2019.4.24 Japan-French Security Workshop, Kyoto

Deployment of EMC-Compliant IC Chip Techniques in Design for Hardware Security

Makoto Nagata

Graduate School of Science, Technology and Innovation,
Kobe University, Japan

nagata@cs.kobe-u.ac.jp
http://www.edu.kobe-u.ac.jp/stin-secafy/index.html

Hardware Security and Safety
Secafy
Kobe University

Kobe University, Japan

KOBE
UNIVERSITY
神戸大学
Kobe
Kyoto
Tokyo
北海道
青森
秋田
岩手
山形
宮城
新潟
福島
富山
石川
栃木
群馬
長野
茨城
福井
埼玉
岐阜
山梨
東京
千葉
鳥取
京都
滋賀
島根
岡山
愛知
静岡
神奈川
大阪
広島
山口
香川
奈良
三重
愛媛
徳島
福岡
高知
和歌山
佐賀
大分
長崎
熊本
宮崎
鹿児島

- Around 16,000 students (1,200 oversea students), 1,600 teaching members.

Research lab. overview

Hardware Security and Safety
Secafy

- 19 students (5 under graduate, 10 master course, 4 doctoral course), 8 staffs (including professors/guest professors.)
- Design methodologies of IC chips and systems for hardware security and safety – "**Secafy**," with deep background of analog, digital, mixed-signal IC techniques.

FR-JP partnership

Creating a safe and robust digitally-connected world

Professors ***Makoto Nagata*** *and* ***Jean-Luc Danger*** *and* ***Associate Professor Noriyuki Miura*** *are united in their belief that the root of trust in the safety and security of electronic systems lies in robustly designed hardware. Here they describe the research goals of their long-term collaboration*

Prof Makoto Nagata

Prof Jean-Luc Danger

AP Noriyuki Miura

Could you begin with a brief description of your backgrounds and research interests?

the Secafy Laboratory at Kobe University?

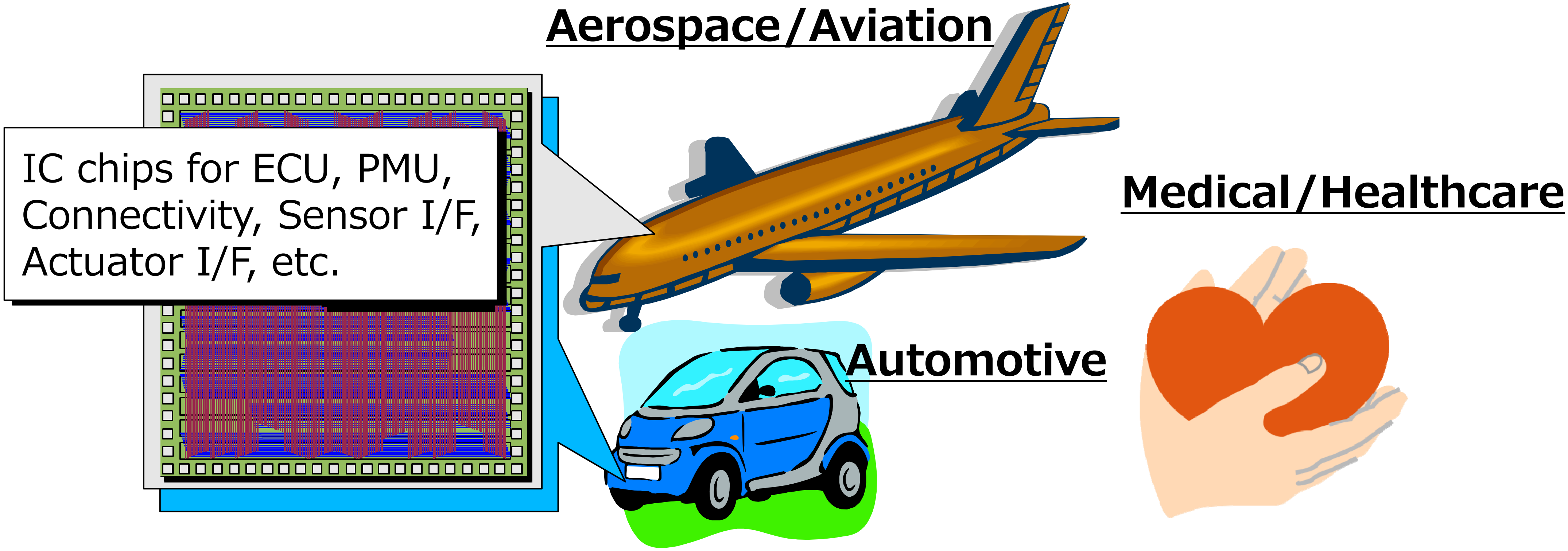
MN: Secafy stands for hardware security and safety and we believe it is vital to design these principles into hardware from the very beginning. I see hardware as being the root of trust on which the security of networks can be built. We are focused on measuring the susceptibility of integrated circuits (ICs)

connectivity. However, all practical hardware is exposed to unseen radio waves, which can sometimes affect the performance of a chip, particularly in VLSI. Therefore, it is important to ensure devices are robust and continue to perform well even in harsh environmental conditions.

JLD: Cyber attacks are increasingly common.

Makoto Nagata, Jean-Luc Danger, Noriyuki Miura, "***Creating a Safe and Robust Digitally-Connected World***," Impact, Vol. 2018, No. 11, pp. 22-25, Dec. 2018.
DOI:10.21820/23987073.2018.11.22

IC chips and systems in critical applications



IC chips for ECU, PMU, Connectivity, Sensor I/F, Actuator I/F, etc.

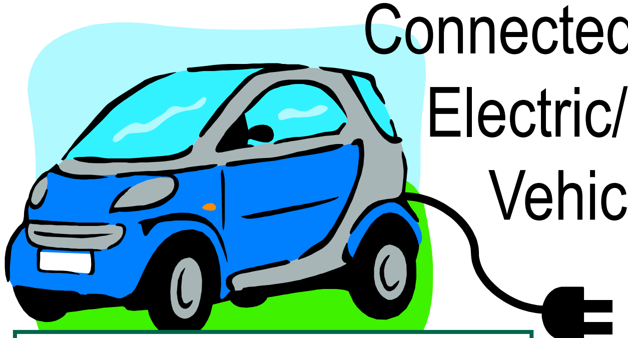
Aerospace/Aviation

Medical/Healthcare

Automotive

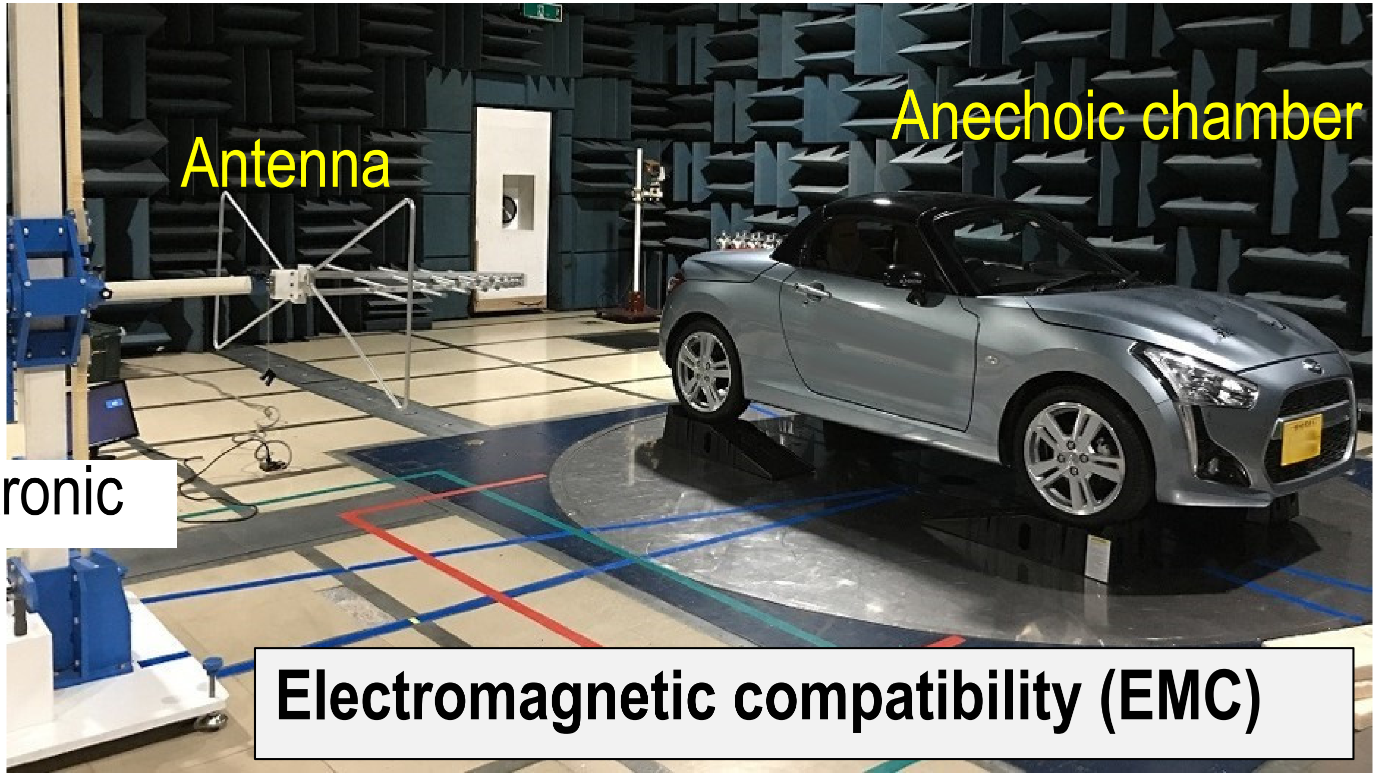
- **Hardware security to be assessed in productization or assured by design of IC chips and electronics assembly for critical applications**
  - ✓ Security performance (Cryptography, Digital signature, Attack resistance, etc.)
  - ✓ Authenticity, Validation, Authentication of IC chips
  - ✓ Side-channel leakage suppression, Fault injection tolerance

EMC as automotive standards



Connected Electric/Electronic Vehicle

EMC = EMI + EMS



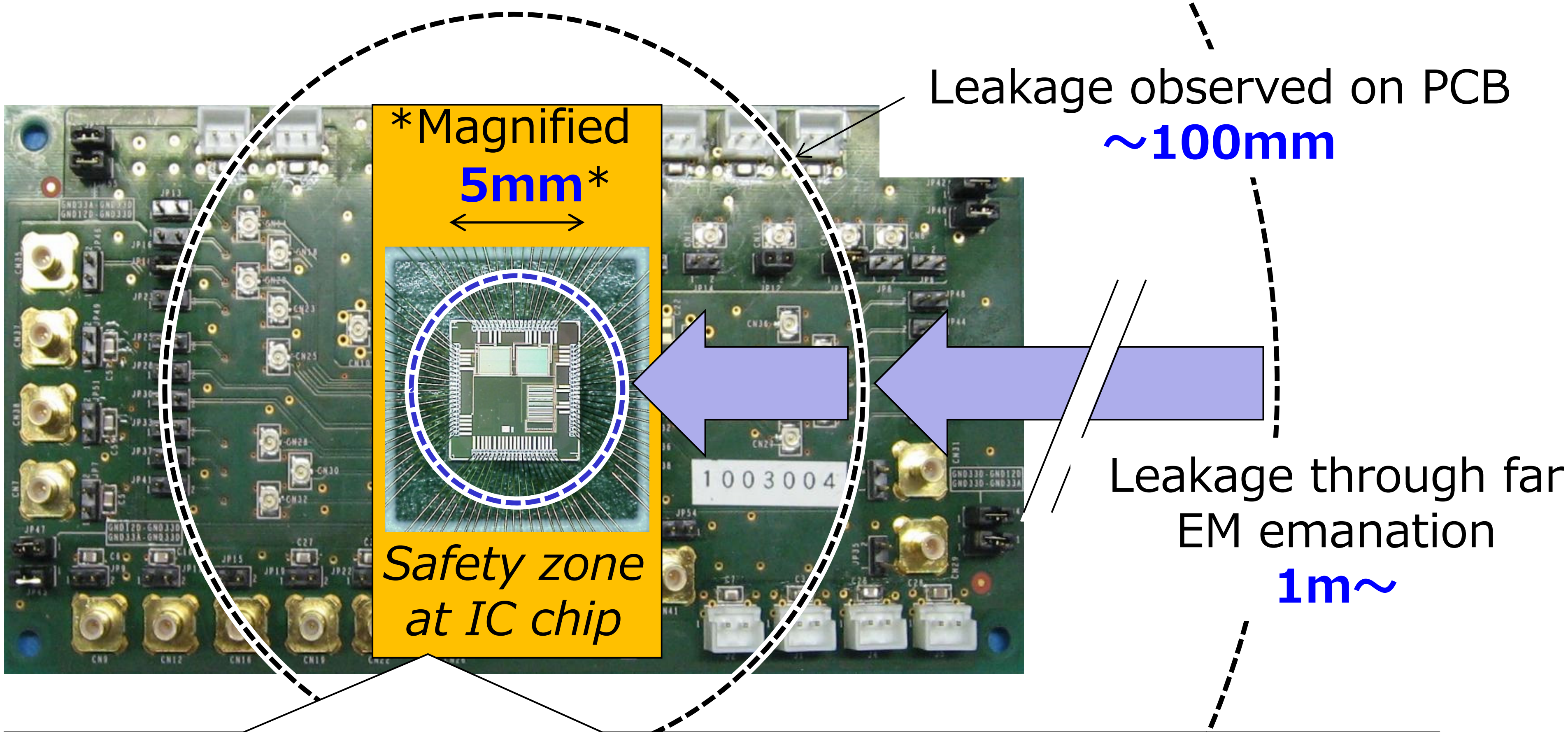
Electromagnetic compatibility (EMC)

