UCSB Scalable and Energy-Efficient Architecture Lab (SEAL)

Thermal-aware 3D Design for Side-channel Information Leakage

Peng Gu[1], Dylan Stow[1], Russell Barnes[1], Eren Kursun[2], and Yuan Xie[1]

University of California, Santa Barbara[1] , Columbia University[2]

UC Santa Barbara
Scalable Energy-efficient
Architecture Lab

https://seal.ece.ucsb.edu/

Columbia University

UC SANTA BARBARA
engineering

Outline

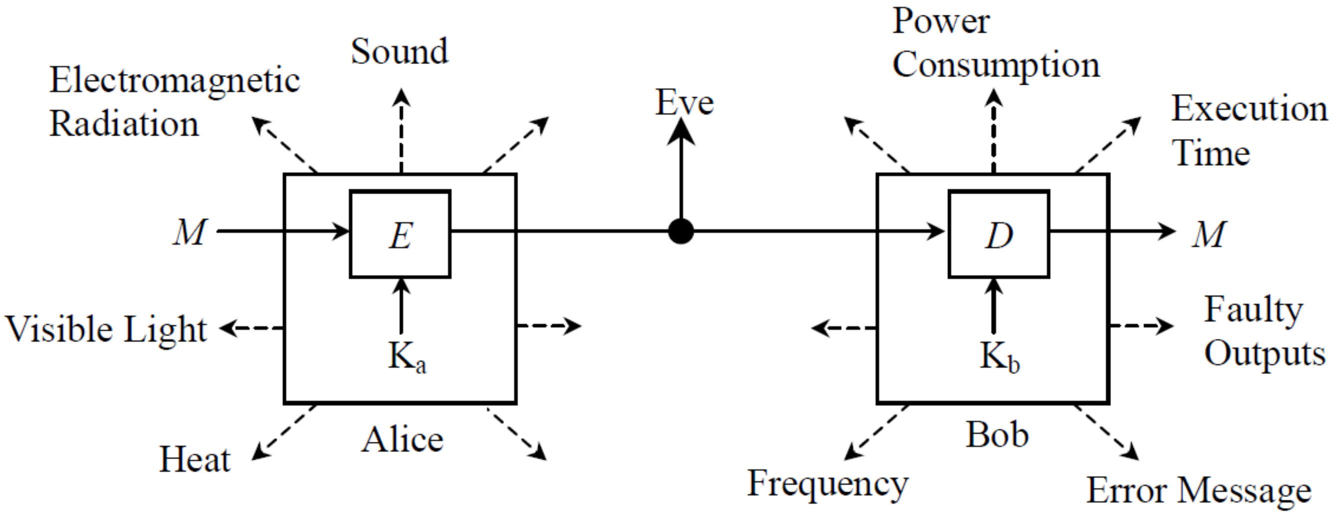
- Background and Key Idea
    - Thermal Side-channel Attack
    - 3D Integration
- Metric
    - Side-channel Vulnerability Factor
    - Spatial Thermal Side-channel Factor
- Our Design
    - Thermal-aware Side-channel Shielding Layer
    - Dynamic Shielding Pattern Generation Algorithm
- Experimental Results

Outline

- Background and Key Idea
- Metric
- Our Design
- Experimental Results

Background: Thermal Side-Channel Attack

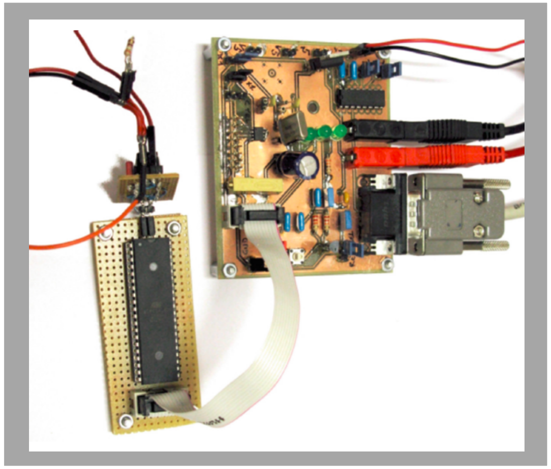
- Side-channel Attack
  - Attackers could take advantage of **unexpected information leakage** through physical side-channels (e.g., timing, power, EM, sound…)



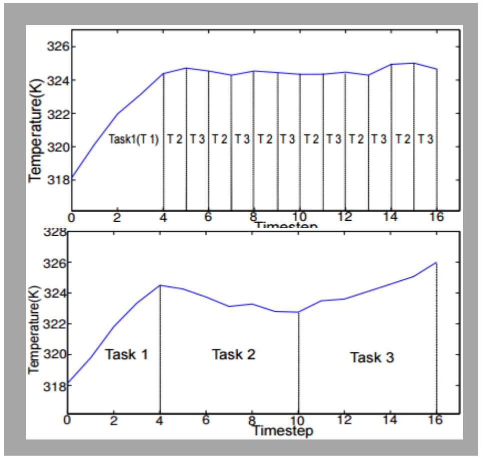
[Zhou, IACR’05]

Background: Thermal Side-Channel Attack

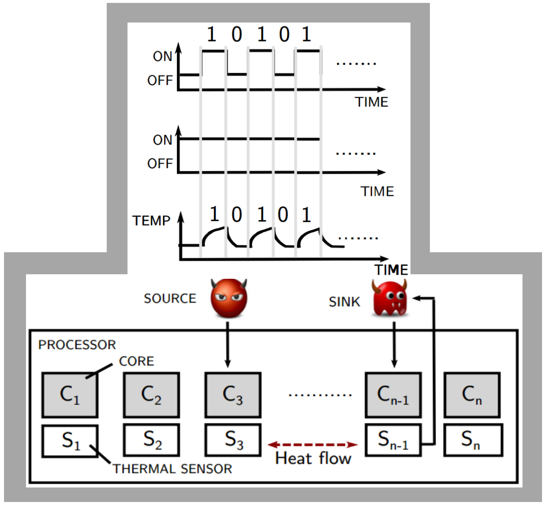
- Thermal Side-Channel Attack is an emerging threat
  - ➢Availability of highly sensitive on-chip and off-chip thermal sensors and infrared cameras → **stand-alone attack**



Use low-cost thermal sensor to get thermal profile for encryption parameters [Hutter,SCRAA'14]



Analyze the task scheduling sequence [Bao,TrustED'14]



A covert communication channel for transferring sensitive information [Masti,usenix'15]

Background: Thermal Side-Channel Attack

- Thermal Side-Channel Attack is an emerging threat
  - ➢Availability of highly sensitive on-chip and off-chip thermal sensors and infrared cameras → **stand-alone attack**
  - ➢Techniques to calculate power consumption from temperature distribution → **enhance existing attack methods** (e.g., Differential Power Analysis).

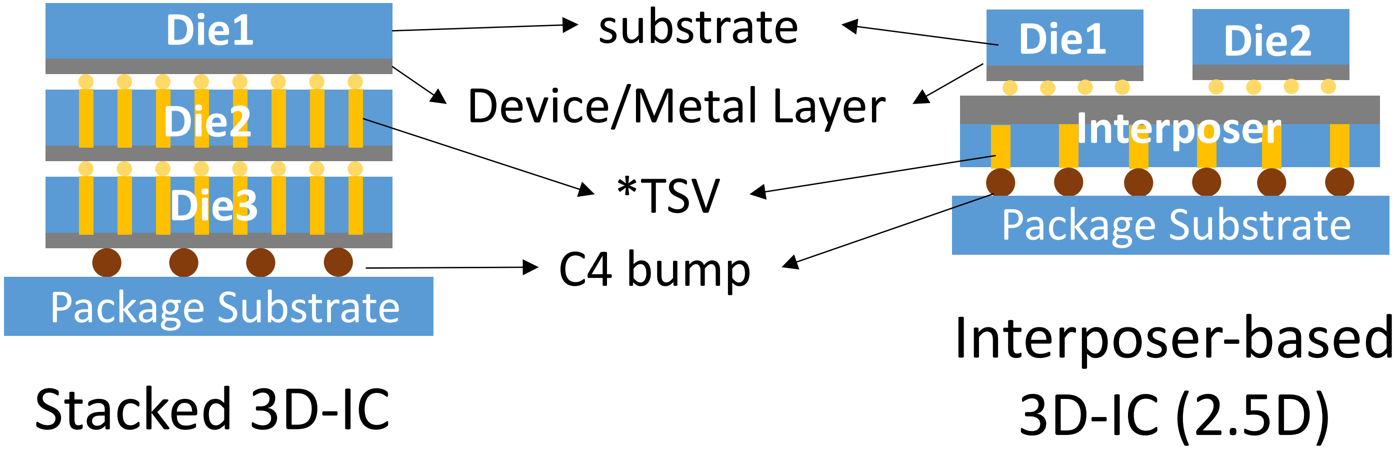
Background: Thermal Side-Channel Attack

- Existing methods:
  - ➢**Software techniques**: aperiodic tasks scheduling [Bao,TrustED'14] restrict access to on-chip thermal sensors [Masti,USENIX'15]
    - ***Cannot fully protect from thermal side-channel leakage***
  - ➢**Hardware techniques**: randomized power supply noise injection [Benini,DAC'03]
    - ***Considerable hardware or power overhead***

Background: 3D stacking for security

- 3D integration

  ➢ Allow multiple dies to be stacked vertically through TSV or connected in an interposer



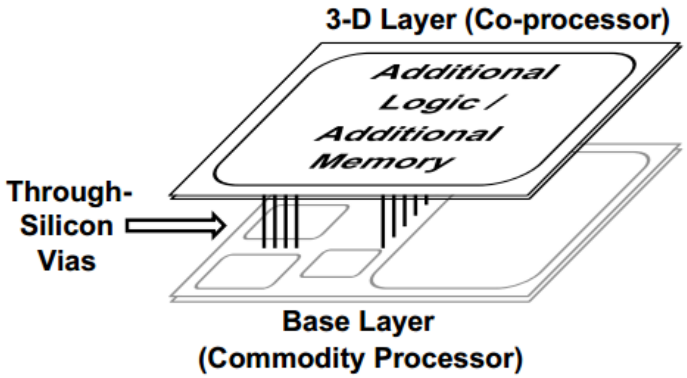
Stacked 3D-IC

Interposer-based 3D-IC (2.5D)

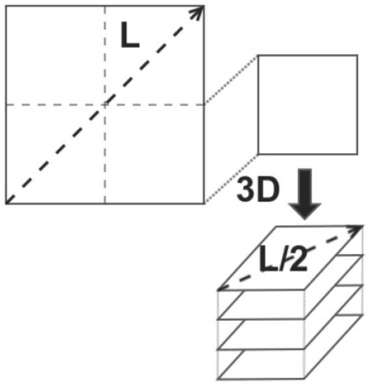
*TSV: Through-Silicon-Via

Background: 3D stacking for security

- Die-stacking structure could be utilized for hardware security enhancement:
  - *Invasive attacks* (e.g., 3D layer could not be removed)
  - *Semi-invasive attacks* (e.g., depackaging is not useful for 3DIC)
  - *Non-invasive attacks* (e.g., 3DIC could prevent timing side-channel attack)


