33rd International Conference on VLSI Design
19th International Conference on Embedded Design
Bangalore, Jan. 5. 2020.

Side-Channel Attack Analysis and Simulation Techniques

Tutorial

Makoto Nagata

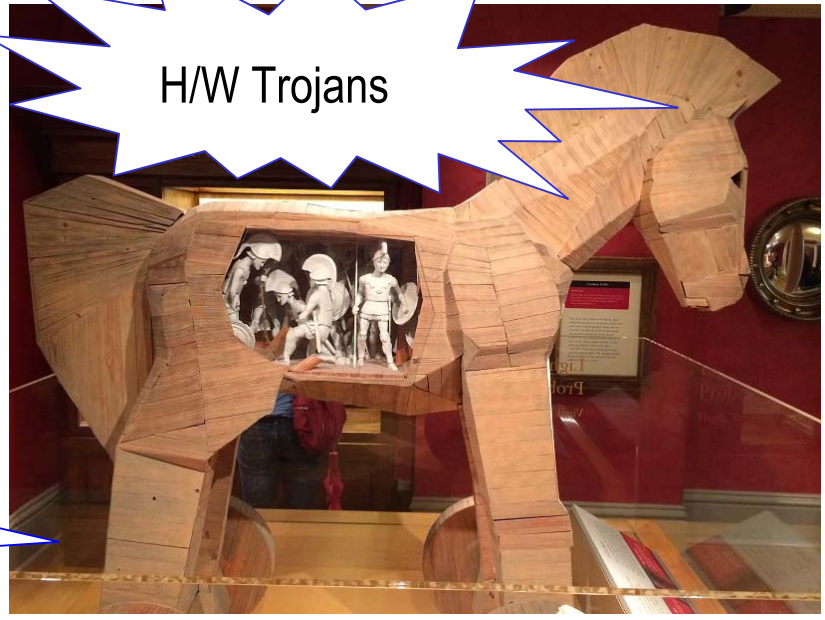
Graduate School of Science, Technology and Innovation,

Kobe University, Kobe, Japan

Advent of adversary among IC chips

Crypto attacks

H/W Trojans



Outline

Background

- Side-channel attacks
- Power noise analysis technique
- Side-channel attack simulation
- Conclusions

Passive attack – power analysis

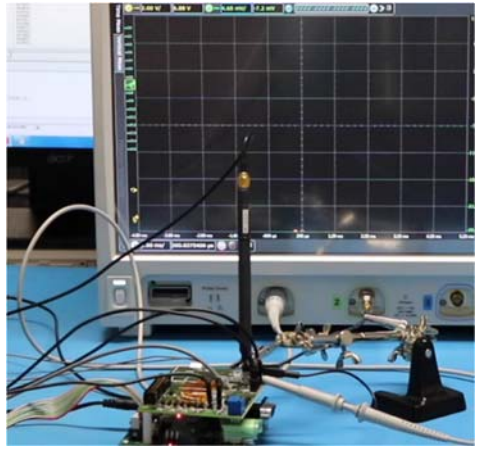
μEM probe
(Attacker)

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



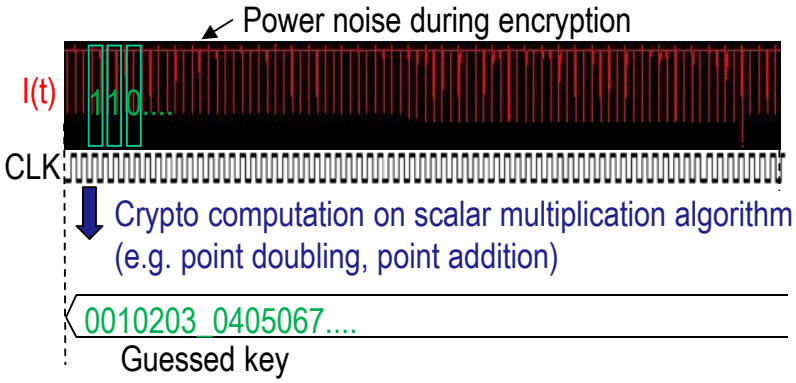
Cryptographic engines

- Public key crypto
  - ✓ Asymmetric key usage for encryption and decryption – a pair of keys for public and private domains
  - ✓ Power side channel leakage analysis: SPA
  - ✓ ECC, ECDSA, RSA

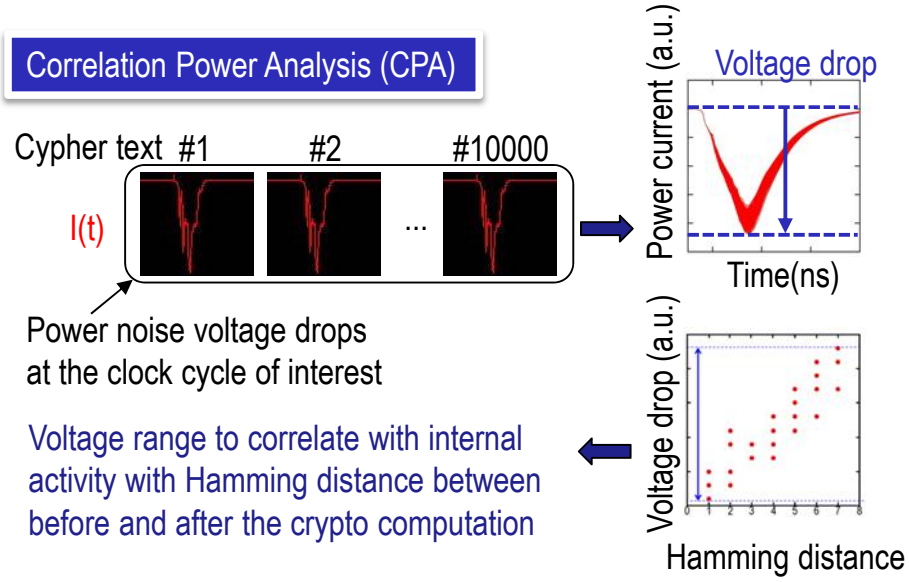
- Private key crypto
  - ✓ Symmetric key usage – a single private key for both encryption and decryption (there is no public domain)
  - ✓ Power side channel leakage analysis: DPA, CPA
  - ✓ AES, DES (obsolete)

Power side channel leakage analysis

Simple Power Analysis (SPA)

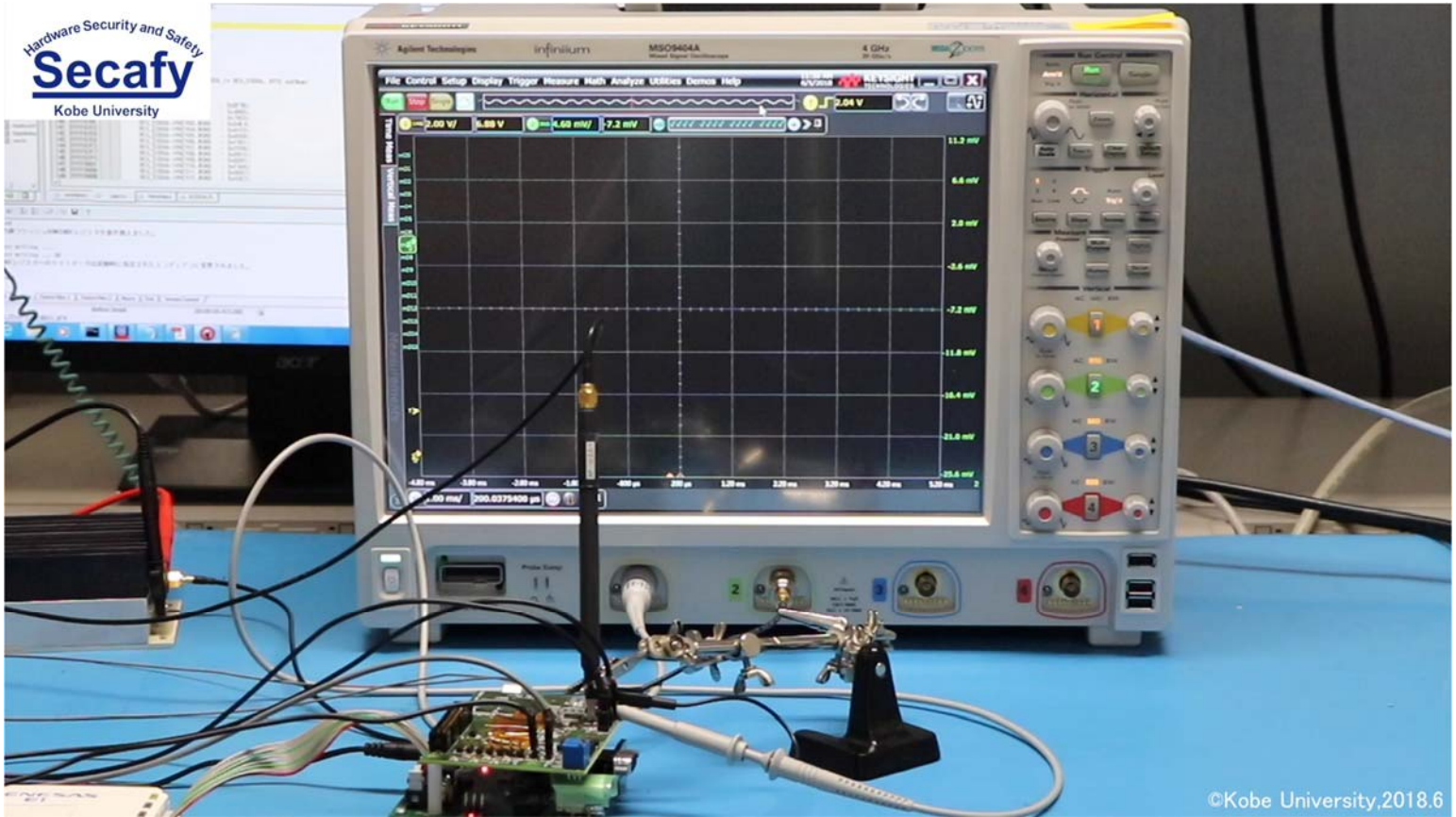


Correlation Power Analysis (CPA)



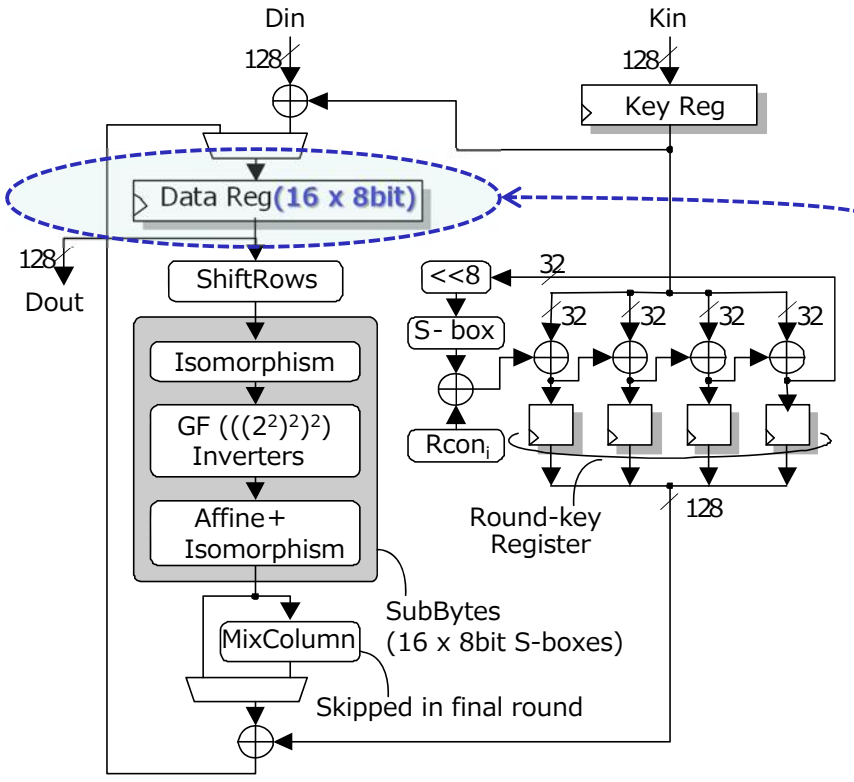
- Analysis (or attacks in a malicious case) to extract a secret key from power-noise waveforms
- Simulation technique to evaluate security risks in design against diversified leakage models

