Multiphysics Simulation of EM and Thermal Side-Channels with ML-based Auto-POI Identification

Norman Chang, Ansys Fellow

Chief Technologist of Electronics, Semiconductor, and Optics BU

CAD4Security Workshop

DAC, 2022

Agenda

- Background of EM and thermal side-channel analysis
- Simulation challenges and identification of POIs for EM side-channel analysis
- Simulation challenges and identification of POIs for thermal side-channel analysis
- Conclusion

©2022 ANSYS, Inc.

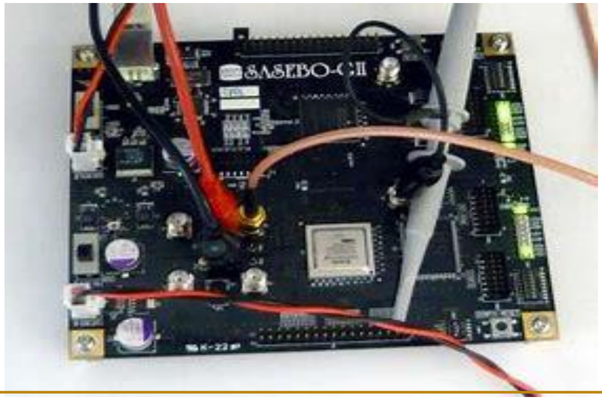
Electromagnetic Side-Channels – A Serious Data Leakage Problem

Unintentional but evitable data leakage from EM emission of microelectronics

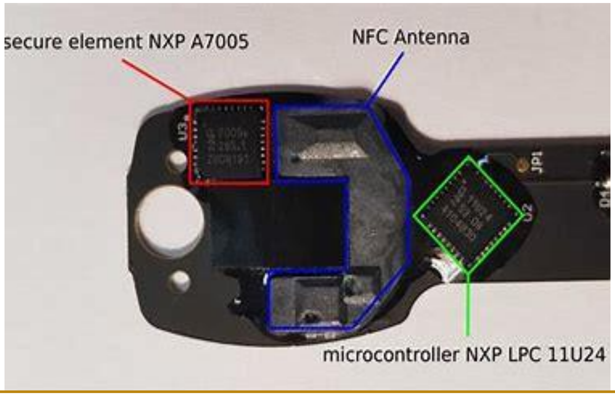
- A wide range of products being vulnerable
- Very difficult to mitigate even with power side-channel countermeasures
- Actually, very complicated to understand and hard to point out location weaknesses

Mobile device

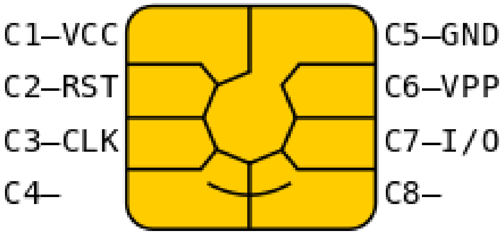
FPGA

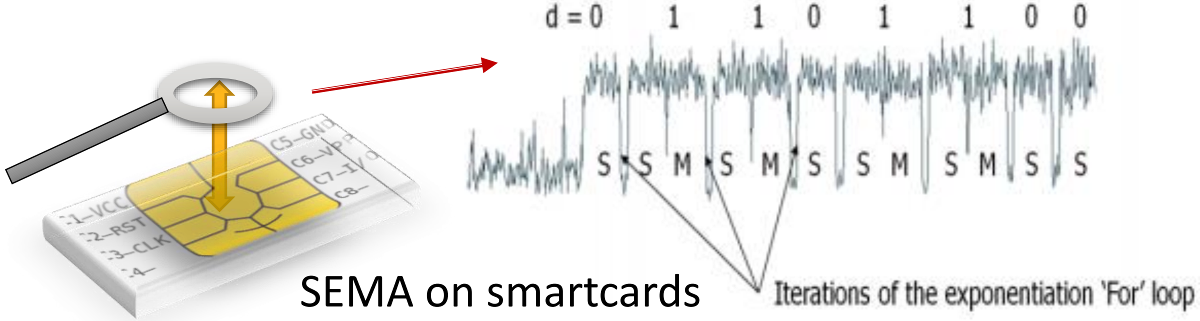


Security module

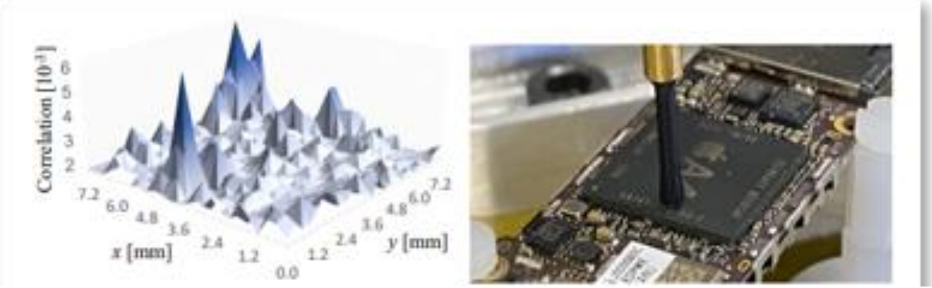


Smartcard





SEMA on smartcards



DEMA on iPhone SoC

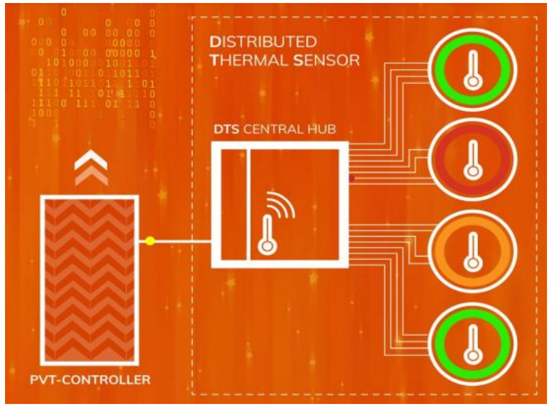
©2022 ANSYS, Inc.

Thermal Threat Modeling for 3DIC in Chip-Package-System

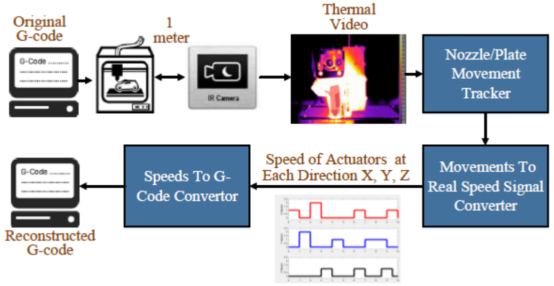
- Embedding Agents for Process Classification, Design Profiling plus measuring Margin, Workload, Voltage Integrity, Clock Integrity, Noise Modulation, Local Temperature and Thermal Gradients

- Agents feed deep data to platform
- Machine learning algorithms and data analytics
- Insights & Alerts

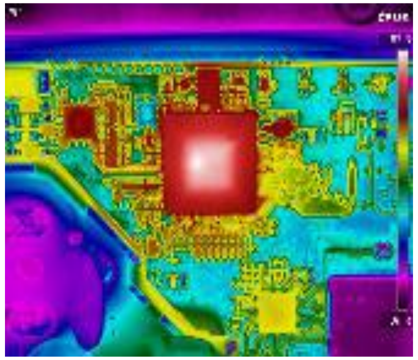
https://www.proteantecs.com/



https://www.moortec.com/dts/



Mohammad A. Faruque, et al, “Forensics of Thermal Side-Channel in Additive Manufacturing Systems”, CECS Technical Report, University of California, Irvine, 2016