3-D Layer (Co-processor)
Additional Logic / Additional Memory
Through-Silicon Vias
Base Layer (Commodity Processor)

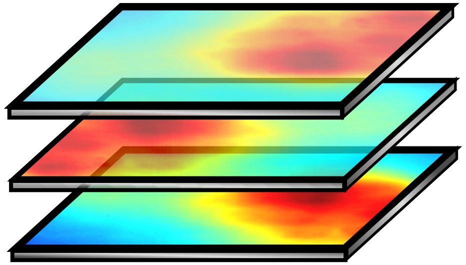
3D Secure Co-processor [Valamehr,CSFTA'12]



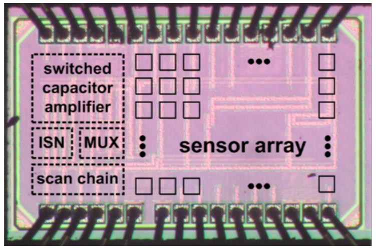
3D Design for Cache-timing Side-channel Attack [Bao,ICCD'15]

Key Idea

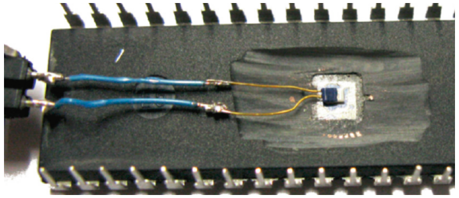
- Utilizing 3D integration to dynamically camouflage the activity in device layers:
  - Intelligent on-chip controller to track key activity patterns
  - Dynamic shielding patterns generation
  - Thermal aware and energy efficient



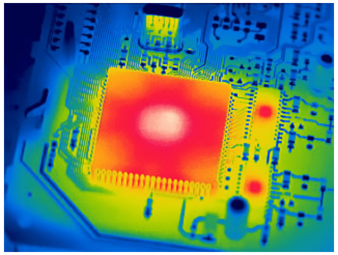
- The proposed scheme can fully protect Thermal Side-channel Attack from three attacking modes:



Built-in Thermal Sensors



External Thermal Sensors



IR Thermal Imaging

Outline

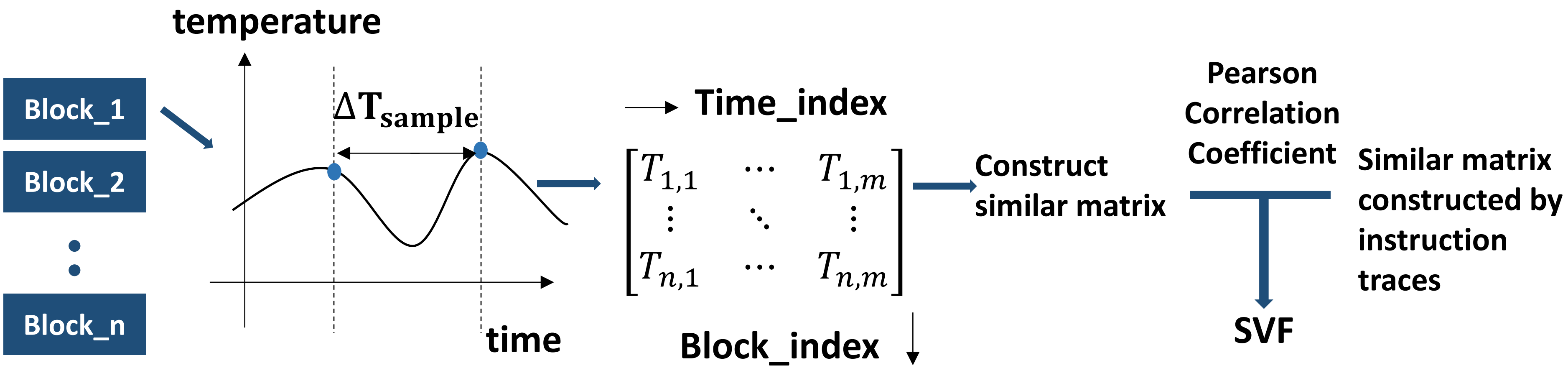
- Background and Key Idea
- Metric
- Our Design
- Experimental Results

Metric

- Side-channel Vulnerability Factor (SVF) [Demme,ISCA'12]
  - ➢ Correlation between the ***chip's actual execution patterns*** and the attacker's ***observations of side-channel information***.
  - ➢ SVF ∈ $[0,1]$, The *smaller* the SVF, the more *secure* the system.

Secret information: the **instruction traces**

Side-channel information: **temperature traces**



$$\begin{bmatrix} T_{1,1} & \cdots & T_{1,m} \\ \vdots & \ddots & \vdots \\ T_{n,1} & \cdots & T_{n,m} \end{bmatrix}$$

Construct similar matrix

Pearson Correlation Coefficient

Similar matrix constructed by instruction traces

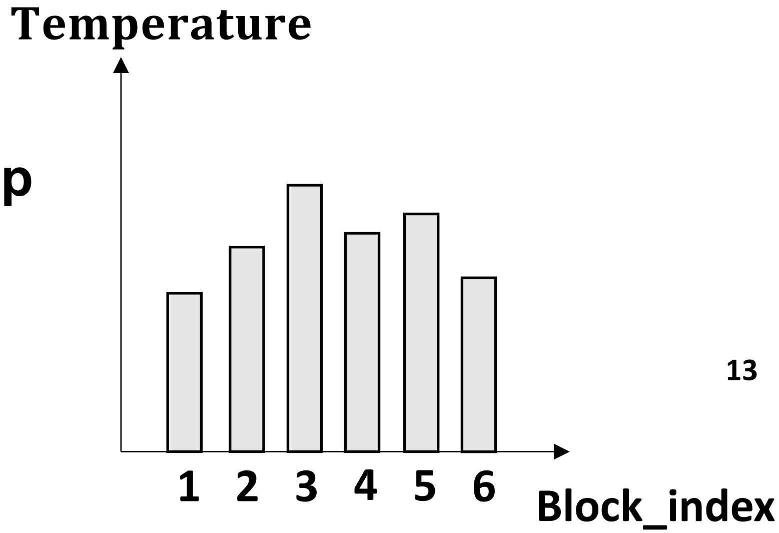
SVF

Metric

- Spatial Thermal Side-channel Factor (STSF)
  - Information may be leaked if the **spatial temperature distribution** among different blocks is acquired.
  - STSF measures the loss of information of **temperature distribution** after noise injection
  - STSF ∊ $[0,1]$, The *smaller* the STSF, the more *secure* the system.

Secret information: **relative relationship of the original temperature traces**

Side-channel information: **observed temperature traces**

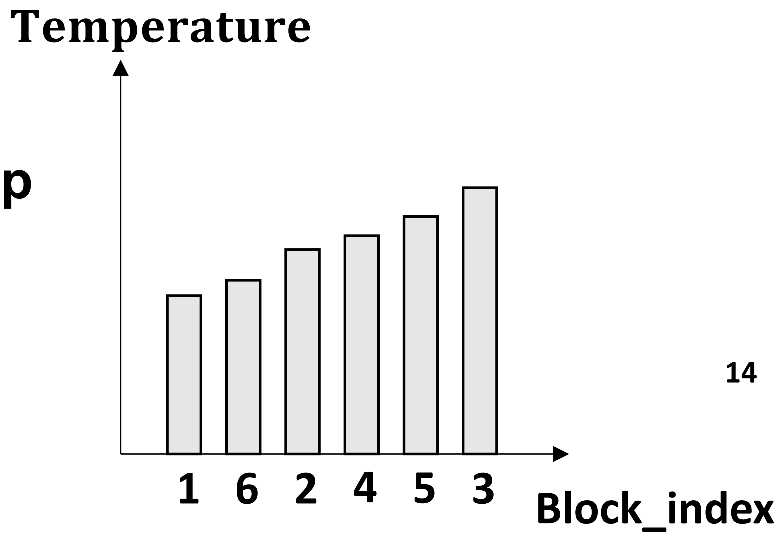


Metric

- Spatial Thermal Side-channel Factor (STSF)
  - Information may be leaked if the **spatial temperature distribution** among different blocks is acquired.
  - STSF measures the loss of information of **temperature distribution** after noise injection
  - STSF $\in [0,1]$, The *smaller* the STSF, the more *secure* the system.

Secret information: **relative relationship of the original temperature traces**

Side-channel information: **observed temperature traces**

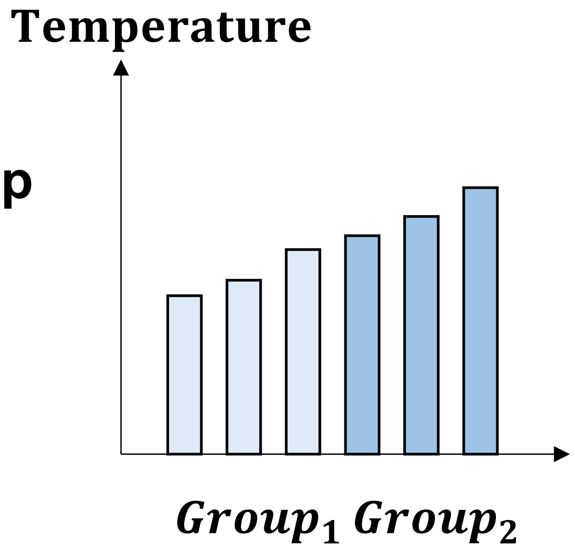


Metric

- Spatial Thermal Side-channel Factor (STSF)
  - Information may be leaked if the **spatial temperature distribution** among different blocks is acquired.
  - STSF measures the loss of information of **temperature distribution** after noise injection
  - STSF $\in [0,1]$, The *smaller* the STSF, the more *secure* the system.

Secret information: **relative relationship of the original temperature traces**

Side-channel information: **observed temperature traces**

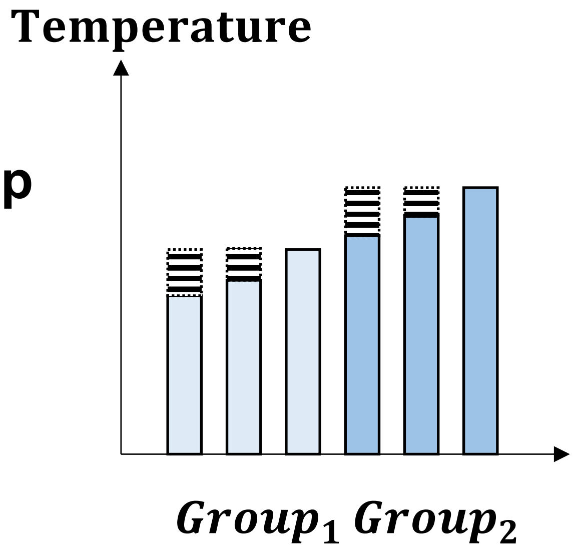


Metric

- Spatial Thermal Side-channel Factor (STSF)
  - Information may be leaked if the **spatial temperature distribution** among different blocks is acquired.
  - STSF measures the loss of information of **temperature distribution** after noise injection
  - STSF $\in [0,1]$, The *smaller* the STSF, the more *secure* the system.