SPA demonstration



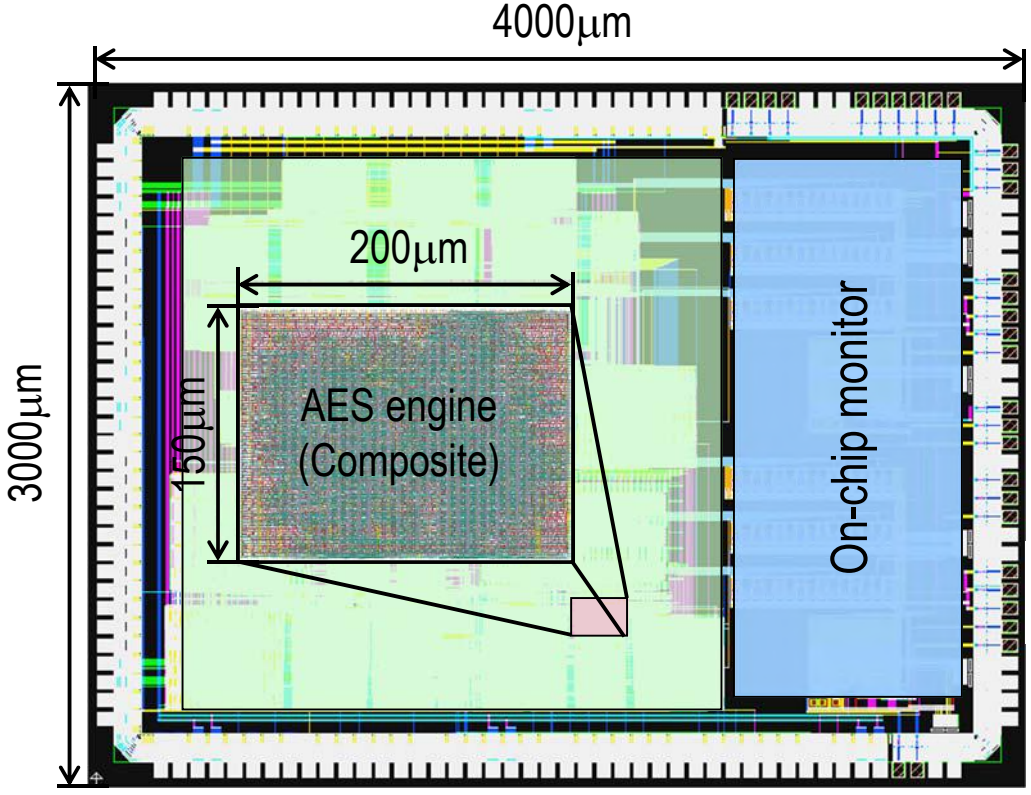
AES* cryptographic architecture

*Advanced Encryption Standard



- A single key byte (8 bit) is used in byte-wise crypto computation.
- For AES with 128-bit key, 16 computations running in parallel.
- Source of correlation:
  PS current and internal activity measured as Hamming distance

Silicon test vehicle

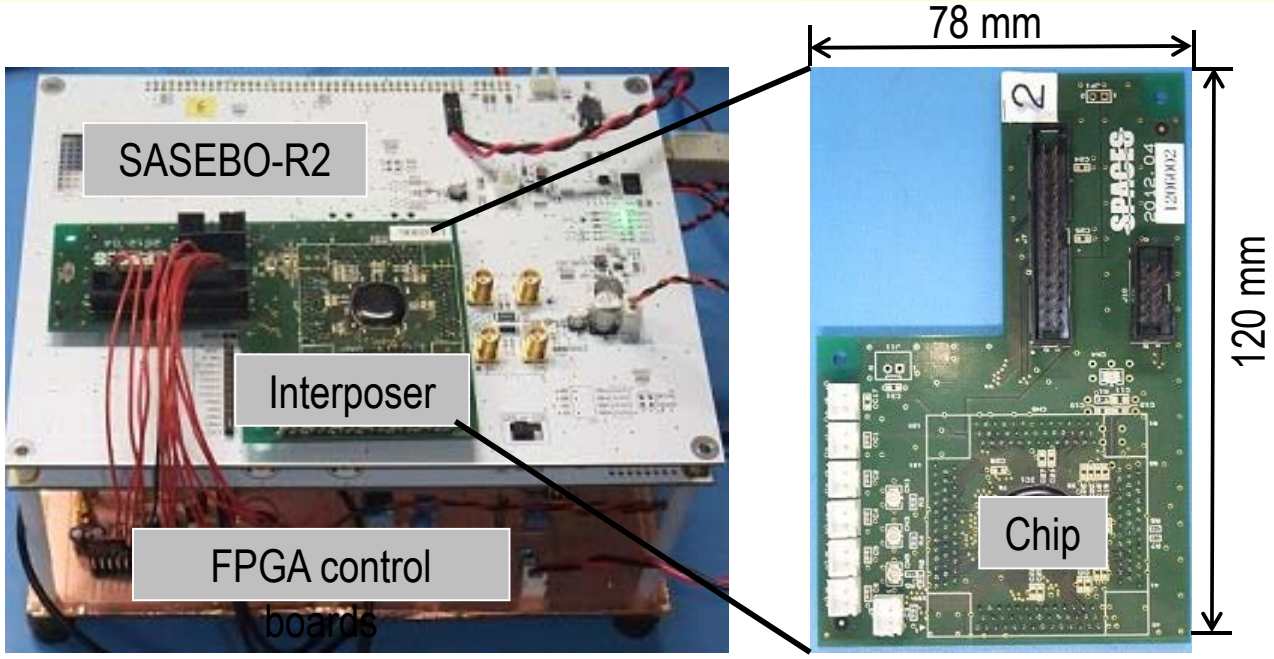


Chip summary*	
Process	65 nm CMOS
Metal	9 layer Cu metal
Cores	AES engines with different S-box implementation (example: Composite)

*SPACES explorer chip
(Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems)

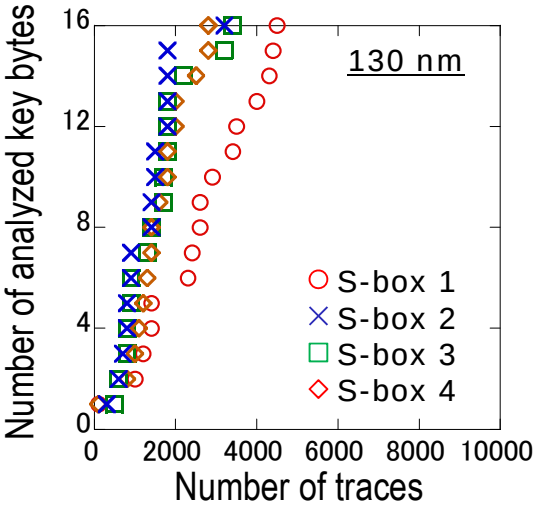
D. Fujimoto, *et al.*, "Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip," HOST 2014.

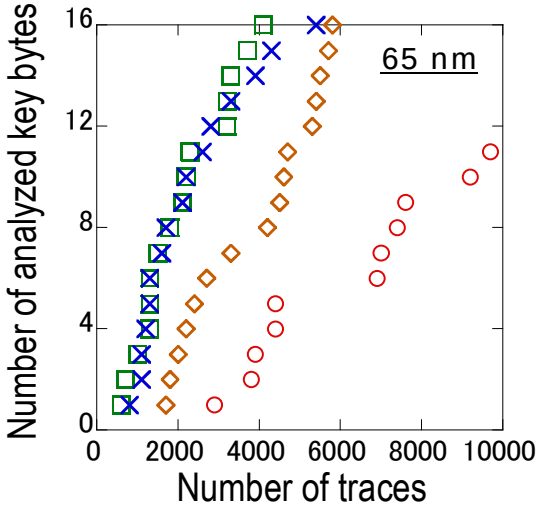
SC leakage measurement system

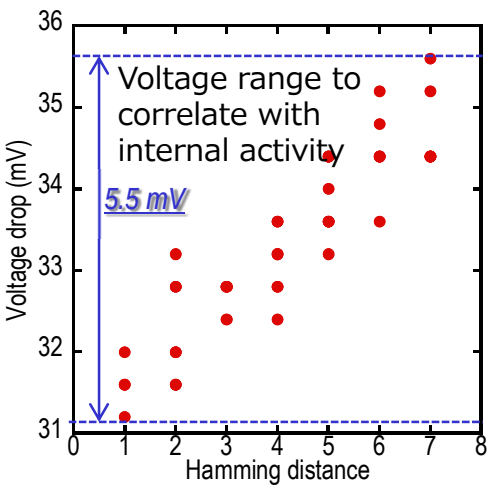


- Exploration of physical mechanisms of SC information leakage
- A test chip directly mounted on an interposer, in the measurement system built on FPGA board called “SASEBO-R2”

SC leakage measurement examples

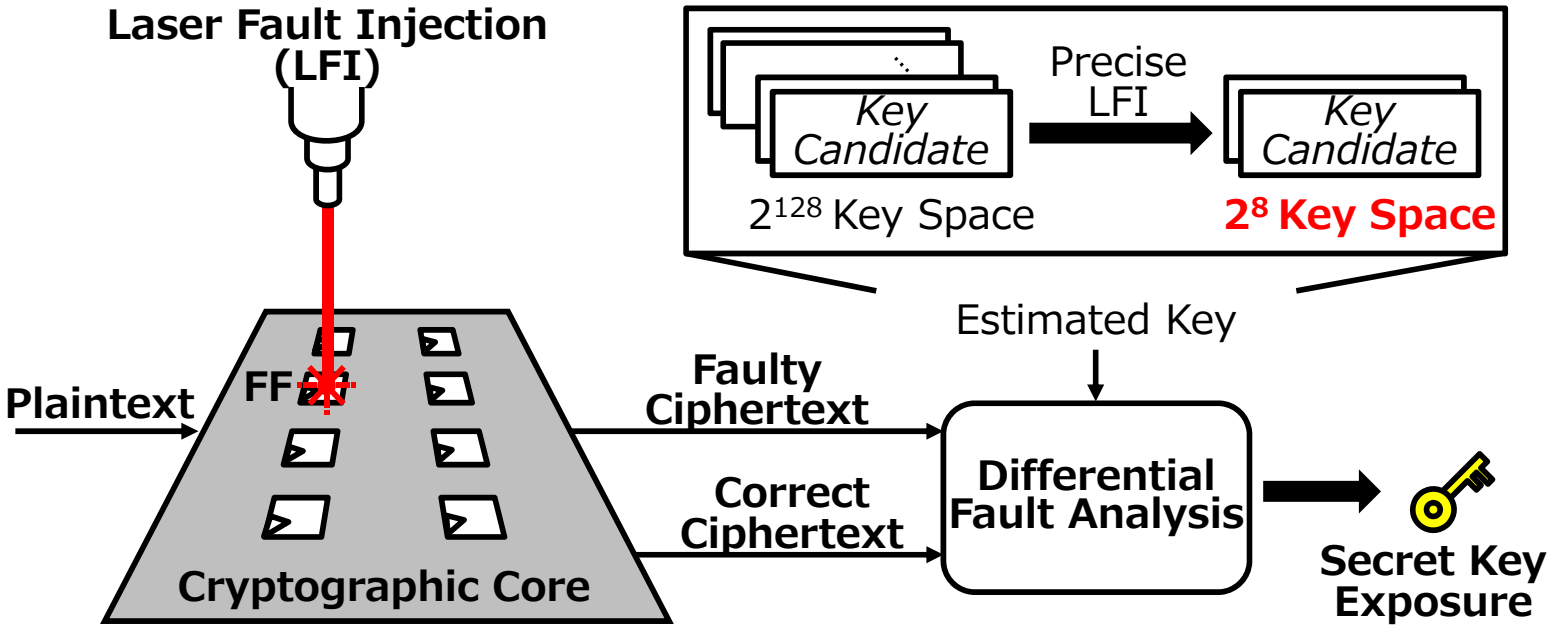






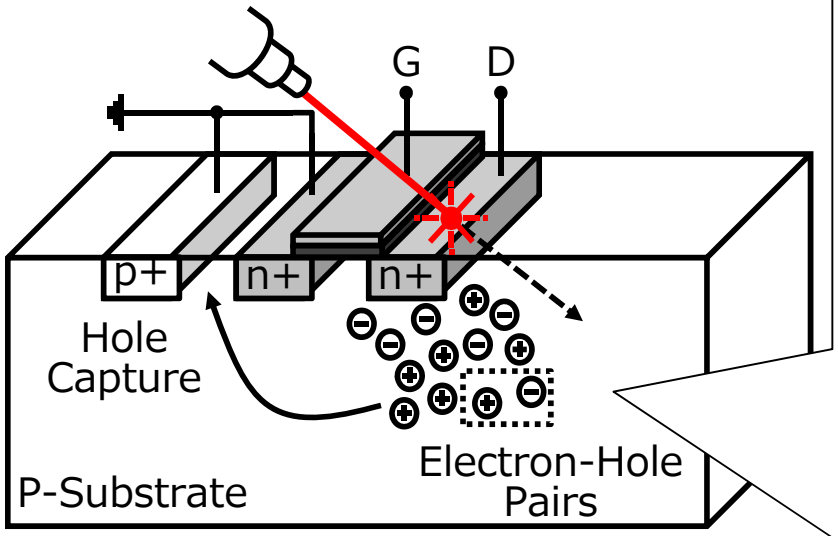
- SC leakage comes from the correlation of S-box internal switching activity and logic operation using secret key bytes.
- It is difficult to achieve complete elimination while possible to mitigate the level of correlation – a design challenge.