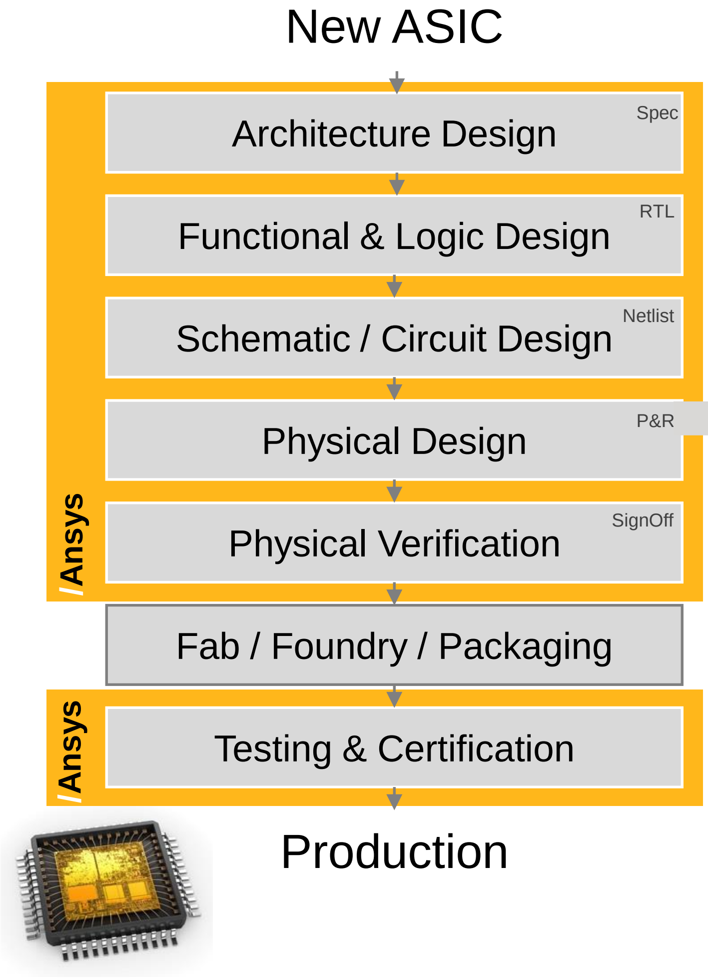


N. Asadi, “Physical Assurance and Inspection of Electronics”, HOST, 2020

- Thermal threat modeling by on-chip thermal sensors and thermal imagers are drawing more attention
  - Distributed on-chip thermal sensors (junction temperature level) accessible from JTAG ports as available from ProteanTecs and Moortec, etc.
  - Sophisticated thermal imagers can measure top metal layer(s) temperature with high resolution
  - Attack surface becomes broader for 3DICs including chip-to-chip communication in chiplet-based and heterogeneous 3DIC architectures
  - The chip temperature profile becomes a noticeable leakage data of the 3DIC chip-package system

©2022 ANSYS, Inc.

Side-channel Leakage Analysis (SCLA) in Design Flow



New ASIC

Architecture Design — Spec

Functional & Logic Design — RTL

Schematic / Circuit Design — Netlist

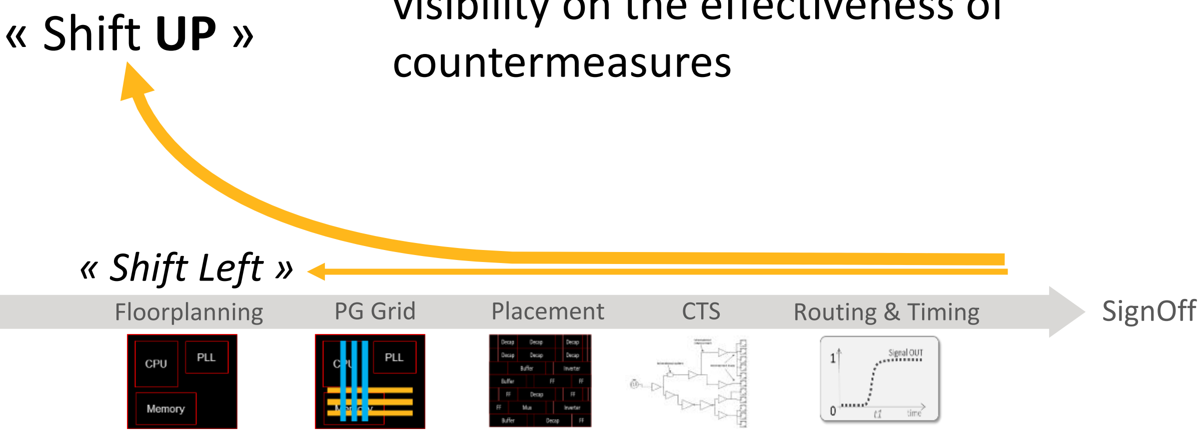
Physical Design — P&R

Physical Verification — SignOff

Fab / Foundry / Packaging

Testing & Certification

Production



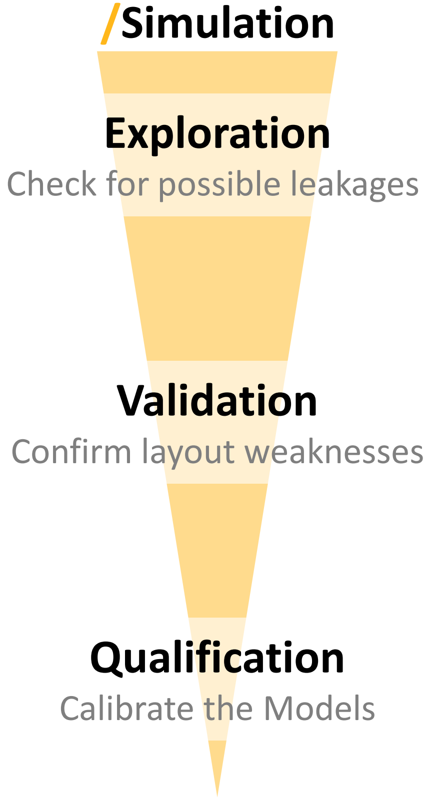
« Shift **UP** »

« Shift Left »

Floorplanning → PG Grid → Placement → CTS → Routing & Timing → SignOff

Designers wish to have earlier visibility on the effectiveness of countermeasures

Step 1	• RTL Power Side-Channel Leakage Sign-Off Flow
Step 2	• Gate Power Side-Channel Leakage Sign-Off Flow
Step 3	• SoC/3DIC EM and Power/Thermal Side-Channel Leakage Sign-Off Flow
Step 4	• Chip-Package-System Side-Channel Leakage Sign-off Flow



/Simulation

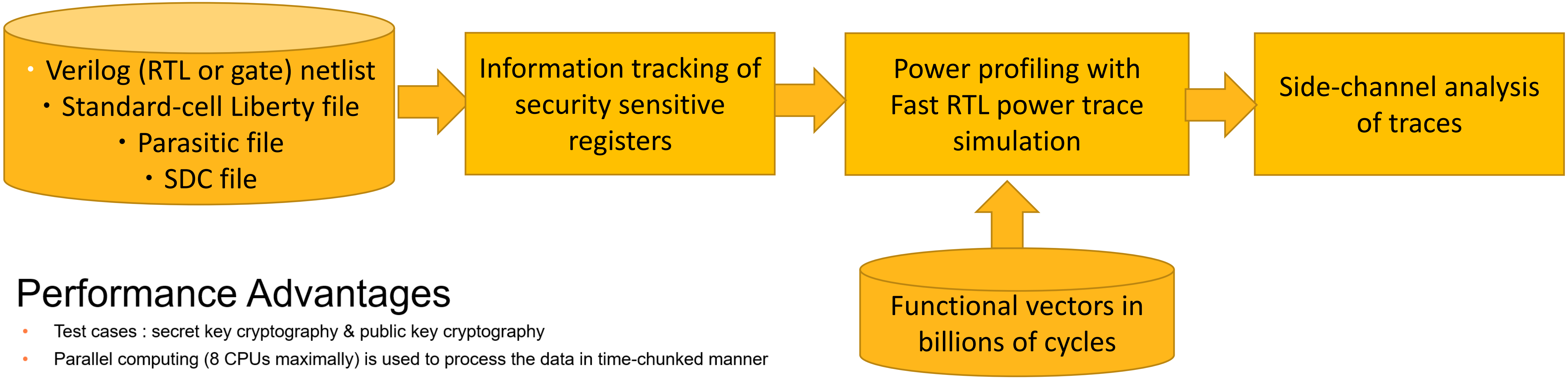
Exploration
Check for possible leakages

Validation
Confirm layout weaknesses

Qualification
Calibrate the Models

©2022 ANSYS, Inc.

Fast RTL Power Side-Channel Simulation is Essential



- Verilog (RTL or gate) netlist
- Standard-cell Liberty file
- Parasitic file
- SDC file

Information tracking of security sensitive registers

Power profiling with Fast RTL power trace simulation

Side-channel analysis of traces

Functional vectors in billions of cycles

Performance Advantages

- Test cases : secret key cryptography & public key cryptography
- Parallel computing (8 CPUs maximally) is used to process the data in time-chunked manner

Test cases	cycles	Test vectors	cell count	Peak memory	Total Runtime
Design 1 – unprotected AES	16M	1M	13k	5 GB	3 min
Design 1 – protected AES (with differential power rail)	27M	1M	24k	10 GB	4 min
Design 2 – protected AES (with masking countermeasure)	432M	2M	50k	64 GB	3 hours
Design 3 – ECC (public key crypto with constant-time Montgomery ladder)	1B	1k	64k	16 GB	5 hours

No leakage at RTL/Gate level does not mean no leakage at layout-level due to implementation

“RTL Design Security Verification for Resisting Power Side-channel Analysis”, K. Monta, M. Nagata, L. Lin, J. Wen, P. Gupta, N. Chang, Design Track, DAC 2022

