CICC

IEEE Custom Integrated Circuits Conference

3-3 Physical Design Strategies for Mitigating Fine-Grained Electromagnetic Side-Channel Attacks

Meizhi Wang[1], Vishnuvardhan V. Iyer[1], Shanshan Xie[1], Ge Li[1], Sanu K. Mathew[2], Raghavan Kumar[2], Michael Orshansky[1], Ali E. Yilmaz[1], and Jaydeep P. Kulkarni[1]

[1]University of Texas, Austin, TX, [2] Intel Labs, Hillsboro, OR

E-mail: wang.mz@utexas.edu, jaydeep@austin.utexas.edu

26 April 2021

TEXAS The University of Texas at Austin

Circuit Research Lab:
https://sites.utexas.edu/CRL/

SSCS IEEE SOLID-STATE CIRCUITS SOCIETY™

IEEE

Outline

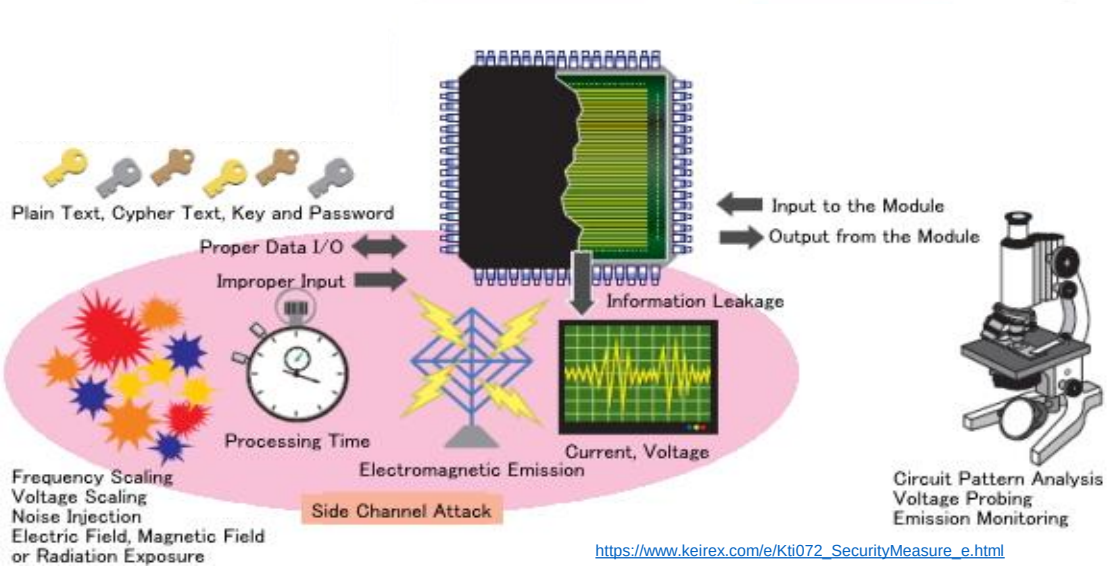
- Side-channel Attacks (SCA)
- Fine-grained EM SCA simulation
- Proposed physical design strategies
- Fine-grained EM measurement
  - Die photo and setup
  - EM measurement
  - SCA results
- Conclusion
- Acknowledgements

Outline

- Side-channel Attacks (SCA)
- Fine-grained EM SCA simulation
- Proposed physical design strategies
- Fine-grained EM measurement
  - Die photo and setup
  - EM measurement
  - SCA results
- Conclusion
- Acknowledgements

Side-channel Attacks (SCA)

- Leaked side-channel info: Power, EM emissions
- Able to Break an algorithmically robust crypto engine
- Easy physical access
- High successful rate



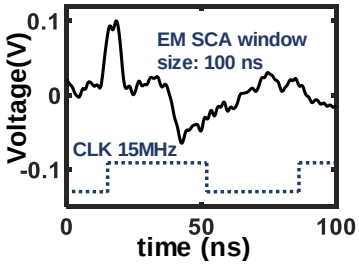
https://www.keirex.com/e/Kti072_SecurityMeasure_e.html

Side-channel Attacks: Fine-grained EM

- Fine-grained EM measurement provide rich spatial content, increasing SCA successful rate

Coarse-grained EM measurement

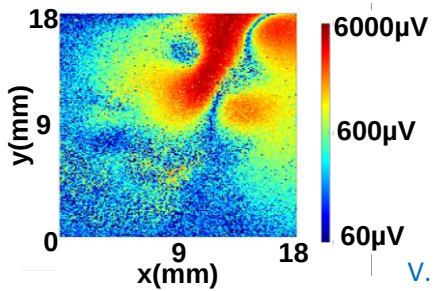
10mm probe



M. Wang, *et al*. CICC, 2021

Fine-grained EM measurement

1mm probe

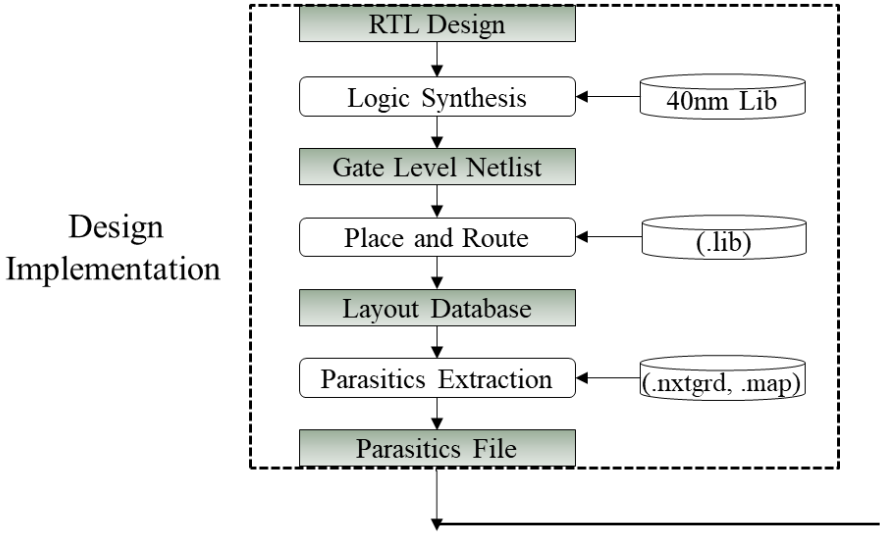


V. V. Iyer, *et al. WMCS*, 2019

Outline

- Side-channel Analysis (SCA)
- Fine-grained EM SCA simulation
- Proposed physical design strategies
- Fine-grained EM measurement
  - Die photo and setup
  - EM measurement
  - SCA results
- Conclusion
- Acknowledgements

