The University of Texas at Austin
Chandra Department of Electrical and Computer Engineering
Cockrell School of Engineering

TECHNISCHE UNIVERSITÄT BERLIN

International Symposium on Physical Design
sigda

PHOTONIC SIDE-CHANNEL ANALYZER: ENABLING SECURITY-AWARE PHYSICAL DESIGN METHODOLOGY

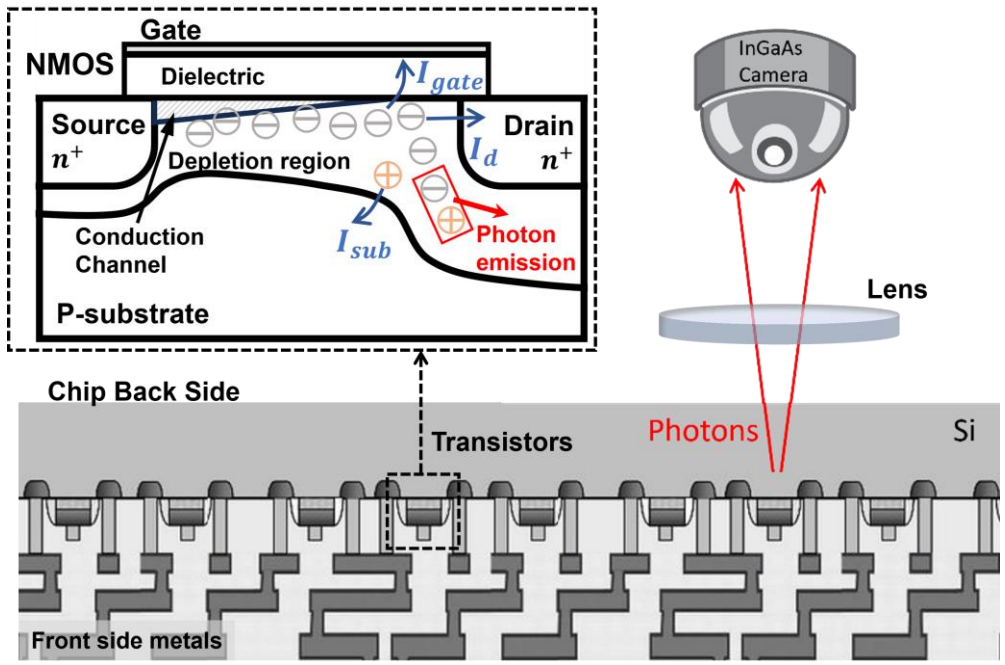
Meizhi Wang[1]*, Yi-Ru Chen[1], S. S. Teja Nibhanupudi[1], Elham Amini[2], Antonio Saaverdra[2], Yinan Wang[1], Daniel Wasserman[1], Jean-Pierre Seifert[23] and Jaydeep Kulkarni[1#]

[1]The University of Texas at Austin, Texas, USA
[2]Technische Universität Berlin, Berlin, Germany
[3]Fraunhofer SIT, Darmstadt, Germany
*wang.mz@utexas.edu; #jaydeep@austin.utexas.edu

Outline

- Introduction:
  - Photon emission (PE) as a side-channel threat
- Photonic Side-Channel Simulation Framework:
  - Standard-cell PE library generation
  - Circuit level PE Heatmap generation
  - PE side-channel analysis
- Measurement & Comparison:
  - Validating simulated PE heatmaps against real chip measurements
- Conclusion

