Nelms Institute for the Connected World
UNIVERSITY of FLORIDA

# **EMSim**: A Fast Layout Level Electromagnetic Emanation Simulation Framework for High Accuracy Pre-Silicon Verifications

Haocheng Ma[1], Max Panoff[2], Jiaji He[3], Yiqiang Zhao[1] and **Yier Jin**[2]

[1]Tianjin University, [2]University of Florida, [3]Tsinghua University

# Outline

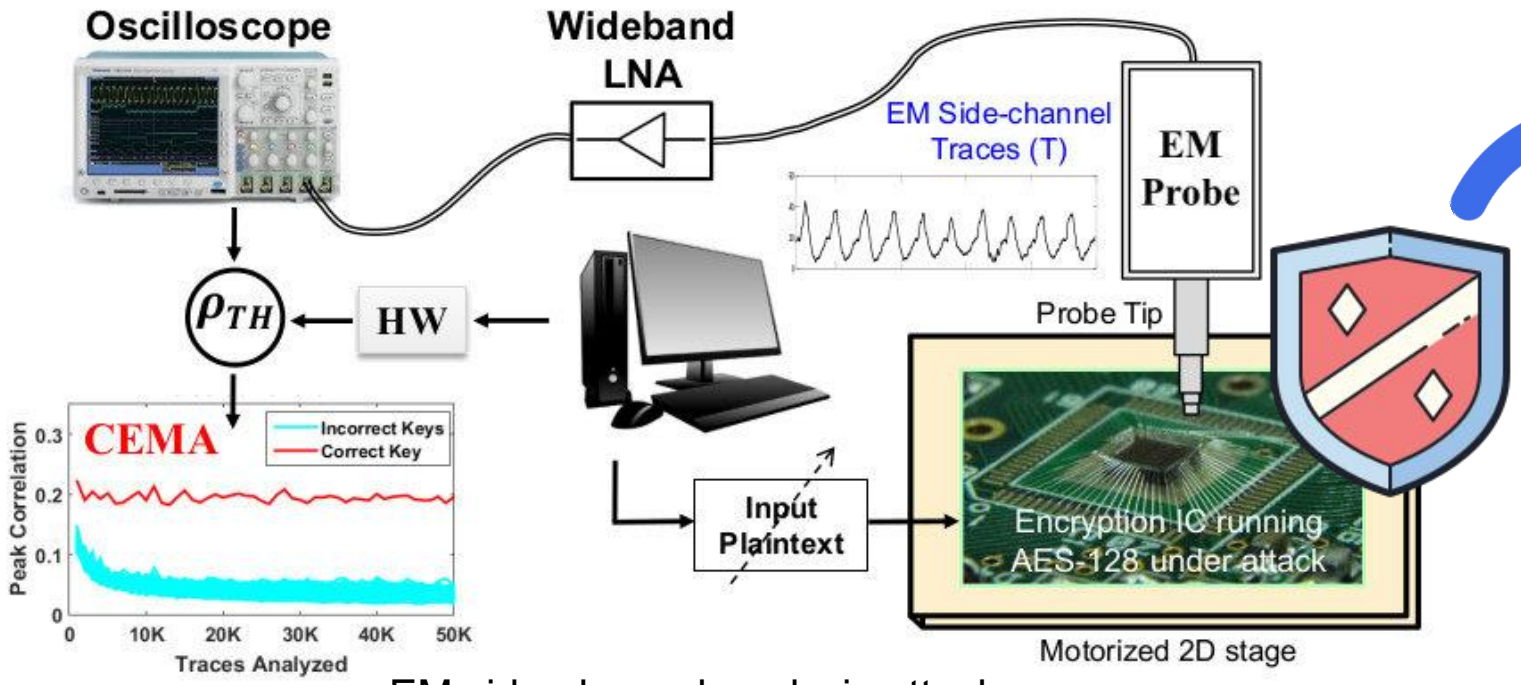
- Motivation
- Modeling Framework
  - Model Analysis
  - Simulation Framework
- Case Studies
  - EMSim vs ConvEM
  - EMSim vs Silicon Measurements
- Conclusions

# Outline

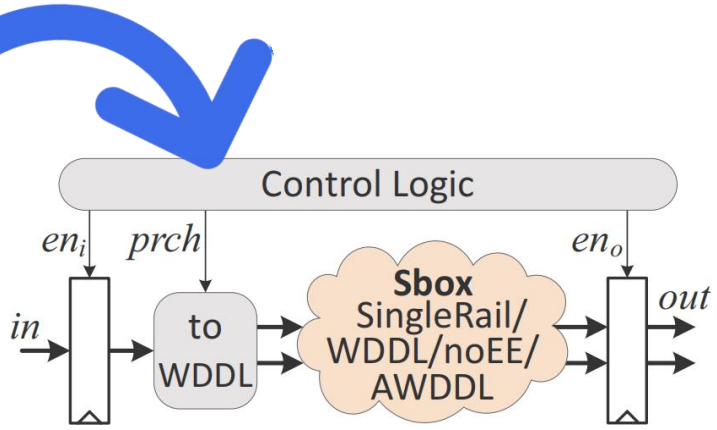
- Motivation
- Modeling Framework
  - Model Analysis
  - Simulation Framework
- Case Studies
  - EMSim vs ConvEM
  - EMSim vs Silicon Measurements
- Conclusions

# Motivation

- Increasingly EM side-channel threats targeting ICs
  - Rich spatial information, contactless collection
  - Break dual-rail logics[1], threshold implementations[2], etc.




