Chip-Backside Vulnerability to Side Channel Attacks Exploiting Intentional Electromagnetic Interference

Makoto Nagata
Kobe University
Graduate School of Science, Technology and Innovation

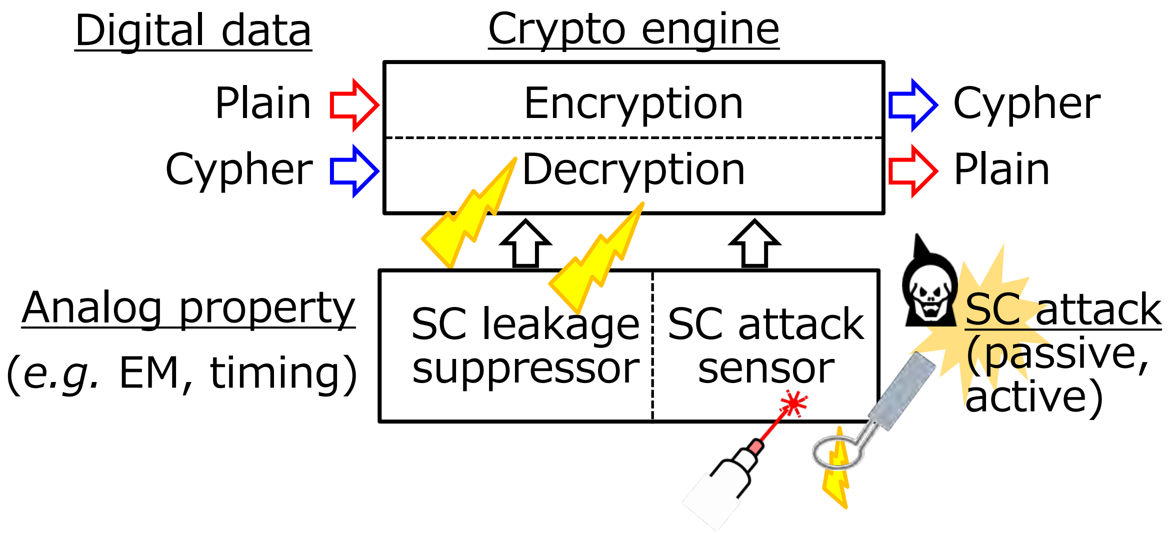
April 18th, 2025

SeaQy
Security, Safety and Quantum

Outline

1. Introduction
2. Passive side channels from IC chip backside
3. Active fault injection on IC chip backside
4. Packaging for security
5. Summary

Analog techniques for digital security



- Analog techniques at the levels of device, circuit, system, package and simulation protect digital security in IC chips.

Makoto Nagata, Noriyuki Miura, and Takuji Miki

Analog Techniques for Digital Security

My gratitudes to visionary discussions

Secure functionality plays a crucial part of SoC integration. Cryptographic engines and random number generators establish data encryption and decryption for secure communication. Semiconductor chip-level ID guarantees the authenticity of a secure system, often enhanced with physically unclonable functions (PUFs.) Secure zones are established through security gateways to incoming and outgoing data. Here, data are digitally represented, and digital circuits dominate secure functionalities. "Hardware security" broadly covers technical fields and scientific communities associated with cryptography and the authenticity of electronics. The associated research topics are naturally cross layer among architectures, algorithms, systems, circuits, and assembly techniques to implement, manage, protect, and sustain the security functionality of SoCs.

Prof. Ingrid Verbauwhede, who is the 2023 recipient of the IEEE Donald O. Pederson Award in Solid-State Circuits, has been leading research communities and promoting technical trends of energy-efficient and high-performance secure ICs and systems. With the aim to proactively develop cross-layer and truly international research activities, a multidiscipline visionary meeting, "Design Methods for Secure Hardware," was initiated by Prof. Verbauwhede, Prof. Patrick Schaumont, and Prof. Kazuo Sakiyama and held in 2011 in the framework of the National Institute of Informatics (NII) Shonan Meeting, in Japan (Figure 1) [1]. It gathered 21 participants from academia and

Digital Object Identifier 10.1109/MSSC.2022.3219780
Date of current version: 18 January 2023

1943-0582/23©2023IEEE

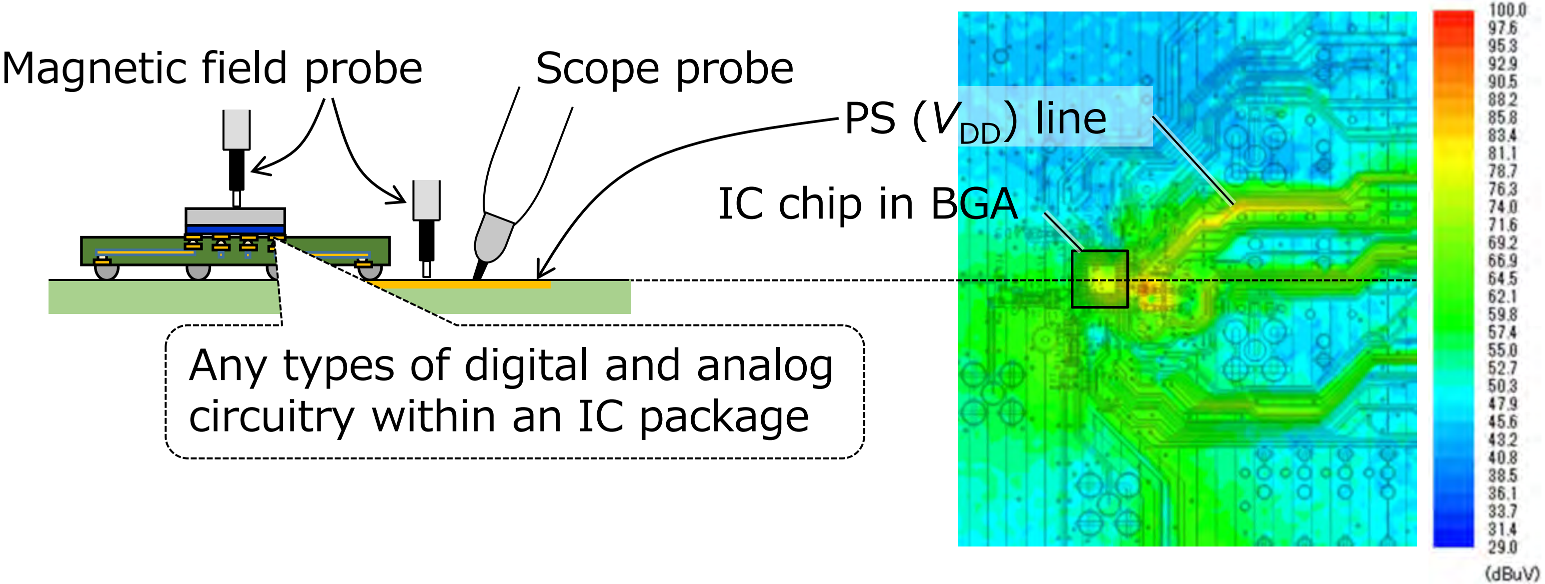
IEEE SOLID-STATE CIRCUITS MAGAZINE / WINTER 2023 25

IEEE Solid-State Circuits Magazine (SSCM), Jan. 2023. DOI: 10.1109/MSSC.2022.3219780

Electromagnetic compatibility (EMC)

IC system-wide EMC

Field map (top view)



- EM noise and power noise from an IC chip are observable on its package and across a whole printed circuit board (PCB).

Relevance among EMC and HWS

EMI

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

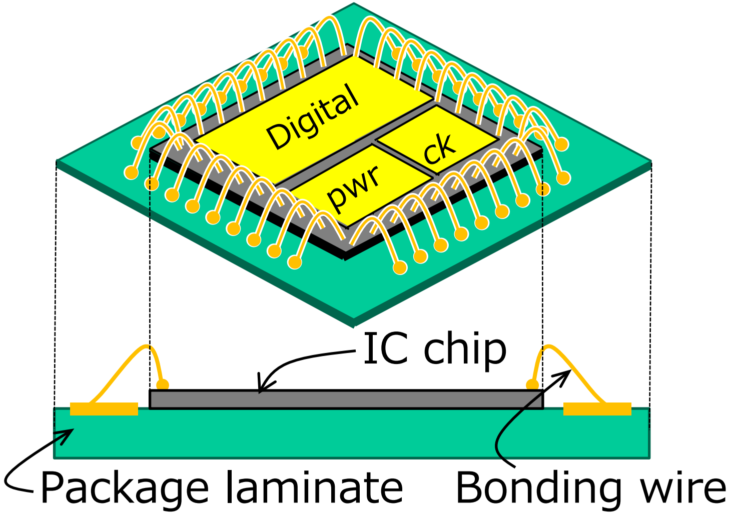
EMS

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

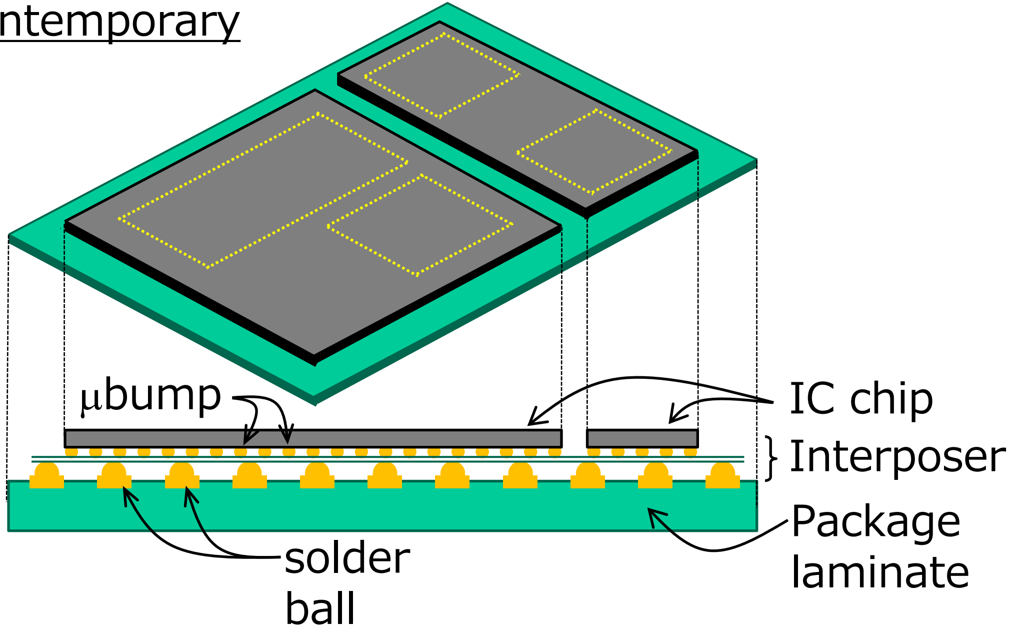
In-depth understandings of IC-chip level EMC, toward the quality design of IC chips for hardware security

Face-up and flip-chip assembly

Traditional

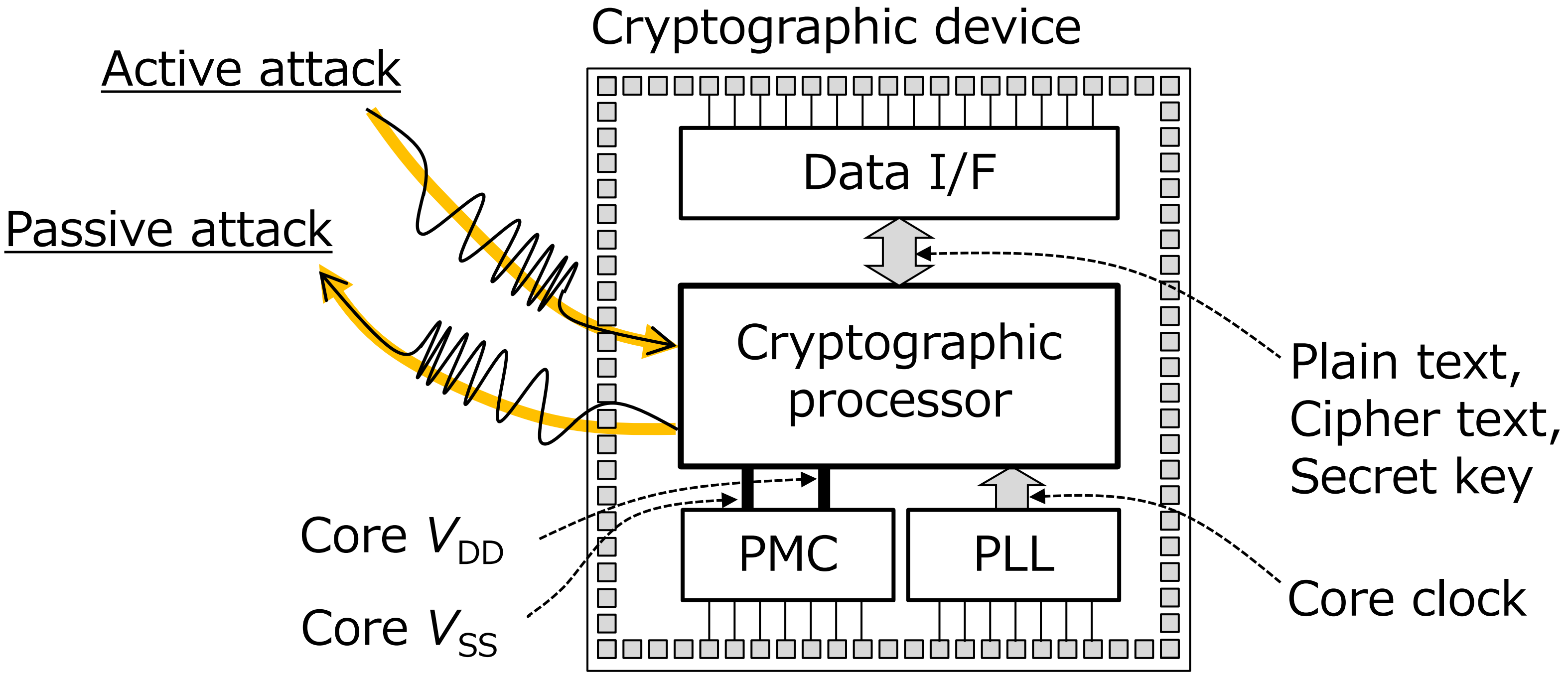


Contemporary



- ► Mega trends: flip chip on membrane interposer with multiple chip(lets)
- ► Silicon substrate backside is open for performance improvements (pros) while also for adversarial approaches (cons).