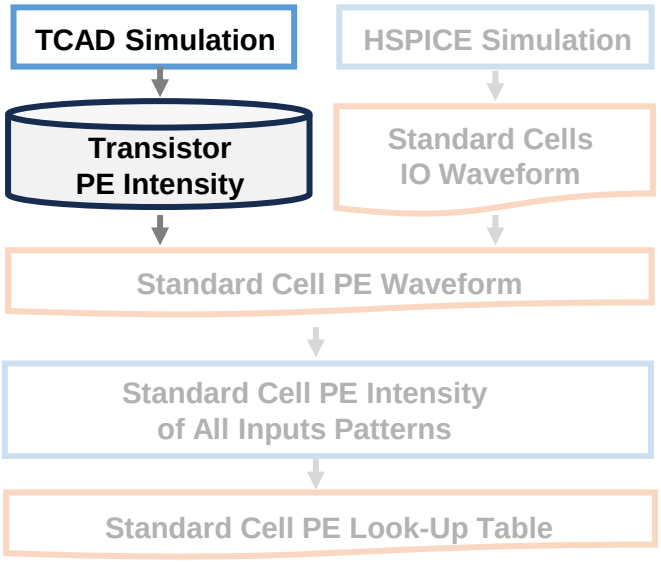
Introduction

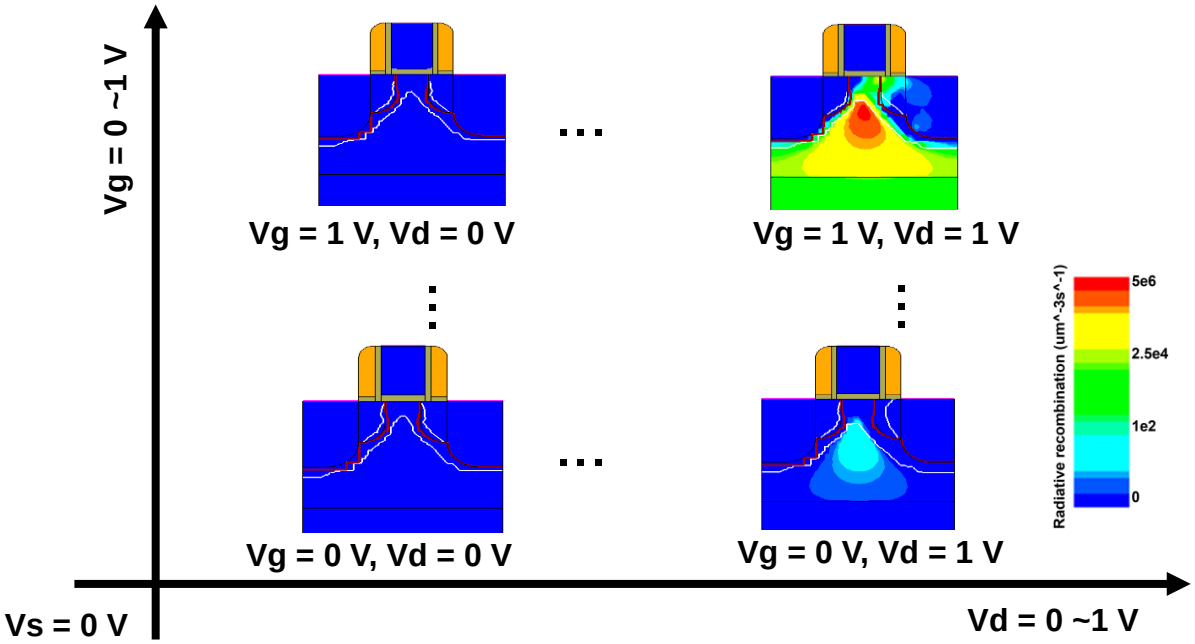


Photon Emission in Integrated Circuit

- Occurs during transistors switching due to electron-hole recombination at the drain region.
- Emits some energy as photons through radiative recombination.
- Passes through the silicon substrate and is captured by a measurement lens.
- Peaks in the saturation region, with intensity correlating to switching activity, making it a potential side-channel leakage source.
- Requires pre-silicon security analysis to mitigate leakage risks early in the design process.