EM side-channel analysis attacks

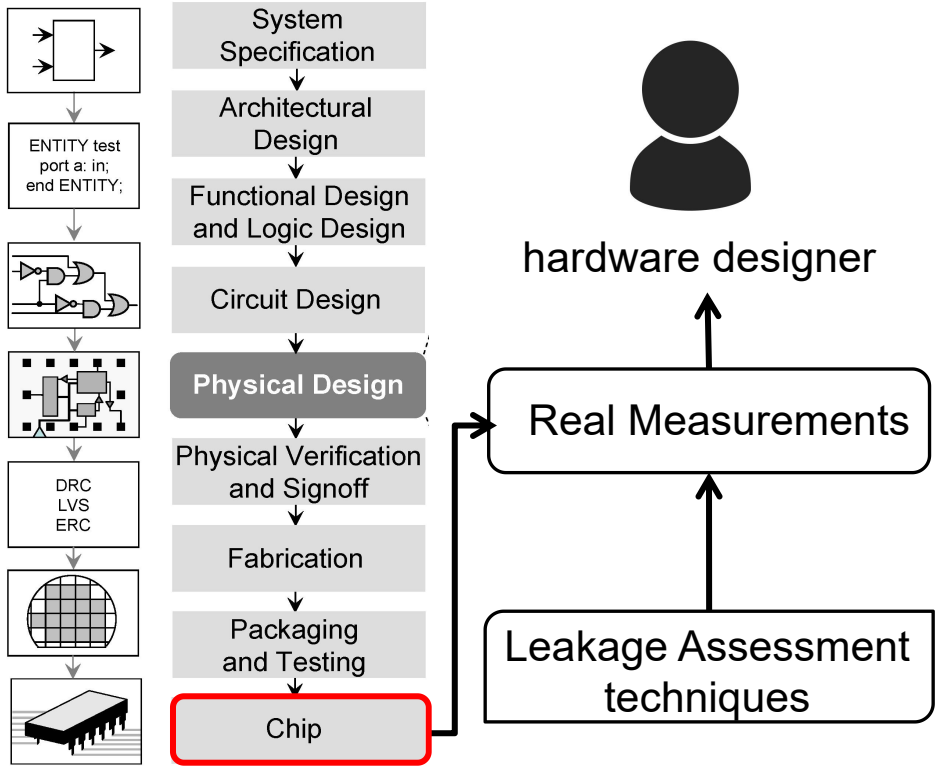



Design block with Dual-rail logics[1]


[1] Immler V, et al. Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs, 2017.
[2] Bilgin B, et al. Higher-order threshold implementations, 2014.

# Motivation

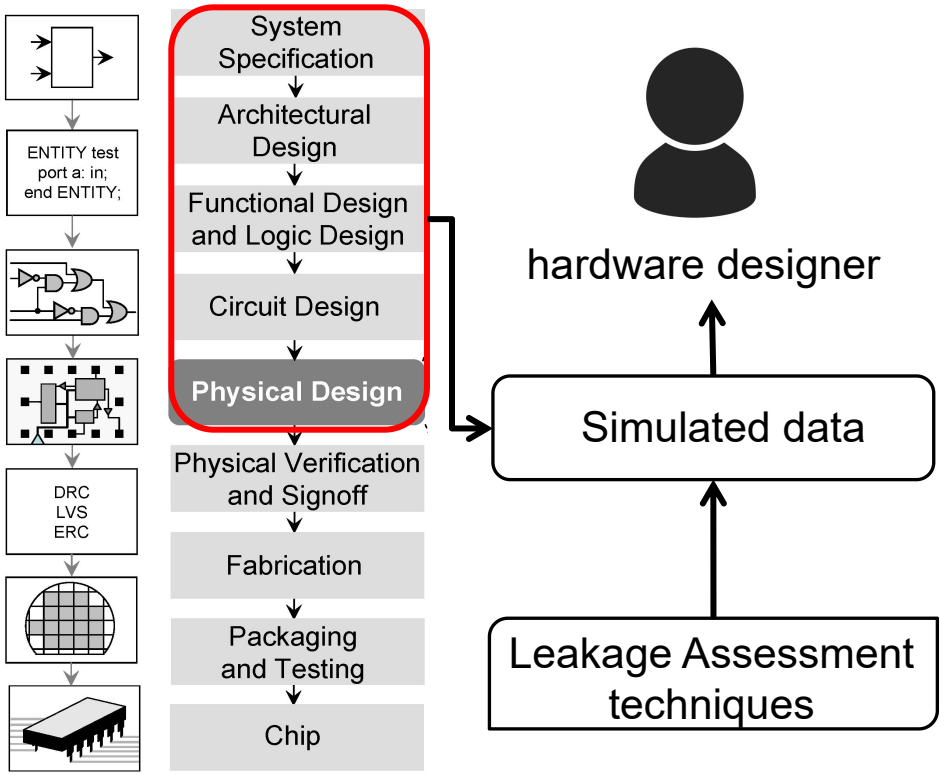
- EM side-channel leakage assessment is of importance
  - Post-silicon assesment with real measurements
    - Only quantify the security level
    - High cost in making design changes




Post-silicon leakage assessment

# Motivation

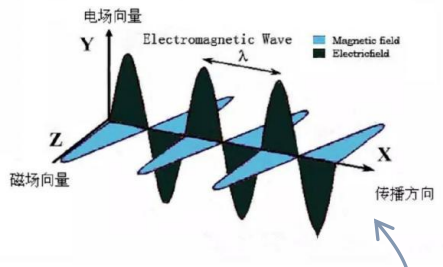
- EM side-channel leakage assessment is of importance
  - Post-silicon assesment with real measurements
    - Only quantify the security level
    - High cost in making design changes
  - Pre-silicon assesment with simulated data
    - Quantify the security level
    - Diagnose vulnerabilities location
    - Flexibility in making design changes
  - EM simulation with layout data can fully indicate the spatial, temporal and amplitude characteristics of EM emanations




Pre-silicon leakage assessment

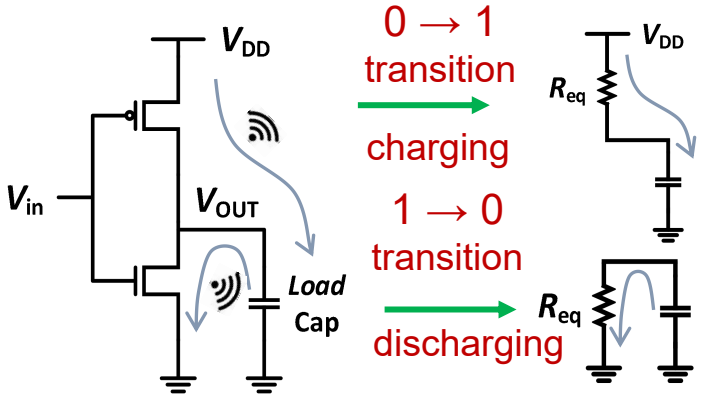
# Motivation

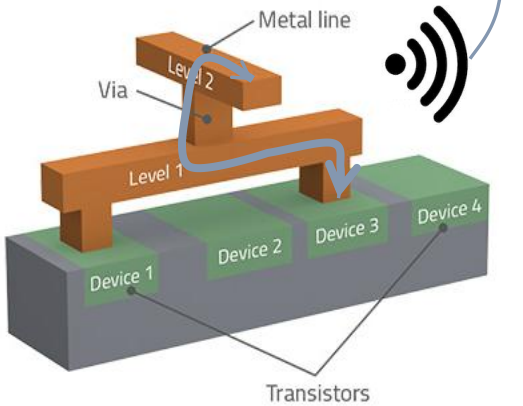
- the procedure of the layout-level EM simulation
  - Multi-level circuit analysis to obtain the current profiles
  - Calculate the probed EM emanations




$$\frac{di_c(t)}{dt} = \frac{d^2q}{dt^2} \neq 0$$

state transitions → changing current




logic cells create varying currents

metal wires emit EM fields

Principle of EM simulation

# Motivation



- the procedure of the layout-level EM simulation
  - Multi-level circuit analysis to obtain the current profiles
  - Calculate the probed EM emanations
- Existing methods suffer from scalability issues
  - Growing circuit sizes, lead to large extracted parasitic networks and complex simulated device models
  - Lack of theoretical guidance to simplify the EM simulation

