



# **Si Substrate Backside of ICs as Attack Surfaces and Countermeasures of Physical Security**

**Makoto Nagata**

Kobe University

Graduate School of Science, Technology and Innovation

May 21<sup>st</sup>, 2025

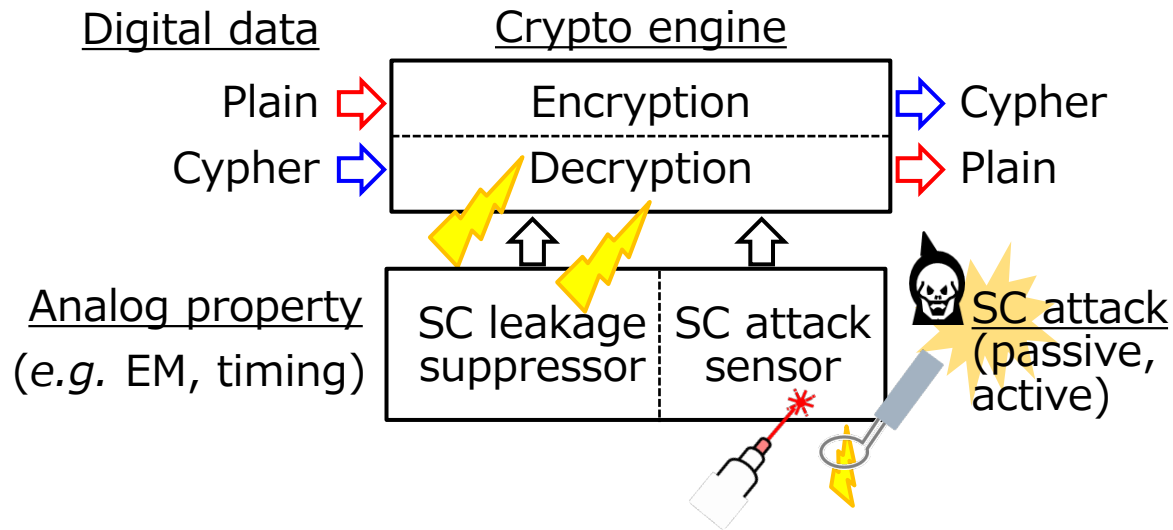


# Outline

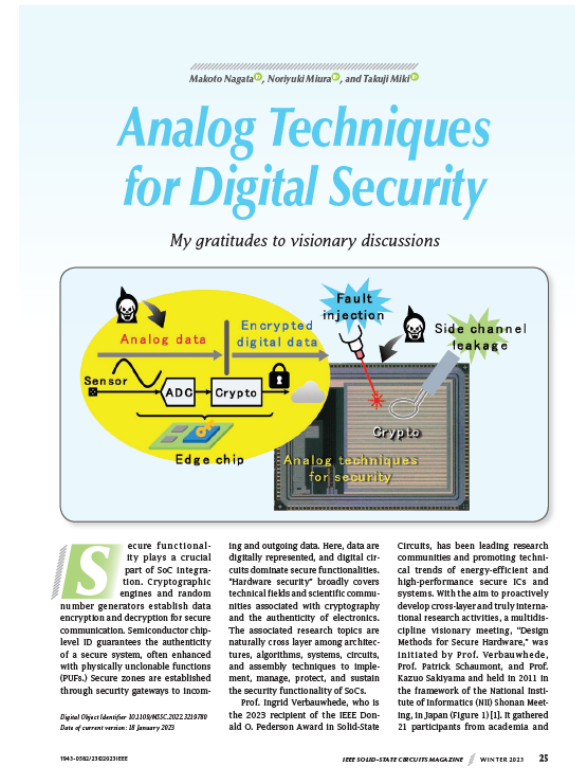
---

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

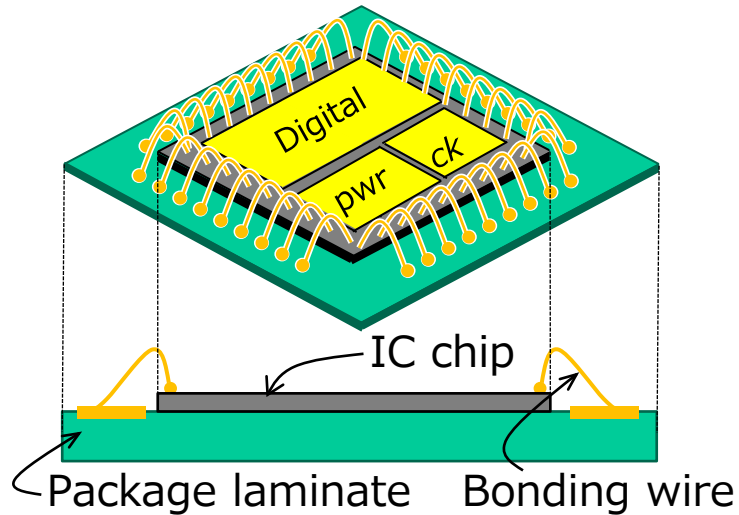


- ▶ Analog techniques at the levels of device, circuit, system, package and simulation protect digital security in IC chips.

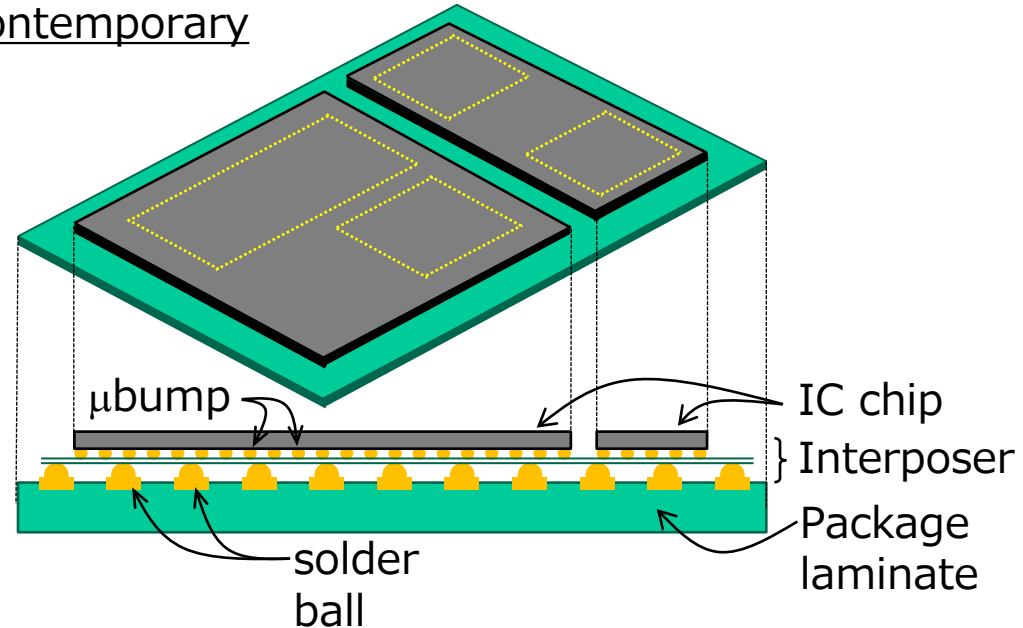


# Face-up and flip-chip assembly

Traditional

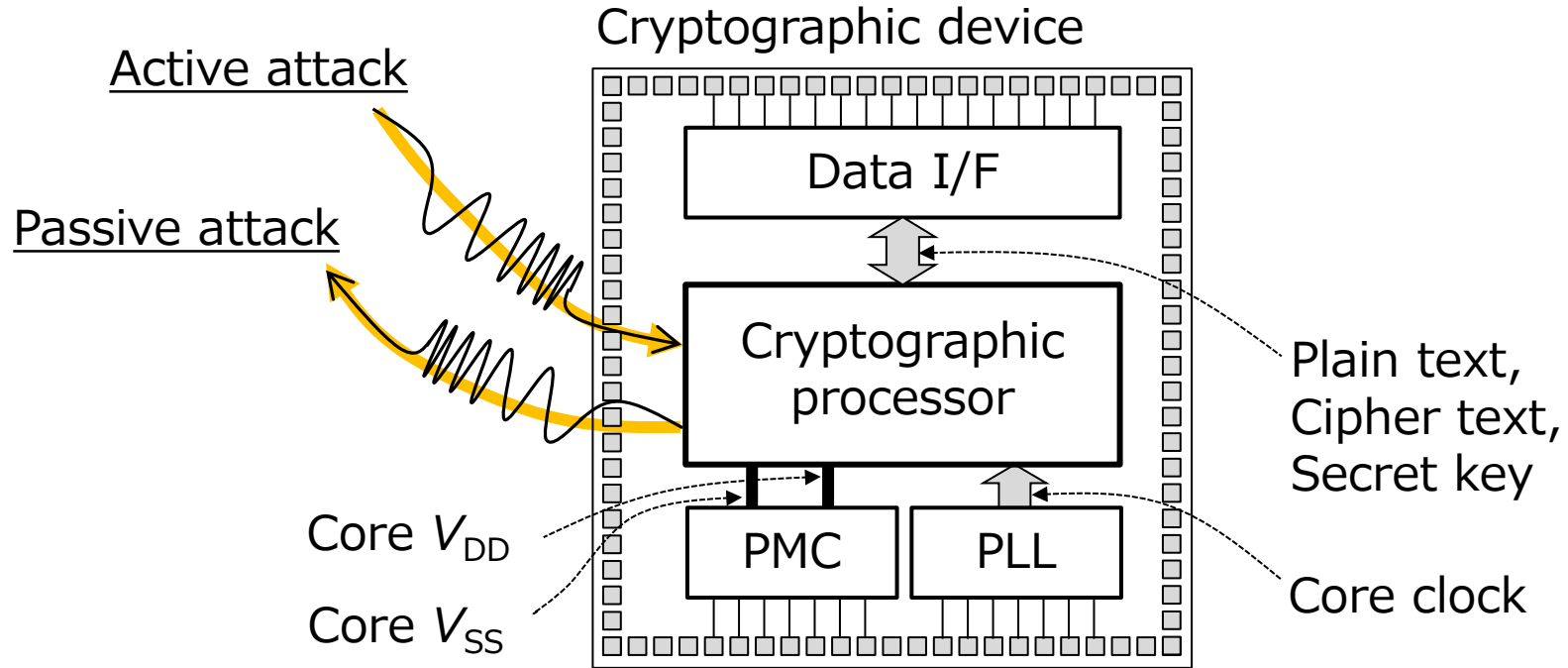


Contemporary



- ▶ 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



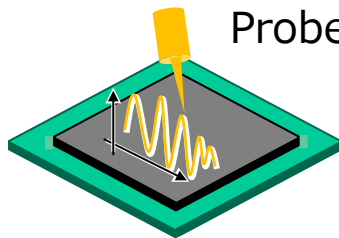
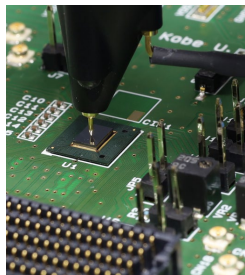
- Architectural explorations for securing horizontal data channels while circuit- and package-level countermeasures needed for vertical EM channels.

# Outline

---

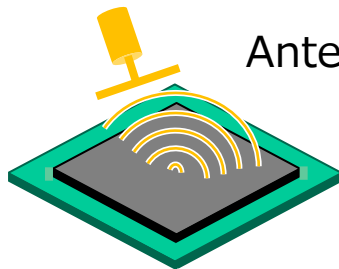
1. Introduction
2. Passive side channels from IC chip backside
3. Active fault injection on IC chip backside
4. Packaging for security
5. Summary

# Passive side channels on Si backside



Probe/needle

- ✓ Si substrate voltage
- ✓ Electric field



Antenna/coil

- ✓ EM waves
- ✓ Magnetic flux

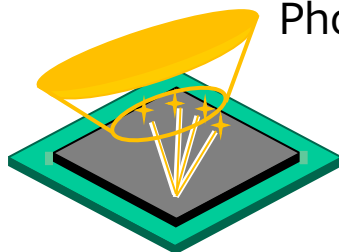
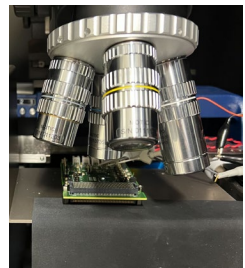
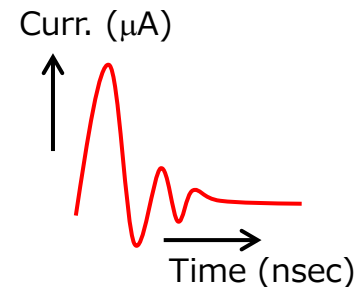