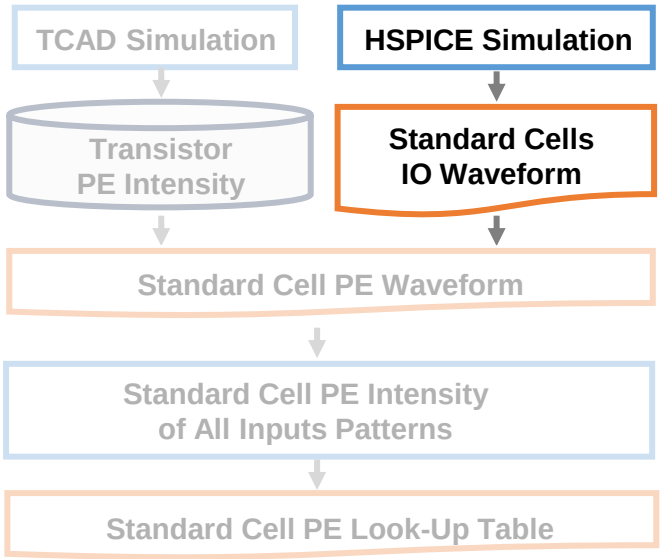
TCAD Simulation

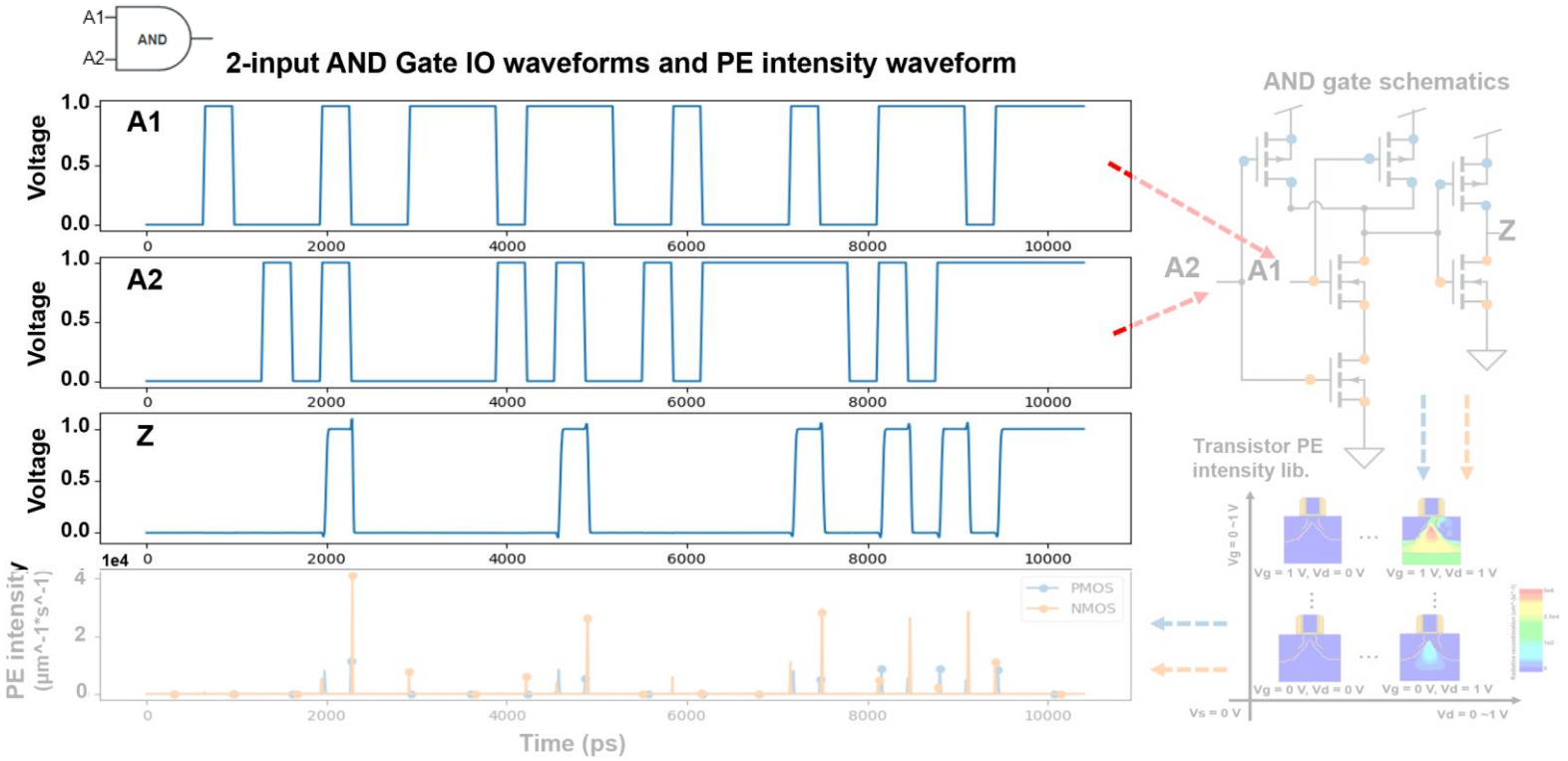




- Develop a Technology Computer-Aided Design (TCAD) model for a representative 40nm P-MOSFET and N-MOSFET.
- Simulate radiative recombination of electron-hole pairs under varying device biasing conditions.
- Generate a PE look-up table using the average radiative recombination (RR) rate, mapped to device biasing parameters.

