A Simulation Technique of Thermal Side-Channels from Cryptographic Circuits

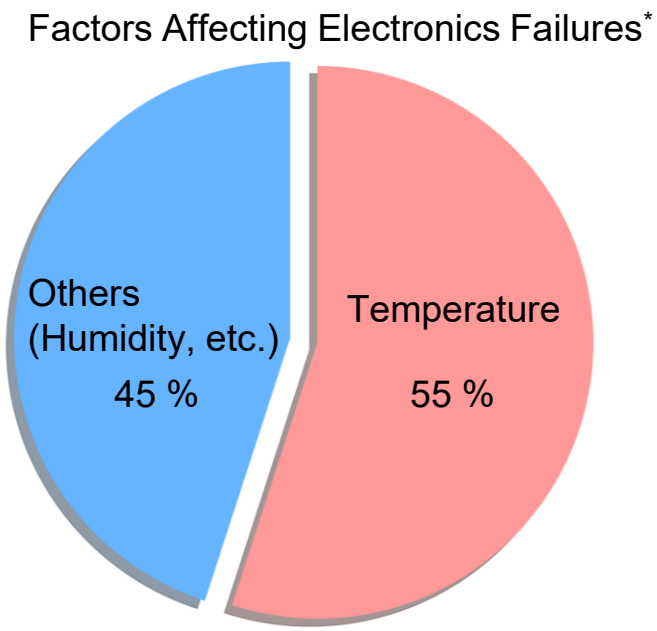
Shuhei Yokota[(1)], Rikuu Hasegawa[(1)], Kazuki Monta[(1)],
Takaaki Okidono[(1)], Takuji Miki[(1)], Makoto Nagata[(1)]
Lang Lin[(2)], Norman Chang[(2)]
[(1)]Kobe University , [(2)]ANSYS Inc.

62 THE CHIPS TO SYSTEMS CONFERENCE

SPONSORED BY CEDA® IEEE Council on Electronic Design Automation sigda acm

Thermal problem: Temperature Variations (TV)

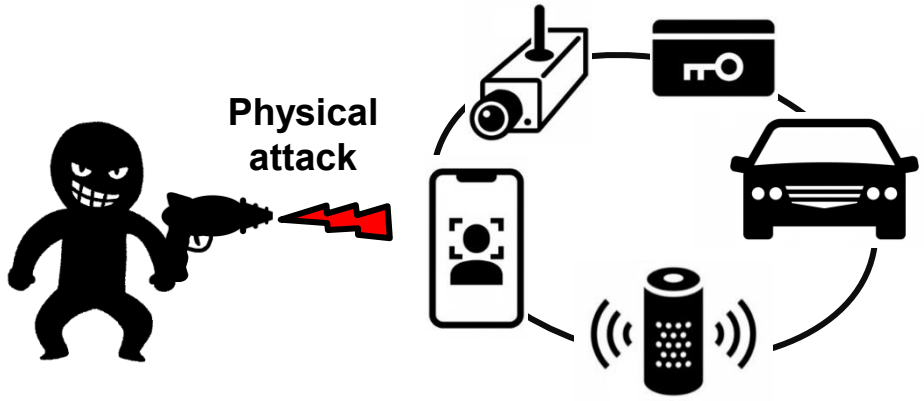
- Quality degradation by Temperature Variations (TV)
  - Majority of electronics failures are caused by heating.
  - Flip-chip structures used in heterogeneous integration are especially critical.
    - 3D:Hot spot
    - 2.5D:Thermal crosstalk



*Amol R. Dhumal, Atul P. Kulkarni, and Nitin H. Ambhore, *"A comprehensive review on thermal management of electronic devices,"Journal of Engineering and Applied Science*, vol. 70, Article 140, 2023. https://doi.org/10.1186/s44147-023-00309-2

Thermal problems: Thermal Side-Channels(TSC)