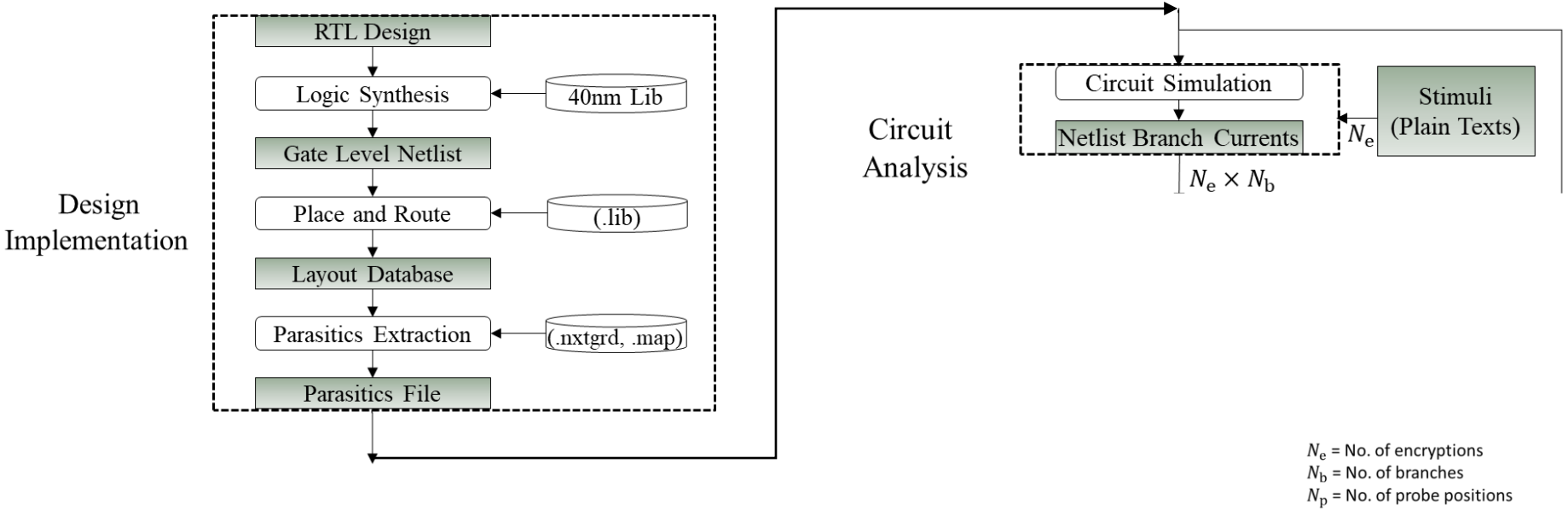
Fine-grained EM SCA Simulation: Flow



- Step 1: ASIC implementation and extract parasitic parameters of the power grid

Source: A. Kumar et al., ICCAD 2017

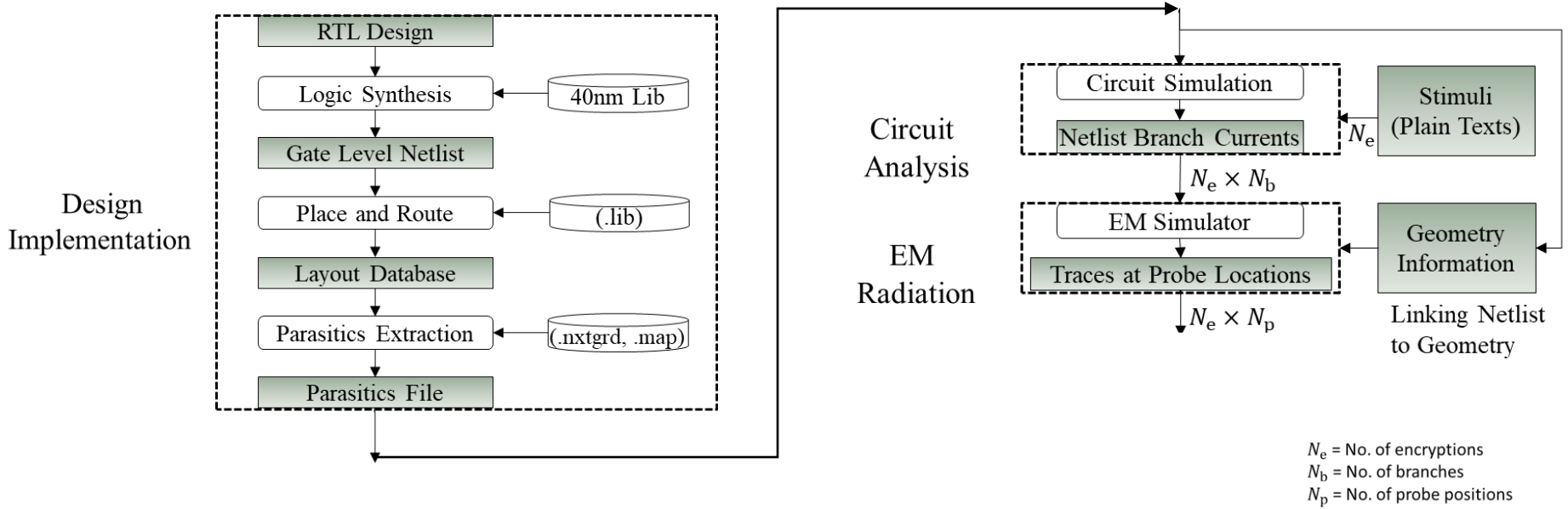
Fine-grained EM SCA Simulation: Flow



- Step 2: Simulate encryption and obtain transient current trace on each parasitic resistor

Source: A. Kumar et al., ICCAD 2017

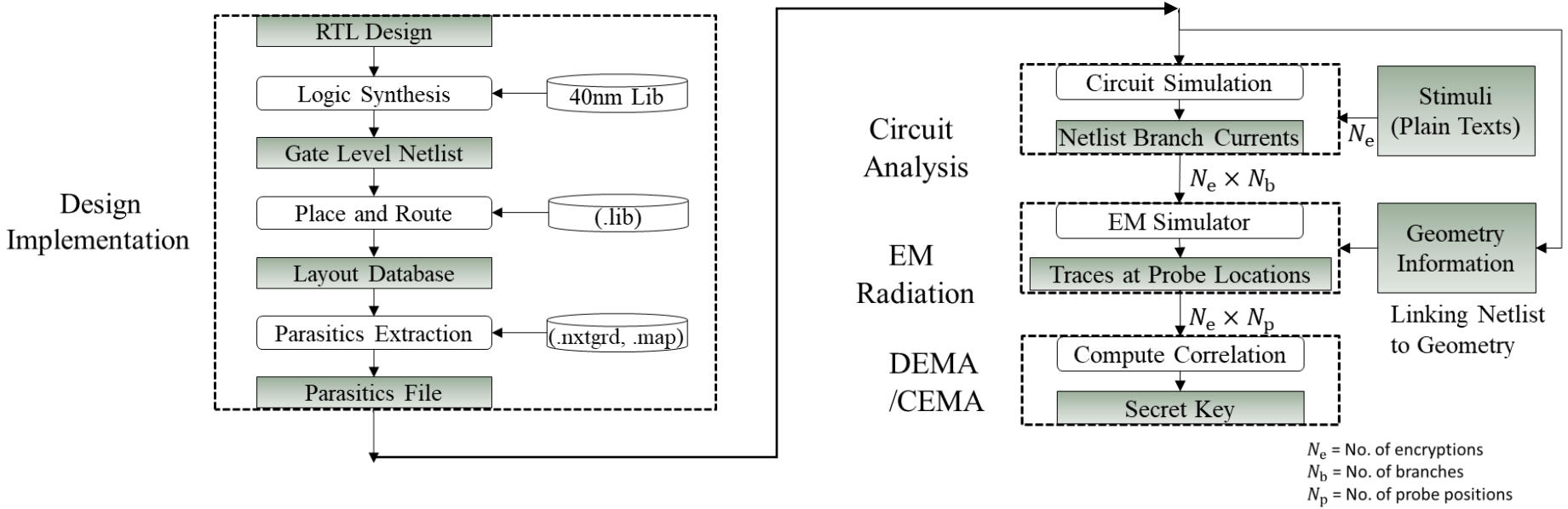
Fine-grained EM SCA Simulation: Flow



- Step 3: Feed parasitic parameters and spatial-temporalcurrent information to the customized EM simulator

Source: A. Kumar et al., ICCAD 2017

Fine-grained EM SCA Simulation: Flow

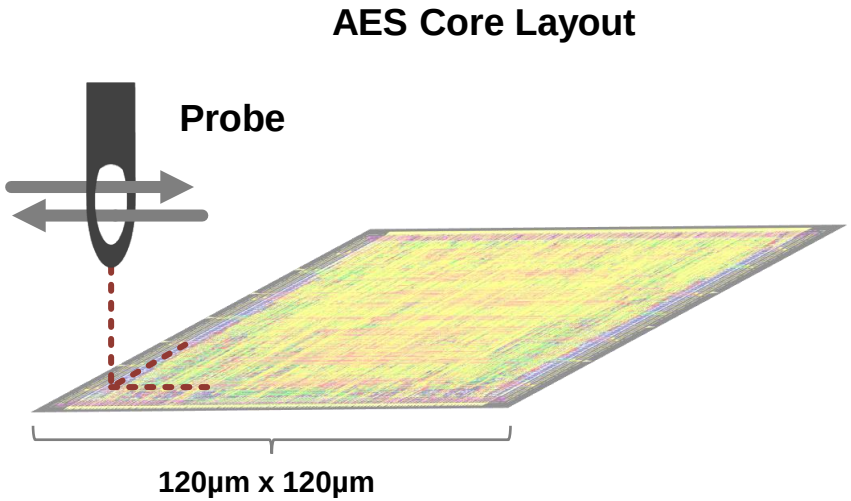


- Step 4: Apply differential/correlation EM analysis (DEMA/CEMA)against the simulated EM radiation

Source: A. Kumar et al., ICCAD 2017

Fine-grained EM SCA Simulation

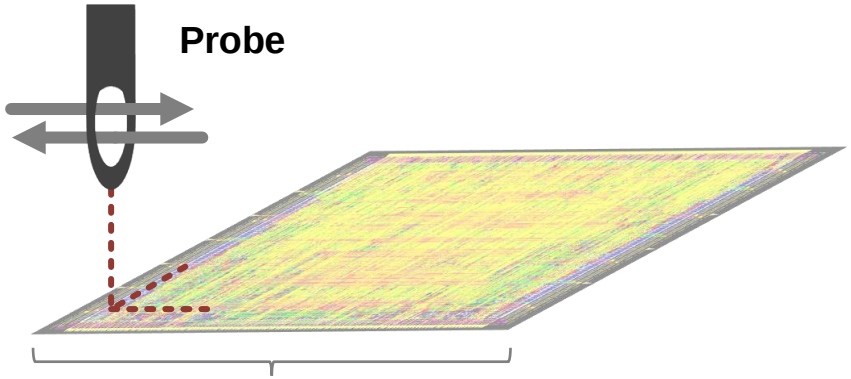
- Implement a 128b Advanced Encryption Standard (AES) design using 40nm technology
- Run EM simulation with probe diameter of 50µm and 75µm above the circuit



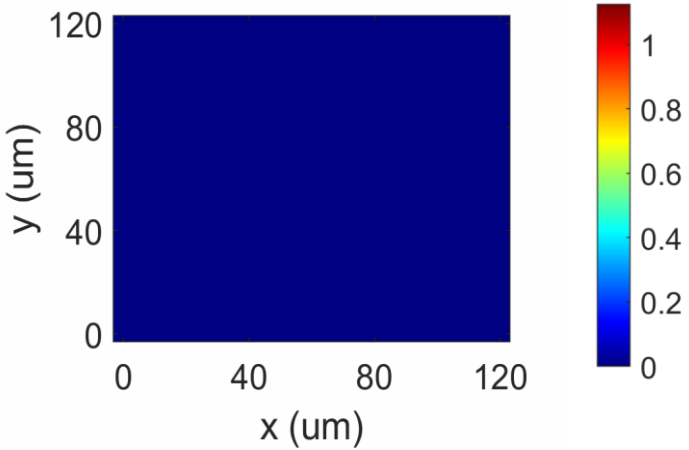
Fine-grained EM SCA Simulation

- Implement a 128b Advanced Encryption Standard (AES) design using 40nm technology
- Run EM simulation with probe diameter of 50um and 75um above the circuit