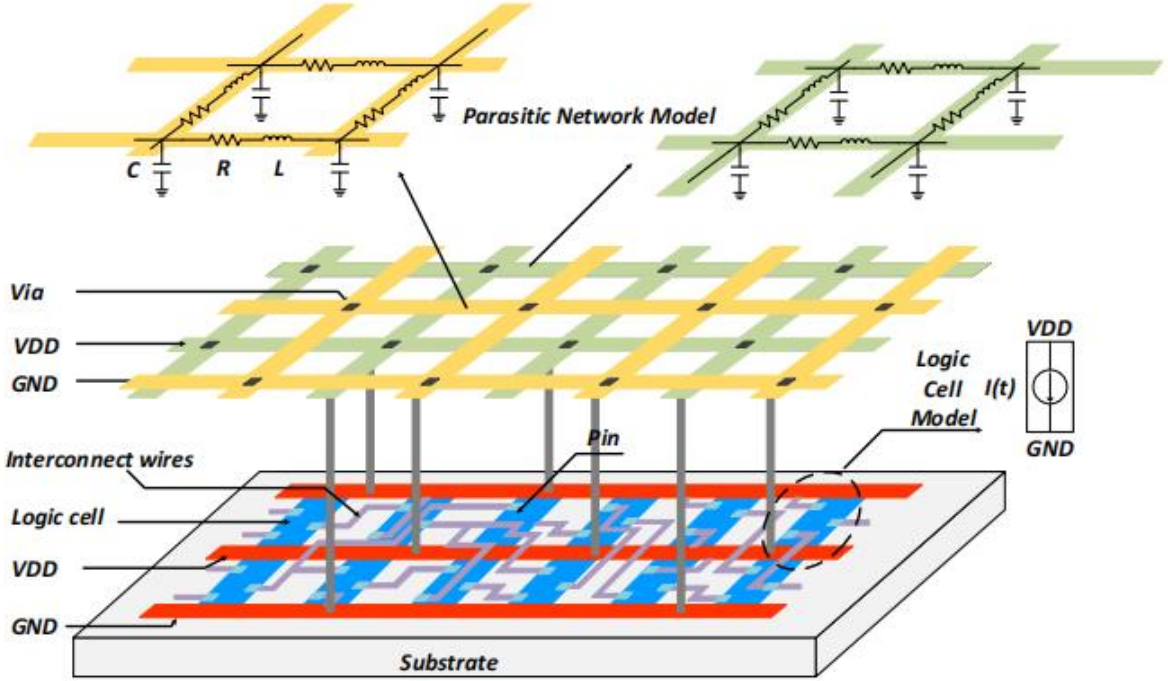
**EMSim**: A Fast Layout Level Electromagnetic Emanation Simulation Framework for High Accuracy Pre-Silicon Verifications

# Outline

- Motivation
- Modeling Framework
  - Model Analysis
  - Simulation Framework
- Case Studies
  - EMSim vs ConvEM
  - EMSim vs Silicon Measurements
- Conclusions

# Modeling Framework

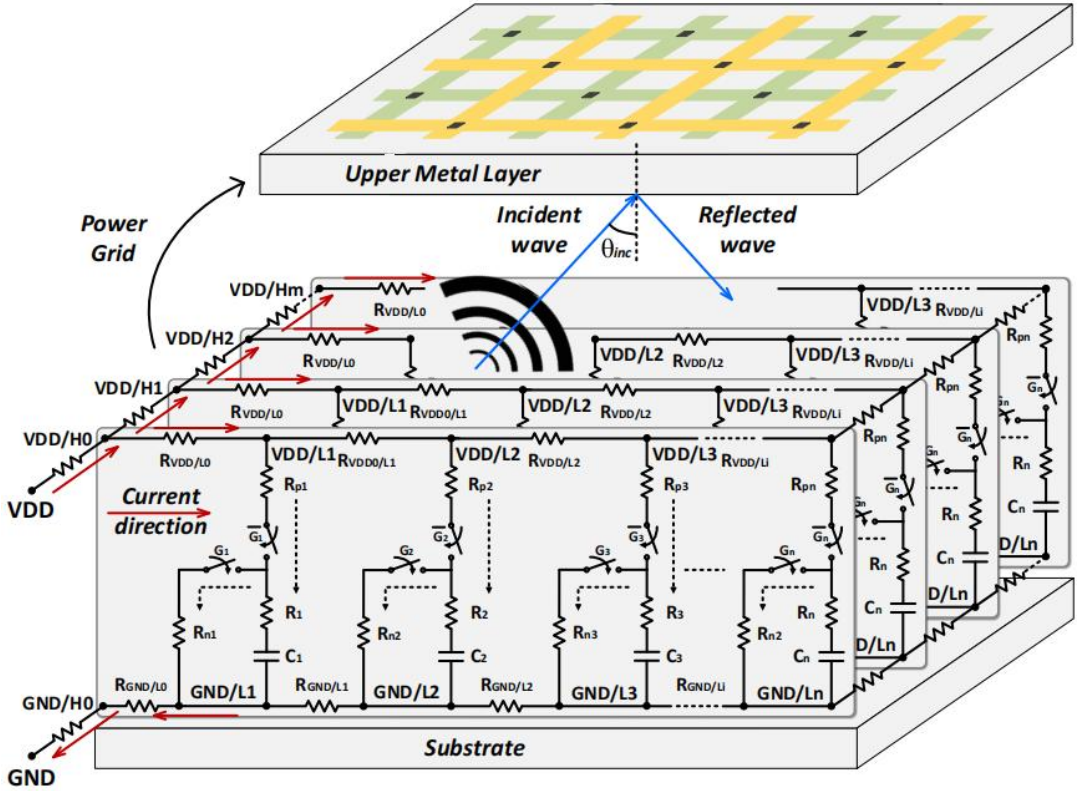
- Physical model of CMOS based ICs
  - Logic cell network is formed by groups of transistors on silicon substrate
  - The power grid combined with interconnect wires, forms the parasitic network