Physical isolation at IC chip level

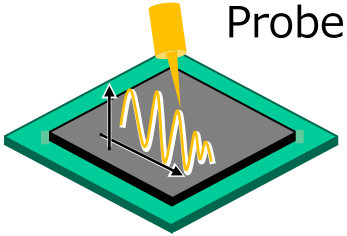


- Architectural explorations for securing horizontal data channels while circuit- and package-level countermeasures needed for vertical EM channels.

Outline

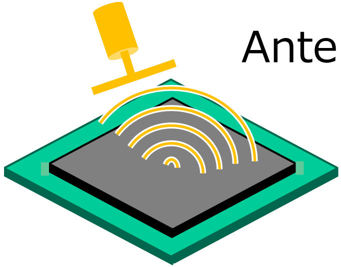
1. Introduction
2. Passive side channels from IC chip backside
3. Active fault injection on IC chip backside
4. Packaging for security
5. Summary

Passive side channels on Si backside



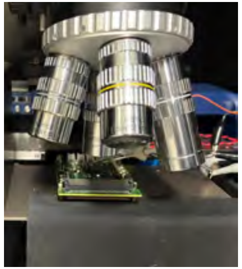
Probe/needle

- ✓ Si substrate voltage
- ✓ Electric field



Antenna/coil

- ✓ EM waves
- ✓ Magnetic flux



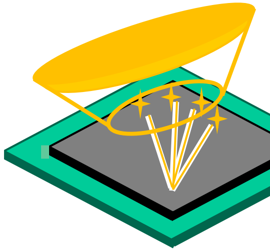
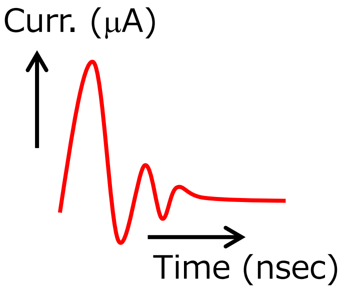


Photo sensor

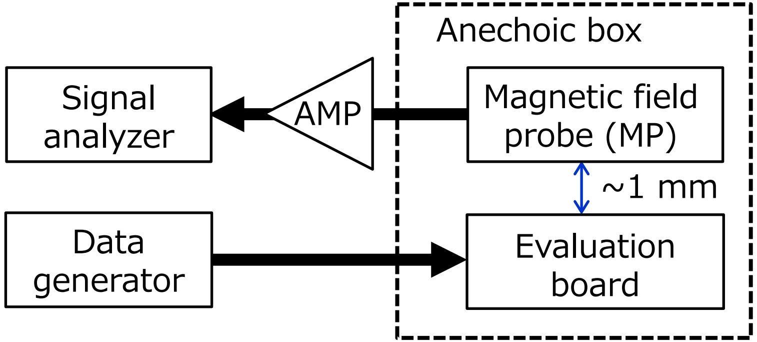
- ✓ IR photons
- ✓ IR microscopy



Matter of power current

IEEE Open Journal of the Solid-State Circuits Society (OJ-SSCS), Nov. 2024.
DOI: 10.1109/OJSSCS.2024.3499967

Electromagnetic (EM) emission by ICs



Anechoic box

Signal analyzer

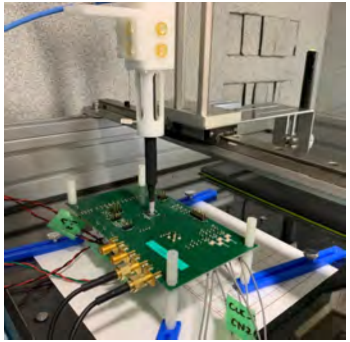
AMP

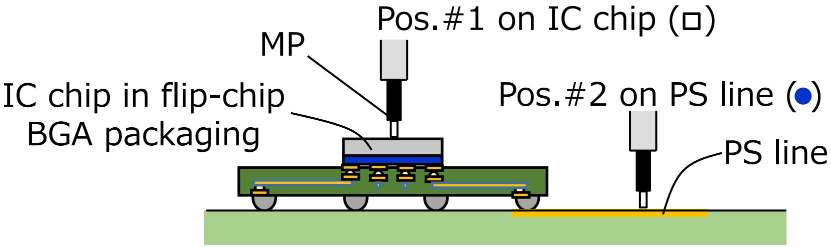
Magnetic field probe (MP)

~1 mm

Data generator

Evaluation board





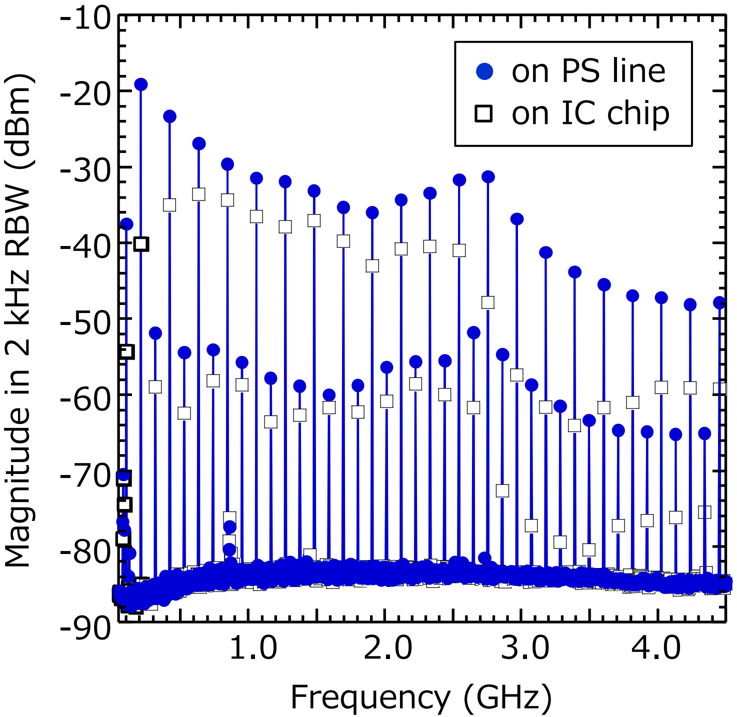
Pos.#1 on IC chip (□)

MP

IC chip in flip-chip BGA packaging

Pos.#2 on PS line (●)

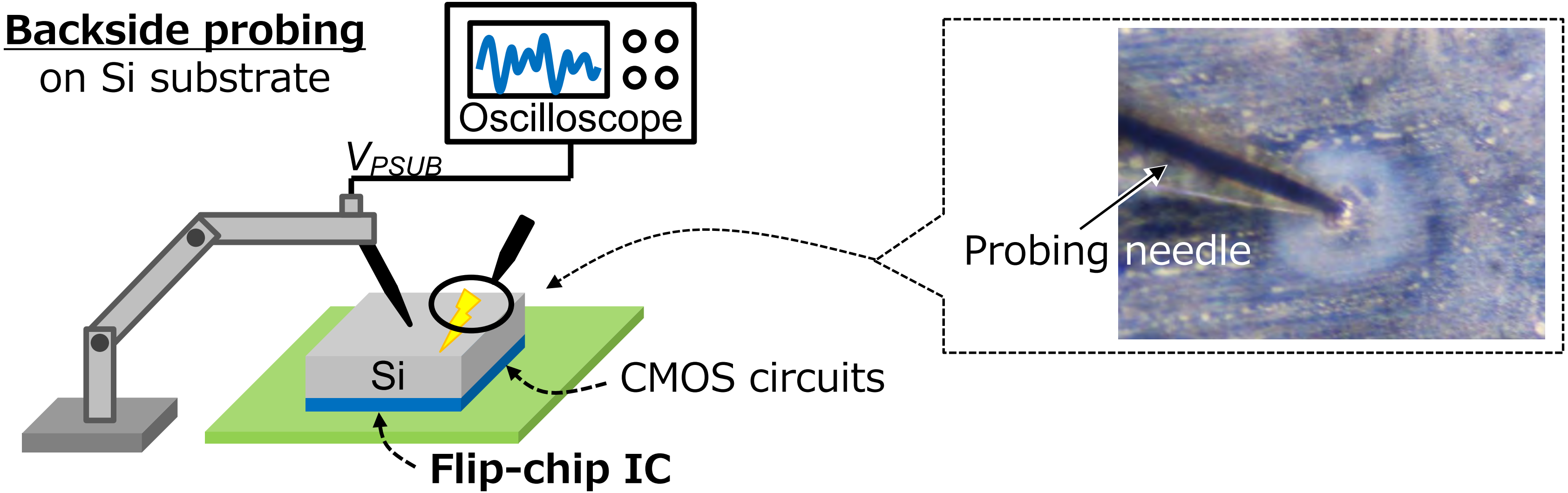
PS line



▶ **<u>Near field magnetic coupling between an IC chip and an antenna</u>** exhibits high order harmonics of digital clocking frequency *(e.g. 106 x n MHz.)*

Si substrate voltage variation

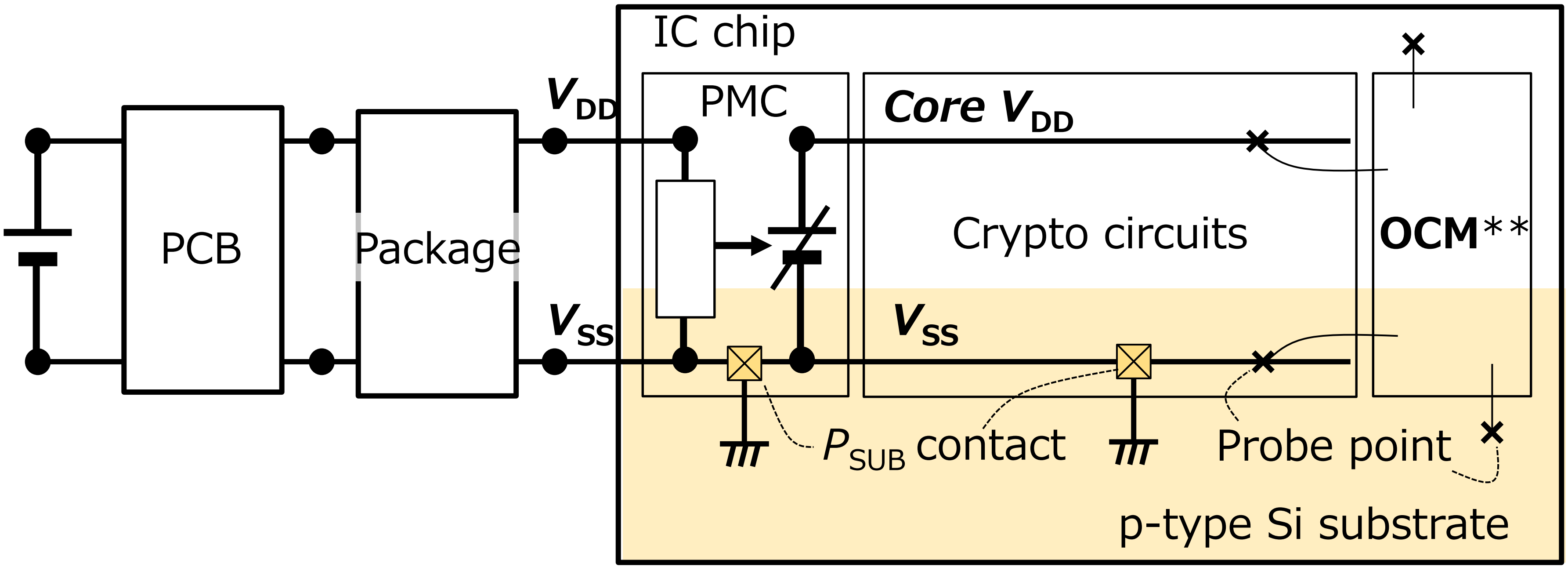
Backside probing
on Si substrate



- **Direct voltage probing on Si substrate backside (=IC chip backside)** with a metallic needle

