A Hybrid Simulation Technique for High-Speed and Accurate System-level Side-Channel Leakage Analysis

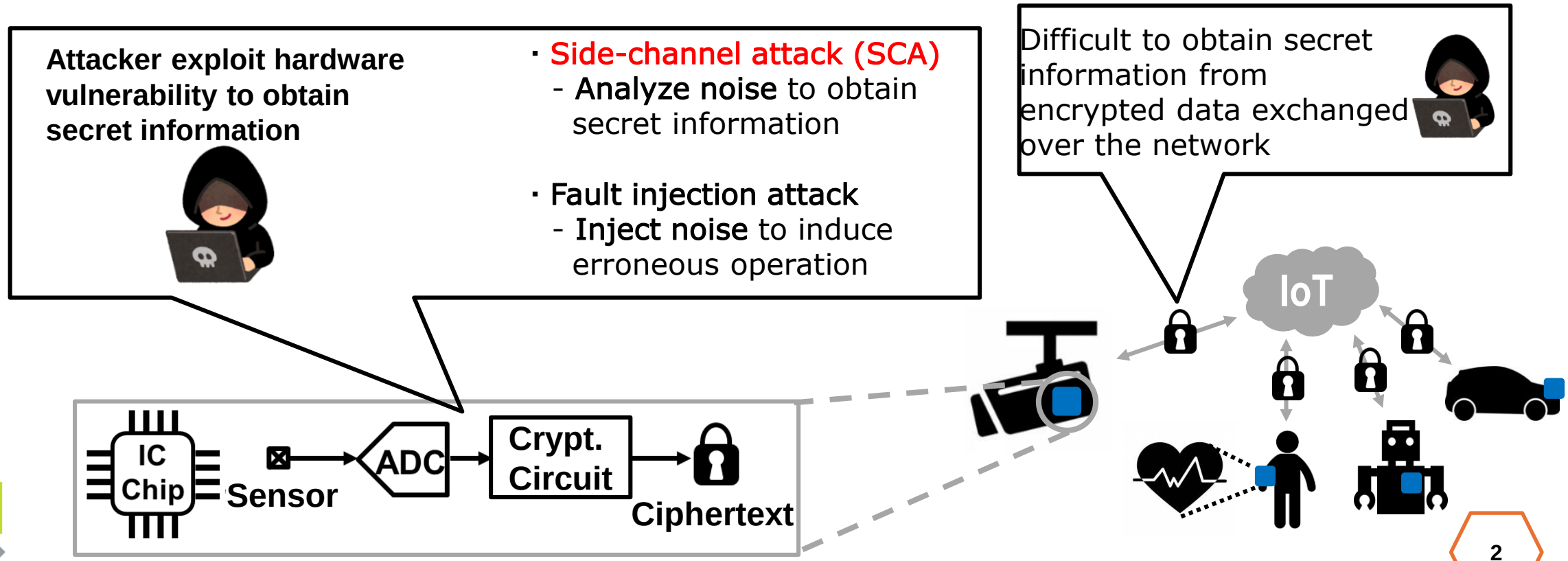
Kazuki Monta[*1,2], Takafumi Oki[*2], Rikuu Hasegawa[*2], Takuya Wadatsumi[*2], Takuji Miki[*2], Makoto Nagata[*2], Lang Lin[*3], Norman Chang[*3]

*1 Secafy Co., Ltd., *2 Kobe University, *3 ANSYS Inc.

SPONSORED BY

Hardware security

- Cryptographic circuits are vulnerable to physical attacks without careful design

