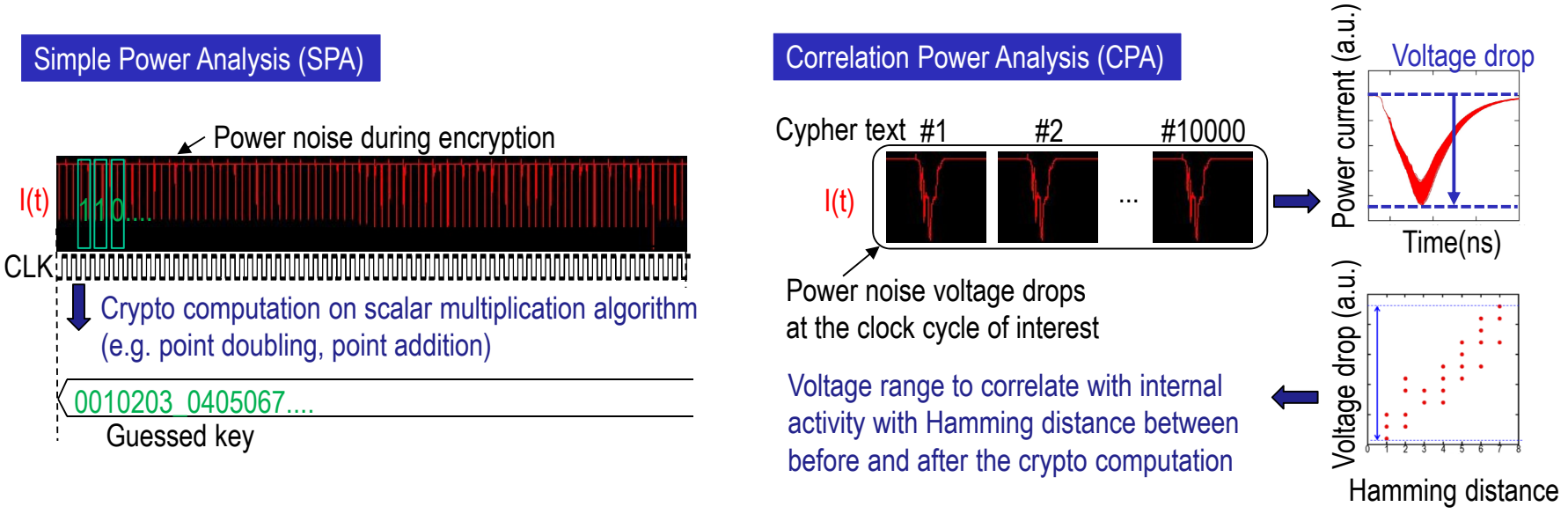
Outline

Physical attacks

On-chip security sensor circuits

- Simulation technique of side-channel leakage
- Conclusions

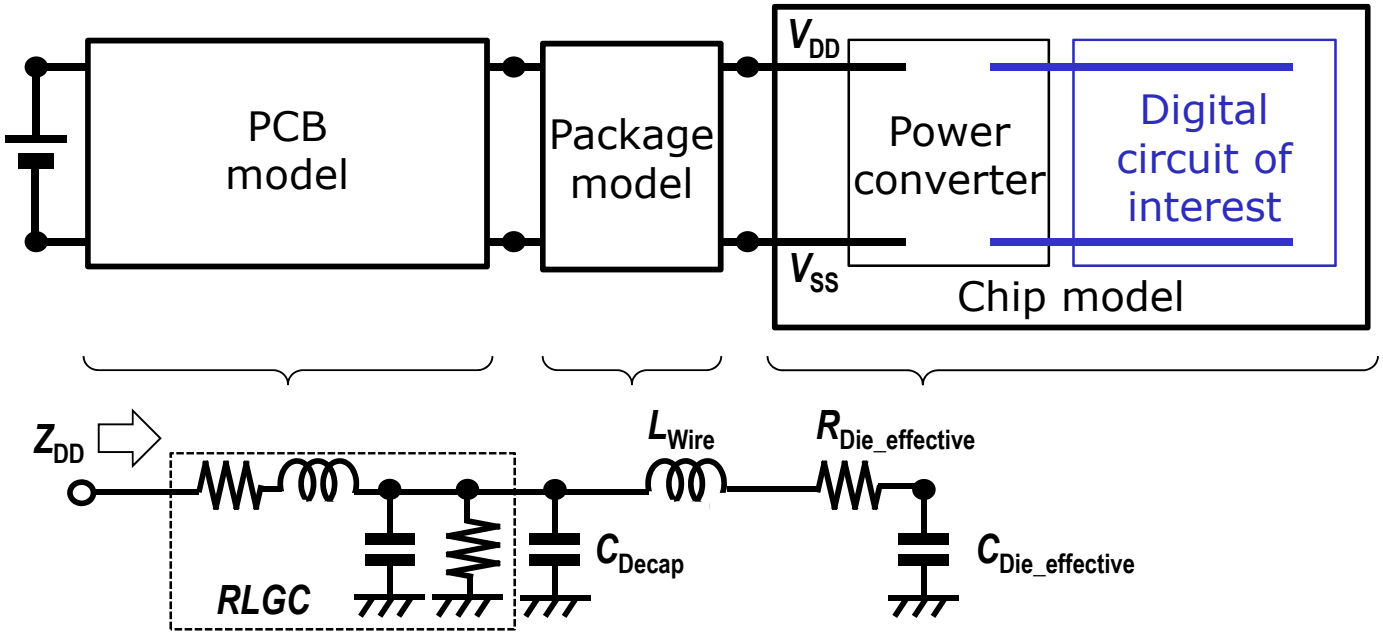
Side-Channel Analysis



- 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

CPS* Model for Diagnosis and Analysis

*Chip-Package-System board



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

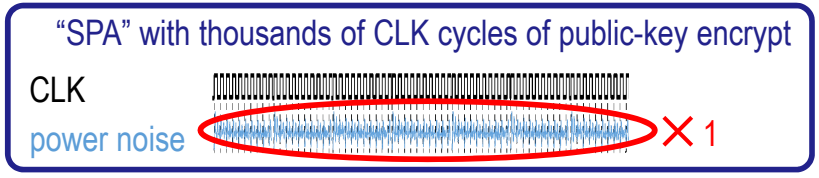
Challenges

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

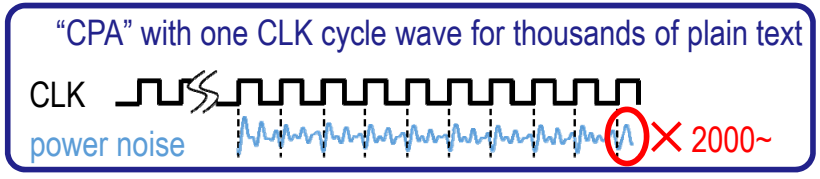
✓ Side-channel leakage is assessed on countermeasure crypto ICs in a design phase.

- 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.