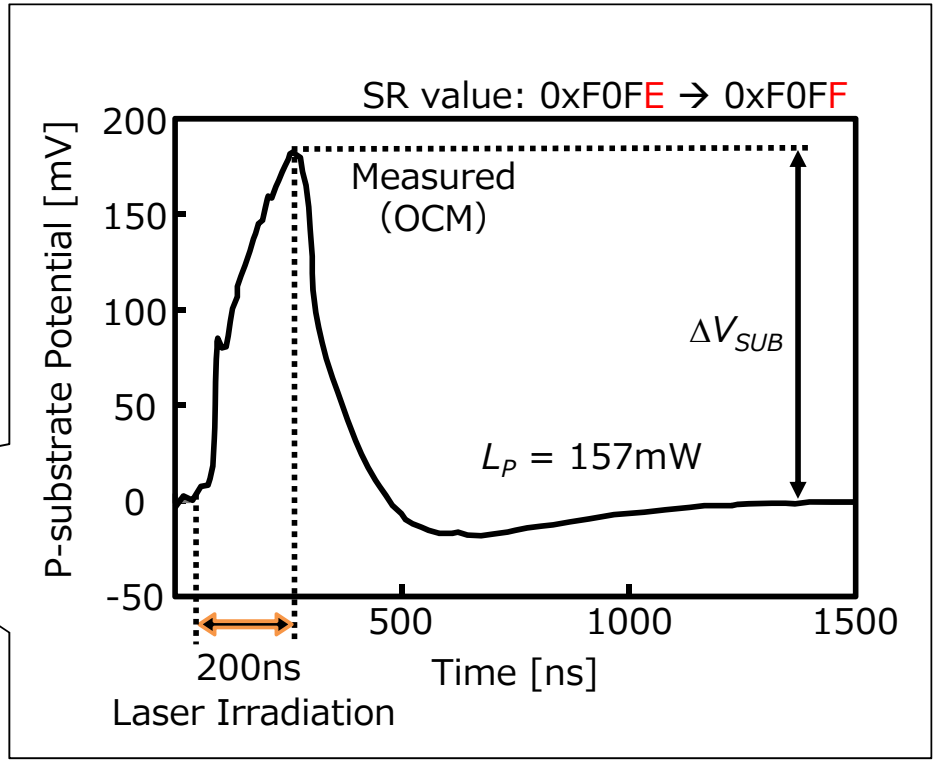
Active attack -- laser fault injection (LFI)



- High resolution fault injection both in time and space, 1-bit fault potentially reduces key space to 28@AES-128.

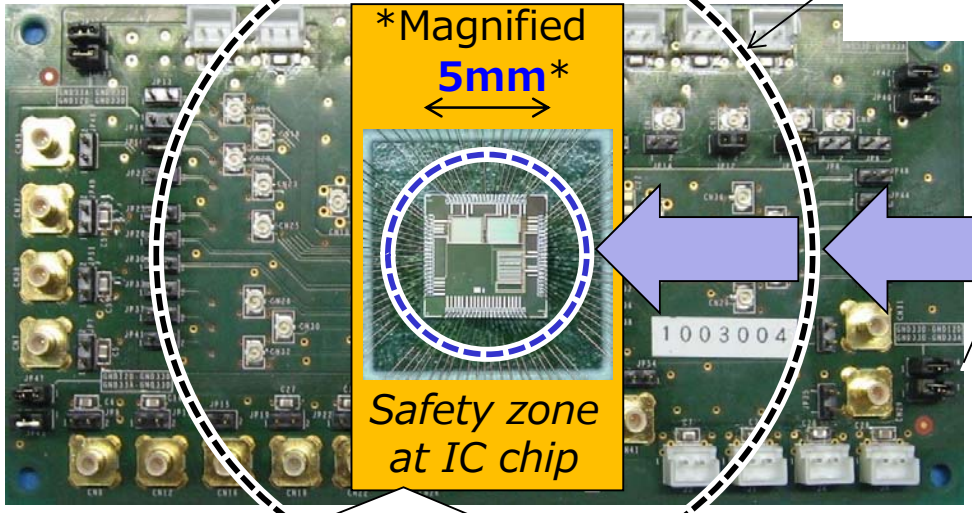
LFI physical mechanism





K. Matsuda *et al.*, "On-Chip Substrate-Bounce Monitoring for Laser-Fault Countermeasure," AsianHOST 2016.

Physical attacks in dimensions

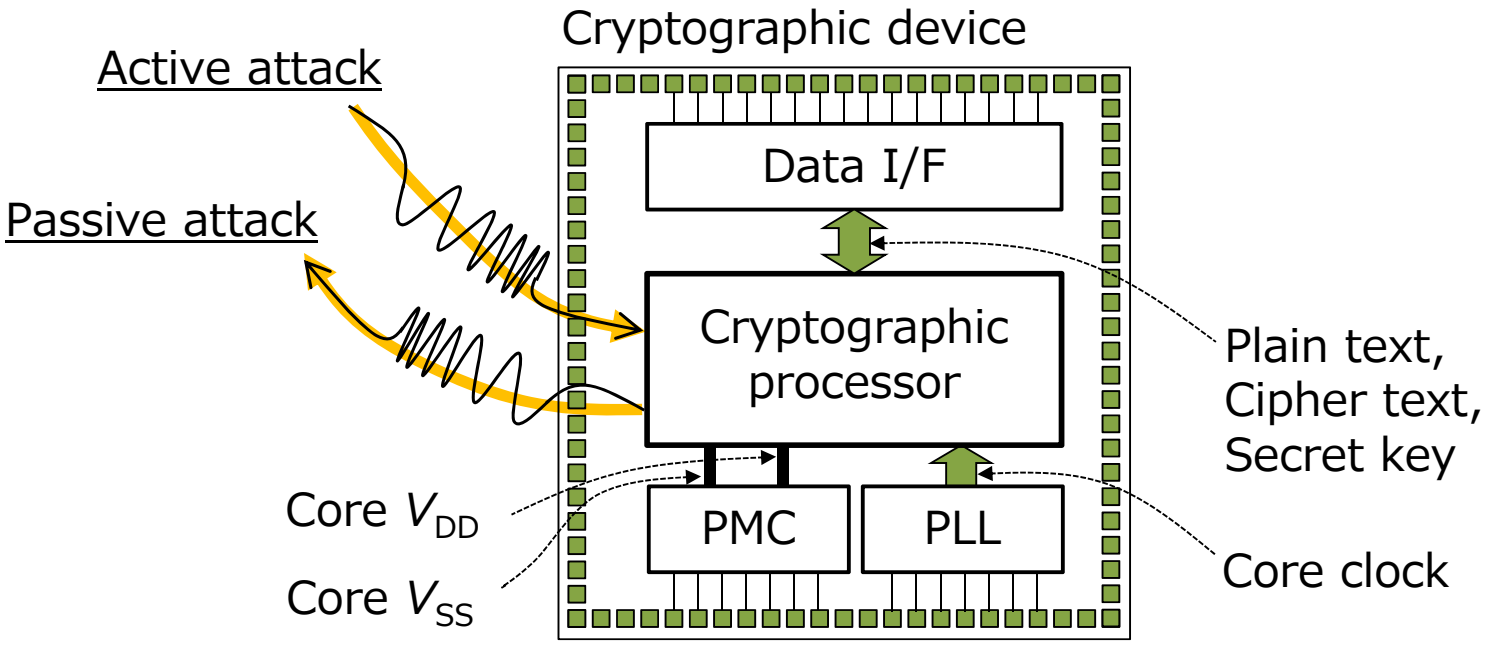


Leakage observed on PCB
~100mm

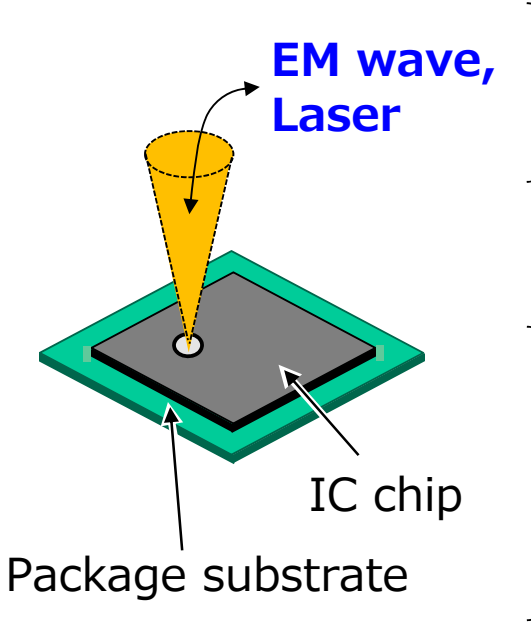
Leakage through far
EM emanation
1m~

Objective: securing crypto-engines in the areas of ICs

Physical attack isolation walls at chip level



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.

M. Nagata *et al.*, "On-Chip Physical Attack Protection Circuits for Hardware Security (Invited)," CICC 2019.

Reported countermeasure techniques

- 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.

Outline

Background

Side-channel attacks

- Power noise analysis technique
- Side-channel attack simulation
- Conclusions

Power SC leakage from EMC viewpoint

EMI

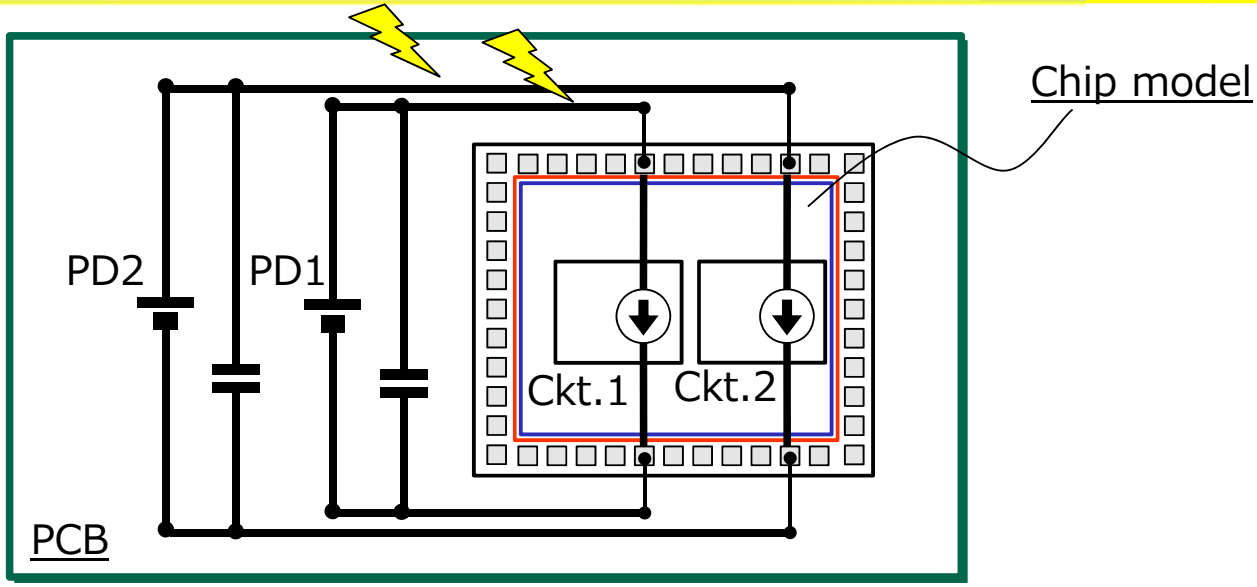
- Electromagnetic emission →Side channel leakage (passive information leakage)
- EMI analysis → SCA analysis

EMS

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

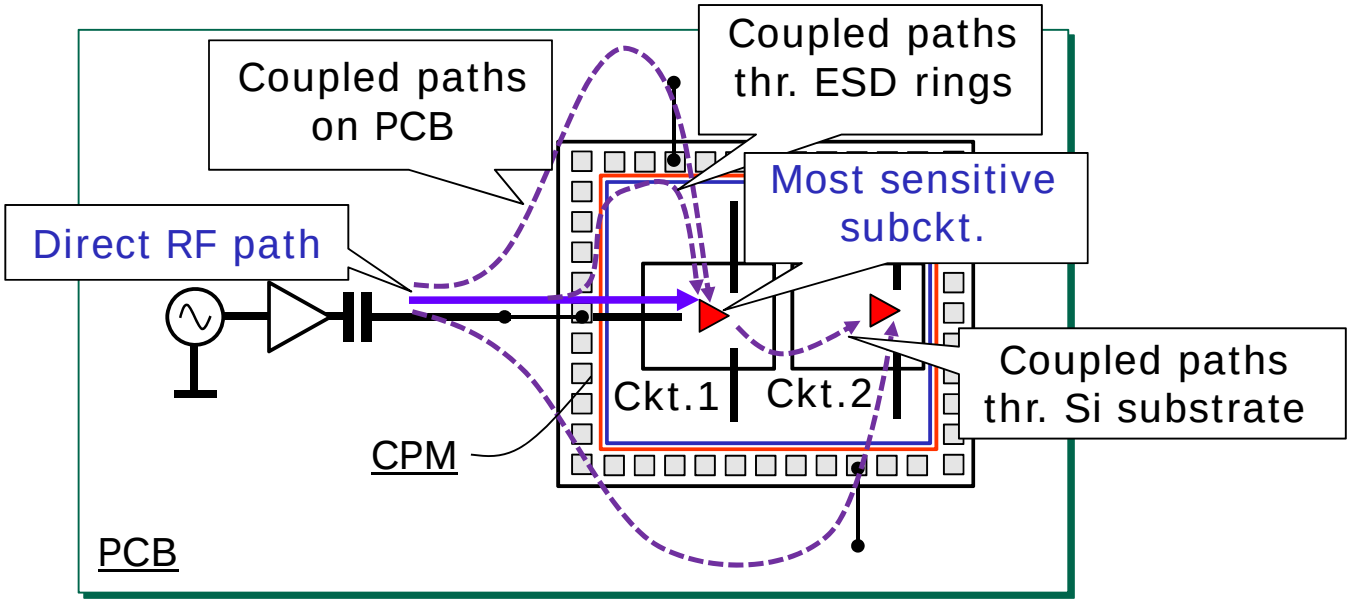
In-depth understandings of IC-chip level EMC, toward the quality design of IC chips for hardware security