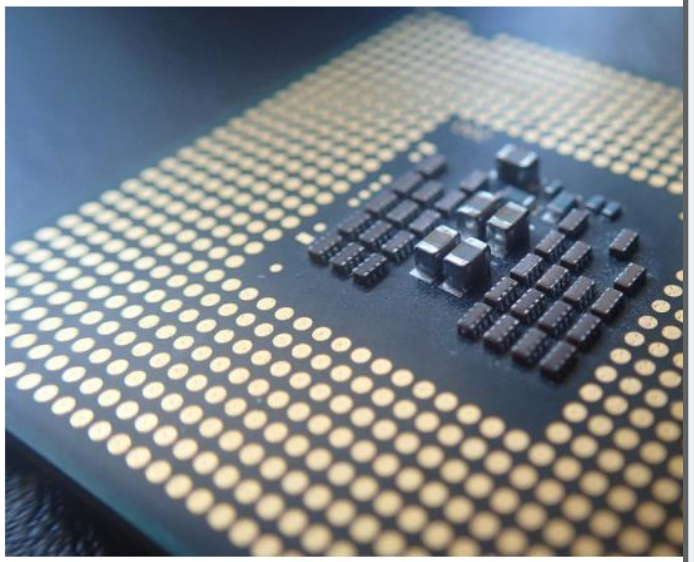


Threat of SCA

Cyber Attack ◇ Cyber Security News ◇ News ◇ Vulnerabilities

Researchers Devise Prefetch Side-Channel Attack Threatening AMD CPUs

written by Abeerah Hashim | October 19, 2021

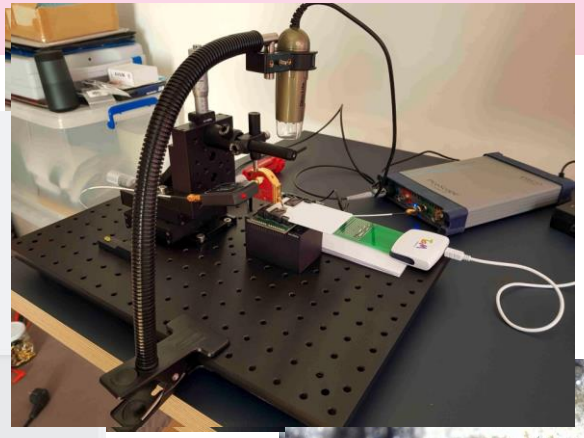


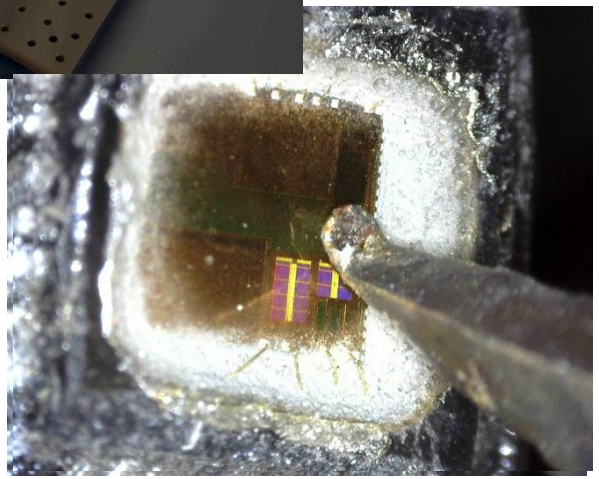
SEND IN THE CLONES —

Hackers can clone Google Titan 2FA keys using a side channel in NXP chips

Yubico and Feitian keys that use the same chip are likely susceptible, too.

DAN GOODIN - 1/8/2021, 9:59 PM





https://latesthackingnews.com/2021/10/19/researchers-devise-prefetch-side-channel-attack-threatening-amd-cpus/

https://arstechnica.com/information-technology/2021/01/hackers-can-clone-google-titan-2fa-keys-using-a-side-channel-in-nxp-chips/

Side-channel(SC) leakage and SNR

- SNR in SC leakage evaluation
  - $P_{total}=P_{exp}+P_{sw.noise}+P_{el.noise}+P_{constant}$
    - P_{exp} : Exploitable noise
    - $P_{sw.noise}$: Switching noise
    - $P_{el.noise}$: Electronic noise(normal distribution)
  - $\mathrm{SNR} = \frac{P_{exp}}{\mathrm{Var}(Psw_{noise}+Pel_{noise})}$
  - SNR & MTD
    - $\mathrm{MTD} \sim \frac{1}{\mathrm{SNR}} = \frac{\mathrm{Var}(Psw_{noise}+Pel_{noise})}{P_{exp}}$

- Two Countermeasure Strategies
  - Reduce the 'S' in SNR
  - Increase the 'N' in SNR

SC leakage countermeasure

- Hiding
  - Conceals Correlation between secret information and noise
    - By lowering “S” or increasing “N” to reduce SNR
  - Decrease the Signal-to-Noise ratio (SNR)

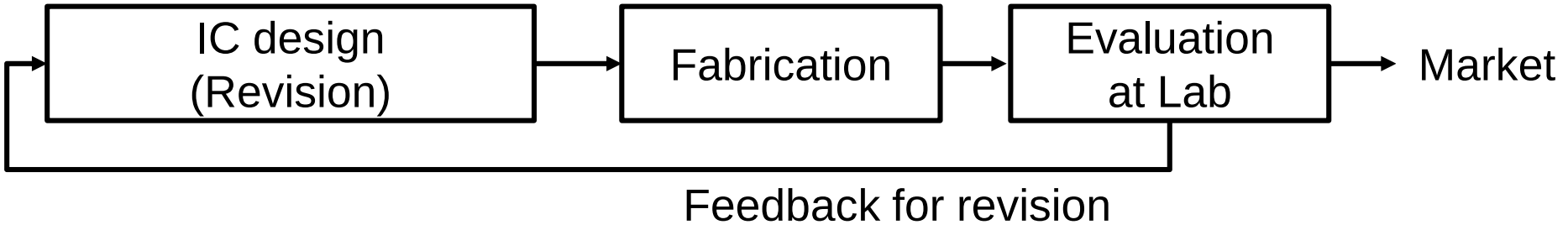
- Masking
  - Reducing Correlation between secret information and noise using random numbers (lowering or removing “S” to reduce SNR)
  - Implemented at the architecture level