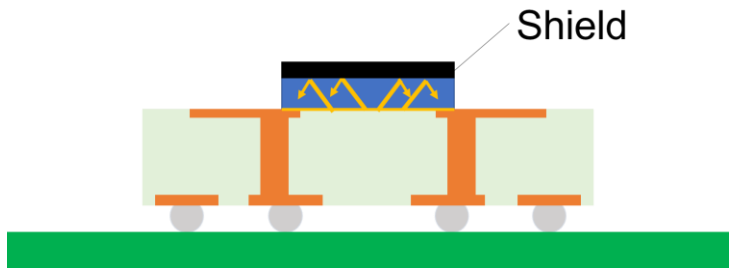
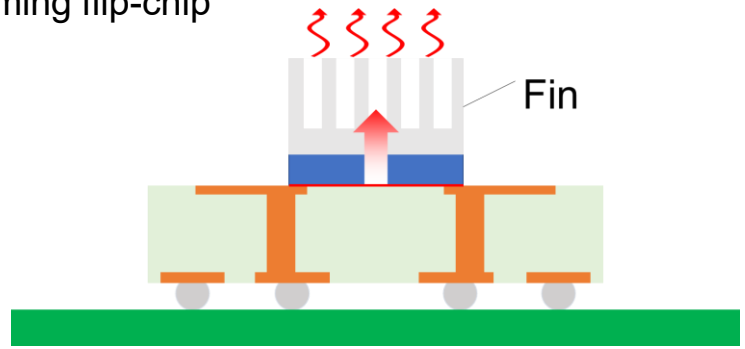
- Information leakage caused by Thermal Side-Channels* (TSC)
  - Side-channel analysis (SCA)
    - Physical information during cryptography operation
    - Example: **Electro magnetic(EM)** , current, etc…



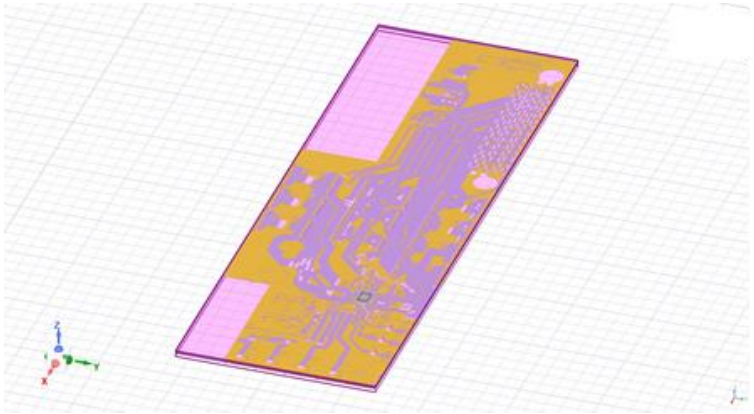
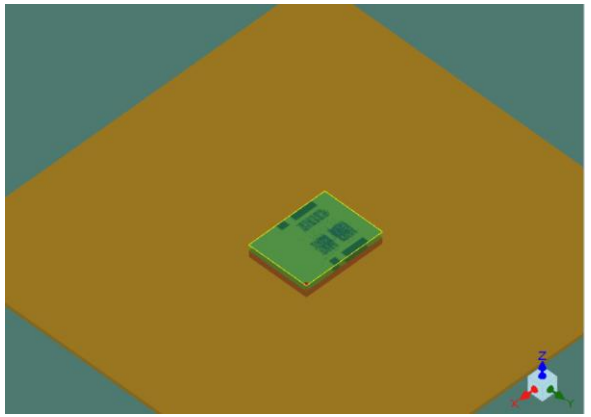
* Norman Chang,et al., ""ML-augmented Methodology for Fast Thermal Side-channel Emission Analysis "Proceedings of the 26th Asia and South Pacific Design Automation Conference (ASP-DAC), 2021.https://doi.org/10.1145/3394885.3431641