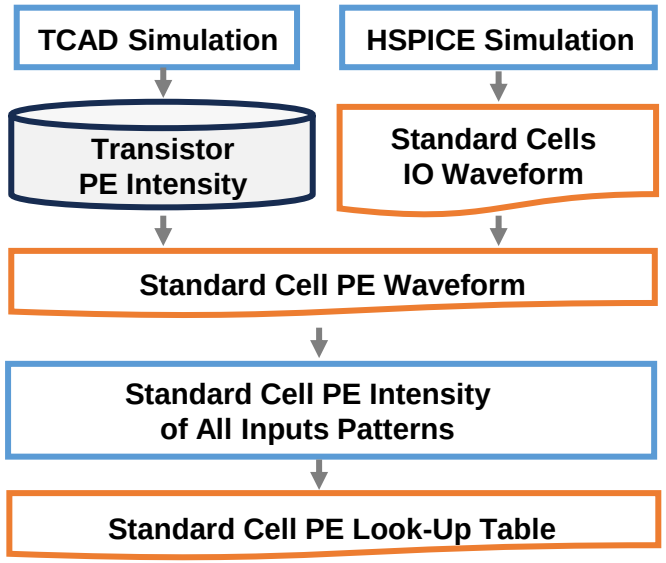
HSPICE Simulation

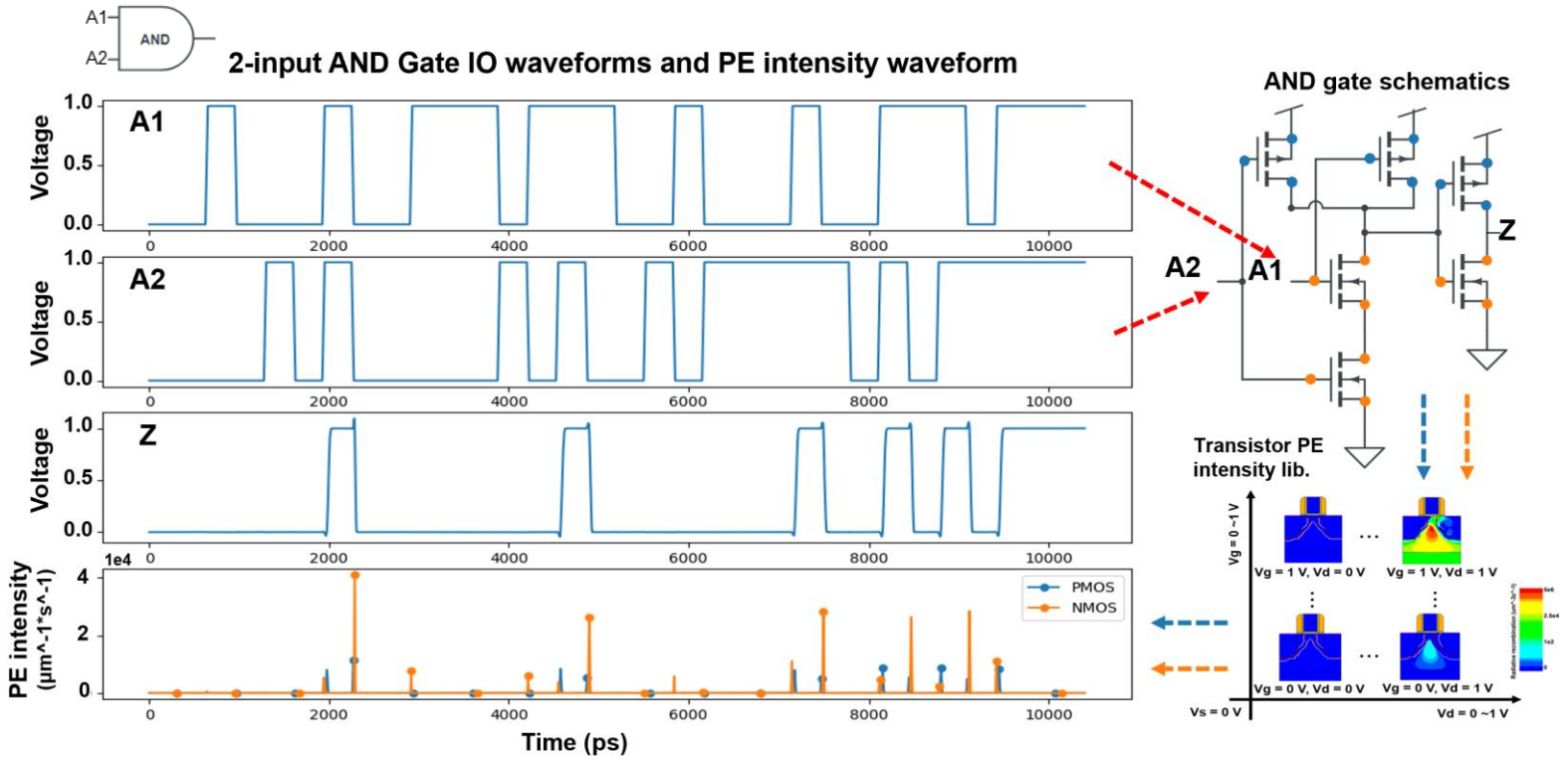




- Generate all possible input transition vectors for standard cells.
- Simulate all input transitions using HSPICE to analyze switching behavior.