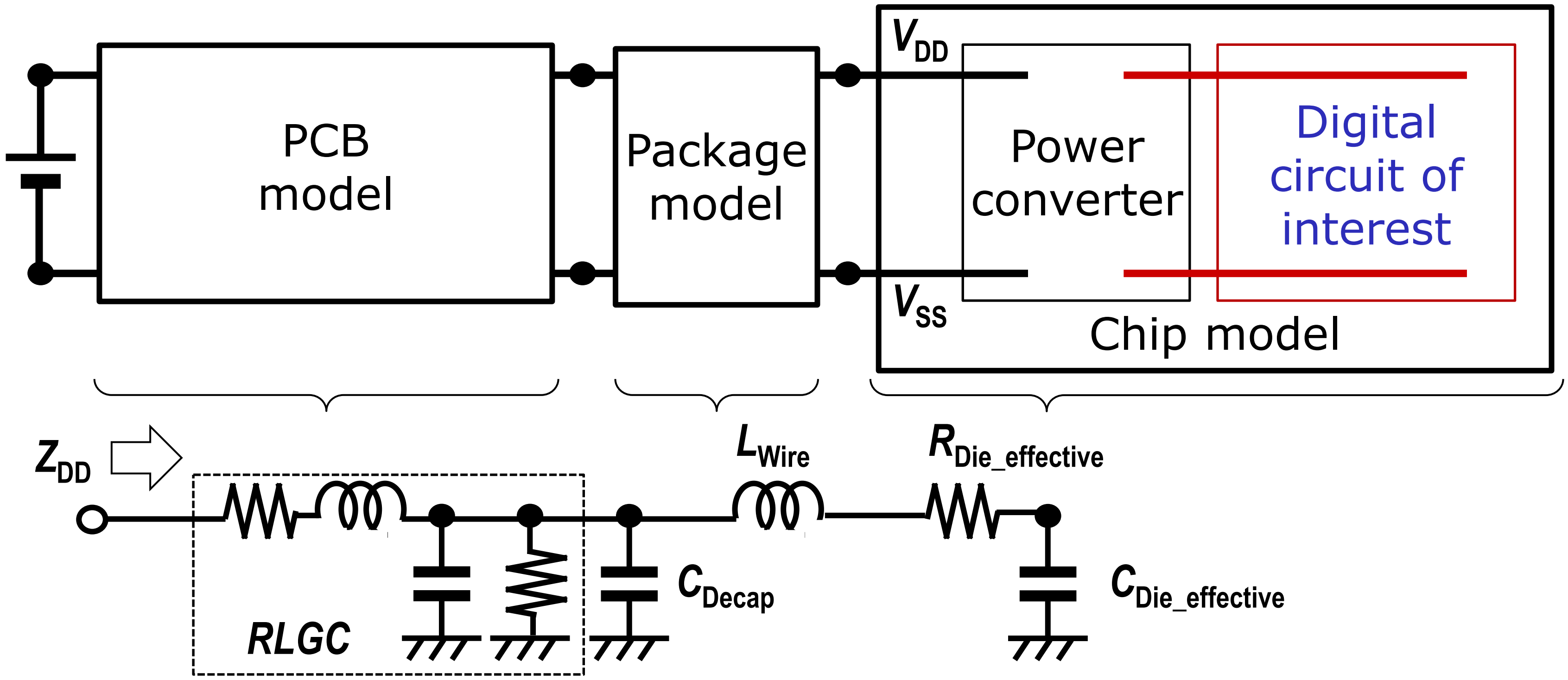
Si substrate as a part of PDN*

*Power delivery network
**On-chip monitor circuit



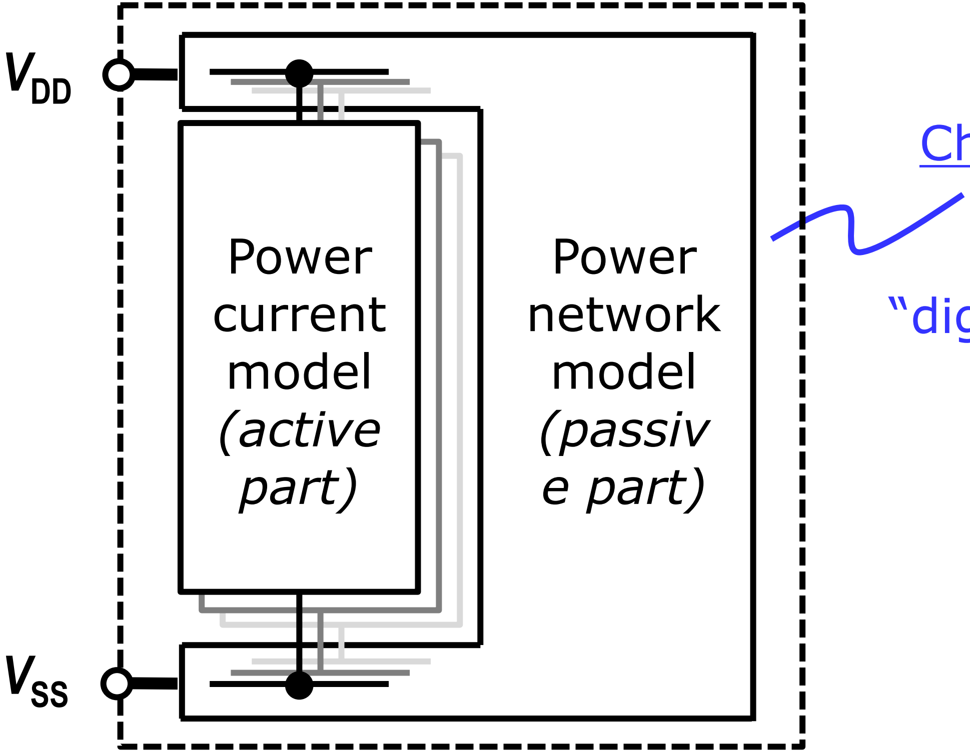
- **Si substrate** is a part of PDN (often of ground side) and the most prominent attack surface in flip-chip assembly (*e.g.* BGA).

System-level power noise analysis



- **Chip-Package-System board (CPS) model** used in system level simulation of power noise generation and propagation

Chip power model

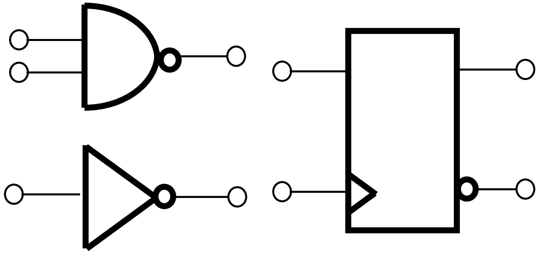

V_{DD}
V_{SS}
Power current model (active part)
Power network model (passiv e part)

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

- A power delivery network involving multiple power current models

Power current - active part of model

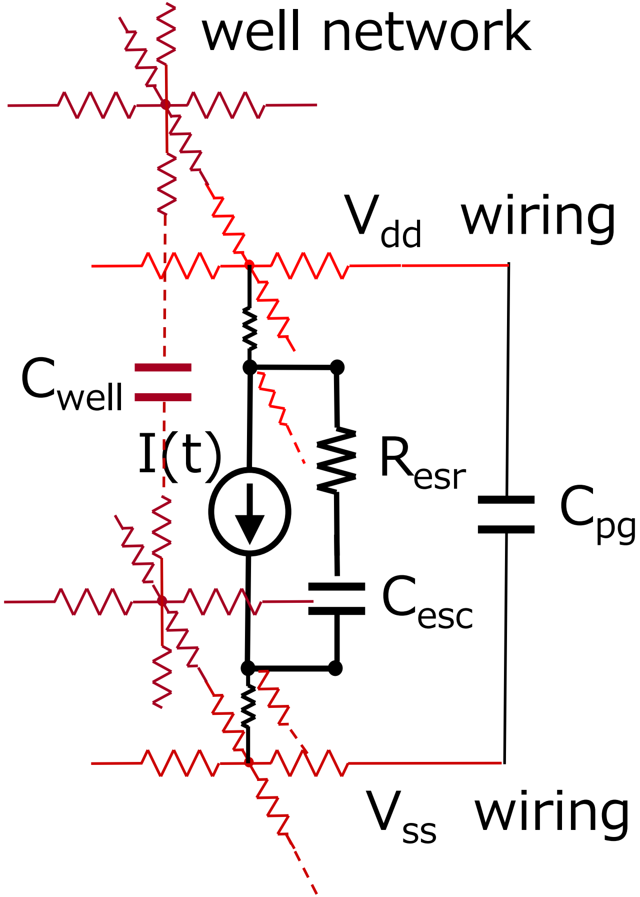
Standard cell library (LEF/DEF)



- SPICE simulation: I(t)

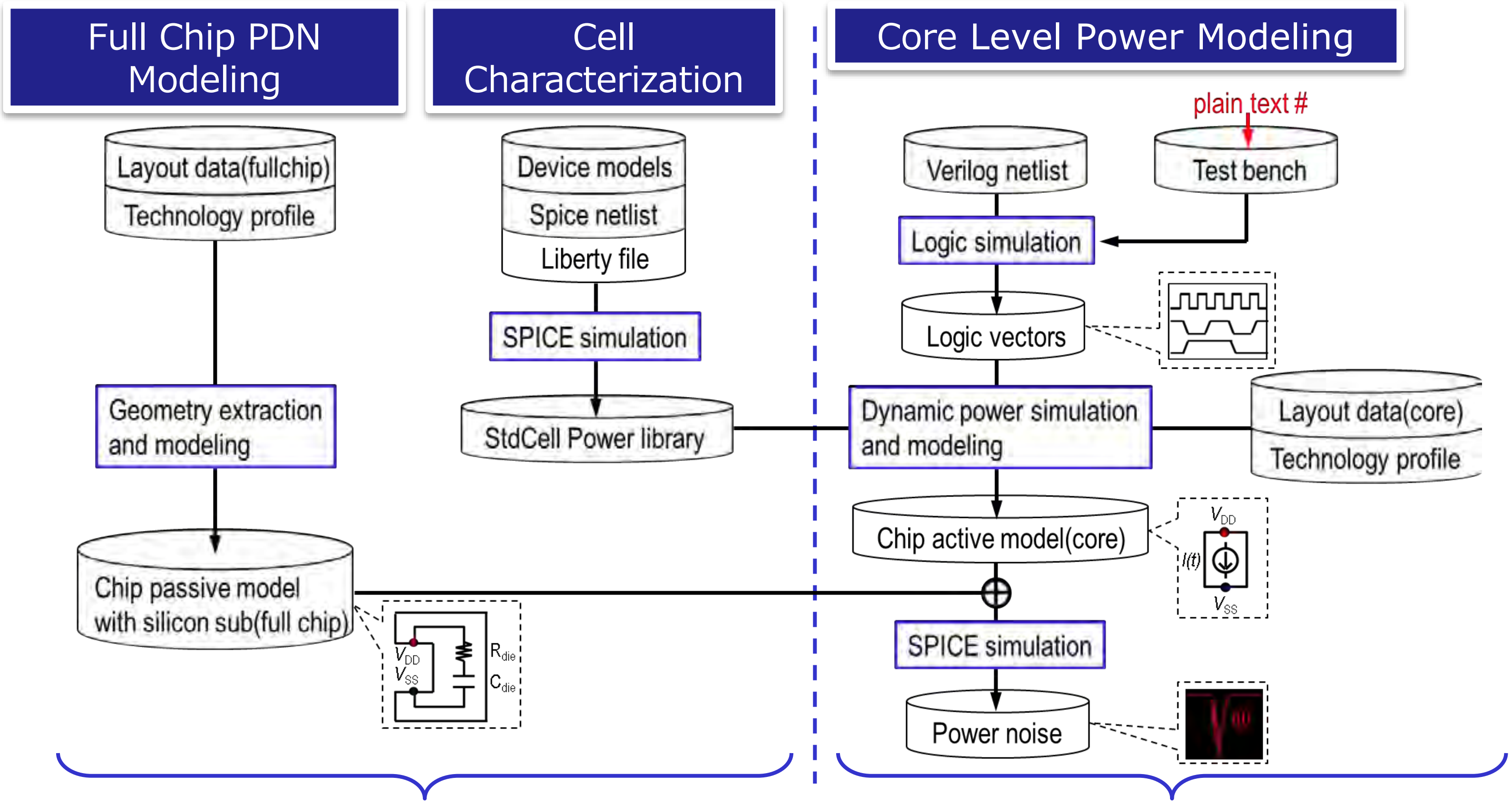
  LUT for in/out condition, load caps
- Post-layout extraction

  logic cell level: C_{esc}, R_{esr}



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

CPS power noise simulation flow

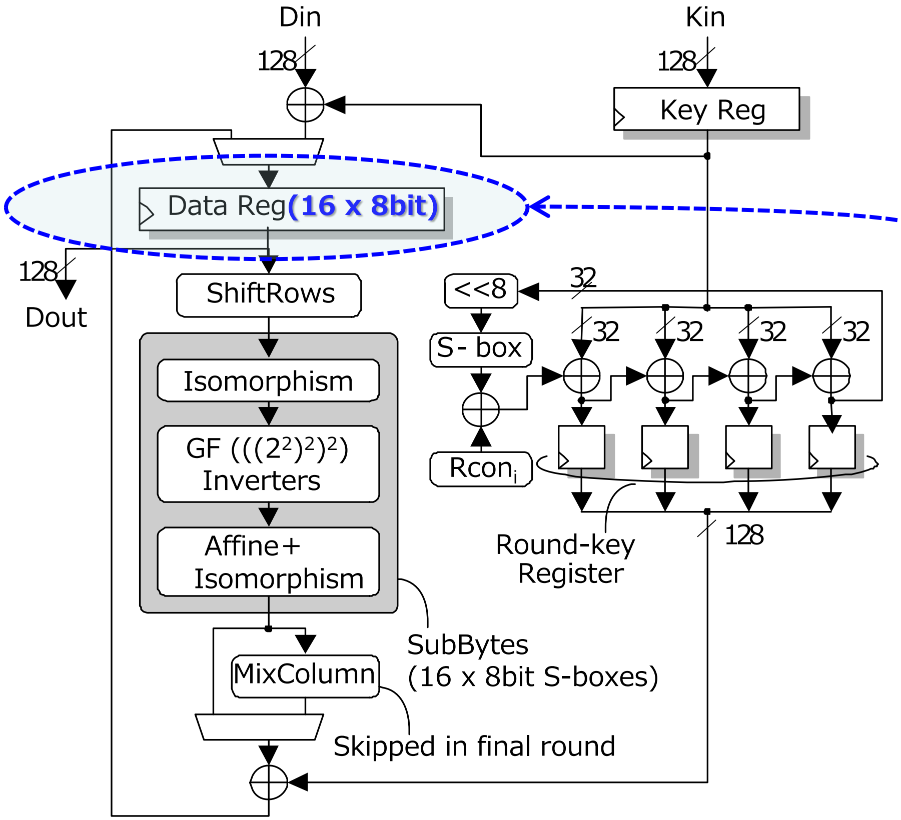


Prepare passive part of CPM and power library

Update active part of CPM with toggle scenarios

AES* cryptographic architecture

*Advanced Encryption Standard

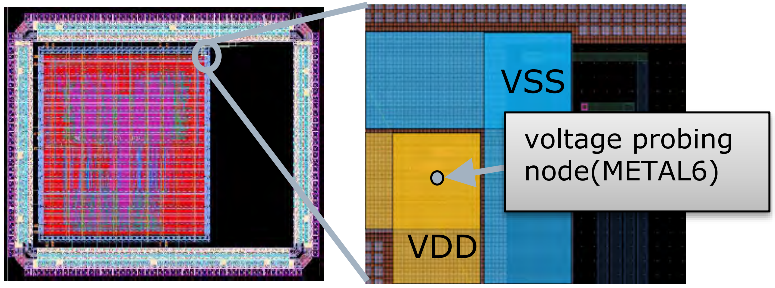


Power side-channel (SC) leakage in AES datapath

- A single key byte (8 bit) is used in byte-wise crypto computation.
- For a 128-bit key, 16 computations running in parallel
- Correlation of power current and internal activity measured as Hamming distance in a data register

AES power noise simulation

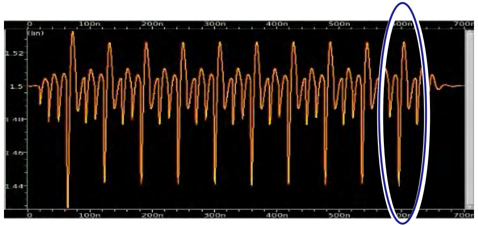
- Case study: private-key crypto IC chip
  - ✓ AES encryption engine (34 K gates)
  - ✓ Operation frequency: 34 MHz