AES Core Layout



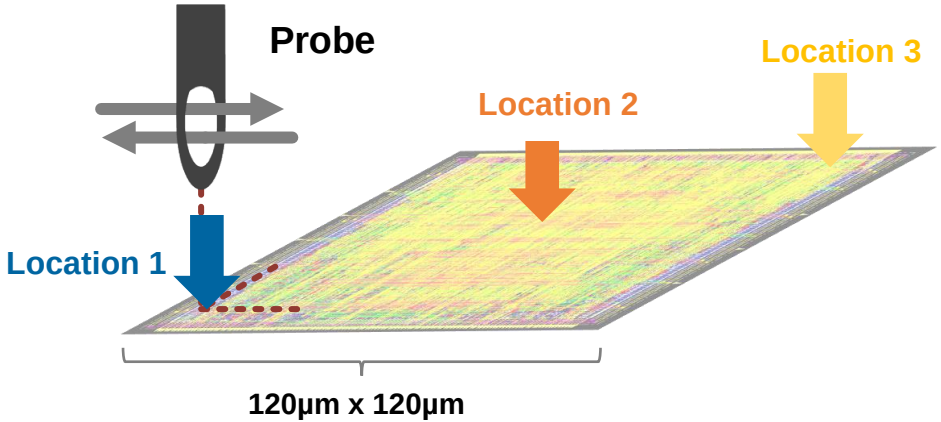
Simulated EM emissions in colormap



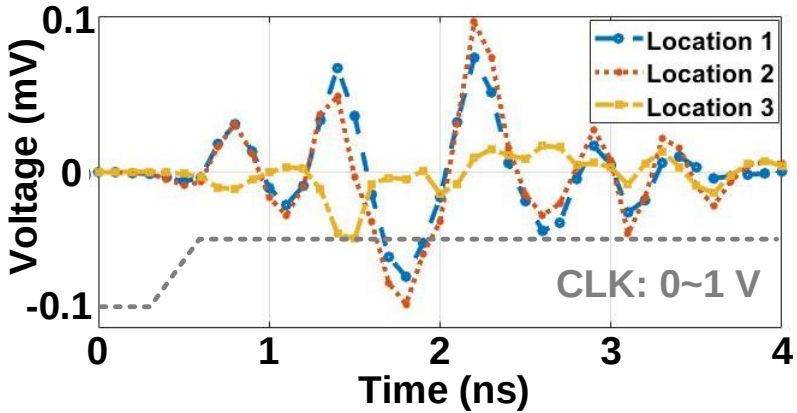
Fine-grained EM SCA Simulation

- Simulate 1000 encryptions and monitor EM waveforms at 3 locations on the layout
- EM waveforms of the last encryption round used for CEMA attacking window

AES Core Layout

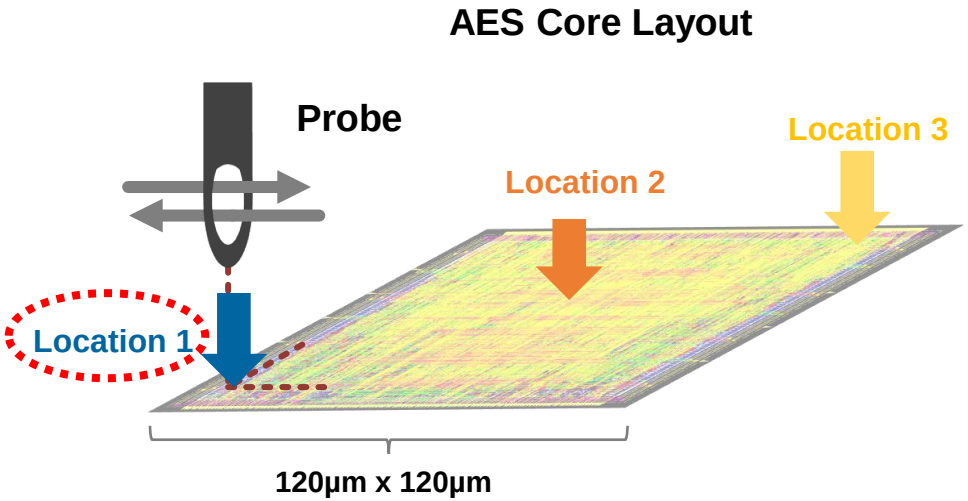


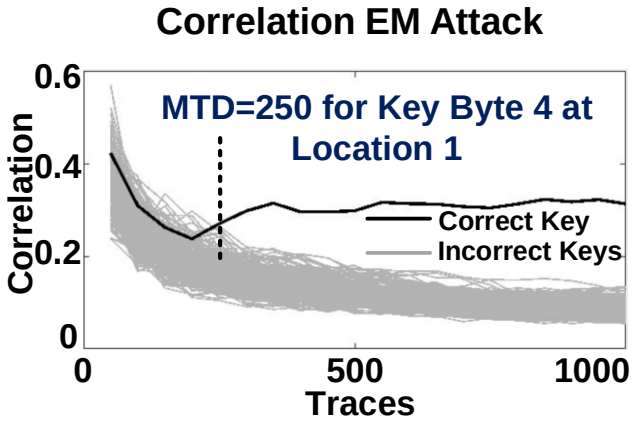
Simulated EM Waveforms



Fine-grained EM SCA Simulation: SCA Results

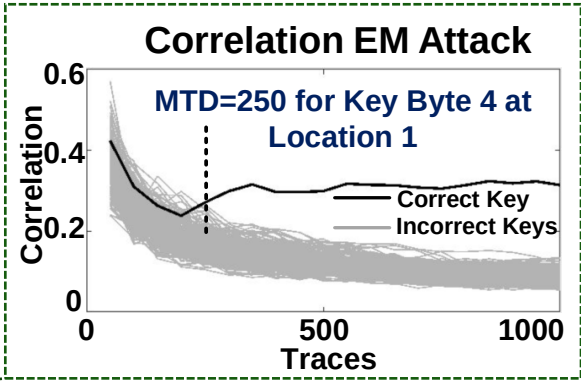
- Run correlation attack using 1000 traces at each location
- At location 1: Key Byte 4 is revealed using about 250 traces

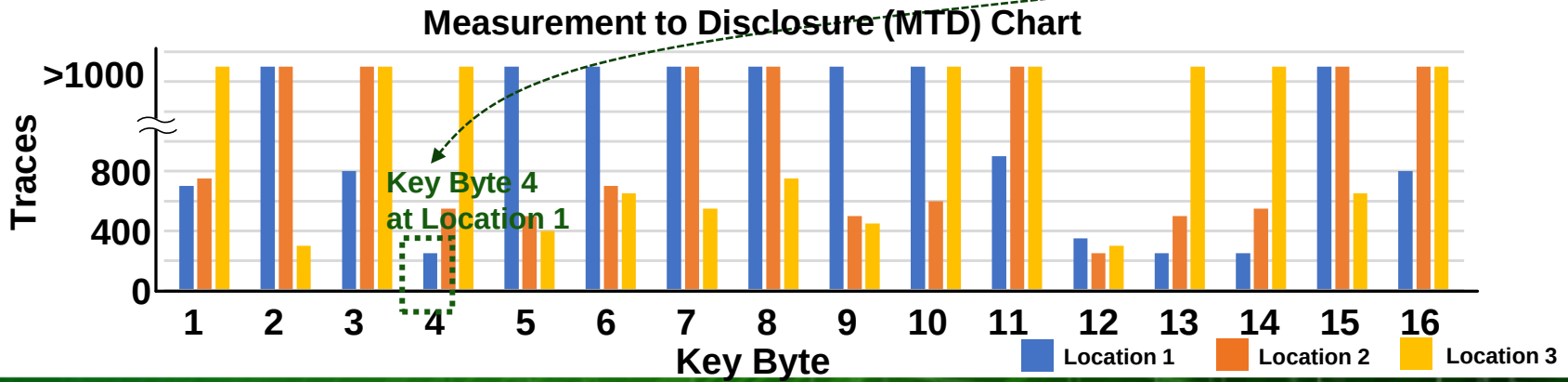




Fine-grained EM SCA Simulation: SCA Results

- Run correlation attack using 1000 traces at each location
- At location 1: Key Byte 4 is revealed using about 250 traces
- All 16 key bytes can be revealed within the 1000 traces collected at 3 locations



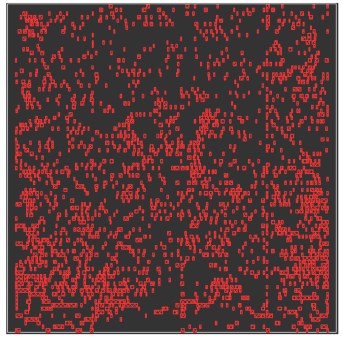


Outline

- Side-channel Analysis (SCA)
- Fine-grained EM SCA simulation
- Proposed physical design strategies
- Fine-grained EM measurement
  - Die photo and setup
  - EM measurement
  - SCA results
- Conclusion
- Acknowledgements

Physical Design strategies: Design 1, Design 2

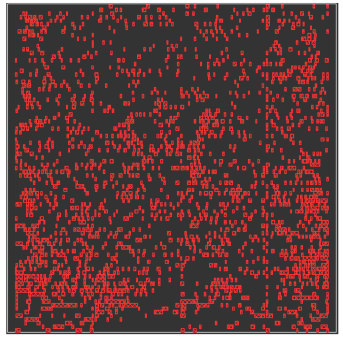
- Exploring different power grid strategies for improving fine-grained EM SCA resilience
- Design 1: (Baseline) A 128 bit AES Computing core using metal M1 ~ M6