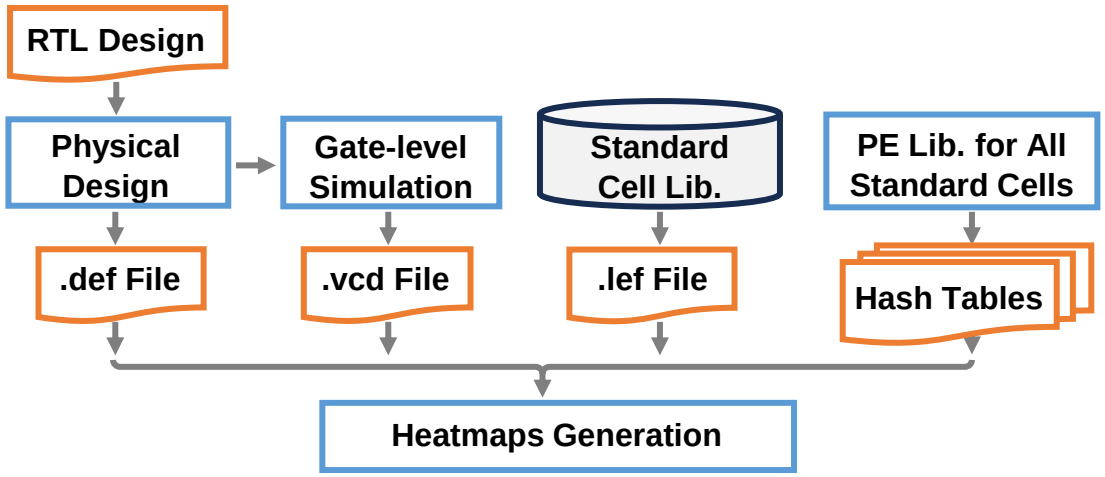
Standard Cell PE Look-Up Table

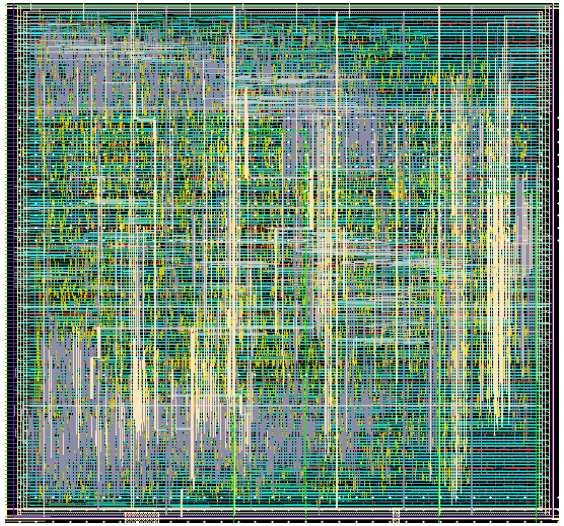


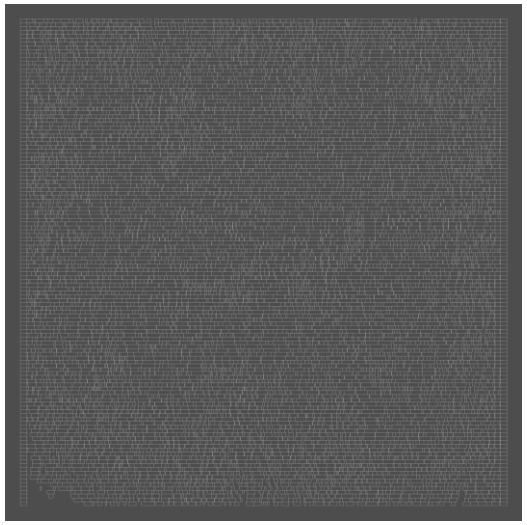


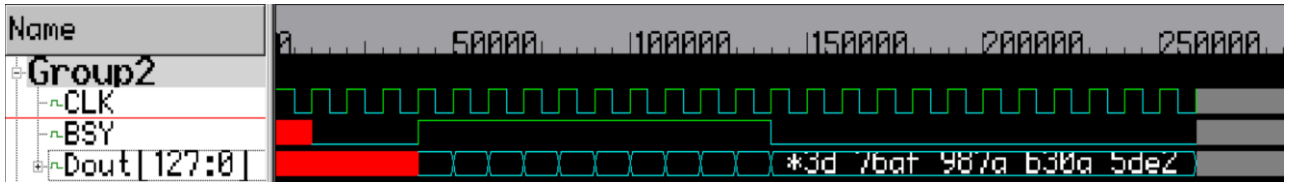
- Reference TCAD results to determine photon emission intensity for all input transition vectors.
- Construct a hash table for each standard cell, mapping NMOS and PMOS emission intensity to corresponding input transitions.