Physical model of CMOS based ICs

# Modeling Framework

- The genesis of ICs' EM emanations
  - Larger currents flows within the power grids in the upper metal layers as current acumulation



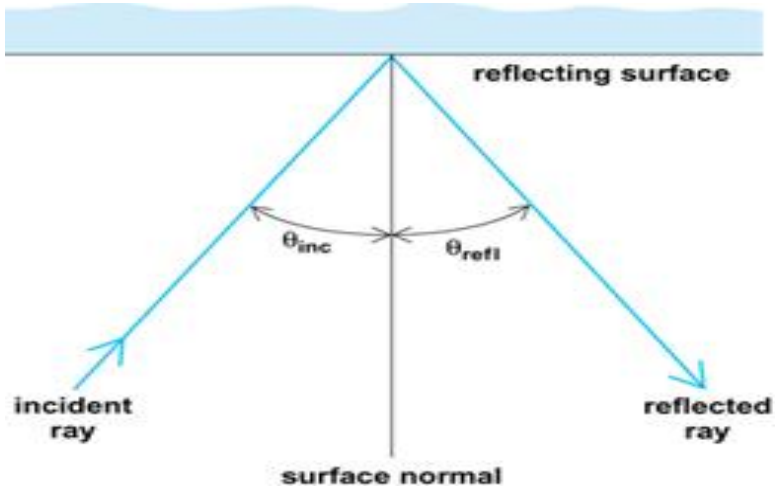

VDD: the power pins around the chip die VDD/Hj: power nodes distributed in the top metal layers of the power grid
VDD/Li: Power nodes in the lower metal layers of the power grid
$R_i$ and $C_i$ : equivalent resistance and capacitance of load (interconnect wires and cells)

$$I_{VDD} = \sum_{j=1}^{m} I_{VDD/Hj} = \sum_{j=1}^{m}\sum_{i=1}^{n} I_{VDD/Li}$$

$$= \sum_{j=1}^{m}\sum_{i=1}^{n}\left[\frac{V_{VDD/Li} - V_{GND/Li}}{R_{pi} + R_{si} - 1/jwC_i} + I_{short} + I_{leak}\right]$$

# Modeling Framework

- The genesis of ICs' EM emanations
  - Larger currents flows within the power grids in the upper metal layers as current acumulation
  - Due to existence of the metal shielding, EM emanations from lower metal layers hardly propagate to the external environment.



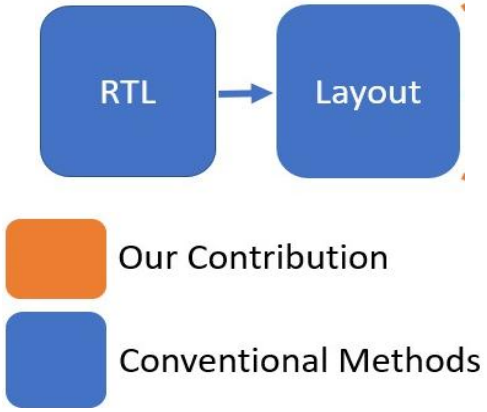

Wave reflection when propagating on the metal surface

$$R = \frac{(1-\sqrt{2\varepsilon_0\omega/\sigma})^2+1}{(1+\sqrt{2\varepsilon_0\omega/\sigma})^2+1} \approx 1-\sqrt{2\varepsilon_0\omega/\sigma}$$

electrical conductivity of Cu: $\sigma = 5.7\mathrm{e}7\ \mathrm{S/m}$
vacuum permittivity $\varepsilon_0 = 8.85\mathrm{e}-12\ \mathrm{F/m}$
ω is circular frequency.

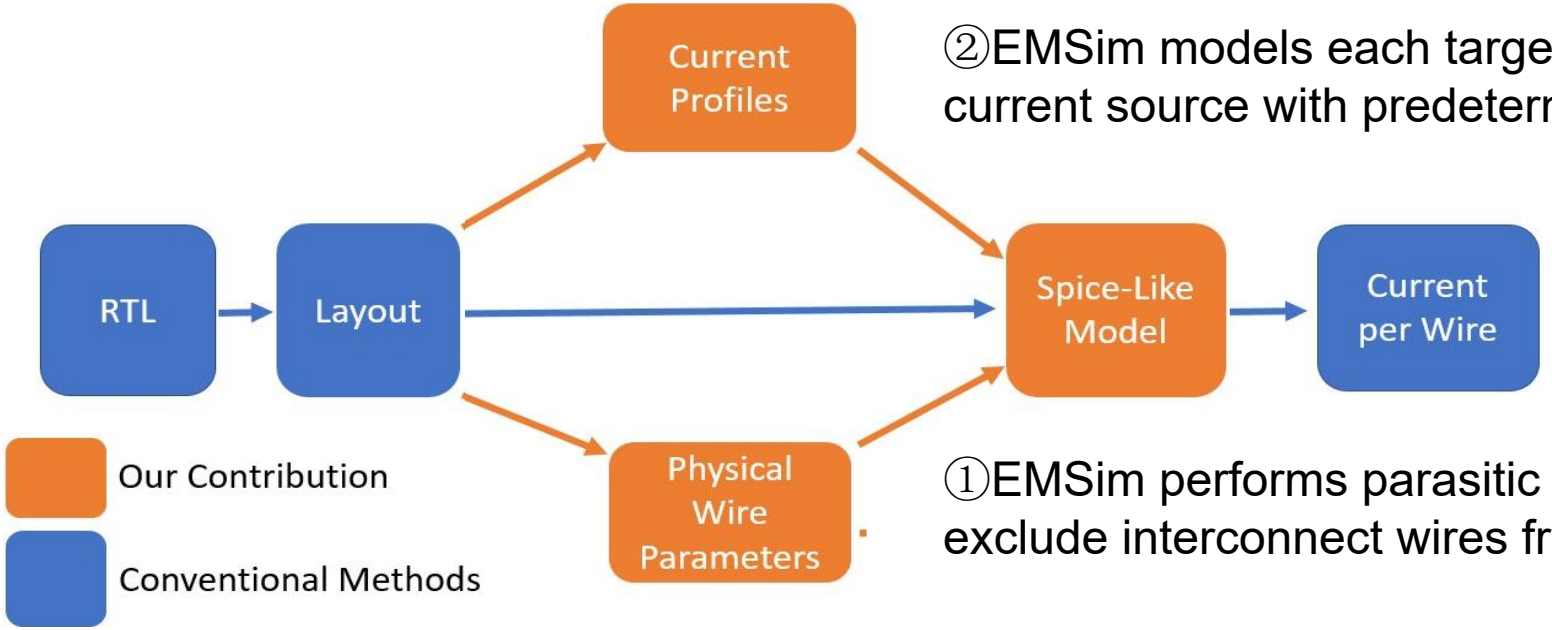
# Modeling Framework

- EMSim Framework
  - Data Preparation: RTL-to-GDS flow to create a layout database