<u>Secret information</u>: **relative relationship of the original temperature traces**

<u>Side-channel information</u>: **observed temperature traces**



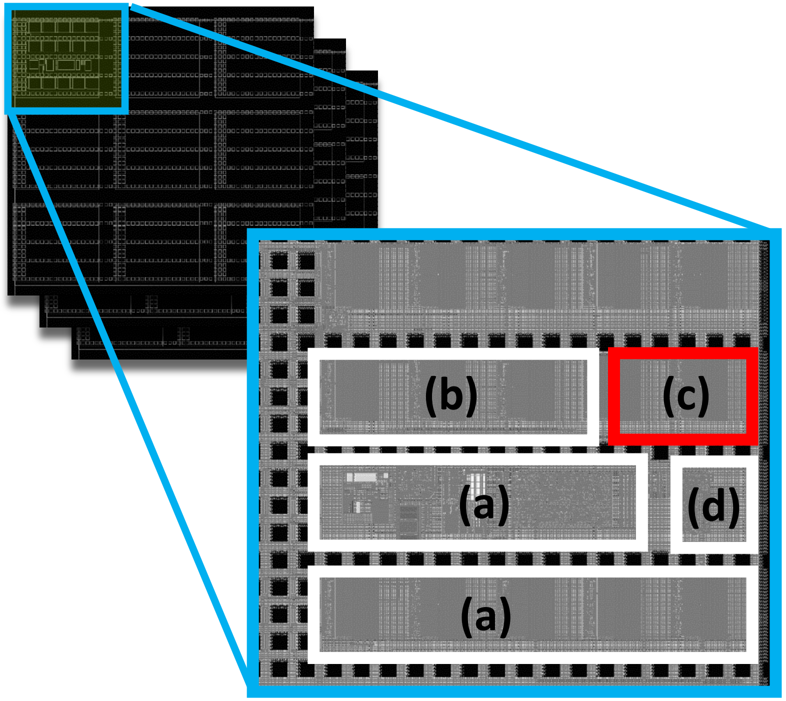
Outline

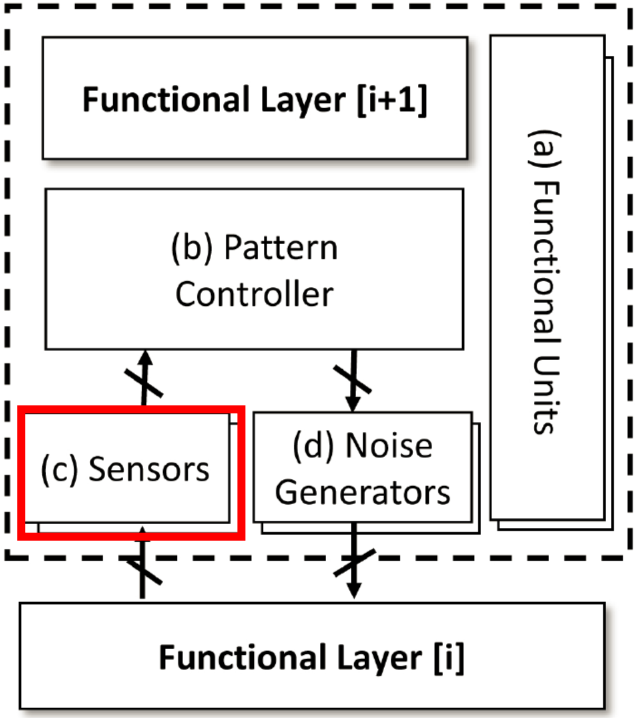
- Background and Key Idea
- Metric
- Our Design
- Experimental Results