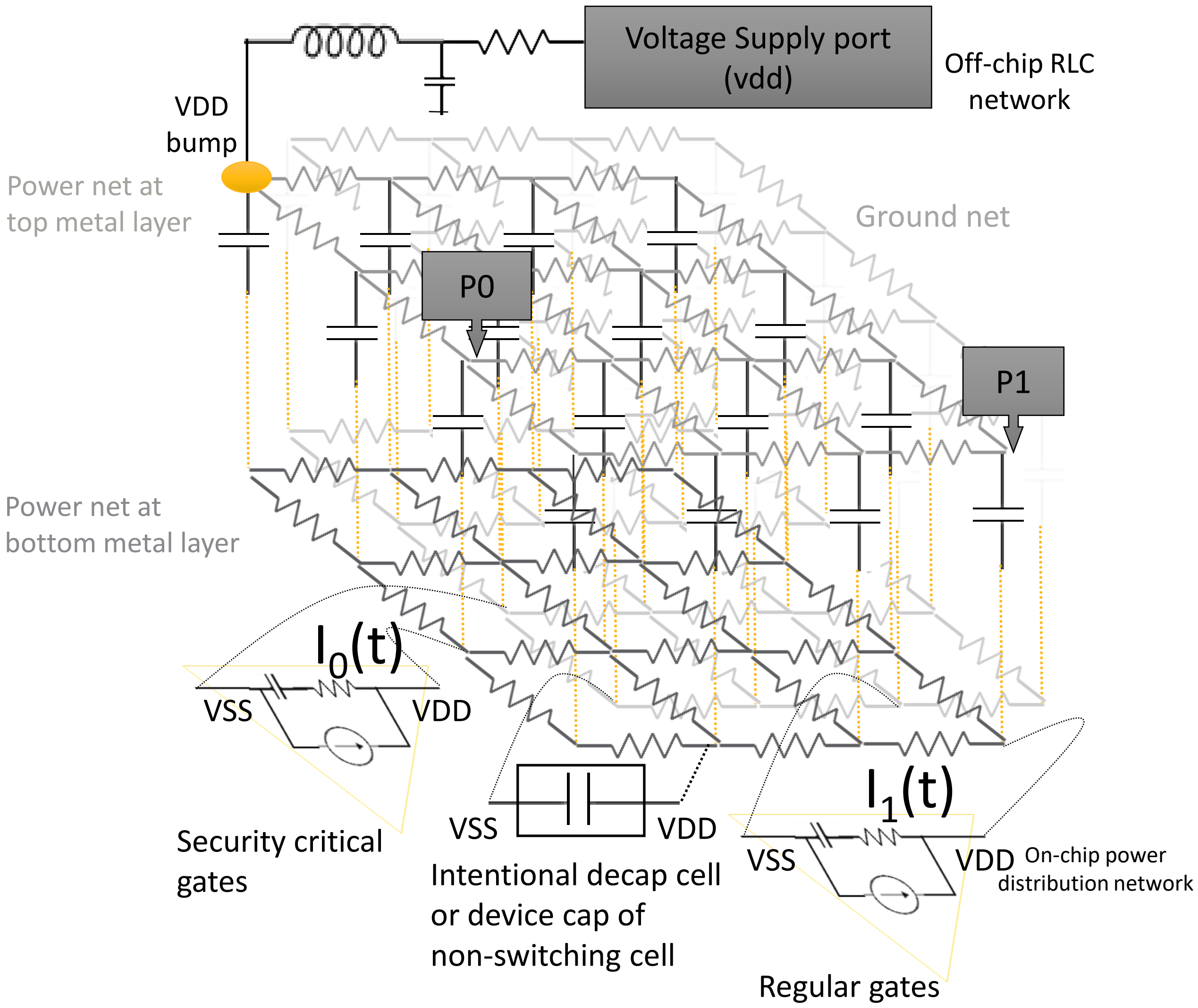
©2022 ANSYS, Inc.

Agenda

- Background of EM and thermal side-channel analysis
- Simulation challenges and identification of POIs for EM side-channel analysis
- Simulation challenges and identification of POIs for thermal side-channel analysis
- Conclusion

©2022 ANSYS, Inc.

Layout-level Power-noise Simulation with Virtual Probes

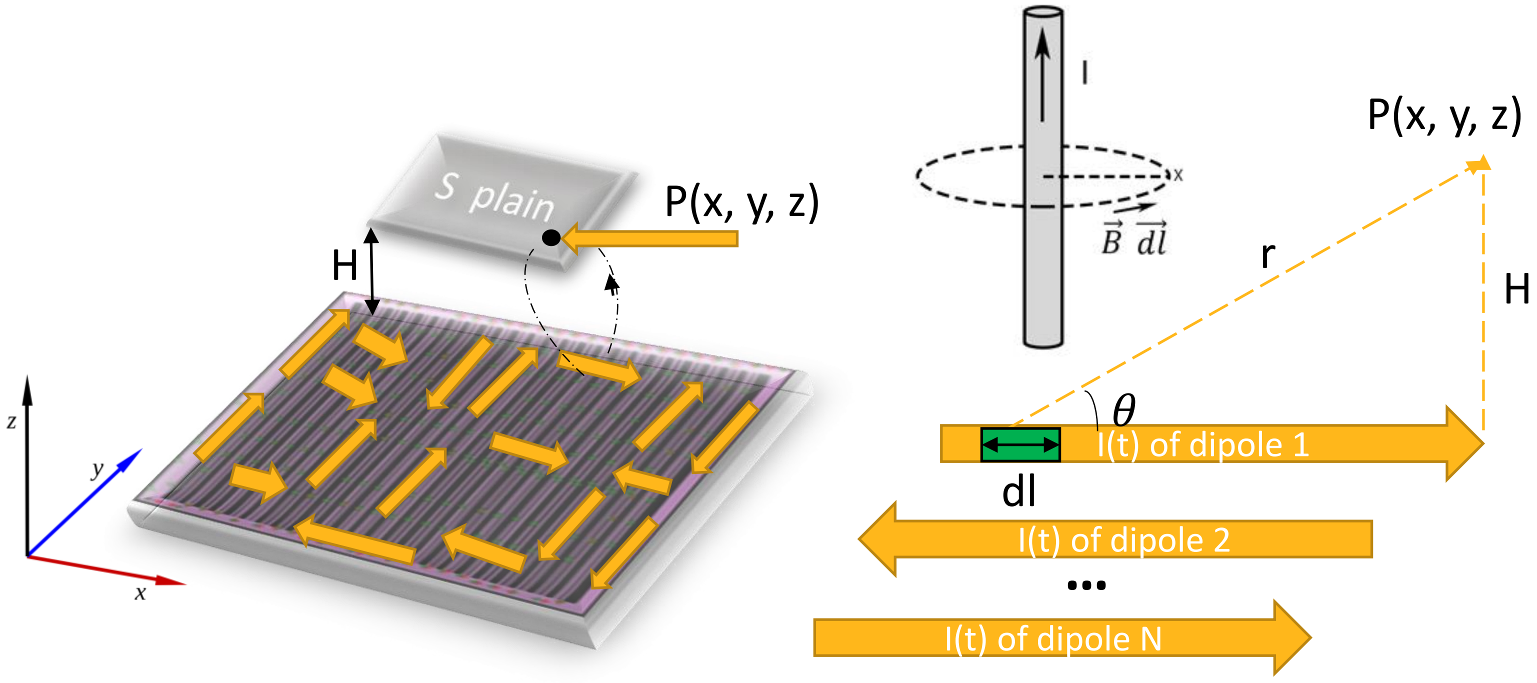


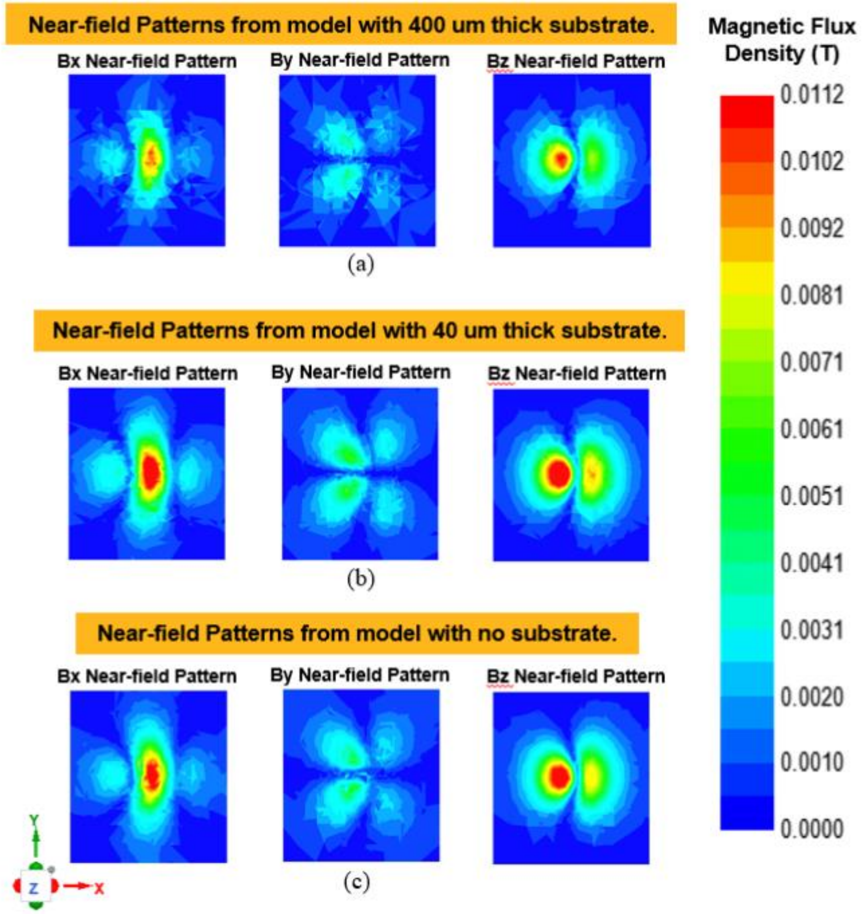
- Cell in design with pre-characterized dynamic power-noise model
  - Cell current I0(t) and I1(t) is controlled by stimuli (e.g., VCD)
  - Slew/Load/voltage conditions included
  - Decap/device cap impact included
- Extraction of on-chip power distribution network (PDN)
- Virtual probes P0/P1 can be inserted at any XY location, any metal layer, to simulate power-noise side-channel traces