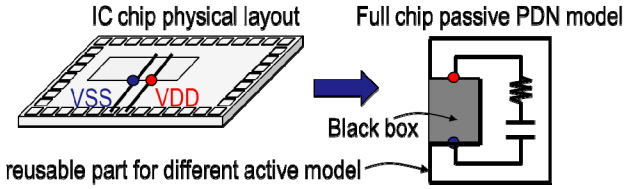


Chip Power Model of Crypto Engines

► Noise paths and noise sources

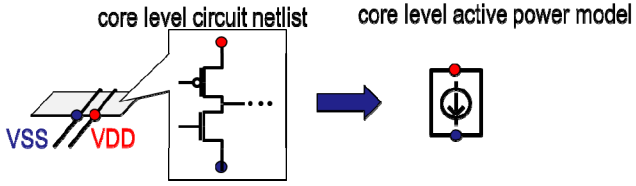
(1) Full chip PDN modeling

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



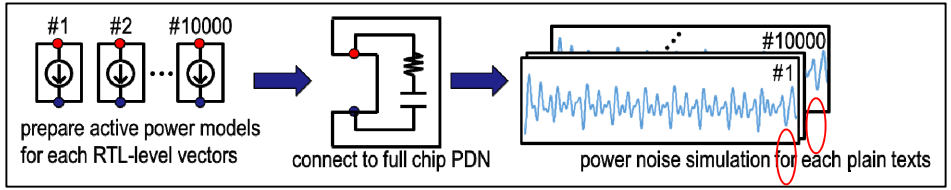
(2) Core level power modeling

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

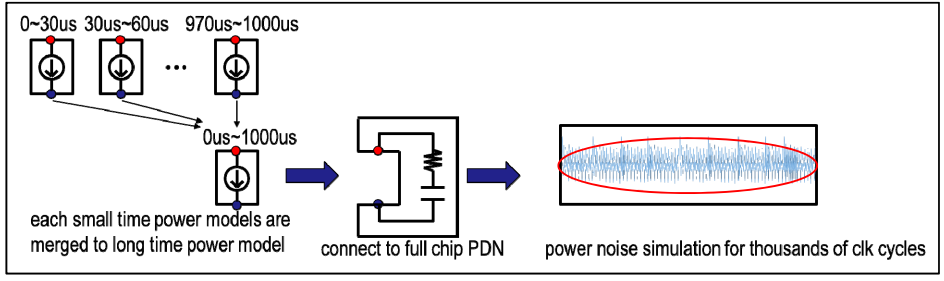


► Power-noise SC leakage simulation

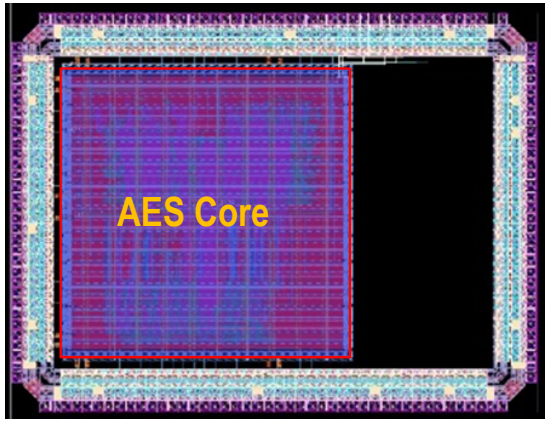
Case1: Private-key (e.g. AES) – power-noise waveforms for thousands of plain texts (#1~#10000) (different test vectors for short CLK cycles)

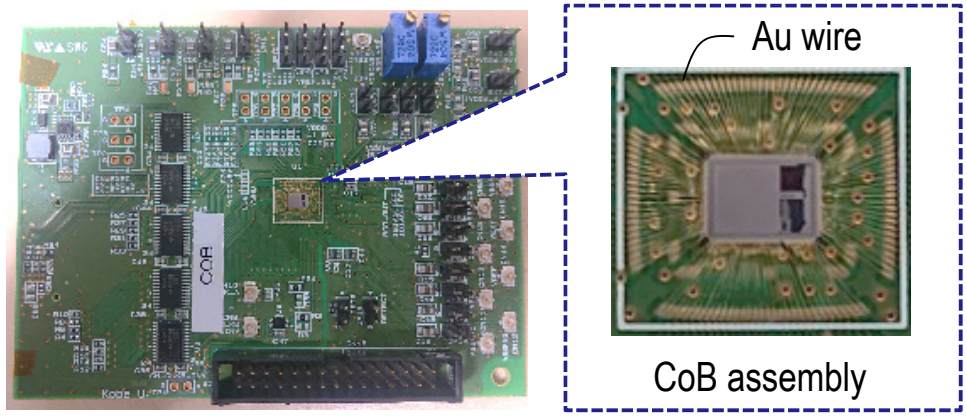


Case2: Public-key (e.g. RSA, DSA, ECDSA) -- a single power-noise waveform of several thousand CLK cycles



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

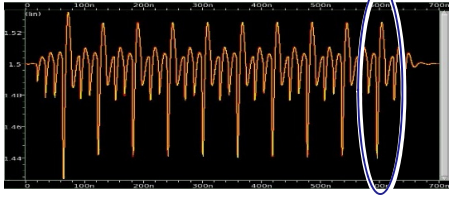
Power-Noise SC Leakage Simulation Results

- 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

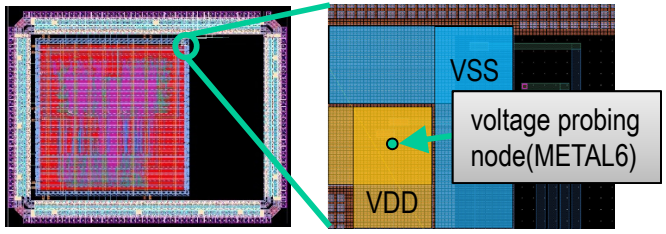


- Simulation cost evaluation
  - ✓ server: Intel Xeon CPU ES-2699 v4 (2.2GHz)