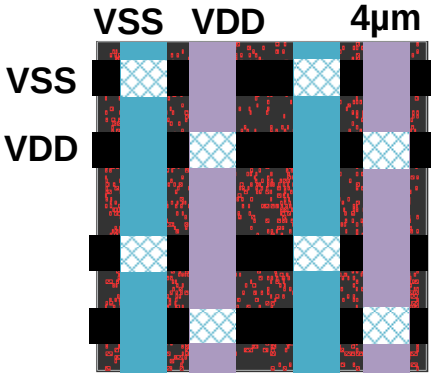
Design 1

Physical Design strategies: Design 1, Design 2

- Exploring different power grid strategies for improving fine-grained EM SCA resilience
- Design 1: (Baseline) A 128 bit AES Computing core using metal M1 ~ M6
- Design 2 = Design 1 + Dense power grid on M7 M8



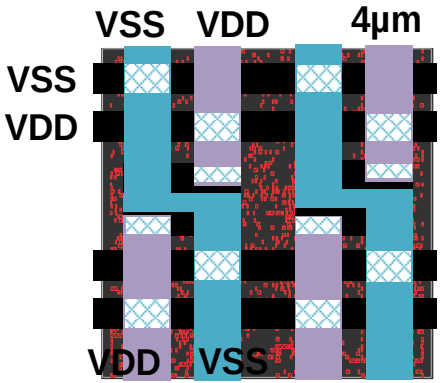
Design 1



Design 2

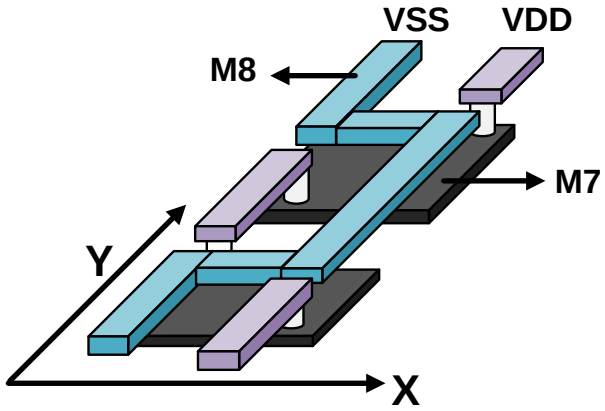
Physical Design strategies: Design 3

- Design 3 = Design 1 + Twisted power grid along Y axis on M7 and M8



Design 3*

Twisted power grid shown in 3-D illustration

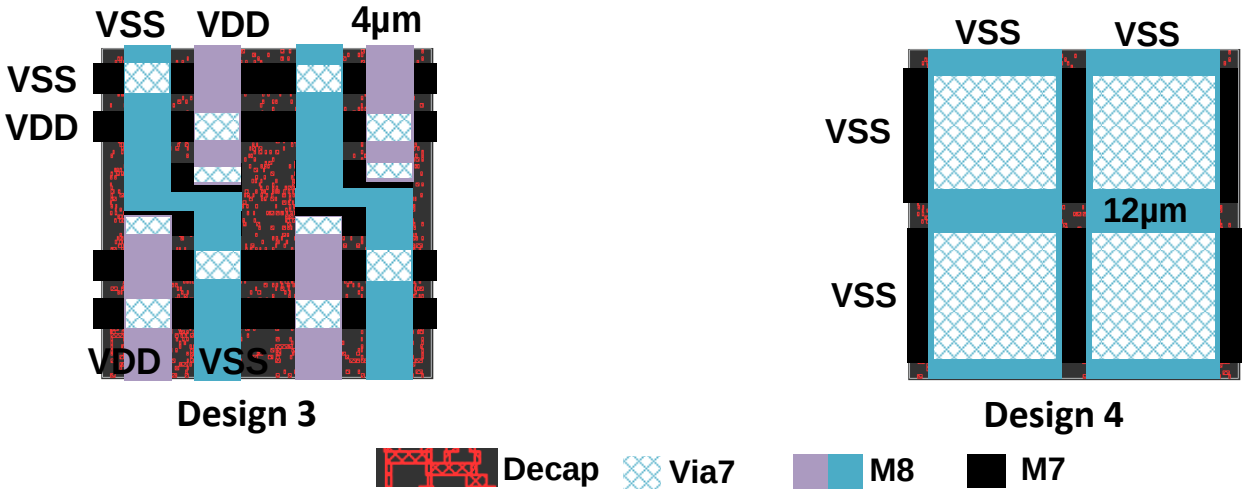


*Only one twist is shown as an illustration

Decap Via7 M8 M7

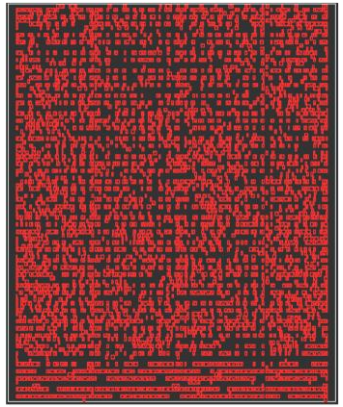
Physical Design strategies: Design 3, Design 4

- Design 3 = Design 1 + Twisted power grid along Y axis on M7 and M8
- Design 4 = Design 1 + Extra wide VSS shield on M7 and M8



Physical Design strategies: Design 5, Design 6

- Exploring Decap cells and VSS shield for improving fine-grained EM resilience
- Design 5: Baseline #2 using M1~M6 with extra Decap with 20% area increase

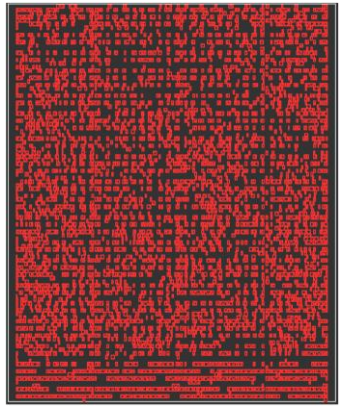


Design 5

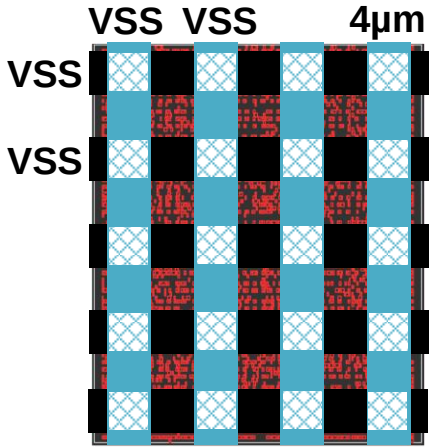
Decap Via7 M8 M7

Physical Design strategies: Design 5, Design 6

- Exploring Decap cells and VSS shield for improving fine-grained EM resilience
- Design 5: Baseline #2 using M1~M6 with extra Decap with 20% area increase
- Design 6 = Design 5 + Thin and dense VSS shield on M7 and M8



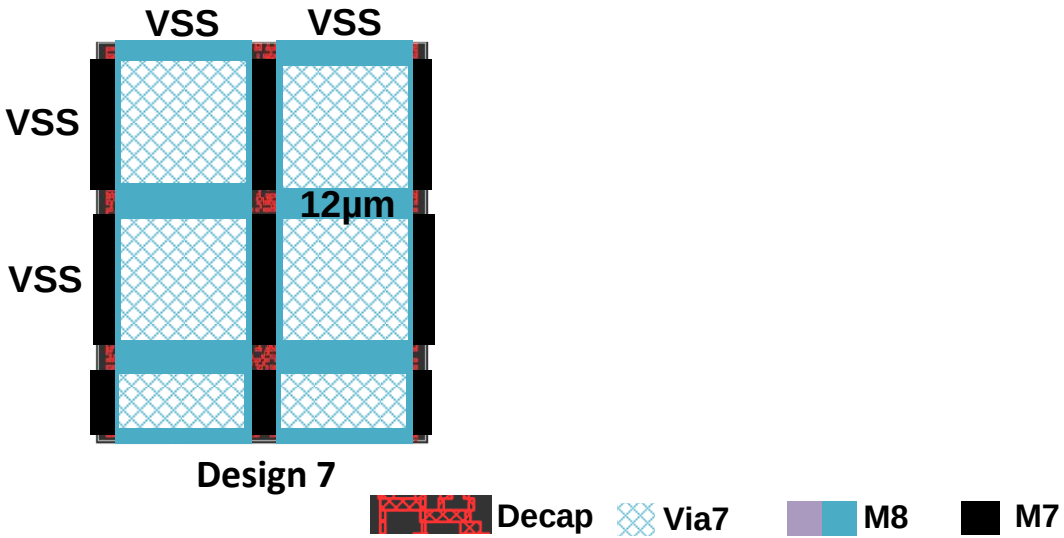
Design 5



Design 6

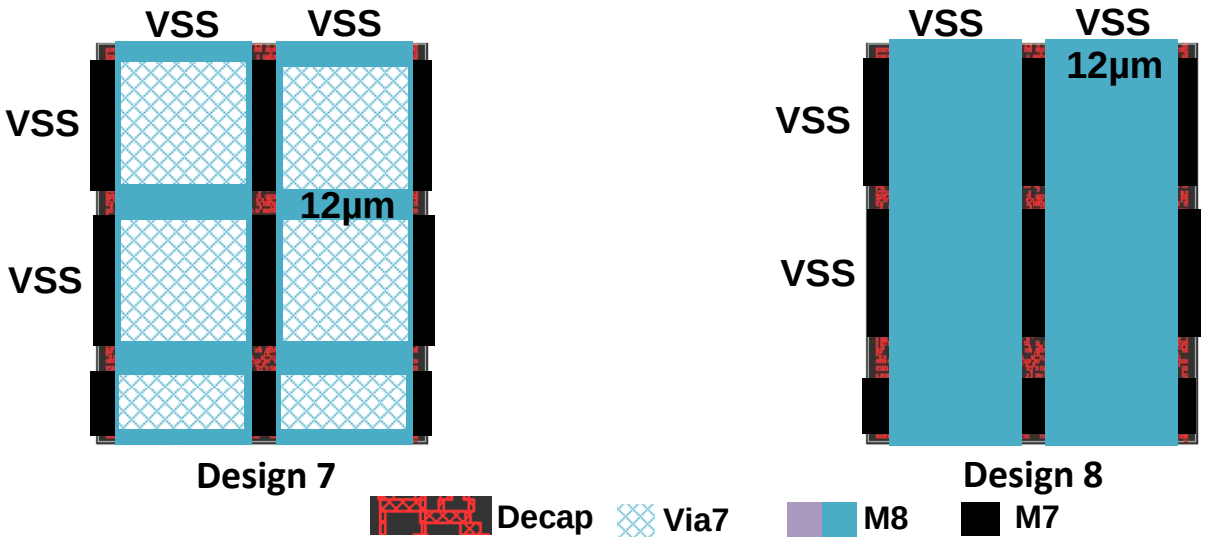
Physical Design strategies: Design 7, Design 8