©2022 ANSYS, Inc.

EMAG Solver

- On-die current modeled as electrical dipoles
- Near-field magnetic traces in time domain: EM side-channel traces
- Substrate impact is ignorable based on HFSS simulation

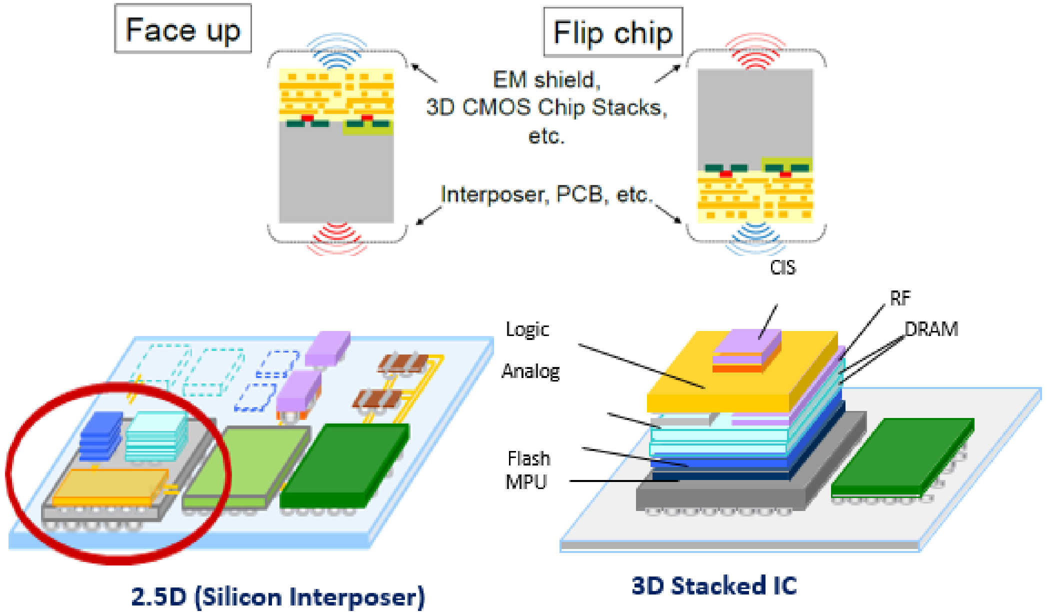




©2022 ANSYS, Inc.

EM SCLA Movie for Transient EM Heatmap and SMTD

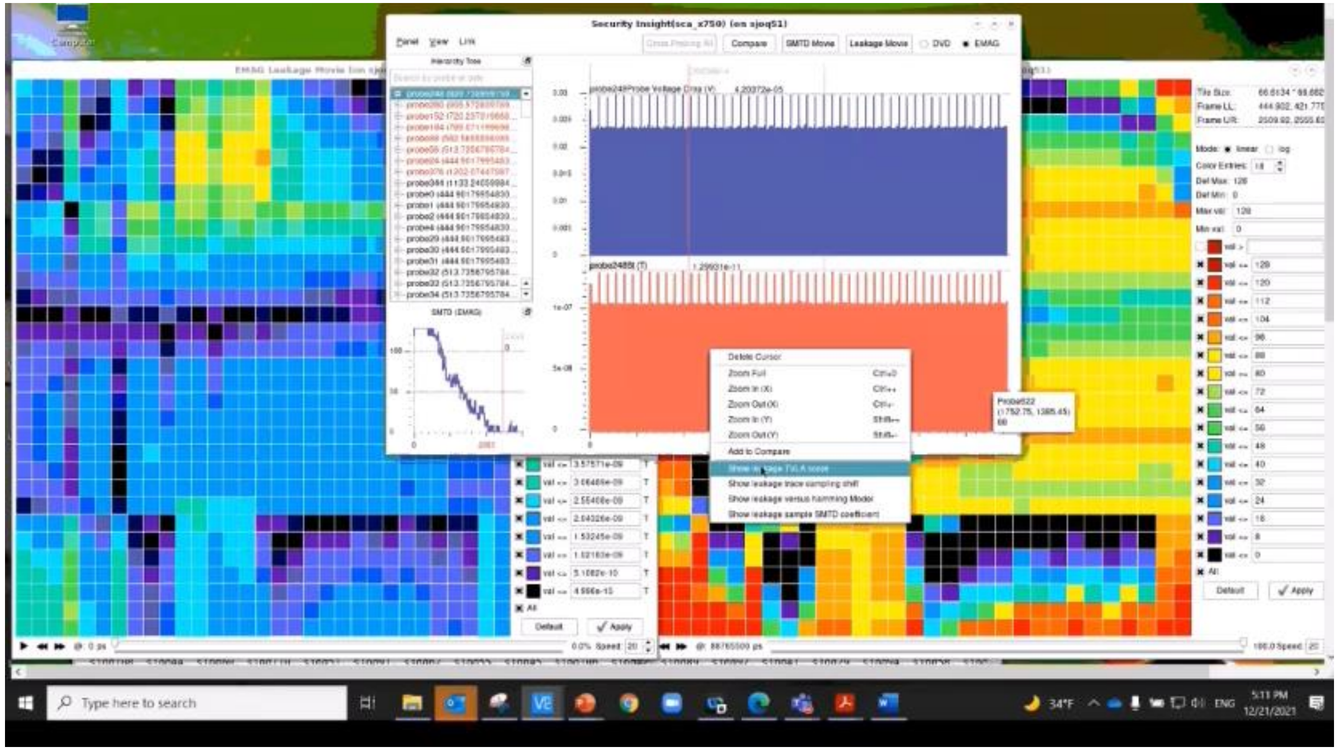
- EM field heatmap helps assess feasibility to measure leakage, but does not capture key disclosure
- The leakiest power side-channel location to disclose keys can be very different from EM location
- Fixing power side-channel leakage may not fully eliminate EM side-channel leakage



2.5D (Silicon Interposer)

3D Stacked IC

Physical model of different chip-package system integration methods

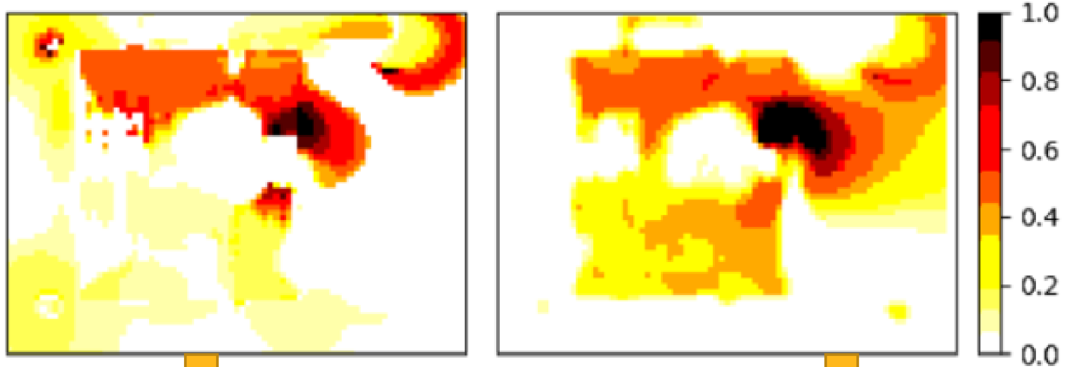


L. Lin, D. Selvakumaran, D. Zhu, N. Chang, C. Chow, M. Nagata, K. Monta, “Fast and Comprehensive Simulation Methodology for Layout-Based Power-Noise Side-Channel Leakage Analysis,” IEEE International Symposium on Smart Electronic Systems, **best paper**, 2020.