Photo sensor

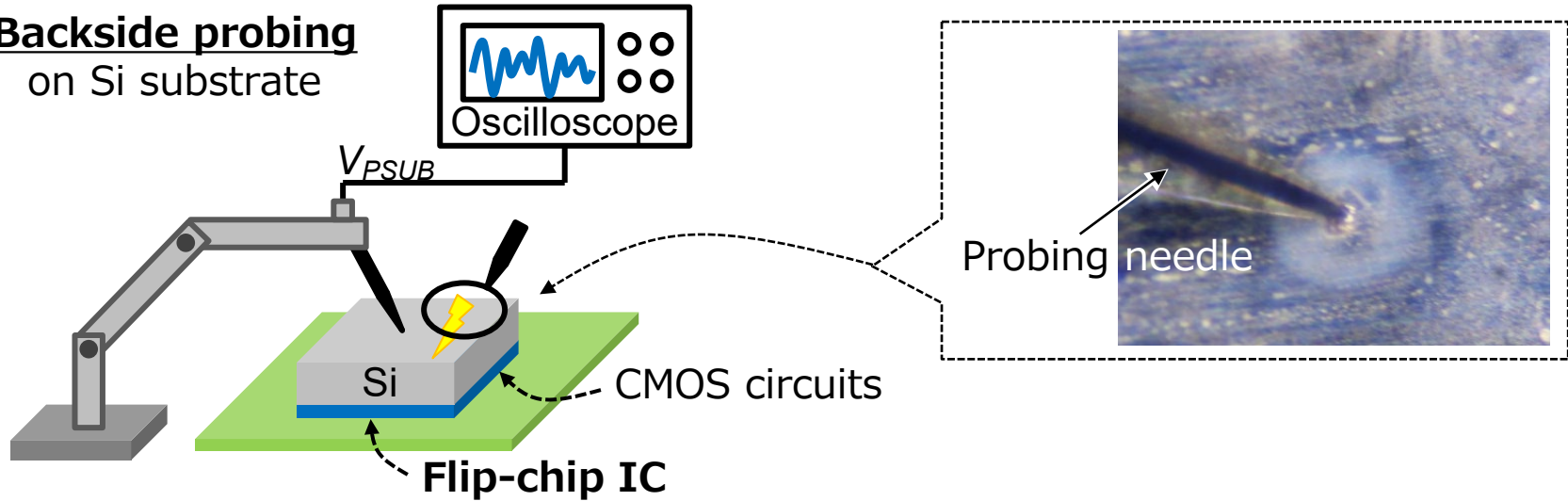
- ✓ IR photons
- ✓ IR microscopy



**Matter of  
power current**

# Si substrate voltage variation

**Backside probing**  
on Si substrate



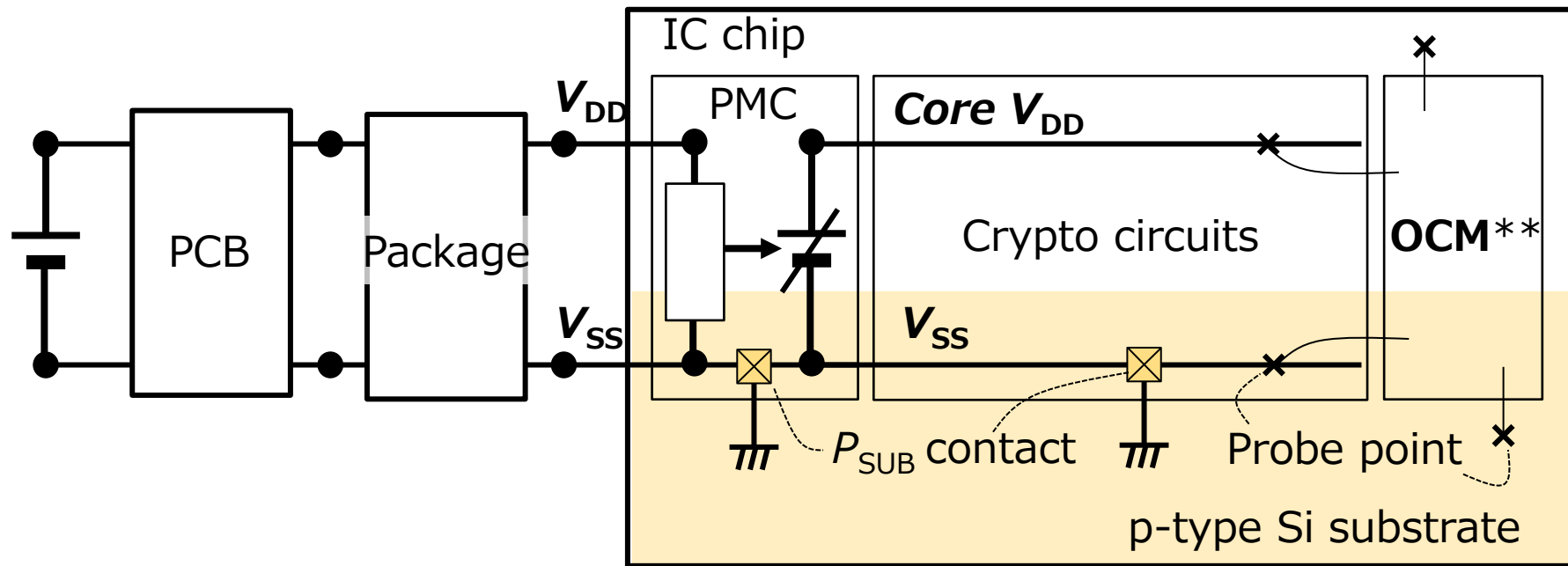
- ▶ **Direct voltage probing on Si substrate backside (=IC chip backside) with a metallic needle**



# Si substrate as a part of PDN\*

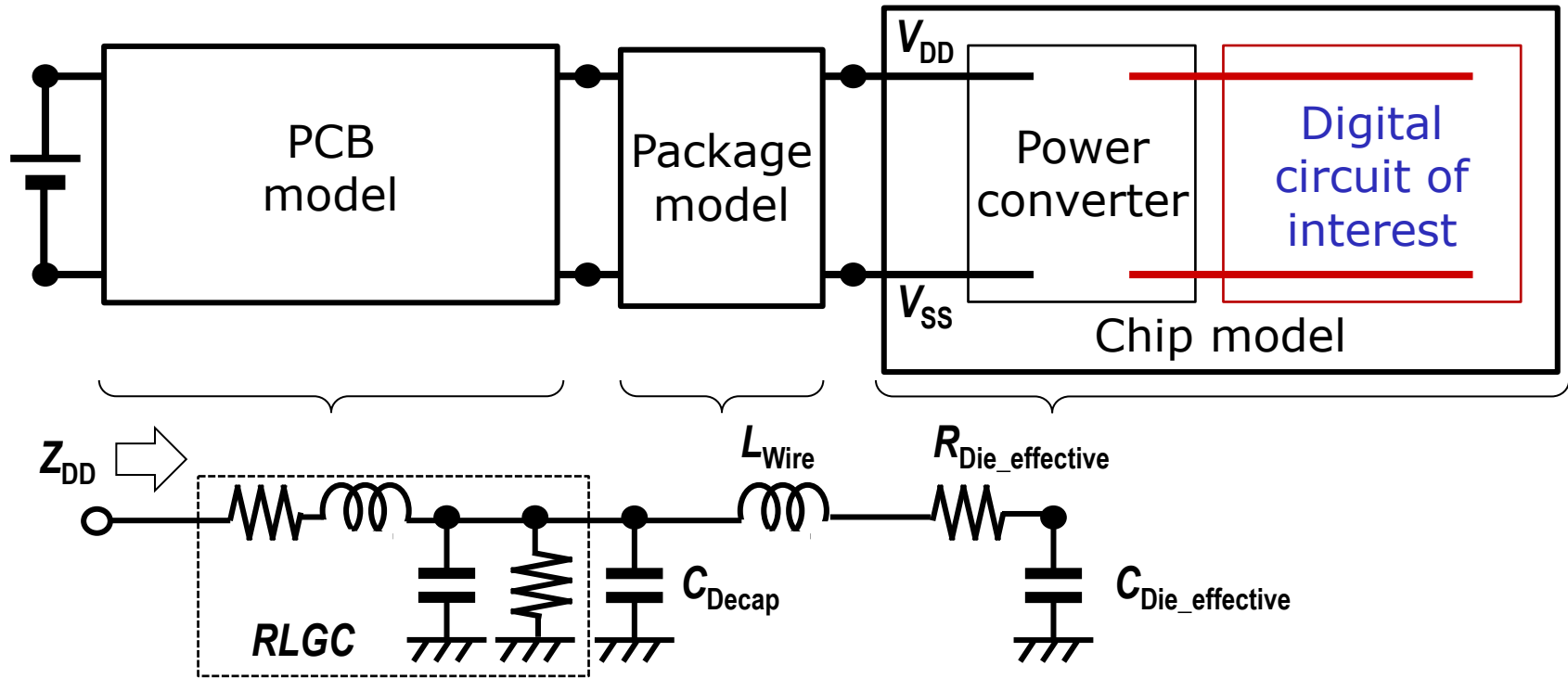
\*Power delivery network

\*\*On-chip monitor circuit



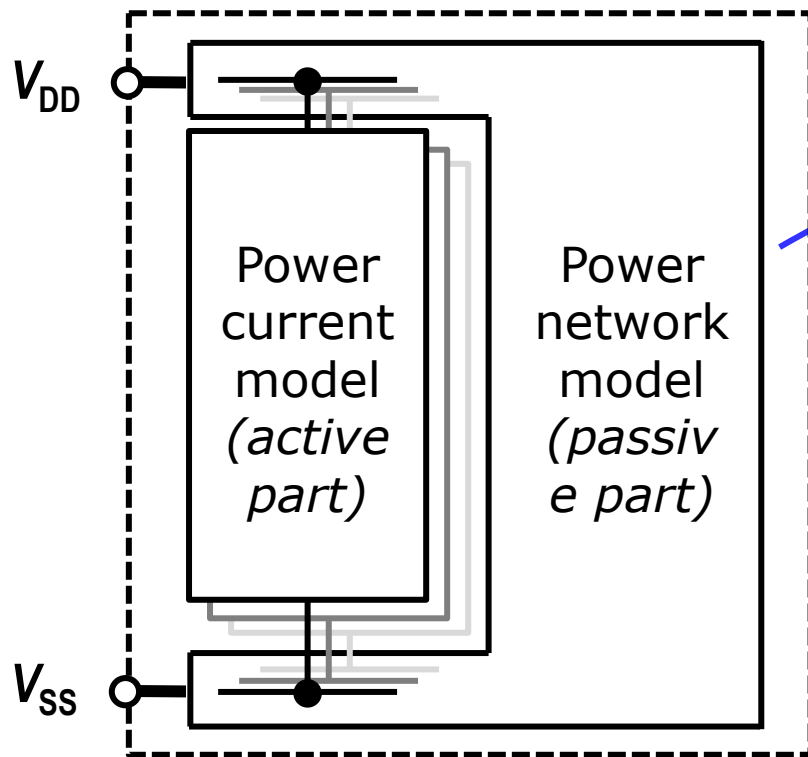
- **Si substrate** is a part of PDN (often of ground side) and the most prominent attack surface in flip-chip assembly (e.g. BGA).

# 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

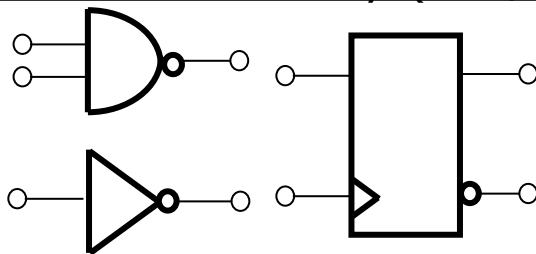


Chip power model  
(CPM)  
of either  
"digital circuit block"  
or  
"whole chip"

- ▶ A power delivery network involving multiple power current models

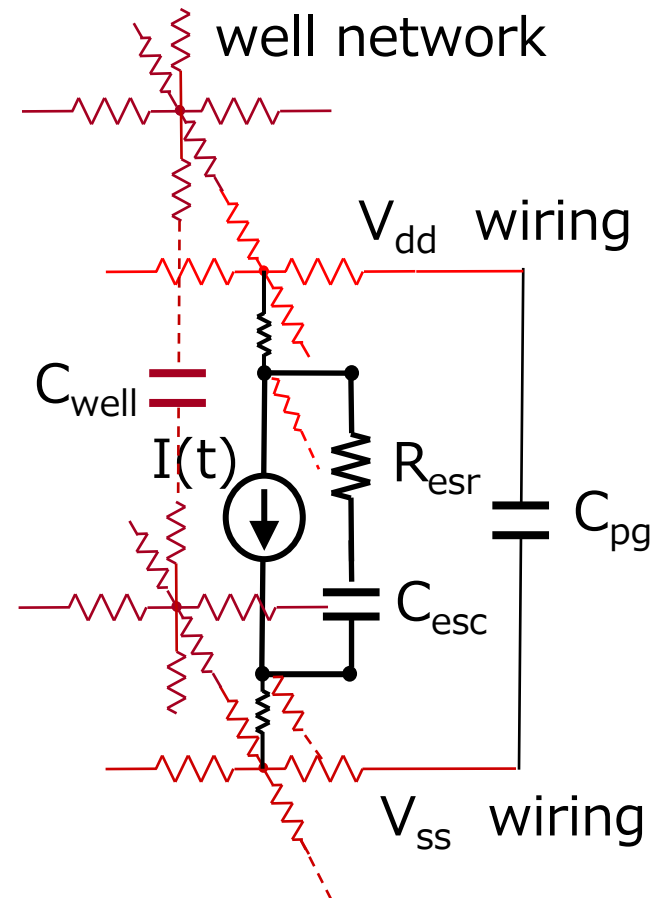
# Power current - active part of model

Standard cell library (LEF/DEF)

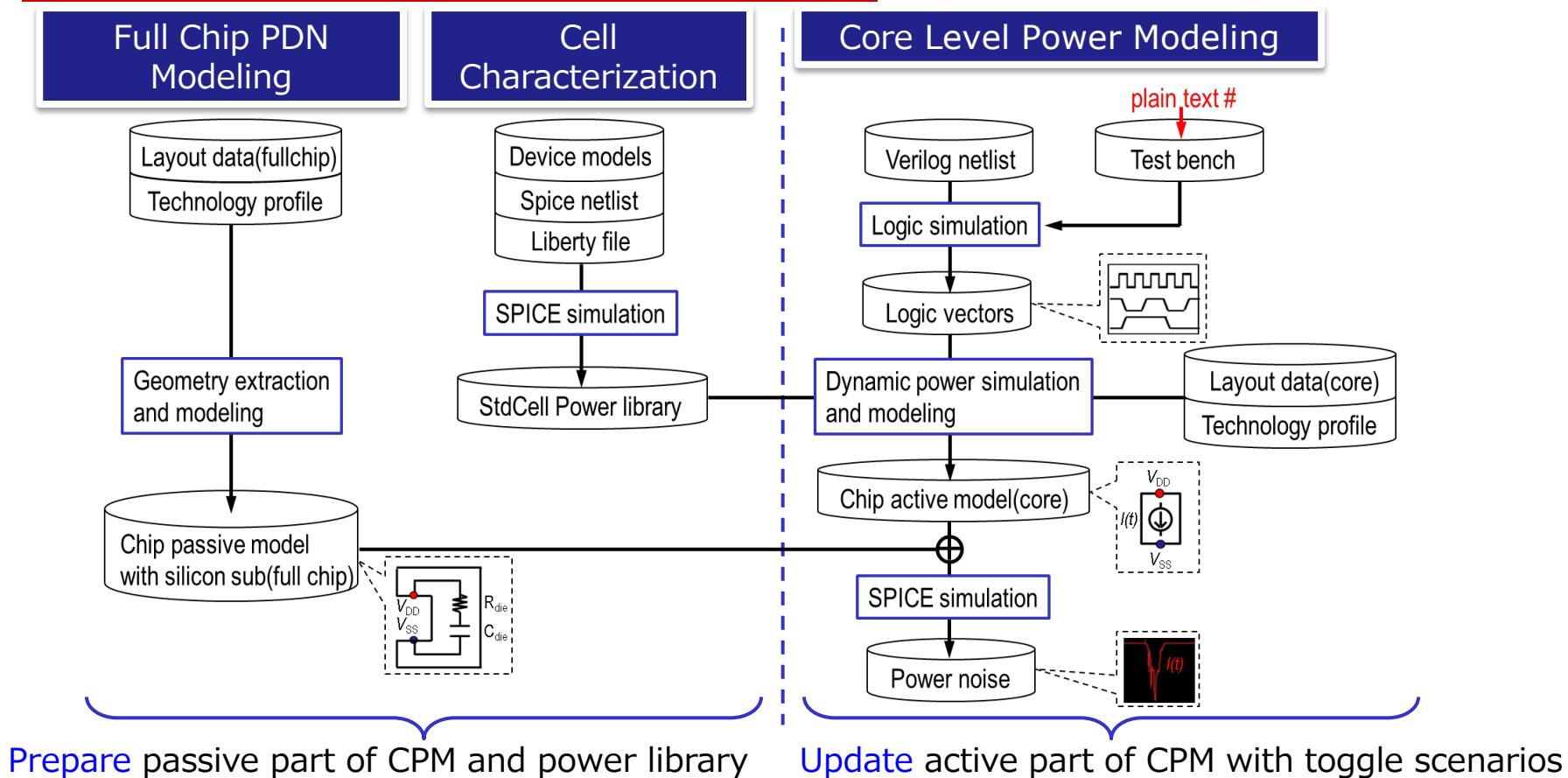


- SPICE simulation:  $I(t)$   
LUT for in/out condition, load caps
- Post-layout extraction  
logic cell level:  $C_{esc}$ ,  $R_{esr}$