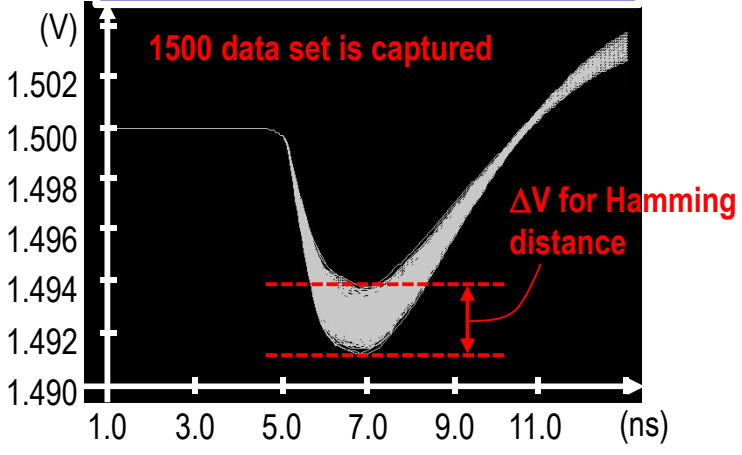
	Memory	Threads	CPU time
PDN modeling	2726MB	8	3.0 hour
power noise modeling	2348MB	8	8.5 min
power noise simulation	229MB	1	2.8 sec

} for a single waveform

Test Chip Layout

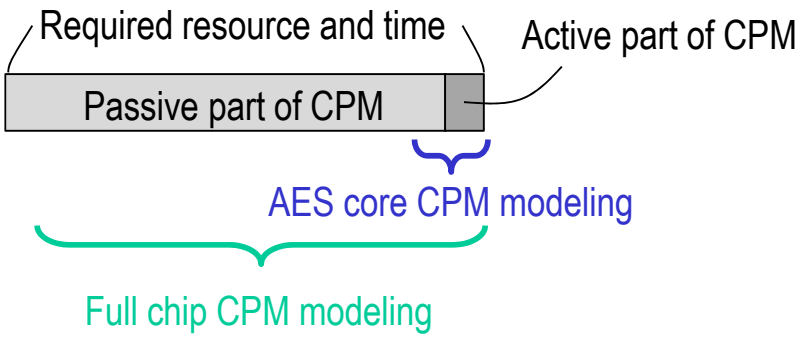


Simulated Power Noise Waveform

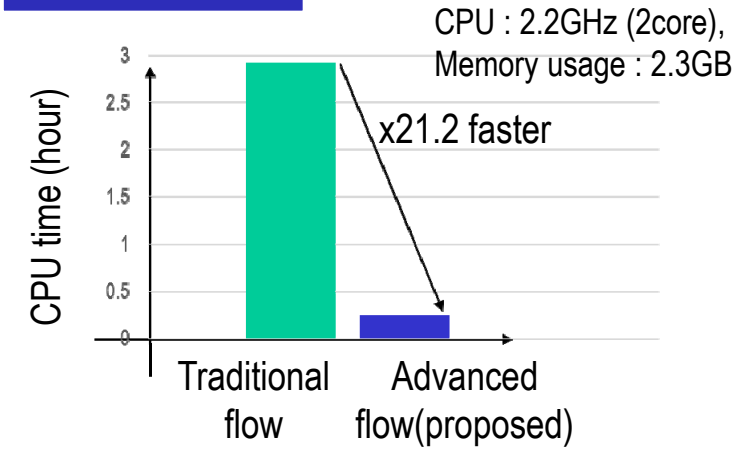


Acceleration of Simulation

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

- **Exploration of on-chip protection circuits against a variety of physical attacks in passive and active manner.**
- **Chip-package system board simulation technique toward the design of crypto circuits for resiliency, and also to design of attack sensors.**
- **Research spaces of on-chip protection against H/W Trojans.**

Acknowledgments: The authors would like to deeply thank Dr. Norman Chang for collaborative research works on SC leakage analysis, and Profs. Noriyuki Miura, Naofumi Homma, Yuichi Hayashi and Kazuo Sakiyama for scientific discussions.