Architecture Level Design

- Thermal-aware Side-channel Shielding Layer Designs

3D-TASCS



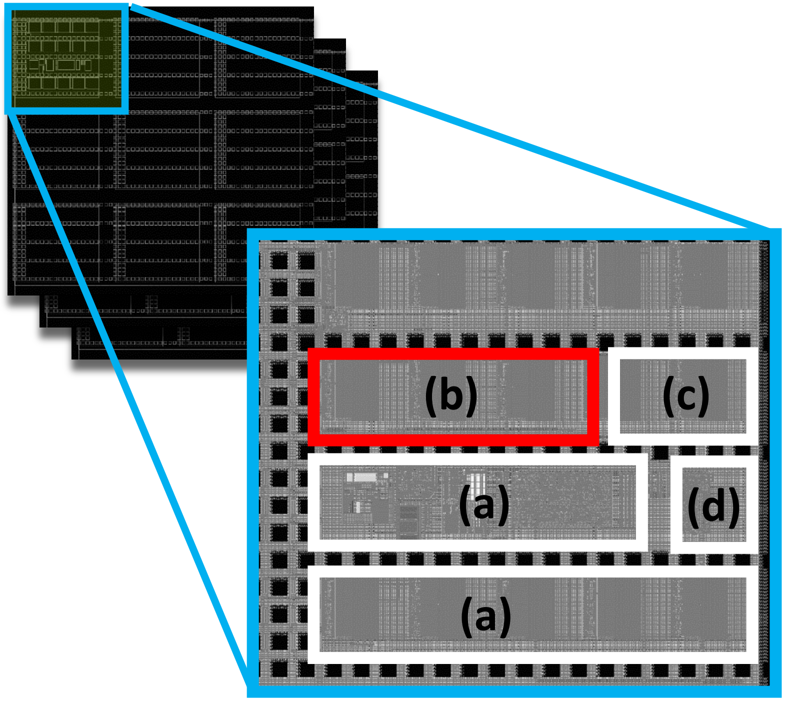


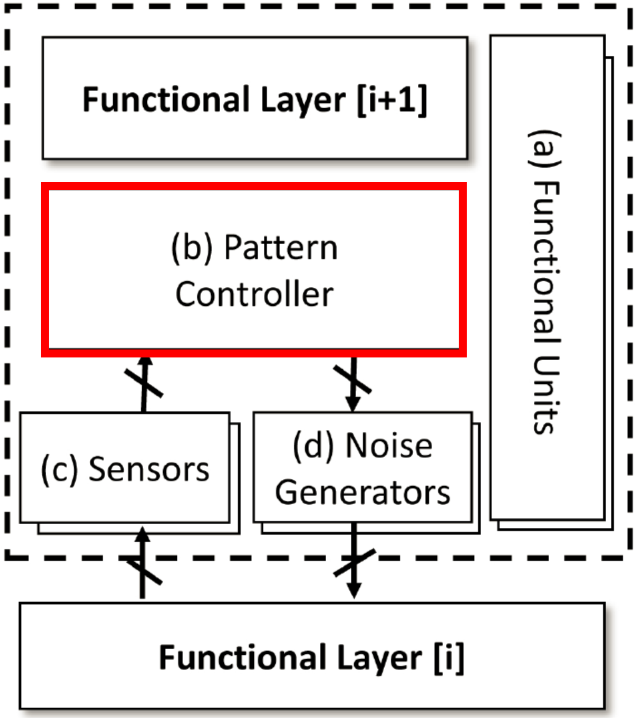
3D-TASCS hardware architecture

Architecture Level Design

- **T**hermal-**a**ware **S**ide-**c**hannel **S**hielding Layer Designs

  3D-TASCS



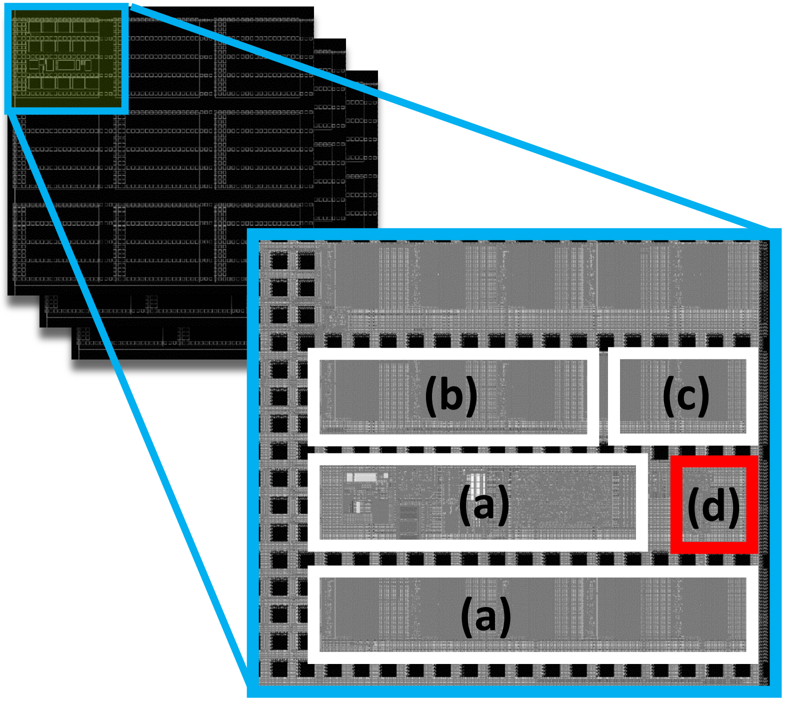


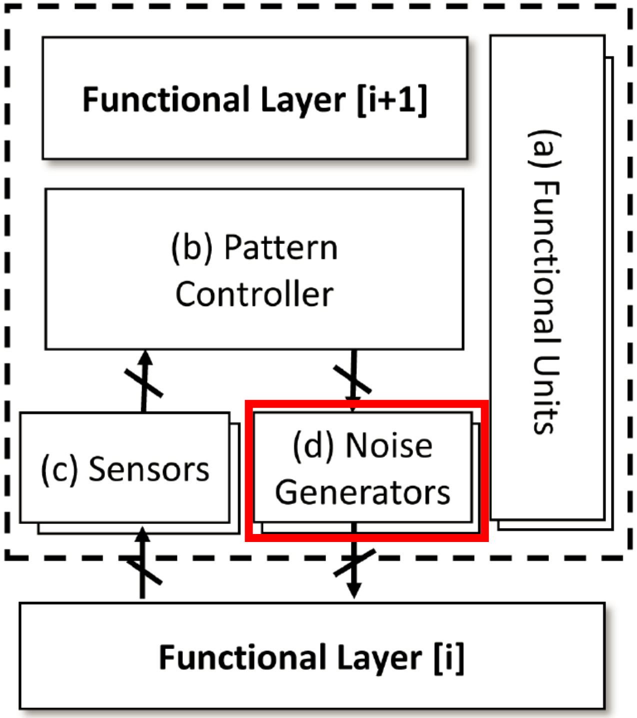
3D-TASCS hardware architecture

Architecture Level Design

- **T**hermal-**a**ware **S**ide-**c**hannel **S**hielding Layer Designs

  3D-TASCS

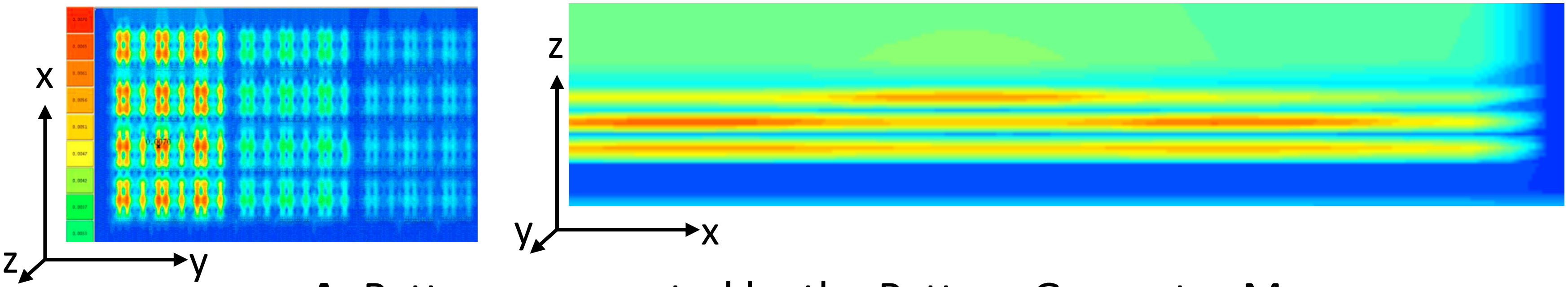




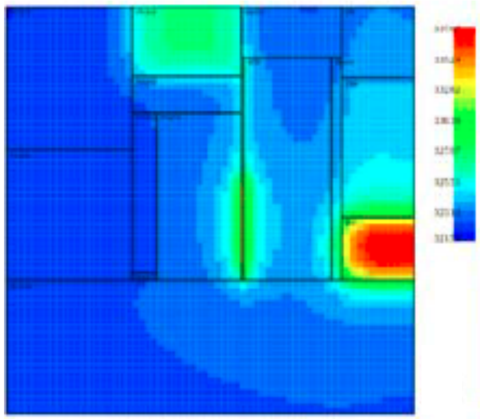
3D-TASCS hardware architecture

Architecture Level Design

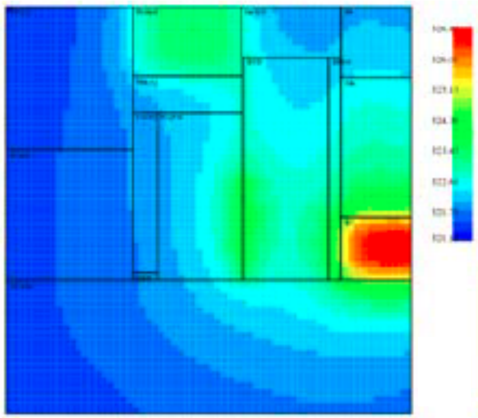
- Thermal-aware Side-channel Shielding Layer Designs



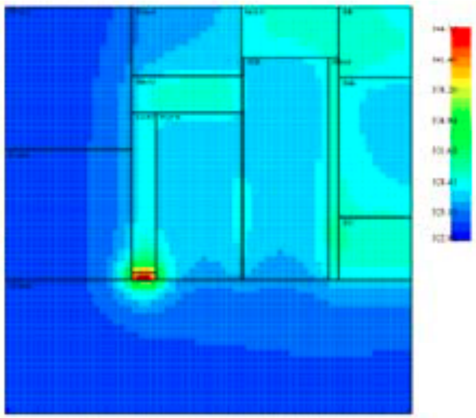
A. Patterns generated by the Pattern Generator Macros



B. No 3D-TASCS



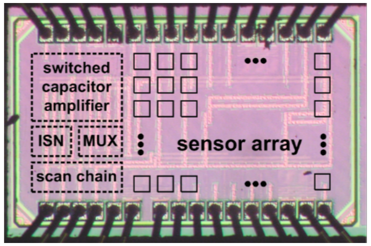
C. 3D-TASCS **OFF**



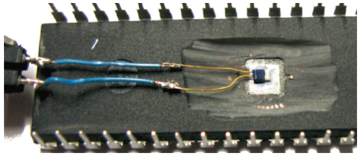
D. 3D-TASCS **ON**

Protection Scheme

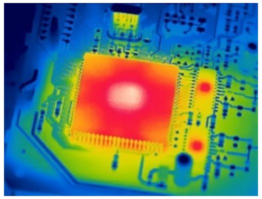
- Protect from *built-in sensors*:
  - Sensors are placed to read out a composite thermal profile of the device and functional blocks.



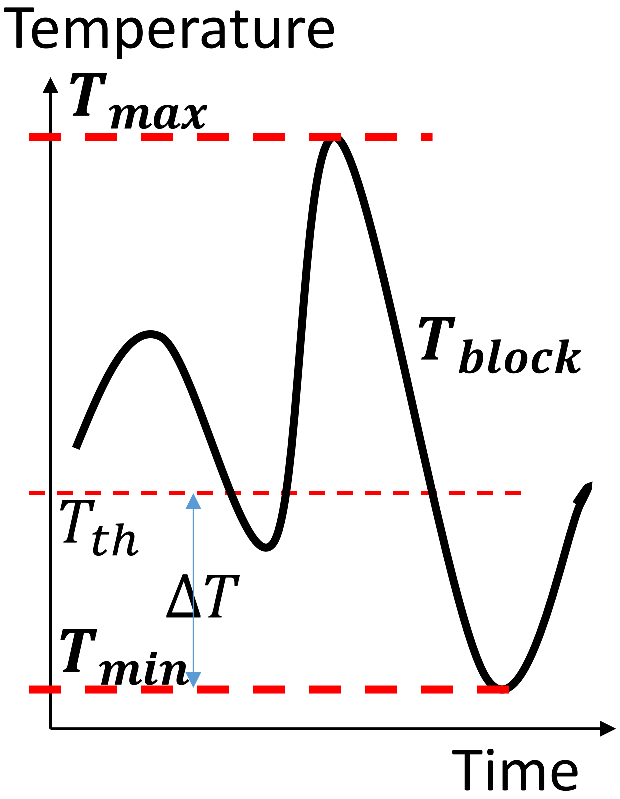
- Protect from *external sensors*:
  - Noise injected by security macros will decrement the side-channel leakage of any critical areas.

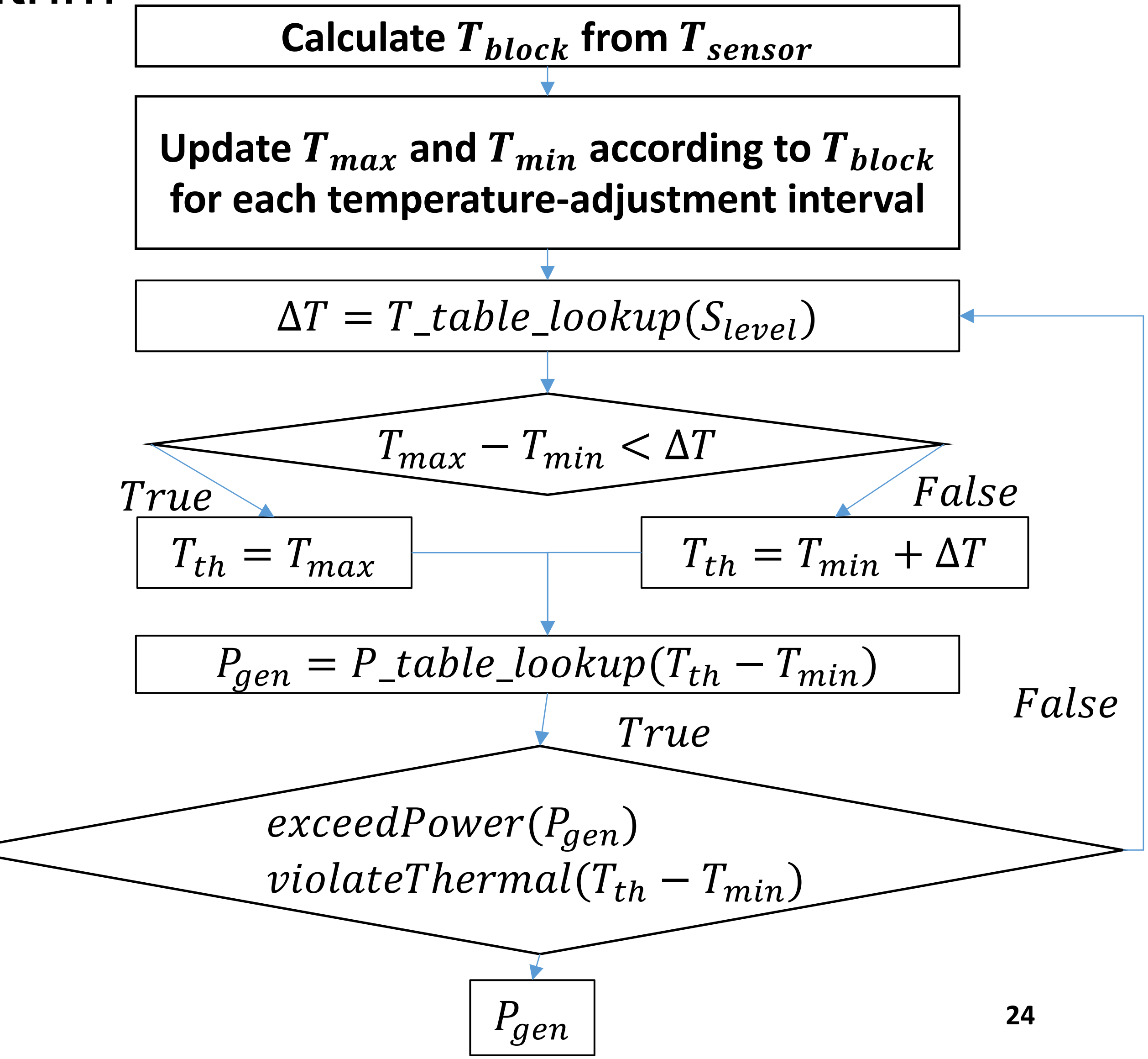


- Protect from *infrared thermal imaging*:
  - The noise generation in the proposed approach conceals the activity patterns of the functional units from infrared cameras and other imaging devices.