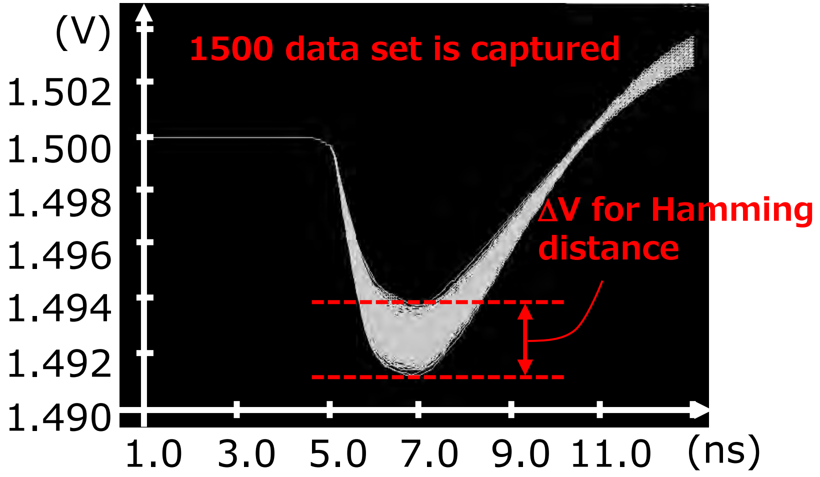


voltage probing node(METAL6)

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

Last round of encryption





1500 data set is captured

ΔV for Hamming distance

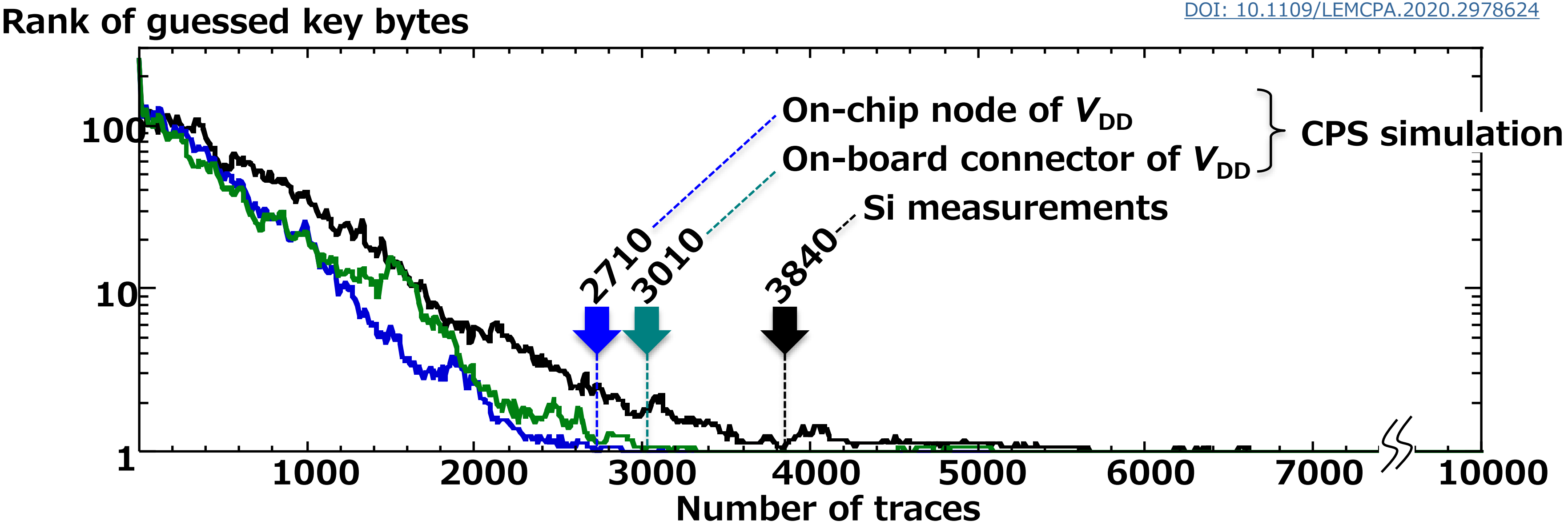
- Simulation cost evaluation

	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

Intel Xeon CPU ES-2699 v4 (2.2GHz)

CPA on AES core

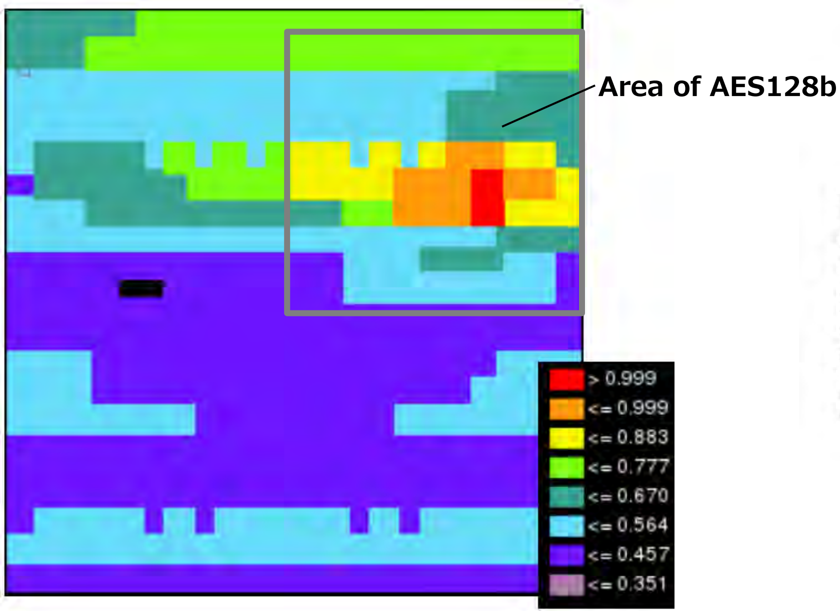
IEEE Letters on Electromagnetic Compatibility Practice and Applications (L-EMCPA), Dec. 2019.
DOI: 10.1109/LEMCPA.2020.2978624



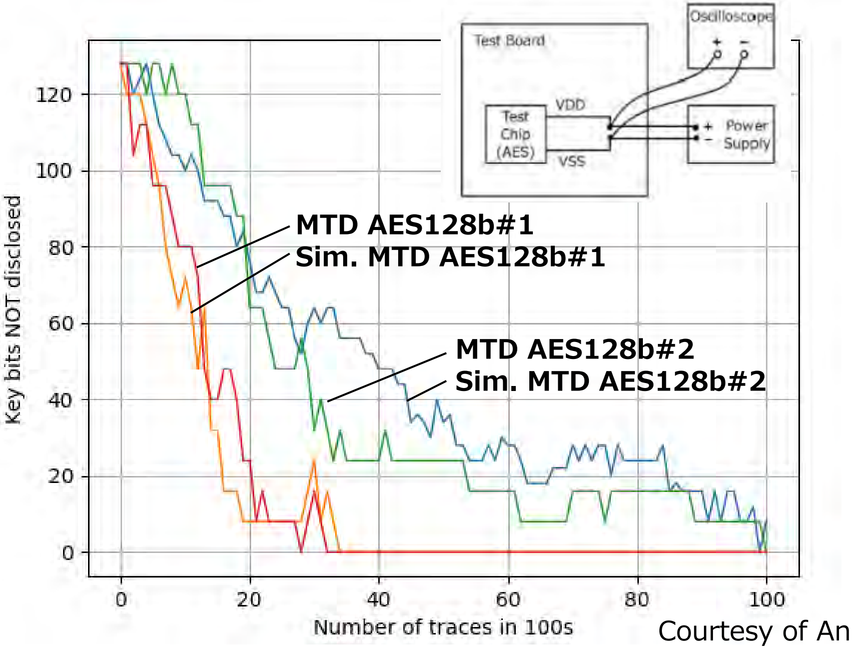
- On-chip measured and CPS simulated power traces for AES 128 bit w/ randomly generated 10k payloads
- Secret 16 key bytes are finally revealed, most pessimistic at on-chip nodes.

Power SC leakage at full-chip level

Power side-channel leakage correlation score (P-SLS)



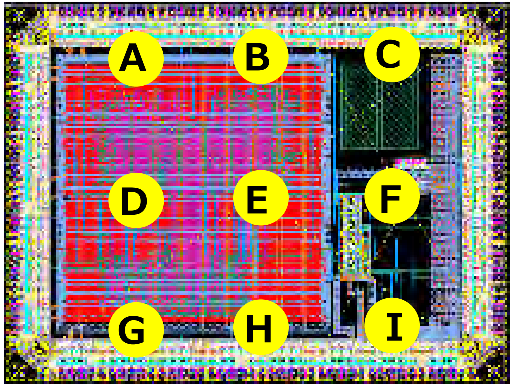
Measurement-to-disclose (MTD)



Courtesy of Ansys

- Chip-level power SC leakage analysis using CPMs
- Direct vector control on security sensitive nets while vector-less mode on non-security nets over an IC chip.

EM SC leakage over IC chip package



Test vehicle

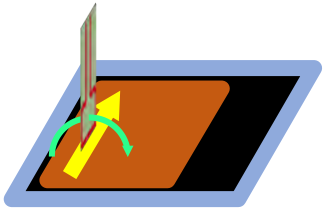
Crypto: 128bit AES

Tech.: 130 nm CMOS

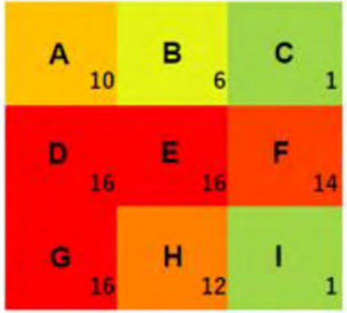
Chip area: 3 mm x 4 mm

Power supply: 1.5 V

B_X Direction

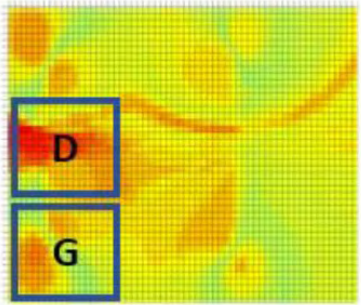


B_X Meas.

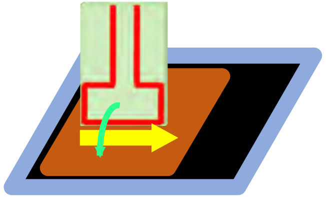


A 10	B 6	C 1
D 16	E 16	F 14
G 16	H 12	I 1

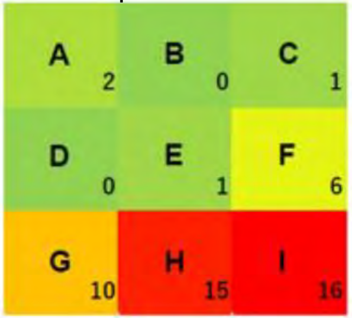
B_X Sim.



B_Y Direction

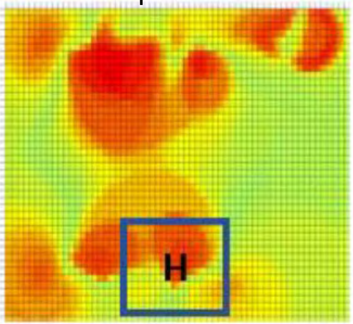


B_Y Meas.



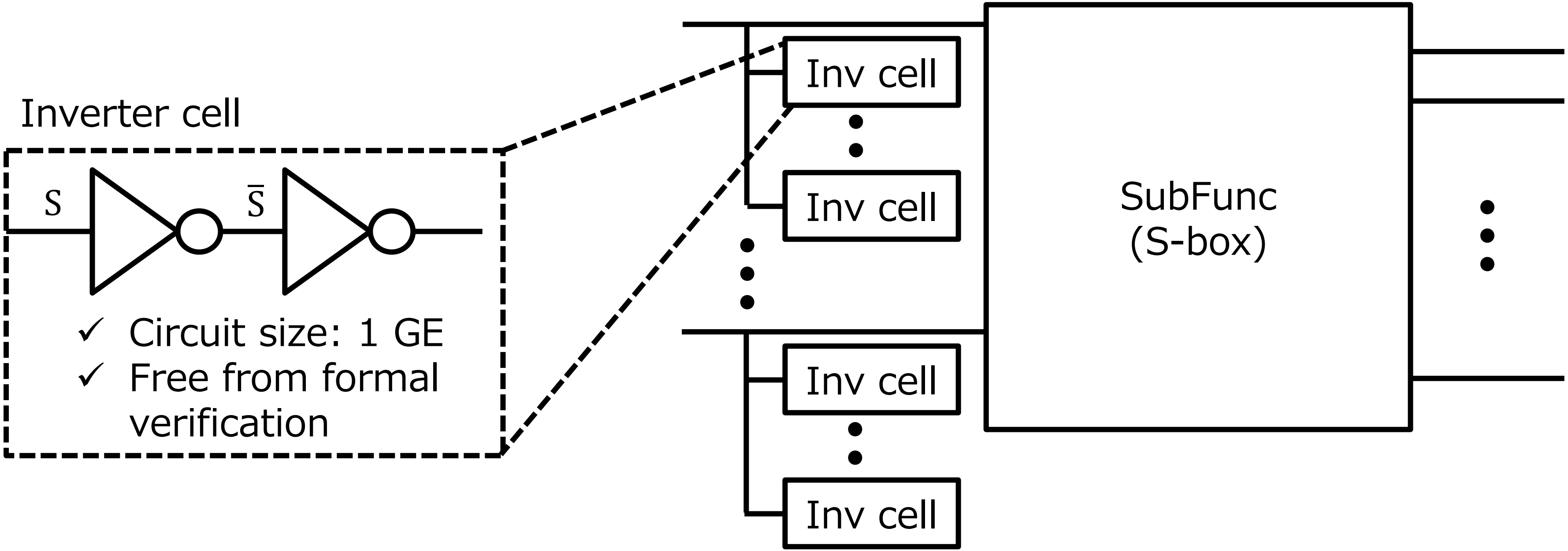
A 2	B 0	C 1
D 0	E 1	F 6
G 10	H 15	I 16

B_Y Sim.