Countermeasures for thermal problems

- Thermal management is important for semiconductor

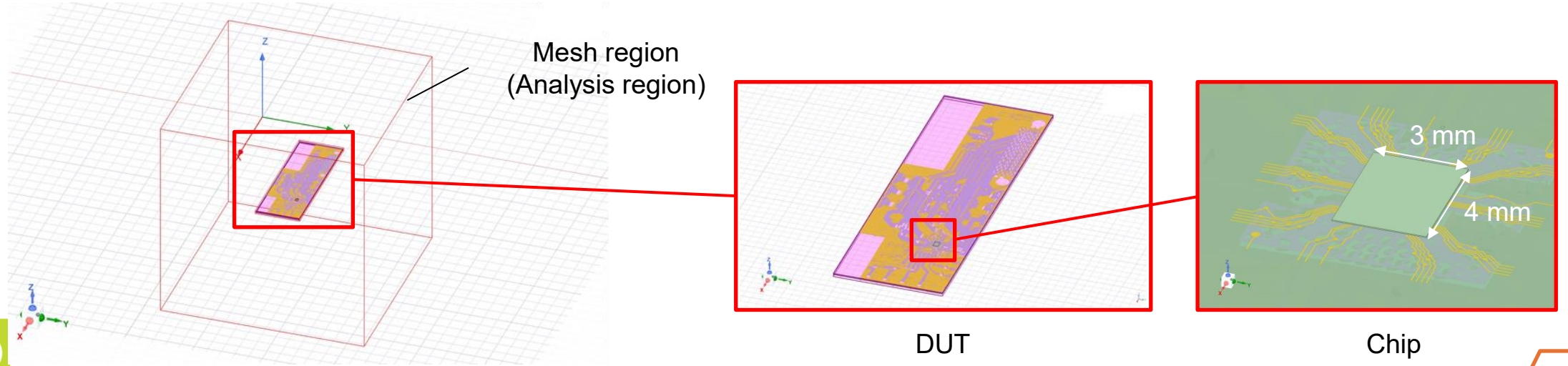
EM problems	Thermal problems
Assuming flip-chip 	Assuming flip-chip 
Problems: Interference, Side channel leakage(SCL) Countermeasures: Preventing emissions using shield	Problems: Quality degradation, SCL Countermeasures: Dissipating heat using fins =>**Can SCL be mitigated by heat dissipation?**

Hierarchical simulation approaches

System level thermal simulation (Overall area)	**IC chip level thermal simulation** (Localized heat sources and paths)
	
✓By incorporating package structures, thermal behavior of the entire system can be analyzed. =>Observing overall area	✓ By incorporating circuit data, in-plane thermal behavior can be analyzed. =>Observing heat generation locality