ECE-R10* (Rev. 5 in 2014)

- ▶ Immunity to radiated and conducted disturbances (EMS)
- ▶ Control of unwanted radiated and conducted emissions (EMI)

*The United Nations Economic Commission for Europe

Physical attacks in dimensions



Magnified 5mm

Safety zone at IC chip

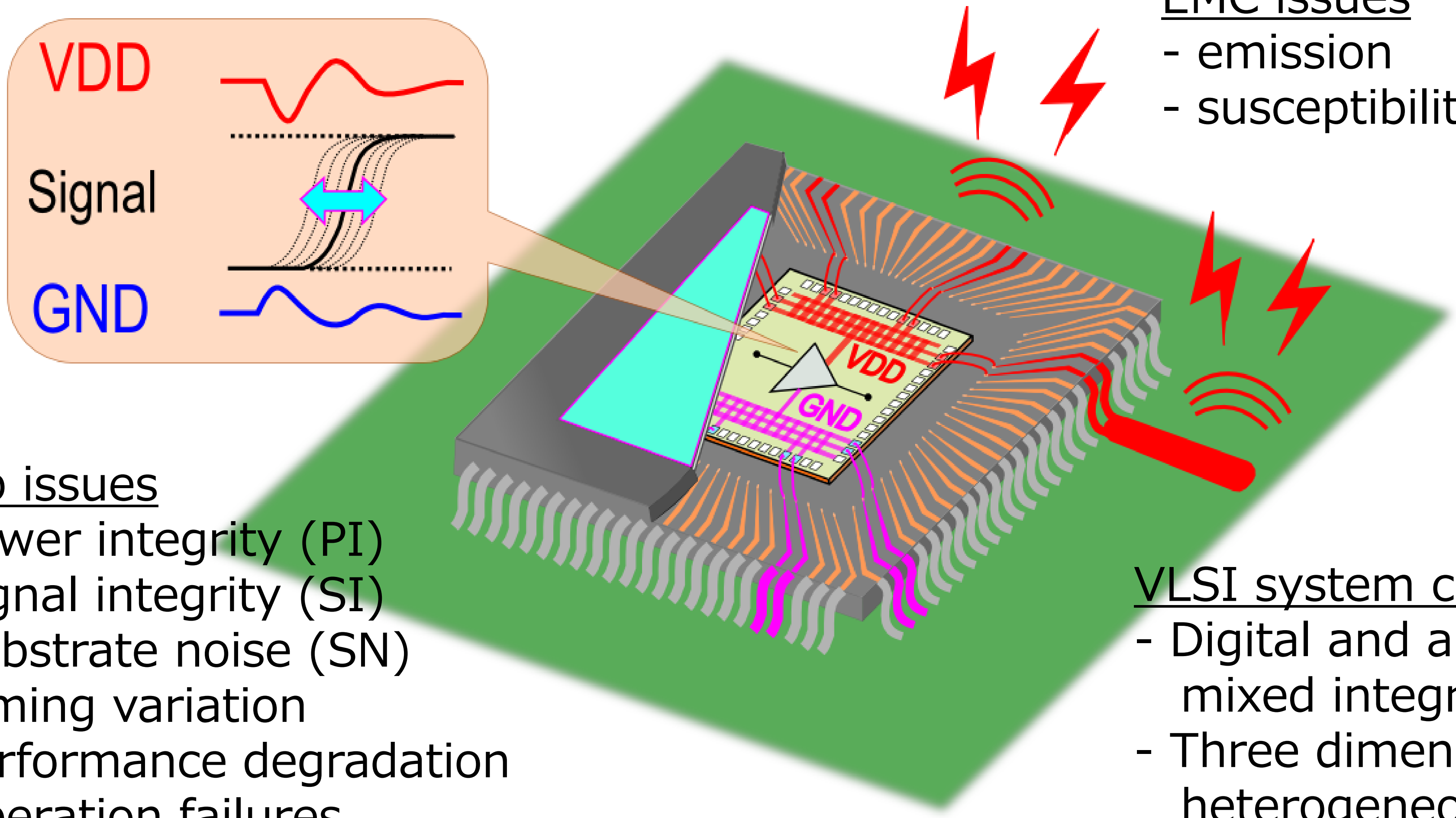
Leakage observed on PCB ~100mm

Leakage through far EM emanation 1m~

Objective: Securing crypto-engines in the areas of ICs

- Physical dimensions at board, package and chip levels.
- EM radiation, EM sensing, EM injection

Power noise problems in IC chip



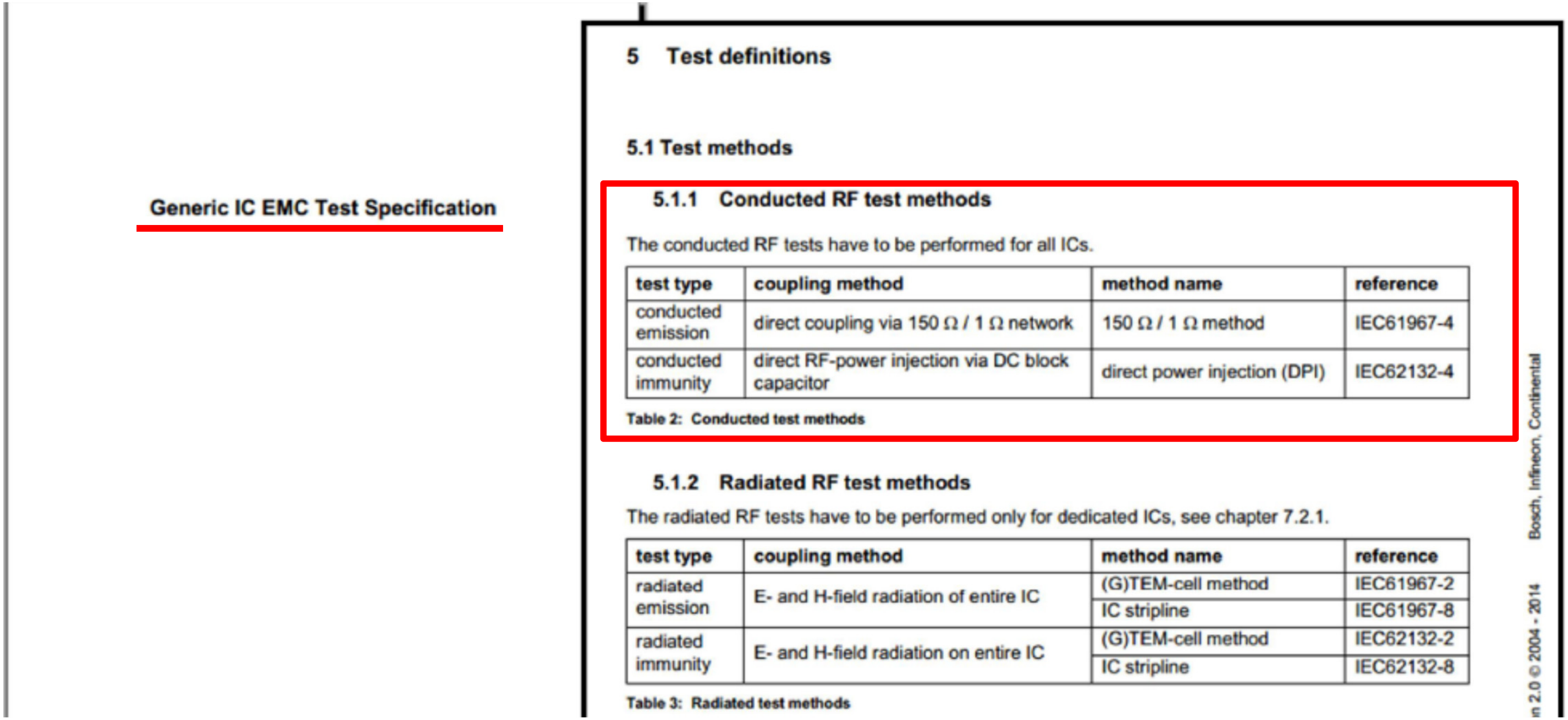
EMC issues
- emission
- susceptibility

Chip issues
- Power integrity (PI)
- Signal integrity (SI)
- Substrate noise (SN)
- Timing variation
- Performance degradation
- Operation failures

VLSI system concerns
- Digital and analog/RF mixed integration
- Three dimensional (3D) heterogeneous integration

▶ Relevant to side-channel (SC) concerns in cryptographic chips

IC chip level EMC test standards



Generic IC EMC Test Specification

5 Test definitions

5.1 Test methods

5.1.1 Conducted RF test methods

The conducted RF tests have to be performed for all ICs.

test type	coupling method	method name	reference
conducted emission	direct coupling via 150 Ω / 1 Ω network	150 Ω / 1 Ω method	IEC61967-4
conducted immunity	direct RF-power injection via DC block capacitor	direct power injection (DPI)	IEC62132-4

Table 2: Conducted test methods

5.1.2 Radiated RF test methods

The radiated RF tests have to be performed only for dedicated ICs, see chapter 7.2.1.

test type	coupling method	method name	reference
radiated emission	E- and H-field radiation of entire IC	(G)TEM-cell method	IEC61967-2
		IC stripline	IEC61967-8
radiated immunity	E- and H-field radiation on entire IC	(G)TEM-cell method	IEC62132-2
		IC stripline	IEC62132-8

Table 3: Radiated test methods

n 2.0 © 2004 - 2014 Bosch, Infineon, Continental

- IEC61967-6: Magnetic probe method, measurement of IC chip for conducted EM emission in 150 kHz – 1 GHz.