# Modeling Framework

- EMSim Framework
  - Data Preparation: RTL-to-GDS flow to create a layout database
  - Current Analysis: parasitic network reduction, device model approximation




②EMSim models each target logic cell as a current source with predetermined currents

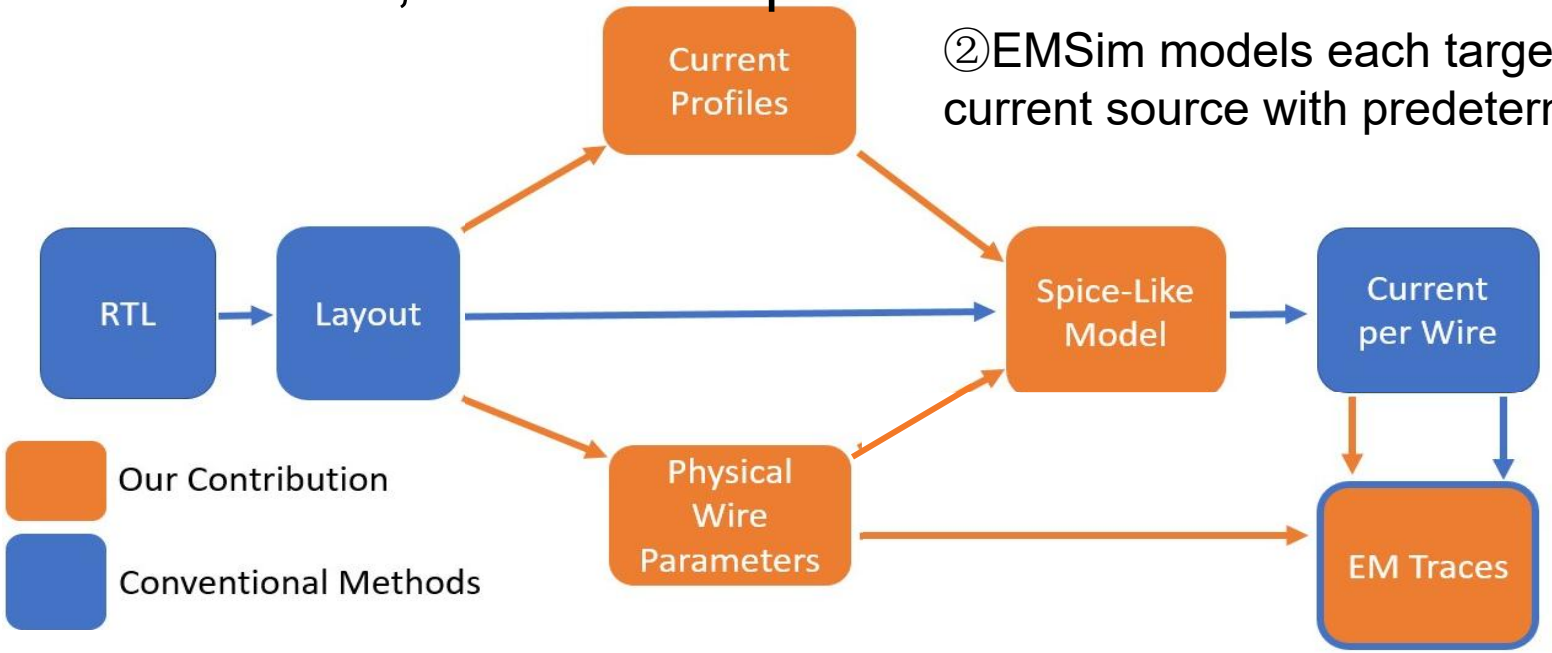
③Through hybridization, EMSim uses HSpice to solve the transient current in each metal wire

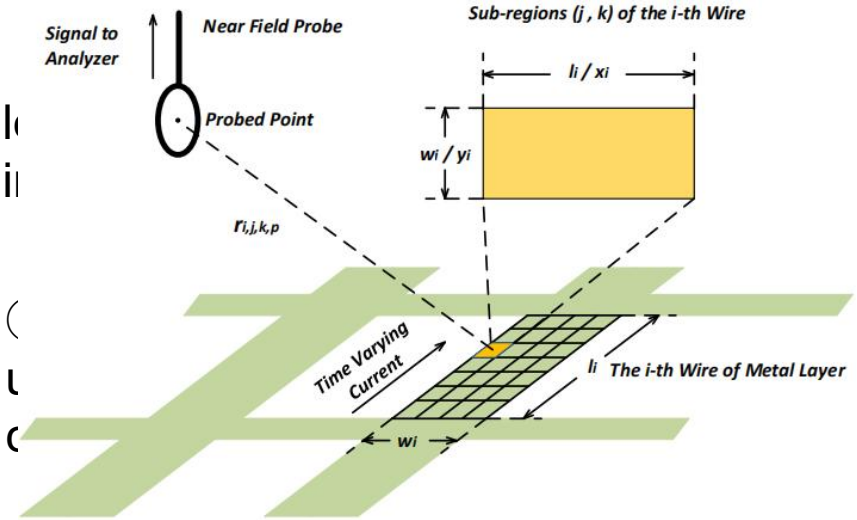
①EMSim performs parasitic network reduction to exclude interconnect wires from the parasitic netlist

# Modeling Framework

- EMSim Framework
  - Data Preparation: RTL-to-GDS flow to create a layout database
  - Current Analysis: parasitic network reduction, device model approximation
  - Electromagnetic Computation: approximate the magnetic field at a certain time, at a certain point