- Number of determined bytes after EM CPA for 10k random input payloads

IC chip falsification with EM amplifier

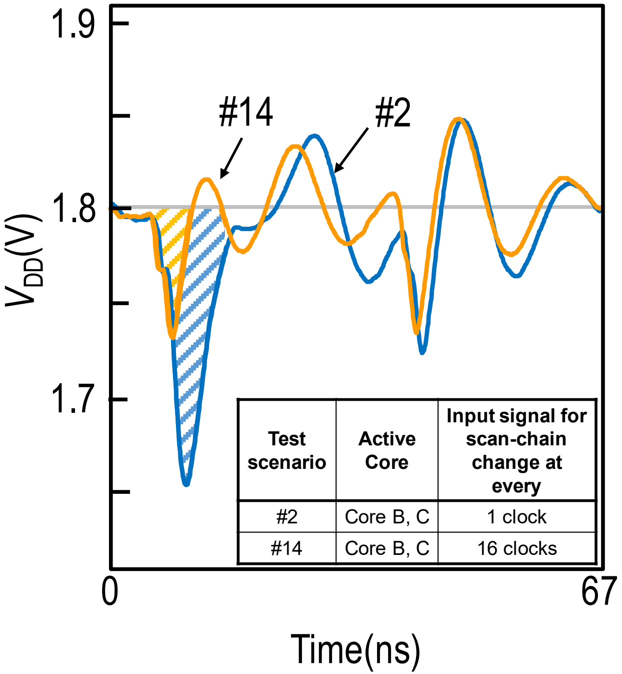


- ✓ Circuit size: 1 GE
- ✓ Free from formal verification

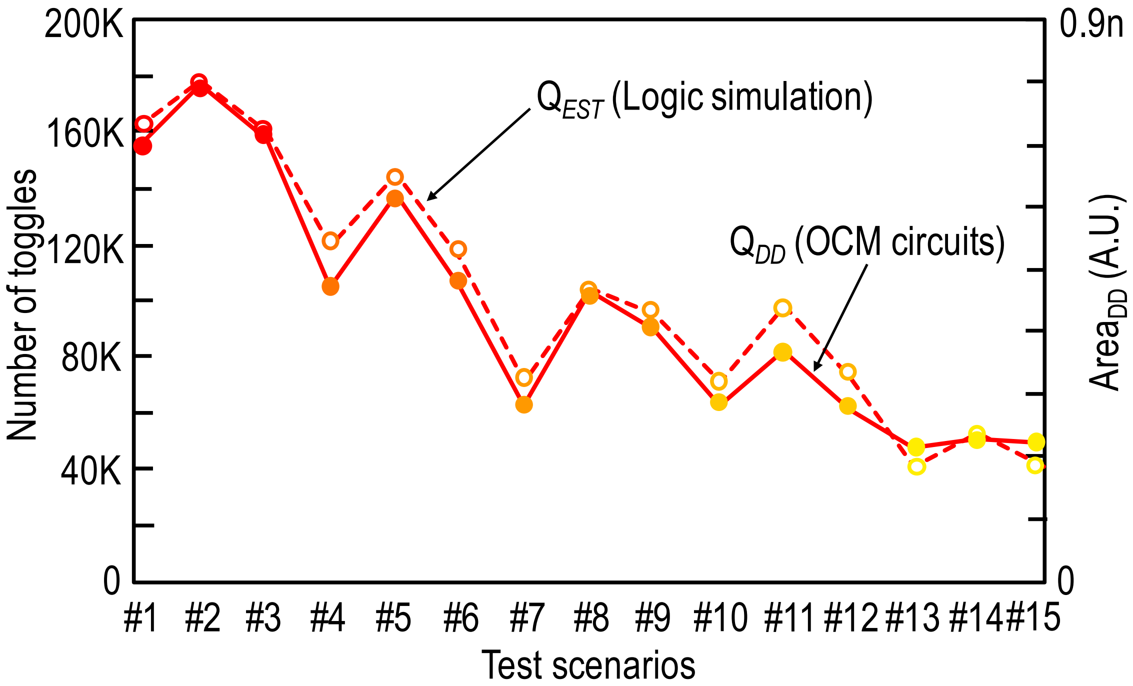
- ▶ This circuit amplifies switching power, while does not change any logic.
- ▶ Neither digital FV* nor analog LVS** could find the insertion of inv. cells.

*Formal verification, **Layout versus schematic

Charge amount as indicator



Test scenario	Active Core	Input signal for scan-chain change at every
#2	Core B, C	1 clock
#14	Core B, C	16 clocks

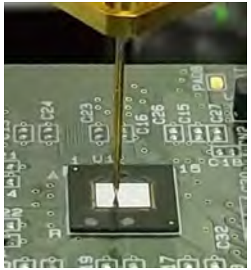


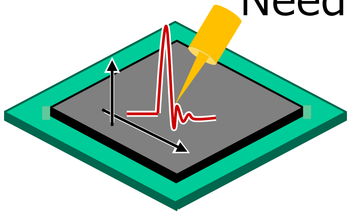
- Power (V_{DD}) waveform to estimate power current consumption, and then to be integrated over time to derive "***charge amount*** (Q_{EST})" for assessments.

Outline

1. Introduction
2. Passive side channels from IC chip backside
3. Active fault injection on IC chip backside
4. Packaging for security
5. Summary

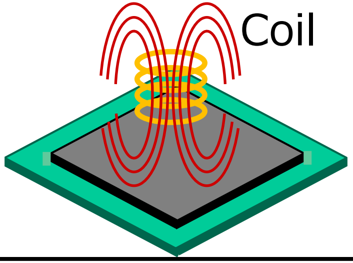
Active fault injection on Si backside





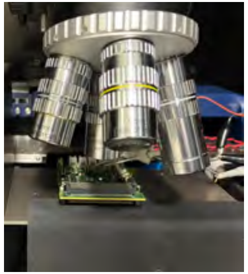
Needle

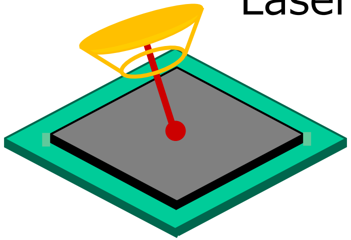
- ✓ DC biasing
- ✓ HV pulsing (High voltage)



Coil

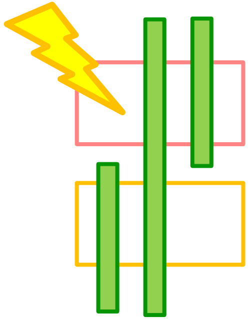
- ✓ Magnetic flux induction
- ✓ EM wave irradiation





Laser

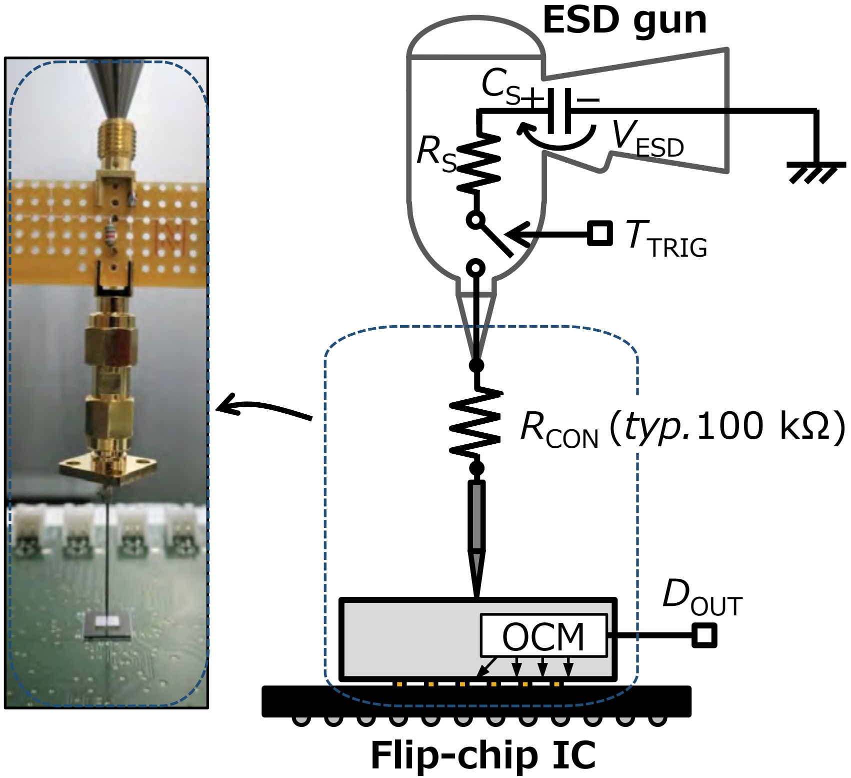
- ✓ IR laser pulsing
- ✓ HP laser drilling (High power)



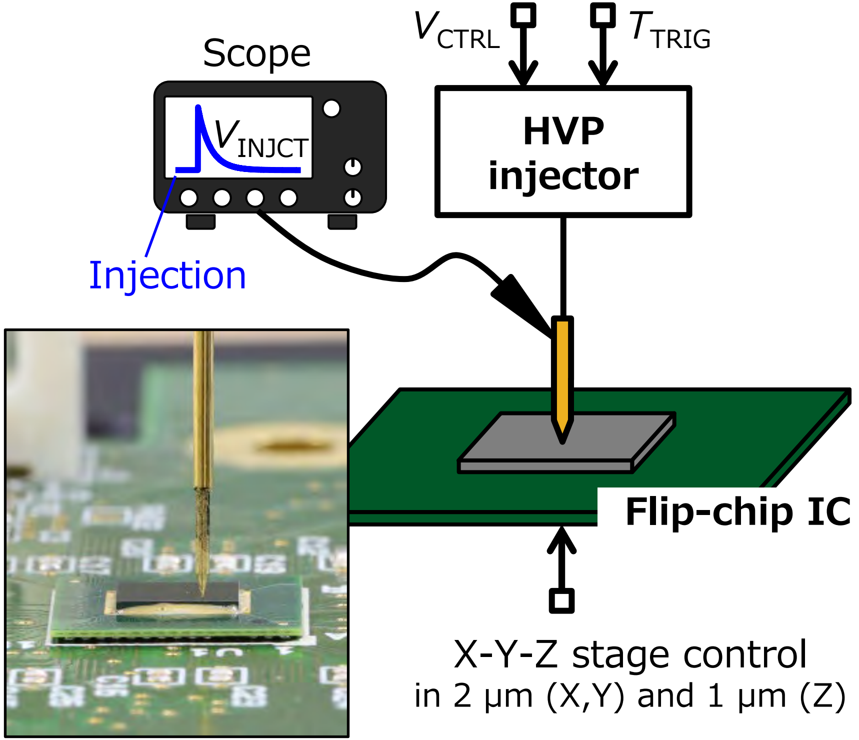
Primary physics is different.

IEEE Open Journal of the Solid-State Circuits Society (OJ-SSCS), Nov. 2024.
DOI: 10.1109/OJSSCS.2024.3499967

Chip backside pulsing

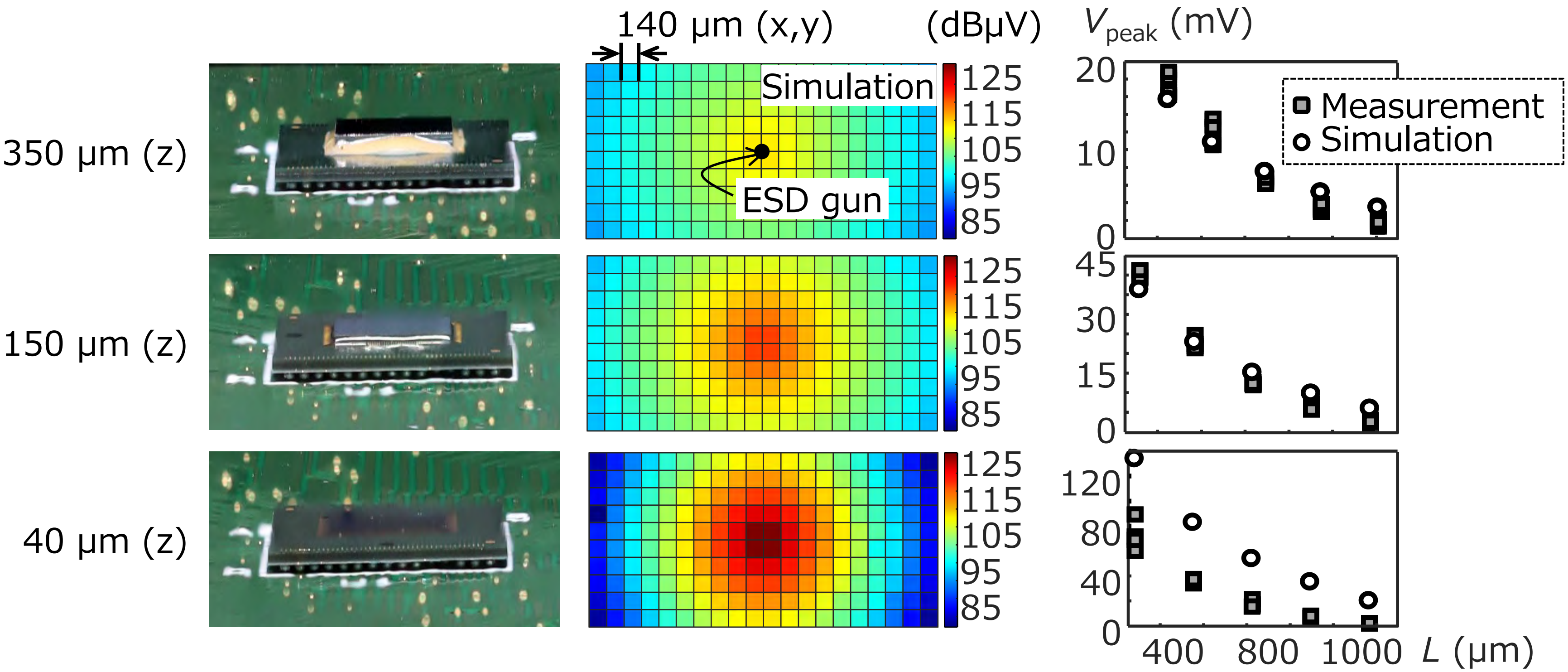


Ref. to ESD tradition (ISO10605, IEC61000-4-2)