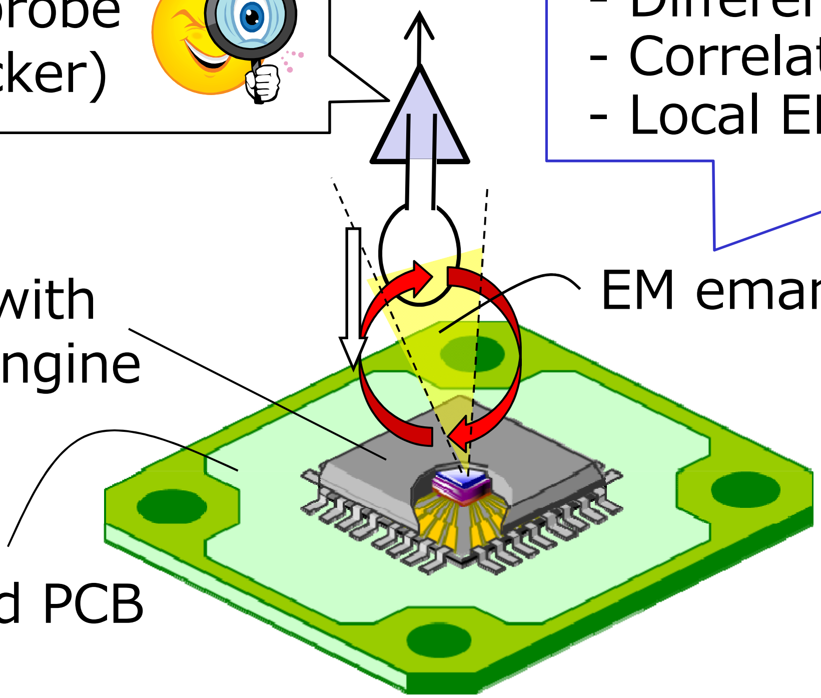
EMI

- IEC62132-4: Direct RF power injection method, measurement of IC chip for conducted EM immunity in 150 kHz – 1 GHz.

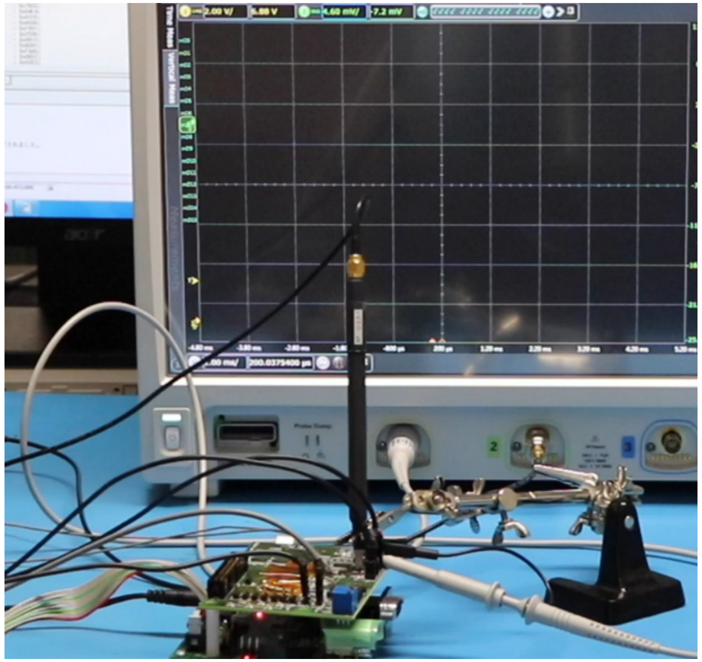
EMS

Side channel information leakage

μEM probe
(Attacker)

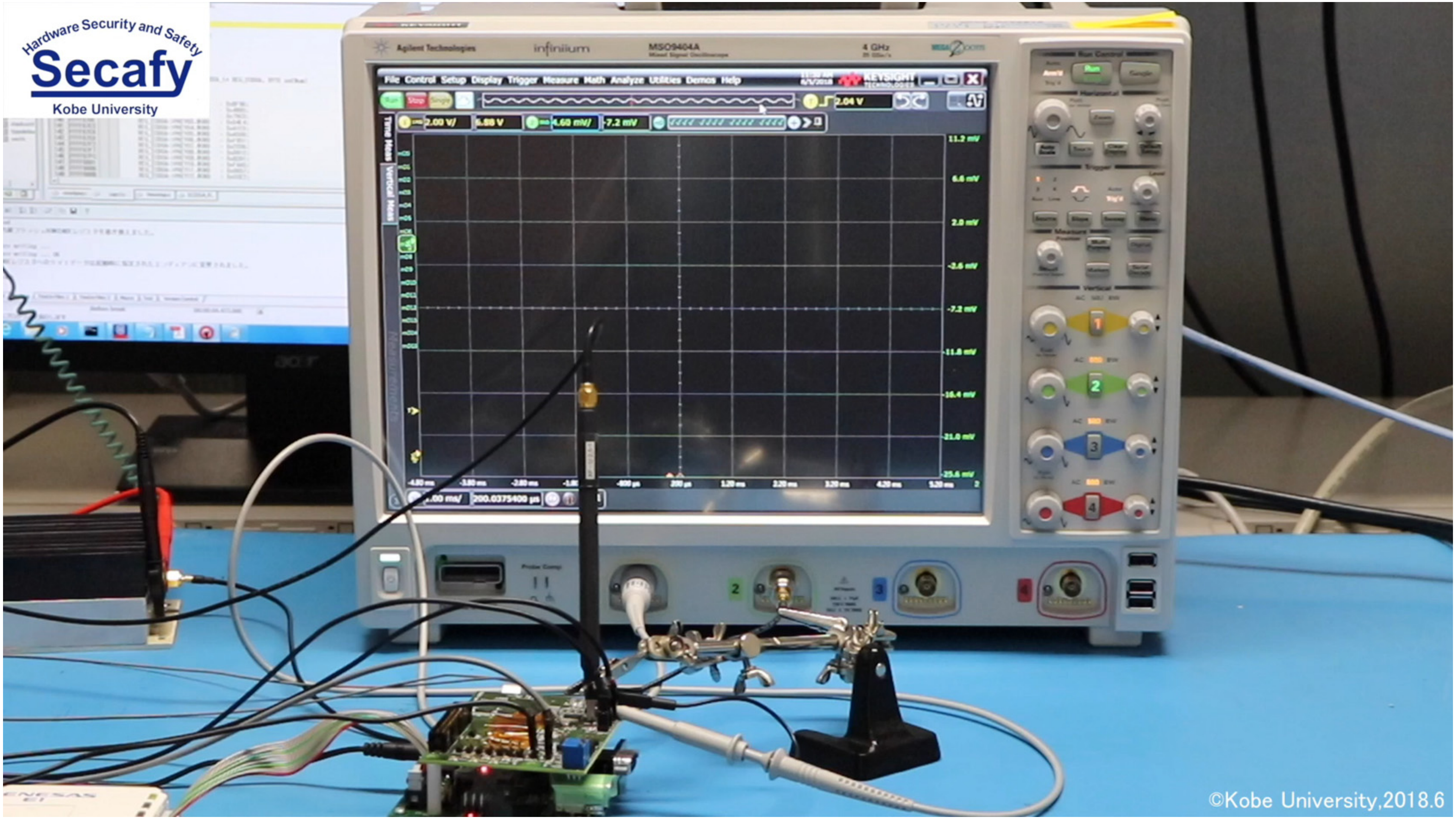


Analysis models (Attacker)
- Simple power analysis (SPA)
- Differential power analysis (DPA)
- Correlation power analysis (CPA)
- Local EM analysis (LEMA)



- Digital data paths are main channels of cryptographic processing.
- Power current consumption and electromagnetic (EM) emanation are potential side channels that might deliver secret information.

Side channel information leakage



©Kobe University,2018.6

Relevance between EMC and HWS

EMI

- ▶Electromagnetic emission →Side channel leakage (passive information leakage)
- ▶EMI analysis → SCA analysis

EMS

- ▶Electromagnetic immunity → Fault injection (active information leakage)
- ▶EMS analysis → Fault analysis

⇨ **In-depth understandings of IC-chip level EMC, toward the quality design of IC chips for HWS**

Deployment of EMC techs. for HWS

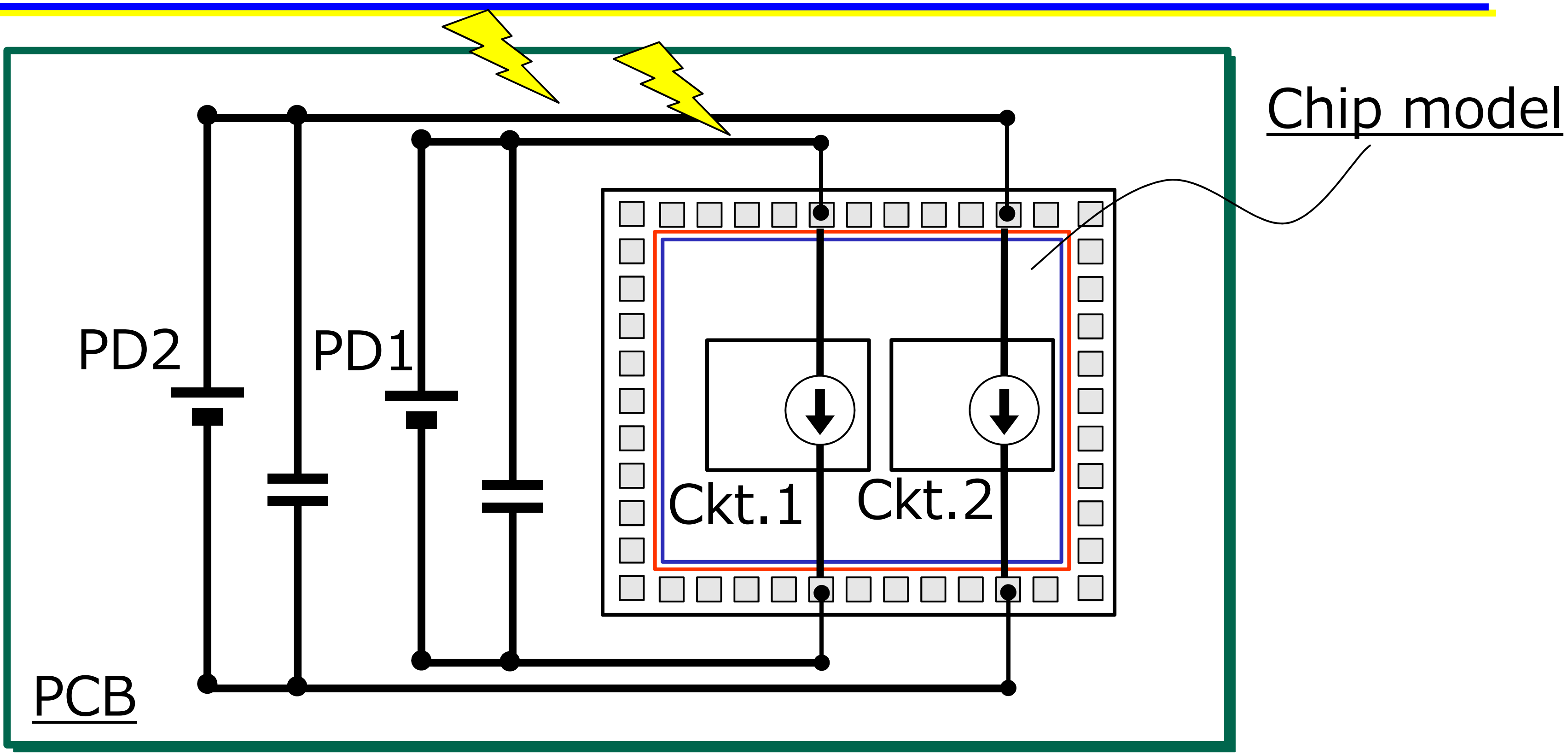
EMI

- ▶Electromagnetic emission →Side channel leakage (passive information leakage)
- ▶EMI analysis → SCA analysis
- ▶EMI reduction --?-- SC leakage suppression