②EMSim models each target l
current source with predetermi




twork reduction to
the parasitic netlist

EMSim leverages GPU
acceleration through Cupy

# Outline

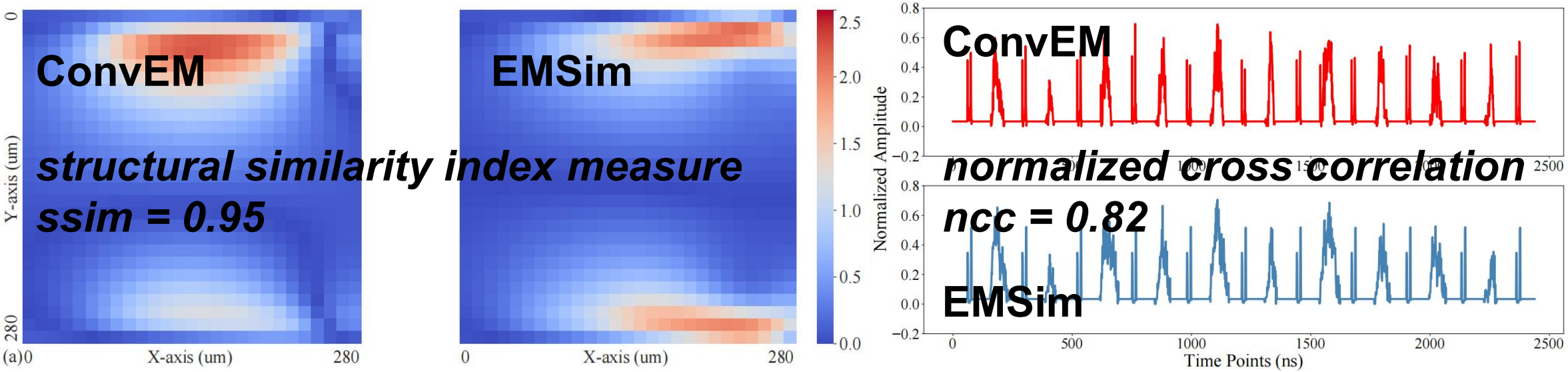
- Motivation
- Modeling Framework
  - Model Analysis
  - Simulation Framework
- Case Studies
  - EMSim vs ConvEM
  - EMSim vs Silicon Measurements
- Conclusions

# Case Studies

- EMSim vs ConvEM
  - Benchmark: 32-bit S-Box design
  - Simulation Accuracy

parasitic network reduction

①180 nm CMOS technology
②900 cells and 31546 wires → 754 wires
③280.36 um x 280.24 um of die size
④supply voltage 1.8 V
⑤clock frequency 20 MHz



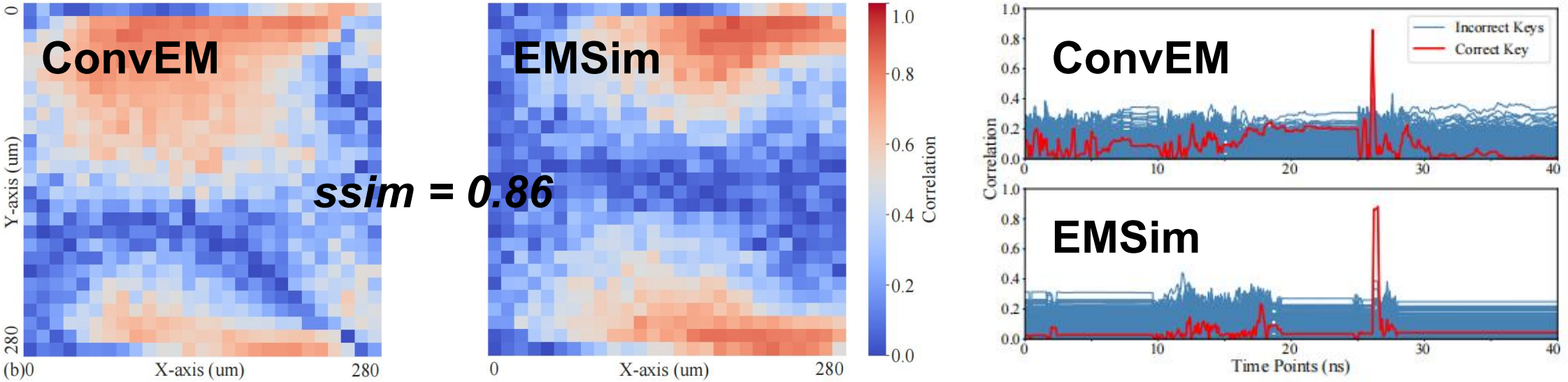

Comparisons between ConvEM (left) and EMSim (right): (a) magnetic map and (b) correnponding traces.

# Case Studies

- EMSim vs ConvEM
  - Benchmark: 32-bit S-Box design
  - Simulation Accuracy
  - Security Evaluation

parasitic network reduction

①180 nm CMOS technology
②900 cells and 31546 wires → 754 wires
③280.36 um x 280.24 um of die size
④supply voltage 1.8 V
⑤clock frequency 20 MHz




CEMA attacks on the S-Box: (a) correlation map and (b) correlation traces as a function of time points obtained from ConvEM and EMSim.

# Case Studies

- EMSim vs ConvEM
  - Benchmark: 32-bit S-Box design
  - Simulation Accuracy
  - Security Evaluation
  - Computation Cost

parasitic network reduction

①180 nm CMOS technology
②900 cells and 31546 wires → 754 wires
③280.36 um x 280.24 um of die size
④supply voltage 1.8 V
⑤clock frequency 20 MHz

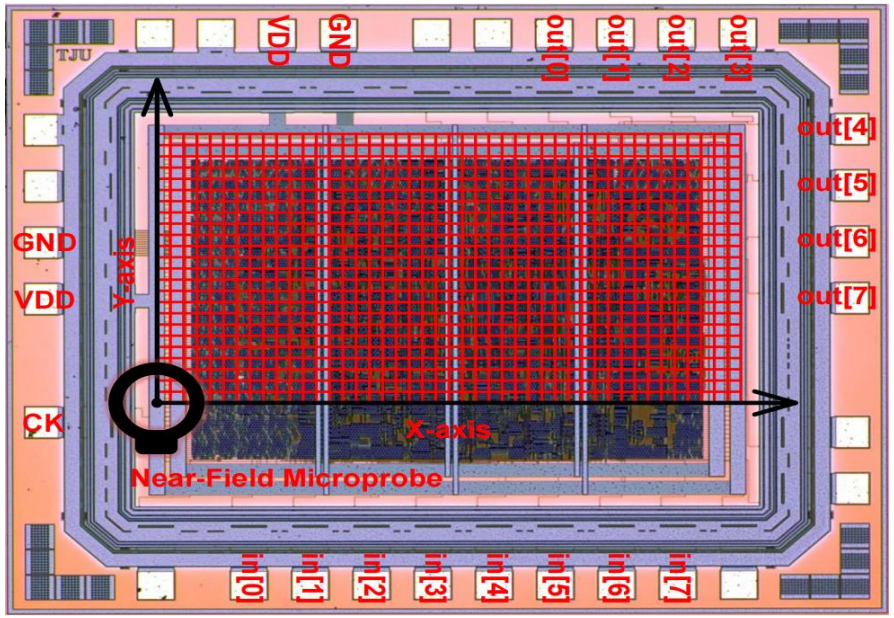
| Method | Current Simulation | EM Computation |
|---|---|---|
| ConvEM | 2.017 s | 0.233 s |
| EMSIM | 0.065 s | 0.003 s |

TABLE II: Real time spent on each simulation time point for a simple 32-bit AES S-Box.