Thermal-aware Dynamic Shielding Pattern Generation Algorithm





Calculate T_{block} from T_{sensor}

Update T_{max} and T_{min} according to T_{block} for each temperature-adjustment interval

$\Delta T = T\_table\_lookup(S_{level})$

$T_{max} - T_{min} < \Delta T$

$True$

$T_{th} = T_{max}$

$False$

$T_{th} = T_{min} + \Delta T$

$P_{gen} = P\_table\_lookup(T_{th} - T_{min})$

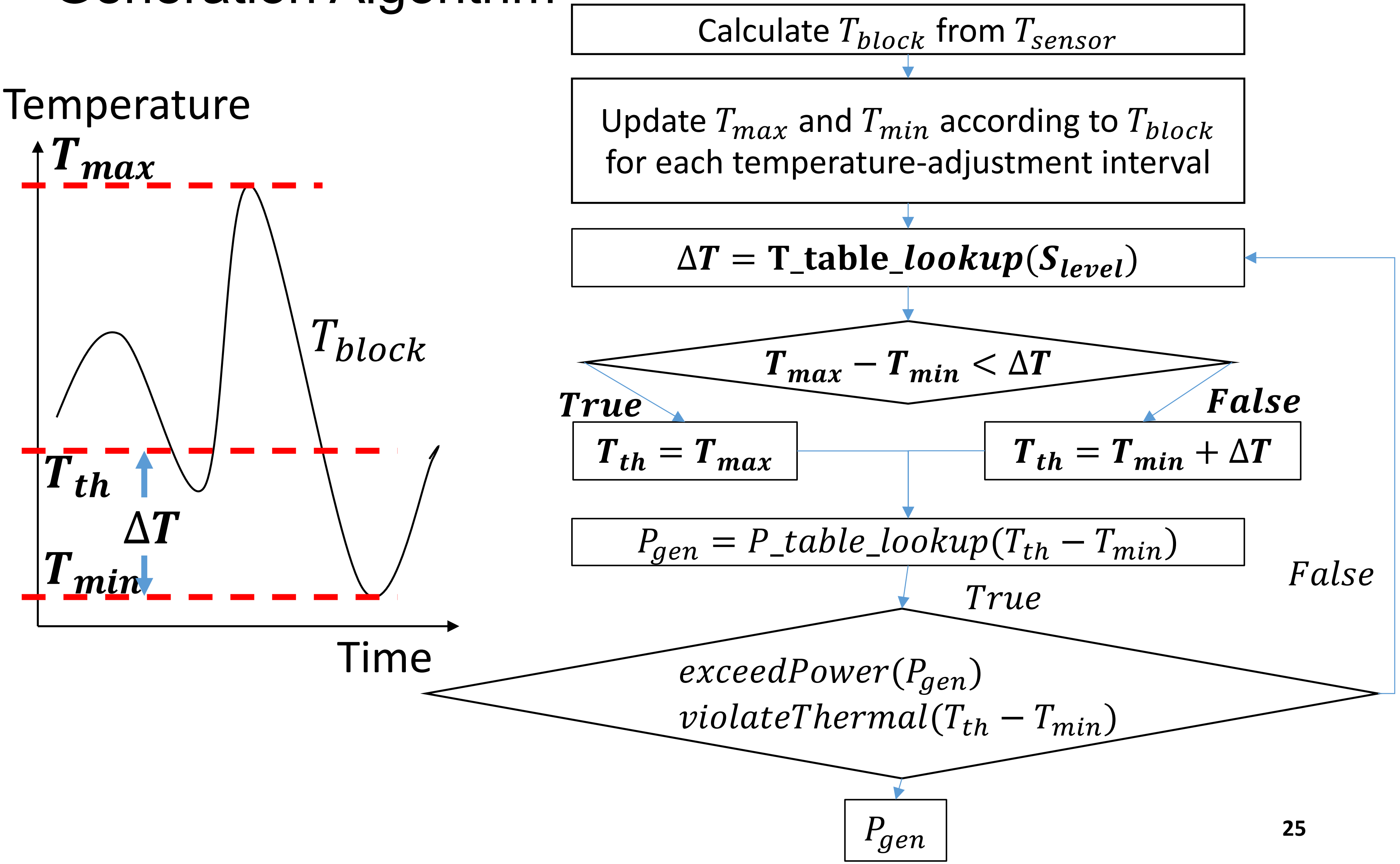
$True$

$False$

$exceedPower(P_{gen})$
$violateThermal(T_{th} - T_{min})$

P_{gen}

Thermal-aware Dynamic Shielding Pattern Generation Algorithm



Calculate T_{block} from T_{sensor}

Update T_{max} and T_{min} according to T_{block} for each temperature-adjustment interval

$\Delta T = \mathbf{T\_table\_lookup}(S_{level})$

$T_{max} - T_{min} < \Delta T$

True

$T_{th} = T_{max}$

False

$T_{th} = T_{min} + \Delta T$

$P_{gen} = P\_table\_lookup(T_{th} - T_{min})$

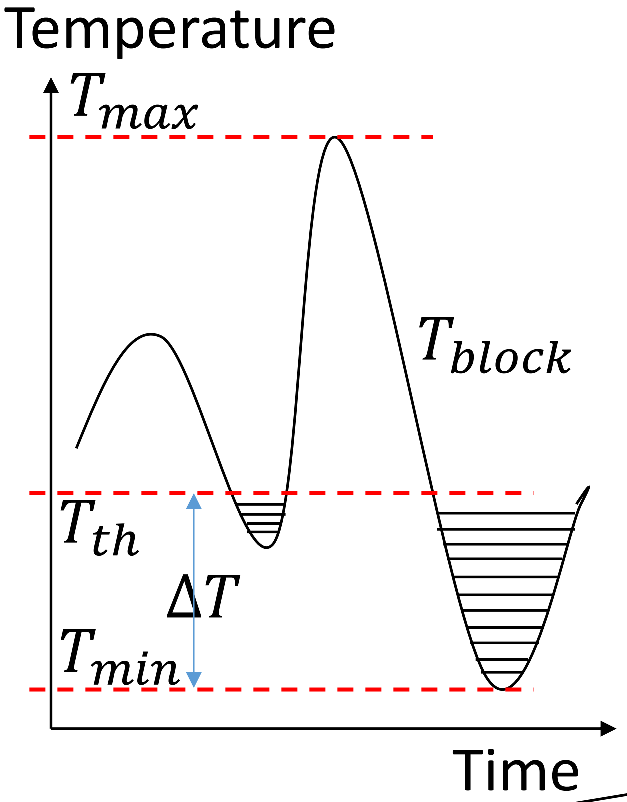
True

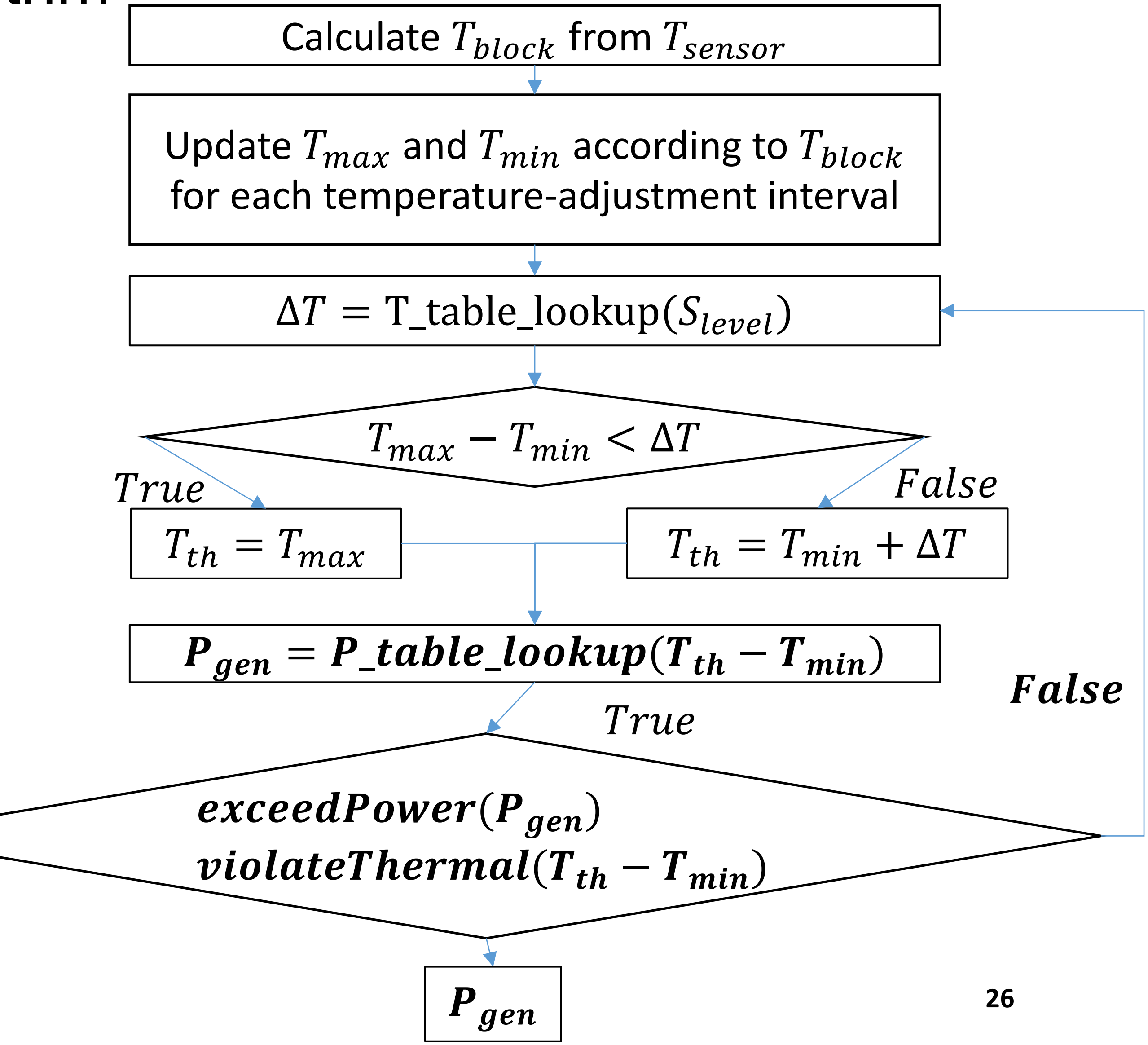
False

$exceedPower(P_{gen})$
$violateThermal(T_{th} - T_{min})$

P_{gen}

Thermal-aware Dynamic Shielding Pattern Generation Algorithm





Calculate T_{block} from T_{sensor}

Update T_{max} and T_{min} according to T_{block} for each temperature-adjustment interval

ΔT = T_table_lookup(S_{level})

$T_{max} - T_{min} < \Delta T$

$True$

$T_{th} = T_{max}$

$False$

$T_{th} = T_{min} + \Delta T$

$\boldsymbol{P_{gen} = P\_table\_lookup(T_{th} - T_{min})}$

$True$

$\boldsymbol{False}$

$\boldsymbol{exceedPower(P_{gen})}$
$\boldsymbol{violateThermal(T_{th} - T_{min})}$