EMS

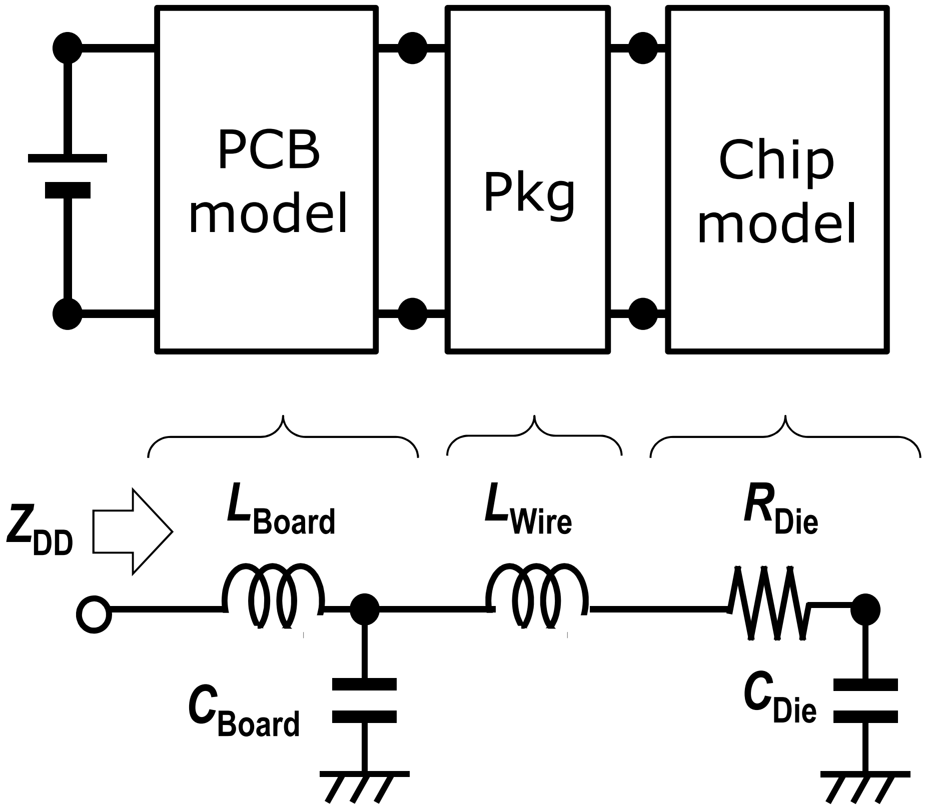
- ▶Electromagnetic immunity → Fault injection (active information leakage)
- ▶EMS analysis → Fault analysis
- ▶EMS resiliency --?-- Fault resiliency

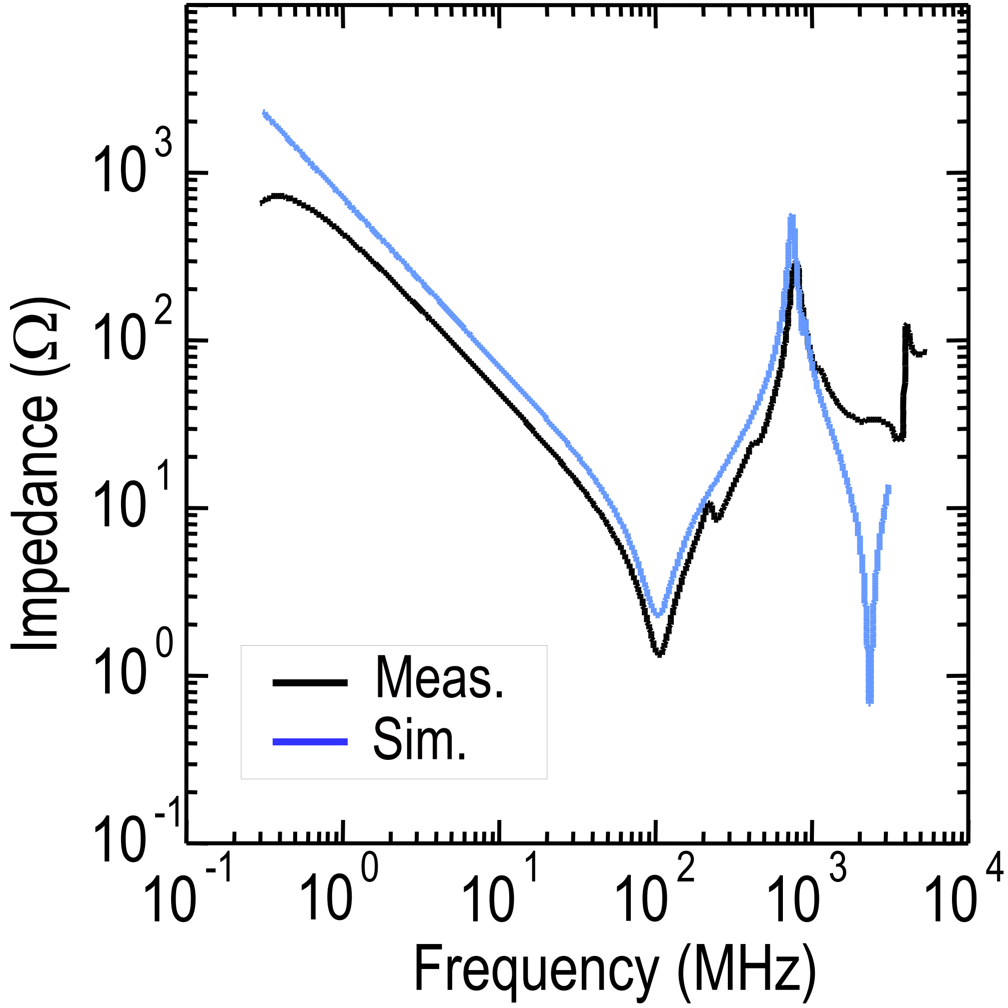
EMI simulation framework



Passive part of EMI models	Active part of EMI models	Challenges
S-parameters or equivalent circuits of PCB, package and IC chip	Power current models of active circuits with multiple power domains (PDs)	Scenarios to properly activate crypto circuits for EMI simulation toward HWS

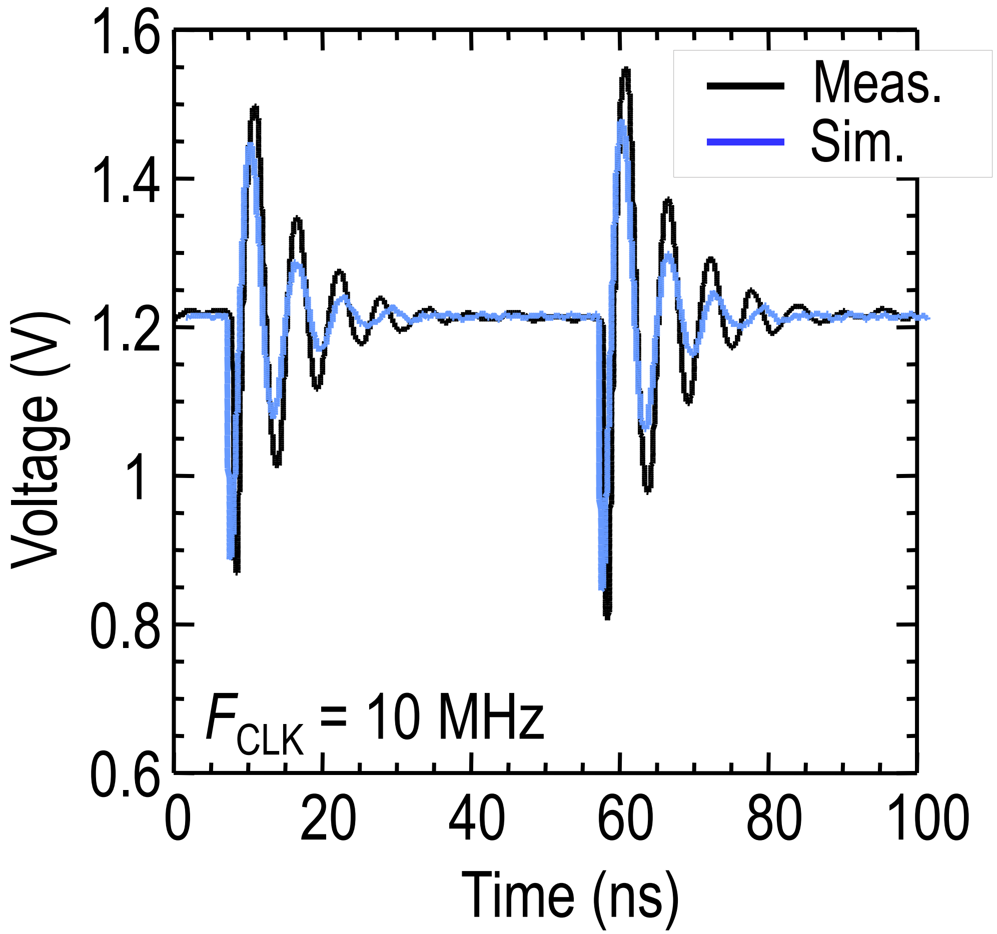
PDN impedance model

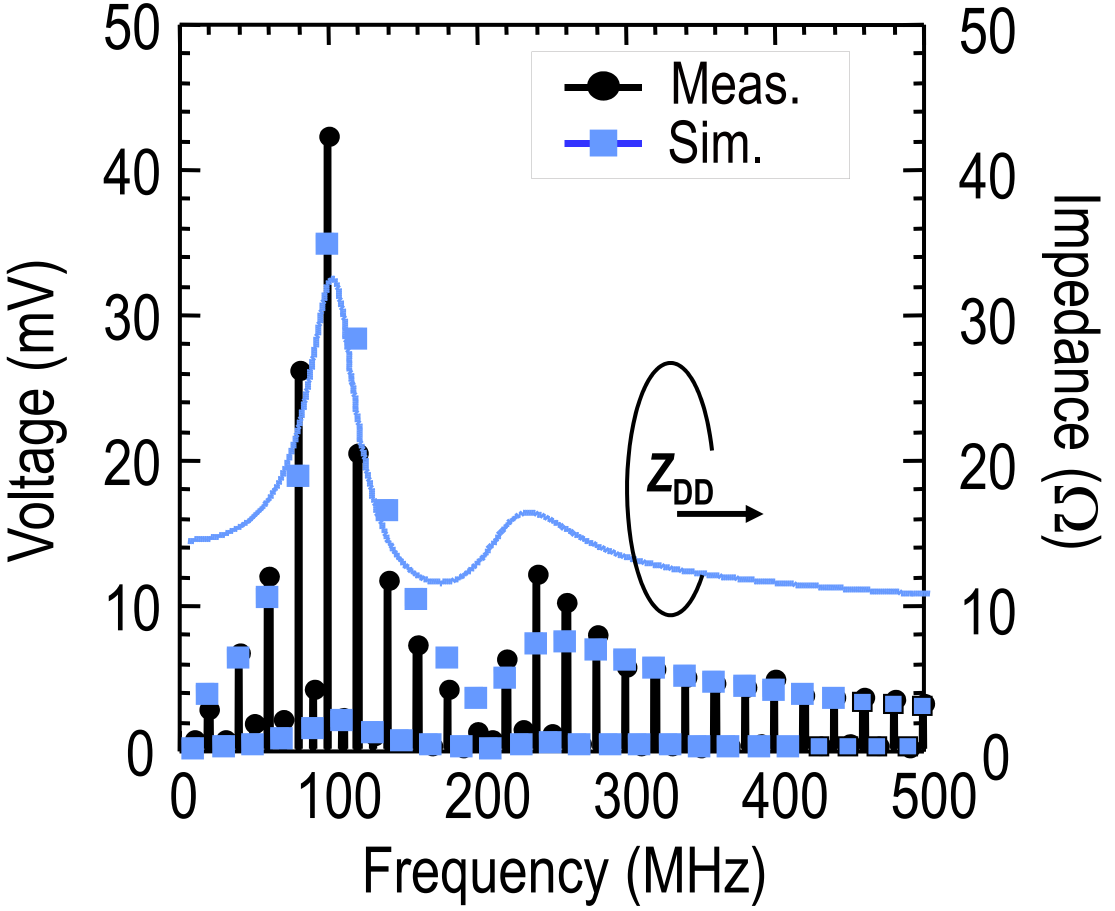




- C-P-B integrated passive model, capturing AC impedance seen from power source side (VDD).

