



JUNE 23-27, 2024

MOSCONE WEST CENTER
SAN FRANCISCO, CA, USA





JUNE 23-27, 2024

MOSCONE WEST CENTER
SAN FRANCISCO, CA, USA



Si Backside Side-Channel Leakage and Simulation of Cryptographic IC Chips

Rikuu Hasegawa⁽¹⁾, Kazuki Monta⁽¹⁾, Takuya Wadatsumi⁽¹⁾, Takuji Miki⁽¹⁾, Makoto Nagata⁽¹⁾

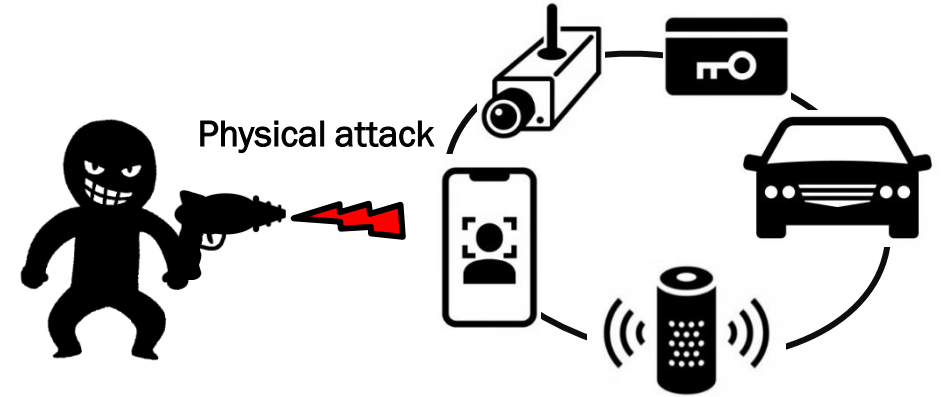
Lang Lin⁽²⁾, Sreeja Chowdhury⁽²⁾, Akhilesh Kumar⁽²⁾, Norman Chang⁽²⁾

Kobe University⁽¹⁾, ANSYS Inc.⁽²⁾



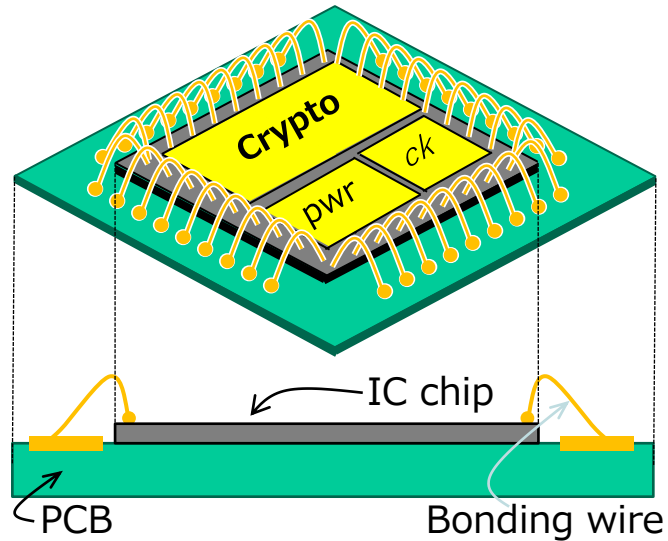
Background

- Security of semiconductor devices
 - Cryptography security measures
- Side-channel analysis (SCA)
 - Physical information during cryptography operation



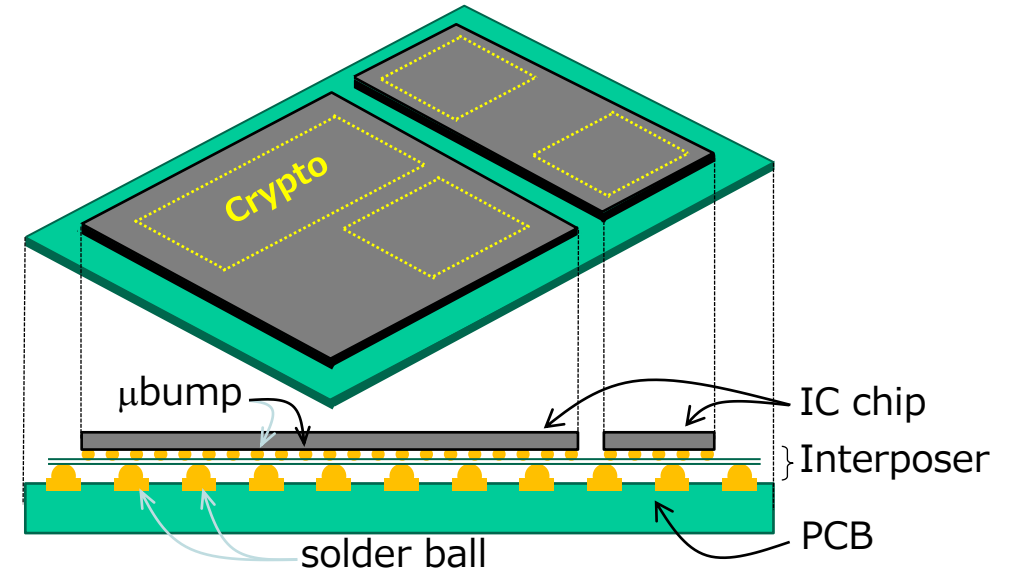
IC Chip Packaging Trends and Attack Surface