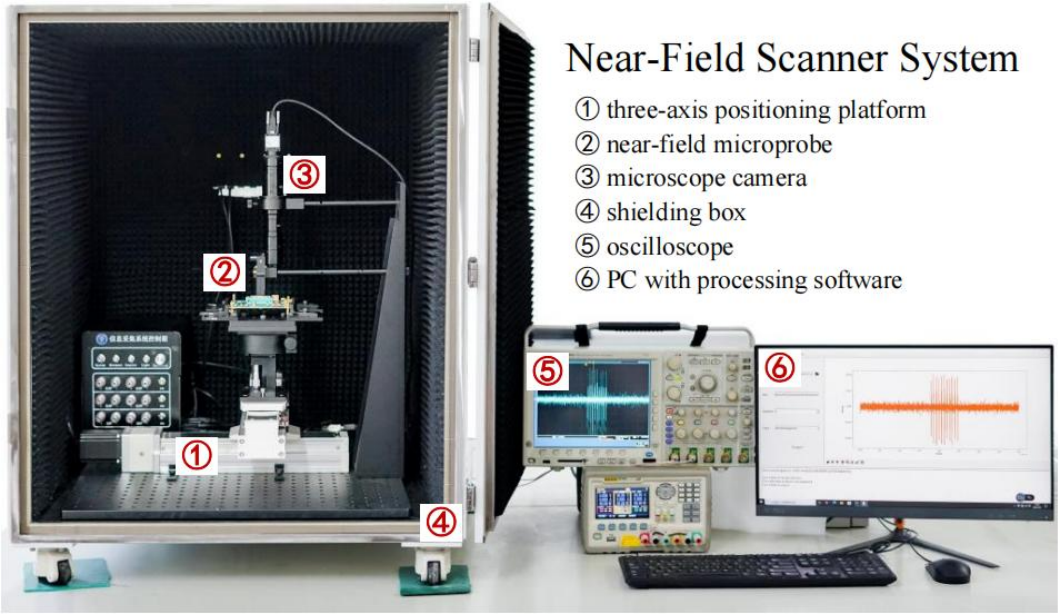
# Case Studies

- EMSim vs Silicon Measurements
  - Benchmark: 128-bit AES design

①180 nm CMOS technology
②14559 cells and 733662 wires
③1.6 mm x 1.3 mm of die size
④supply voltage 1.8 V
⑤clock frequency 25 MHz
365529 for current analysis
1424 for electromagnetic computation




The die image of the fabricated AES design.

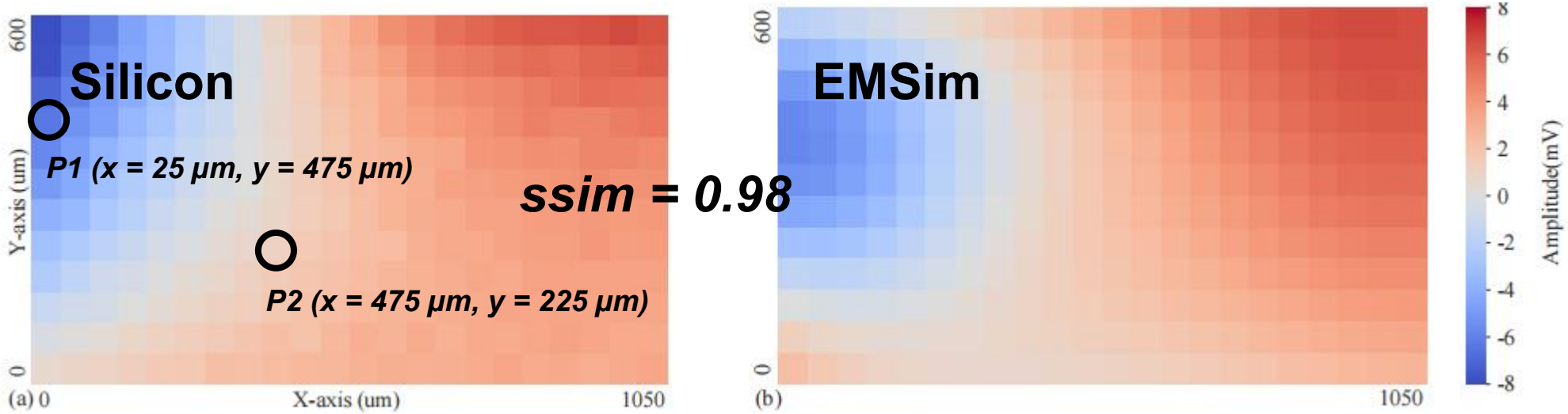



The overview of the experimental setup.

# Case Studies

- EMSim vs Silicon Measurements
  - Benchmark: 128-bit AES design
  - Simulation Accuracy

①180 nm CMOS technology
②14559 cells and 733662 wires
③1.6 mm x 1.3 mm of die size
④supply voltage 1.8 V
⑤clock frequency 25 MHz
365529 for current analysis
1424 for electromagnetic computation