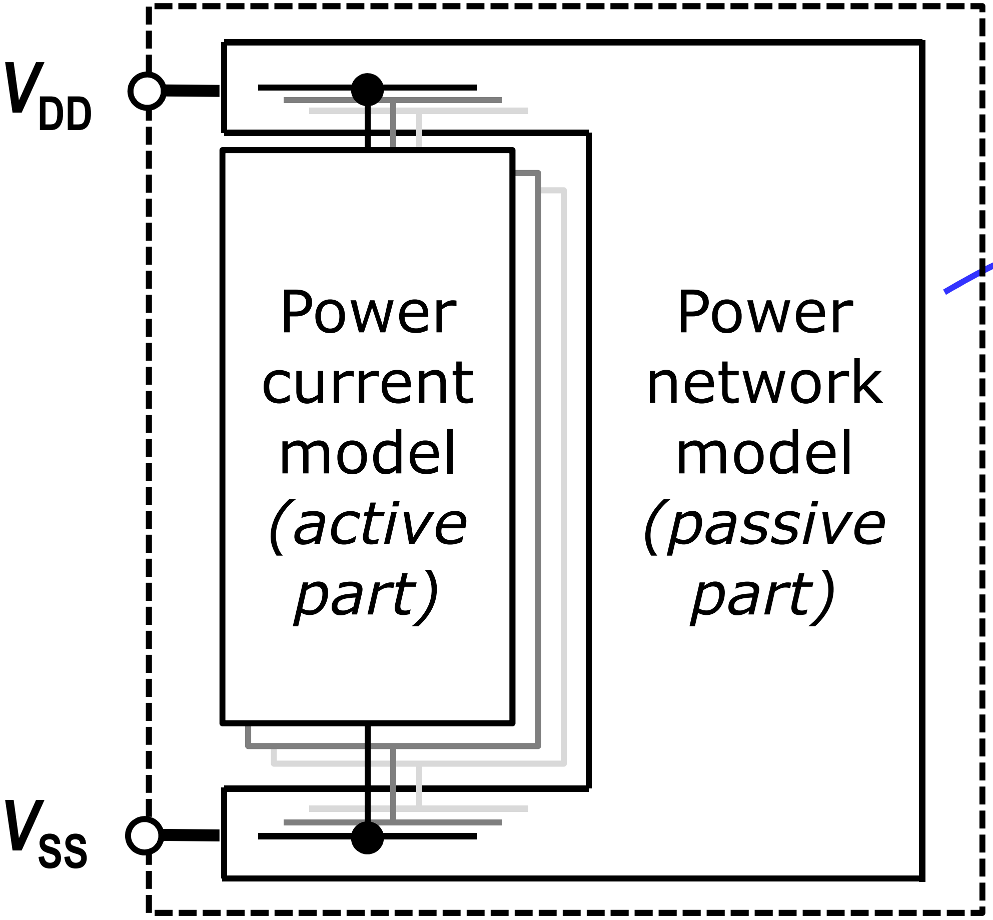
Power noise: C-P-B active interaction





- Power current (I_{DD}, active part of IC) interacts with PDN AC impedance.
- C-P-B integrated models for power noise in IC chips and PCB.

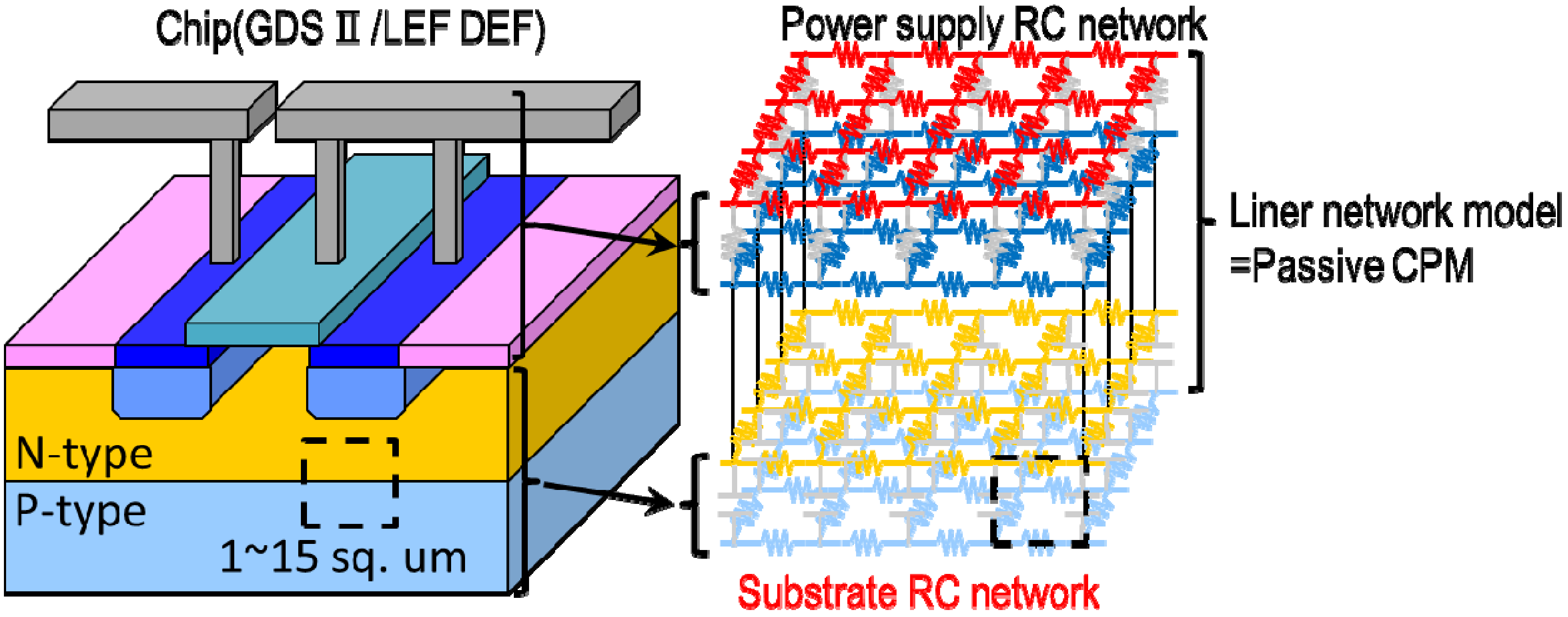
Chip power model


V_{DD}
V_{SS}
Power current model *(active part)*
Power network model *(passive part)*

Chip power model (CPM) of either "digital circuit block" or "whole chip"

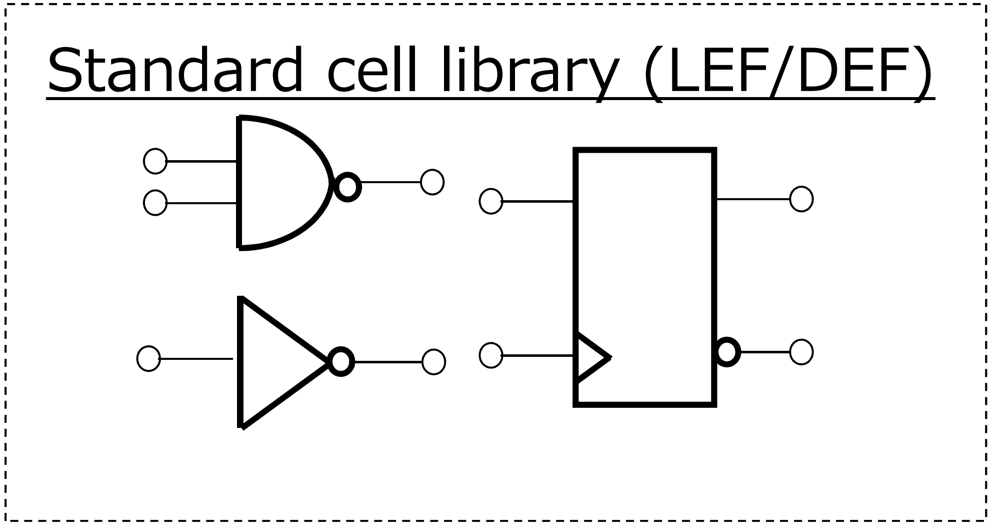
- CPM -- A power delivery network involving multiple power current models.

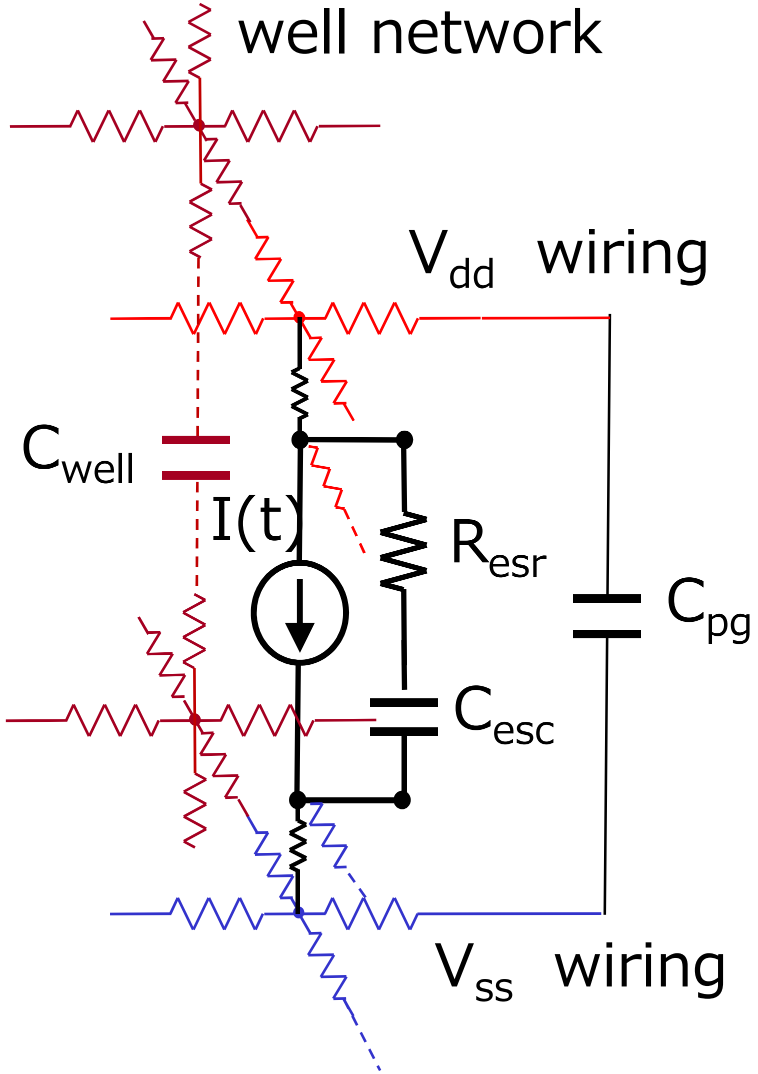
Liner network model (passive part)



- ▶ Liner network model (Passive CPM)
- ✓ Behavioral of PDN of IC
- ✓ SPICE compatible model
- ✓ Reduced and distributed RC network among ports (hundreds or thousands ports)
- ✓ Require : Layout data, technology profile

Power current model (active part)



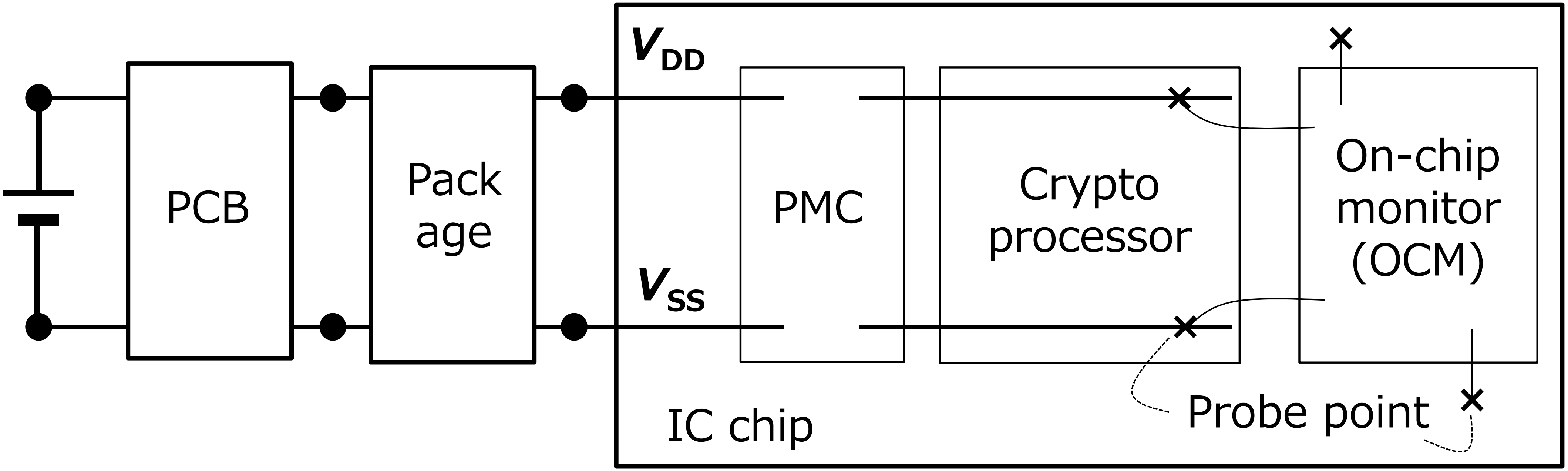


- SPICE simulation: I(t)
  LUT for in/out condition,
  load caps
- Post-layout extraction
  logic cell level: C_{esc}, R_{esr}

▶ Cell based -- logic cells are characterized in power current model.

