



SHAPING THE NEXT GENERATION OF ELECTRONICS

JUNE 23-27, 2024

MOSCONE WEST CENTER
SAN FRANCISCO, CA, USA



Pre-Silicon Photon Emission Modeling and Optical Side-Channel Simulation

Henian Li¹, Lang Lin², Norman Chang², Sreeja Chowdhury²,
Kazuki Monta³, Makoto Nagata³, Mark Tehranipoor¹

¹University of Florida, USA

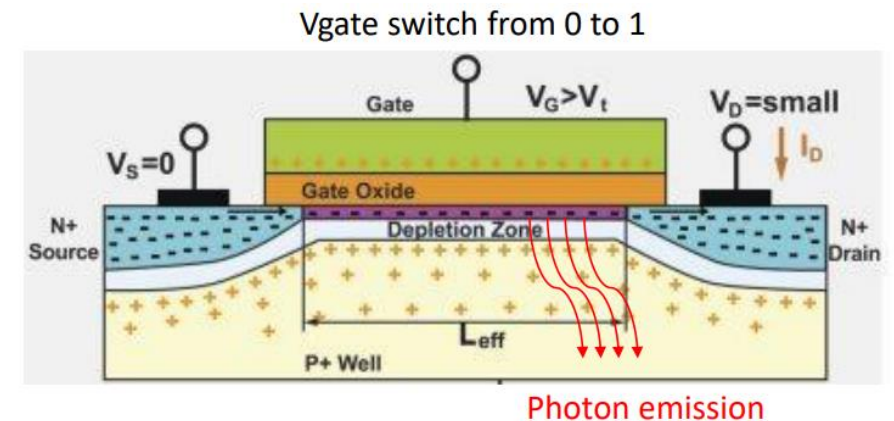
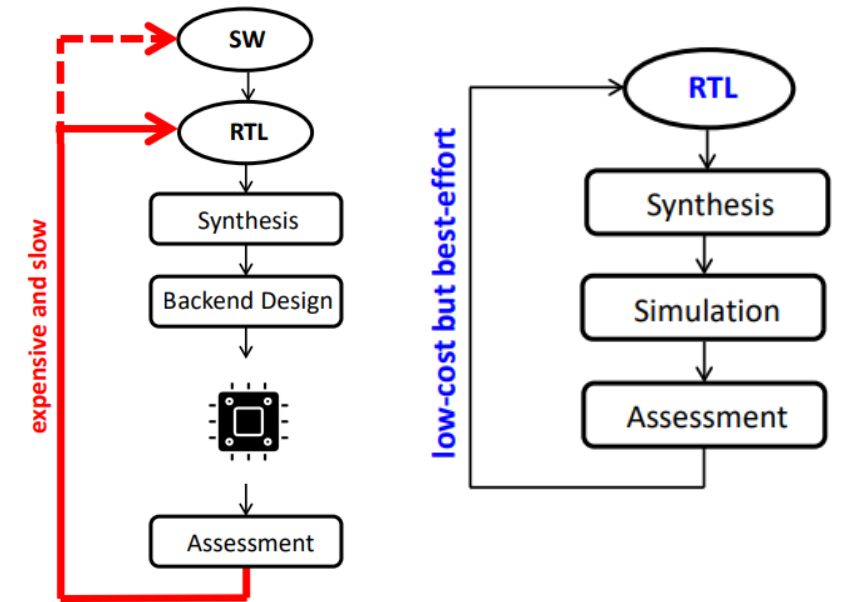
²Ansys, Inc.,

³Kobe University, Japan



Motivation of Pre-Silicon Side-Channel Analysis

- Currently side-channel validation is conducted post-silicon in security labs
 - Too primitive for basic testing, and expensive/slow process for high security critical applications
 - Information leakage mechanism is a black box for chip designers
 - Too late to make design changes after silicon is found leaky
- Pre-silicon assessments
 - Use modeling and simulation to estimate implementation properties
 - Design-time mitigations
 - Enable adding security as a fourth constraint to go with PPA
- Device photon emissions
 - NMOS channel current is the dominant source
 - Can be captured by NIR cameras, leaking the device activities