- Form the Standard Cell PE Library, where the hash table enables fast lookup of emission intensities during circuit-level analysis.

PE Heatmap Generation



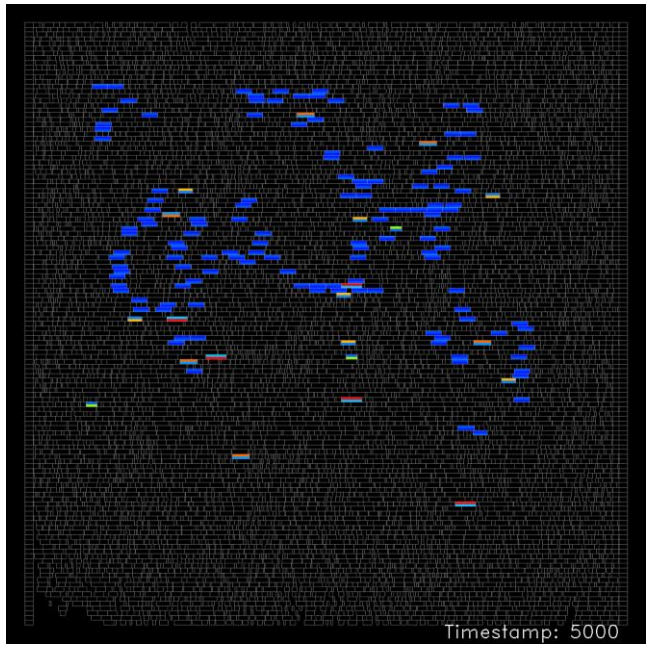






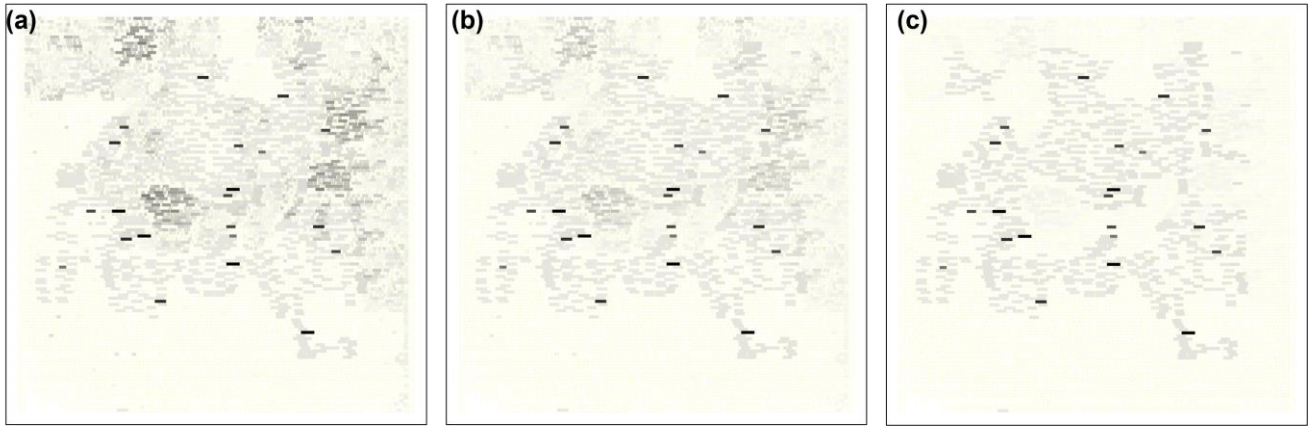
- Extract circuit information (die dimensions, standard cell attributes) from library files.
- Track input vector transitions for all standard cells during post-layout simulation.
- Generate photonic heatmaps by referencing the Standard Cell PE Library to assign emission intensities over time.