- Face up (Traditional)



- Bonding wire
- Adversarial access
 - Probing on crypto from front side

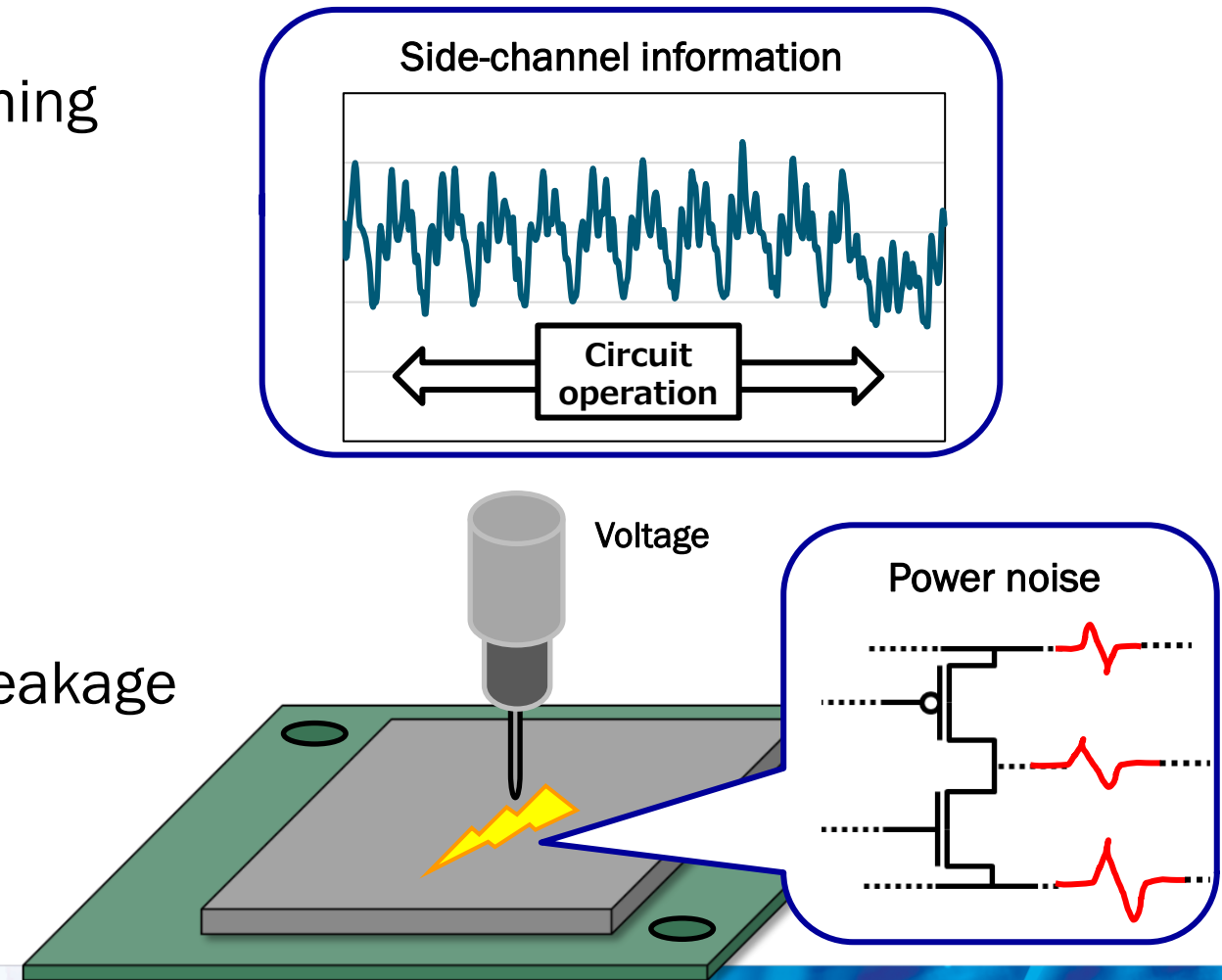
- Flip chip (Contemporary)



- μbump and ball grid array
- Trend towards thinner chips
- Adversarial access
 - Probing on crypto from the backside