Proposed system level thermal simulation

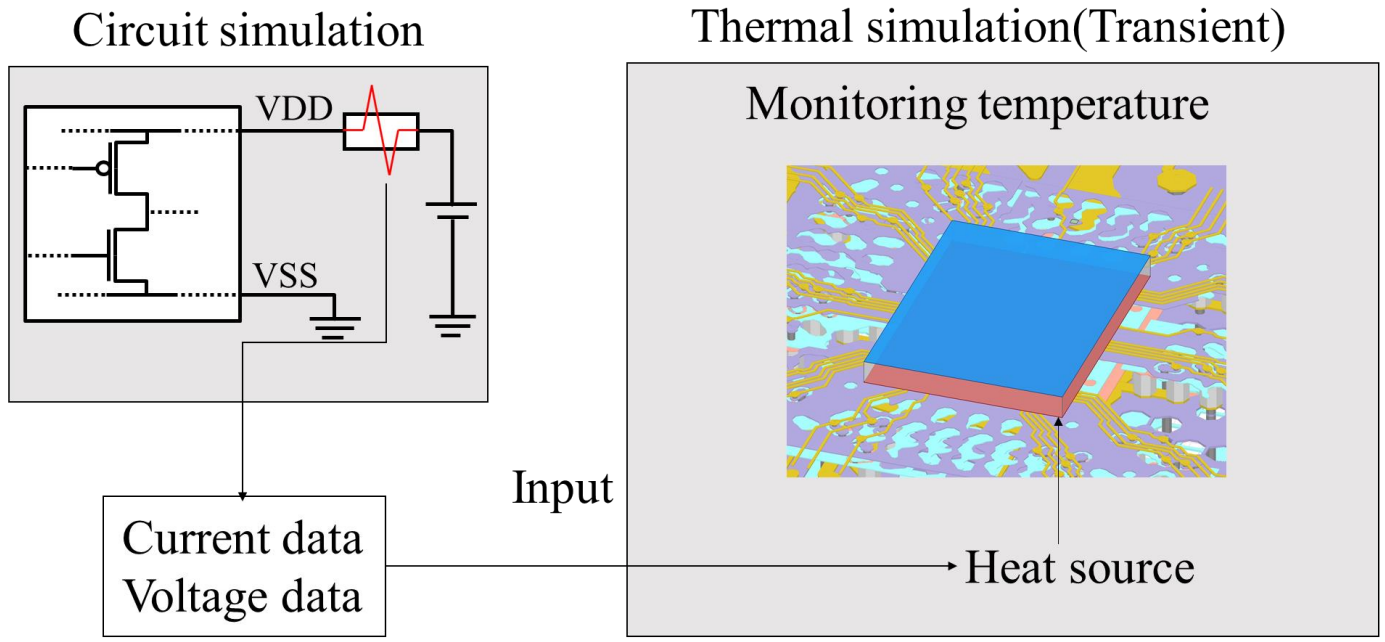
- Transient thermal flow simulation is done.
  - Simulating 3 modes of heat transfer (Conduction, Convection, Radiation)
- Enables simulation of overall area



System level thermal simulation model

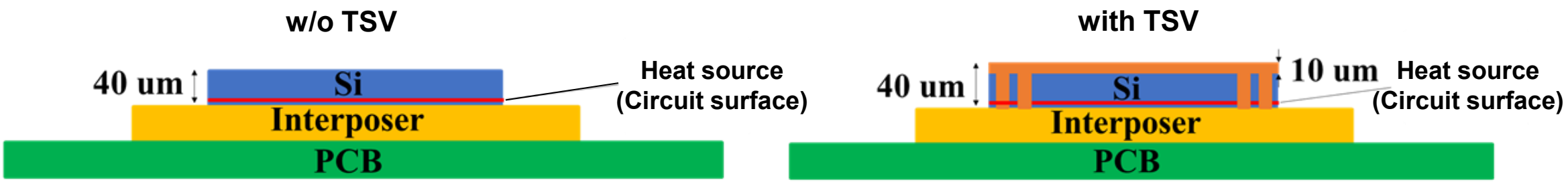
Simulation flow

- Current and voltage are obtained from circuit simulation during AES, and used to calculate heat generation.
- The heat source is assumed to be uniformly distributed over the entire circuit surface.