Simulated PE Heatmap



Time-Resolved PE Heatmap

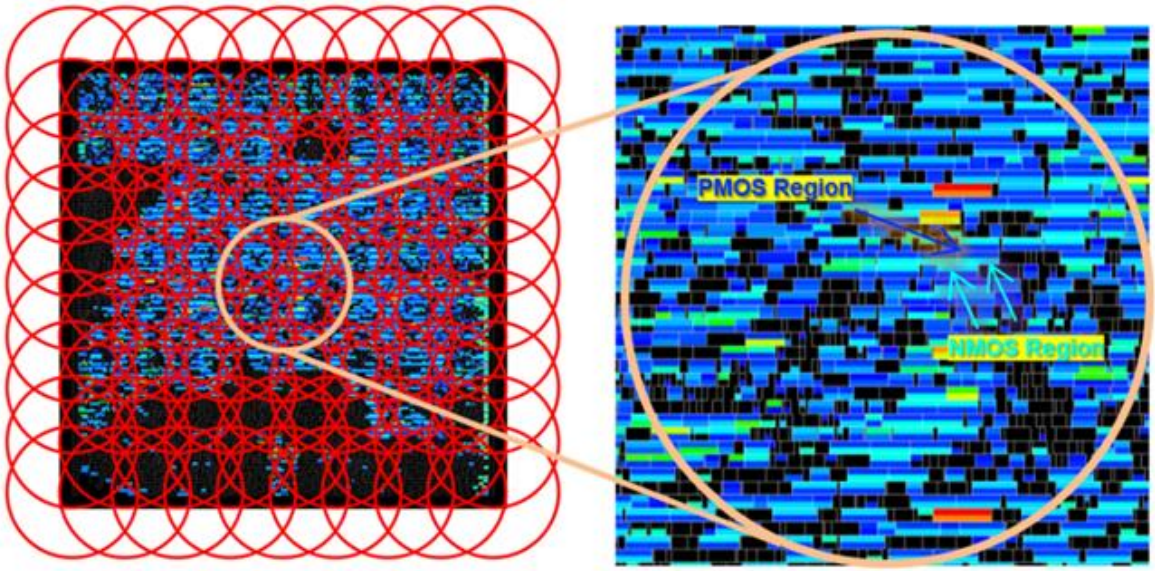
- Captured PE variations across different clock cycles during AES encryption, providing spatial and temporal insights.

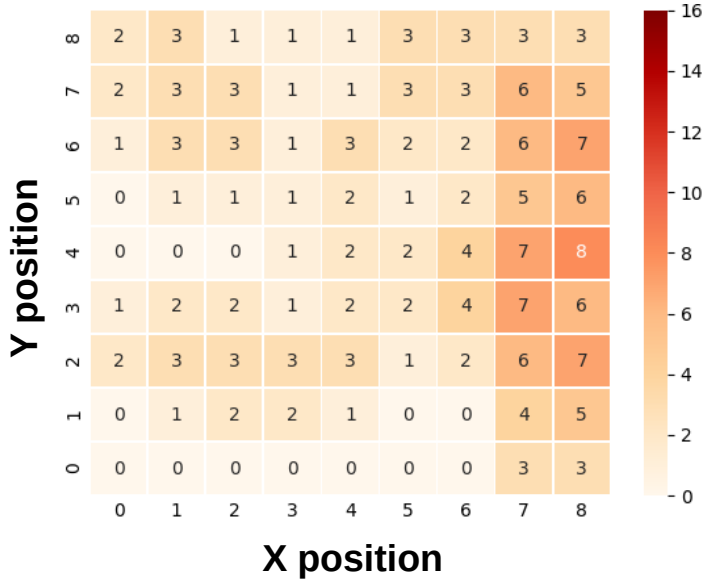


Time-Accumulated PE Heatmap

- Shows PE emissions over extended operation times (15, 25, 150 ms), where a few cells begin to dominate.
- As accumulation increases, emission details in less active regions are lost, with darker areas indicating higher PE intensity.