Power noise side-channel attacks

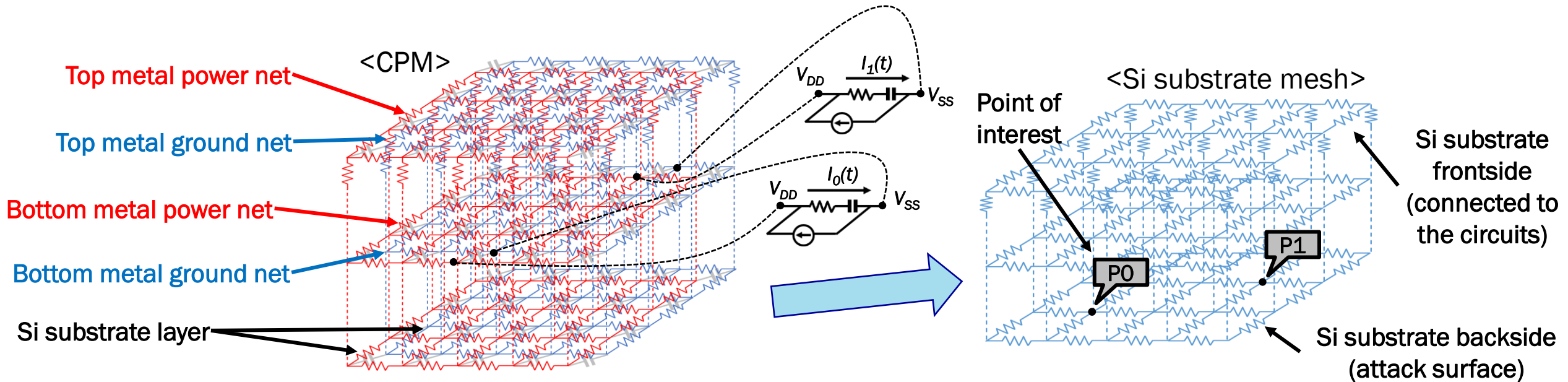
- Side-channel leakage
 - Power noise caused by transistor switching
- Verification is needed
 - Accurate power noise analysis
 - Power noise analysis for side-channel leakage



Si Substrate Voltage Simulation using CPM

- Create CPM (Chip Power Model) for side-channel analysis
 - Power library of standard cells
 - Logic transition
 - Design data