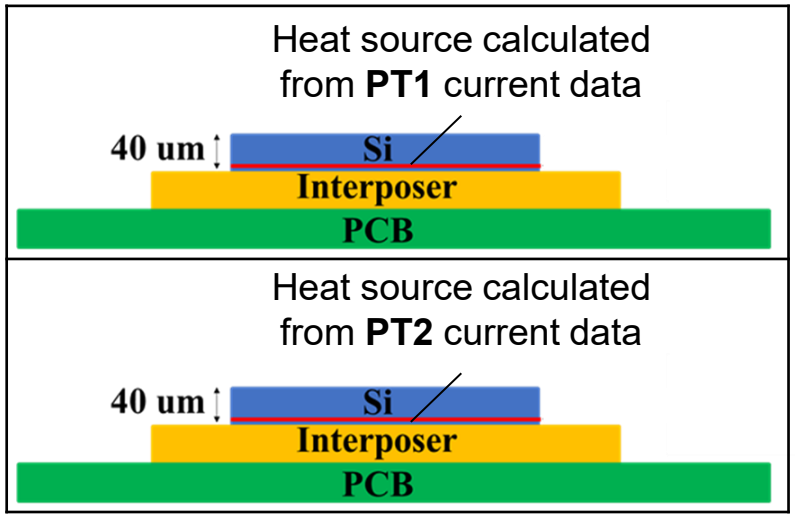
Thermal suppression using TSV

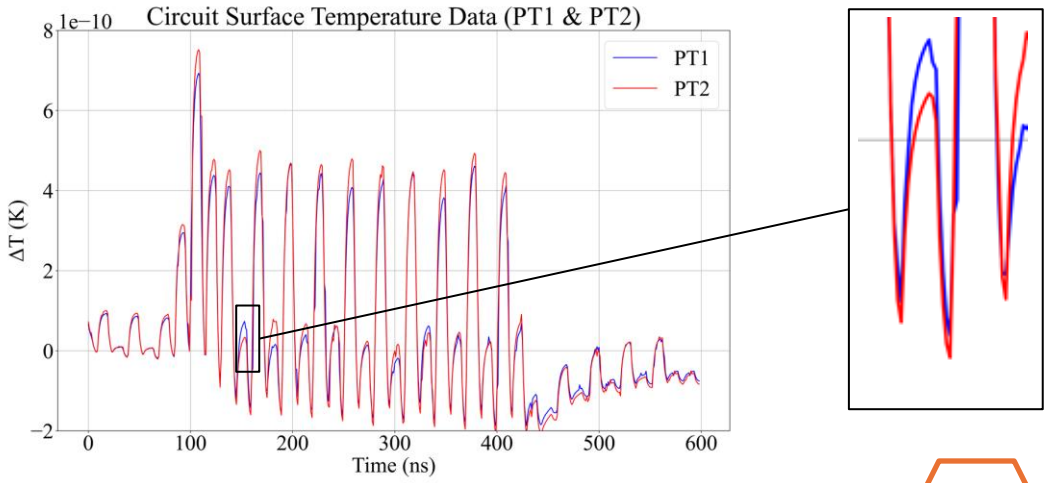
- Two models were prepared
  - w/o TSV
  - with TSV
- Assessing temperature variations and leakage suppression by TSVs



Interpretation of temperature data

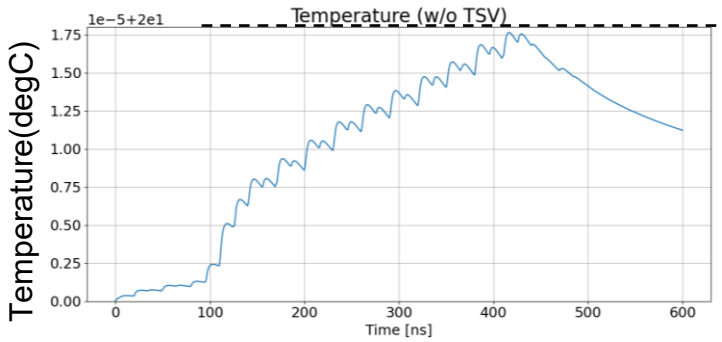
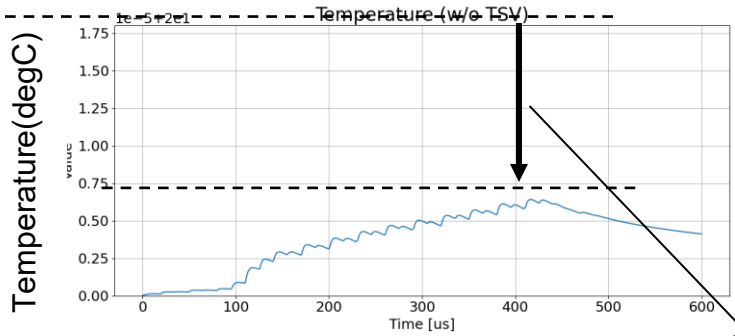
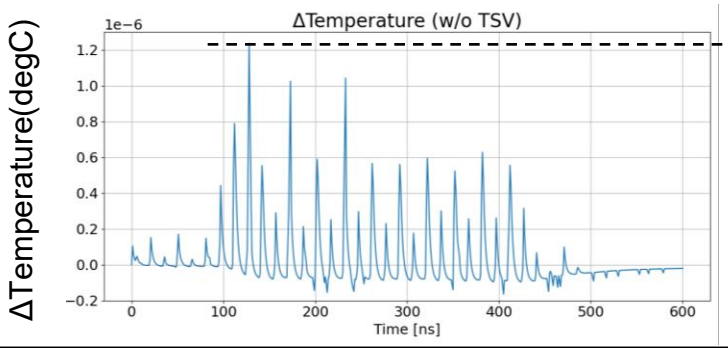
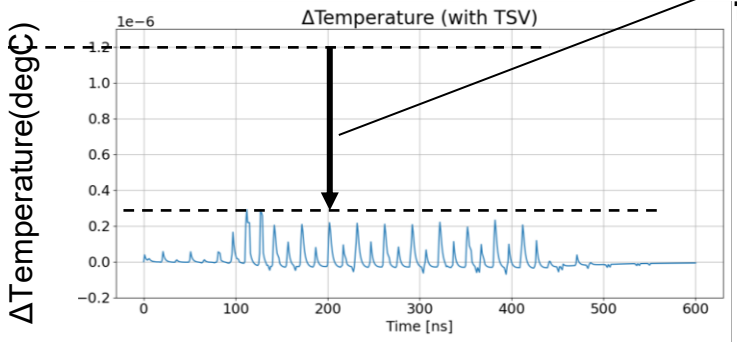
- Variations in current lead to corresponding changes in temperature variations.
- Time derivative of temperature is used to infer circuit behavior.
- In fact, plaintext (PT) dependent behavior was observed in time derivative of circuit surface temperature.