- Exploring Decap cells and VSS shield for improving fine-grained EM resilience
- Design 7 = Design 5 + Extra wide VSS shield on M7 and M8



Physical Design strategies: Design 7, Design 8

- Exploring Decap cells and VSS shield for improving fine-grained EM resilience
- Design 7 = Design 5 + Extra wide VSS shield on M7 and M8
- Design 8 = Design 5 + Extra wide VSS shield on M7 and M8, no intermediate connection



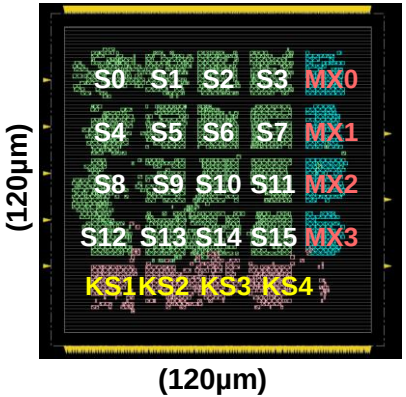
Physical Design strategies: Design 9

- Design-9: Isolated S-Box placement using M1~M6 with no extra Decap nor VSS shield
  - AES core layout showing S-Box (S*), MixColumn (MX*), and Key Schedule (KS*) module locations

Design 9

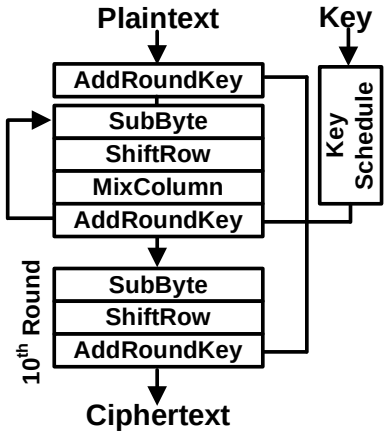
Physical Design strategies: Design 9

- Design-9: Isolated S-Box placement with no extra Decap nor VSS shield
  - AES core layout showing S-Box (S*), MixColumn (MX*), and Key Schedule (KS*) module locations

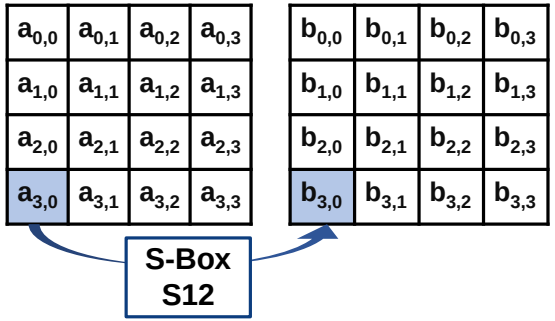


Design 9

AES encryption flowchart



SubByte illustration



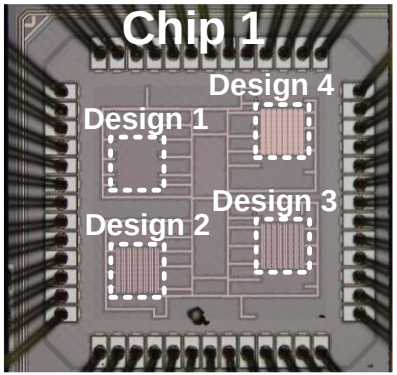
- S-Box isolation reduces current path within S-box modules and mitigate EM signatures

Outline

- Side-channel Analysis (SCA)
- Fine-grained EM SCA simulation
- Proposed physical design strategies
- Fine-grained EM measurement
  - Die photo and setup
  - EM measurement
  - SCA results
- Conclusion
- Acknowledgements

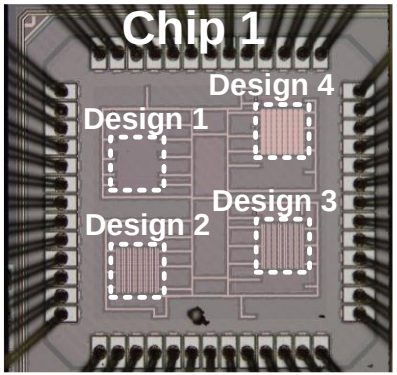
Die photos

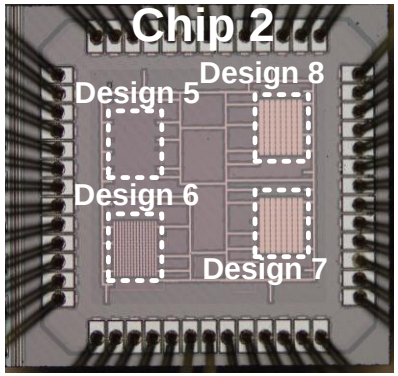
- Chip-1: Design 1 to Design 4: Different power grid strategies



Die photos

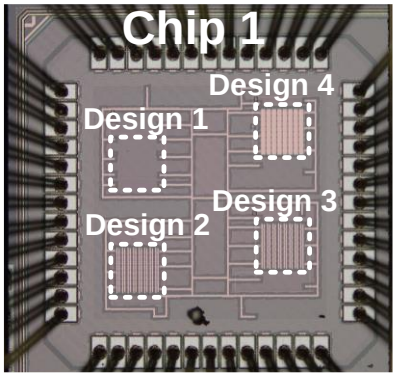
- Chip-1: Design 1 to Design 4: Different power grid strategies
- Chip-2: Design 5 to Design 8: Decap cells and VSS shield strategies

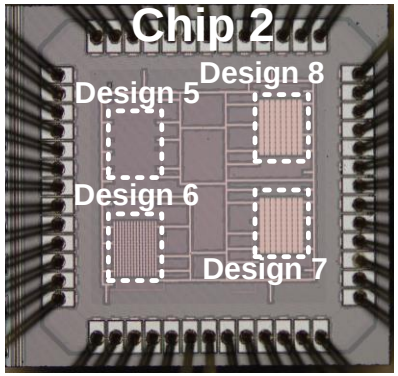


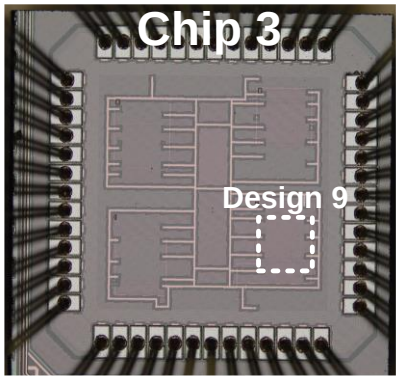


Die photos

- Chip-1: Design 1 to Design 4: Different power grid strategies
- Chip-2: Design 5 to Design 8: Decap cells and VSS shield strategies
- Chip-3: Design 9: Isolated S-Box placement



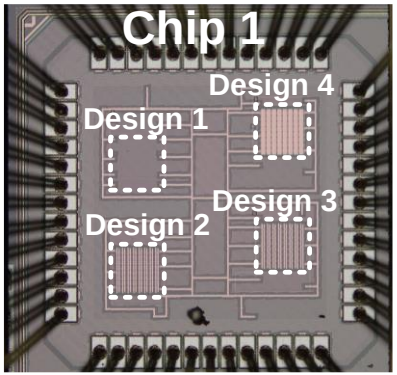


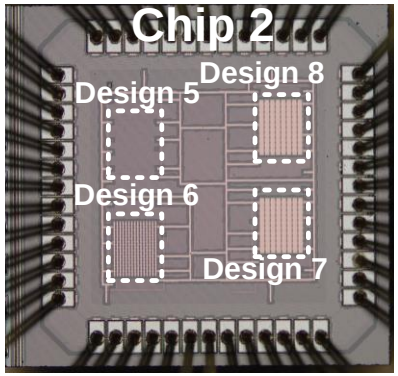


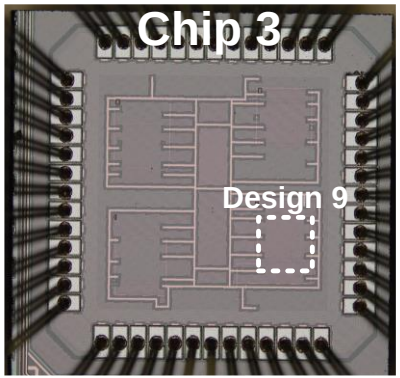
Die photos

- Chip-1: Design 1 to Design 4: Different power grid strategies
- Chip-2: Design 5 to Design 8: Decap cells and VS
- Chip-3: Design 9: Isolated S-Box placement