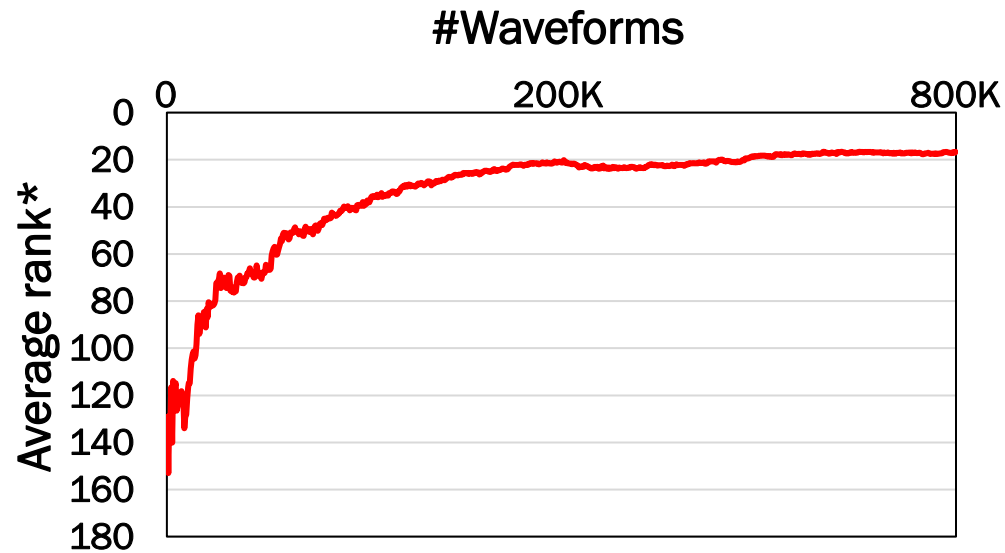
CPM



Side-channel Leakage Evaluation by CPA*

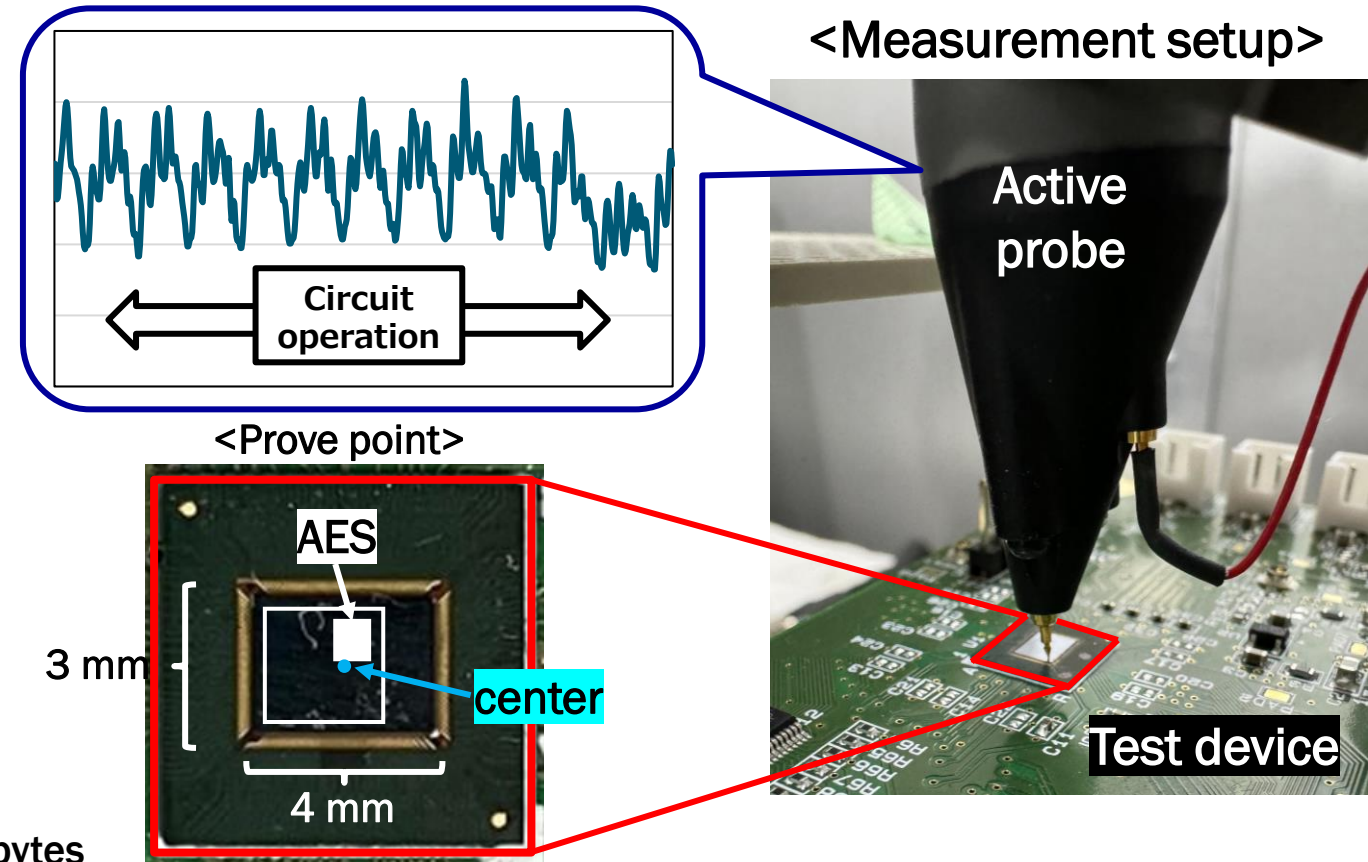
***CPA : Correlation Power Analysis**

- Leakage at the center of the chip



***Average lank :**

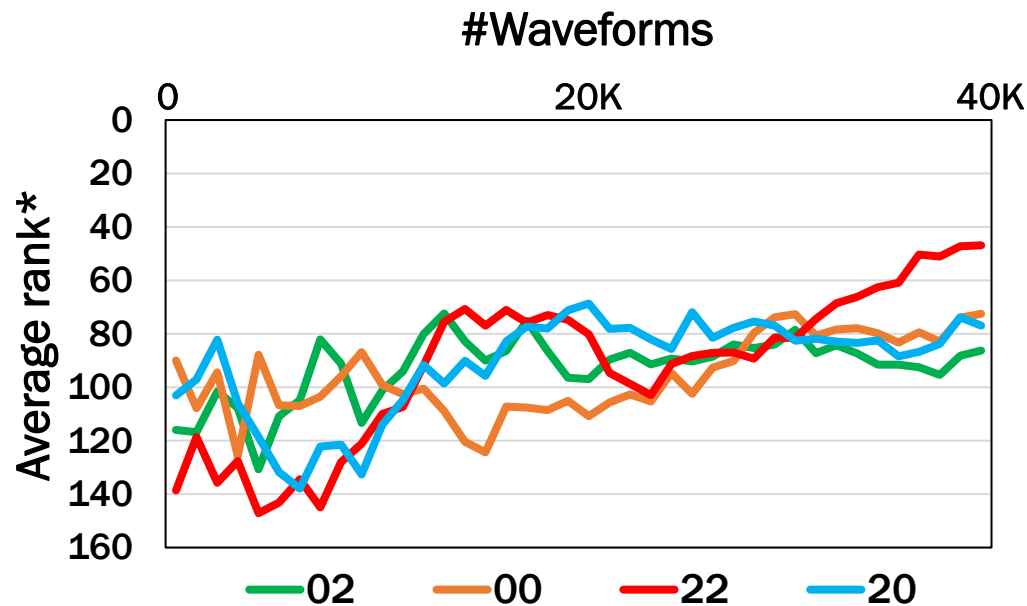
Take the average of the correlation value ranks of all bytes