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

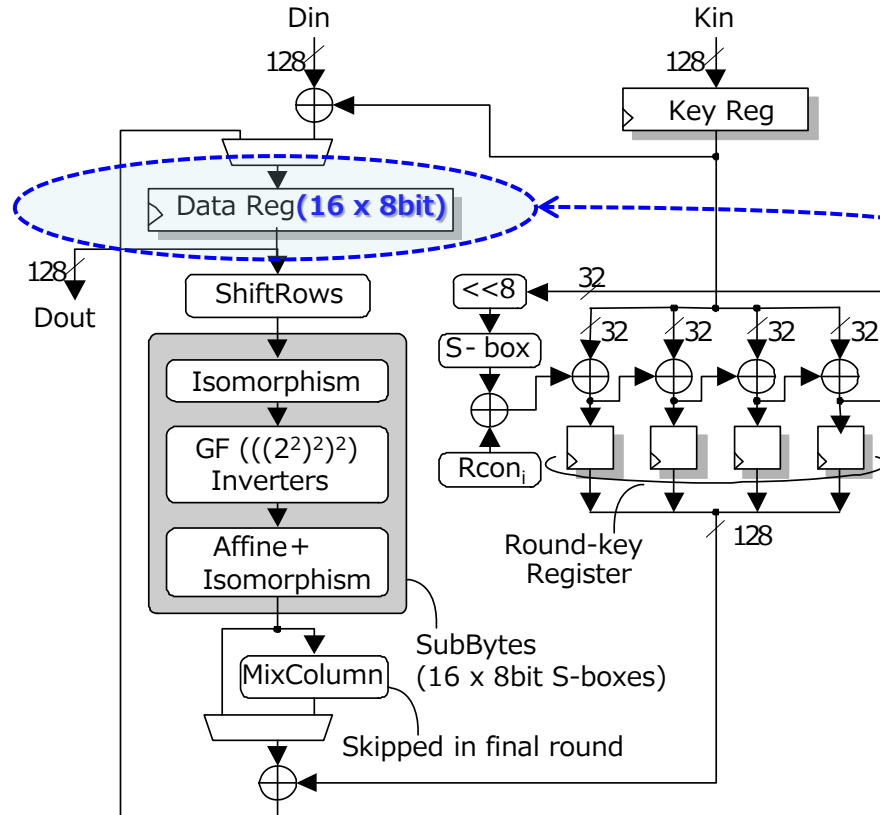


# CPS power noise simulation flow



# AES\* cryptographic architecture

\*Advanced Encryption Standard

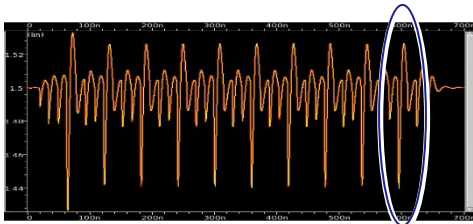


## Power side-channel (SC) leakage in AES datapath

- ▶ 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

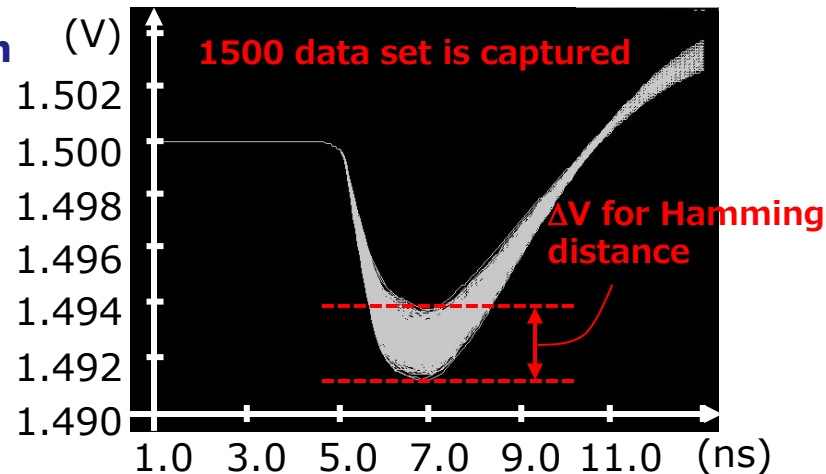
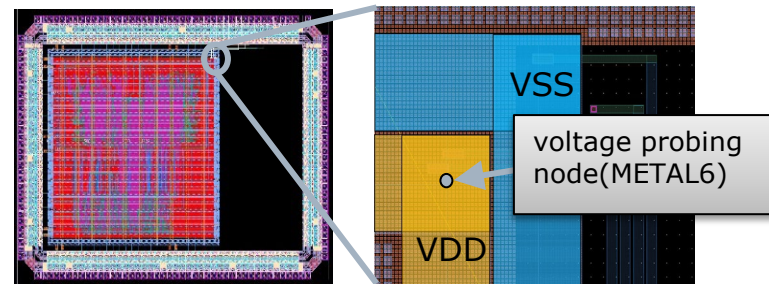
# AES power noise simulation

- ▶ Case study: private-key crypto IC chip
  - ✓ AES encryption engine (34 K gates)
  - ✓ Operation frequency: 34 MHz
- ▶ Power noise on VDD during crypto operation of last round (12 ns) in CPS simulation
  - ✓ # of plain texts: 1500 **Last round of encryption**



- ▶ 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

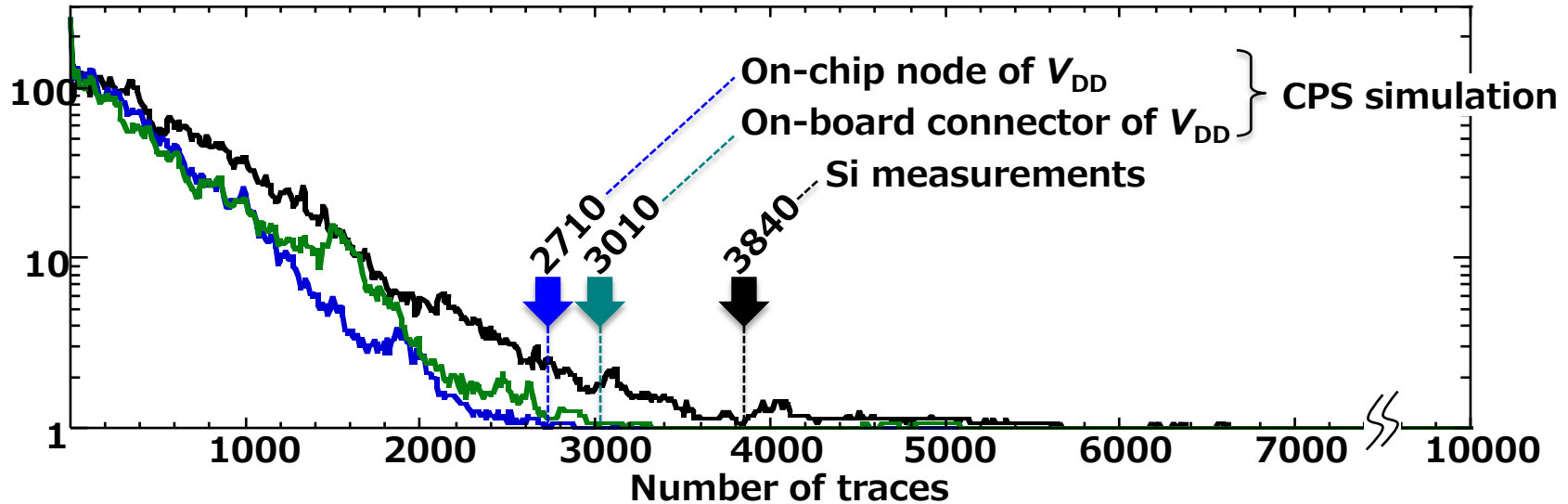


Intel Xeon CPU ES-2699 v4 (2.2GHz)

# CPA on AES core

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

Rank of guessed key bytes

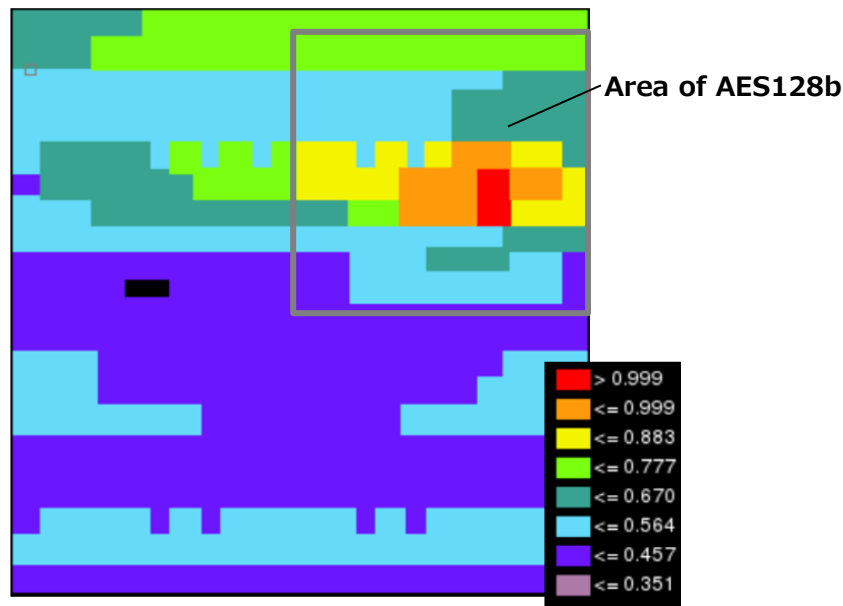


- ▶ On-chip measured and CPS simulated power traces for AES 128 bit w/ randomly generated 10k payloads
- ▶ Secret 16 key bytes are finally revealed, most pessimistic at on-chip nodes.

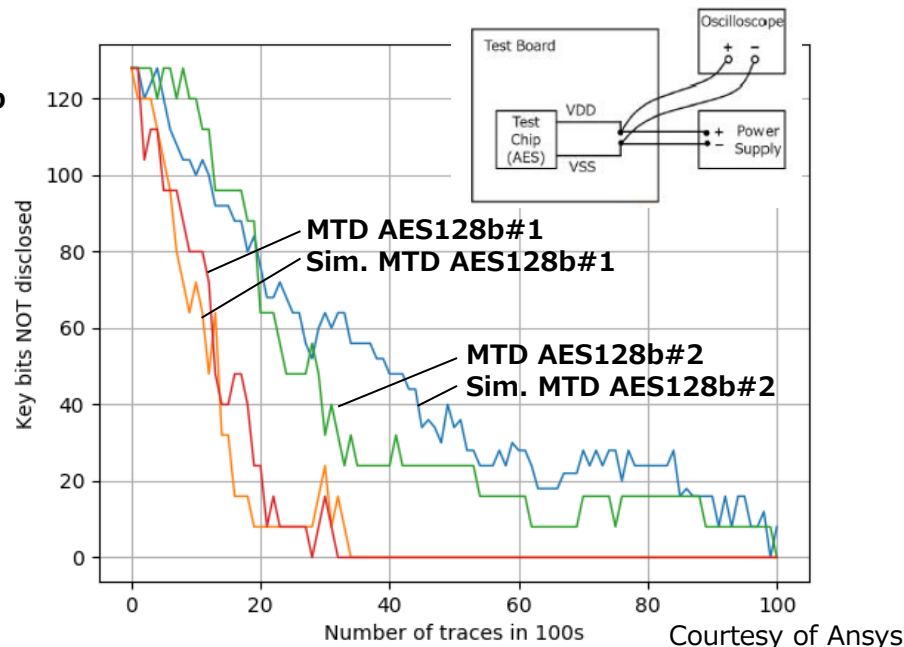


# Power SC leakage at full-chip level

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



## Measurement-to-disclose (MTD)



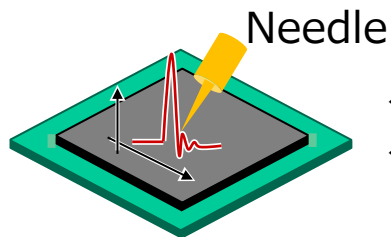
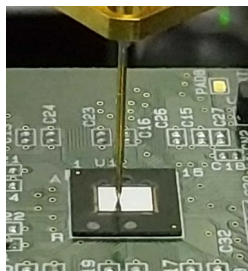
- ▶ Chip-level power SC leakage analysis using CPMs
- ▶ Direct vector control on security sensitive nets while vector-less mode on non-security nets over an IC chip.