SCA tolerance evaluation of ASIC chip

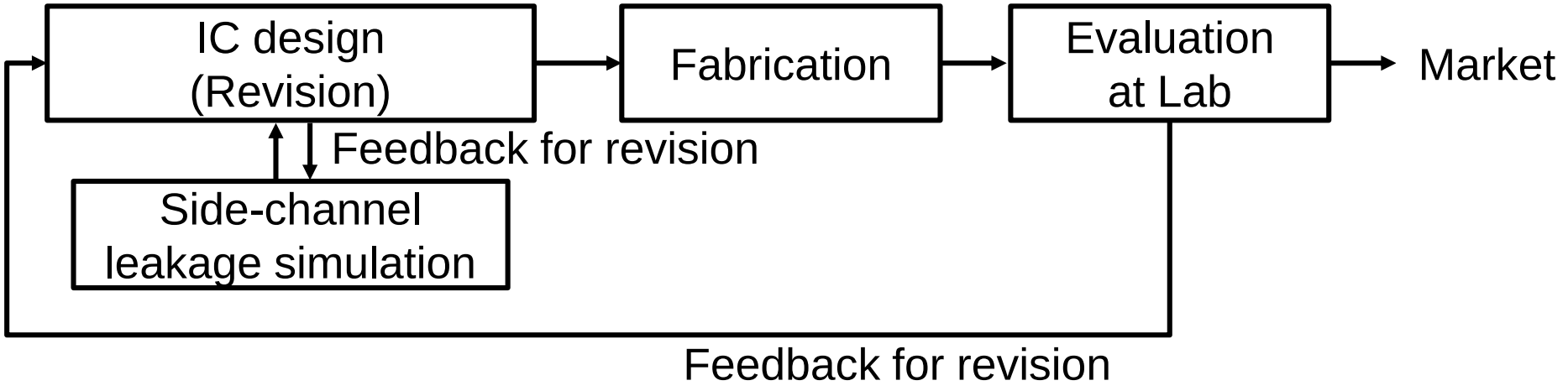
- Prototype chip
  - Expensive, Time consuming
- FPGA
  - Different from ASIC
- Simulation
  - Evaluate just after the design
  - Explore vulnerable point inside the IC chip

Design flow with SCA simulation

- Verification at design stage
  → Immediate revision
  - Without SCA simulation



  - With SCA simulation



Two types of SCA simulation

- Logic-based simulation
  - Very fast
  - RTL netlist / Post-synthesis netlist / Post-layout netlist
  - Low accuracy
- Transistor level simulation
  - High accuracy
  - Post-synthesis netlist / Post-layout netlist
  - More computation time

Trade-off between simulation accuracy and simulation efficiency

Problem in evaluation of masking/hiding countermeasure

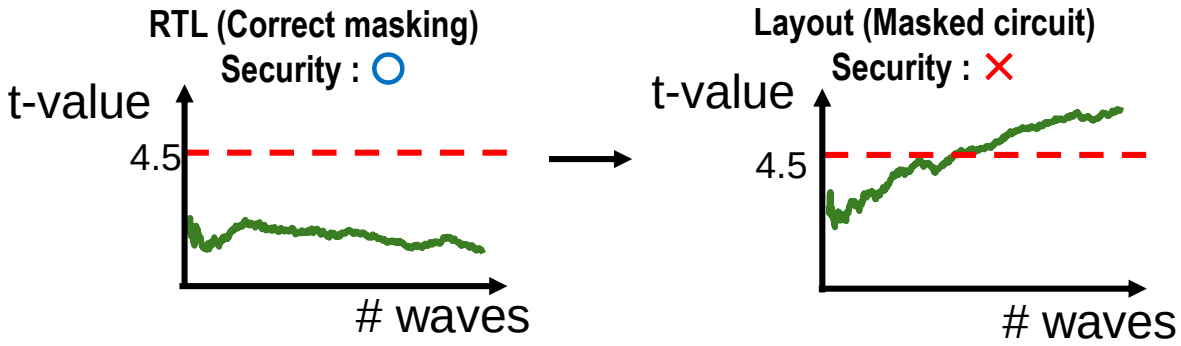
Simulation of Hiding

- Hiding is highly depend on the SNR
  - Accurate estimation of the noise in the target of evaluation
    - Small difference in timing or circuit size may cause leakage
  - Estimating the system-level noise across the entire chip

Accurate and efficient simulation technique
that can handle the system-level SNR is needed

Simulation of Masking

- Masking (DOM , TI)
  - Provable security
    - Assumption: Leakage is independent
    - Implementation violates security of masking [*1,*2,*3] [*1] COSADE 2017, [*2] DATE 2020, [*3] TCHES 2019
      - Placement proximity and the on-chip/off-chip Power Delivery Network (PDN) might cause nonlinear coupling
    - Sufficient noise is important for a secure masking
  - System-level PDN and system-level SNR are essential