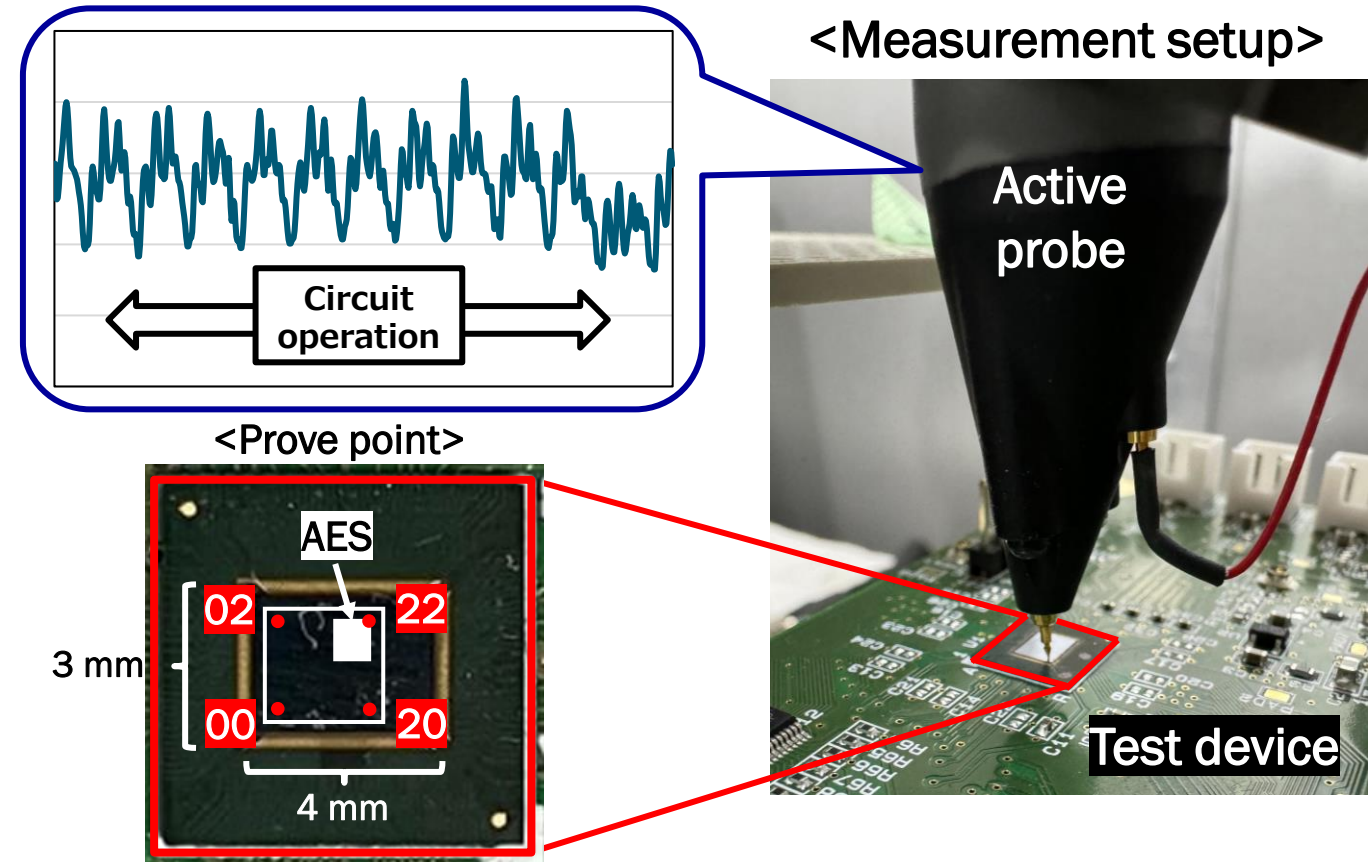
Side-channel Leakage Evaluation by CPA*

*CPA : Correlation Power Analysis

- Leakage at the corner of the chip
 - Strong leakage at proximity of AES
 - Possibility of locality