©2022 ANSYS, Inc.

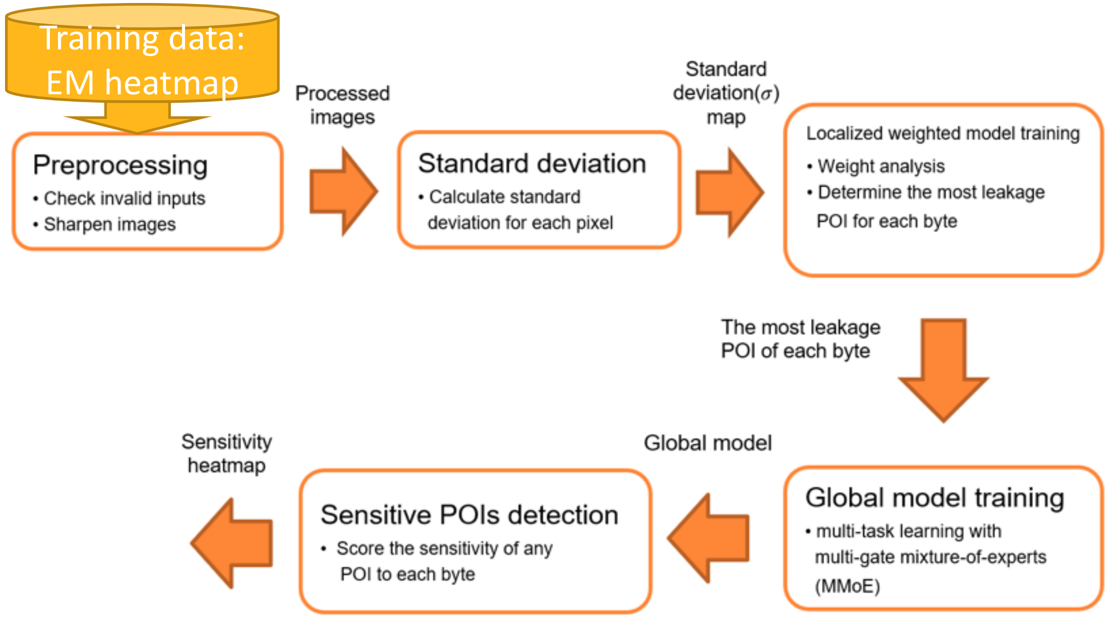
ML-based Auto-POI Identification

- Given a set of EM simulation traces at thousands of observation points, **<u>machine-learning based auto POI</u>** (point-of-interest) is a viable approach to reach key disclosure result
- Optimized flow shows much faster and scalable runtime over the traditional T-score and correlation-based statistical approach to disclose secret key bytes



Traditional CPA flow	Runtime with 16 workers
sensitivity score computation	67 hours
EMAG computation (50k traces)	157 hours 40 mins

ML-based auto POI flow	Runtime with 16 workers
sensitivity score computation	1 hours 20 mins
EMAG computation (~1k traces)	3 hours 30 mins



Preprocessing
- Check invalid inputs
- Sharpen images

Standard deviation
- Calculate standard deviation for each pixel

Localized weighted model training
- Weight analysis
- Determine the most leakage POI for each byte

Global model training
- multi-task learning with multi-gate mixture-of-experts (MMoE)

Sensitive POIs detection
- Score the sensitivity of any POI to each byte

☐ Automatically detects the sensitive POIs

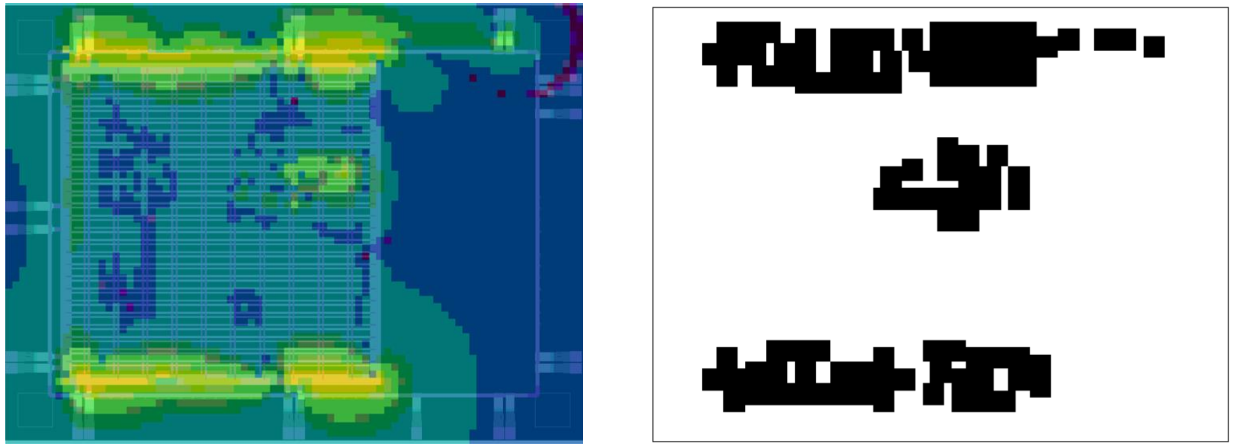
☐ Get the leakage contribution to each byte at the same time

☐ No dependency on the crypto block design

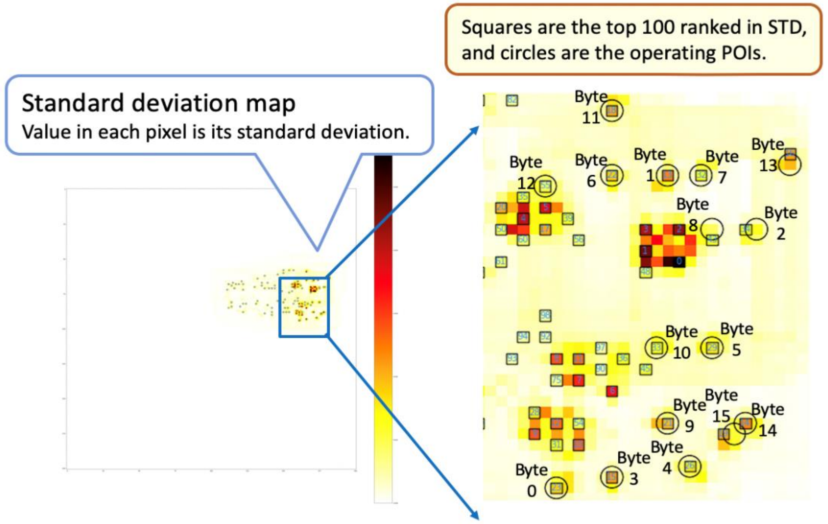
©2022 ANSYS, Inc.

Auto-POI Initial Filtering

- Goal
  - Efficiently and effectively find the initial vulnerable POIs from the original EM maps.
- Steps
  - Apply Laplacian filters in order to recover the original map without losing accuracy.
  - Calculate the standard deviation (STD) of every tile among all the traces.
  - Select top 100 ranked in the STD as inputs for the subsequent localized weighted model.



A typical example of an EM trace/map before and after the Laplacian filter.



Squares are the top 100 ranked in STD, and circles are the operating POIs.

Standard deviation map
Value in each pixel is its standard deviation.

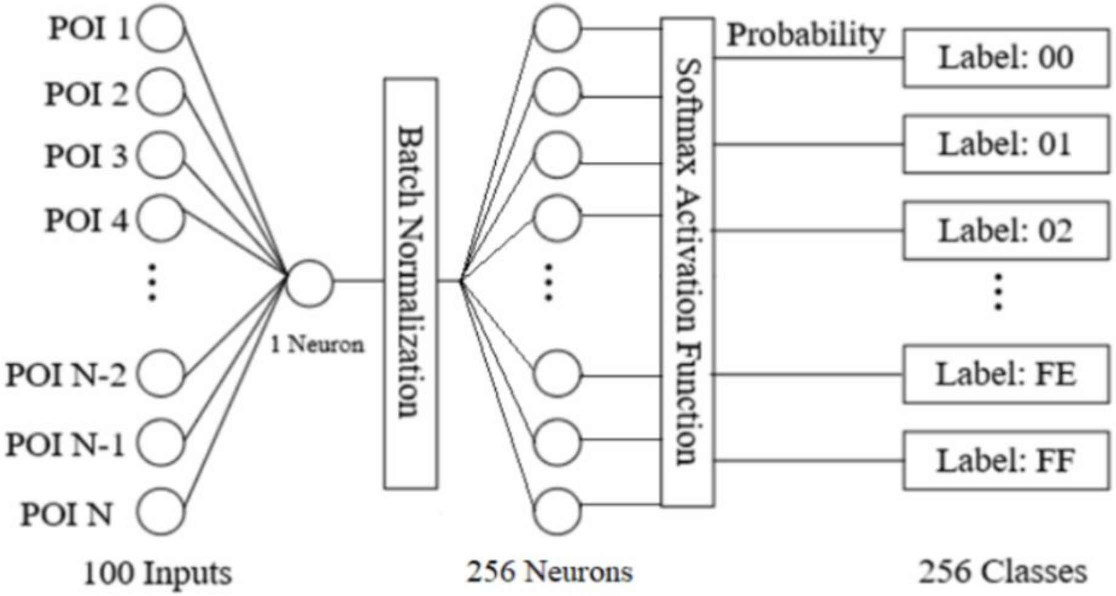
The locations of top 100 ranked in the STD

©2022 ANSYS, Inc.