$\boldsymbol{P_{gen}}$

Outline

- Background and Key Idea
- Metric
- Our Design
- Experimental Results

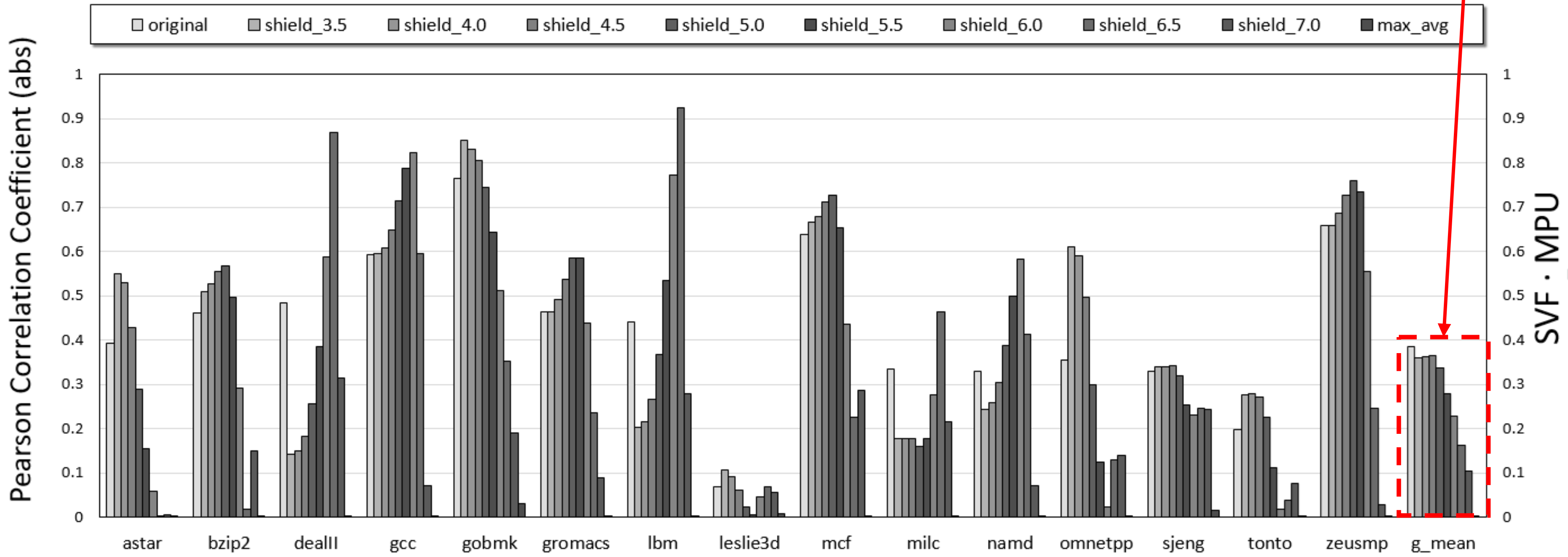
Evaluation

- Benchmarks
  - ➢15 benchmarks from SPEC CPU2006
- Hardware Configuration
  - ➢Simulated on GEM5 using general purpose processor
  - ➢4GHz out-of-order CPU, with a 4-way 64KB L1 cache, a 16-way 4MB L2 cache and 2GB main memory
- Data Collection
  - ➢Statistics of instruction counts for each functional block are collected every 2ms
  - ➢McPAT is used for power analysis
  - ➢Hotspot is used for 3D thermal analysis

Experimental Results

- Security enhancement

Geometric mean of SVF across all benchmarks **decreases** as thermal noise injection increases

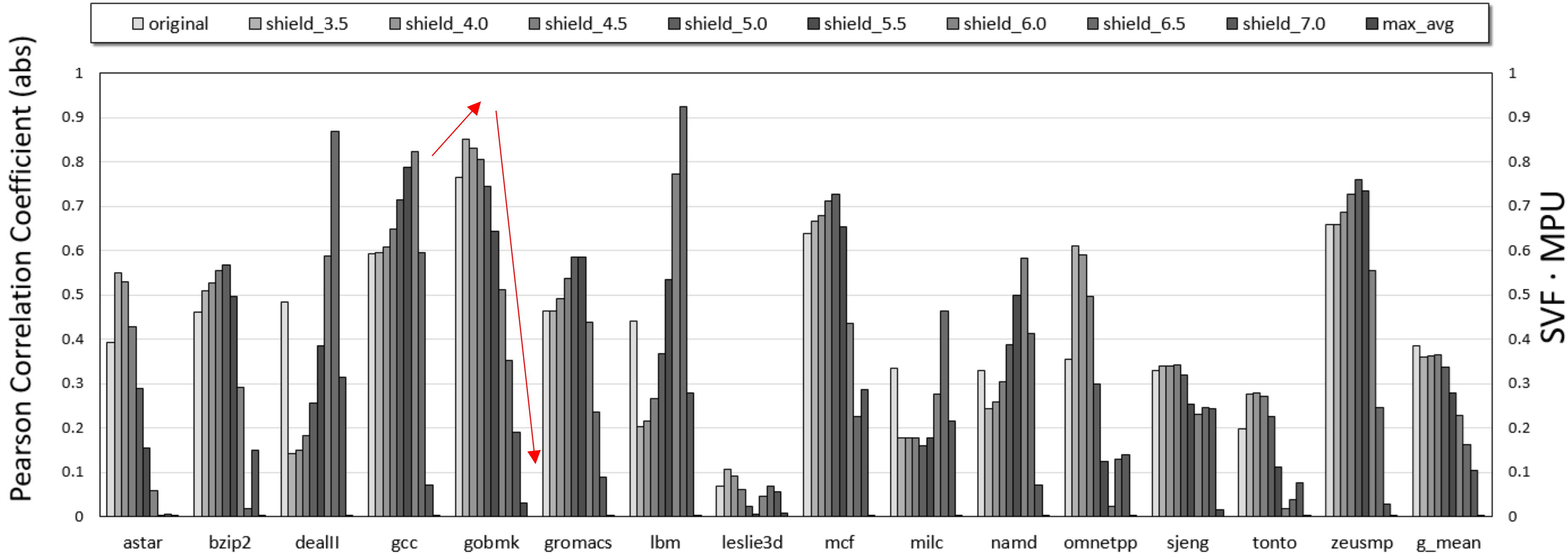


Temperature increment ($T_{th} - T_{min}$) is varied from 3.5^{o}C to 7.0^{o}C with the step size 0.5^{o}C

Experimental Results

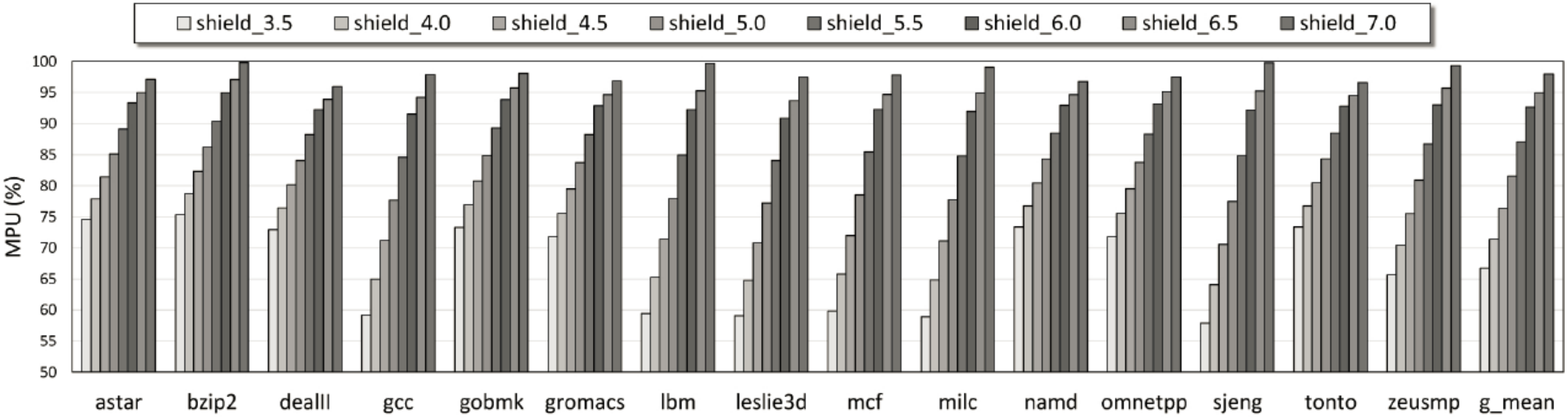
The change of SVF values with increasing temperature increment is different

- the temperature increments with SVF values higher than the original SVF value should be eliminated
- the rest of the temperature increments should be sorted according to their corresponding SVF values, and security levels should match the temperature increments through the relative ranking of the SVF values



Experimental Results

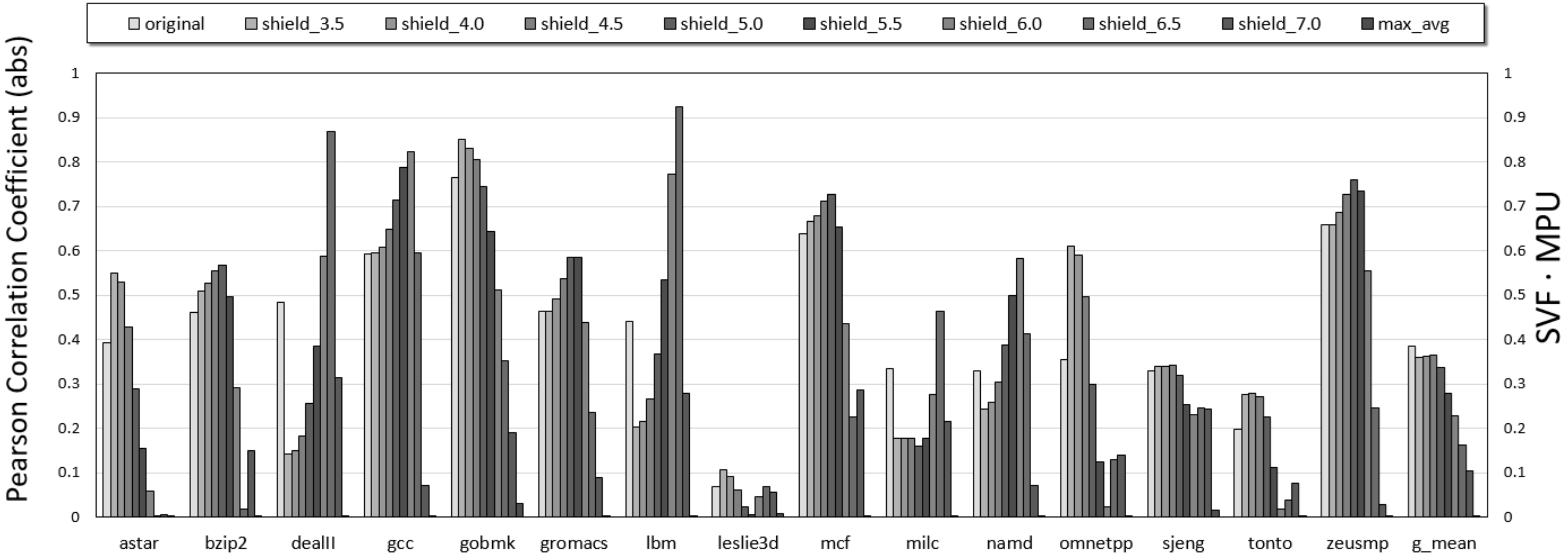
- Power Utilization



*This **metric of power utilization (MPU)** is calculated in percentage as the average power of the pattern generators over the average power of the same generators with the maximum level of noise injection