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

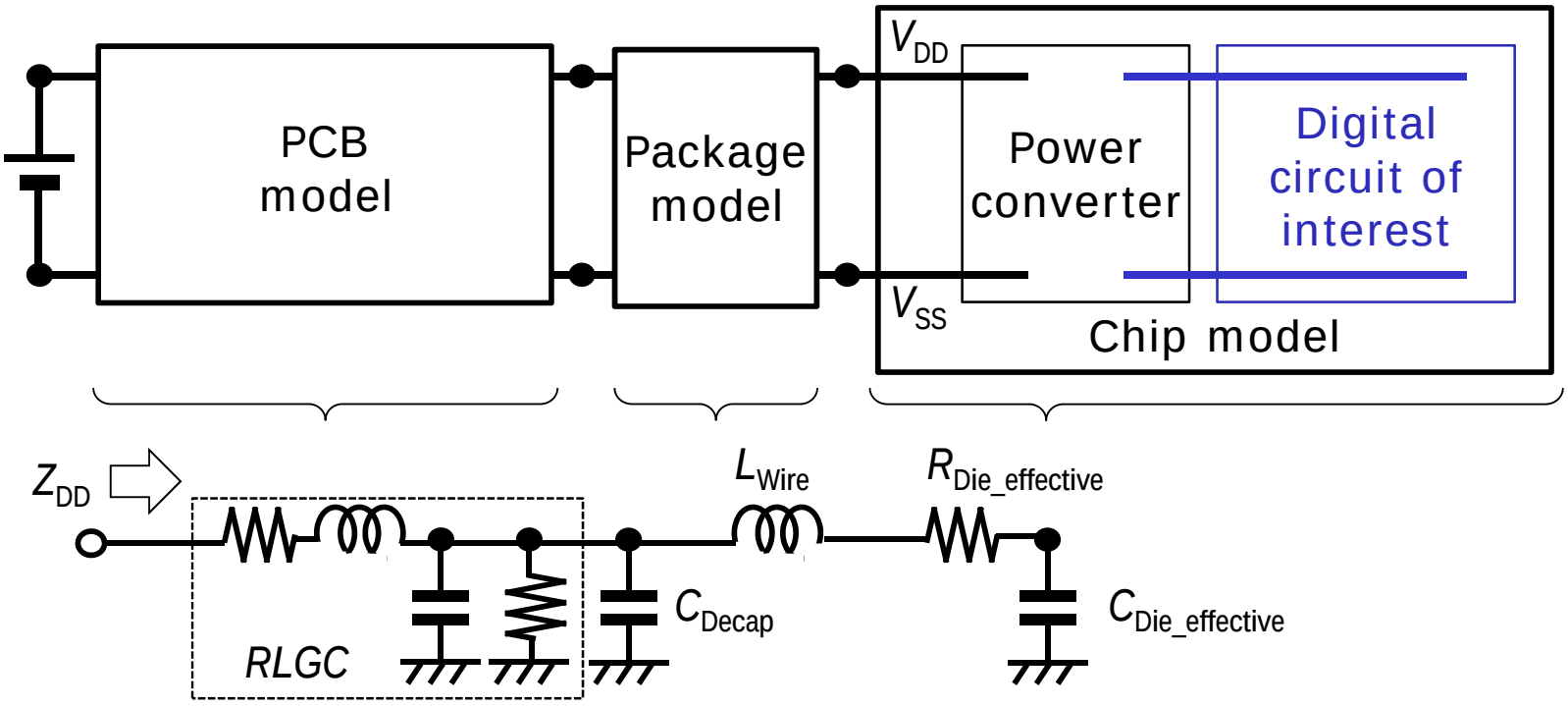
EMS simulation framework



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

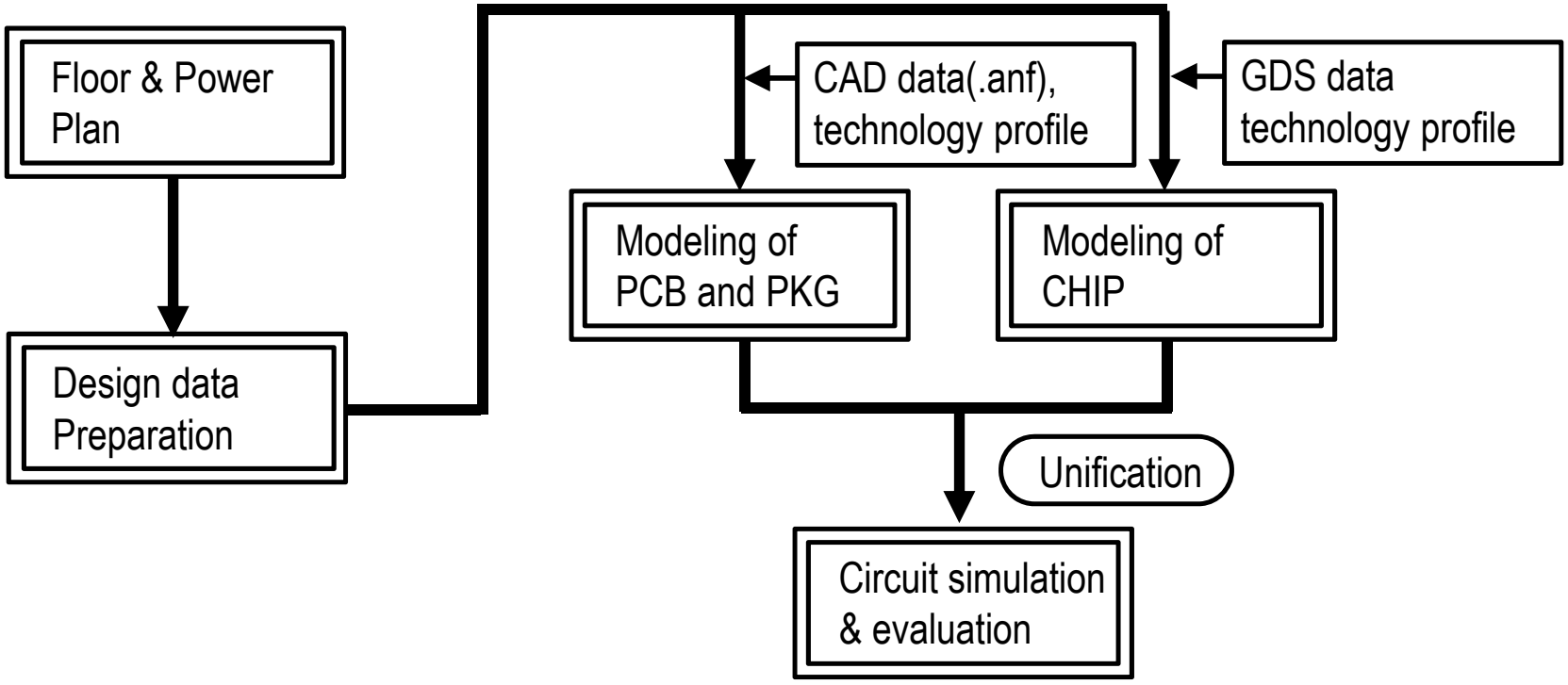
C-P-S* model for power noise analysis

*Chip-Package-System board

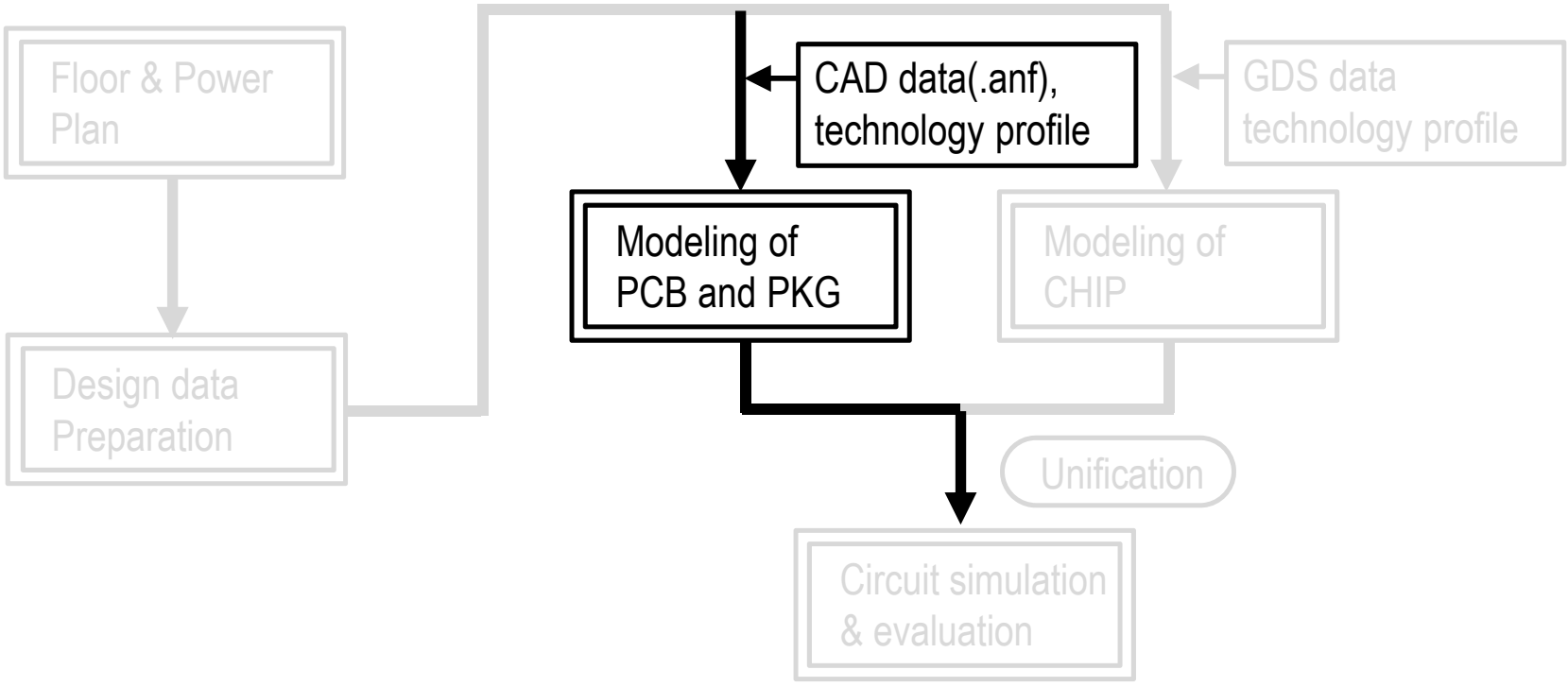


- Full-system level simulation of power-noise generation and interference

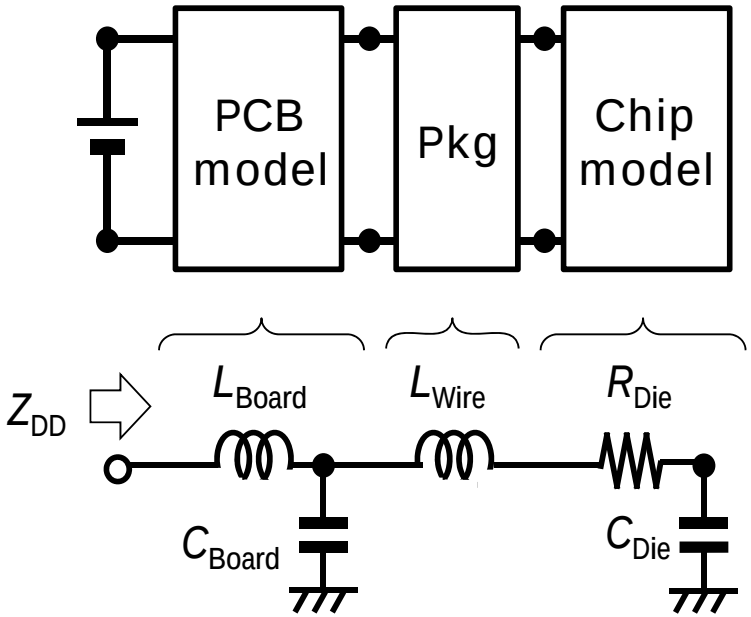
General flow of C-P-S modeling

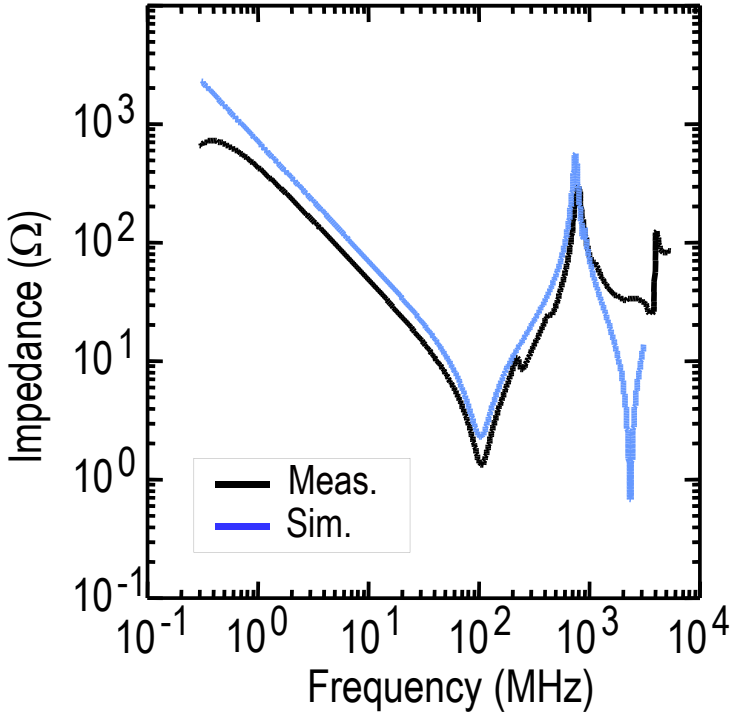


General flow of C-P-S modeling



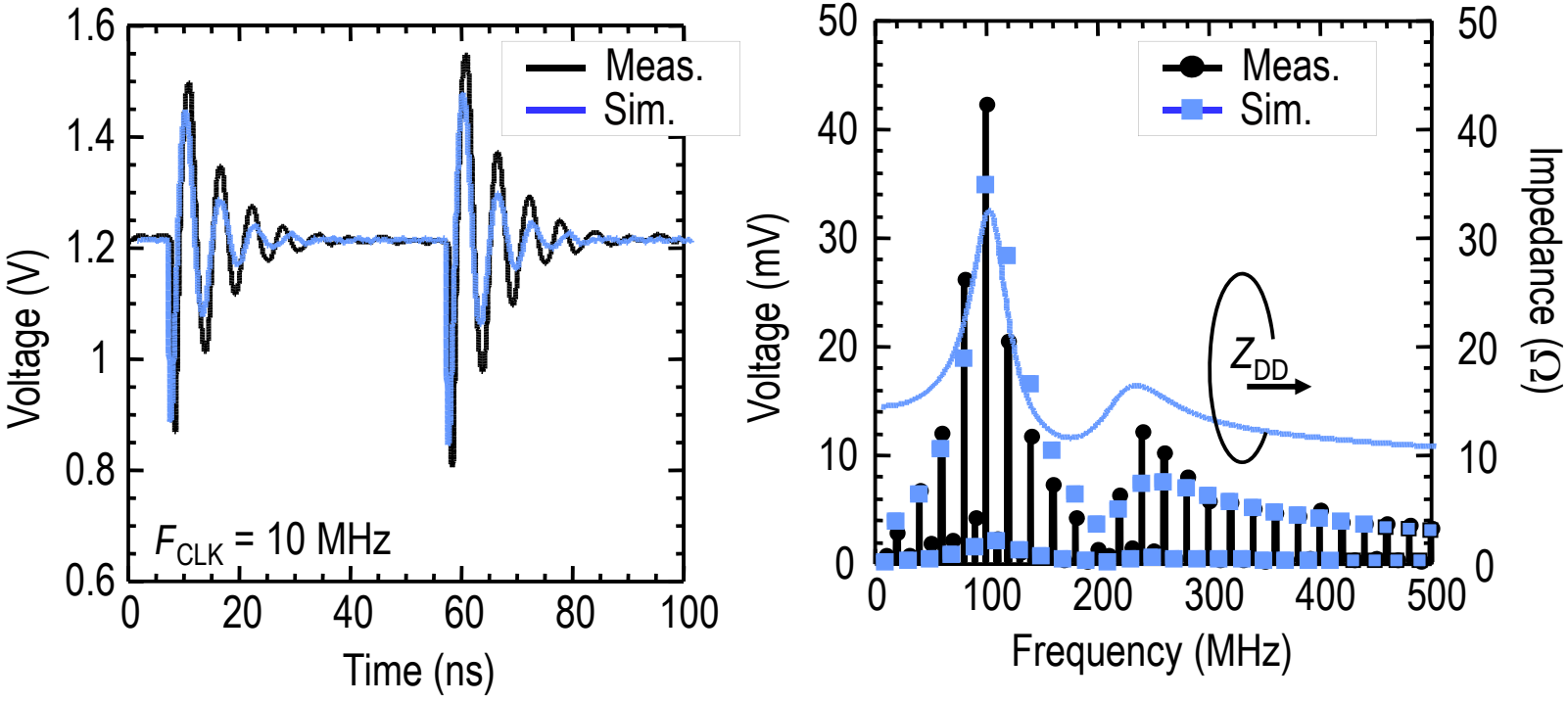
PDN impedance model