Time derivative of temperature(Circuit surface)

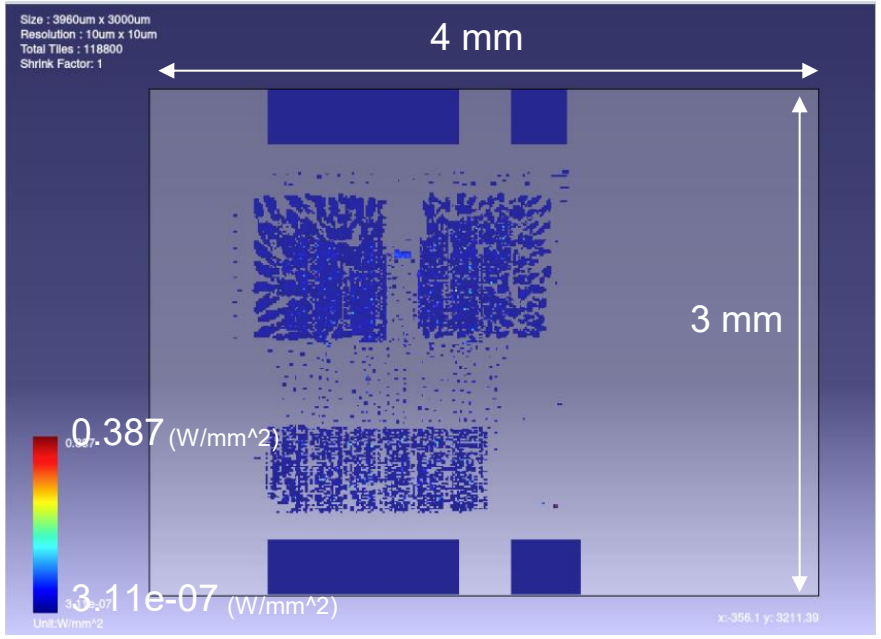
Simulation results

	w/o TSV	with TSV
Temperature variation on the circuit surface		
Time derivative of temperature on the circuit surface		