Each design is operated individually to reduce EM noise from other AES cores

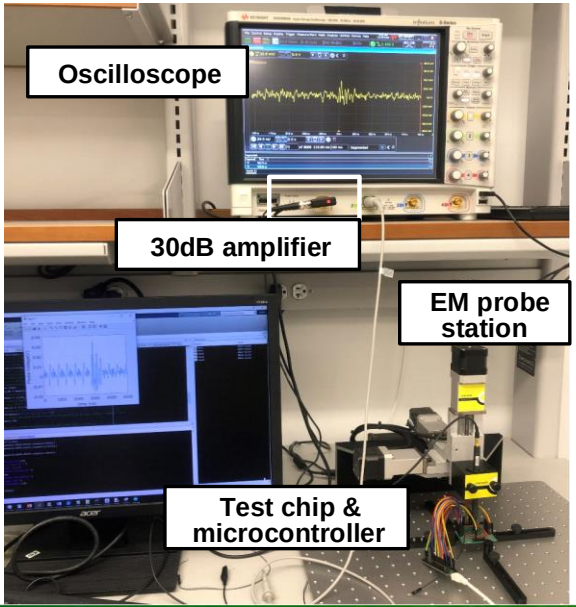






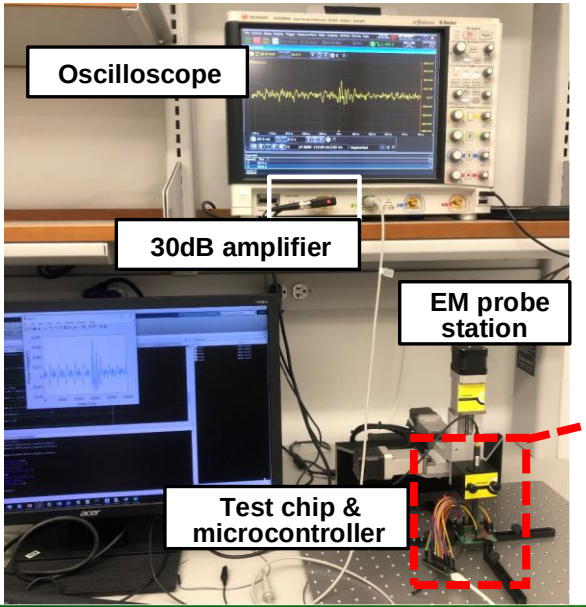
Measurement Setup

- Riscure EM probe station
- 1mm diameter EM probe

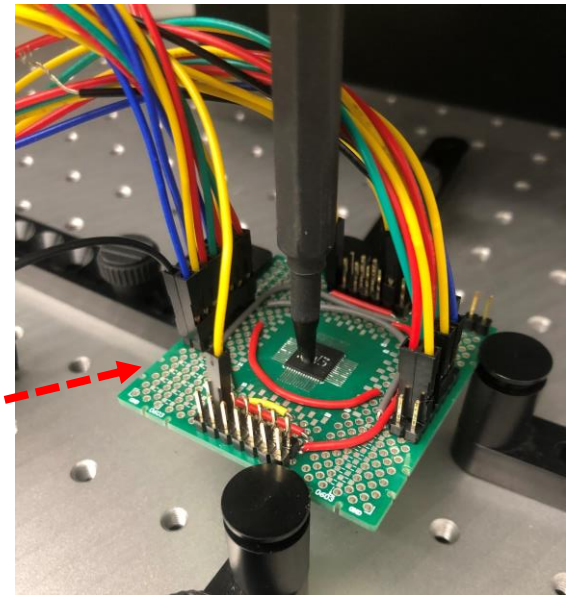


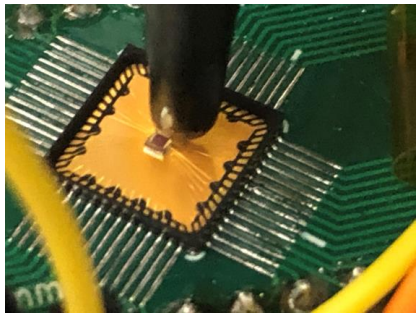
Measurement Setup

- Riscure EM probe station
- 1mm diameter EM probe



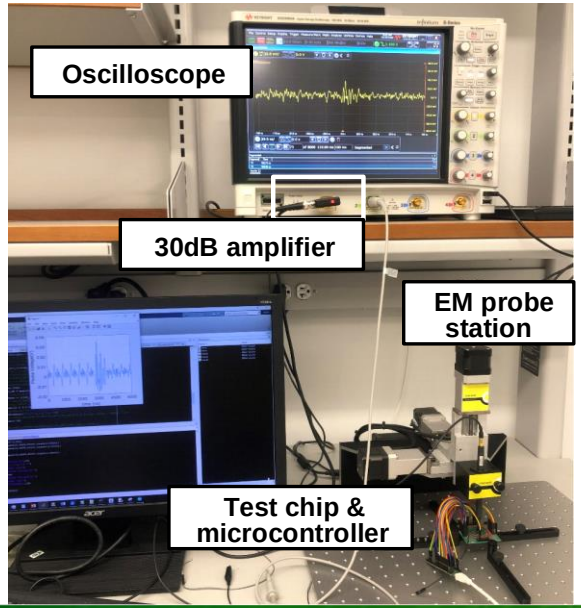
Closeup photo of the EM probe with the packaged and de-packaged chip





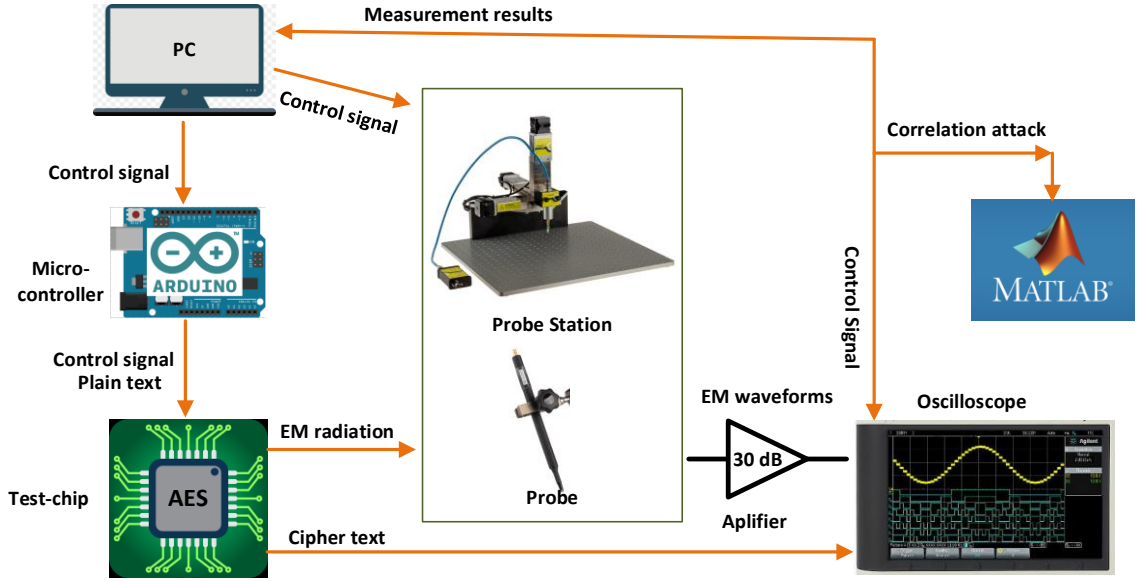
Measurement Setup

- Riscure EM probe station
- 1mm diameter EM probe



All scans are automated using a python script

Measurement flow



Measurement Summary

- Design 1: Baseline design
- Design 2: Dense power grid
- Design 3:Twisted power grid
- Design 4: Extra wide VSS shield
- Design 5: Extra Decaps
- Design 6: Thin and dense VSS shield
- Design 7: Extra wide VSS shield
- Design 8: Extra wide VSS shield, without Via7
- Design 9: Isolated S-Box placement

Technology	40nm CMOS
Operating Voltage	1.1V
Package	QFN56
Clock Frequency	75MHz~37.5MHz
AES Core Area	15,625μm^2
Throughput	128b/10 clock
S-Box Algorithm	Composite Arithmetic
Power @ 75MHz	(mW)
Design 1	2.60
Design 4	2.53
Design 5	2.51
Design 8	2.46

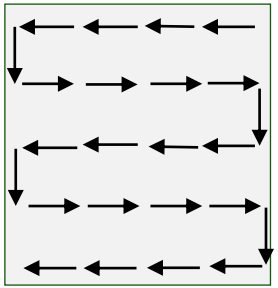
Outline

- Side-channel Analysis (SCA)
- Fine-grained EM SCA simulation
- Proposed physical design strategies
- Fine-grained EM measurement
  - Equipment and setup
  - EM measurement
  - SCA results
- Conclusion
- Acknowledgements