Localized Weighted Model Training

- **Goal**
  - Find the most leakage tiles for each byte.
- **Steps**
  - Use 100 POIs as inputs to output the probability of the correct key for each byte.
  - Rank the most leakage probes for each byte by analyzing the incoming weights from single neuron in the hidden layer.

$$probability = prediction[Sbox(keyi) \oplus plaintext]$$

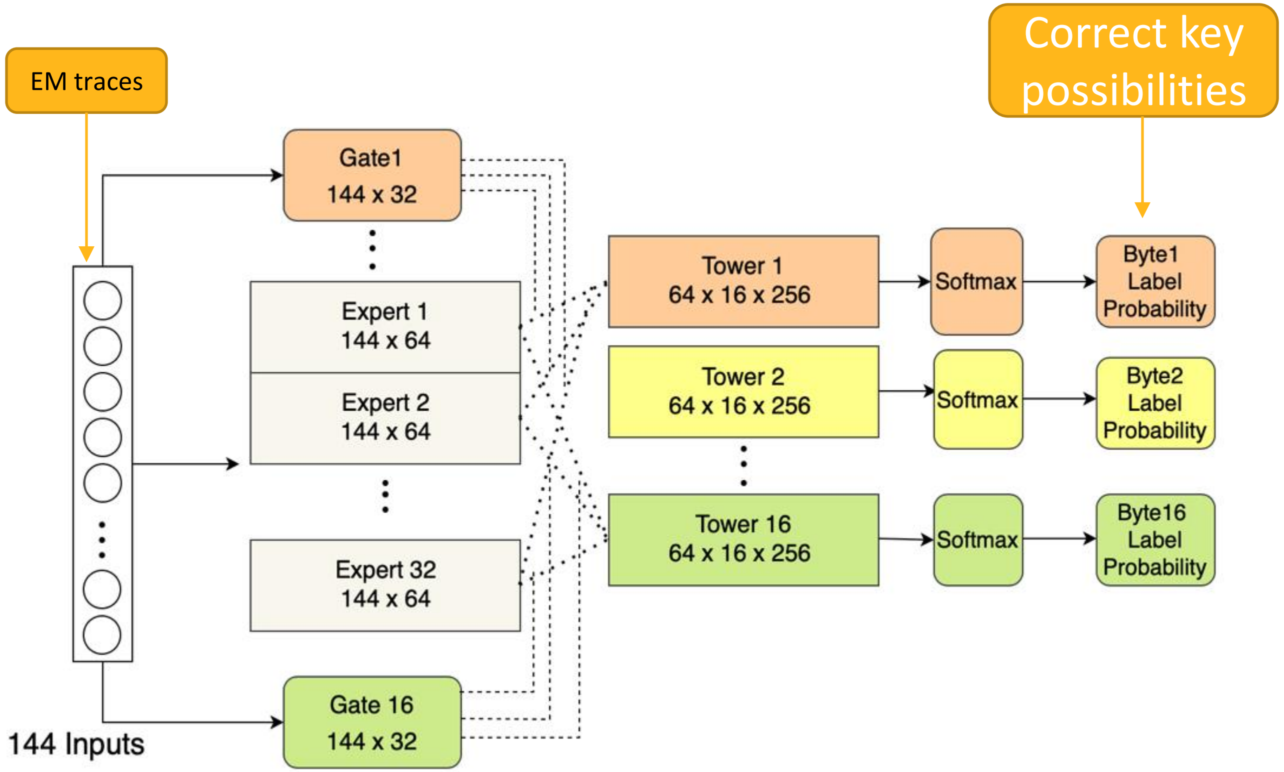


The structure of the localized weighted neural network

©2022 ANSYS, Inc.

Global Model Training

- Goal
    - Obtain better performance by a global model to identify all the bytes simultaneously
- Steps
    - Build global model based on MMoE and with DNN on individual byte
    - Concatenate features from the EMAG probes centered on the most vulnerable leakage POIs as input.



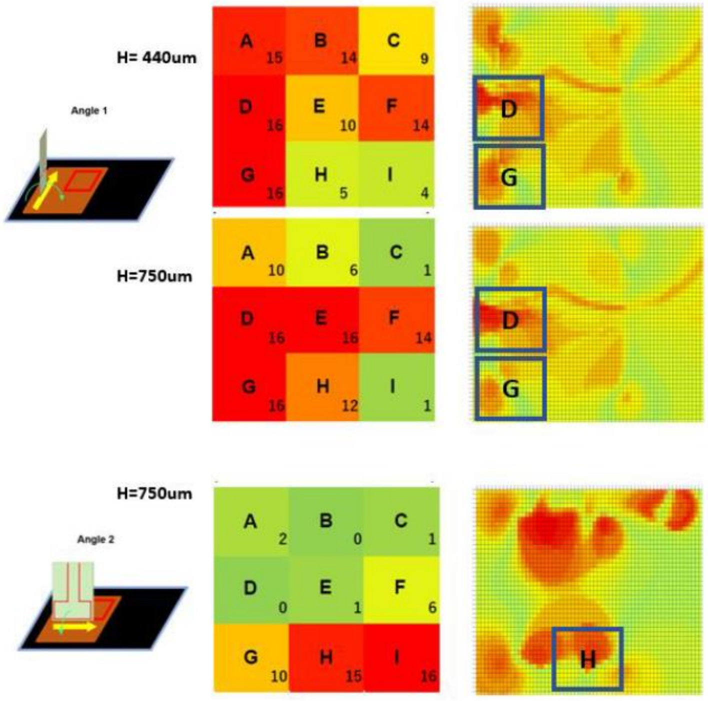
Structure of the global model based on MMoE for key disclosure of 16 bytes simultaneously from EM traces

Lin, L., Zhu, D., Wen, J., Chen, H., Lu, Y., Chang, N., Chow, C., Shrivastav, H., Chen, C.W., Monta, K. and Nagata, M., "Multiphysics Simulation of EM Side-Channels from Silicon Backside with ML-based Auto-POI Identification", best paper, HOST, *2021.*

©2022 ANSYS, Inc.

Silicon Correlation Study

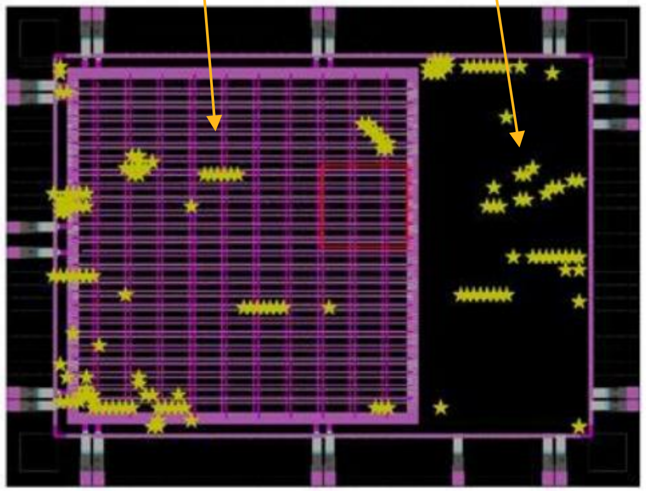
- Simulation gives sharp resolution while merging into 9 measurement regions.
- Correlating the design weakness regions: unprotected AES crypto core area and ring side metal
- Simulation result uncovers additional leakage regions than silicon, which turns out to be caused by silicon noise from the package routing => noise modeling in simulation is very flexible