✓**TSVs contribute to suppress thermal**

Proposed IC chip level thermal simulation

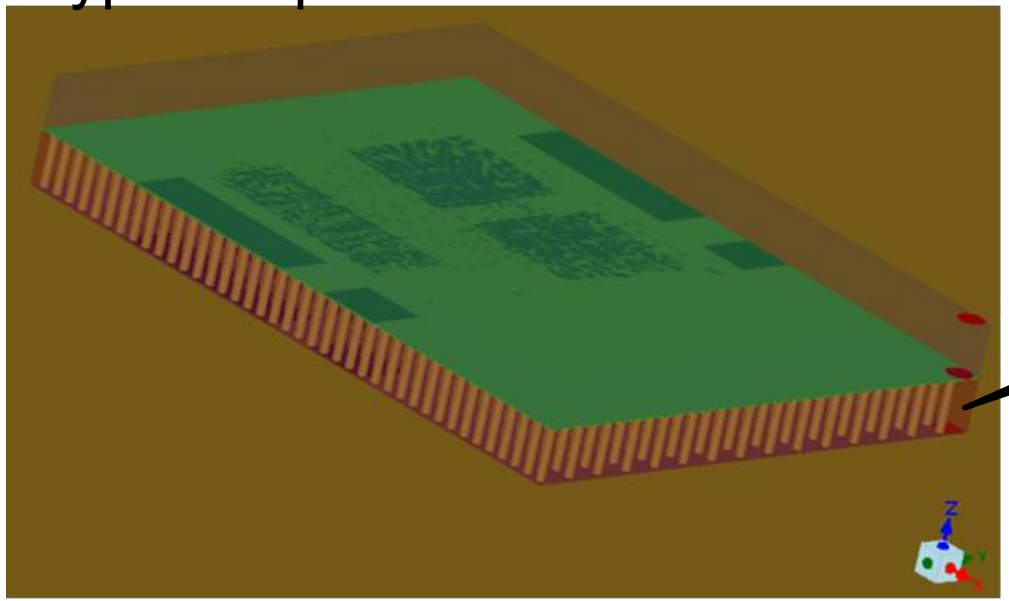
- AES design with 6 metal layers
- 10 μm x 10 μm tile resolution for chip thermal model (CTM) generation
- This size is same as system level thermal simulation's one.

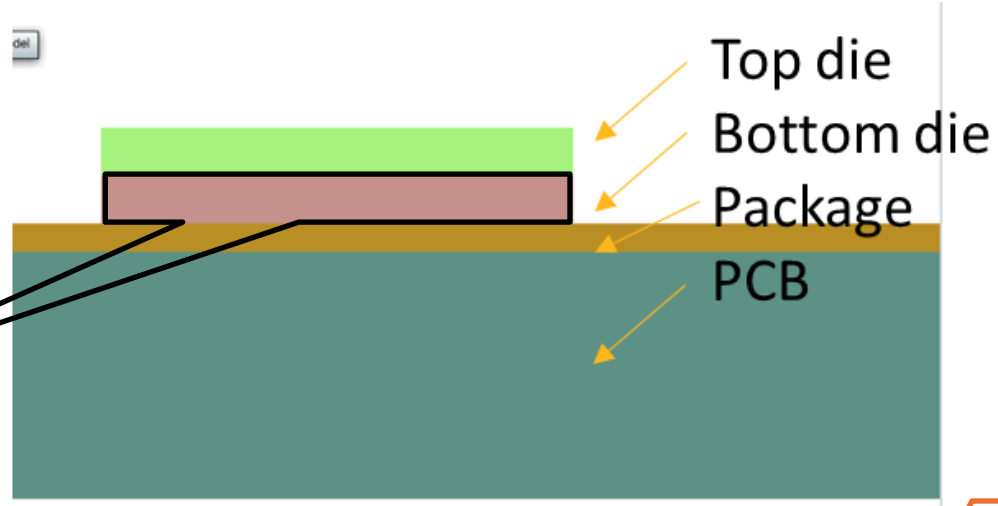


Layout power map

System assembly and thermal simulation

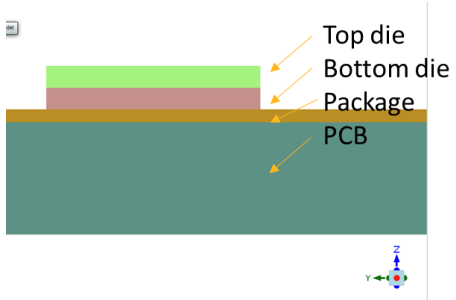
- Transient thermal simulation is done.
- To study the TSVs impact on thermal vertical coupling, TSVs are inserted between two dies. The top die has no activity while the bottom die has encryption operation.