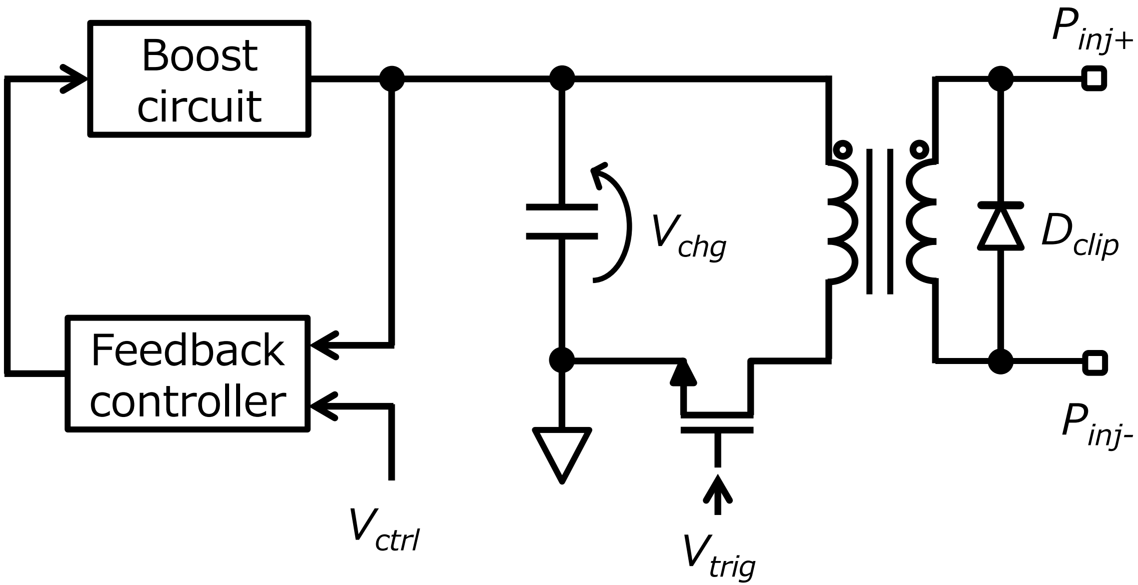
HVP injector (custom made)

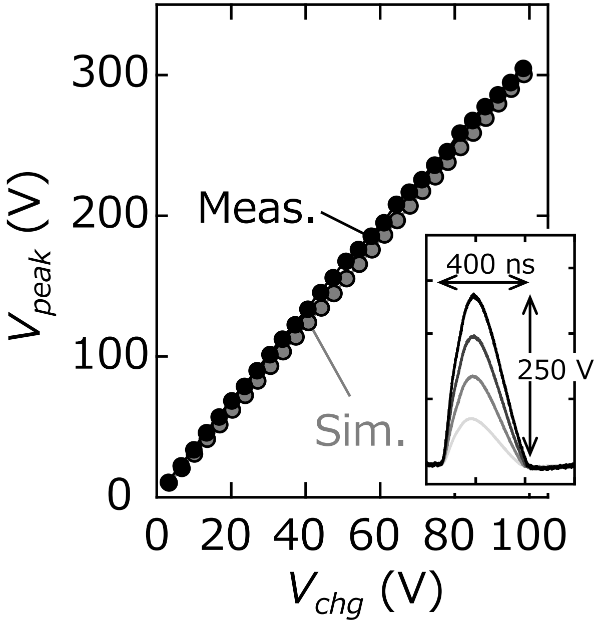
Voltage spreads on IC chip frontside



- ESD gun applied on Si backside, Si voltage measured on-chip on its frontside.
- Si substrate impedance model was simulated and calibrated.

High voltage pulsing (HVP) injector

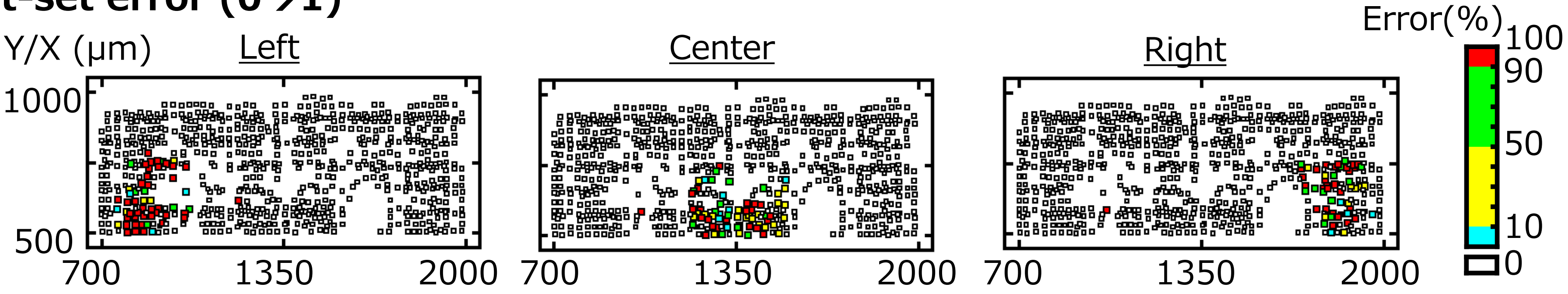




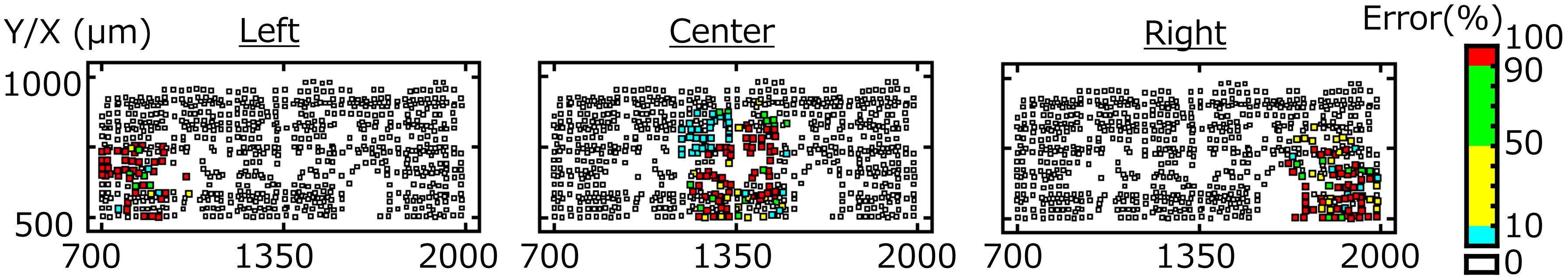
- ▶ Controllability, reproducibility and predictability of voltage pulsing in the range up to 300 V were confirmed.
- ▶ Polarity of pulsing is reversable by the connection to a needle.

Si experiments

Bit-set error (0→1)



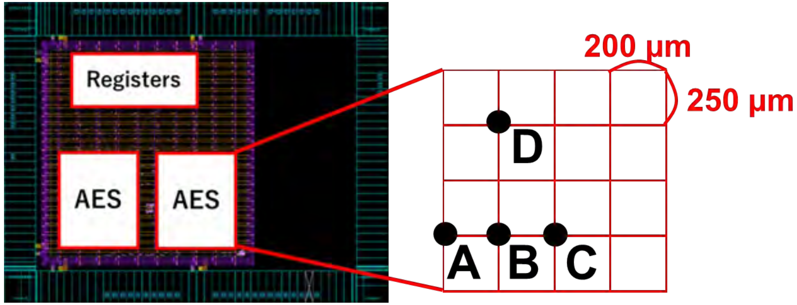
Bit-reset error (1→0)



- Error bits induced by HVP among F/Fs – strongly location dependent.

Si experiments – security threats

IEEE Fault Diagnosis and Tolerance in
Cryptography (FDTC), Sep. 2024.



Si-backside HVP for DFA*

- Positive pulse : 320V
- Negative pulse : -120V

*Differential fault analysis

A

C_0	C_4	🟦 C_8	C_{12}
C_1	🟦 C_5	C_9	C_{13}
🟦 C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	🟦 C_{15}

B

C_0	🟦 C_4	C_8	C_{12}
🟦 C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	🟦 C_{14}
C_3	C_7	🟦 C_{11}	C_{15}

C

C_0	C_4	C_8	🟦 C_{12}
C_1	C_5	🟦 C_9	C_{13}
C_2	🟦 C_6	C_{10}	C_{14}
🟦 C_3	C_7	C_{11}	C_{15}

D

🟦 C_0	C_4	C_8	C_{12}
C_1	C_5	C_9	🟦 C_{13}
C_2	C_6	🟦 C_{10}	C_{14}
C_3	🟦 C_7	C_{11}	C_{15}

Faulty ciphertext with **single-bit error in every byte**

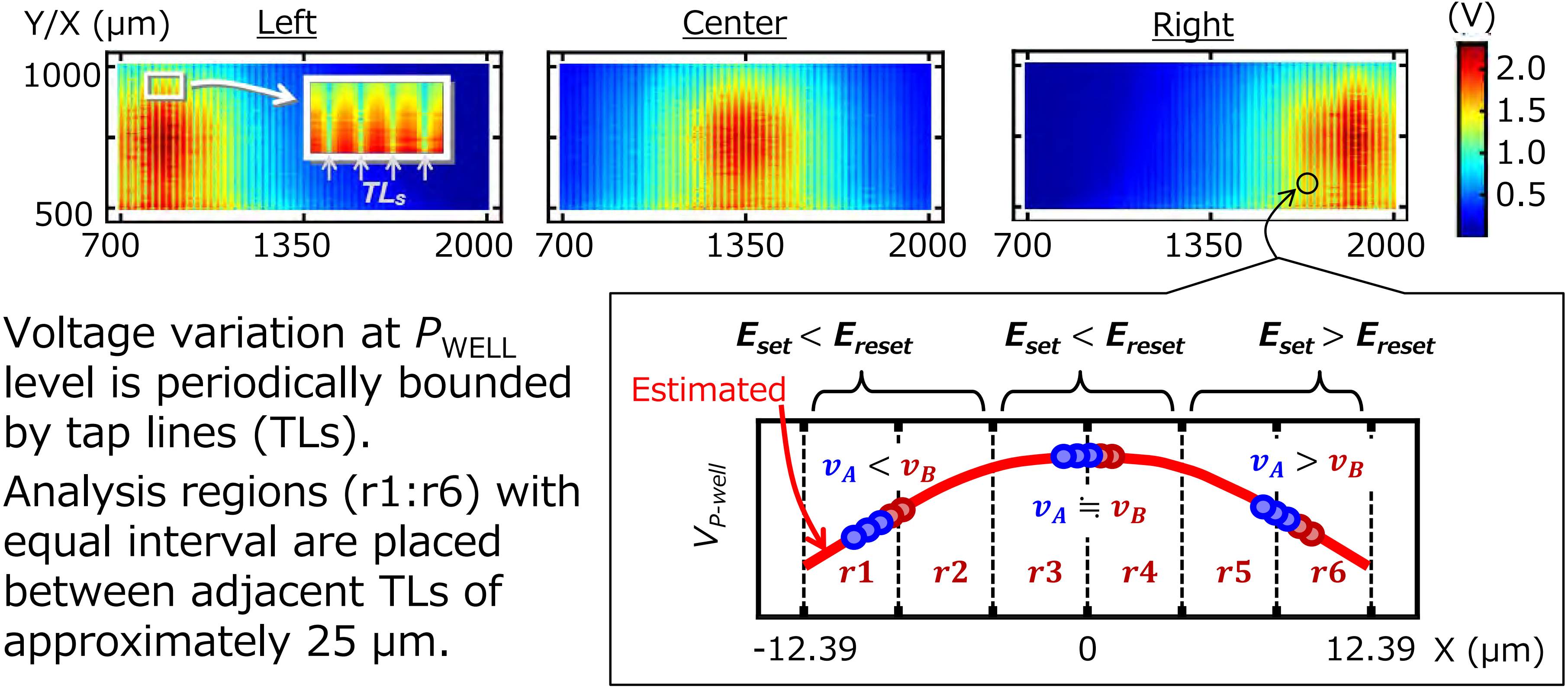
🟦 Faulty byte

- A single bit could be intentionally flipped – alignments of placements and timing of HVP injection w.r.t. the operation of AES crypto engine.

Simulated voltage distribution

IEEE Transactions on Electromagnetic Compatibility (TEMC), Oct. 2024.
DOI: 10.1109/TEMC.2024.3440919

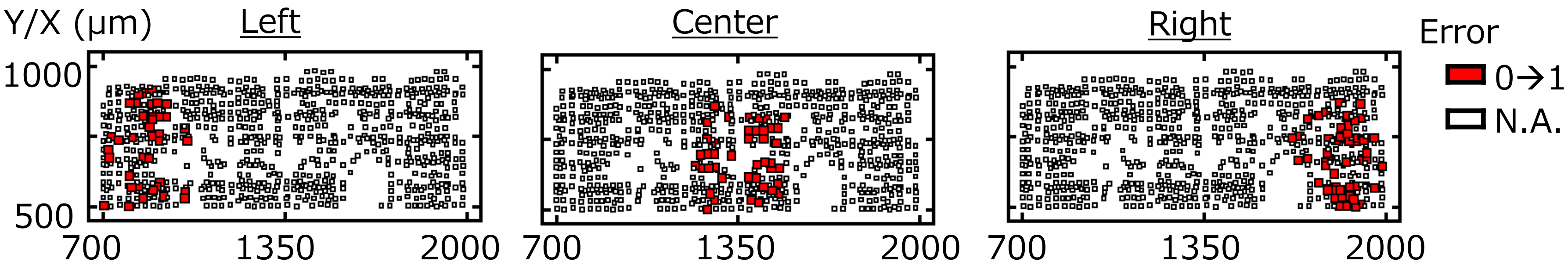
P_{WELL} voltage intensity map



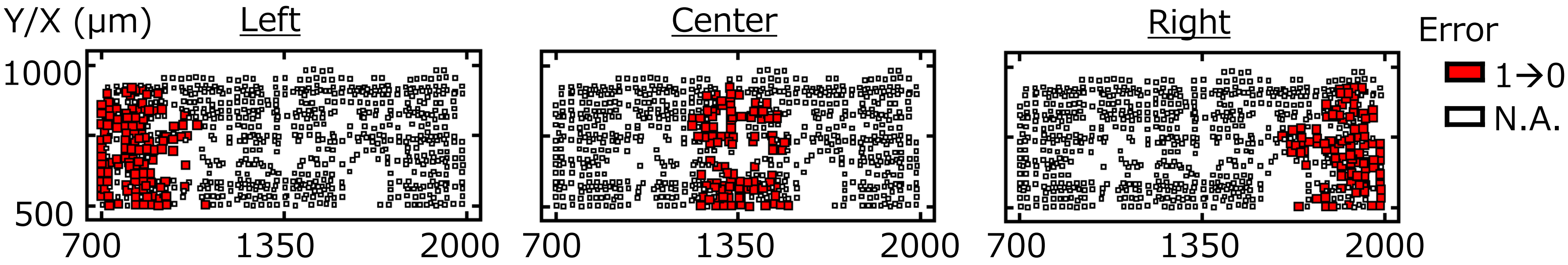
- Voltage variation at P_{WELL} level is periodically bounded by tap lines (TLs).
- Analysis regions (r1:r6) with equal interval are placed between adjacent TLs of approximately 25 μm.