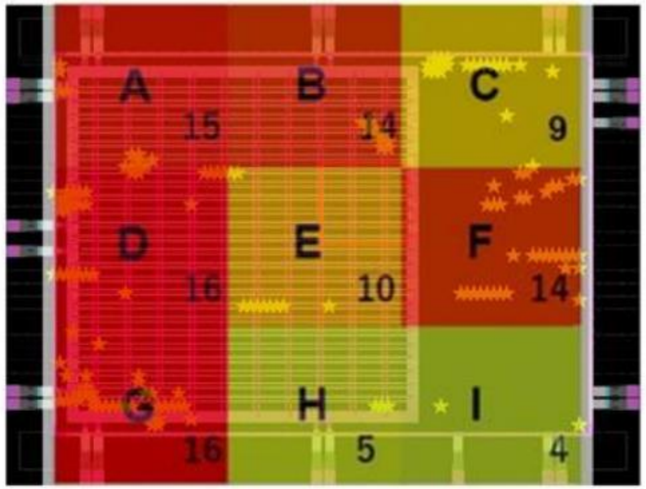


Silicon result Simulation result

AES testchip

On-die control logic & power management





Silicon result

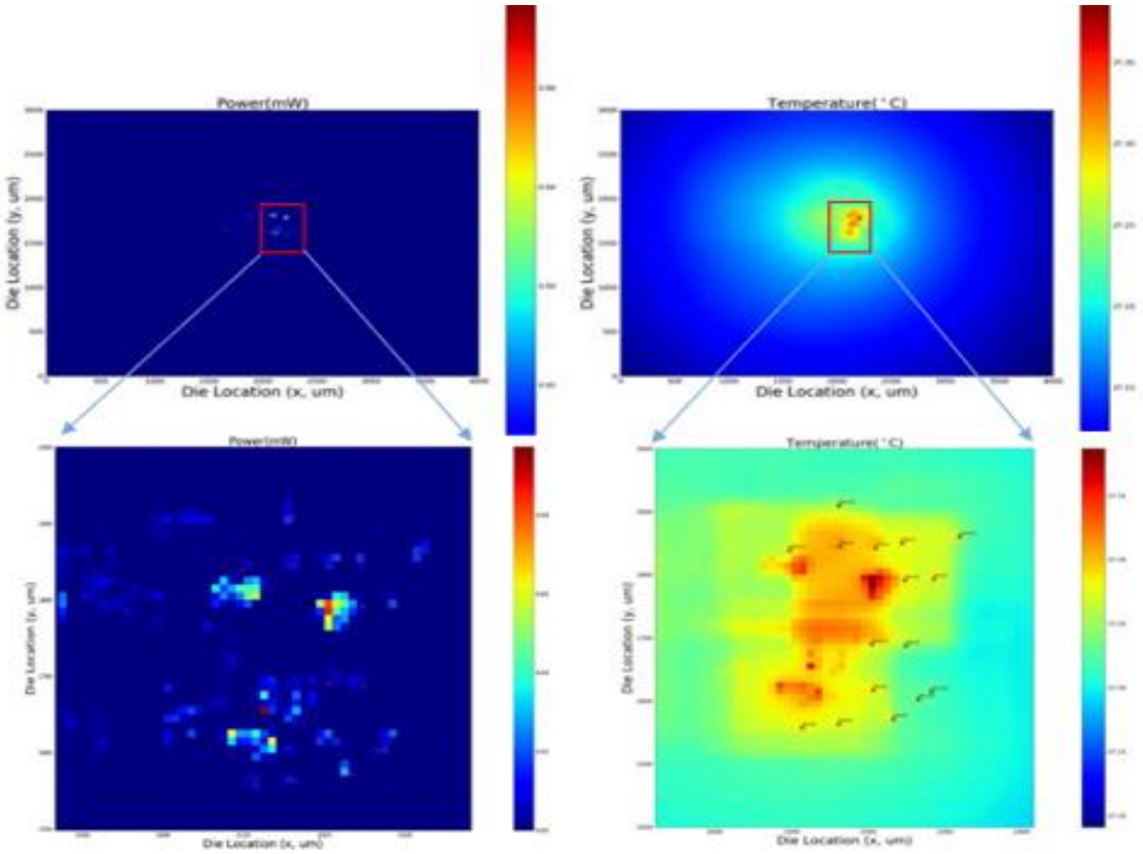
©2022 ANSYS, Inc.

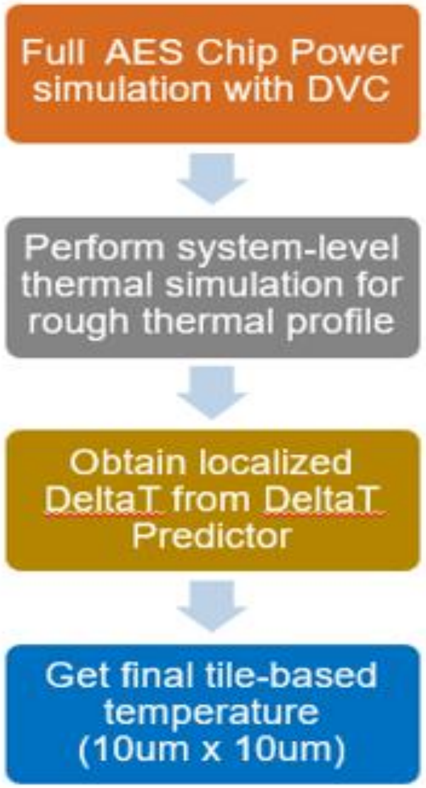
Agenda

- Background of EM and thermal side-channel analysis
- Simulation challenges and identification of POIs for EM side-channel analysis
- Simulation challenges and identification of POIs for thermal side-channel analysis
- Conclusion

©2022 ANSYS, Inc.

Location-dependent Device Level Power/Thermal Profiles as Side-channel





Full AES Chip Power simulation with DVC

Perform system-level thermal simulation for rough thermal profile

Obtain localized DeltaT from DeltaT Predictor

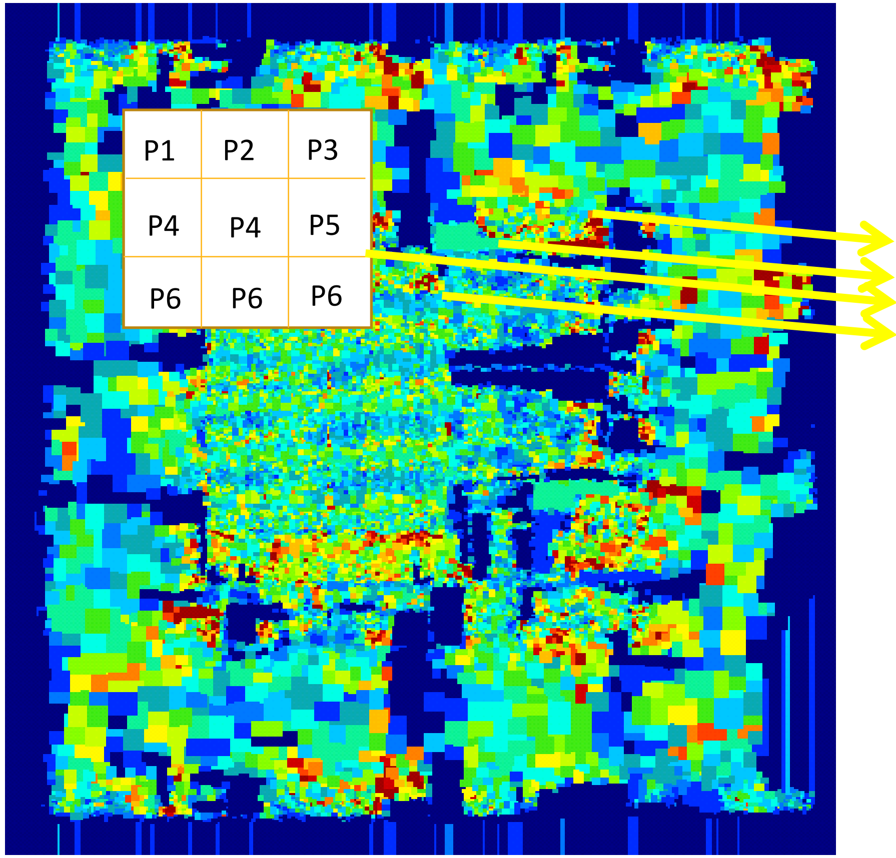
Get final tile-based temperature (10um x 10um)

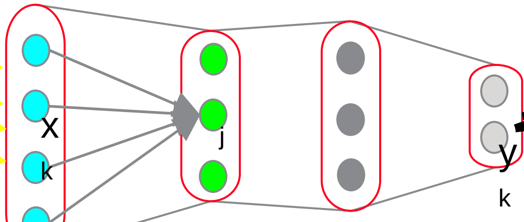
Tile-based power map with 10μmx10μm resolution (left) and thermal profile (right) of a 4mmx3mm AES test chip with 800k instances