# Outline

---

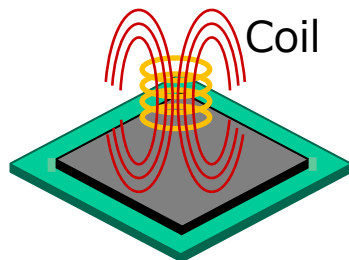
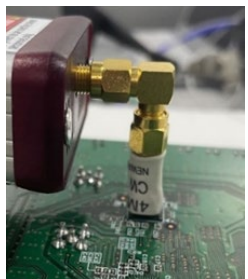
1. Introduction
2. Passive side channels from IC chip backside
3. Active fault injection on IC chip backside
4. Packaging for security
5. Summary

# Active fault injection on Si backside



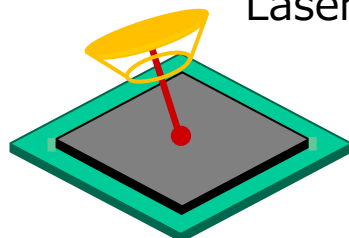
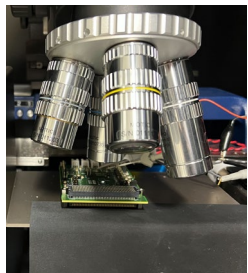
Needle

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



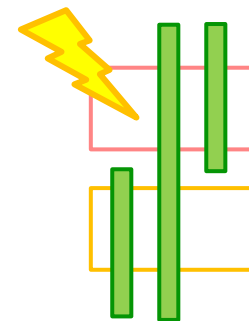
Coil

- ✓ Magnetic flux induction
- ✓ EM wave irradiation



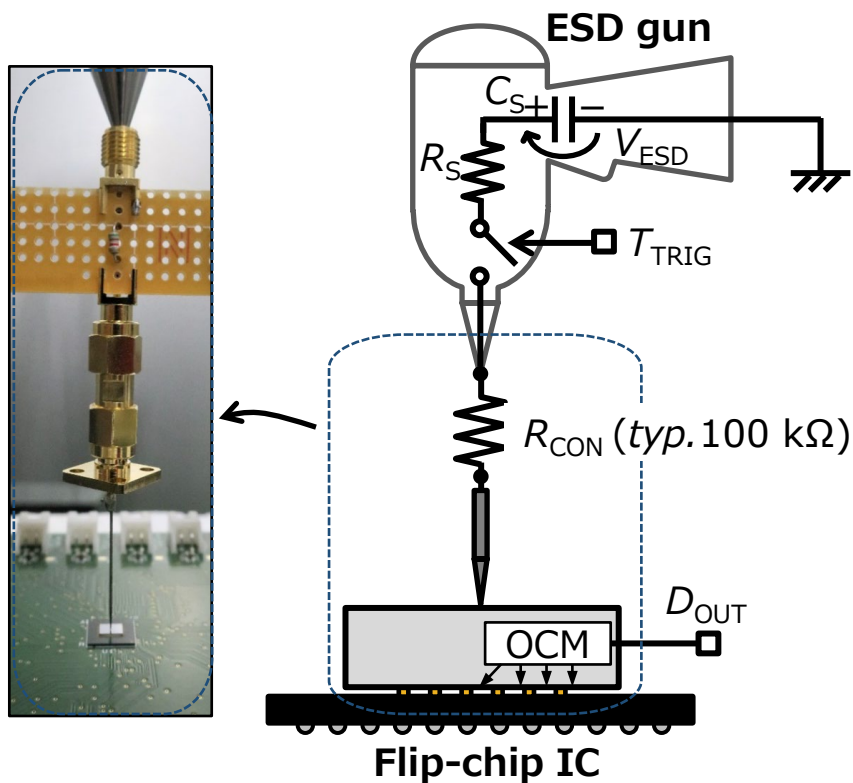
Laser

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

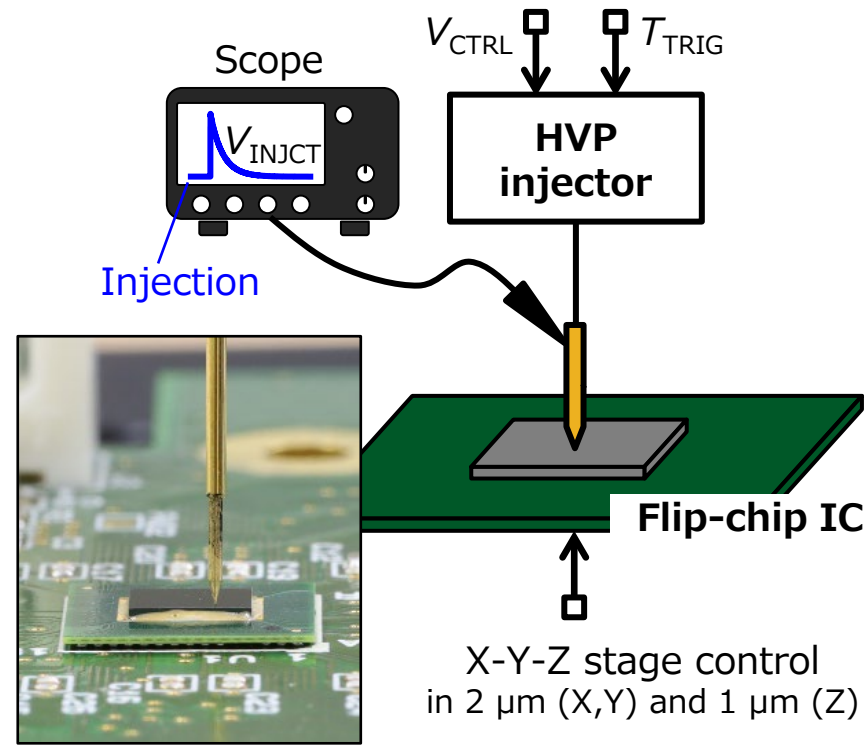


**Primary physics is different.**

# Chip backside pulsing

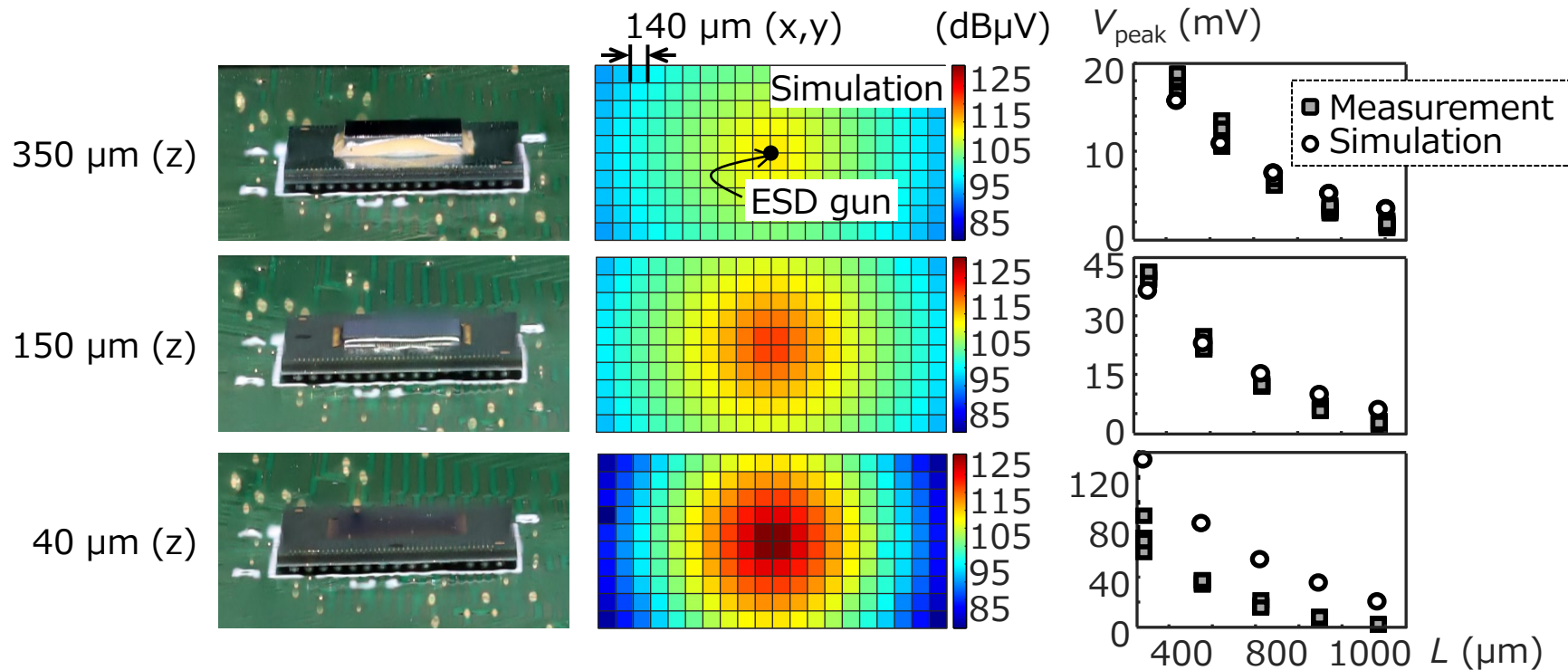


Ref. to ESD tradition (ISO10605, IEC61000-4-2)



HVP injector (custom made)

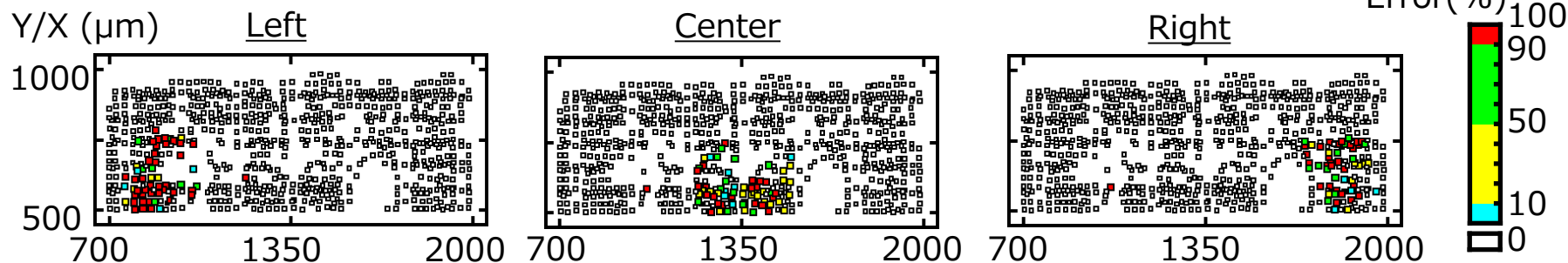
# Voltage spreads on IC chip frontside



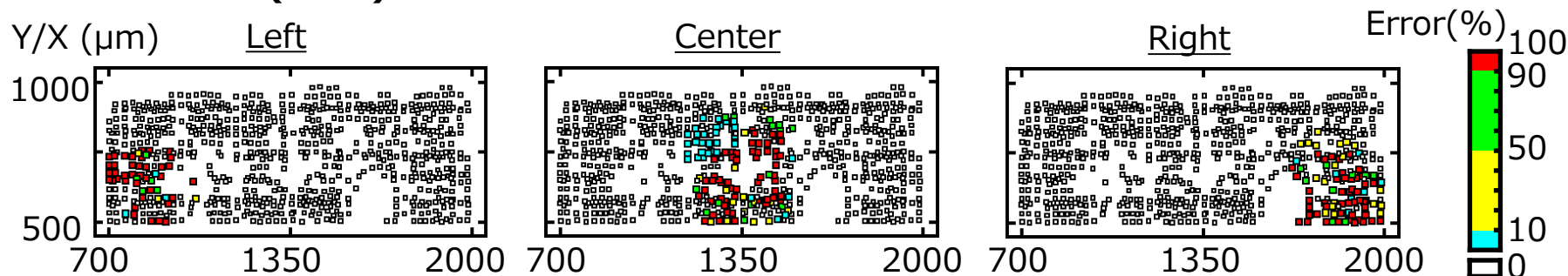
- ▶ ESD gun applied on Si backside, Si voltage measured on-chip on its frontside.
- ▶ Si substrate impedance model was simulated and calibrated.

# Si experiments

## Bit-set error (0→1)



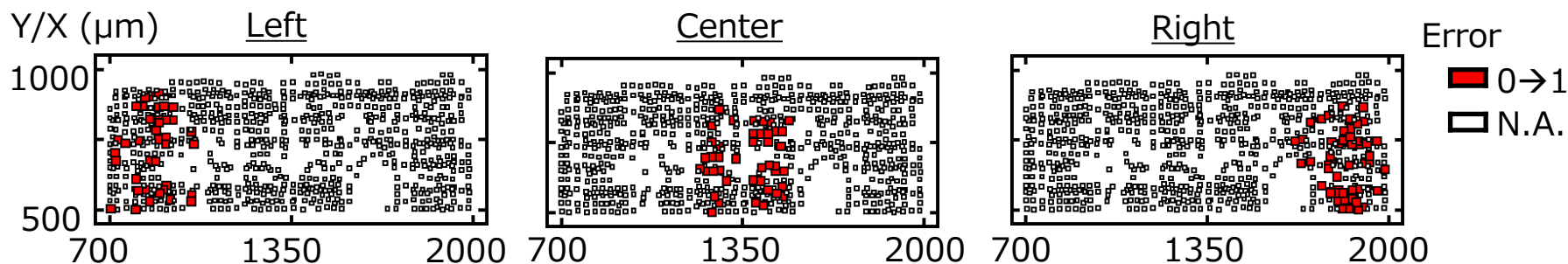
## Bit-reset error (1→0)



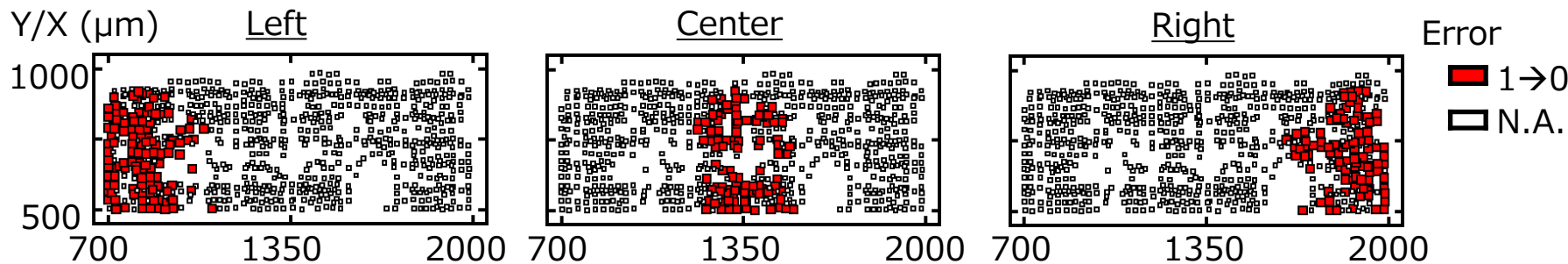
► Error bits induced by HVP among F/Fs – strongly location dependent.