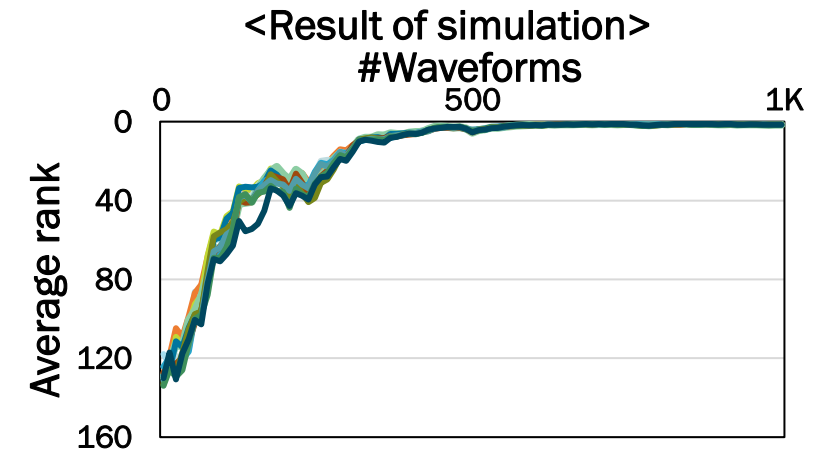
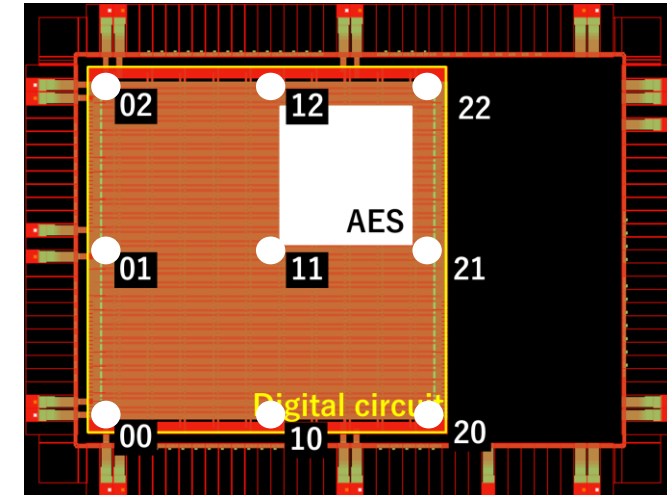
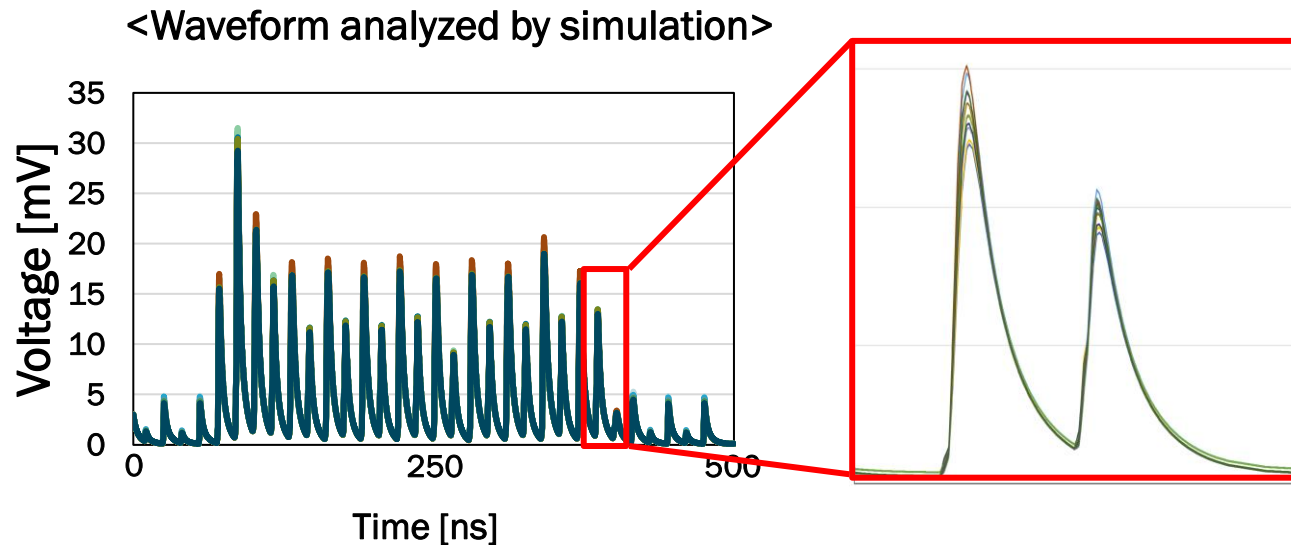