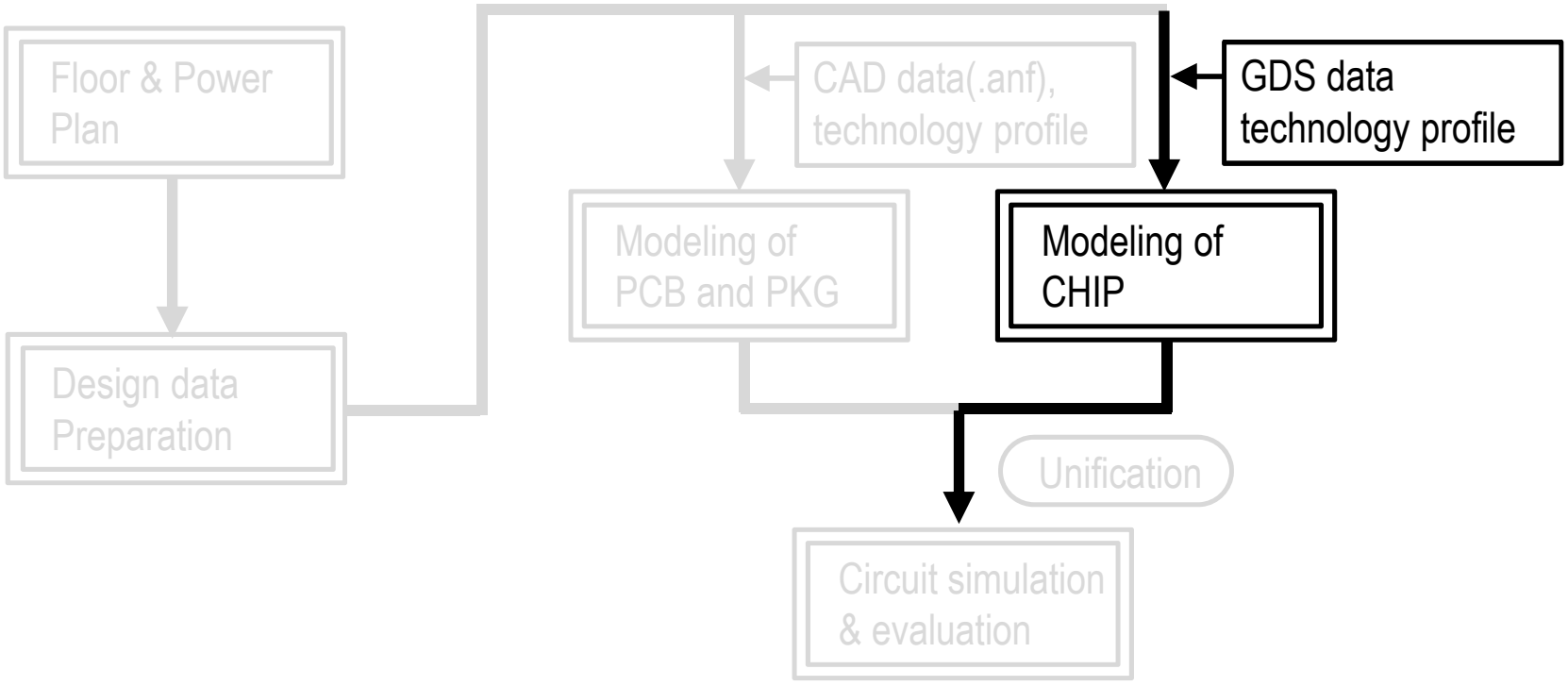
- C-P-B integrated passive model, capturing AC impedance seen from power source side (VDD)

Power noise: C-P-S active interaction

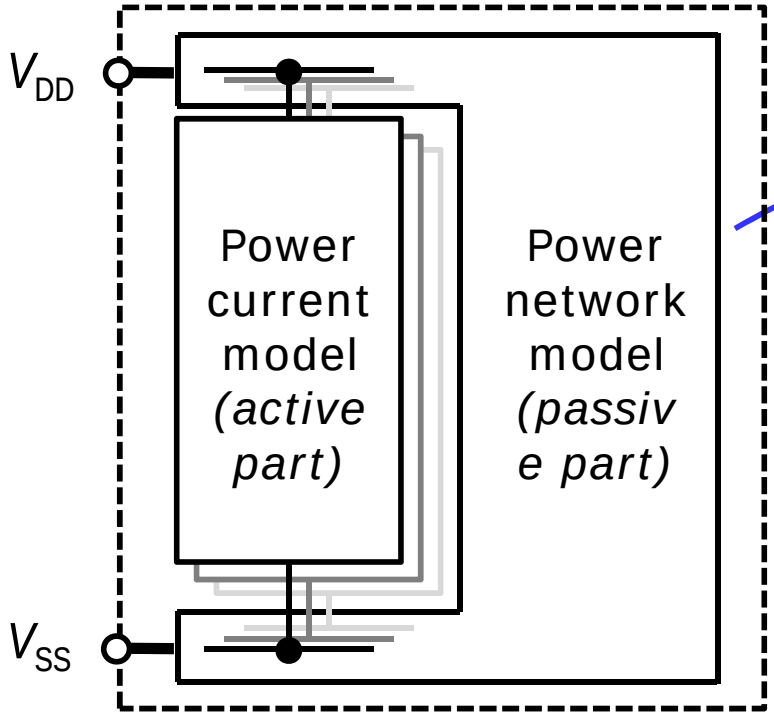


- Power current (I_{DD}, active part of IC) interacts with PDN AC impedance.
- C-P-S integrated models for power noise in IC chips and PCB

General flow of C-P-S modeling



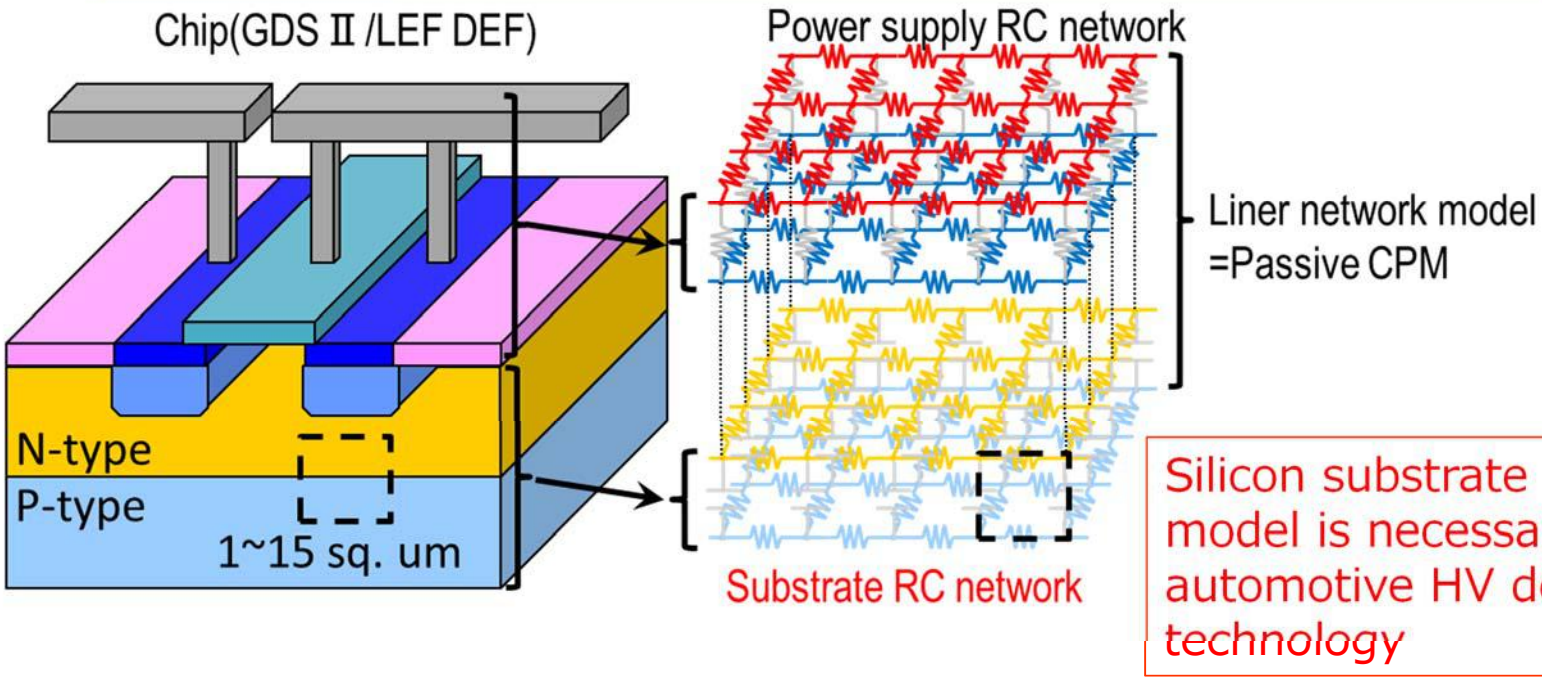
Chip power model



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

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

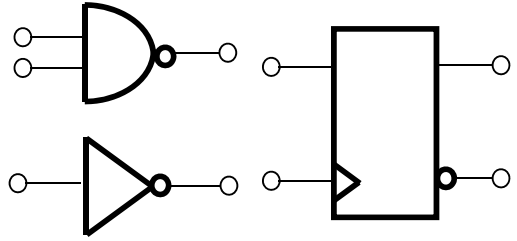
Liner network model (passive part)