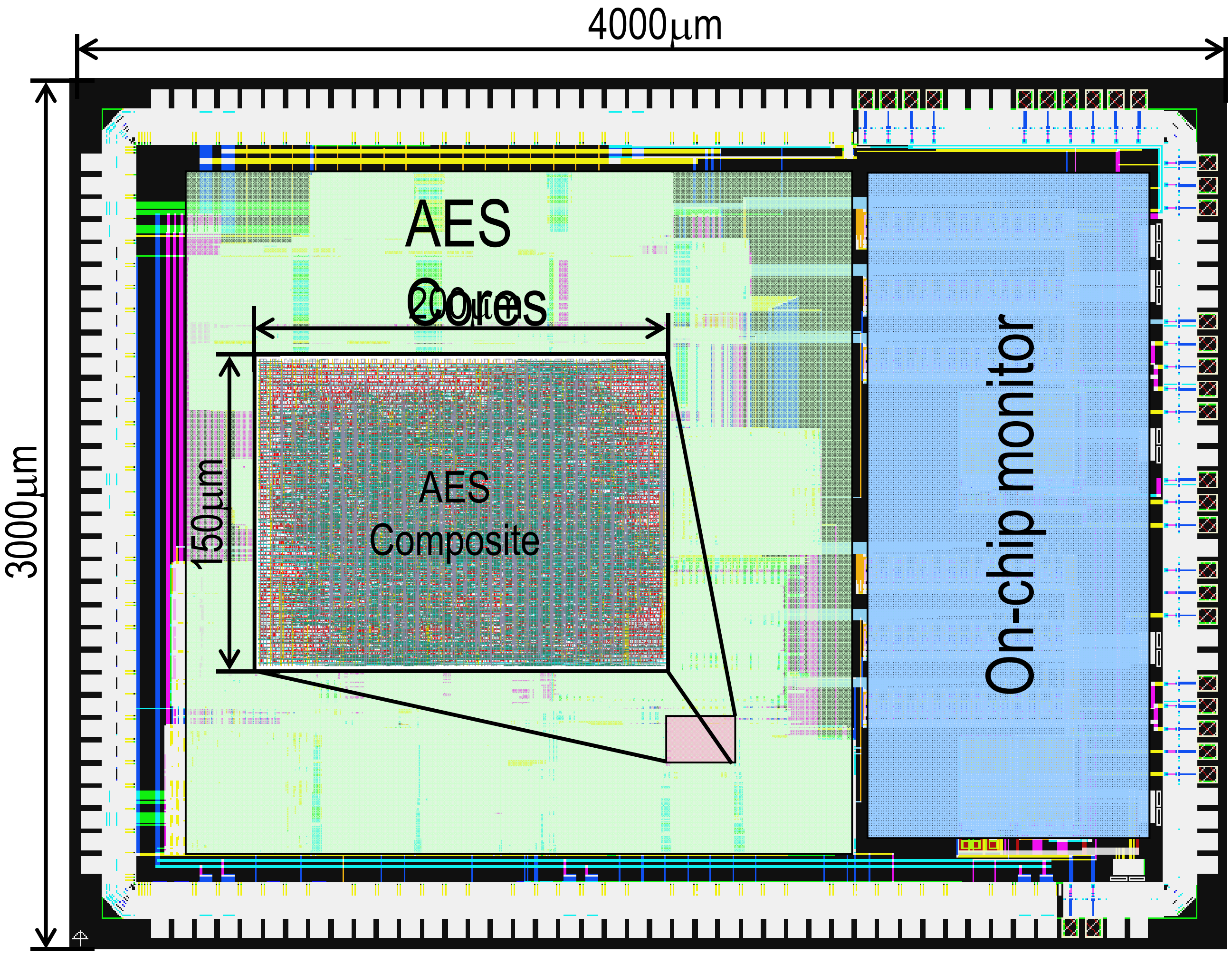
C-P-S* model for diagnosis and analysis

*Chip-Package-System board



- Full-system level simulation of power side-channel leakage
- On-die diagnosis of physical attacks

Silicon test vehicle

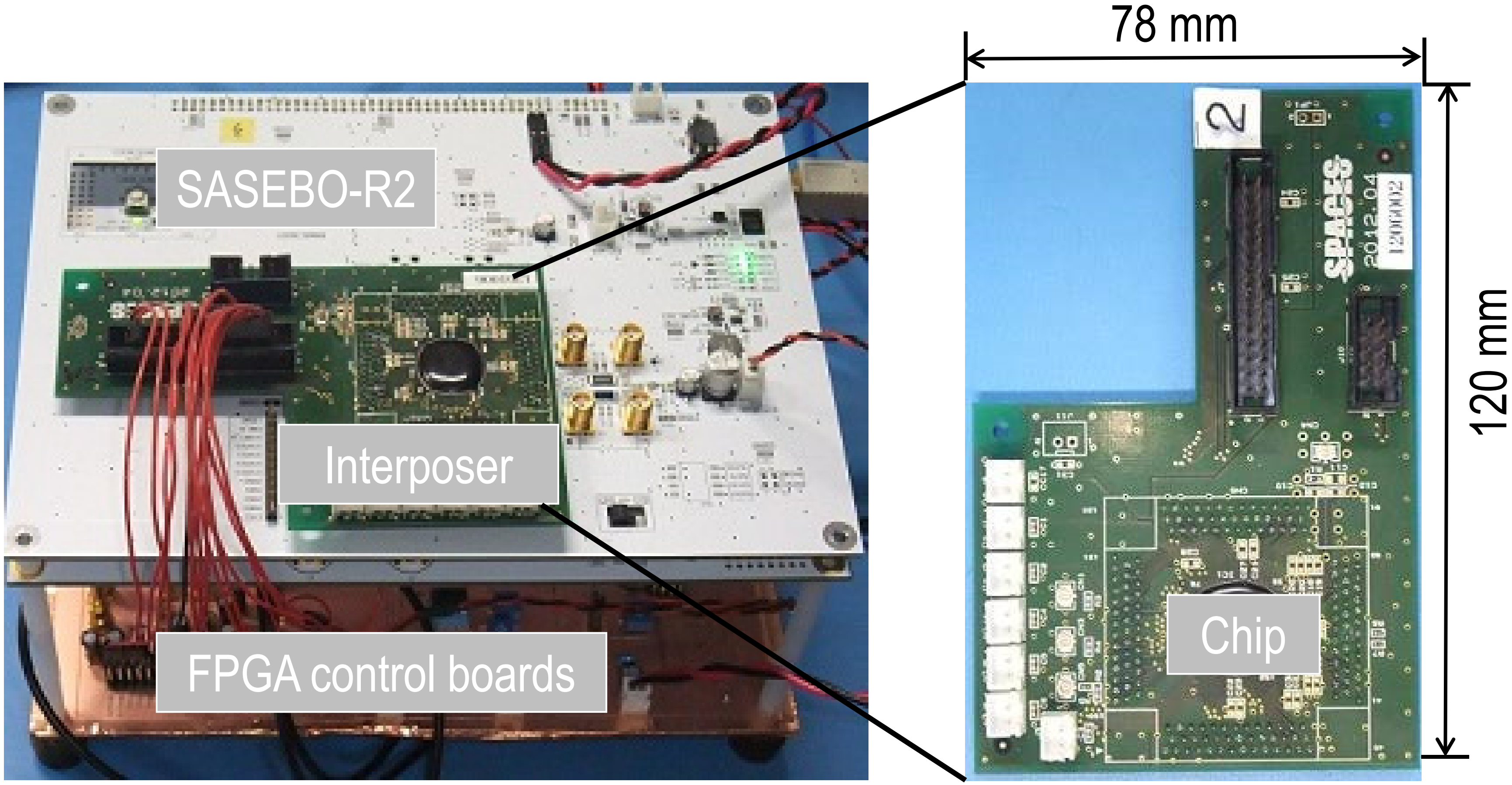


Chip summary*	
Process	65 nm CMOS
Metal	9 layer Cu metal
Cores	AES cores with different S-box implementation
Target core in this paper	AES Composite S-box implementation

***SPACES explorer chip,** for Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems

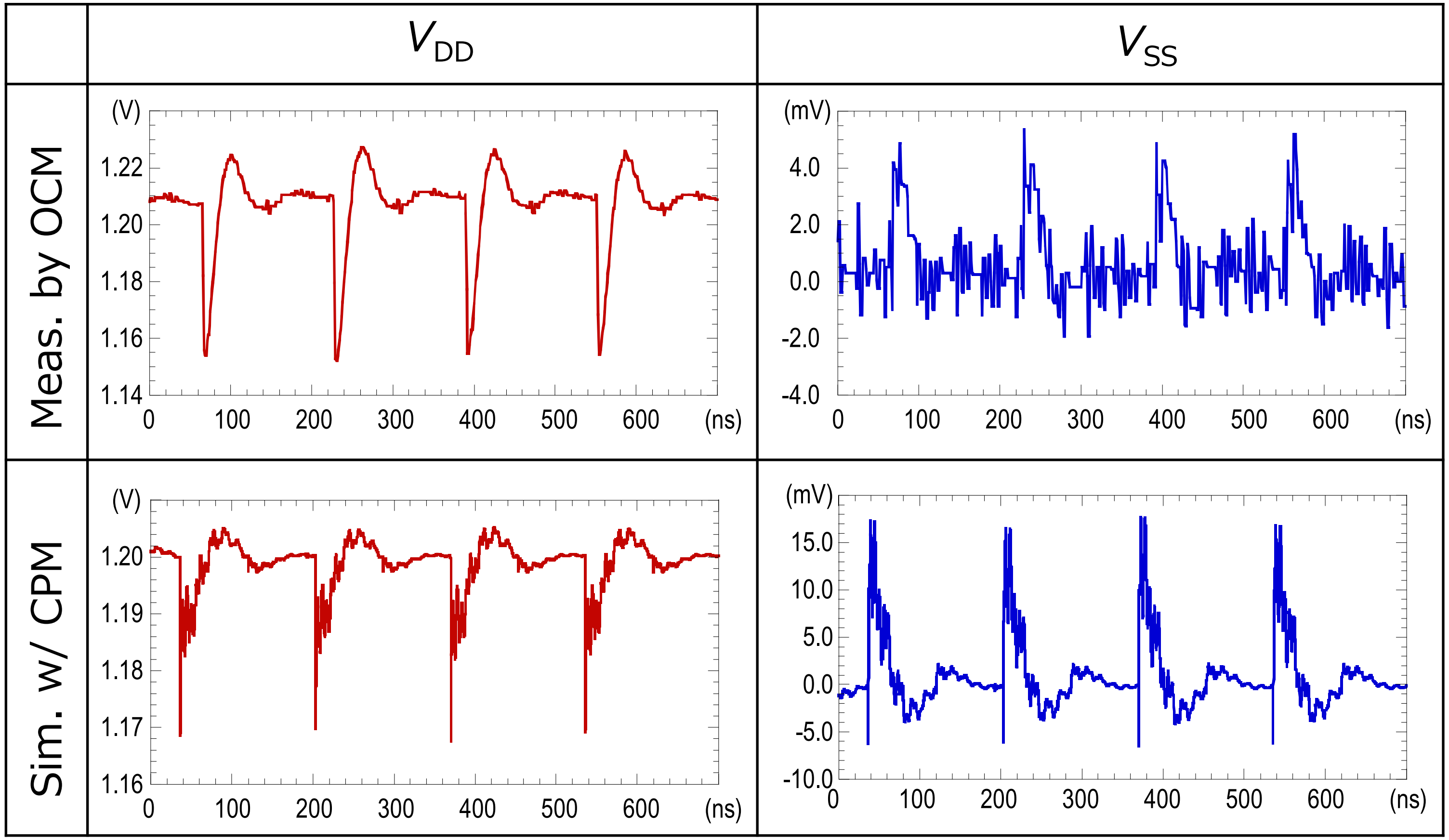
*D. Fujimoto, *et al.*, "Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip," HOST 2014.