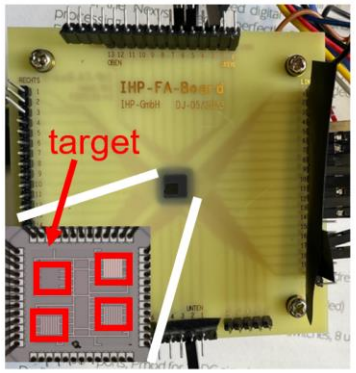
PE Side-Channel Analysis



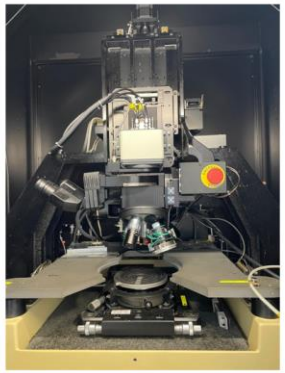


- Overlay probing grid on the AES core to analyze photon emission distribution.
- Aggregate PE values from all standard cells within each probing area.
- Calculate PE intensity at each location and run a side-channel attack to analyze leakage.
- Mitigate leakage by redesigning the most vulnerable areas to enhance security.

Measurement & Comparison

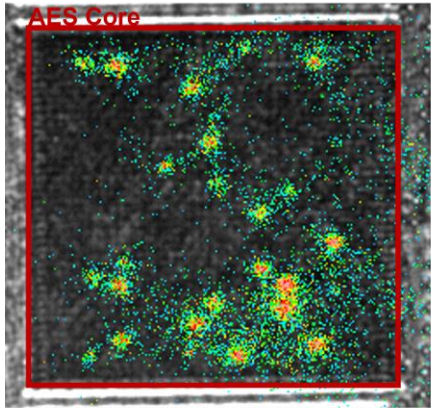


(a) Testchip

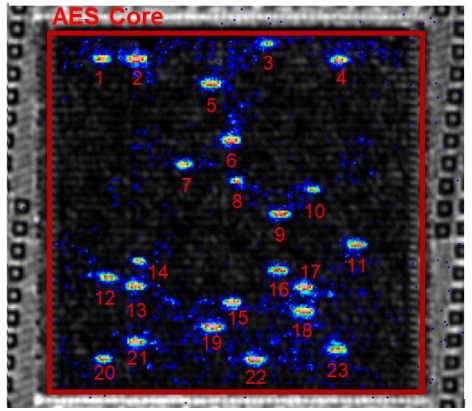


(b) Microscopy

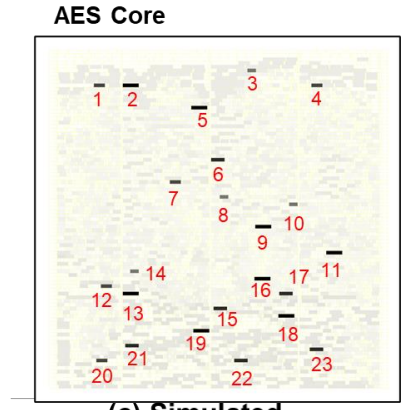
(c) Hamamatsu PHEMOS 1000



(a) Measured PE at 60s



(b) Measured PE at 300s



(c) Simulated accumulated PE map

- The PE intensity of the AES core is measured using a Microscopy System equipped with an InGaAs camera inside the Hamamatsu PHEMOS-100.

- Repeat encryption operations and measure PE for 60s and 300s.
- 60s Measurement: High noise, making emission details harder to distinguish.
- 300s Measurement: More stable, showing strong hotspot consistency with the simulated PE map but losing finer details over time.

Conclusion

- Developed an analysis framework to assess PE vulnerabilities in digital ASIC circuits during pre-silicon design.
- Simulated time-resolved PE maps for a 128-bit AES core and conducted localized CPEA analysis, showing that finer attack granularity increases leakage risks.
- Validated framework accuracy by comparing simulated and measured PE maps on a 40nm chip, confirming its reliability for security evaluations.
- Enables early identification of vulnerable regions and facilitates mitigation strategies to reduce side-channel leakage.
- Enhances security-aware design by integrating side-channel analysis into the design phase, improving circuit security and reliability.

Acknowledgement

- This research is supported in part by Intel Resilient Architectures and Robust Electronics (RARE) security research center, Silicon Labs, and the German Research Foundation (DFG) Priority Program SPP 2253 Nano Security for the projects "NanoE-beam" and "OnESecure".

- The authors would like to thank Dr. Norbert Herfurth from Innovations for High Performance Microelectronics (IHP), Germany, for preparing the adapter board.

The University of Texas at Austin

Chandra Department of Electrical and Computer Engineering

Cockrell School of Engineering