Simulation results

Bit-set error (0→1)

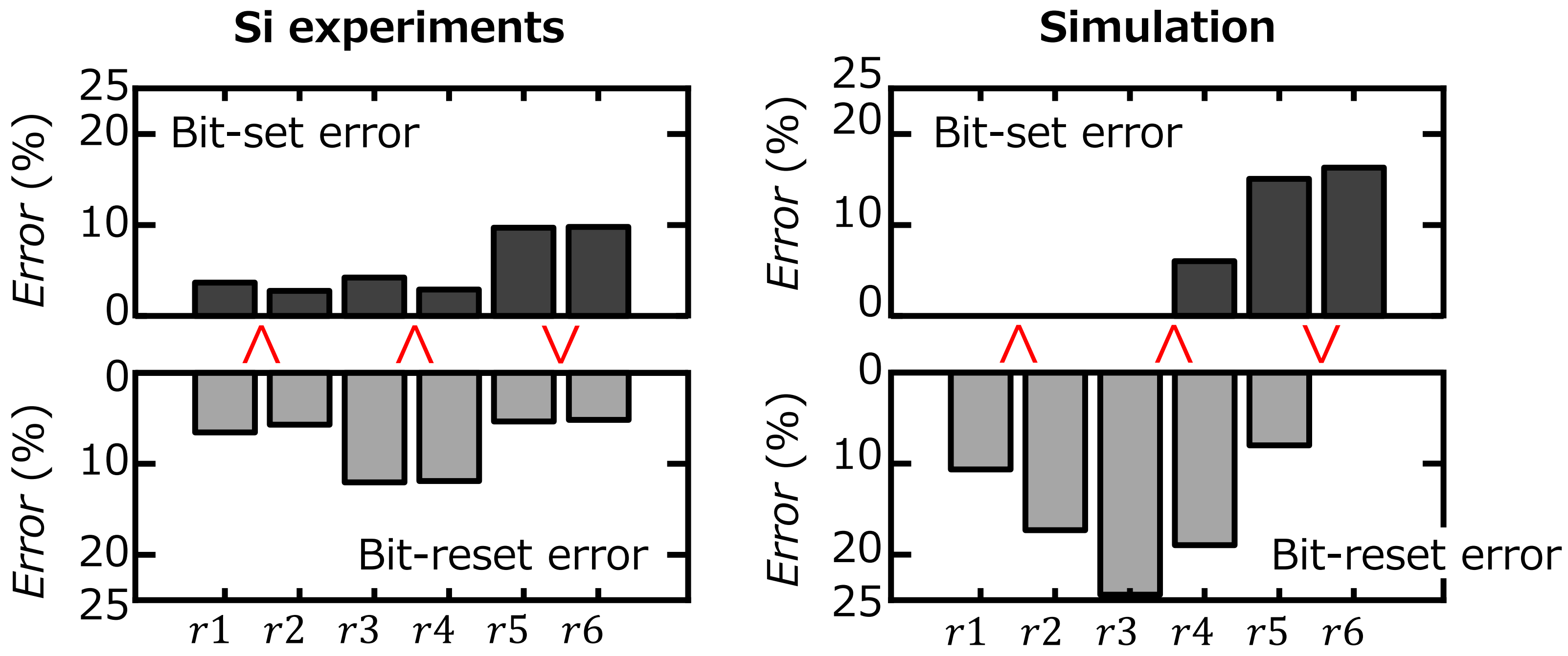


Bit-reset error (1→0)



- Location dependency and asymmetry among bit-set/bit-reset errors

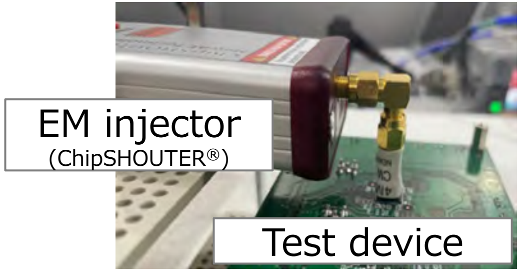
Si experiments vs. simulation

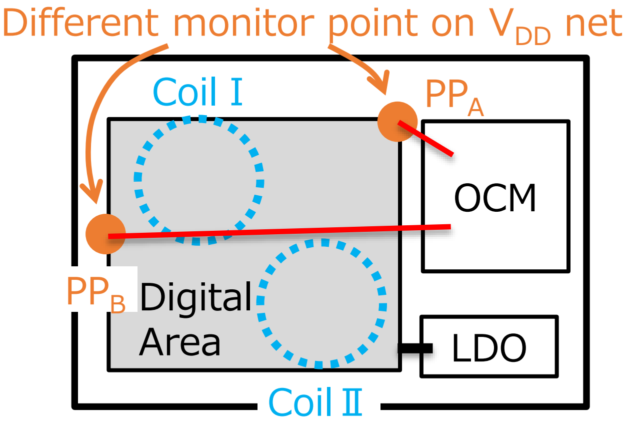


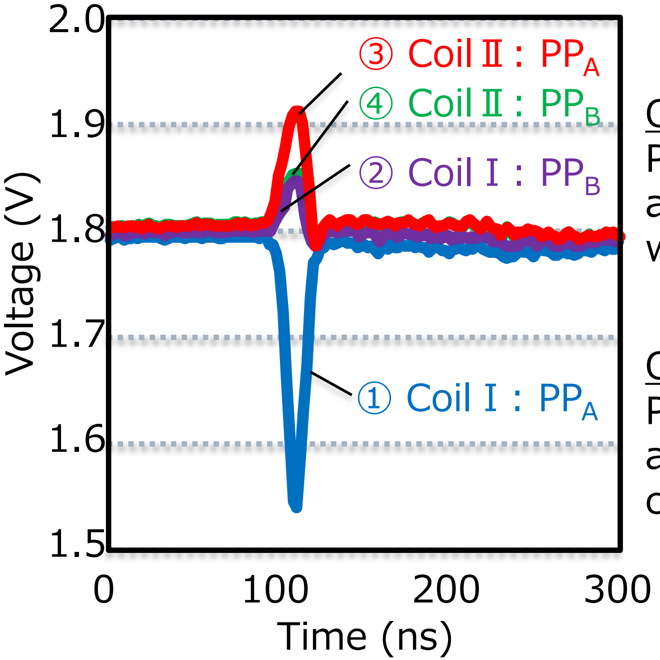
- Simulation explains **the presence of asymmetry** among the bit-set/bit-reset errors and the regions about error occurrences.

EM induced voltage on Si backside

International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), Apr. 2024.







Observation #1 (from ① vs. ②)

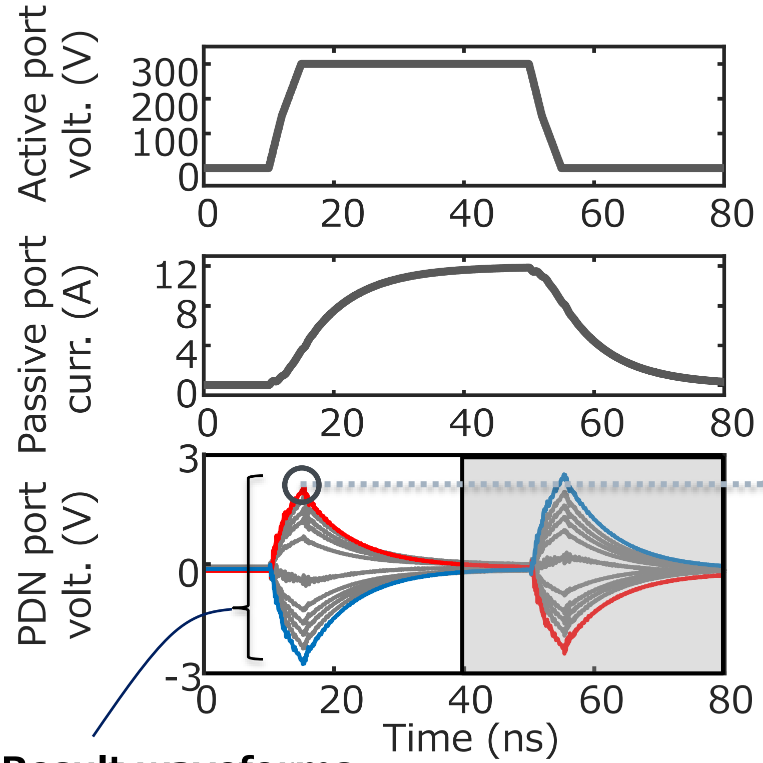
Positive and negative swings are observed in **PP_A and PP_B** when **Coil I** is used.

Observation #2 (from ① vs. ③)

Positive and negative swings are observed in **PP_A** when comparing **Coil I and Coil II**.

- EM fields create voltage glitches that spread across wide chip area.

Simulation of magnetic field coupling

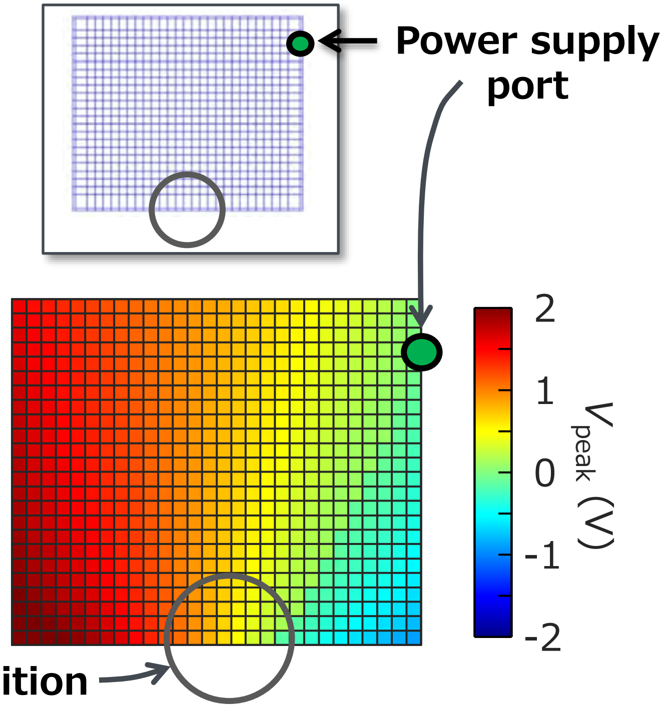


Result waveforms

28×24 = 672

① Extract the V_{peak} of each waveform (At first peak, 0 ~ 40ns)

② Generate a color map based on the V_{peak} at each PDN location

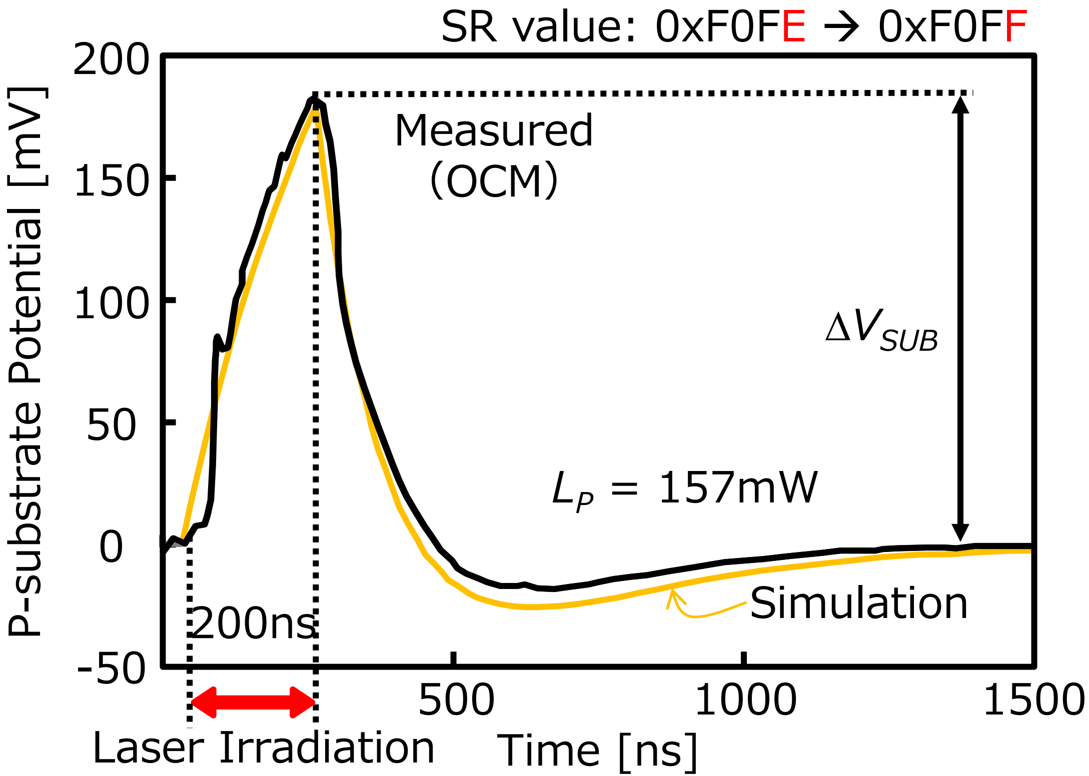


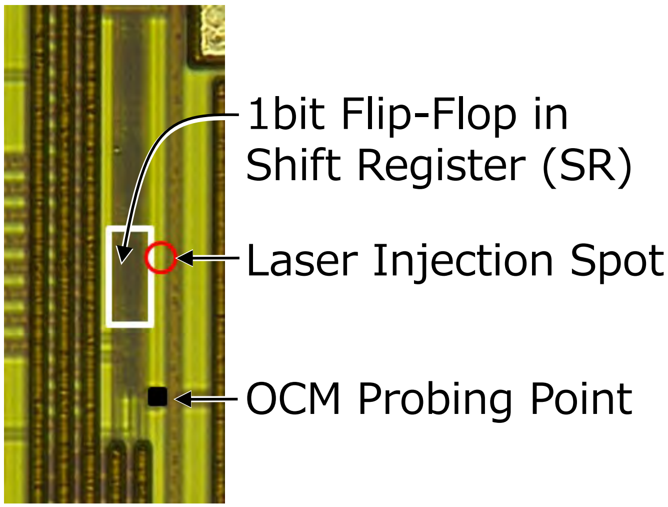
Power supply port

Coil position

- Simulation explains **the presence of pos. and neg. drops with physical position dependency**.