Pre-Silicon Optical Side-Channel Simulation Flow

- **Simulation**

- Transistor-level dynamic IR drop simulated at the layout level across NMOS (Totem-SC)

- **Modeling**

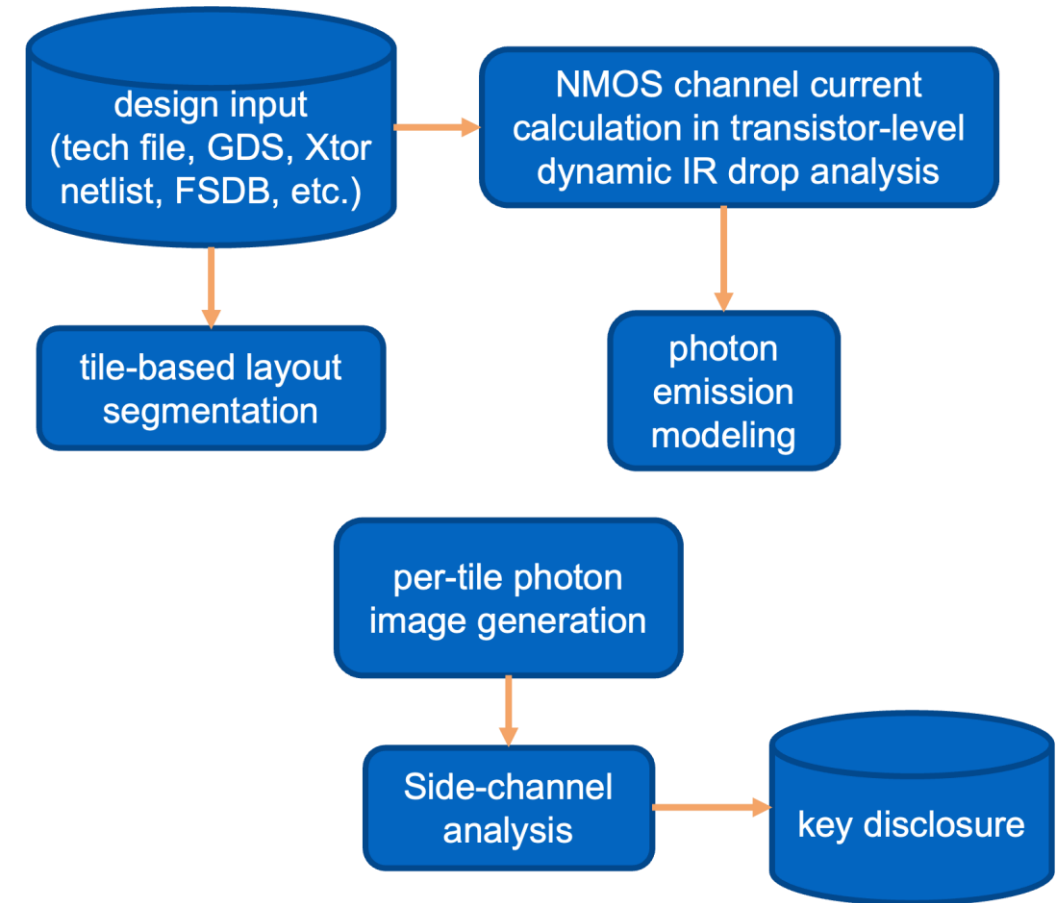
- Multiphysics modeling for building the connection between simulated NMOS channel current photon emissions

- **Analysis**

- Attack scenario-based tile arrangement
- Side-channel analysis based on custom leakage model and attack scenario (Redhawk-SC Security)

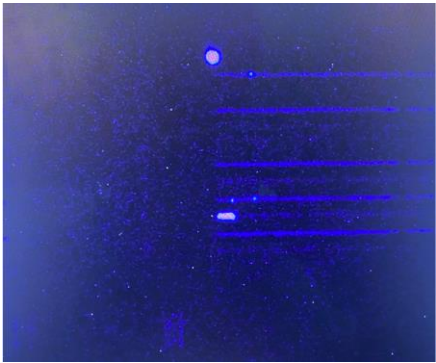
- **ML acceleration**

- Predict fine-grained tiles' leakage based on coarse-grained training to accelerate the flow
- Traces prediction to reduce the MTD