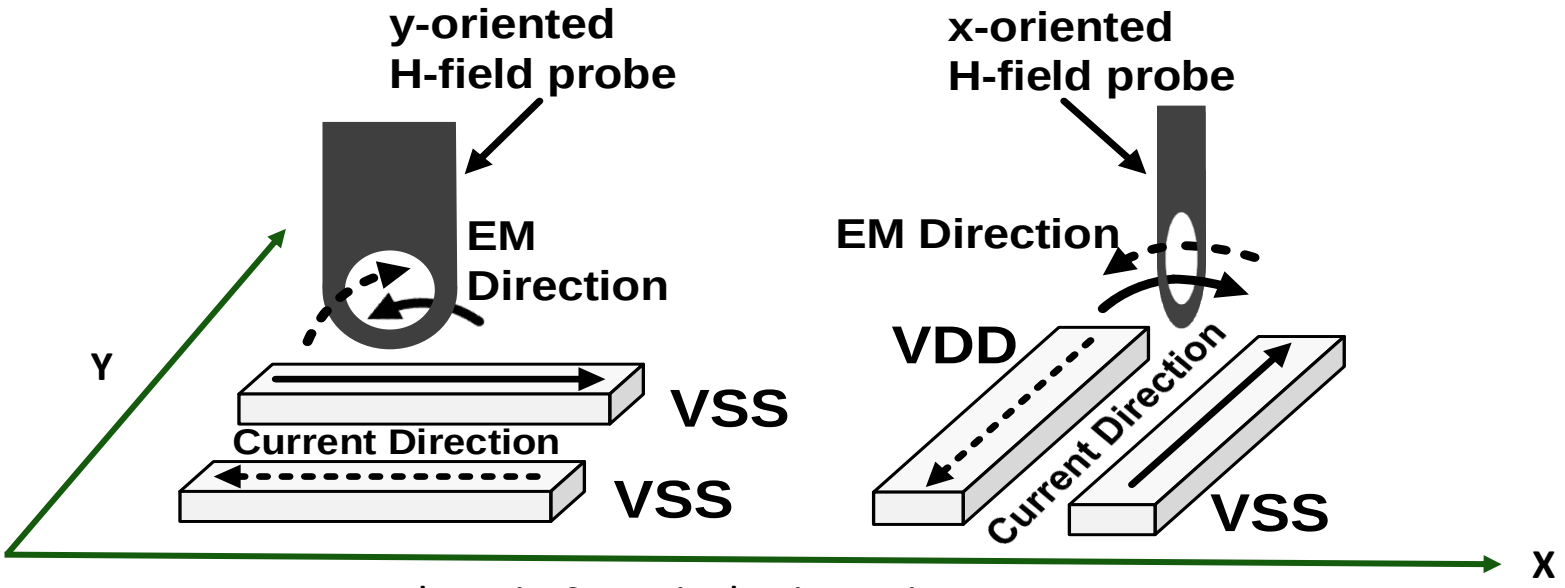
EM Measurement: Adaptive scan approach

- Measurements are performed in 2 phases
  - Phase I: scan entire chip surface for initial successful acquisition
  - Phase II: perform localized scans to optimize acquisition

- Probe scan across the package in zig zag pattern



EM Measurement: Scan Orientation

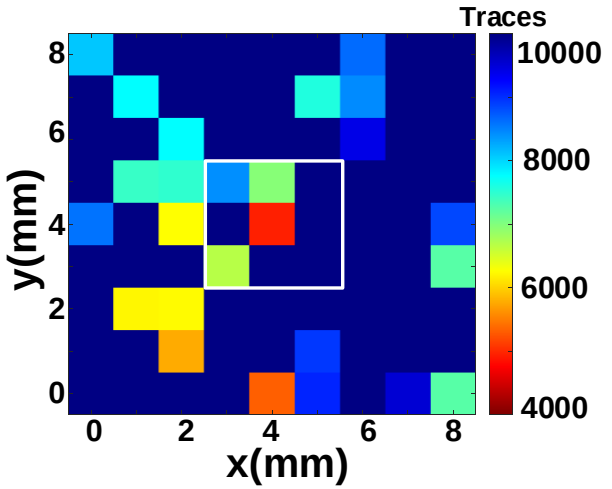


- Measurements are done in 2 vertical orientations
- Y-oriented probe measures current flowing in x direction
- X-oriented probe measures current flowing in y direction

EM Measurement: Adaptive scan approach Phase I

- Phase I scans entire chip surface
- Recover every key byte for at least one orientation and one position
- Location, orientation and min. MTD corresponding to each byte will be passed on to phase II

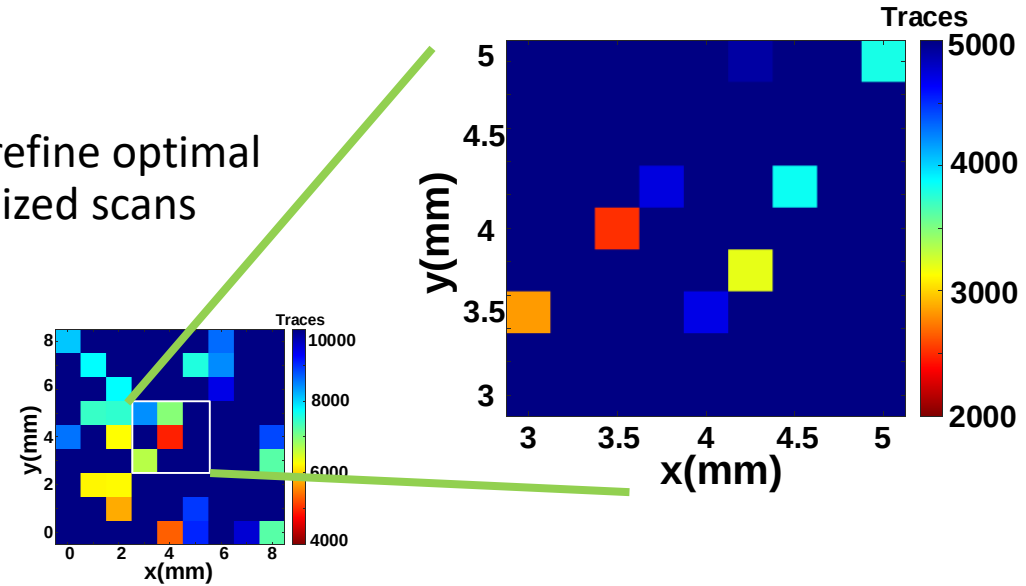
MTD Map for Design #1 Key Byte 1



EM Measurement: Adaptive scan approach Phase II

- Phase II performs localized scans for individual bytes
- Using info found in phase I, refine optimal location by increasingly localized scans
- Measurement cost

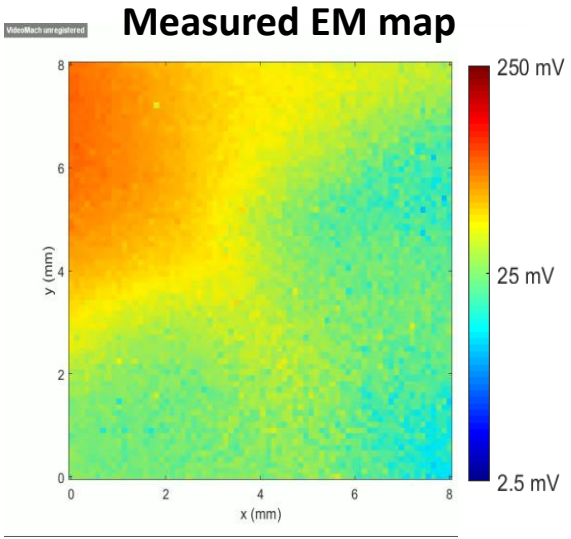
$$\sum_{b=1}^{16} mMTD_b^{N_{\text{scan}}^{\text{II}}}$$



Outline

- Side-channel Analysis (SCA)
- Fine-grained EM SCA simulation
- Proposed physical design strategies
- Fine-grained EM measurement
  - Equipment and setup
  - EM measurement
  - SCA results
- Conclusion
- Acknowledgements

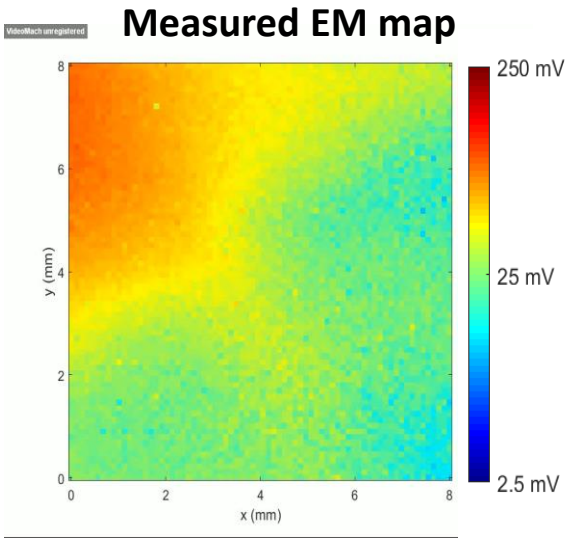
Design 1 fine-grained EM measurement Results

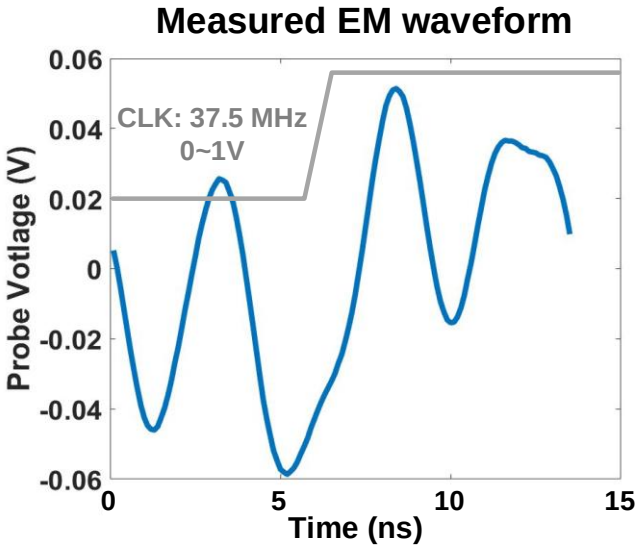


Design 2 ~ 4 are powered off when Design 1 is operating

- Observe fine-grained EM emanations on Design 1 (baseline) during the last encryption cycle at 101 × 101 locations across the package in x-orientation