Laser induced V_{SUB} waveforms





- Simulation with equivalent circuits estimates photo-voltage conversion.

Lack of models

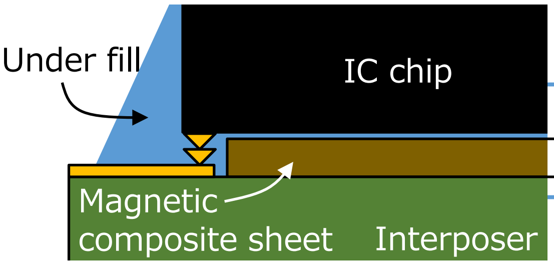
- Vertically integrated models of failures - material, device, circuits and systems – need to be explored.

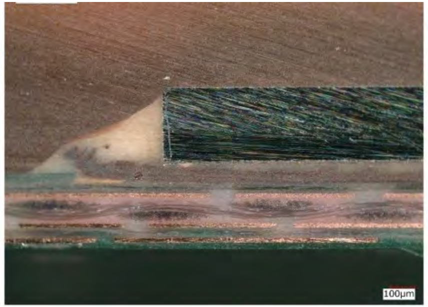
Outline

1. Introduction
2. Passive side channels from IC chip backside
3. Active fault injection on IC chip backside
4. Packaging for security
5. Summary

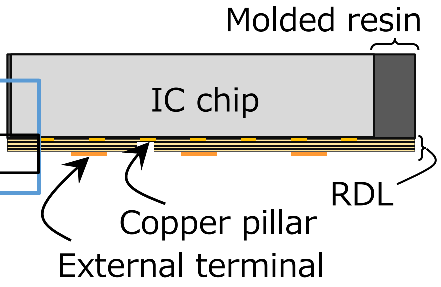
EM noise suppressors

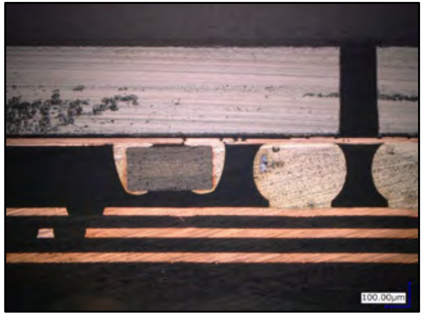
Flip-chip packaging with magnetic materials (EM power absorption)



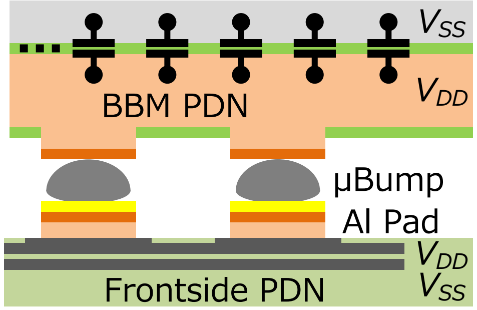


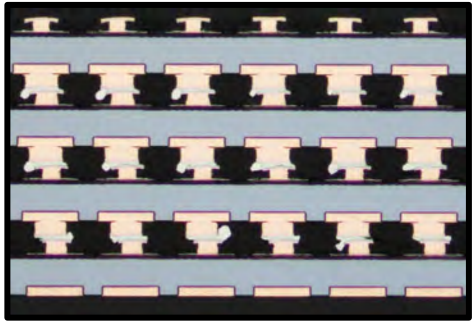
Fan-out laminates embedding land-side capacitors





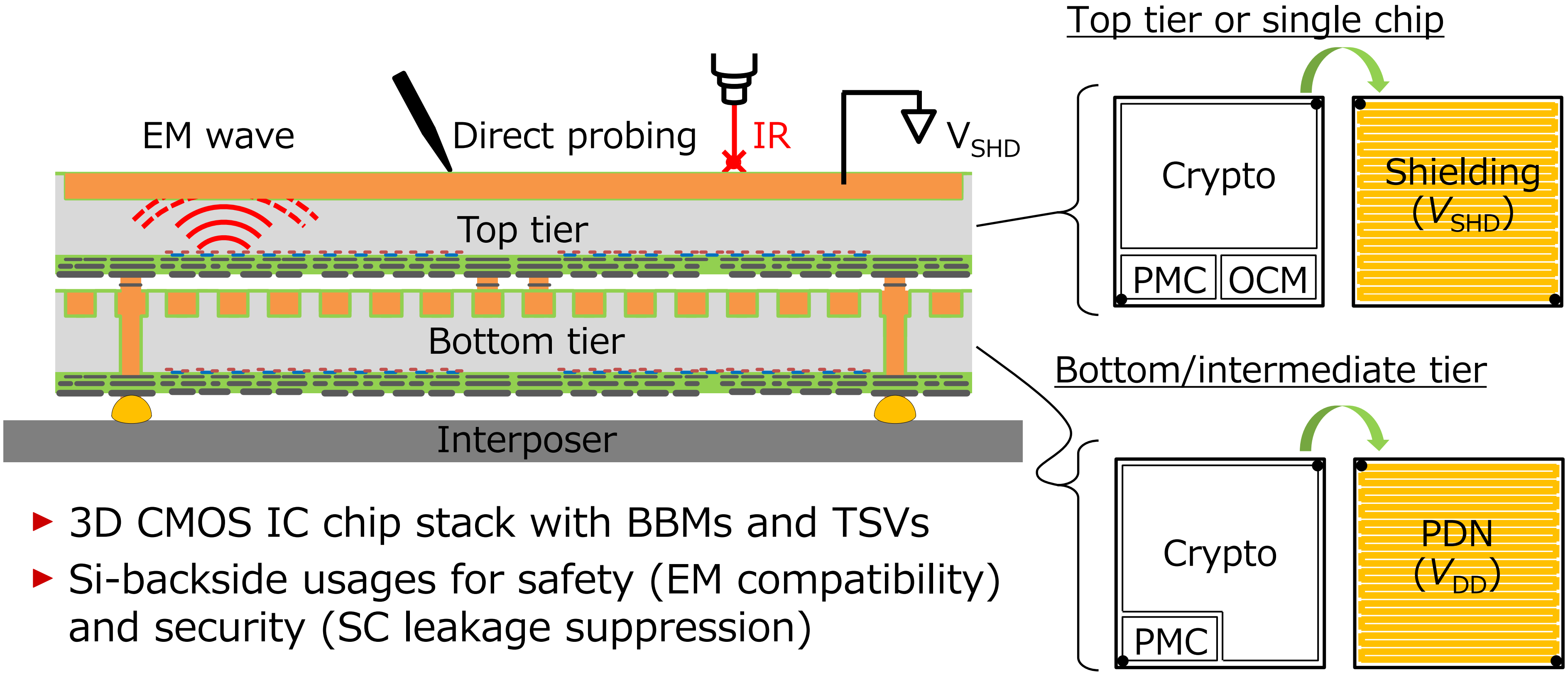
3D chip stacking with backside buried metal (BBM) capacitors





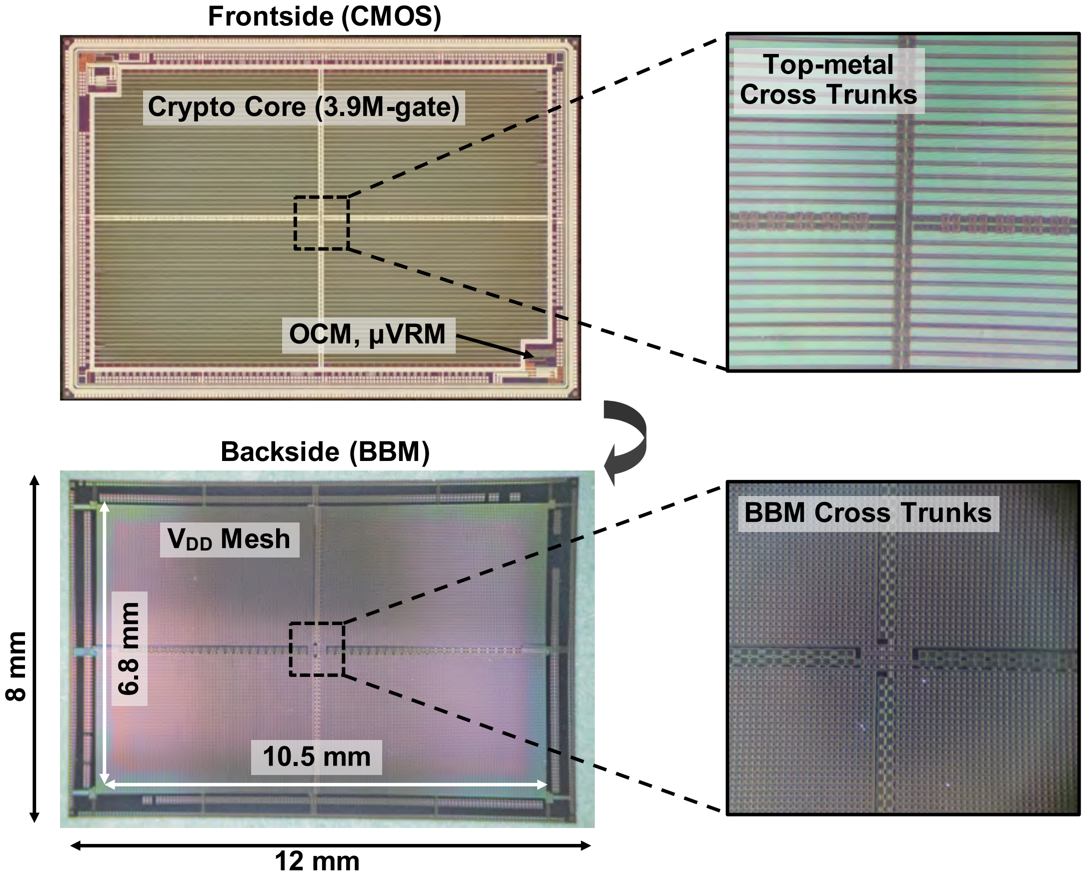
Secure 3D IC chip stack using BBM

IEEE Transactions on Very Large Scale Integration Systems (TVLSI), Jan. 2022. DOI: 10.1109/TVLSI.2021.3073946



- 3D CMOS IC chip stack with BBMs and TSVs
- Si-backside usages for safety (EM compatibility) and security (SC leakage suppression)

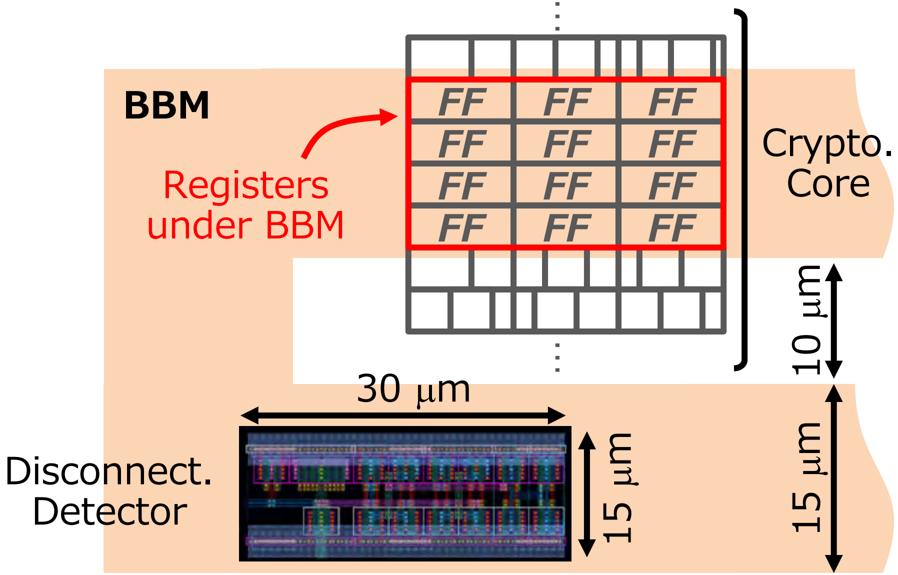
Tier photos on front and back sides



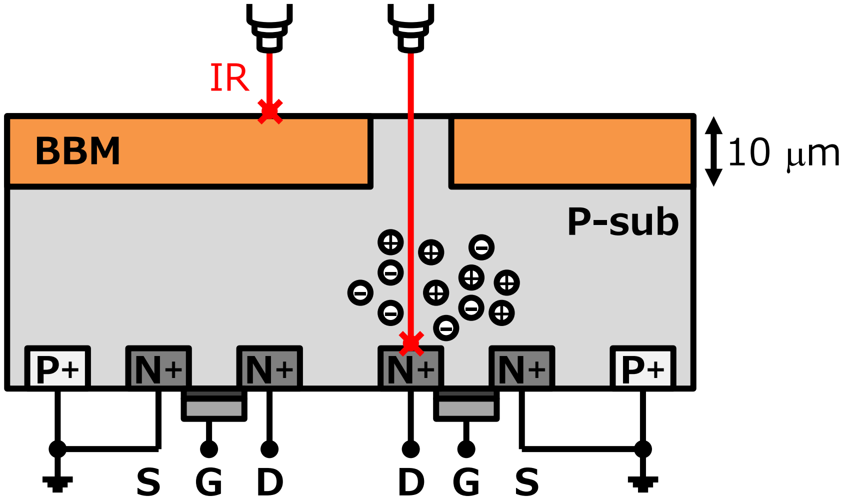
Thanks to AIST team:
Yuuki Araga
Naoya Watanabe
Haruo Shimamoto
Katsuya Kikuchi

IEEE Transactions on Electron Devices (TED), Apr. 2021.
DOI: 10.1109/TED.2021.3058226

Si-backside attack protection



Backside LFI is blocked or detected



- **Front side (IC) and back side (BBM) co-design** makes circuits of interest hidden from backside injection, as well as sensor circuits to detect injection.

Summary

- **Disciplines are common to EMC and HWS, and "good to know" in any system development.** The knowledge is complementary among security and safety problems in general IC chips and electronic systems.
- **Analog techniques for digital security:** simulation, modeling, device, circuit, packaging and manufacturing are all to be exploited for the higher levels of HWS (and EMC.)
- **Pre-silicon assessments and design justification:** relying on advanced simulation and modeling for security and safety metrics. Theory is further needed.

Acknowledgments: This work was in part based on the results obtained from a project, JPNP23013, commissioned by the New Energy and Industrial Technology Development Organization (NEDO). This work was also supported in part by JSPS KAKENHI under Grant JP22H04999. Many thanks to ANSYS – Kobe U joint research teams.