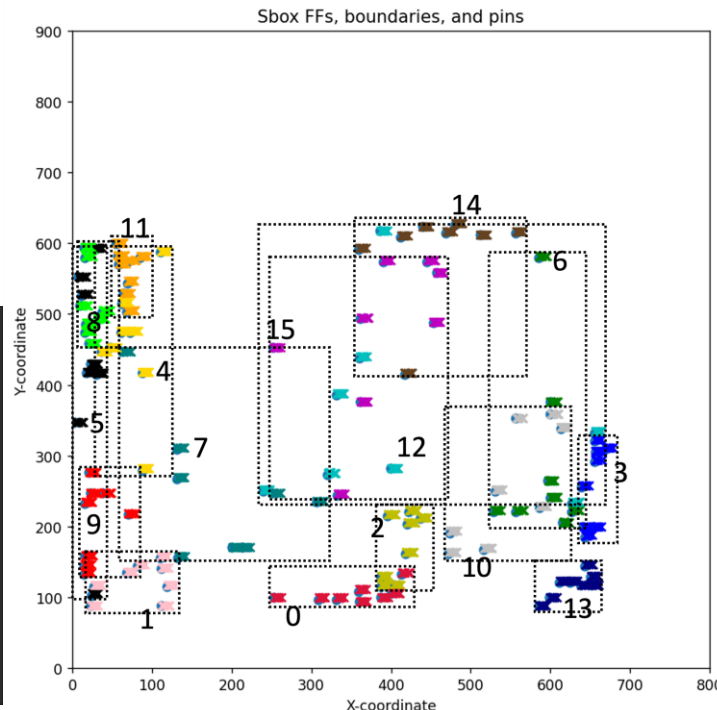


Main Values and Findings

- Transistor-level dynamic IR drop simulated at the layout level for photon emission calculation
 - Modeling based on the theory of hot carrier scattering in the conduction band due to bremsstrahlung (braking radiation)
 - Simulated photon emission images
- Pre-silicon optical side-channel analysis flow
- Two attack scenarios considered
 - White/grey box: emission intensities are spatially integrated within each byte bound
 - Black box: intensities are spatially integrated within each tile, which is from evenly segmenting the layout



Short-time-integrated
photon emission vs.
simulated emission
image

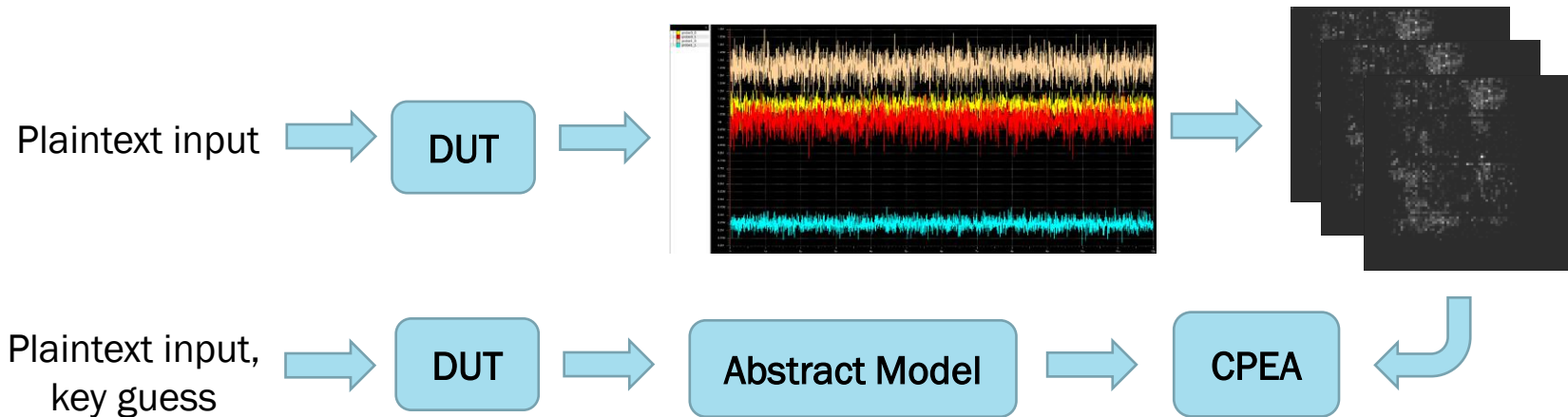


Besides regular leakages, **out-of-model leakage due to current coupling is observed**