# Simulation results

## Bit-set error (0→1)

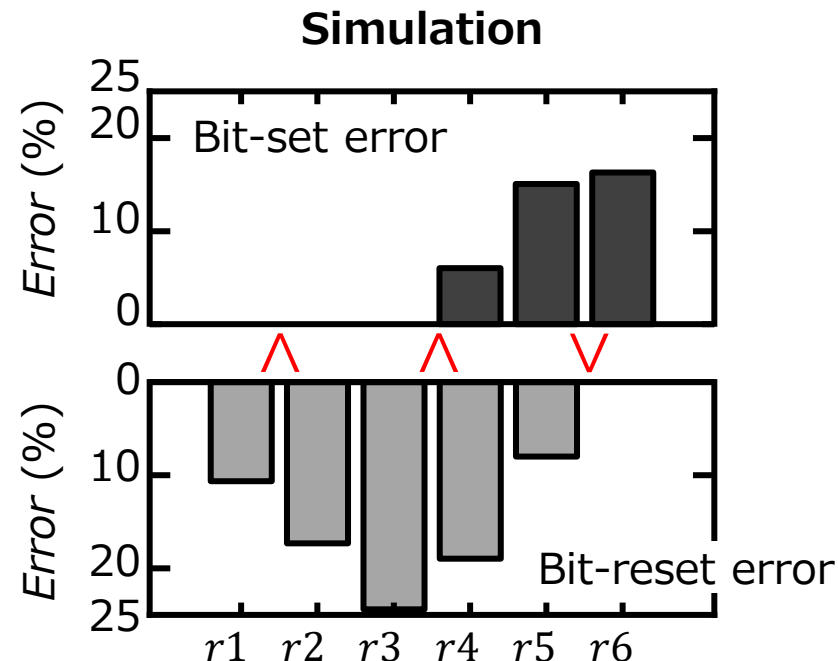
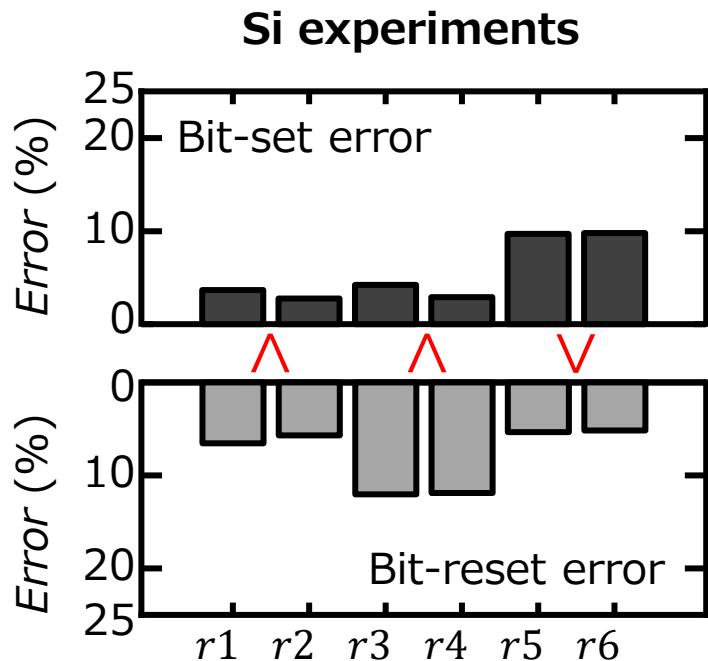


## Bit-reset error (1→0)



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

# Si experiments vs. simulation

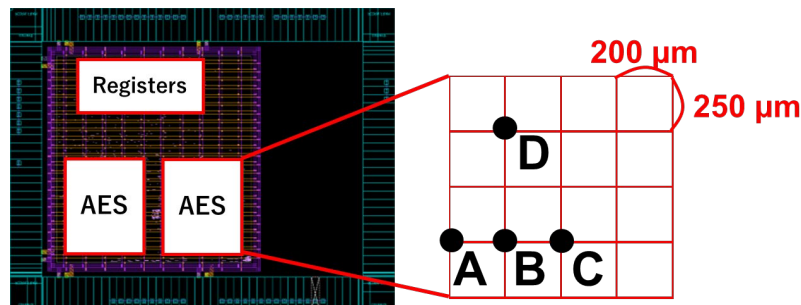


- Simulation explains **the presence of asymmetry** among the bit-set/bit-reset errors and the regions about error occurrences.



# Si experiments – security threats

IEEE Fault Diagnosis and Tolerance in  
Cryptography (FDTC), Sep. 2024.  
[DOI: 10.1109/FDTC64268.2024.00014](https://doi.org/10.1109/FDTC64268.2024.00014)



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**

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

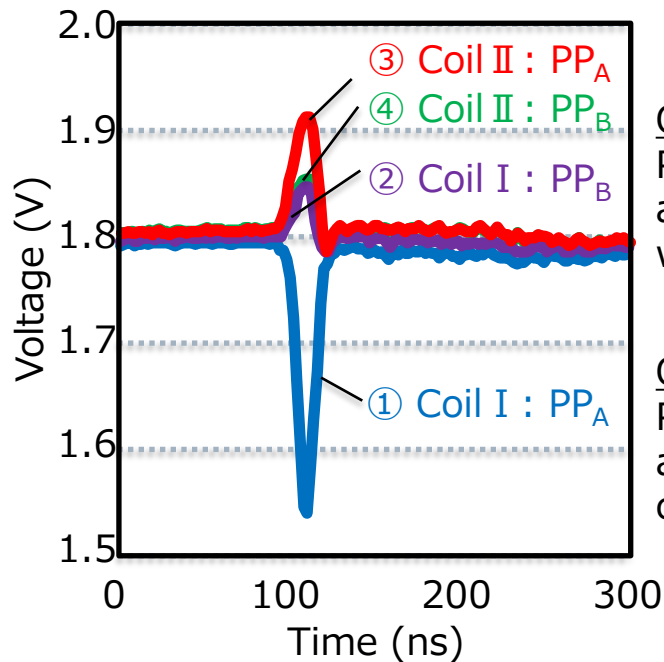
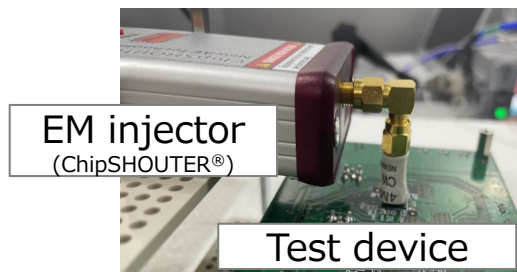
Faulty ciphertext with **single-bit error in every byte**

  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.

# EM induced voltage on Si backside

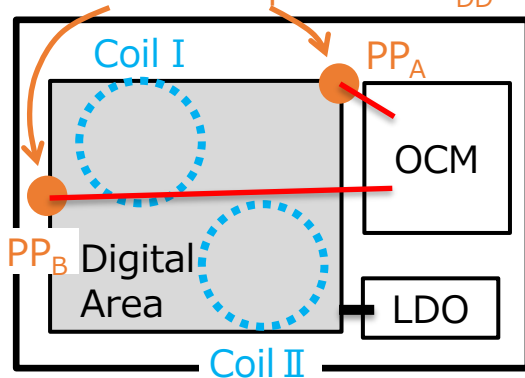
International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE),  
Apr. 2024. DOI: [10.1007/978-3-031-57543-3\\_2](https://doi.org/10.1007/978-3-031-57543-3_2)



Observation #1 (from ① vs. ②)  
Positive and negative swings are observed in PP<sub>A</sub> and PP<sub>B</sub> when **Coil I** is used.

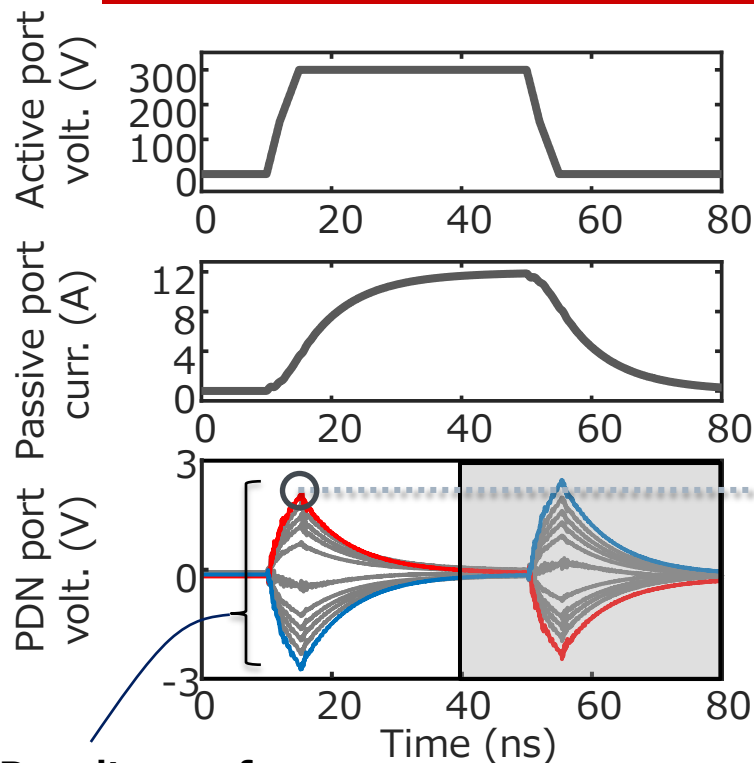
Observation #2 (from ① vs. ③)  
Positive and negative swings are observed in PP<sub>A</sub> when comparing **Coil I** and **Coil II**.

Different monitor point on V<sub>DD</sub> net



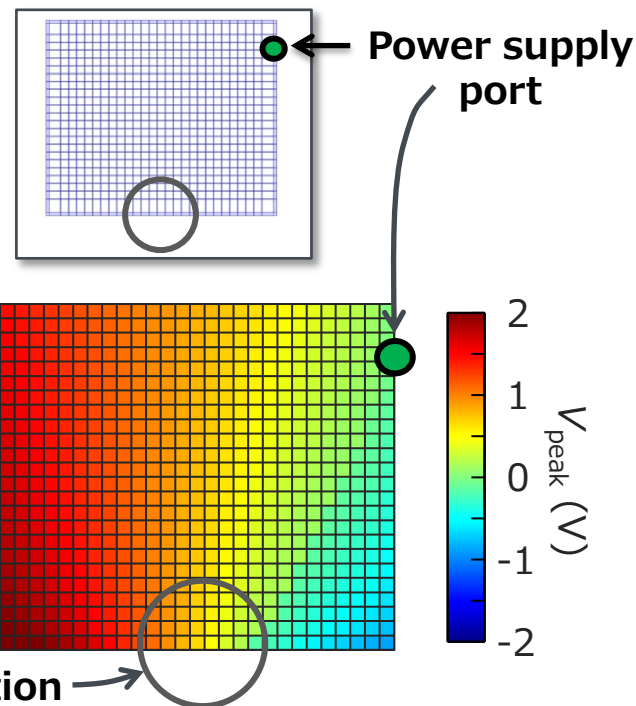
► EM fields create voltage glitches that spread across wide chip area.

# Simulation of magnetic field coupling



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

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

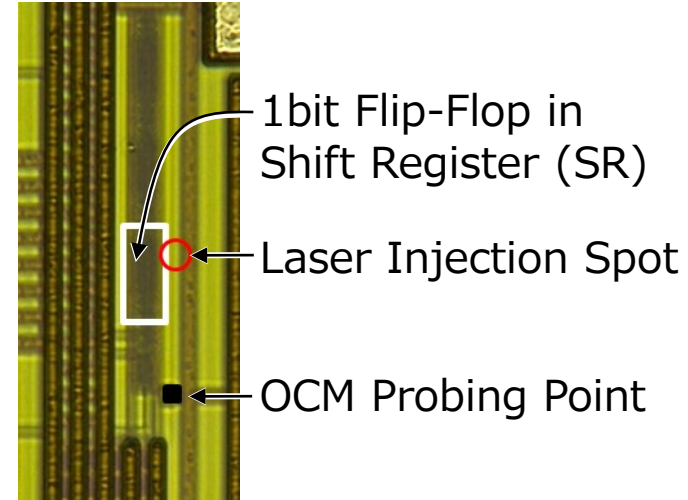
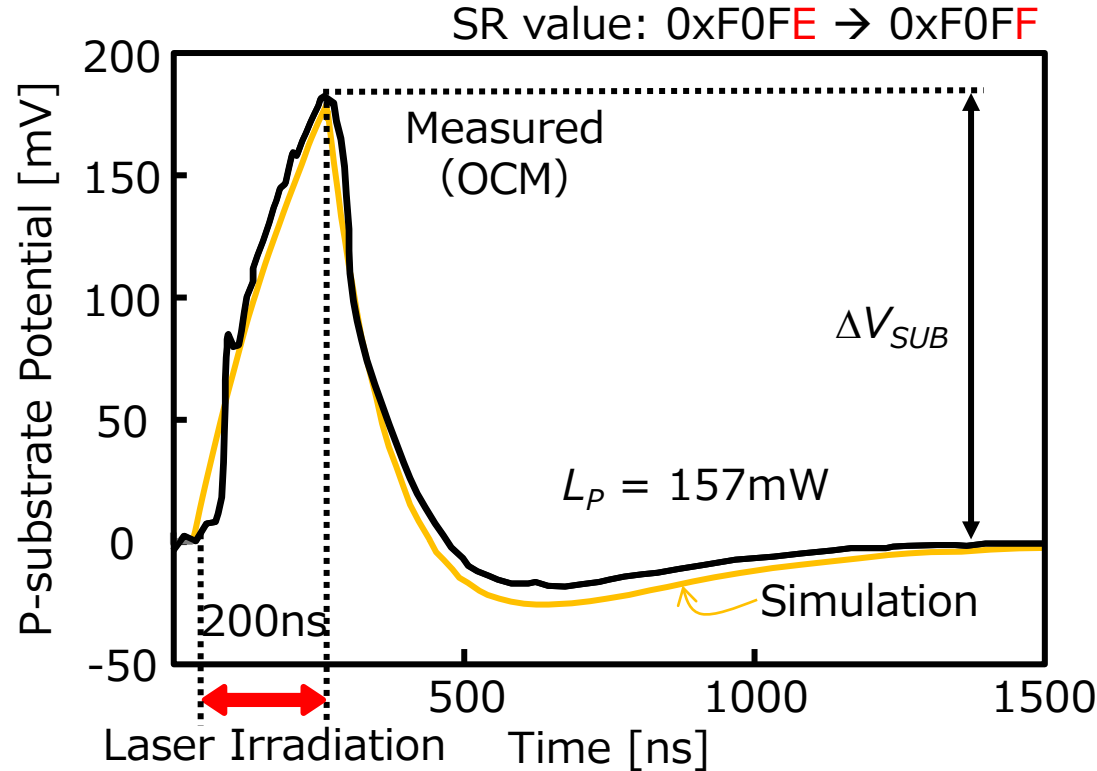


Result waveforms

$$28 \times 24 = 672$$

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

# Laser induced $V_{SUB}$ waveforms



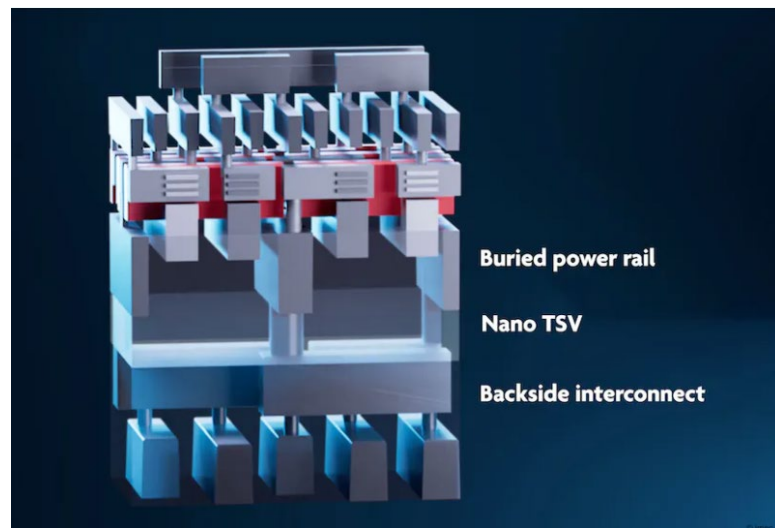
- Simulation with equivalent circuits estimates photo-voltage conversion.