Design 1 fine-grained EM measurement Results

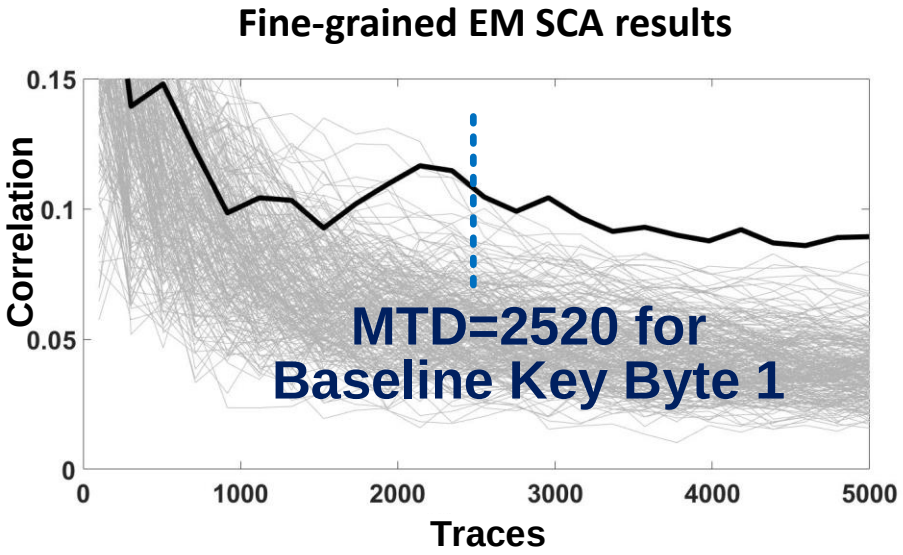


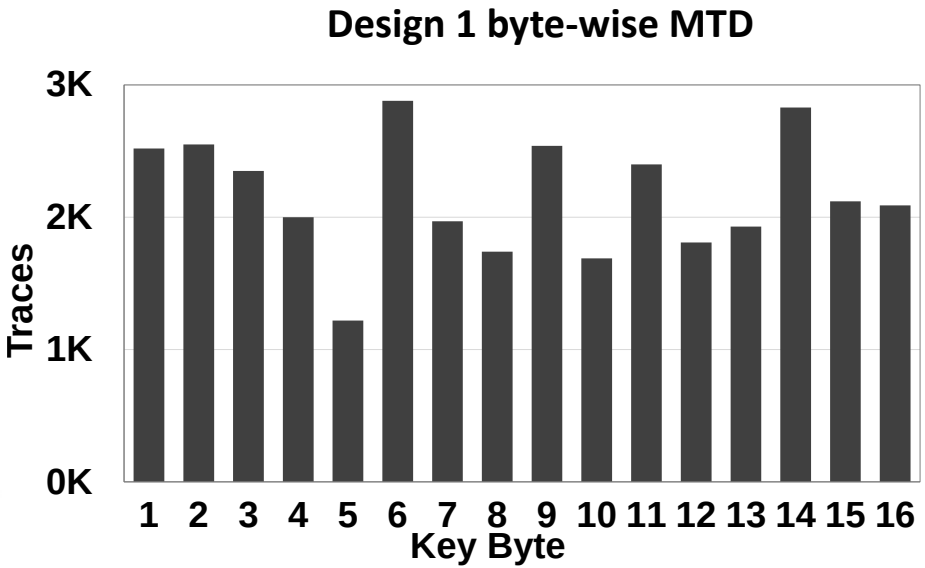


Design 2 ~ 4 are powered off when Design 1 is operating

- Observe fine-grained EM emanations on Design 1 (baseline) during the last encryption cycle at 101 × 101 locations across the package in x-orientation
- Observed EM trace at the package center

Design 1 fine-grained EM SCA Results

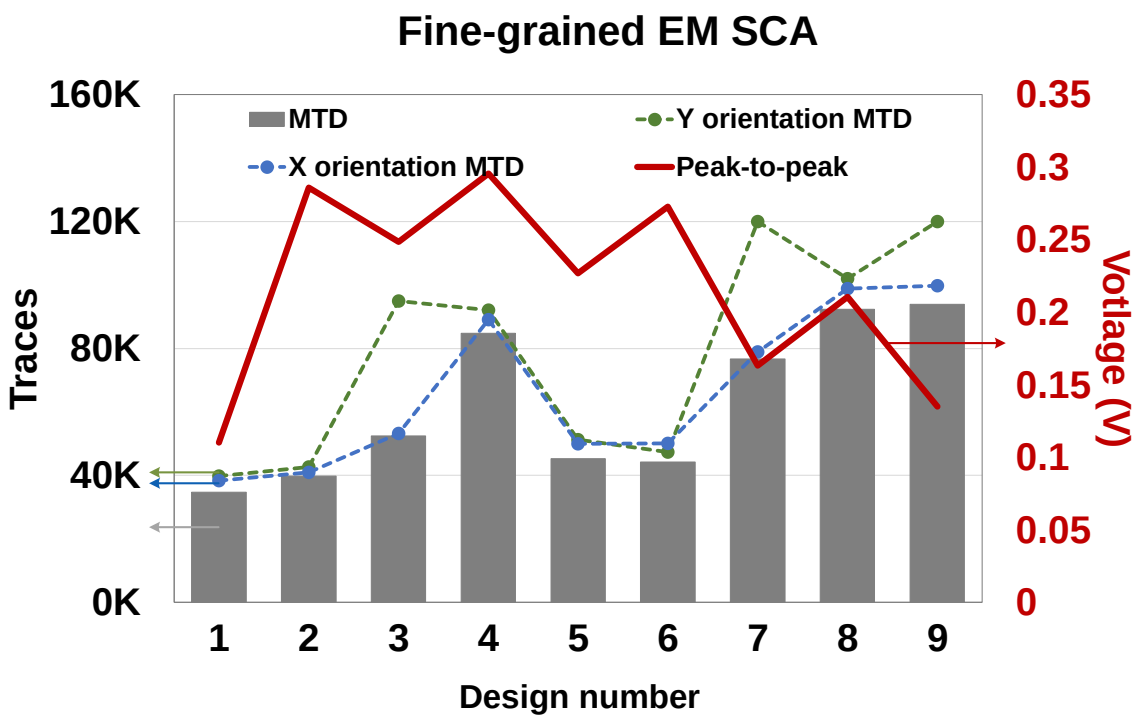




- Correlation result showing Key Byte 1 is revealed using 2520 traces
- MTD of each key byte is in range of 1000 traces to 3000 traces

Fine-grained EM SCA Results

- For each proposed design
  - MTD cost of recovering key for each orientation along with final MTD cost of attack
  - Peak-to-peak EM signal measured at chip center



Fine-grained EM SCA analysis

- Improvement of fine-grained EM SCA resilience for each of the proposed physical design strategies

Design #	Design strategy	$\sum_{b=1}^{16} \mathrm{MTD}_b^y$	$\sum_{b=1}^{16} \mathrm{MTD}_b^x$	$\sum_{b=1}^{16} min\{\mathrm{MTD}_b^x, \mathrm{MTD}_b^y\}$	Improvement compared to Design 1
Design 1	Baseline Design	39850	38400	34650	-
Design 2	Dense PG on M7/8	42650	41000	39850	1.15x
Design 3	Dense twisted PG on M7/8	94970	53170	52500	1.51x
Design 4	Wide VSS shield on M7/8	92030	89010	84750	2.45x

Fine-grained EM SCA analysis

- Improvement of fine-grained EM SCA resilience for each of the proposed physical design strategies

Design #	Design strategy	$\sum_{b=1}^{16} \mathrm{MTD}_b^y$	$\sum_{b=1}^{16} \mathrm{MTD}_b^x$	$\sum_{b=1}^{16} min\{\mathrm{MTD}_b^x, \mathrm{MTD}_b^y\}$	Improvement compared to Design 1
Design 1	Baseline Design	39850	38400	34650	-
Design 2	Dense PG on M7/8	42650	41000	39850	1.15x
Design 3	Dense twisted PG on M7/8	94970	53170	52500	1.51x
Design 4	Wide VSS shield on M7/8	92030	89010	84750	2.45x
Design 5	Extra DeCap cells	51250	50000	45300	1.31x
Design 6	Extra DeCap + Thin VSS shield on M7/8	47400	50100	44200	1.28x
Design 7	Extra DeCap + Wide VSS shield on M7/8	120000<	78850	76650	2.21x
Design 8	Extra DeCap + Wide VSS shield on M7/8 (no Via7)	101950	98850	92350	2.67x
Design 9	Isolated S-box placement	120000<	99800	93850	2.71x

Conclusion

- Fine-grained EM SCA is powerful yet can be mitigated using basic physical design strategies with no power overhead
  - Adding extra DeCap
  - Adding shielding grid

- Multiple strategies can be combined to father increase SCA resilience.

Acknowledgements

This research is supported in parts by Intel, Silicon Labs, and NSF. Authors thank TSMC for chip fabrication.


OBRIGADO
gracias
どうも
ARIGATO
hvala
DANK U
takk
MERSI
merci
謝謝
obrigado
danke schön
köszi
سپاس
PALDIES
muchas gracias
ありがとう
TEŞEKKÜR EDERIM
MOLTE GRAZIE
GO RAIBH MAITH AGAT
danke
grazas
GRAZZI
THANKS
THANK YOU
благодаря
TAK
どうも
quan
TAK
asante
muchas gracias
vielen dank
PALDIES
OBRIGADO
mesi
DANK U
danke
감사합니다
köszi
благодаря
grazie
DZIEKI
TACK
Gràcies
MULTUMESC
多謝
شکراً
TEŞEKKÜR EDERIM
NA GODE
muchas gracias
obrigado
спасибо