Accurate and efficient simulation technique that can handle the system-level PDN and system-level SNR is needed

A Hybrid Simulation Approach for System-level SC Leakage Evaluation

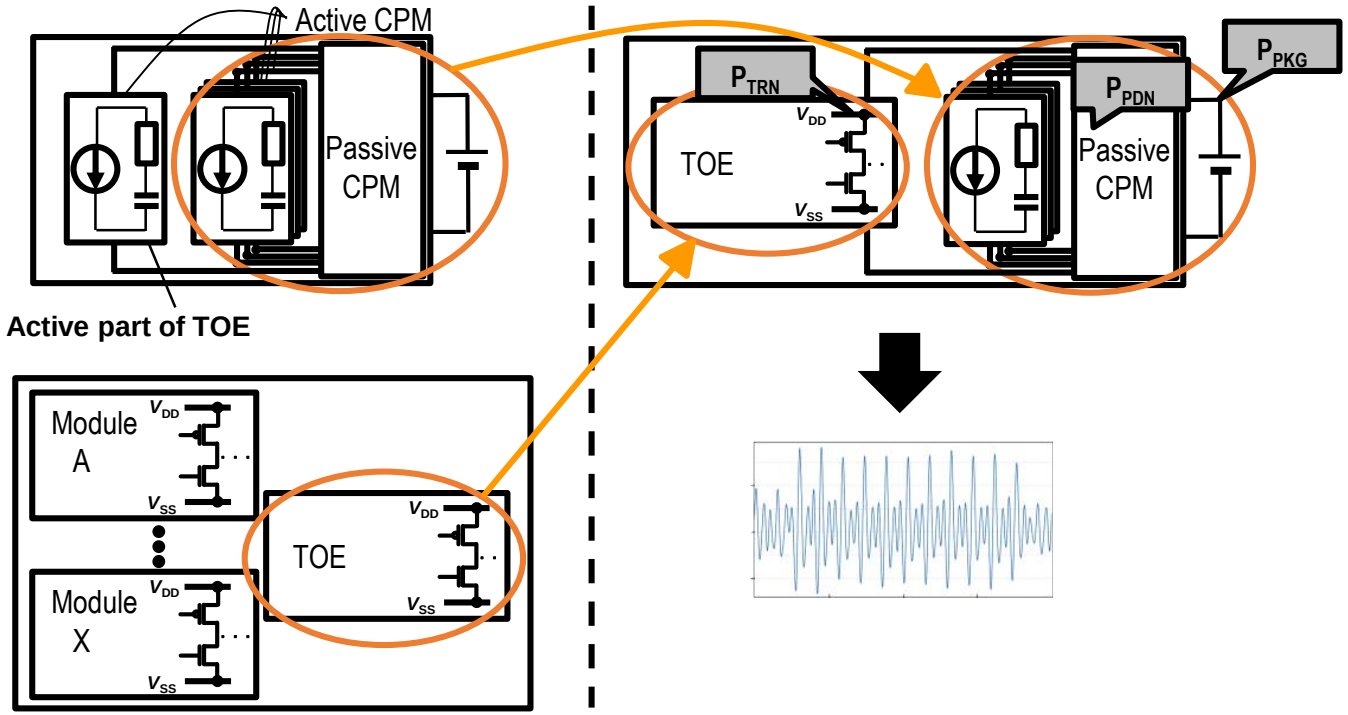
- Novel hybrid simulation approach
  - Combines transistor-level power estimation for critical circuits (target of evaluation, TOE) and fast logic based simulation for system-level PDN and SNR analysisFaster than transistor level simulation

Chip power model (CPM) of the whole chip (.sp)

- **Passive CPM: System level PDN**
- **Active CPM:**
  Power consumption model (Logic based power noise estimation)
- **Using Non-TOE Parts**

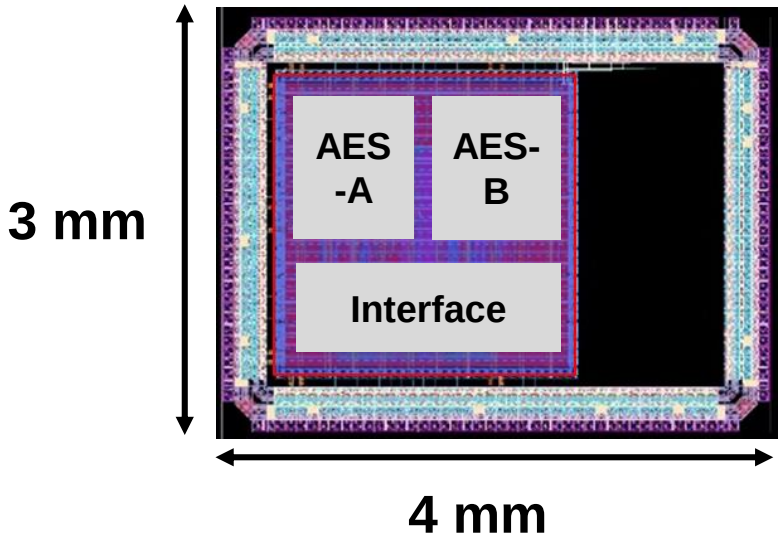
SPICE netlist of the whole chip (.sp)