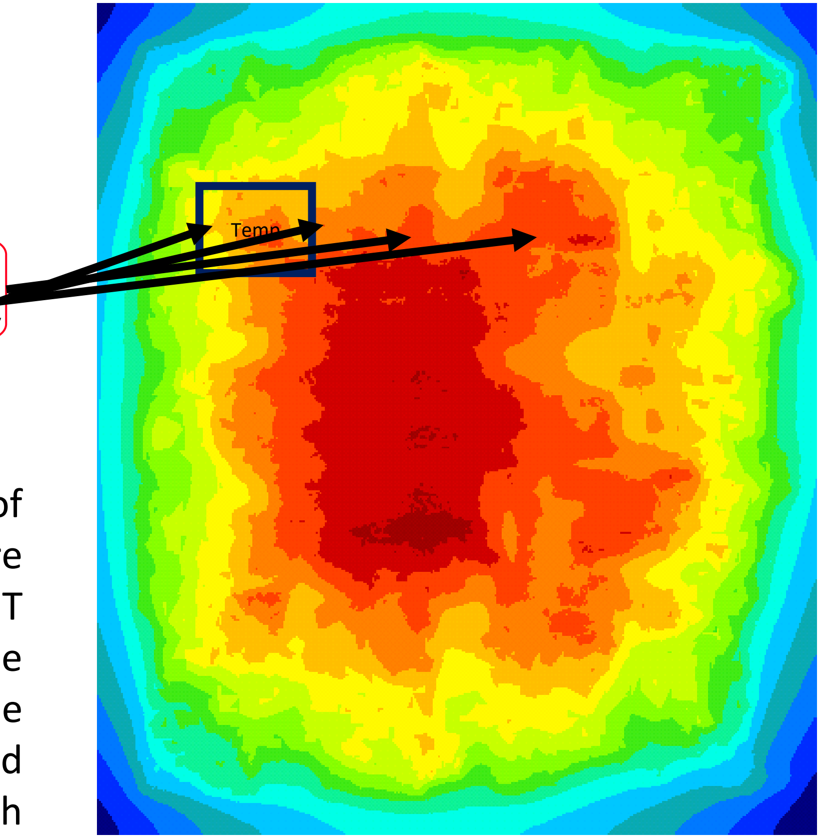
"ML-augmented Methodology for Fast Thermal Side-channel Emission Analysis", N. Chang, et al., ASP-DAC, 2021.

©2022 ANSYS, Inc.

Fast ML-based Static Thermal Solver for On-chip Temperature Calculation for Repeated Plaintext/Key Patterns







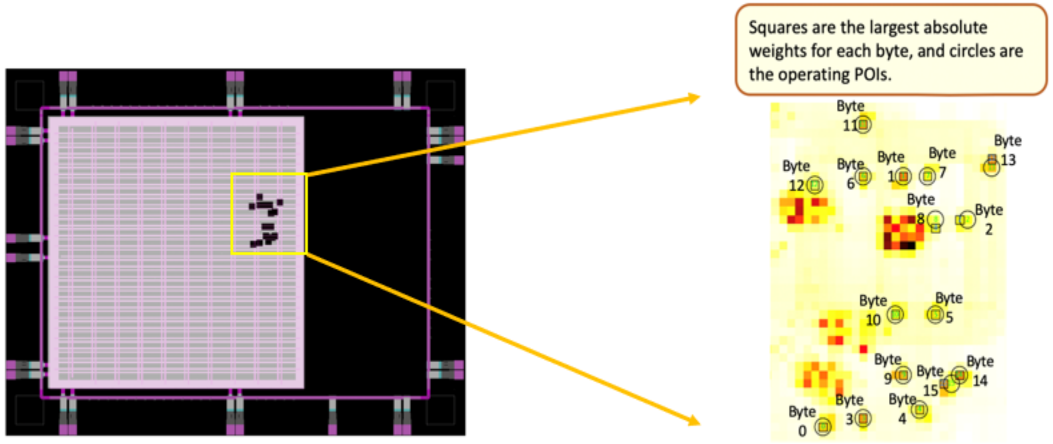
For each tile location, a set of tile powers and Theta-JA are input to the trained DeltaT Predictor to predict the temperature at the corresponding tile and added to the Temp from rough thermal profile

“DNN-based Fast Static Thermal Solver”, J. Wen, S. Pan, N. Chang, et al., IEEE SEMI-THERM and Nvidia GTC, 2020.

©2022 ANSYS, Inc.

Localized Weighted Model and Global Model Training

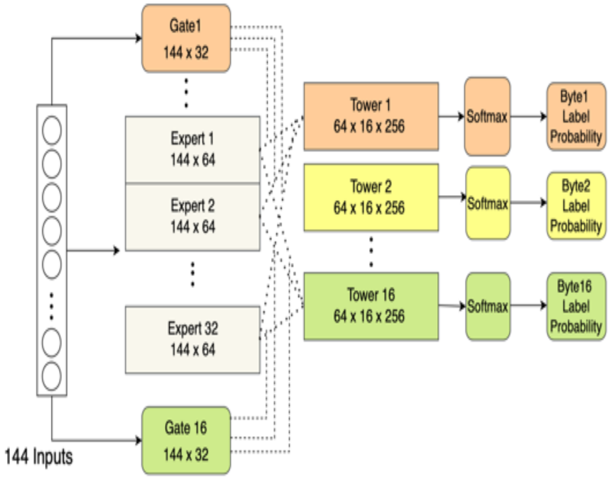
- After training, the POI with the largest weight is pretty close to the operating POI
- The POI with the largest weight is seen as the most vulnerable leakage POI



Squares are the largest absolute weights for each byte, and circles are the operating POIs.

The 16 most leakage POIs identified by the localized weighted model

- Goal
  - Obtain better performance by a global model to identify all the bytes simultaneously
- Steps
  - Build global model based on MMoE
  - Concatenate features from the 3x3 10um x 10um patterns centered on the most vulnerable leakage POIs as input.



Structure of the global model based on MMoE

“Security Integrity Analytics by Thermal Side-Channel Simulation: an ML-Augmented Auto-POI Approach”, J. Wen, N. Chang, et al., DesignCon, 2022.

©2022 ANSYS, Inc.

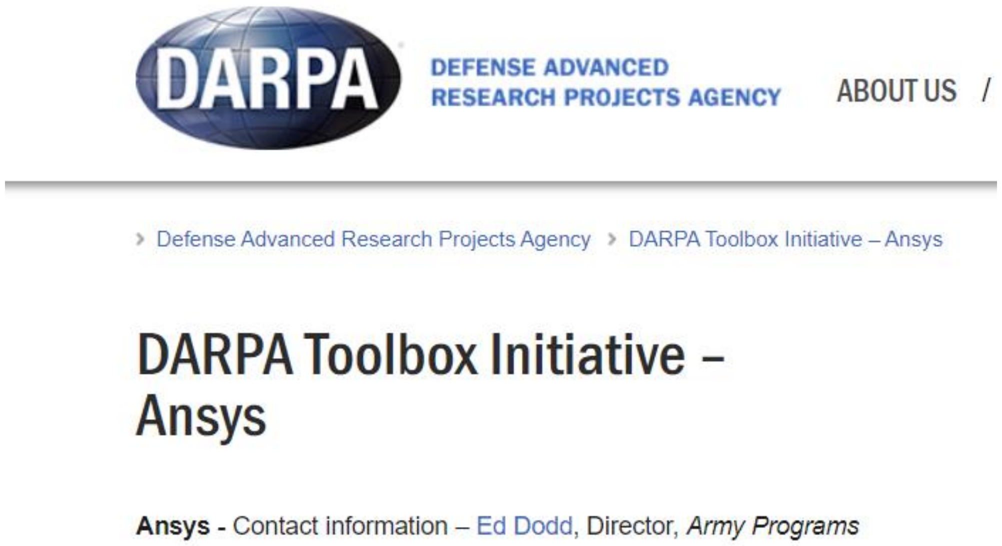
Conclusion

- A fast and accurate ML augmented multiphysics simulation platform with Auto-POI identification for EM and Thermal side-channel leakage analysis
- Identification of POIs are critical to assess the effectiveness of countermeasures for resisting both EM and Thermal side-channels
- Hardware security verification from backside is important for SoC and 3DIC designs
- Ansys security talks at DAC, 2022
  - “RTL Design Security Verification for Resisting Power Side-channel Analysis”, K. Monta, M. Nagata, L. Lin, J. Wen, P. Gupta, N. Chang, Design Track
  - “Emerging Opportunities in CAD for Security”, N. Chang, in New Directions in Silicon Solutions
  - Power and EM side-channel solution demo at Ansys booth

©2022 ANSYS, Inc.

Acknowledgement

- Thanks to Lang, Jimin, Hua, Weike, Gang, Jerome, Thomas, Harsh, Bo, Ozgur, Sreeja, Kayhan, Preeti, Akhilesh, Calvin, Ying, Youlin, and Gary for many discussions of side-channel and fault injection simulations
- Thanks to Nagata-san and Monta-san of Kobe University for RTL and layout-level power/EM side-channel discussion
- Thanks to Nitin, Henian, Farimah, and Mark of UFL for laser FI discussion
- Thanks to Gary, David, and Roger of NTU for thermal/FI ML discussion
- Also thanks to AFRL for the support of IDEAS project on power and EM SCLA



› Defense Advanced Research Projects Agency › DARPA Toolbox Initiative – Ansys

DARPA Toolbox Initiative – Ansys

Ansys - Contact information – Ed Dodd, Director, *Army Programs*

©2022 ANSYS, Inc.

Ansys