# Outline

---

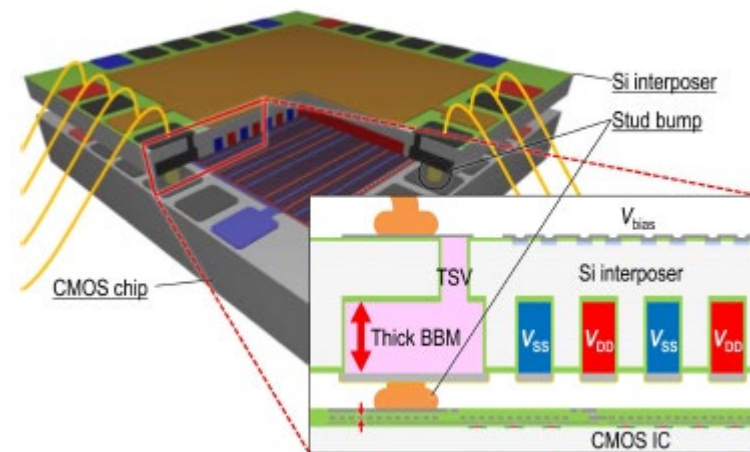
1. Introduction
2. Passive side channels from IC chip backside
3. Active fault injection on IC chip backside
4. Packaging for security
5. Summary

# Si-backside integration technology



Source: IMEC

<https://www.imec-int.com/en/articles/how-power-chips-backside>



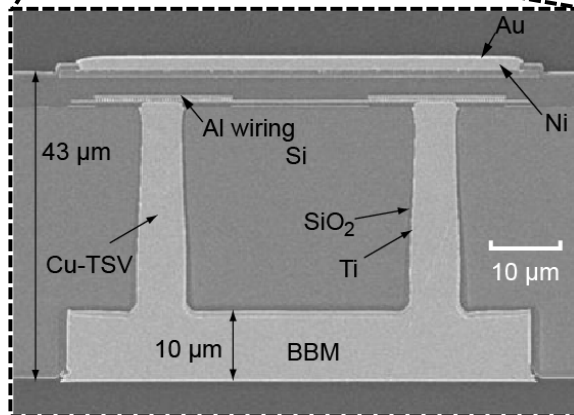
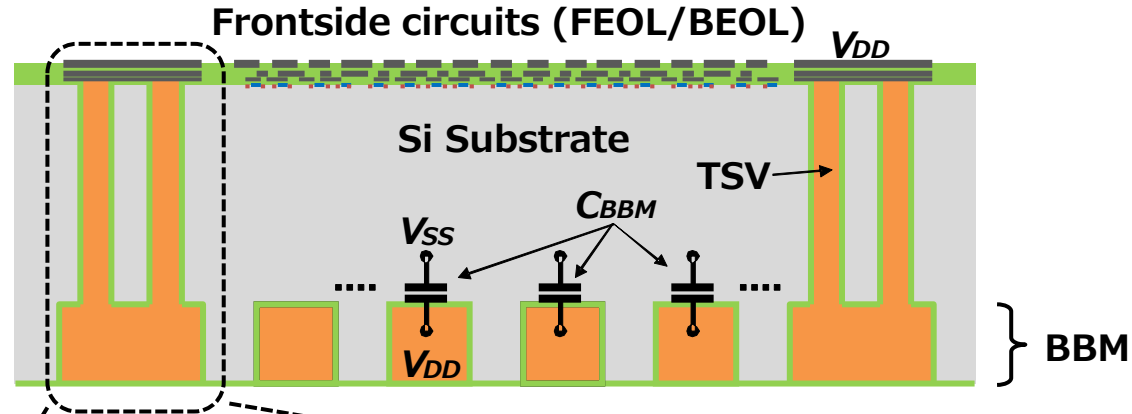
Source: IEEE Trans. CPMT, 2018.

<https://doi.org/10.1109/TCPMT.2018.2877211>

- ▶ Mega trends: full-stack process modules of Si-backside power delivery and interconnect networks in advanced FF technology nodes – Intel, ARM, Synopsys, IMEC
- ▶ Advanced packaging technology uses Si-backside buried metal (via-last) process in traditional CMOS technology nodes – AIST, Kobe U.

# Backside buried metal (BBM)

IEEE Transactions on Components,  
Packaging and Manufacturing  
Technology (CPMT), Mar. 2019.  
[DOI: 10.1109/TCPMT.2018.2877211](https://doi.org/10.1109/TCPMT.2018.2877211)

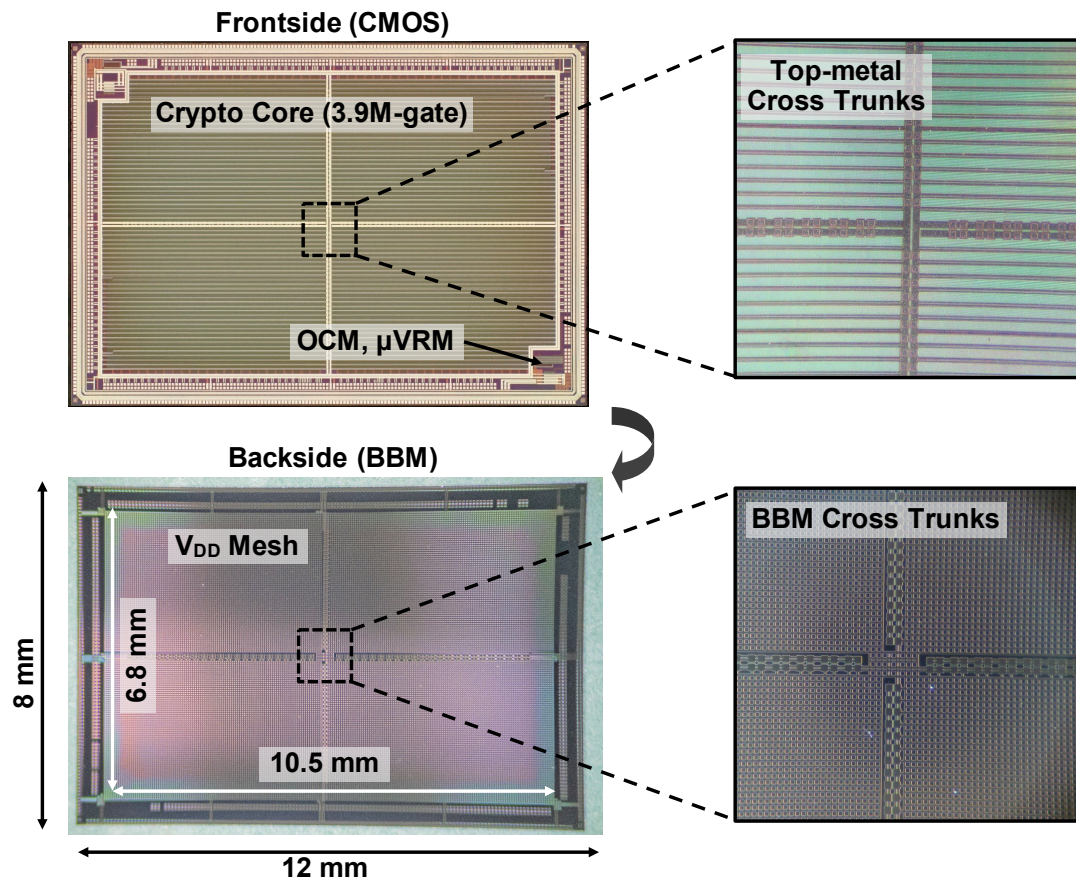


## Post wafer (via-last) manufacturing

BBM Depth	10 $\mu\text{m}$
BBM width	15 $\mu\text{m}$
BBM space	10 $\mu\text{m}$
TSV depth	40 $\mu\text{m}$
TSV diameter	10 $\mu\text{m}$
TSV pitch	40 $\mu\text{m}$



# Tier photos on front and back sides

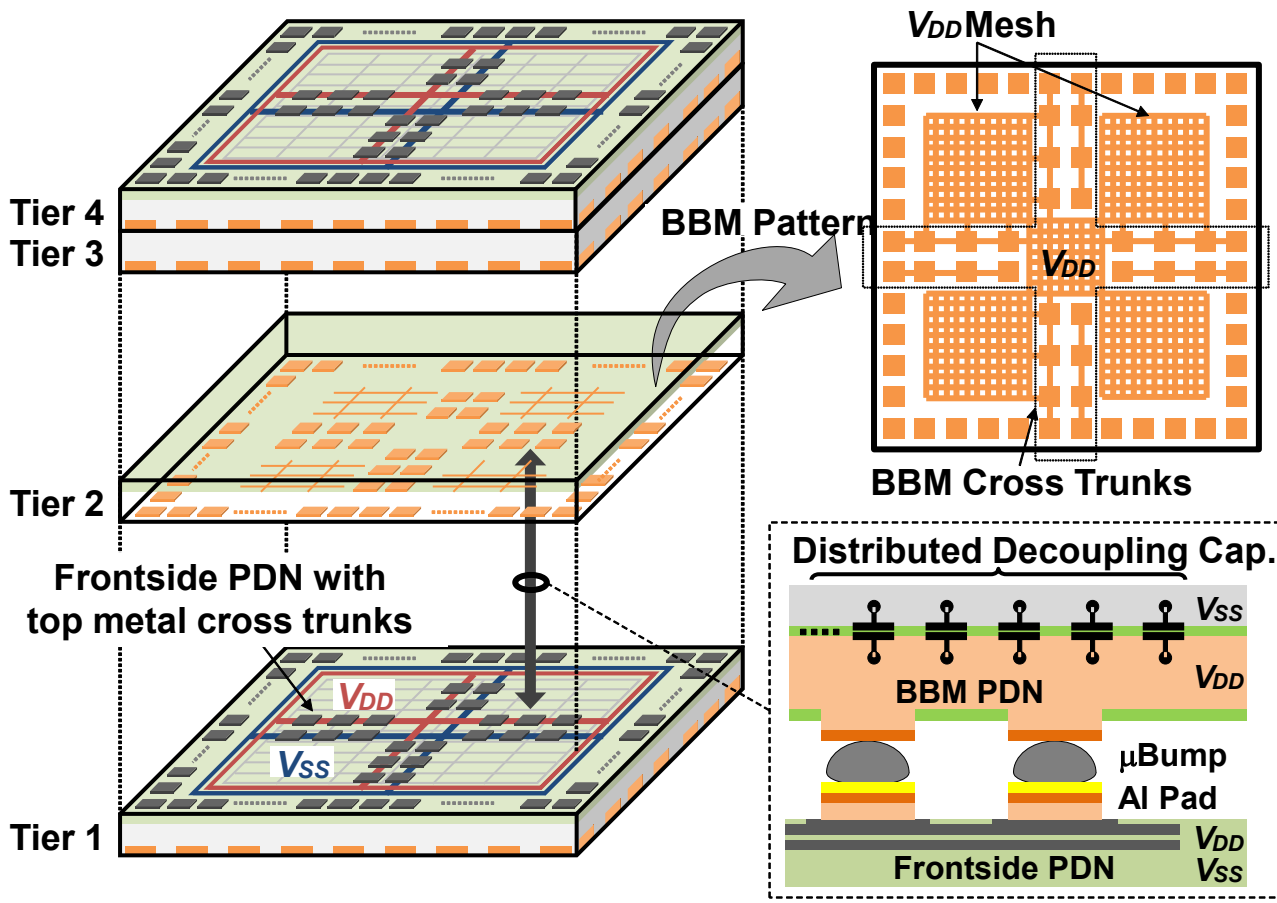


**Thanks to AIST team:**

Yuuki Araga  
Naoya Watanabe  
Haruo Shimamoto  
Katsuya Kikuchi

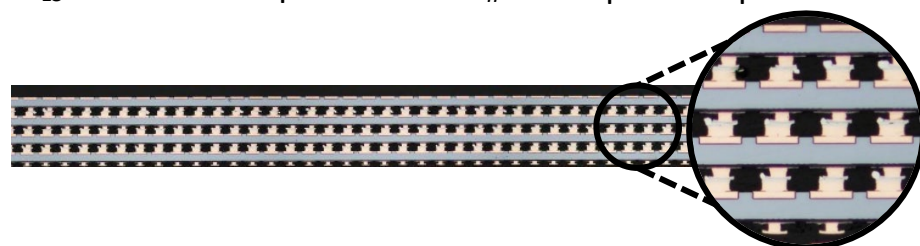
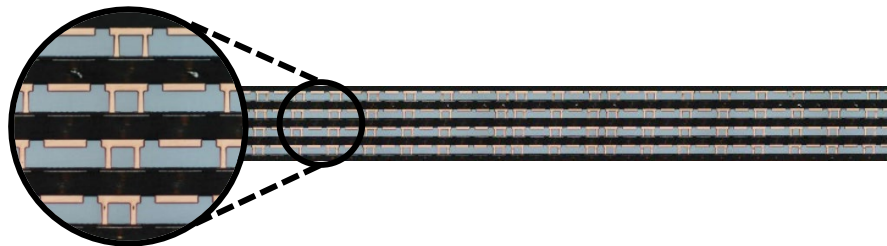
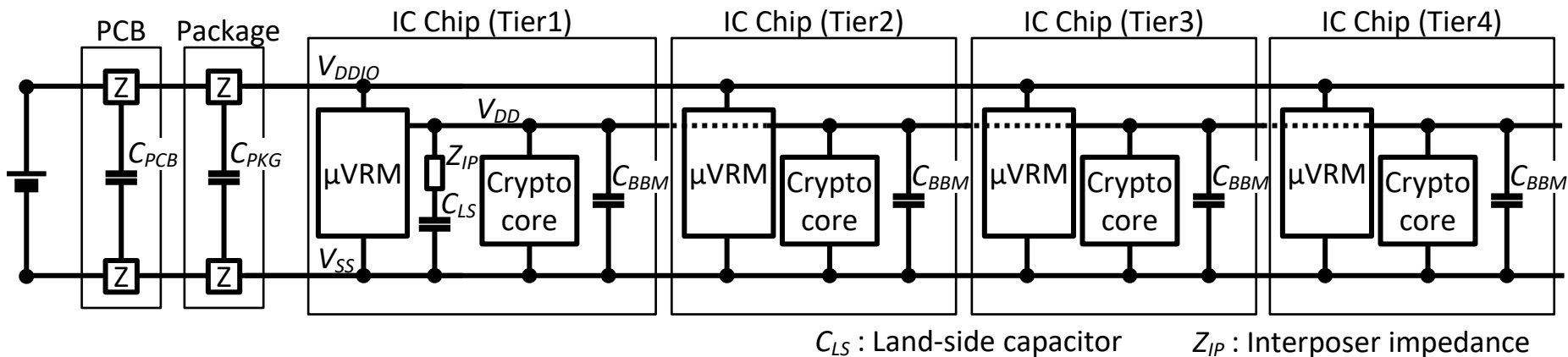