*Average rank : Take the average of the correlation value ranks of all bytes



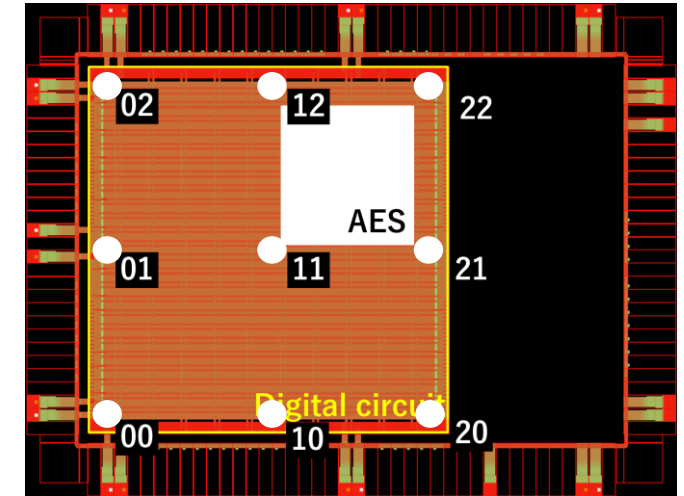
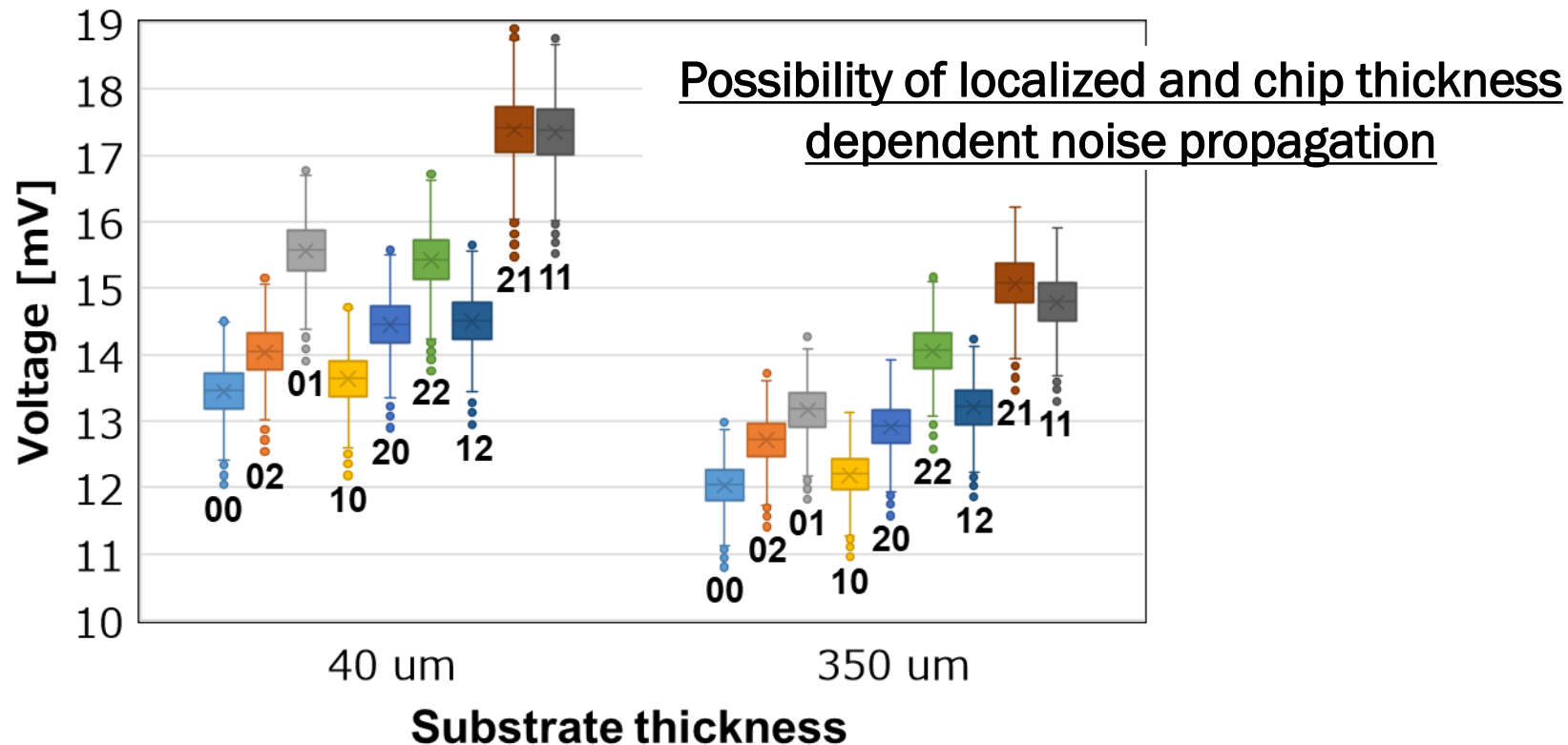
Side-channel Leakage Evaluation by CPA

- Evaluation by simulation
 - Waveform change depends on position
 - Too high S/N might cause these results

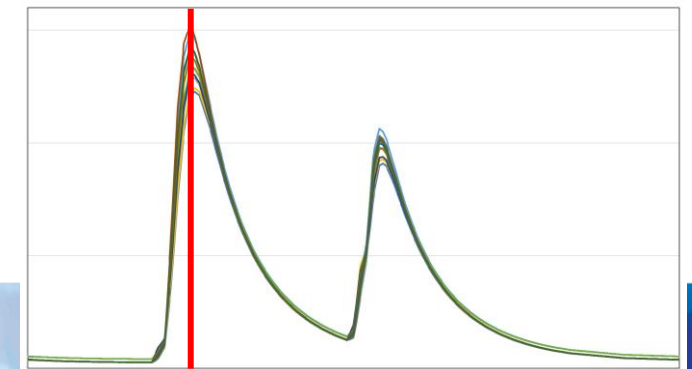


Side-channel waveform evaluation

- 1000 waveforms acquired for different substrate thicknesses CPM
 - V_{pp}^* variation