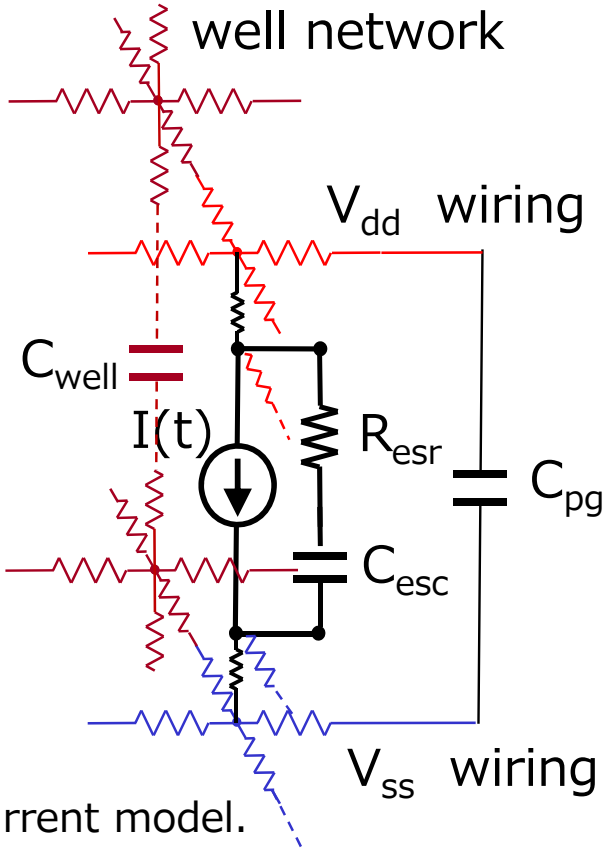
- Liner network model (Passive CPM) -- Reduced and distributed RC network among explicit ports

Power current model (active part)

Standard cell library (LEF/DEF)

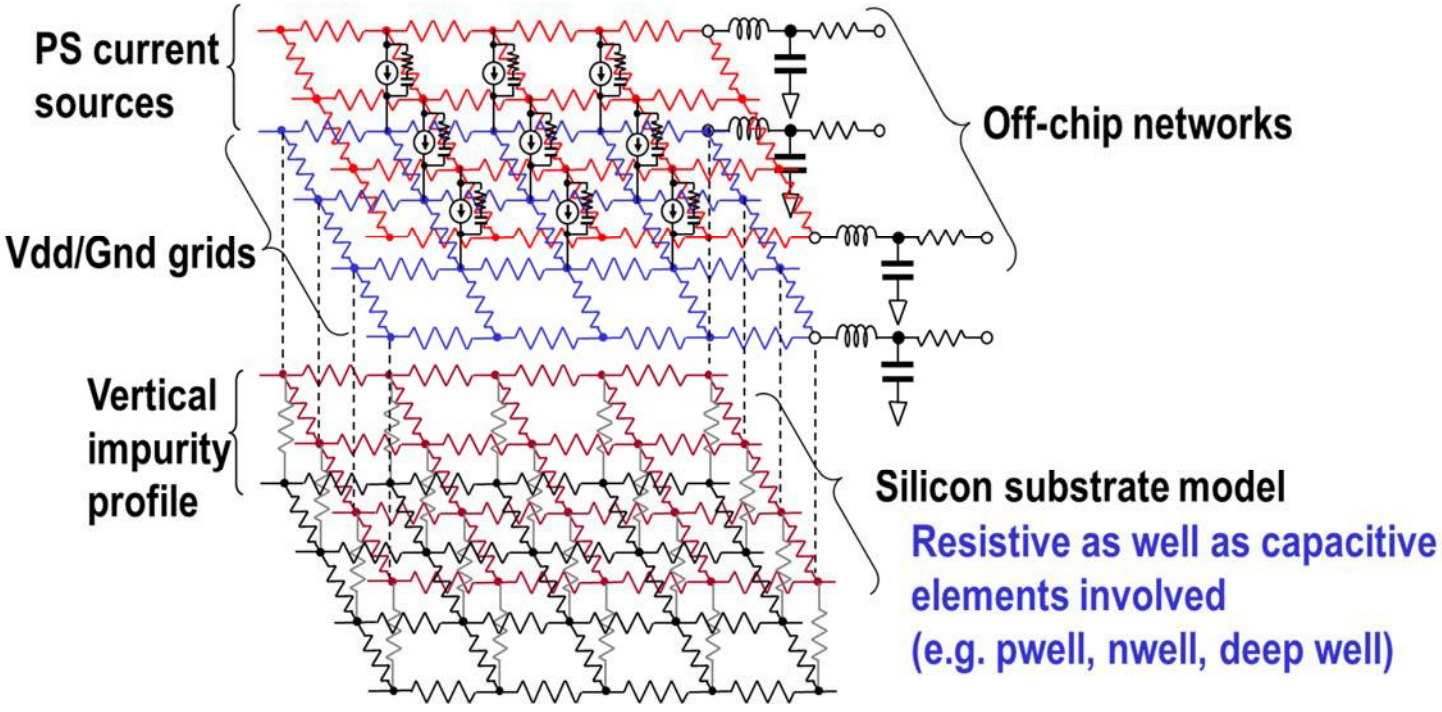


- SPICE simulation: I(t)
  LUT for in/out condition, load caps
- Post-layout extraction
  logic cell level: C_{esc}, R_{esr}



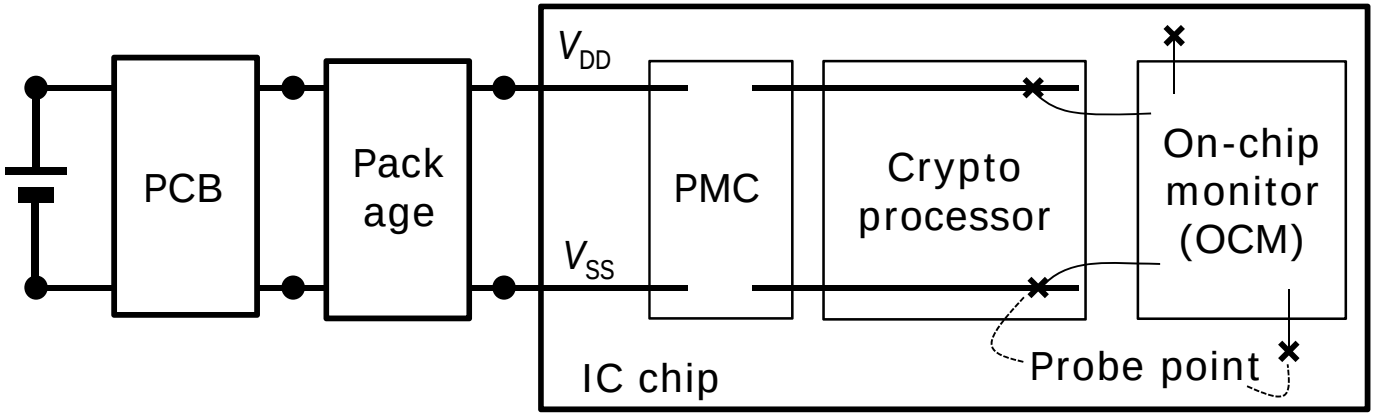
- Cell based -- Logic cells are characterized in power current model.

Full chip level model



- Active current models and passive network models are represented in respective sub circuits and then unified in a single netlist (SPICE compatible).

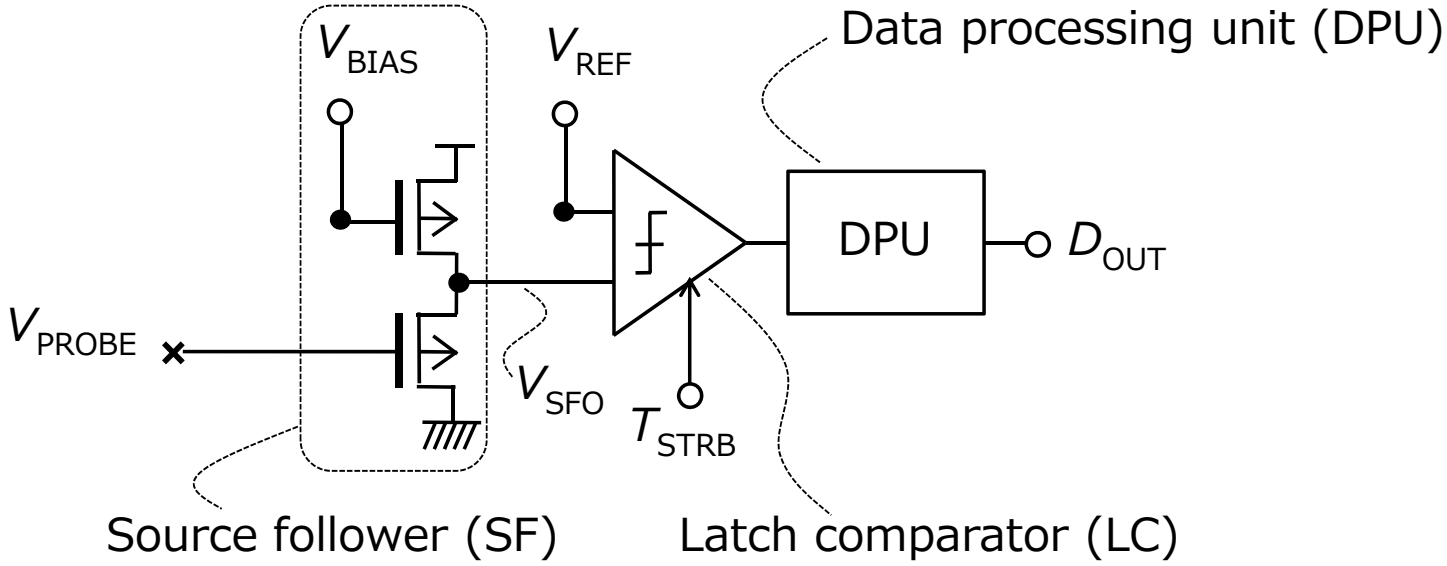
Analysis and diagnosis of SC leakage



- Full-system level simulation of power side-channel (SC) leakage using C-P-S models[1]
- On-die diagnosis of physical attacks using OCM[2]

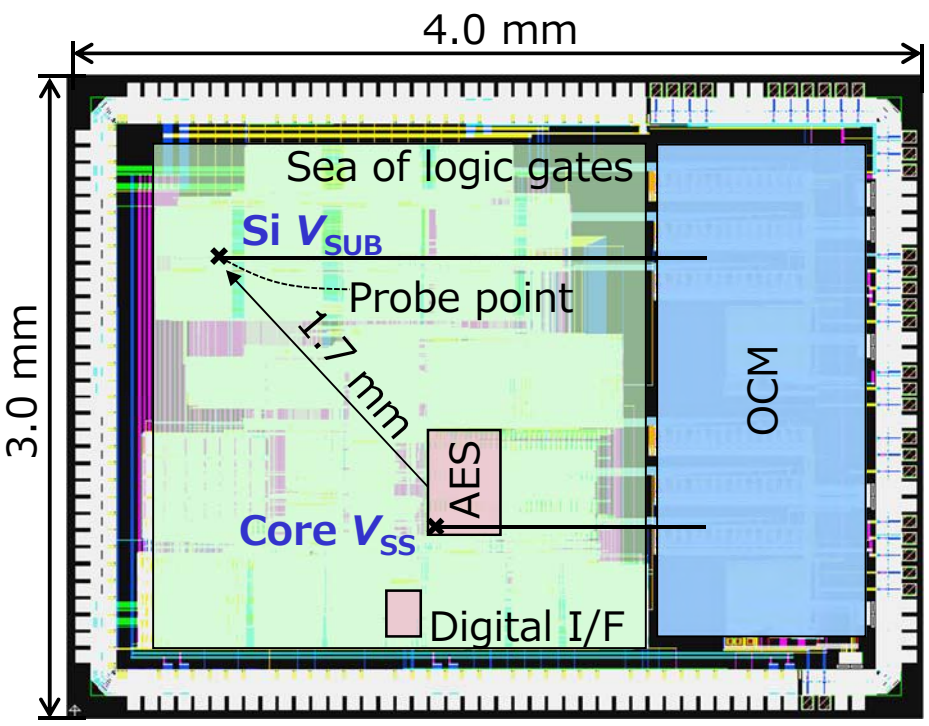
[1]Chip-Package-System board
[2]On-Chip Monitor