# Si-backside usage in 3D chip stack



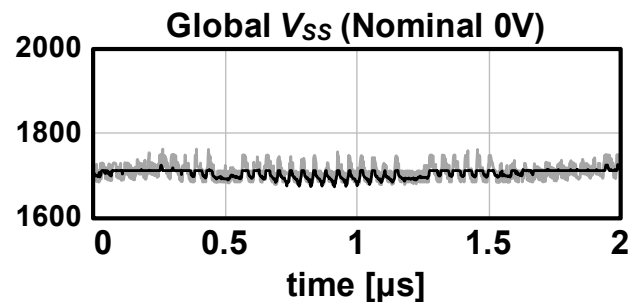
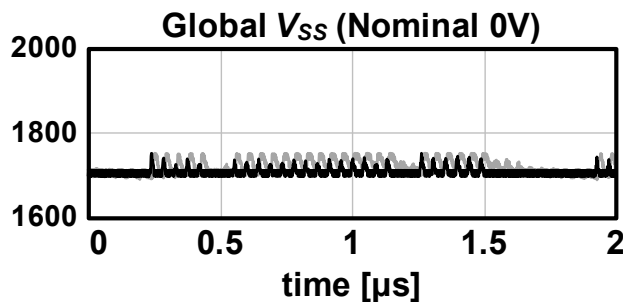
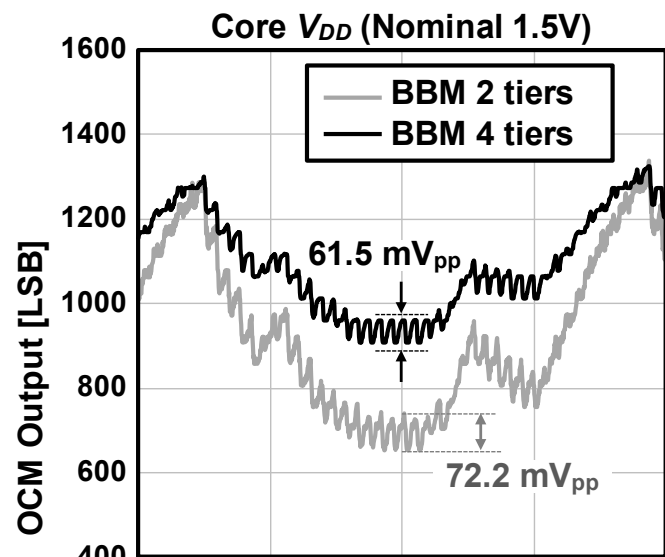
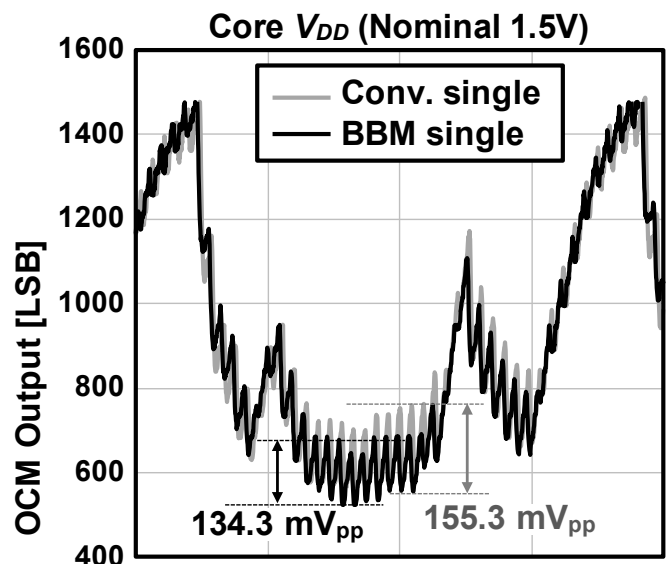
# 3D PDN\* with BBM

\*Power Delivery Network

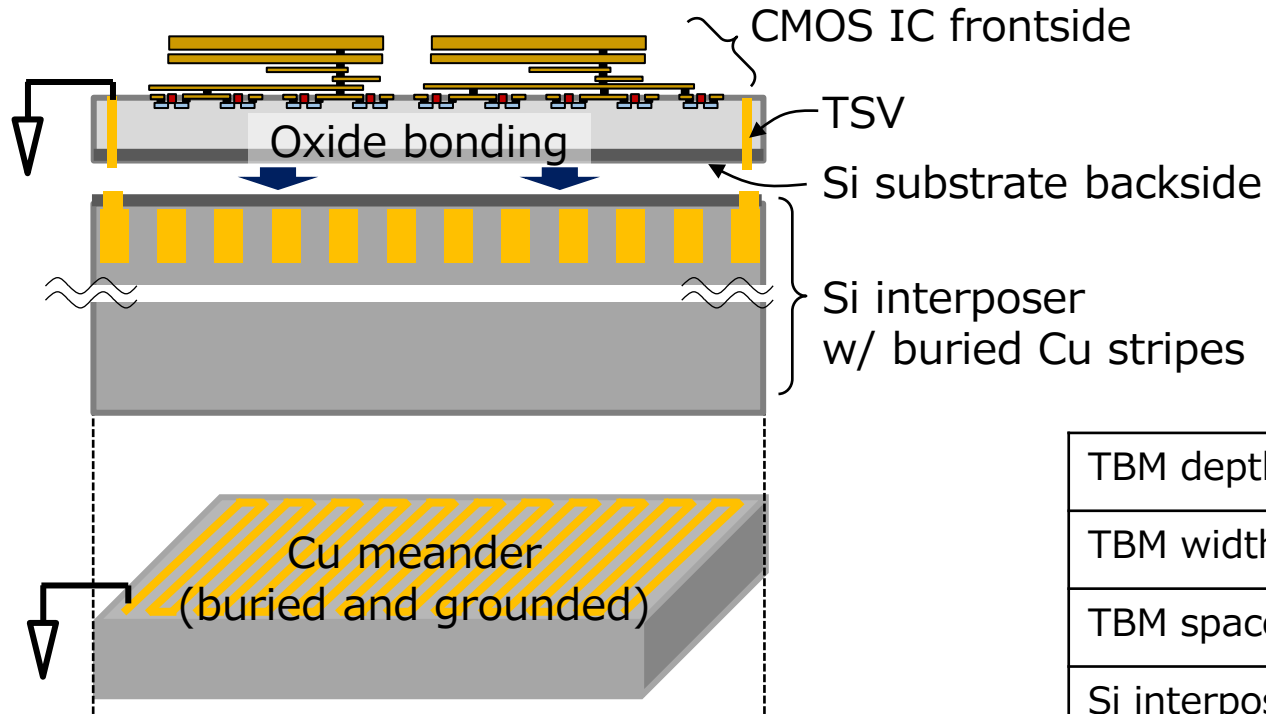


- Secure IC chips with backside caps ( $C_{BBM}$ ) are integrated in a 4-tier stack.

# Power noise in 3D stack (measured)



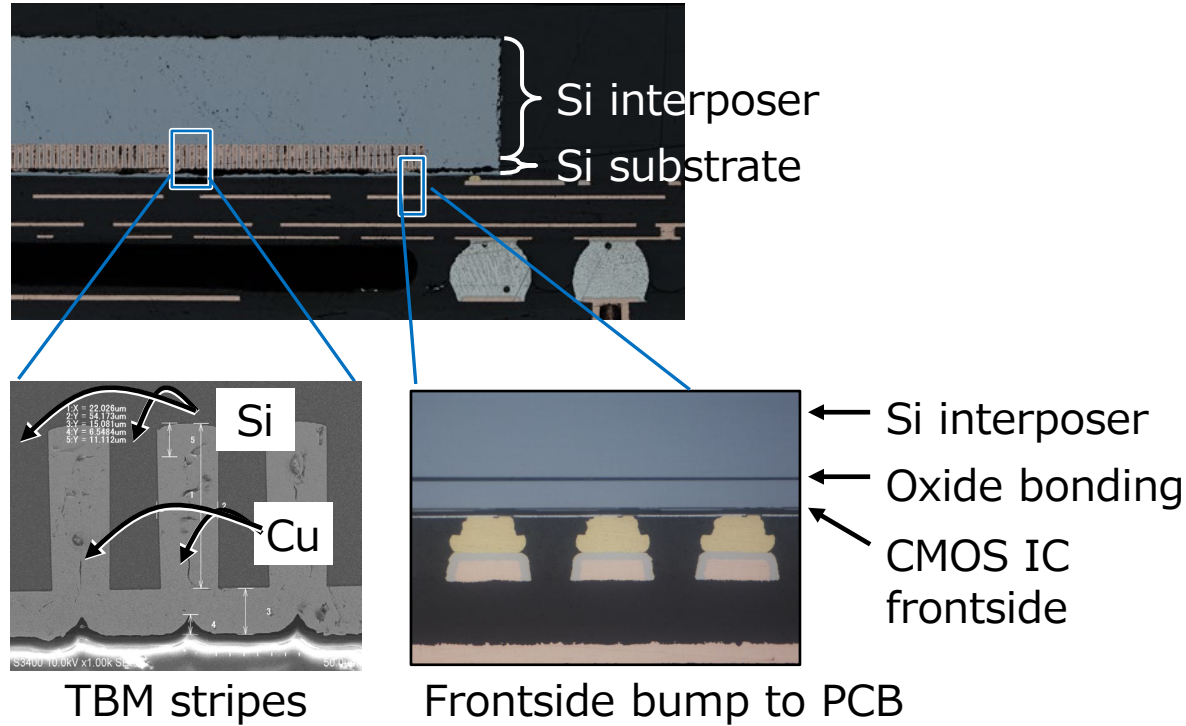
# Si backside bonded and buried metal (TBM)



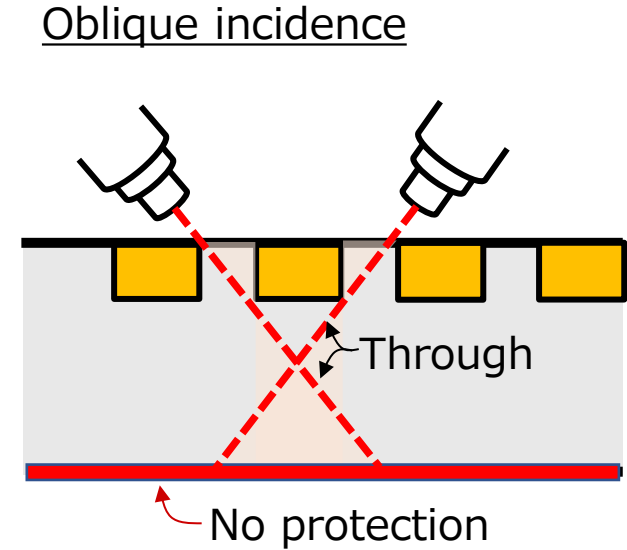
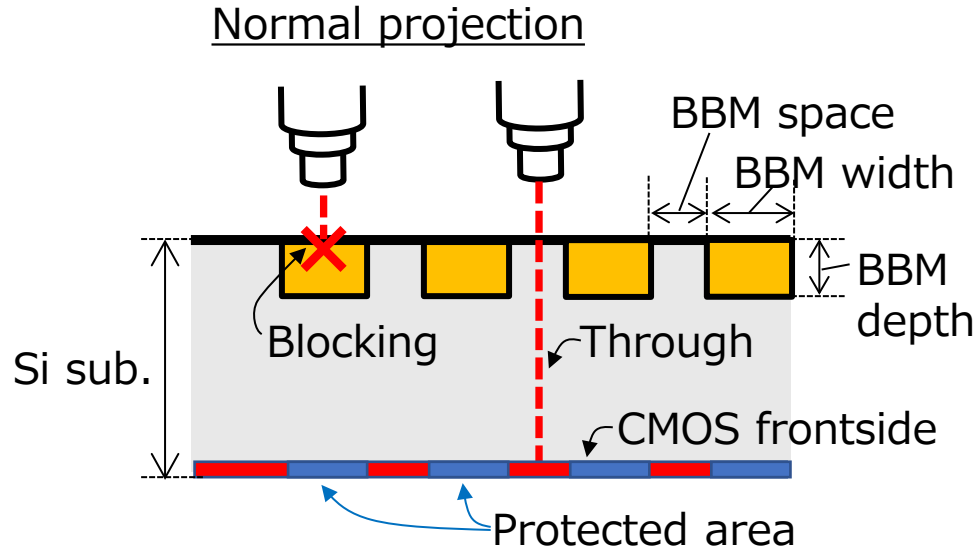
- ▶ Extended depth of backside buried Cu metal  
e.g. 50  $\mu\text{m}$  (TBM) vs. 10  $\mu\text{m}$  (BBM)

TBM depth	50 $\mu\text{m}$
TBM width	20 $\mu\text{m}$
TBM space	20 $\mu\text{m}$
Si interposer thickness	350 $\mu\text{m}$
Si substrate thickness	20 $\mu\text{m}$