SC leakage measurement system



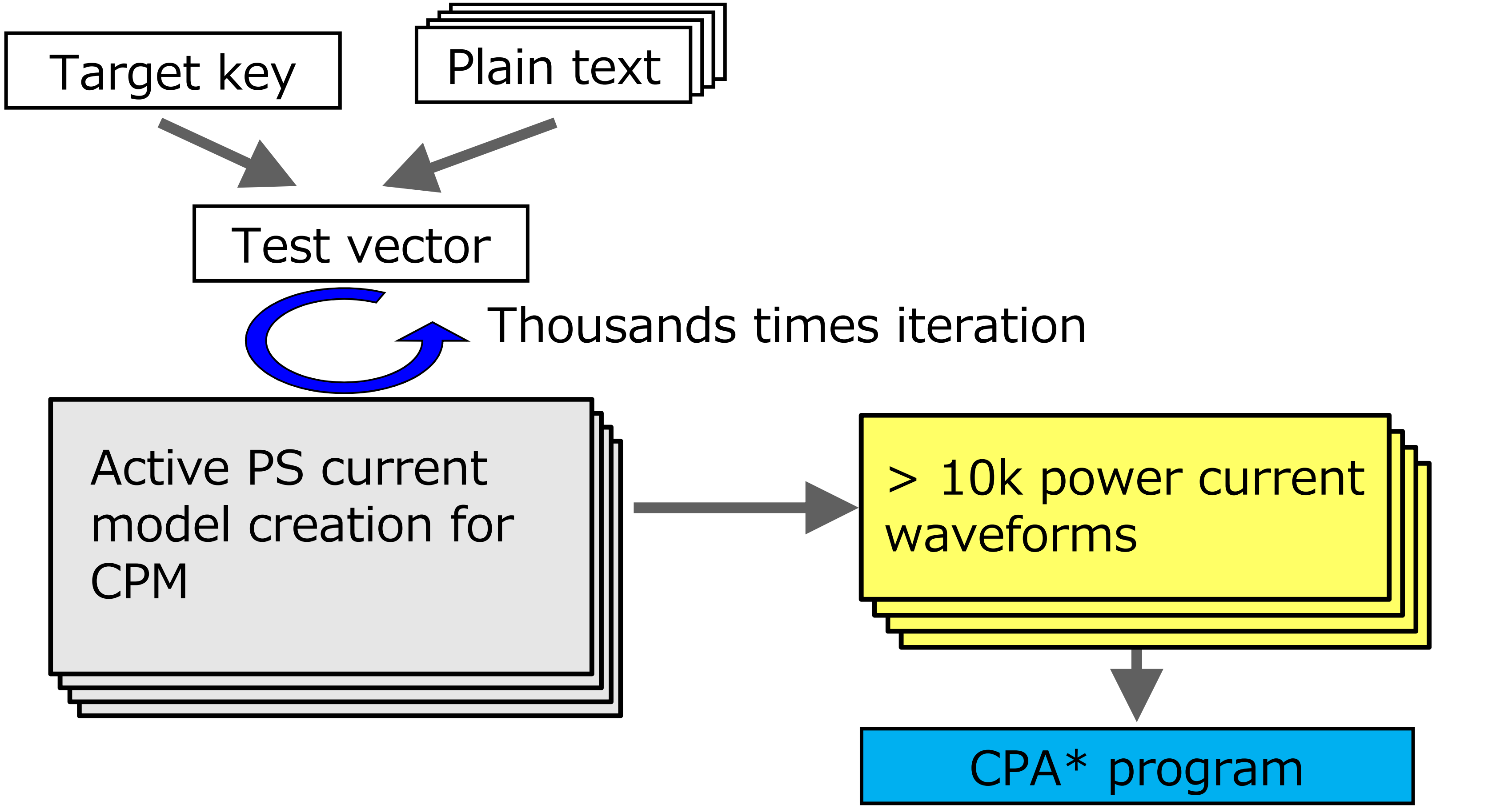
- Exploration of physical mechanisms of SC information leakage.
- A test chip directly mounted on an interposer, in the measurement system built on FPGA board called “SASEBO-R2.”

Simulation versus measurements



- ► CPM of AES circuits in C-P-S EMI simulation
- ► On-chip noise monitoring (OCM) of AES circuits
- ► The overall shape of the waveform and size of peak drops are almost consistent.

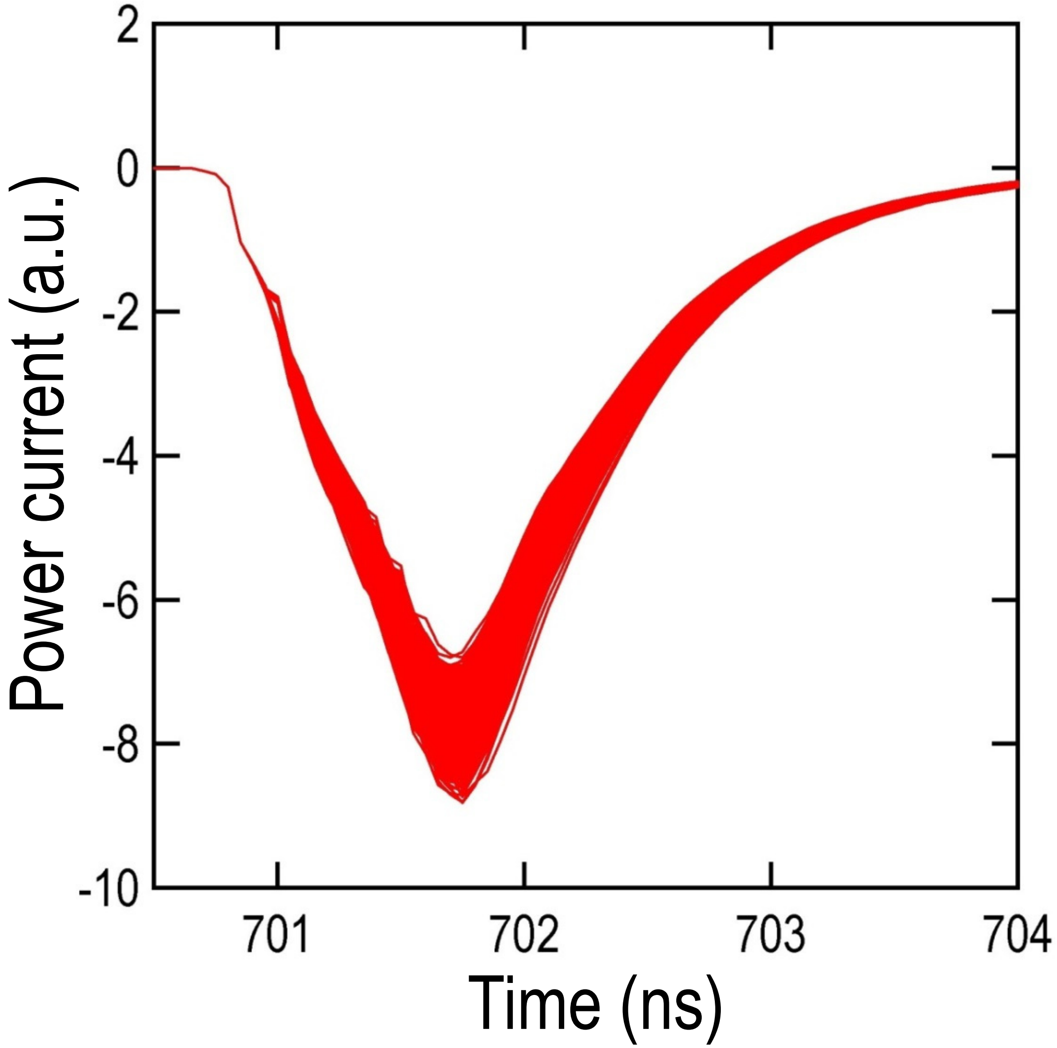
SC leakage simulation flow


Target key
Plain text
Test vector
Thousands times iteration
Active PS current model creation for CPM
> 10k power current waveforms
CPA* program

*correlated power analysis (CPA)

- Time-domain simulation for a set of plain texts to be encrypted with a private key.

PS current wvfms for CPA (sim.)



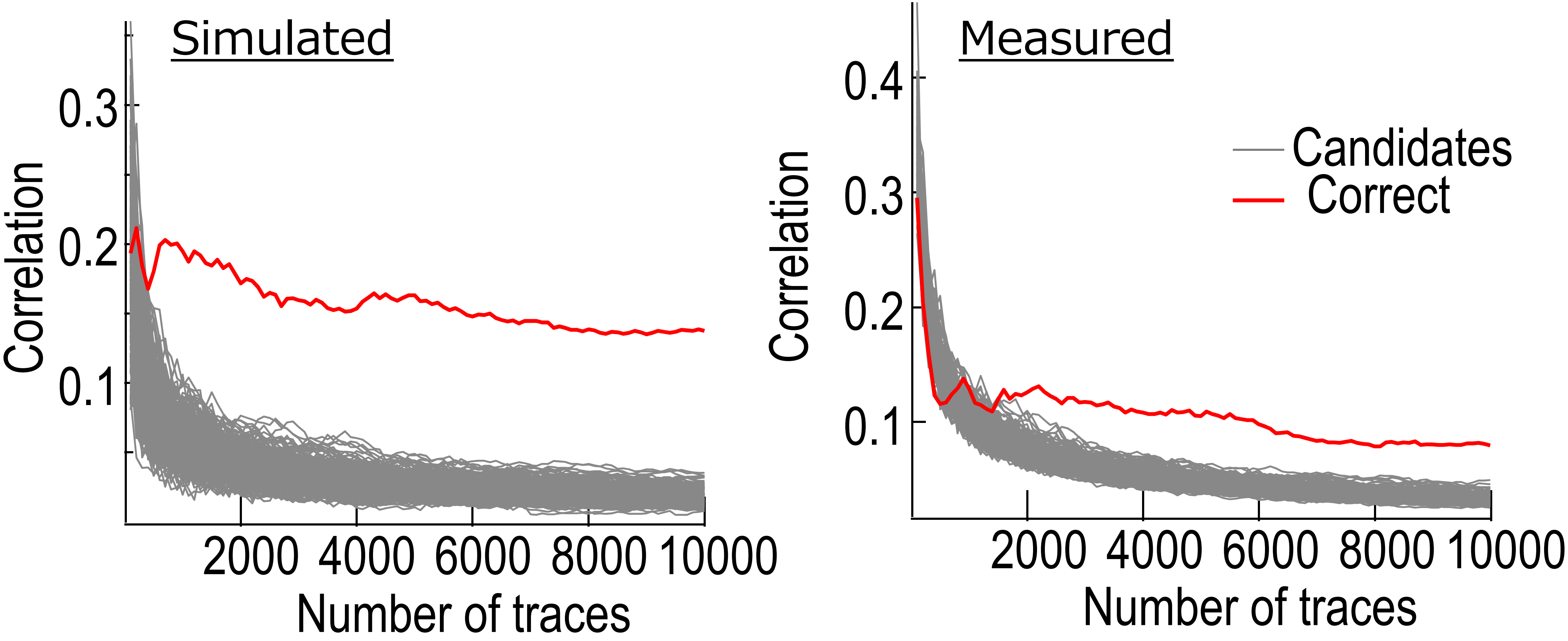
Cost of simulation for 10,000 plain texts

Model	cost
Full transistor (pre-layout)	115 days
Full transistor (post-layout)	Unlikely
Active PS current model	10 hours

280 times acceleration is achieved.