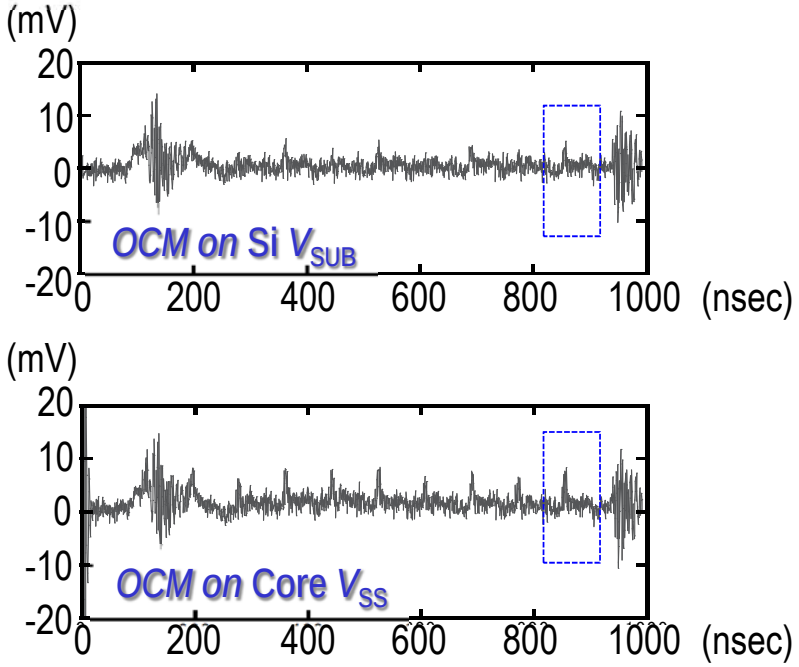
On-chip power noise monitor (OCM)



M. Nagata *et al.*, "Measurements and Analyses of Substrate Noise Waveform in Mixed Signal IC Environment," CICC 1999.

On-chip waveforms during crypto operation

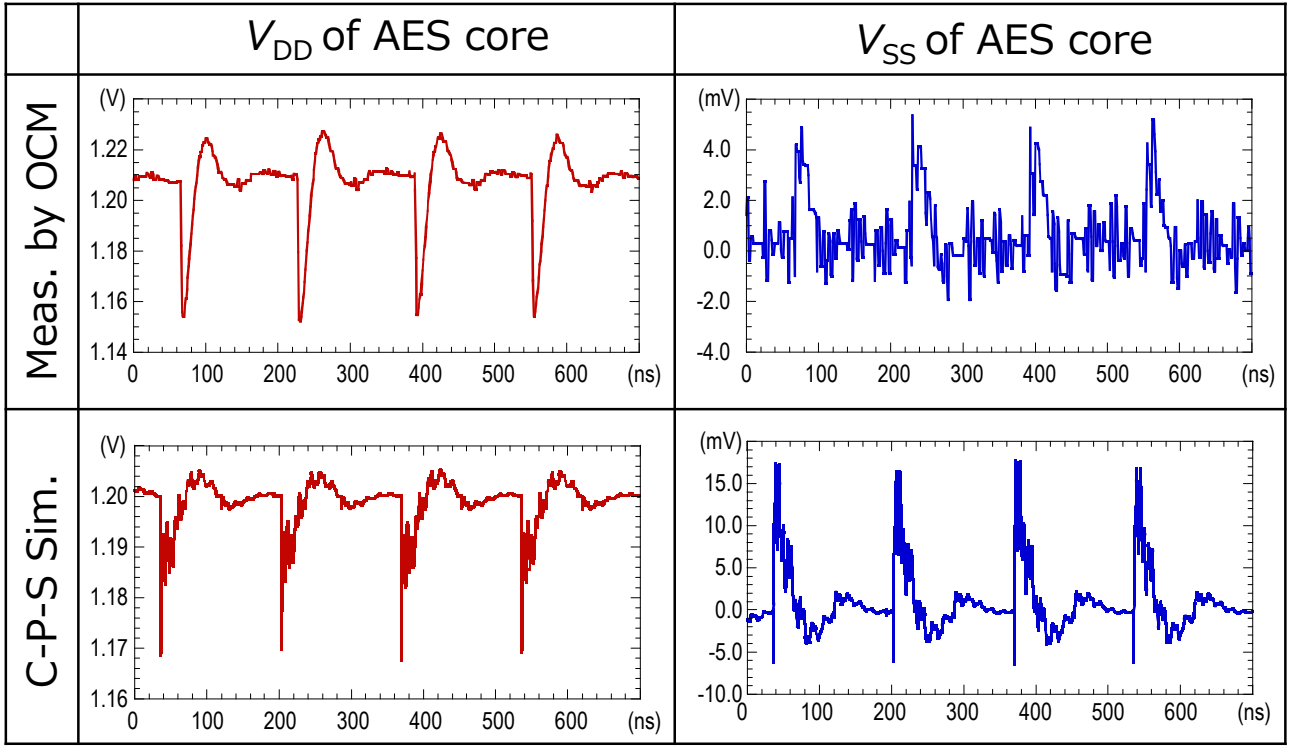




D. Fujimoto *et al.*, "Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip," HOST 2014.

- SC leakage is observable everywhere on a die – even in the backside.

Simulation versus measurements



A. Tsukioka *et al.*, "Active Power Noise Modeling toward Design for EMI Compliance of IC Chips," DesignCon 2017.

Outline

Background

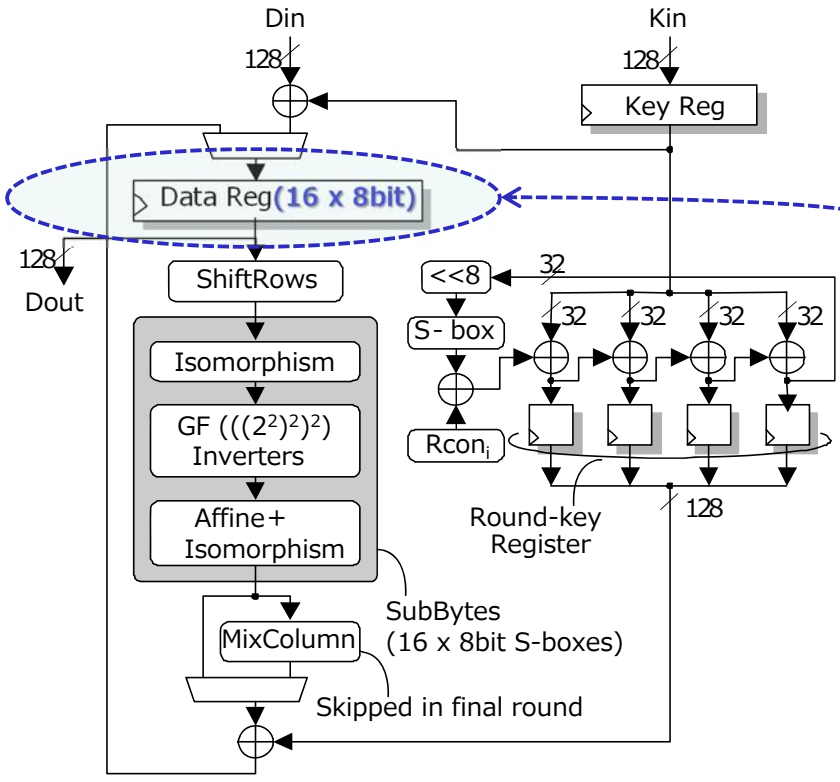
Side-channel attacks

Power noise analysis technique

- Side-channel attack simulation
- Conclusions

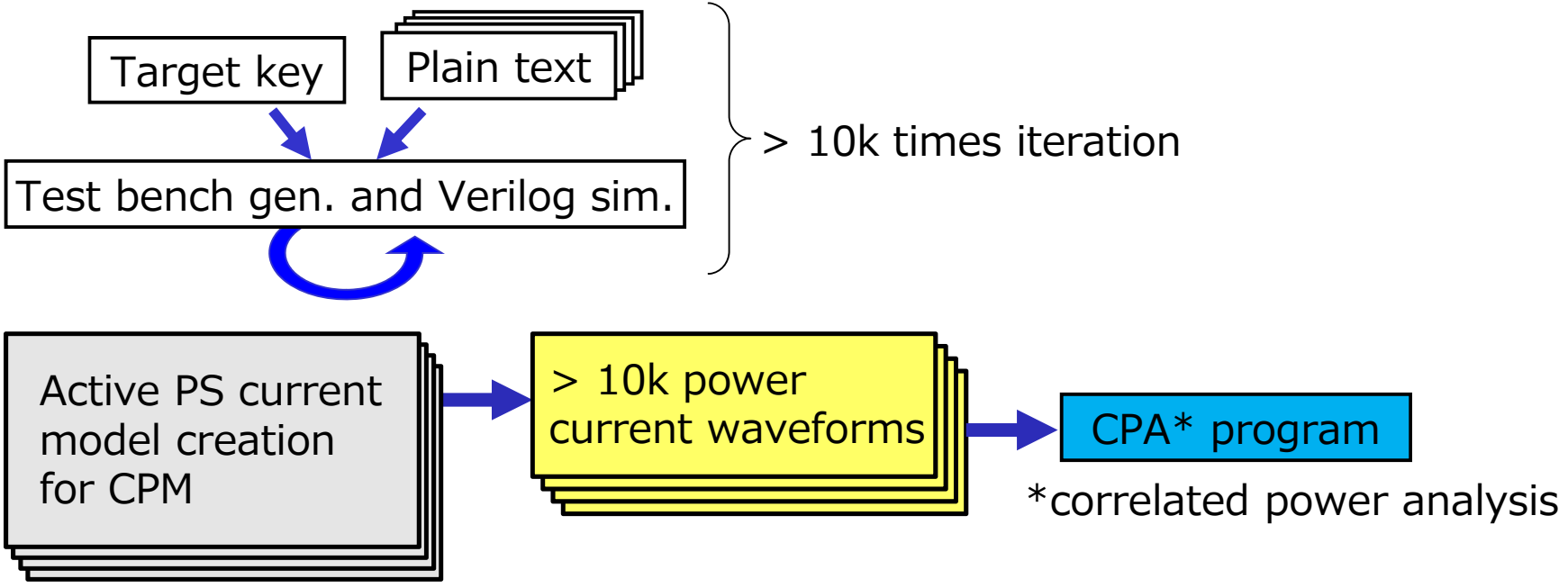
AES* cryptographic architecture

*Advanced Encryption Standard



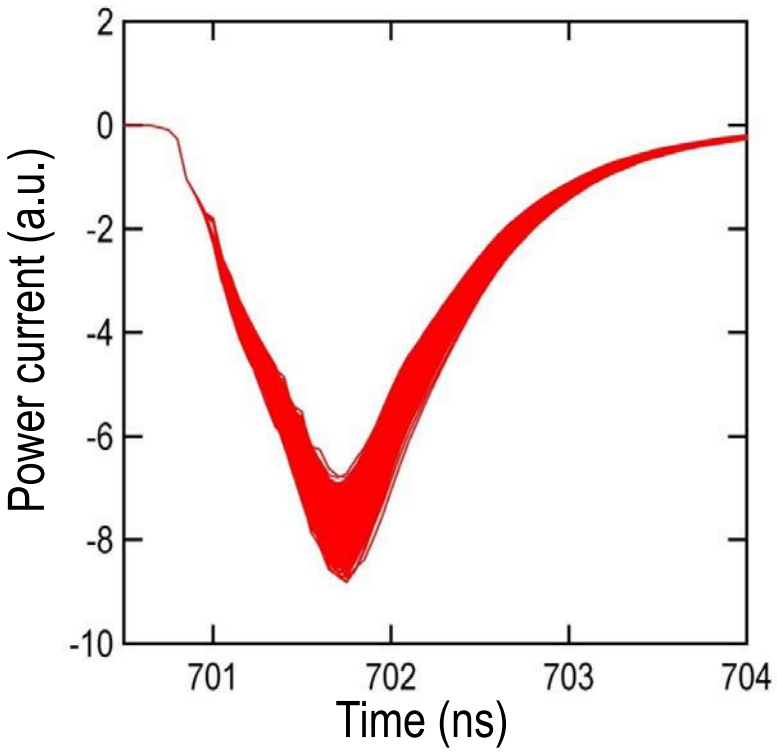
- A single key byte (8 bit) is used in byte-wise crypto computation.
- For AES with 128-bit key, 16 computations running in parallel
- Source of correlation:
  PS current and internal activity measured as Hamming distance

SC leakage simulation flow



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

PS current waveforms for CPA (sim.)