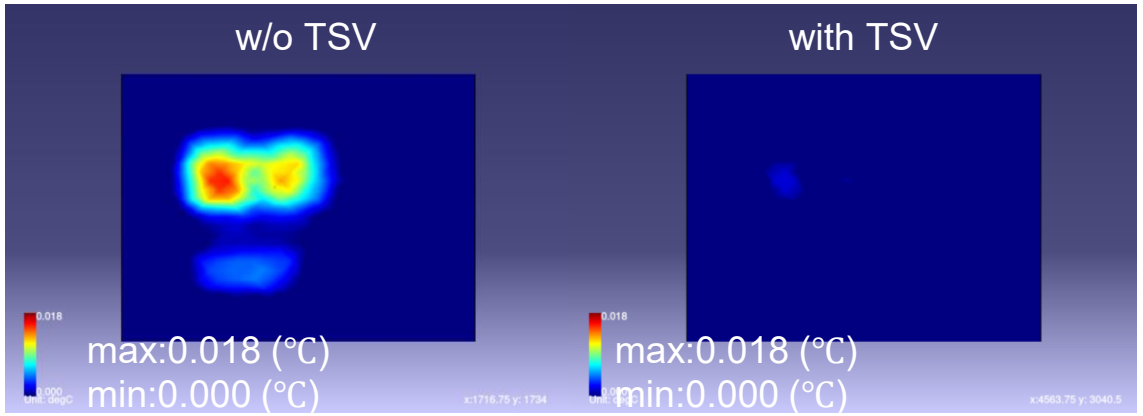




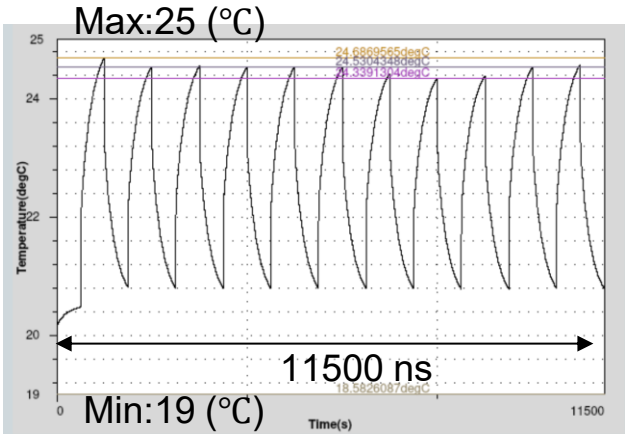
IC chip level thermal simulation results

- Strong thermal coupling between top die and bottom die is seen from the case with TSVs.
- With TSVs, thermal side-channel simulation is performed on 10+ AES encryption transactions
  - Each transaction has 16 cycles of 30 ns (clock period) → 480 ns
  - To reach the system thermal equilibrium state, repeat the duration of each transactions





Difference of top and bottom die



Transient thermal result with 10+ AES transactions observed on top die

Discussion

- Introducing heat dissipation paths such as TSVs can suppress thermal problems at front-side circuits.
  - Temperature variation
  - Information leakage
- Heat dissipation paths may increase the risk of leakage from other regions.
- Time derivative of temperature is extremely small and high frequency.
- If such variations become observable, thermal side-channel attacks could pose a serious threat.

Summary

- Established thermal simulation technique
  - System level thermal simulation
  - IC chip level thermal simulation
- A potential trade-off relationship between heat dissipation and leakage
  - By introducing heat dissipation paths (TSVs)
- We will investigate the observability of temperature variations using simulations and experimental measurements.