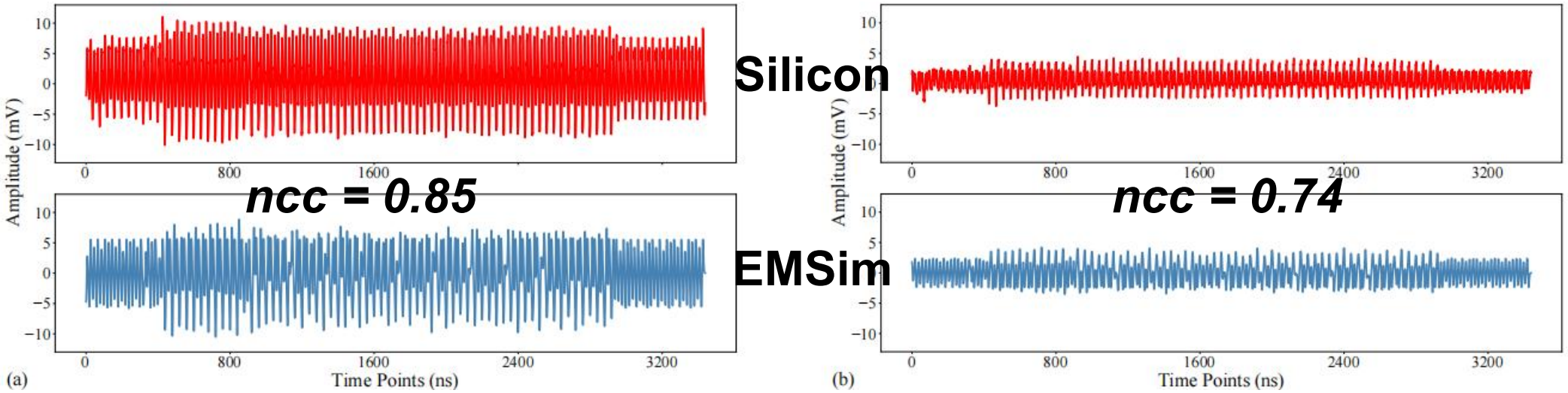



The map of EM signals obtained by (a) silicon measurements, (b) EMSim results

# Case Studies

- EMSim vs Silicon Measurements
  - Benchmark: 128-bit AES design
  - Simulation Accuracy

①180 nm CMOS technology
②14559 cells and 733662 wires
③1.6 mm x 1.3 mm of die size
④supply voltage 1.8 V
⑤clock frequency 25 MHz
365529 for current analysis
1424 for electromagnetic computation

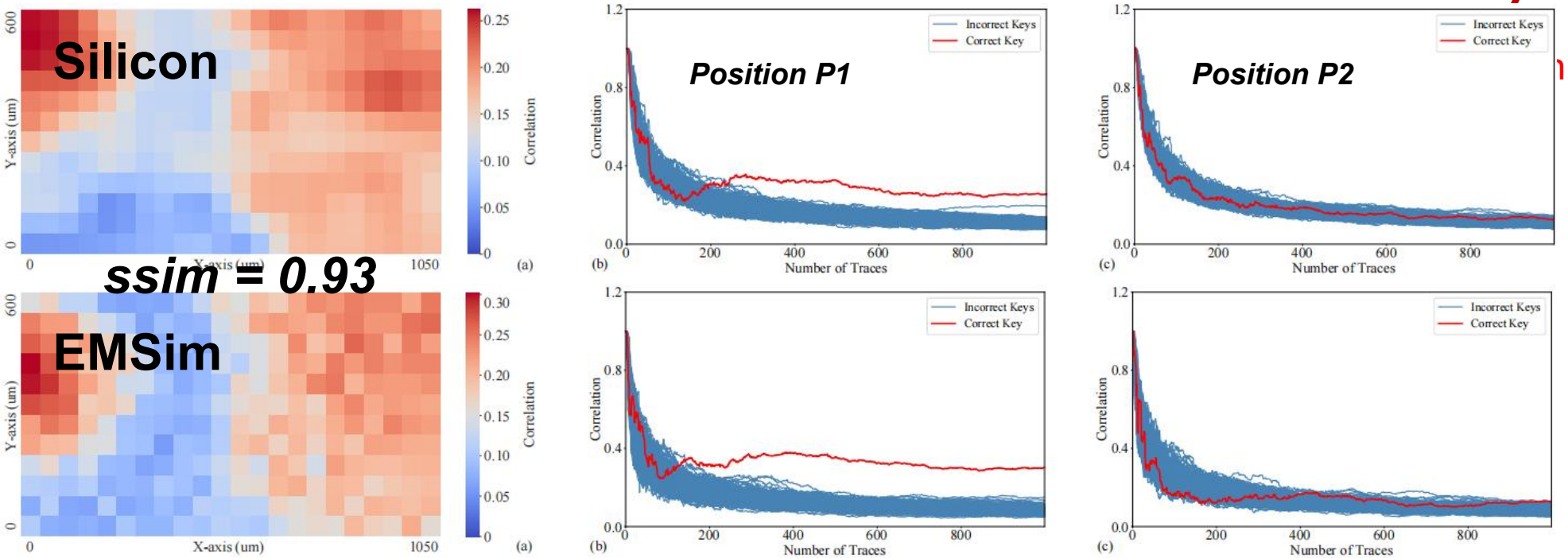



The comparisons of EM signals obtained by silicon measurements (top) and EMSIM results (bottom), at (a) position P1 and (b) position P2

# Case Studies

- EMSim vs Silicon Measurements
  - Benchmark: 128-bit AES design
  - Security Evaluation

①180 nm CMOS technology
②14559 cells and 733662 wires
③1.6 mm x 1.3 mm of die size
④supply voltage 1.8 V
⑤clock frequency 25 MHz




CEMA attacks on the fabricated AES-128: (a) correlation of the correct key as a function of spatial locations. correlation traces as a function of stimuli number for (b) position P1 and (c) Position P2

# Case Studies

- EMSim vs Silicon Measurements
  - Benchmark: 128-bit AES design
  - Simulation Accuracy
  - Security Evaluation
  - Computation Cost

①180 nm CMOS technology
②14559 cells and 733662 wires
③1.6 mm x 1.3 mm of die size
④supply voltage 1.8 V
⑤clock frequency 25 MHz
365529 for current analysis
1424 for electromagnetic computation

| Method | Current Simulation | EM Computation |
|---|---|---|
| EMSIM | 3.860 s | 3.451 s |

TABLE II: Real time spent on each simulation time point for AES-128 design.

# Outline

- Motivation
- Modeling Framework
  - Model Analysis
  - Simulation Framework
- Case Studies
  - EMSim vs ConvEM
  - EMSim vs Silicon Measurements
- Conclusions

# Conclusions



- we develop the EMSim framework to significantly speed up EM simulation from the layout level, making EM side channel simulation for larger-scale circuits practical.
- We implement multiple techniques, including device model approximation and parasitic network reduction for the current analysis and GPU acceleration for EM computation, to achieve this.
- These simulated EM traces can be used for design-time security evaluation on an IC's resilience against EM side channel attacks.

# Thank You!
# Any Questions?