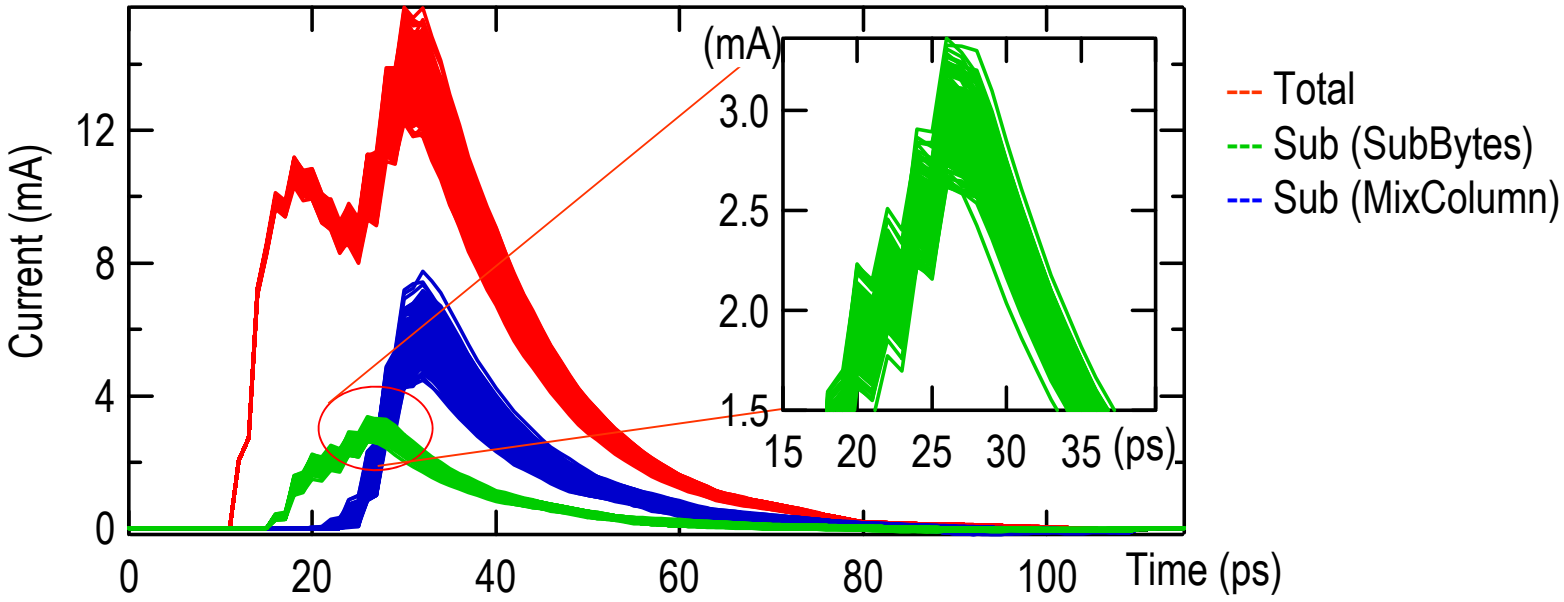
Cost of simulation for 10,000 plain texts

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

280 times acceleration demonstrated

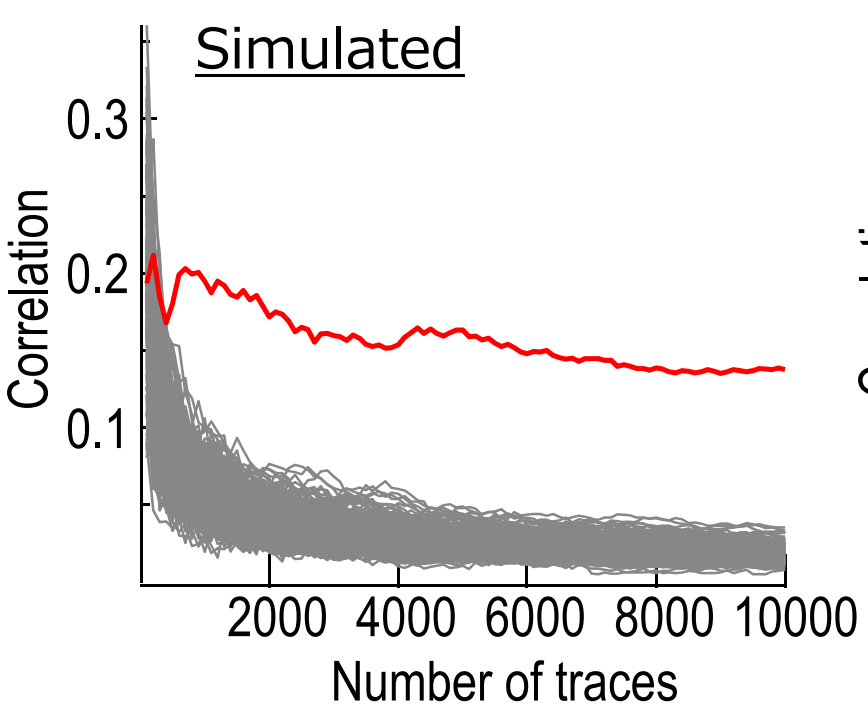
D. Fujimoto, *et al.,* "A Fast Power Current Analysis Methodology Using Capacitor Charging Model for Side Channel Attack Evaluation," HOST 2011.

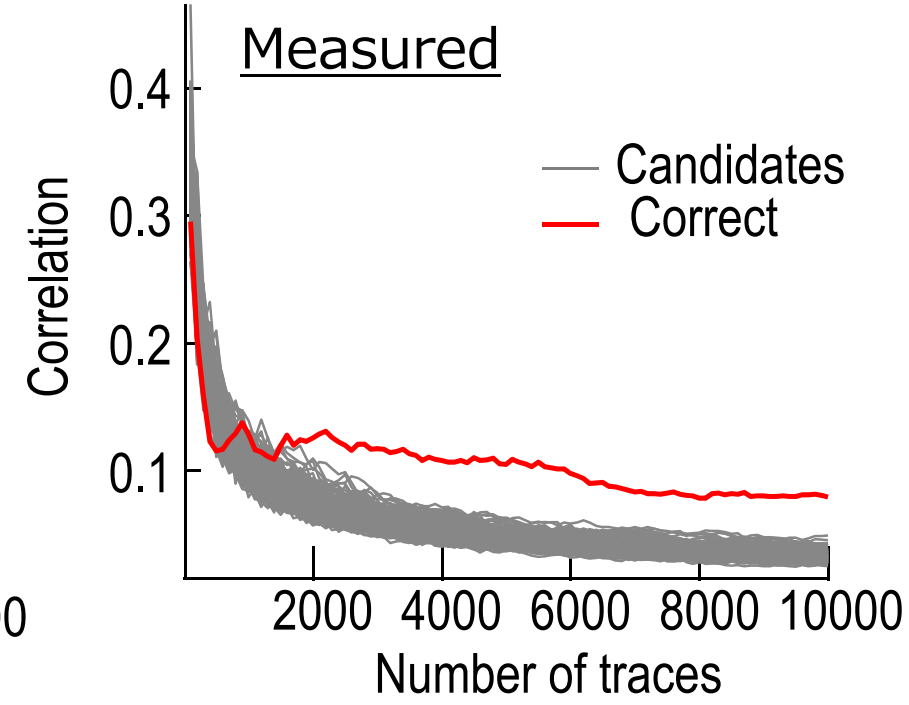
PS current breakdown (sim.)



- Sub (SubBytes) exhibits clear correlation with bits in plain texts, on the other hand, Sub (MixColumn) is shown to be random.

CPA simulation and measurements

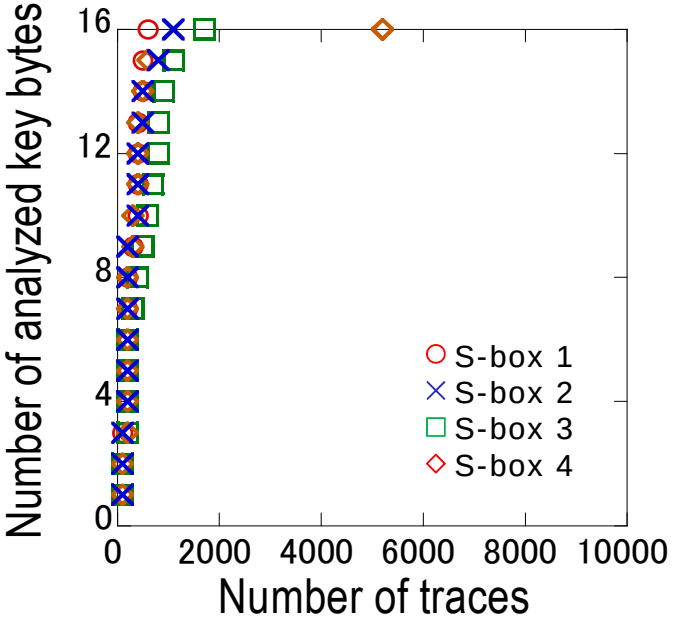




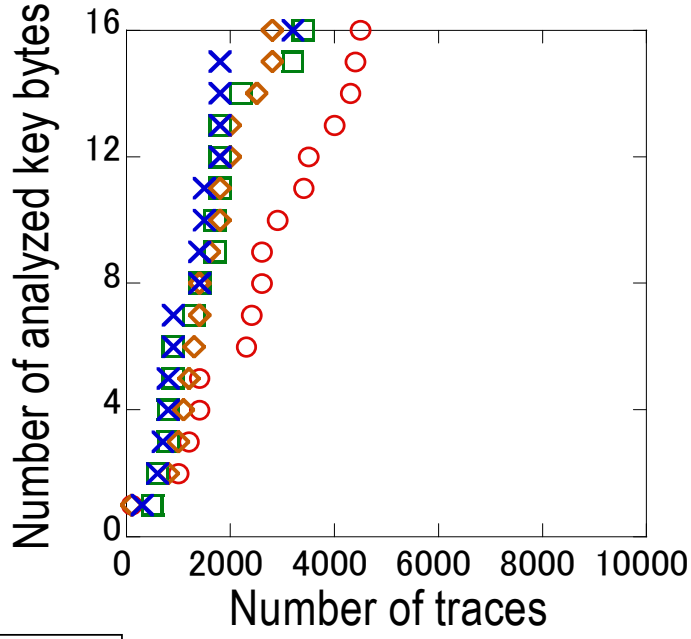
- Correlation between Hamming distance and PS waveforms

SC leakage of AES in 130 nm CMOS

Simulated



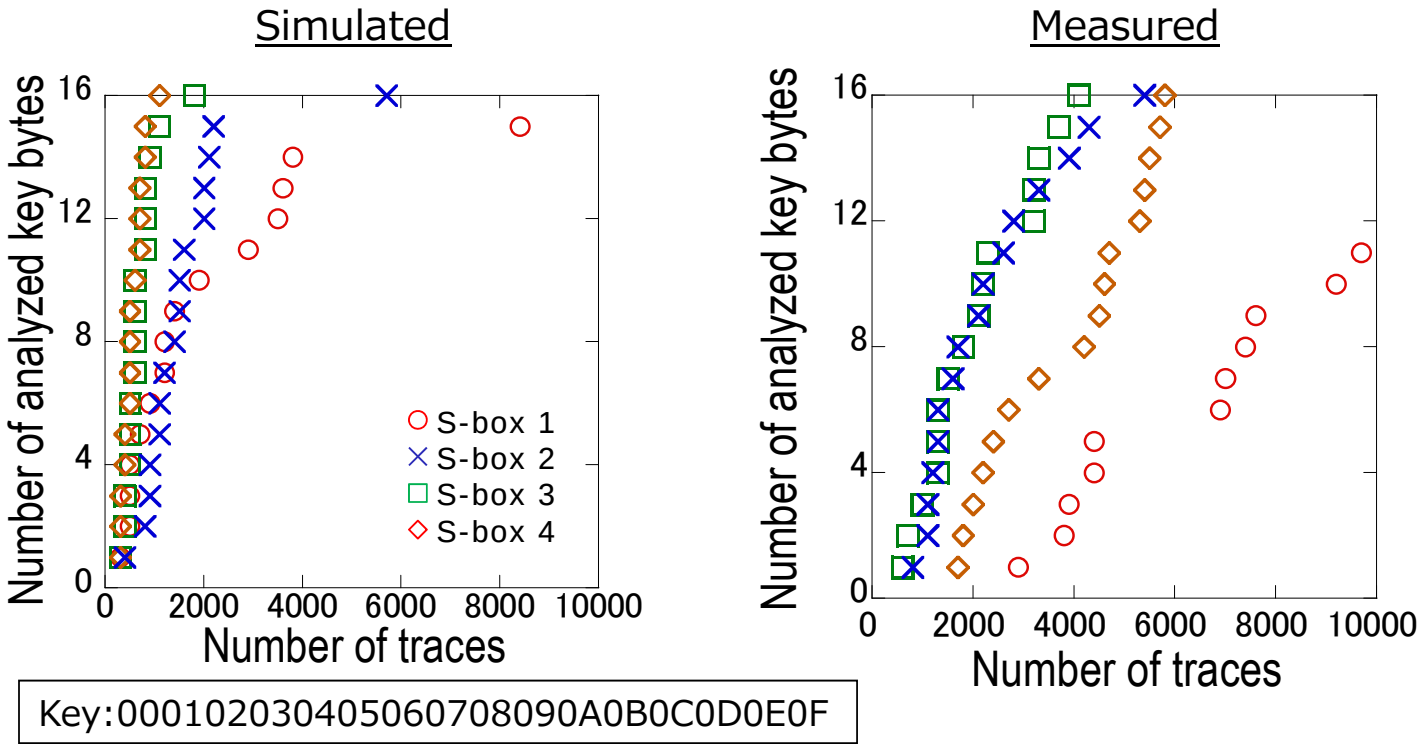
Measured



Key:000102030405060708090A0B0C0D0E0F

- Comparison among 4 different S-box implementations

SC leakage of AES in 65 nm CMOS



- Comparison among 4 different S-box implementations

Conclusion

- **C-P-S power noise simulation accelerates CPA and clarifies vulnerability of AES cores against attacks in design phase.**
  It will play a key role in the co-design of cryptographic circuits and PDNs for suppressing SC information leakage through PS as well as electromagnetic (EM) channels.
- **There are relevant disciplines between EMC and HWS fields.**
  The knowledge (both for emission and immunity) is to be wisely integrated for HW and SW design toward secure and safe society.

Acknowledgements: This work was in part based on results obtained from a project commissioned by the New Energy and Industrial Technology Development Organization (NEDO). The authors would like to deeply thank K. Matsuda, A. Tsukioka, and Prof. N. Miura for their valuable help and valuable scientific discussions.