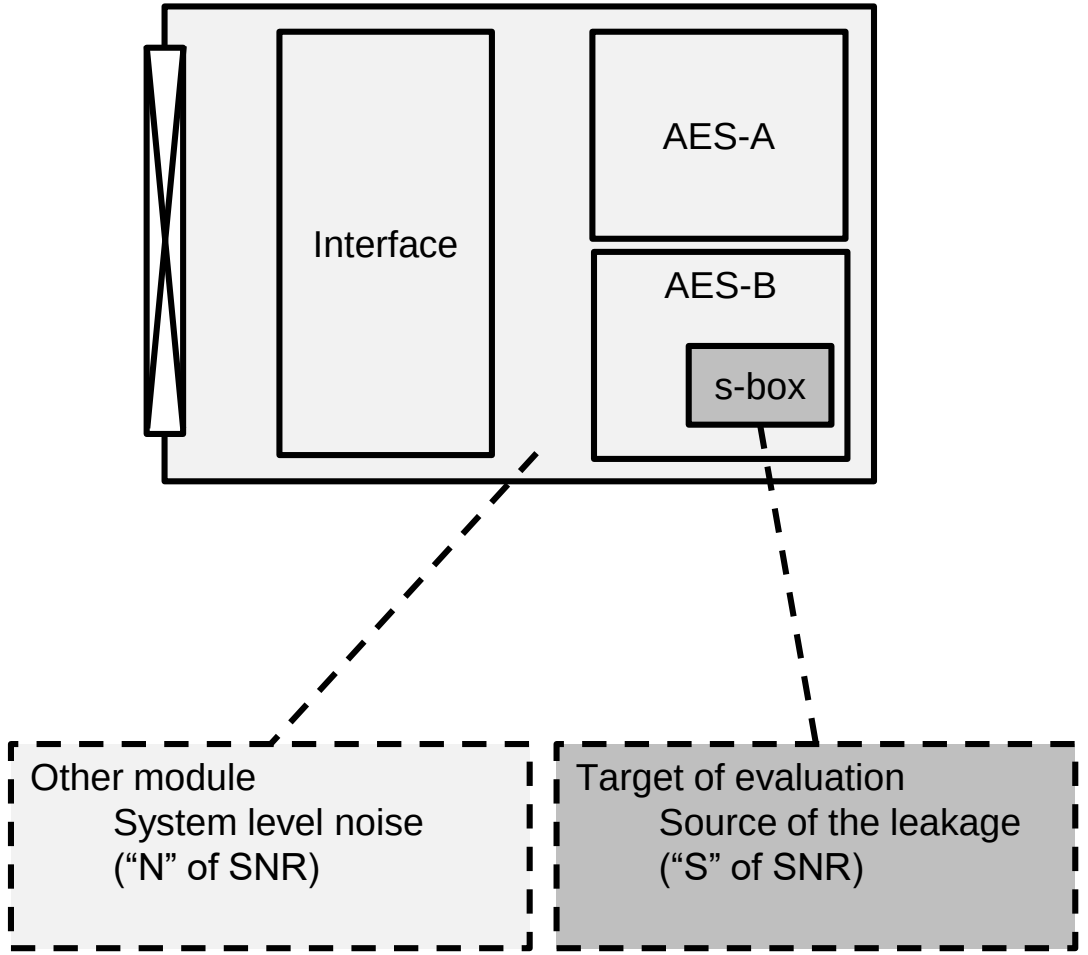
- **Using only TOE part**



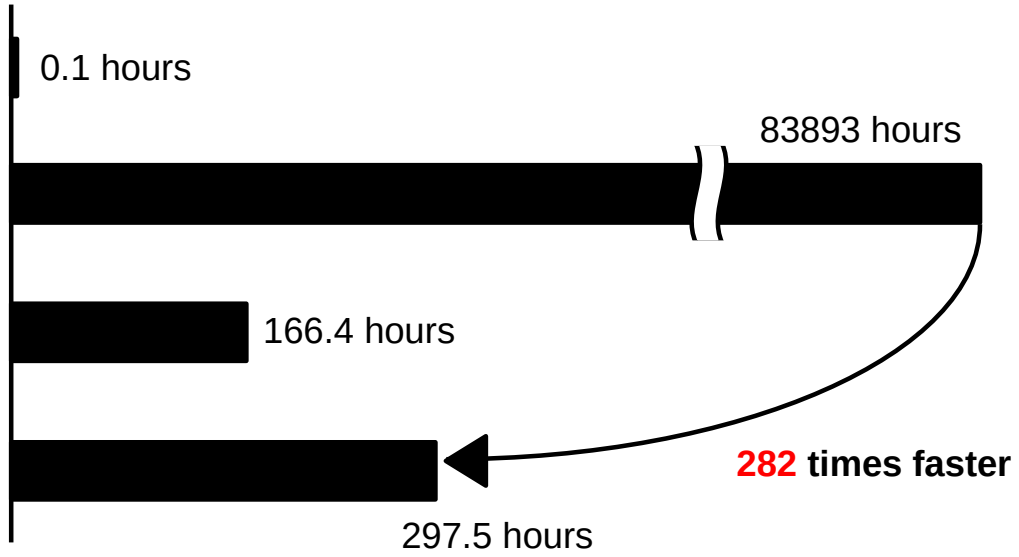
Evaluation target

- CMOS process 4mm×3mm
- 2 cores of 128bit-AES
- TOE is s-box in AES-B

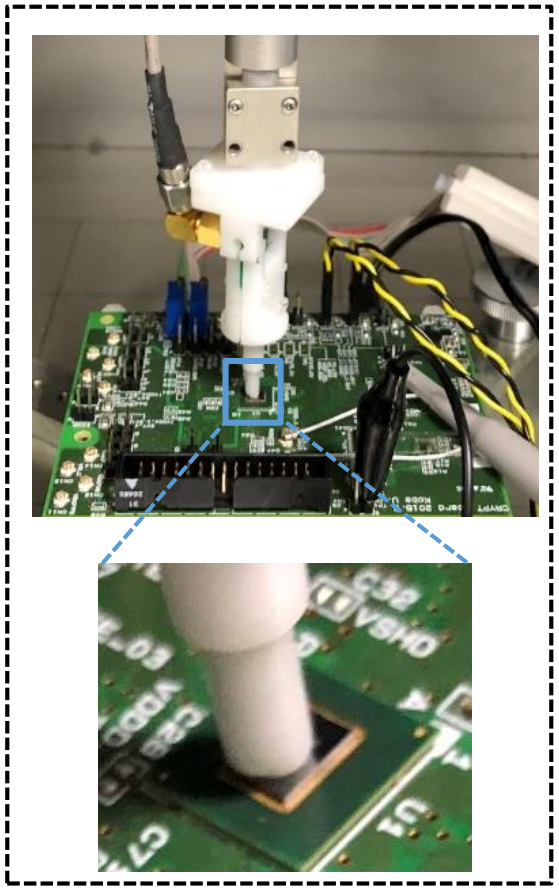


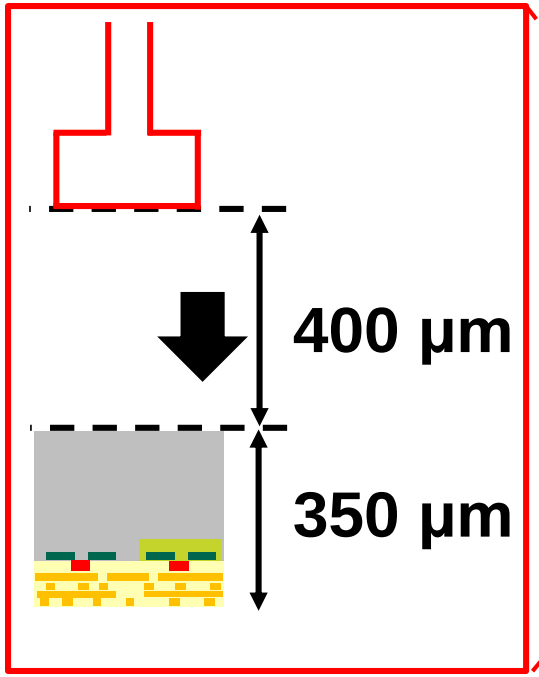


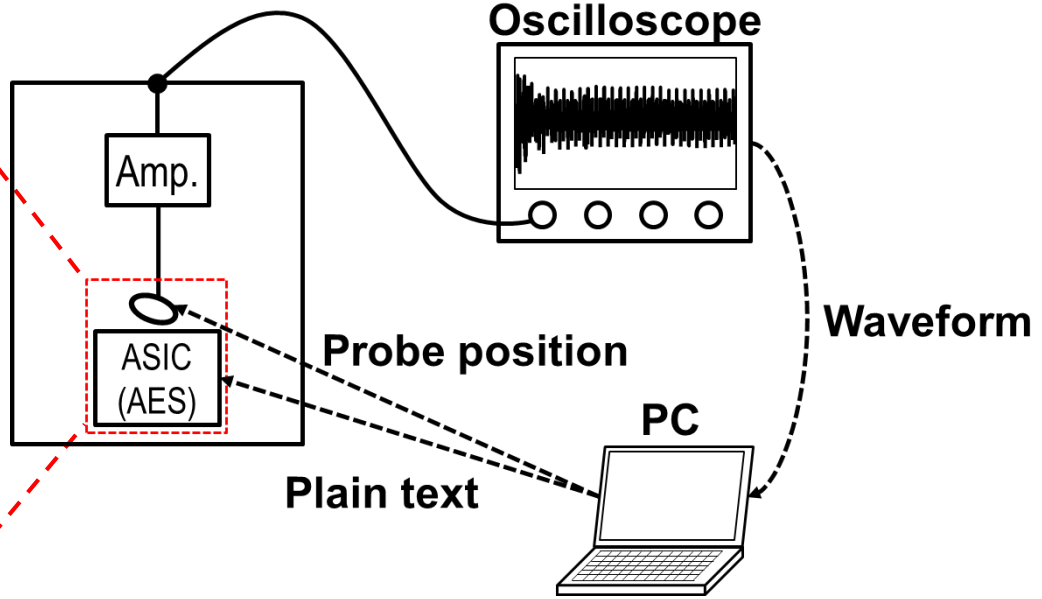
Comparison between the proposed approach and traditional approaches

	Simulation CPU time for 1000 traces	Detailed and accurate analysis of the target core	System/IC-chip level PDN and SNR
Core level SPICE simulation (Target: s-box 220GE)		○	×
Chip level SPICE simulation (Estimated) (Target: Chiptop 70K GE)		○	○
Chip level simulation using standard-cell power consumption models (Target: Chiptop 70K GE)		×	○
Proposed hybrid approach (Target: Chiptop 70K GE)		○	○