Experimental Results

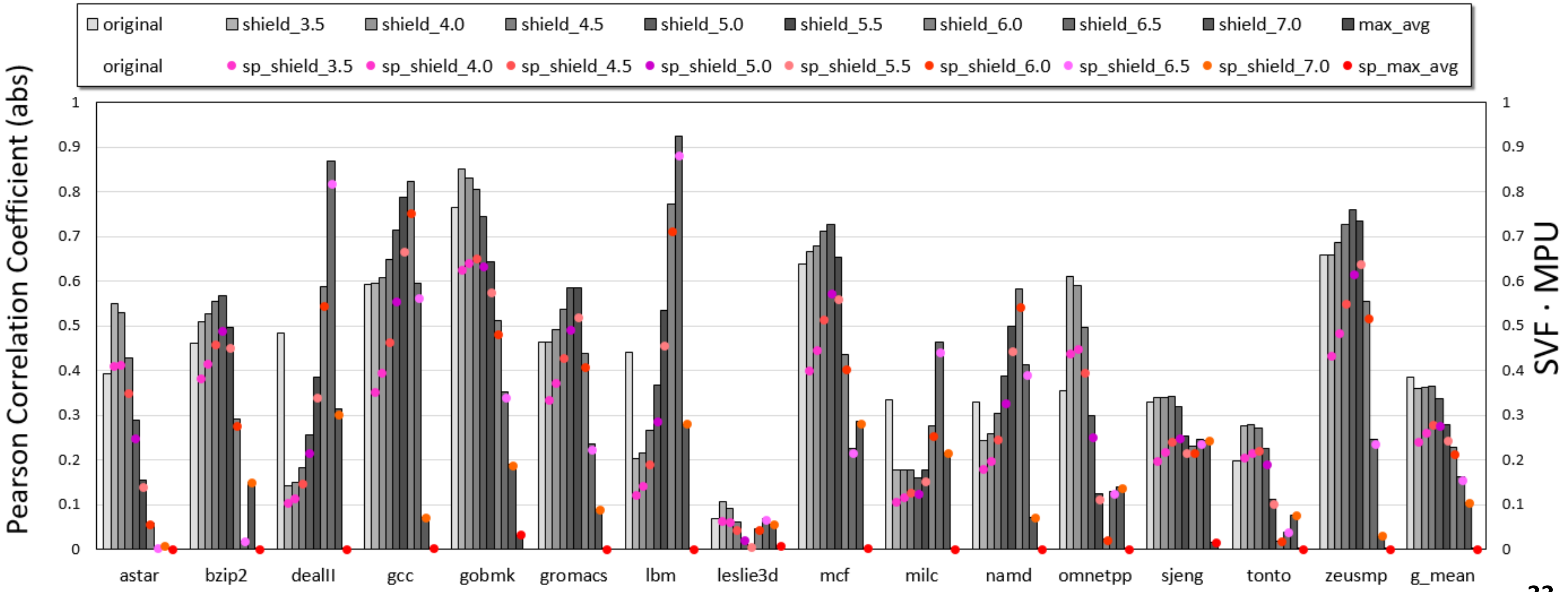
- Scaled SVF with Power Utilization
  - SVF values with low temperature increments (T<4.5C) are scaled lower than SVF values with high temperature increments (T>6.5C)
  - The distribution of scaled SVF values is the same as the original distribution of SVF values for all benchmarks



Experimental Results

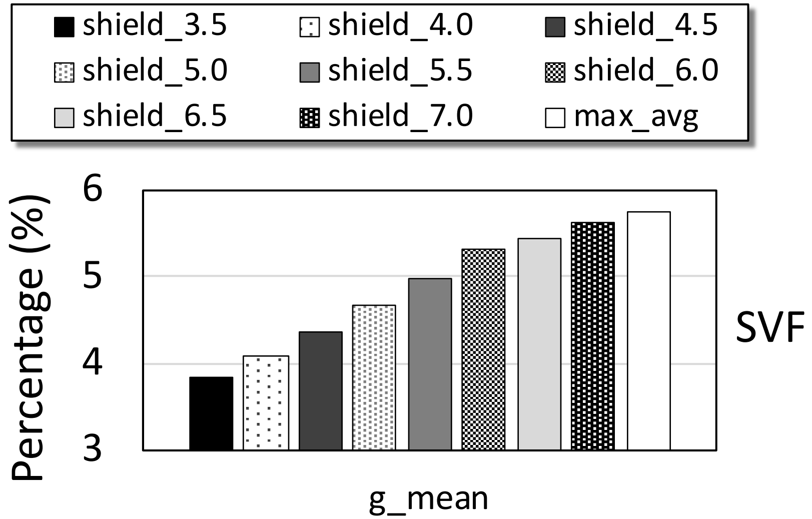
- Scaled SVF with Power Utilization

  - SVF values with low temperature increments (T<4.5C) are scaled lower than SVF values with high temperature increments (T>6.5C)
  - The distribution of scaled SVF values is the same as the original distribution of SVF values for all benchmarks

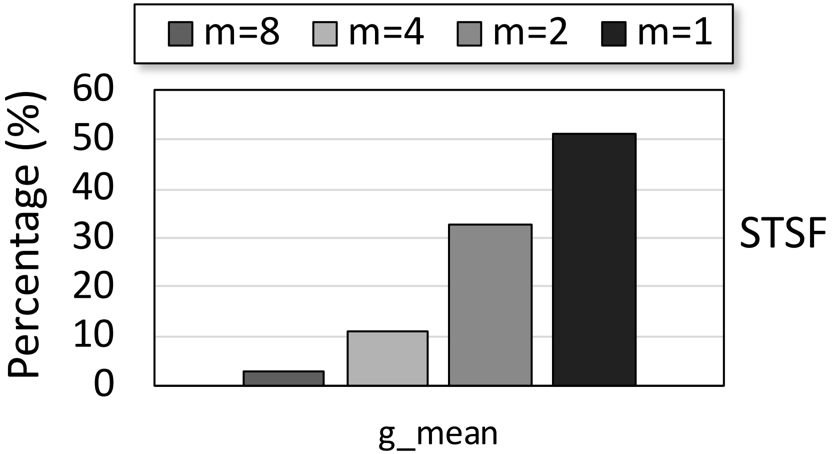


Experimental Results

- Overhead Discussion



*The metric for power overhead is calculated as the average power of pattern generations over the total system power.



SVF could be reduced to 0 with 5.74% power overhead
STSF could be reduced to 0.5855 (m=4) with 10.82% power overhead

Summary

- The proposed scheme leverages inherent characteristics of 3D integration and dynamically generates custom activity patterns to shield from thermal side-channel attacks in three modes.

- TASCS algorithm can provide effective side-channel shielding in energy efficient way:
  - With 5.74% power overhead SVF could be reduced to 0
  - With 10.82% power overhead STSF could be reduced to 0.59

Thermal-aware 3D Design for Side-channel Information Leakage

Peng Gu[1], Dylan Stow[1], Russell Barnes[1], Eren Kursun[2], and Yuan Xie[1]

University of California, Santa Barbara[1] , Columbia University[2]

Thank You!

UC Santa Barbara
Scalable Energy-efficient Architecture Lab

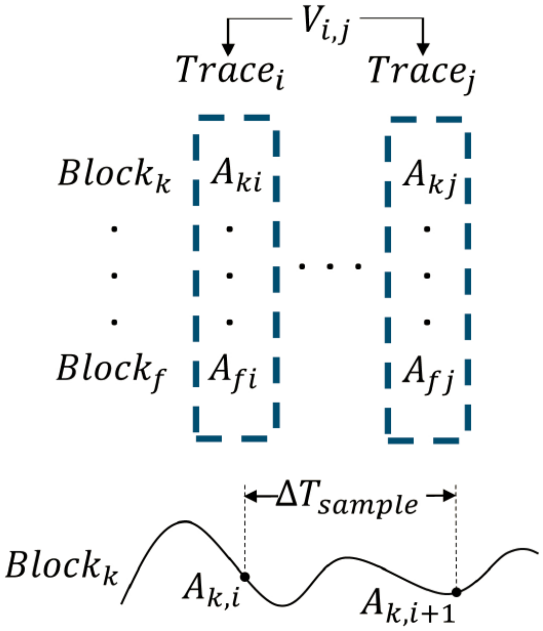
https://seal.ece.ucsb.edu/

UC SANTA BARBARA engineering

Backup Slides

Metric

- Side-channel Vulnerability Factor (SVF)



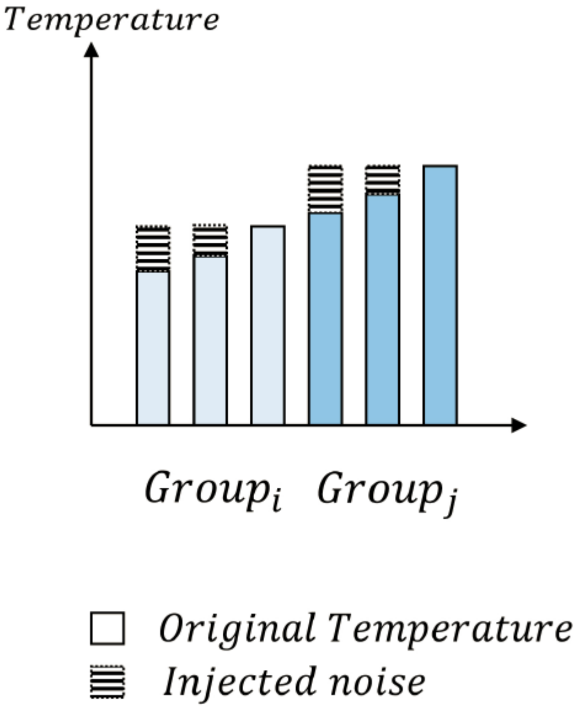
$$V_{i,j} = Dist(Trace_i, Trace_j) \quad i > j,\ j > 0$$

$$r = \frac{\sum_{i>j>0}^{n} (V_{inst(i,j)} - \overline{V_{inst}})(V_{temp(i+k,j+k)} - \overline{V_{temp}})}{\sqrt{\sum_{i>j>0}^{n} (V_{inst(i,j)} - \overline{V_{inst}})^2} \sqrt{\sum_{i>j>0}^{n} (V_{temp(i+k,j+k)} - \overline{V_{temp}})^2}}$$