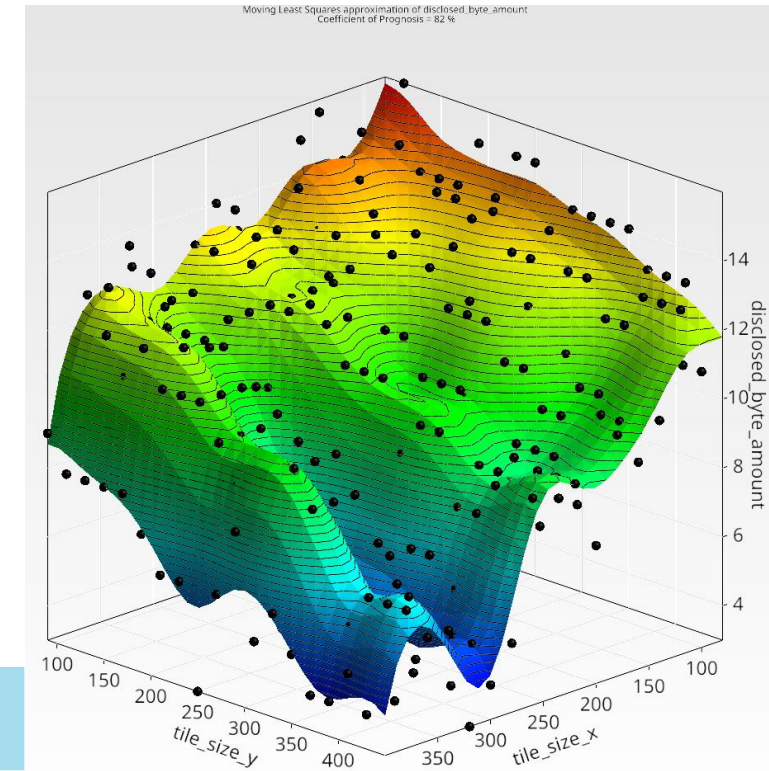
- Results show that bytes 7, 8, 14, and 15's boundary-based traces can also strongly disclose bytes 5, 9, 2, and 4, respectively
- However, the bounding boxes are not overlapped with those disclosed bytes' bound
- For the first time, the effect of IR drop on SCA has been observed and discussed

Evidence: Pre-Silicon Modeling and Assessment

- 3000 photon emission images simulated
- Performed correlation photon emission analysis (CPEA)
- Key disclosures observed from all 16 bytes of AES Sbox



Tile Arrangements	Attack Scenario	Abstraction Model	Custom Leakage Model	Disclosure
Per byte bound	White/grey box	Hamming Weight	Last round	16 Sbox bytes
Evenly segmenting the layout	Black box	Hamming Weight	Last round	Depends on tile-sizings, summarized in the 3D fig.



Impact of tile size on uniform segmentation of photon emission image: exploring the effects on disclosed byte amount

Conclusion and Future Work

- **Conclusion**

- By modeling the photon emission behavior of NMOS, we propose a framework performing the optical side-channel verification at the pre-silicon stage.

- **The correlation between byte placement and optical side-channel leakage**

- Some placement features (e.g., mutual distances of FFs within a byte) can be added to observe their impact on leakage level
- The goal is to provide mitigation suggestions / security-aware design constraints

- **Silicon validation feasibilities**

- Optical leakage has been proved to facilitate extracting values from SRAM/PUFs, etc.
- Fast sampling of certain AES rounds' emissions is feasible using existing NIR cameras (InGaAs, CCD, etc.)