# TBM demonstrator photo

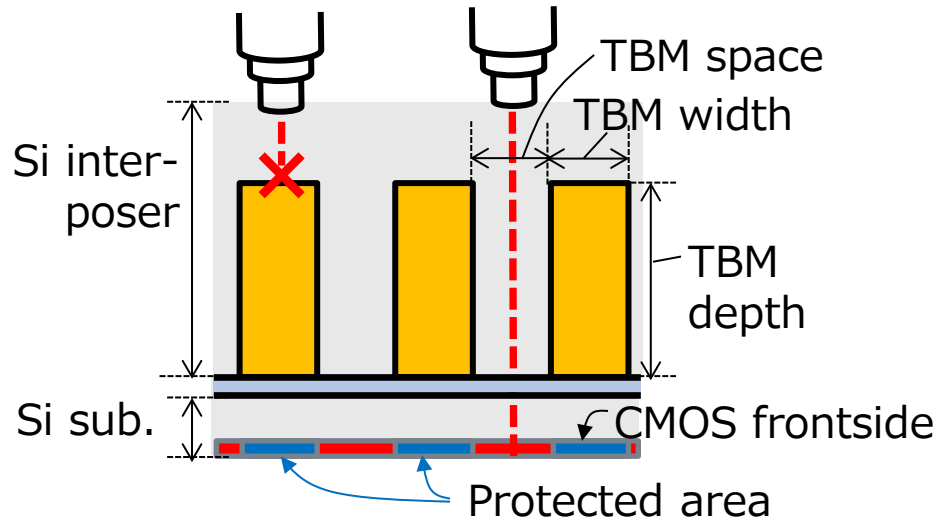


# Blockage of IR laser exposure by BBM

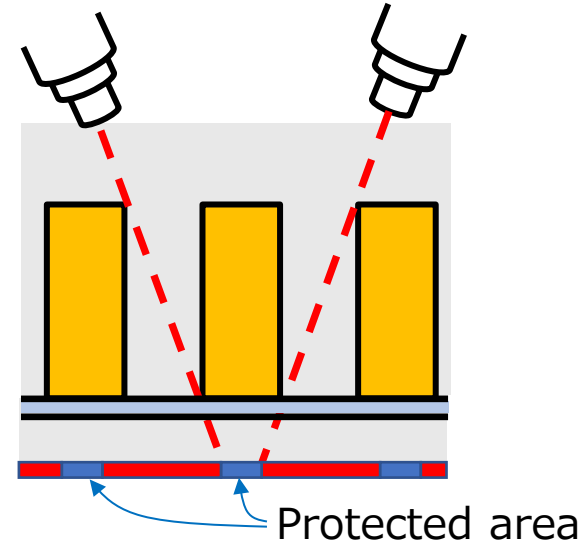


# Blockage of IR laser exposure by TBM

Normal projection

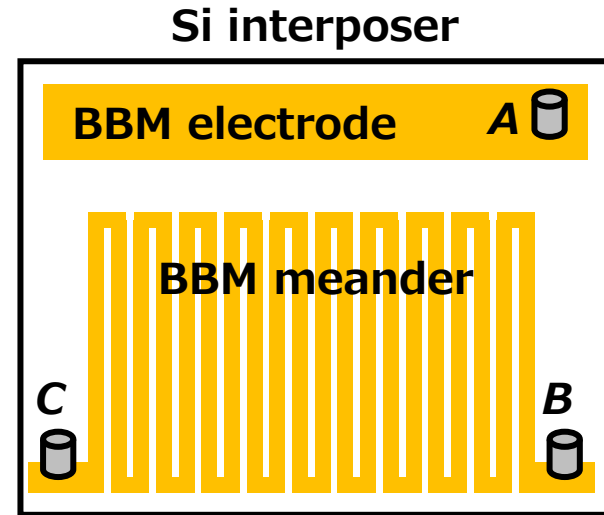
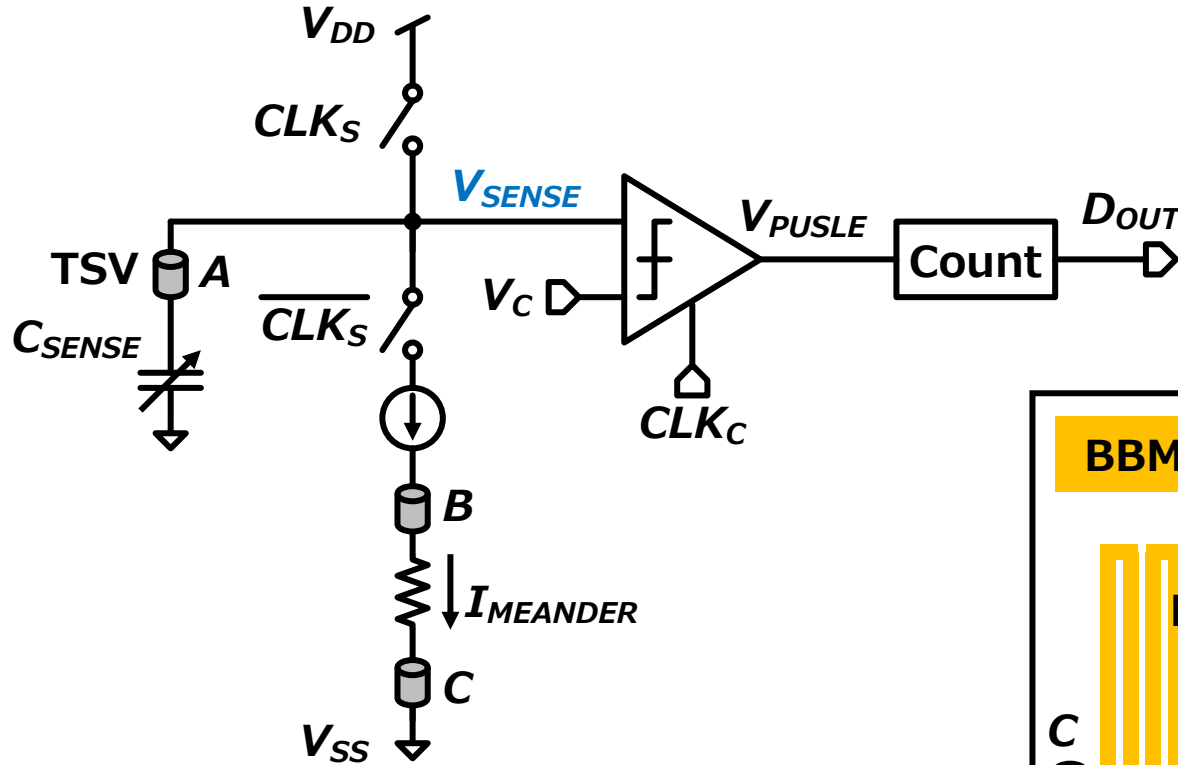


Oblique incidence



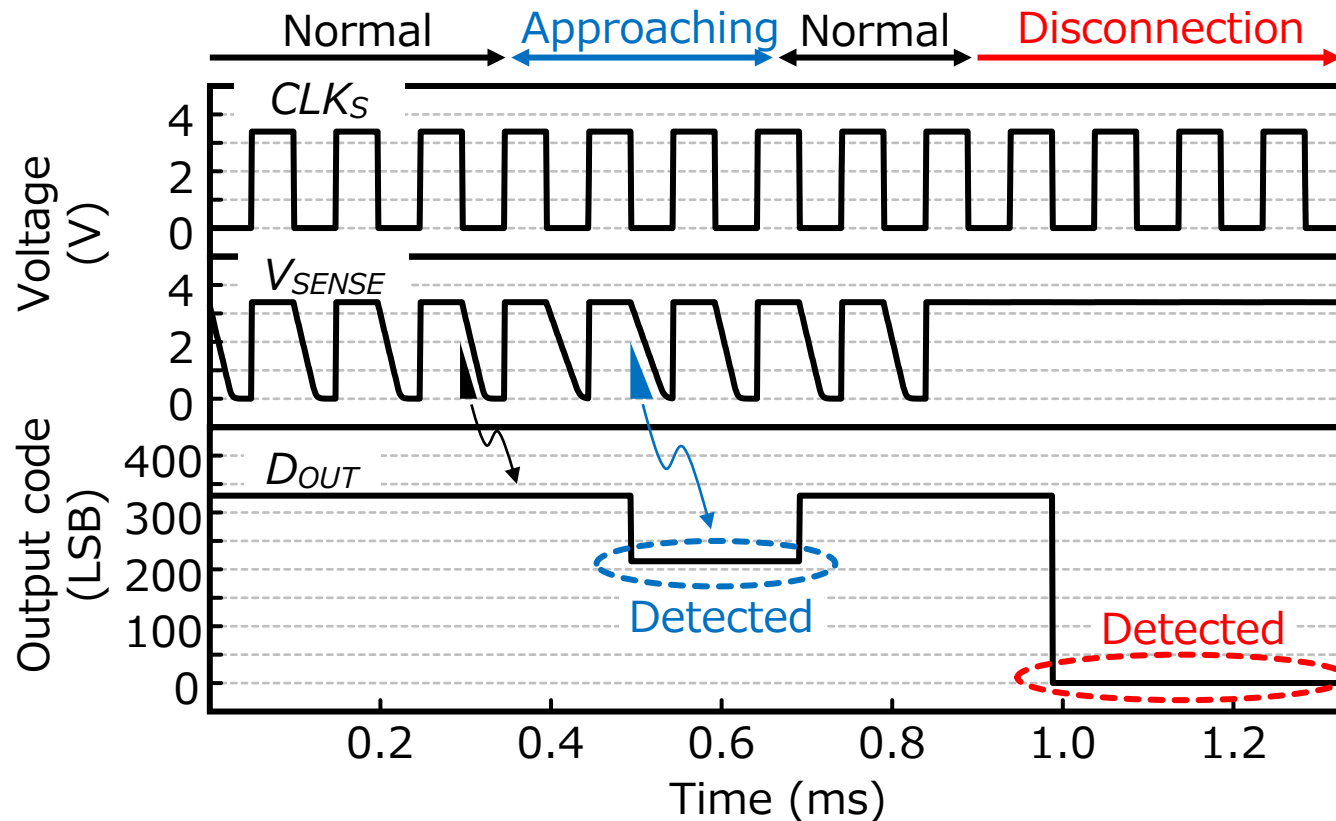
# Si-backside attack detection

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

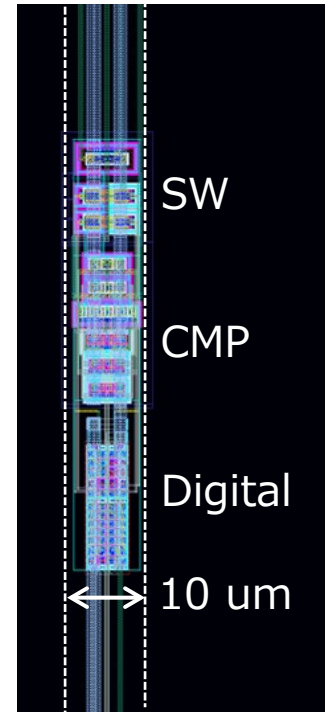
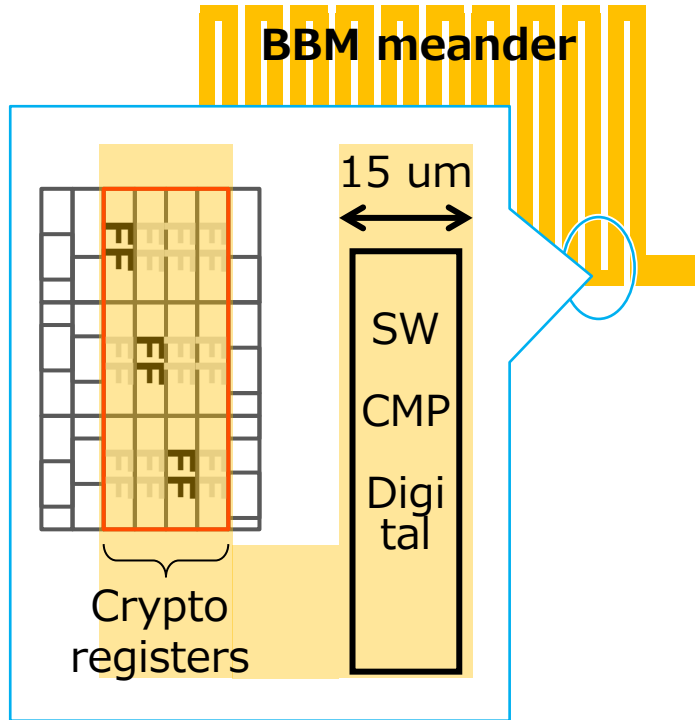




# Simulated waveforms



# Attack protection structure

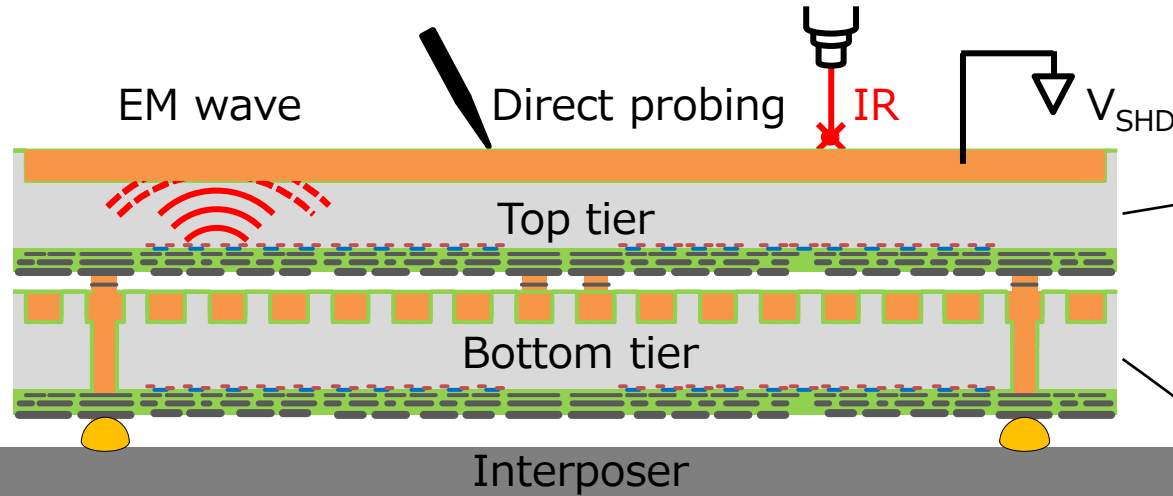


SW: switches  
CMP: Comparator

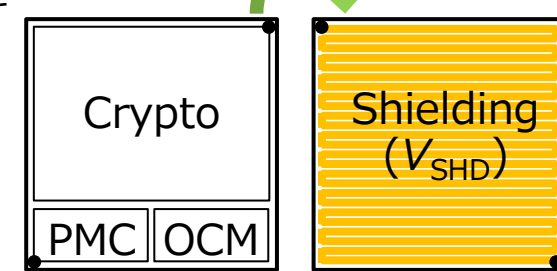
- **Front side (IC) and back side (BBM) co-design** makes circuits of interest hidden from backside injection, as well as sensor circuits to detect injection.

# Secure 3D IC chip stack using BBM

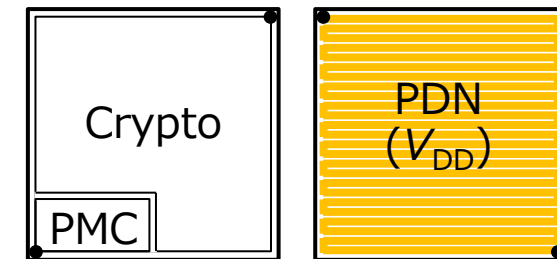
IEEE Transactions on Very Large Scale Integration Systems (TVLSI), Jan. 2022. DOI: [10.1109/TVLSI.2021.3073946](https://doi.org/10.1109/TVLSI.2021.3073946)



Top tier or single chip



Bottom/intermediate tier



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

# Summary

---

- ▶ **Analog techniques for digital security:** simulation, modeling, device, circuit, packaging and manufacturing are to be synergistically exploited toward the higher levels of HWS.
- ▶ **Pre-silicon assessments and design justifications:** relying on advanced simulation and modeling for security and safety metrics.
- ▶ **Deployment of chiplets and advanced packaging:** more scientific exploration across multi-dimensional design space for system-level performance, security assurance and manufacturing costs. Theory, modeling and methodology are 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.