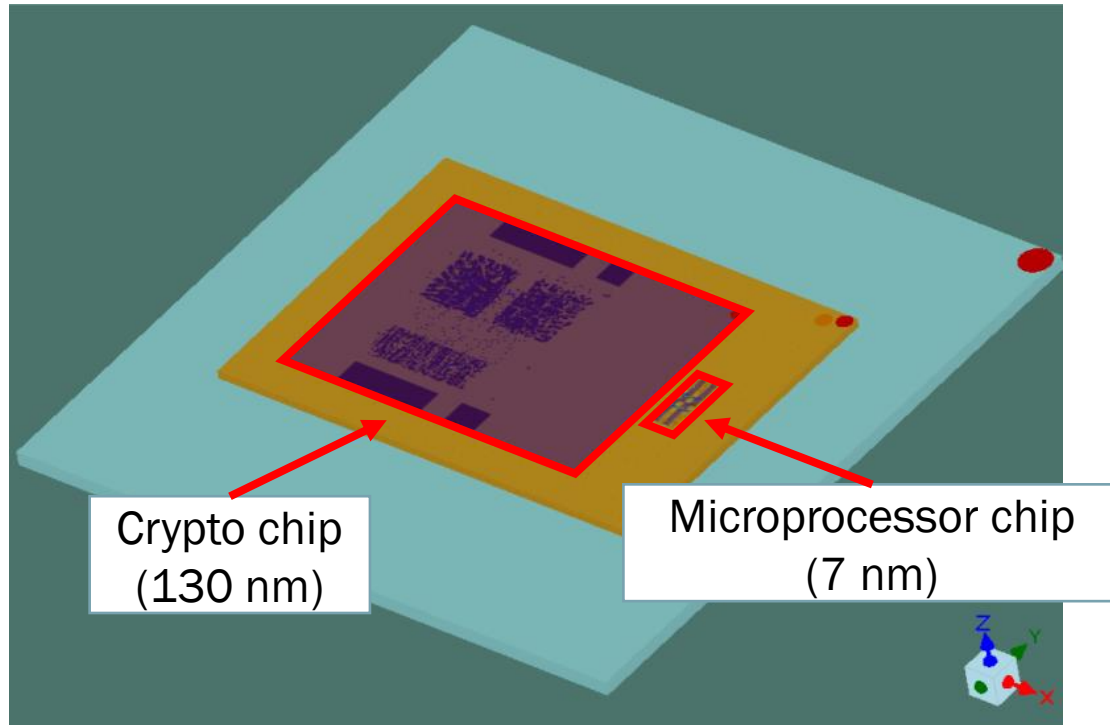


* V_{pp}^* : Voltage of first peak of target round



Multichip side-channel analysis

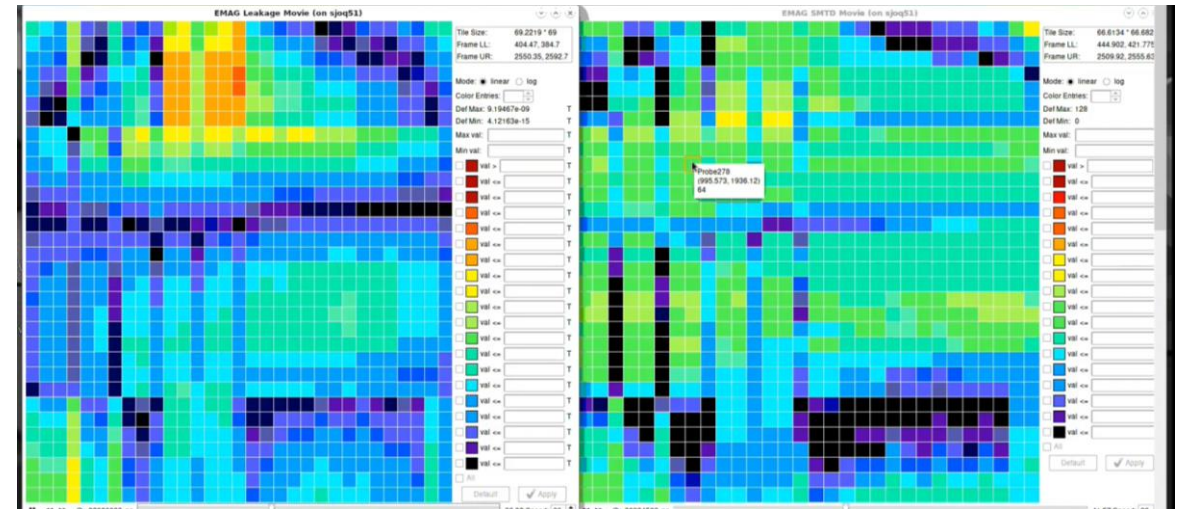
- Modeling of 2.5D IC



<Analysis results of the crypto chip>

EM emission

MTD



Summary

- Si substrate voltage can be the side-channel information
 - Growing threat with the increasing number of flip chip packaging
- Achievements
 - Modeling flow for Si backside side-channel leakage
- Our on-going focus
 - Analysis multichip device using CPM

This work has been partly supported by JSPS KAKENHI Grant No. JP22H04999
and by SECOM Science and Technology Foundation