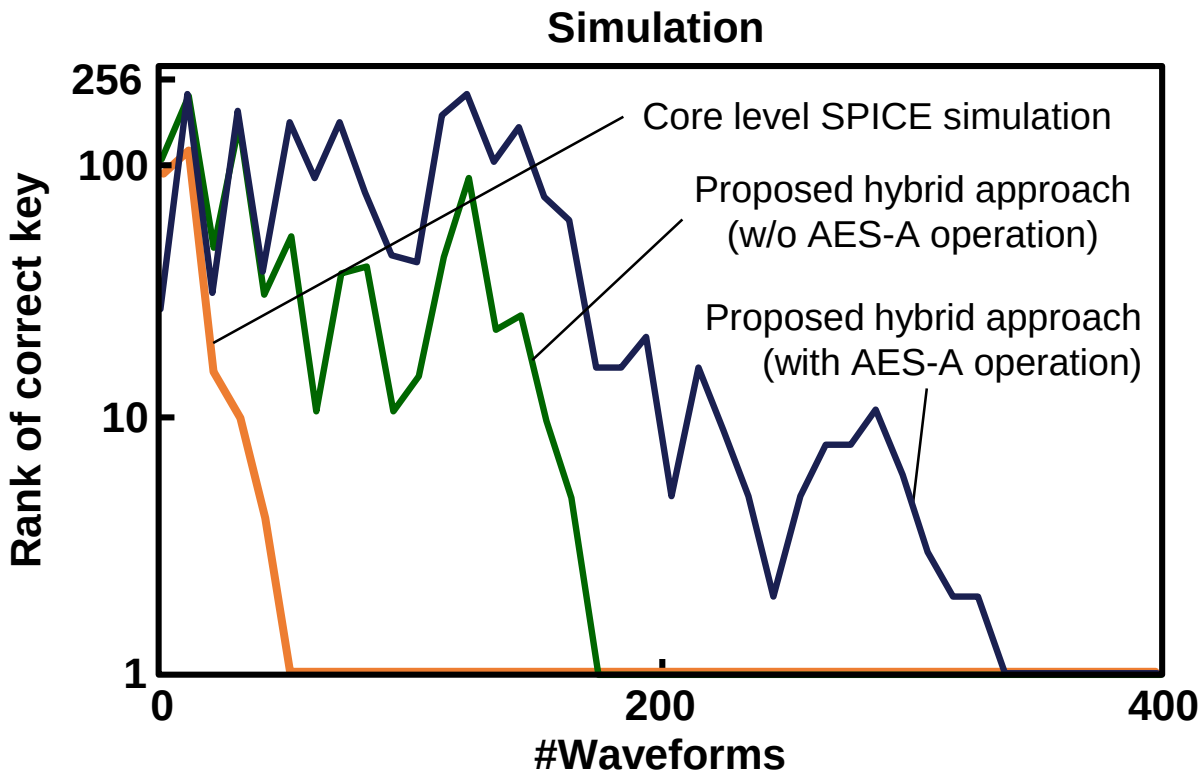
Measurement setup

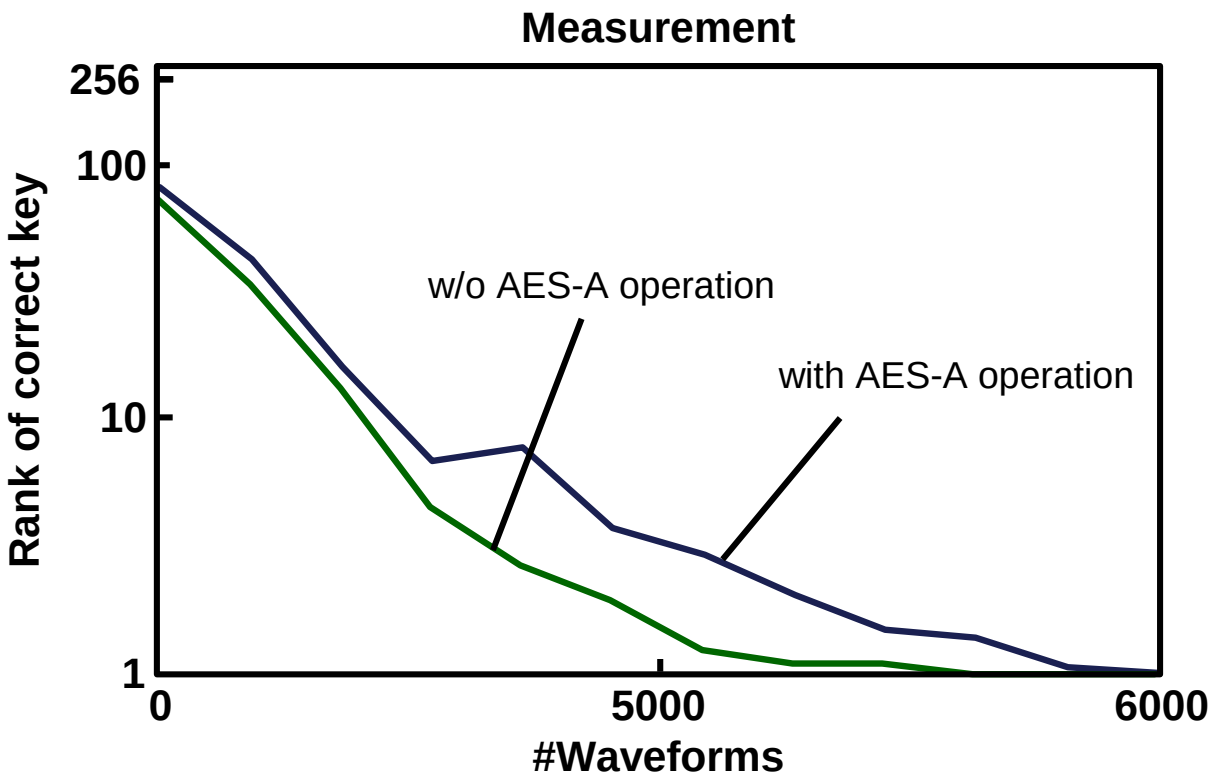






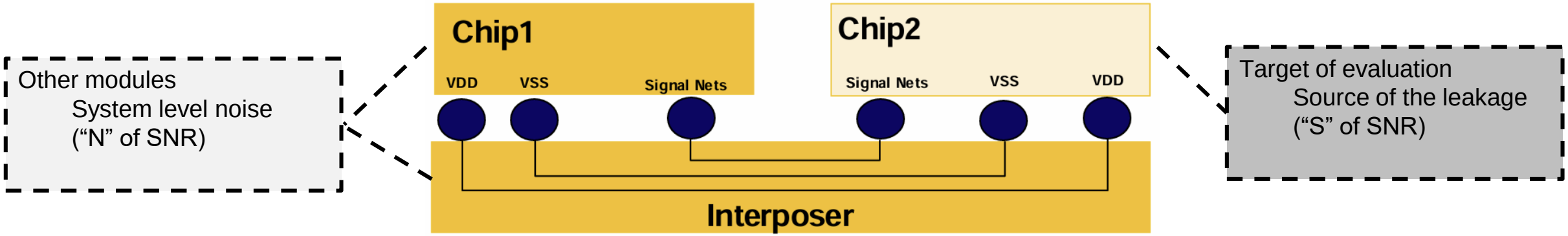
SC leakage evaluation result





Multi-chip simulation overview

- Hybrid simulation approach for 2.5D/3D packaging



- Chip 1: CPM
- Interposer: CPM
- Chip 2: Transistor level simulation /
  Layout-aware logic-based simulation

Conclusion

- Hybrid simulation approach for accurate and fast system-level side-channel leakage evaluation
  - Combines transistor-level power estimation for critical circuits and system-level PDN and SNR analysis
  - 282x higher efficiency compared to full-chip transistor-level simulation
- This simulation may provide insights into security order degradation in masking schemes