Metric

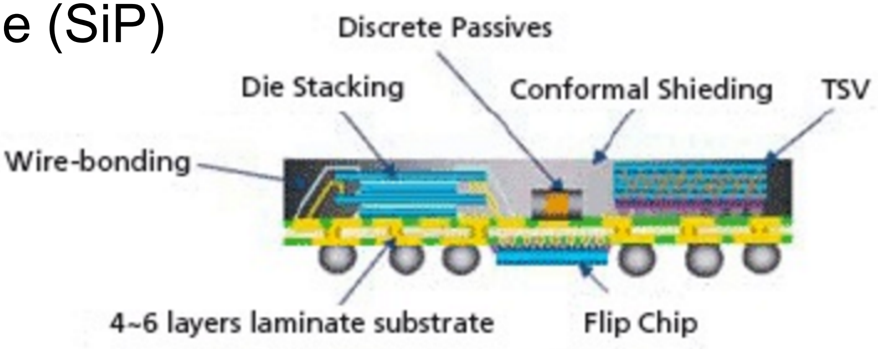
- Spatial Thermal Side-channel Factor (STSF)

$$r = \frac{-\log(\frac{1}{n!}) - (-\log(\frac{1}{((n/m)!)^m}))}{-\log(\frac{1}{n!})}$$

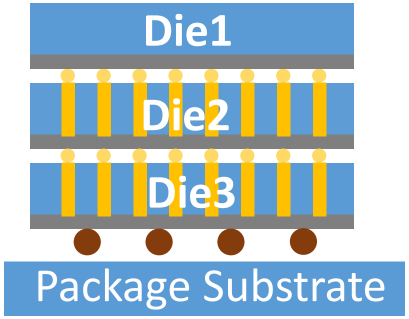


3D Design Specification

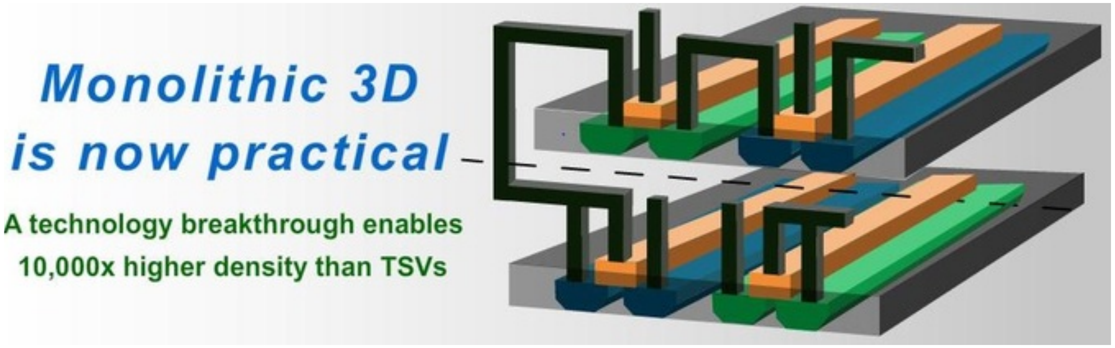
- System in Package (SiP)



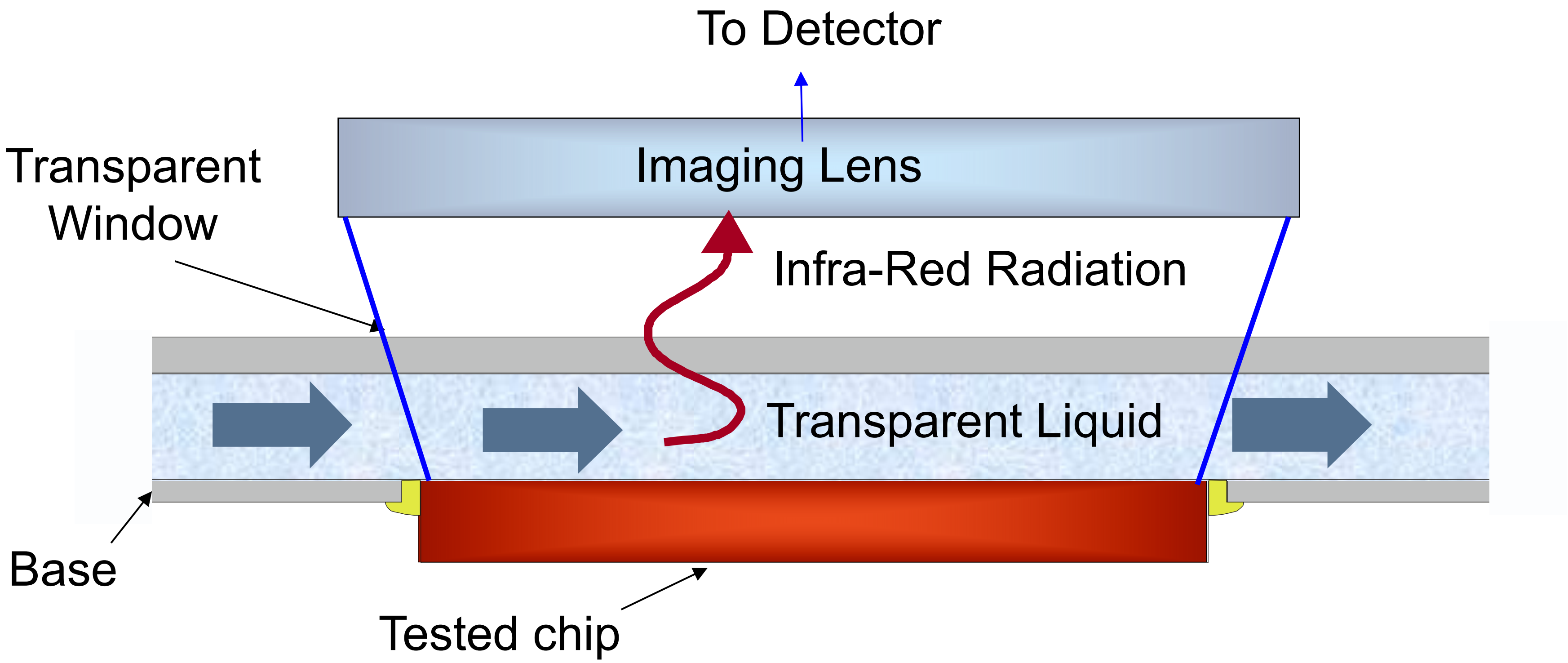
- TSV-based 3D IC



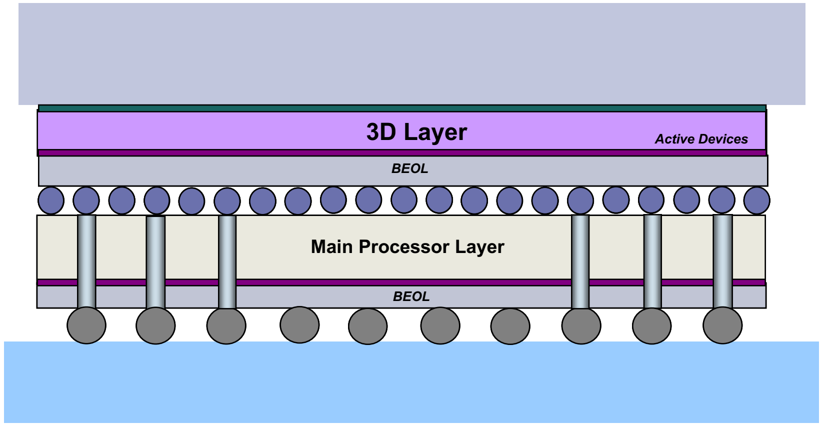
- Monolithic 3D

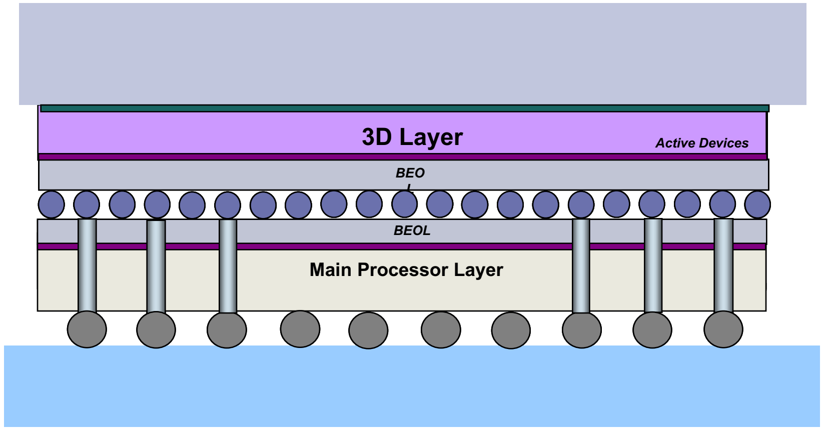

Monolithic 3D
is now practical
A technology breakthrough enables
10,000x higher density than TSVs

IR-imaging

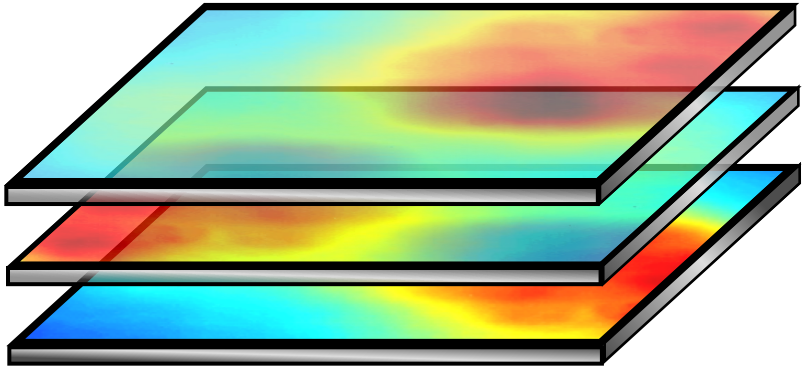

To Detector
Imaging Lens
Transparent Window
Infra-Red Radiation
Transparent Liquid
Base
Tested chip

Face-to-Back and Face-to-Face Implementation Alternatives

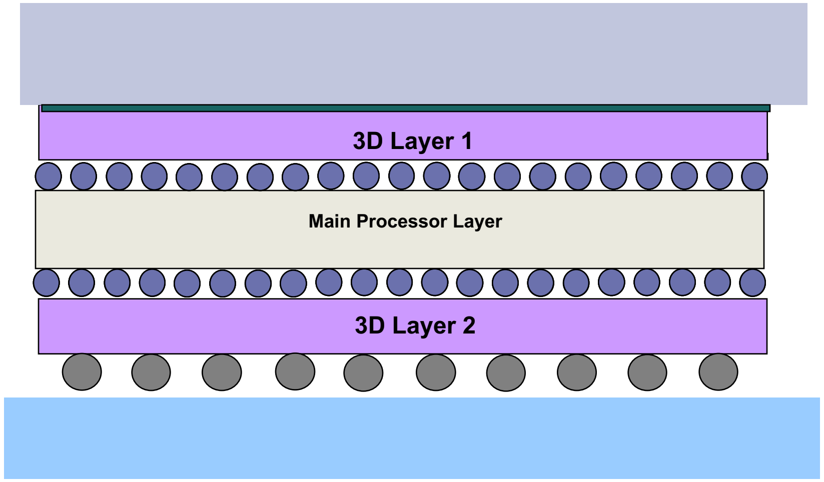




Concealing/Diverting pattern generation in critical area



Multi-layer Implementation for increased security


3D Layer 1
Main Processor Layer
3D Layer 2