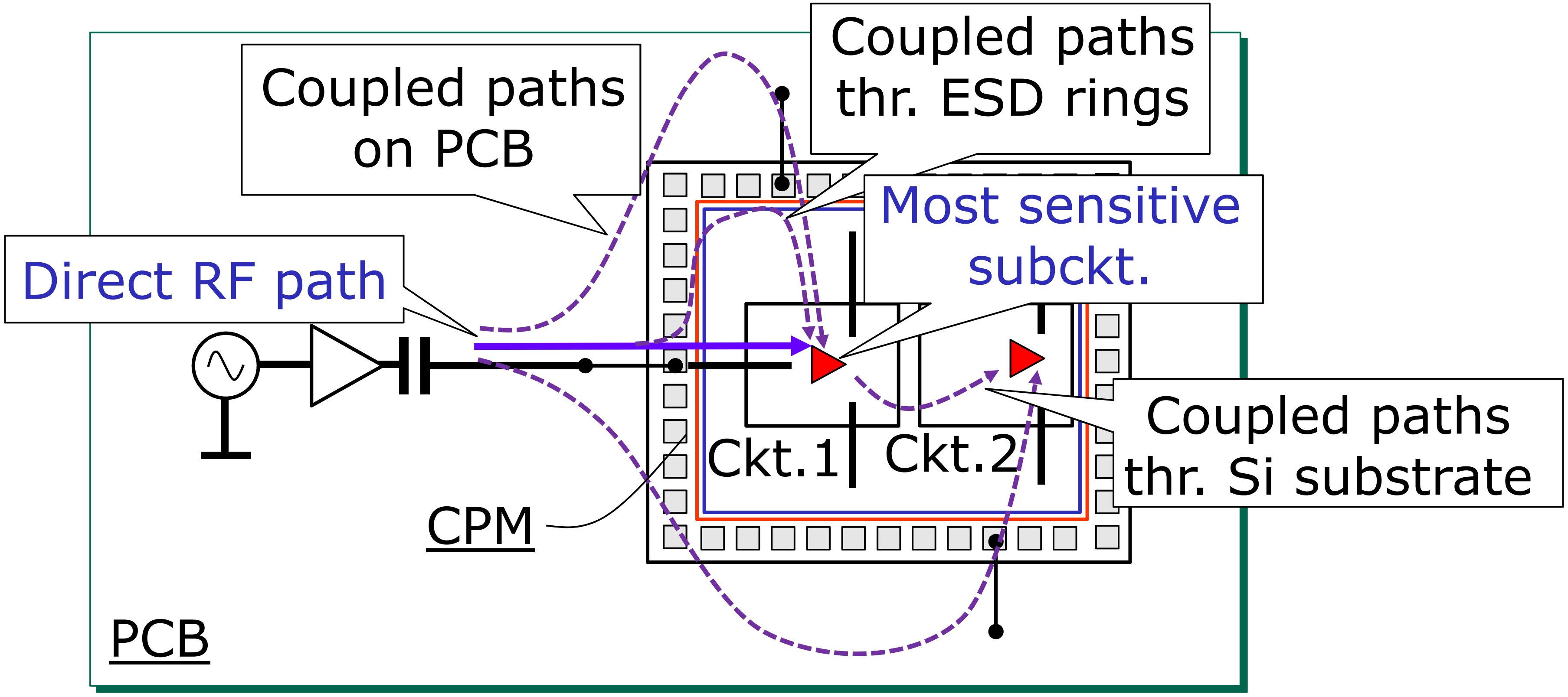
*D. Fujimoto, *et al*., "A Fast Power Current Analysis Methodology Using Capacitor Charging Model for Side Channel Attack Evaluation," HOST 2011.

CPA sim. and meas.



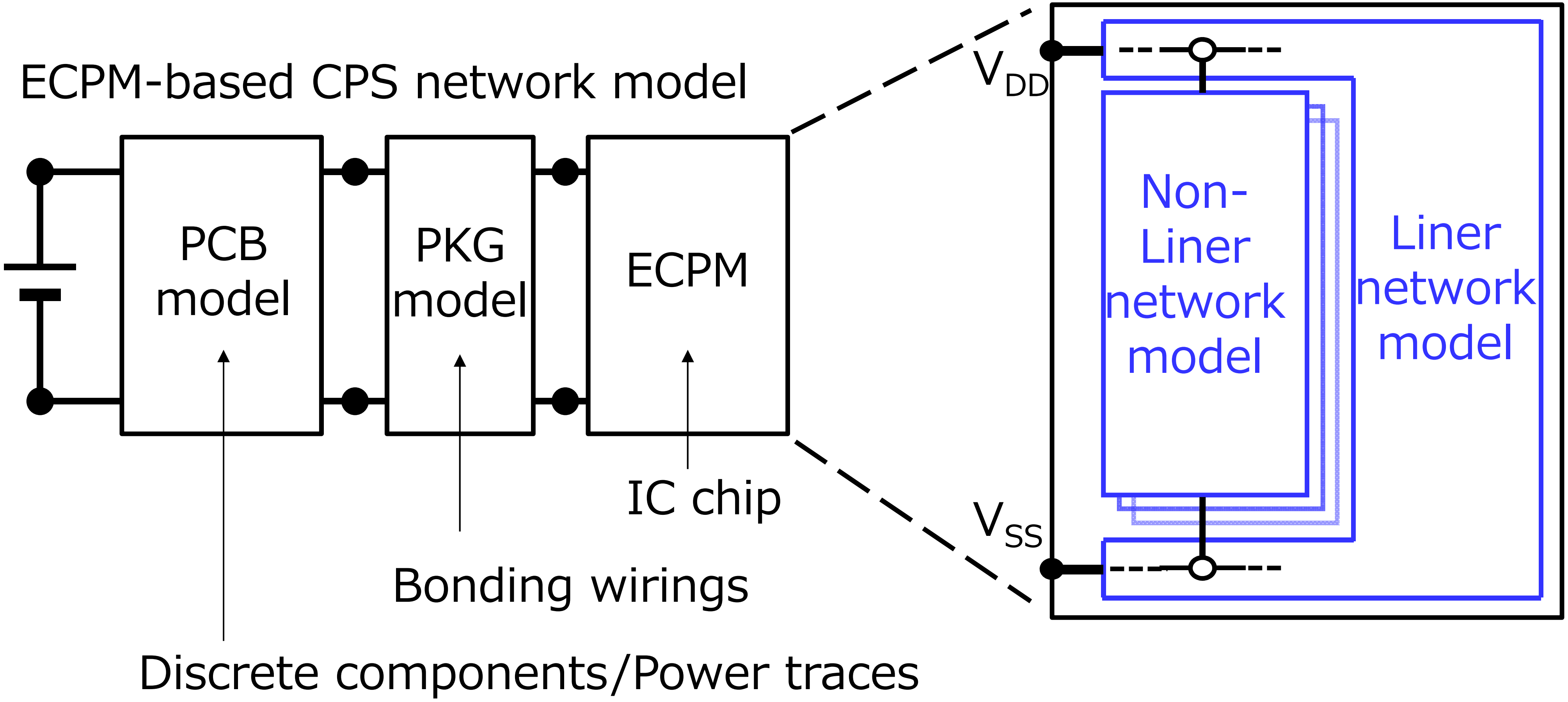
- Correlation between Hamming distance and PS waveforms

EMS simulation framework



External part of EMS	Internal part of EMS	Challenge
Limited to the direct and associated RF paths of the most significance	On-die paths of ESD I/O rings and Si substrate, in addition to PDN of circuits	Specification of the most sensitive part of circuits to RF disturbance

EMS simulation model

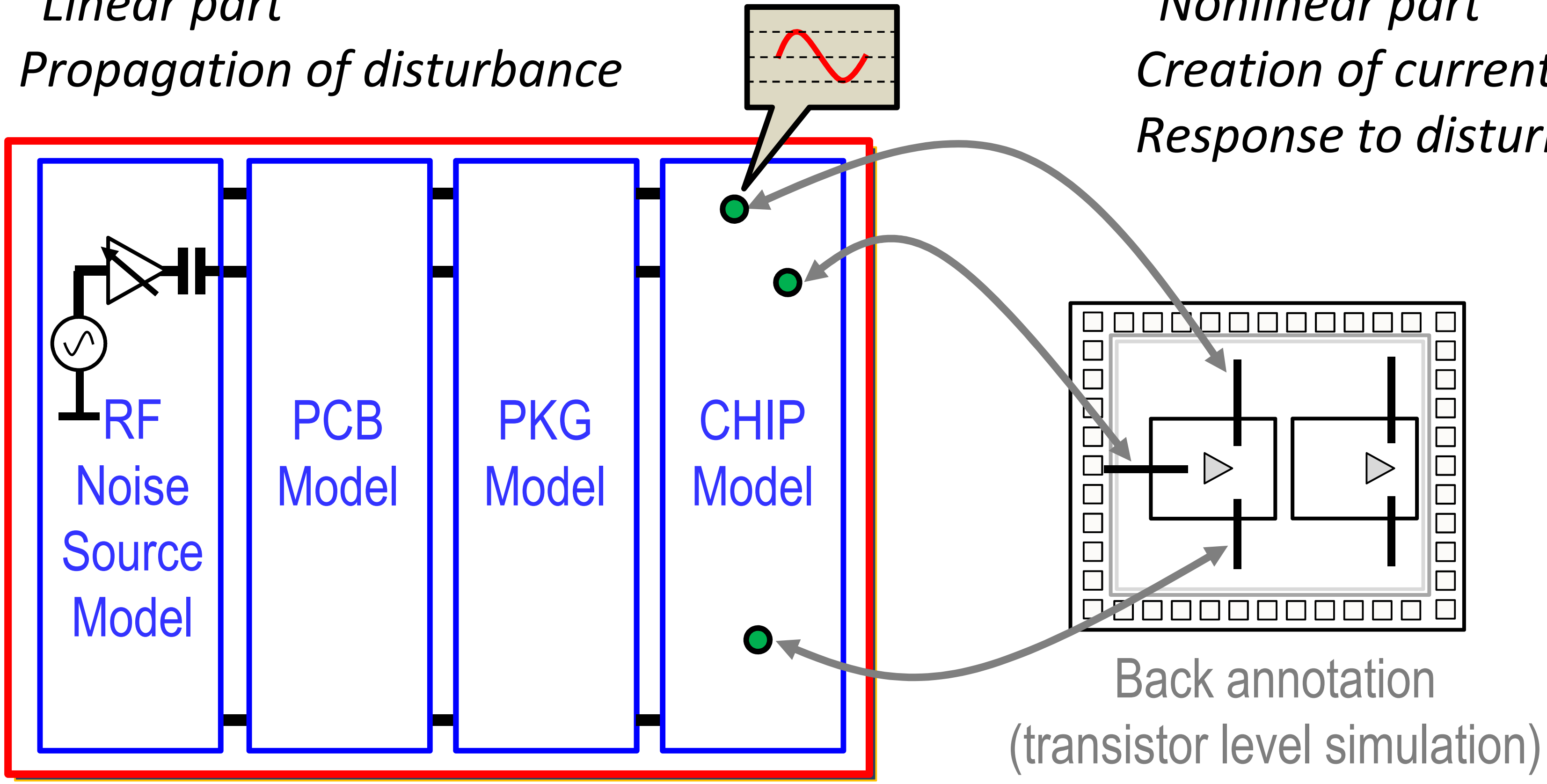


- ▶ The whole model captures chip-package-system board interaction

EMC simulation for HWS

"Linear part"
Propagation of disturbance

"Nonlinear part"
Creation of current,
Response to disturbance



- ▶ Propagation of power current (EMI) or disturbance (EMS) in linear network
- ▶ Creation of power current (EMI) or response to disturbance (EMS) in nonlinear operation of semiconductor devices

Summary

- ***“IC-chip level EMC simulation”* is established with chip power models (CPM) and chip-package-system board integrated models (CPS).**
- **Deployment of *“IC-chip level EMC simulation”* faces the challenges to be solved:**

  EMI: Full-system level power noise emission for private key and public crypto processors.

  EMS: Response of crypto processors to intentional disturbances by EM, Laser and other physical equivalents.

Acknowledgements: This work was in part supported by Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Cyber-Security for Critical Infrastructure” (funding agency: NEDO).