CICC

IEEE Custom Integrated Circuits Conference

15-2: Power and Electromagnetic Side-Channel Attack Resilient Secure AES Core utilizing Galvanic Isolation approach with Integrated Charge Pump based Power Management

Meizhi Wang, Shanshan Xie, Ping Na Li, Aseem Sayal, Ge Li, Vishnuvardhan V. Iyer, Aditya Thimmaiah, Michael Orshansky, Ali E. Yilmaz, and Jaydeep P. Kulkarni
ECE Department, University of Texas at Austin
E-mail: wang.mz@utexas.edu, jaydeep@austin.utexas.edu

28 April 2021

TEXAS
The University of Texas at Austin

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

IEEE SOLID-STATE CIRCUITS SOCIETY™

IEEE

Outline

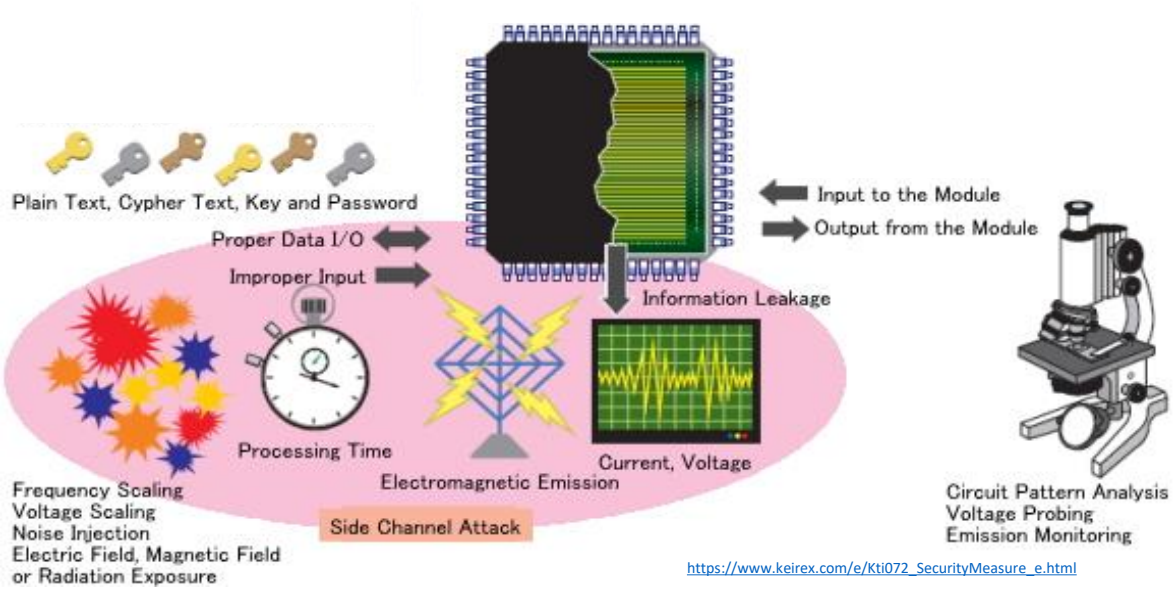
- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

Side Channel Analysis

- Easy physical access
- Inexpensive
- High successful rate



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

Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

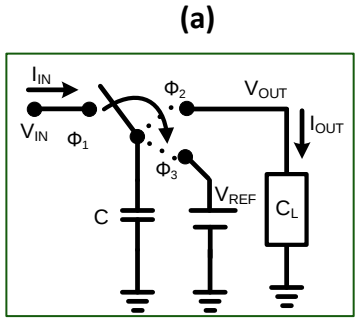
Prior Work: Power SCA resilient approaches

- Constant Current Signature

- Randomized Current Signature

Prior Work: Power SCA resilient approaches

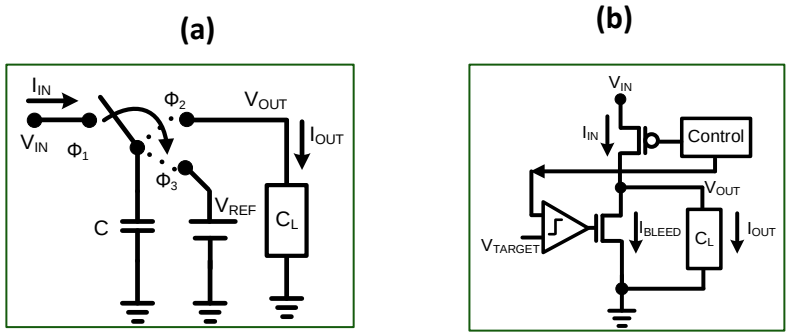
- Constant Current Signature
  - (a) Switch Capacitor Current Equalizer



- Randomized Current Signature

Prior Work: Power SCA resilient approaches

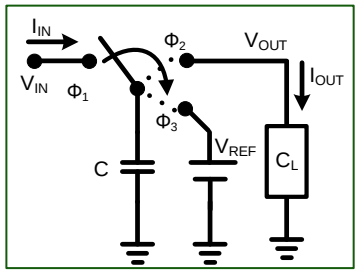
- Constant Current Signature
  - (a) Switch Capacitor Current Equalizer
  - (b) Shunt Regulator
- Randomized Current Signature



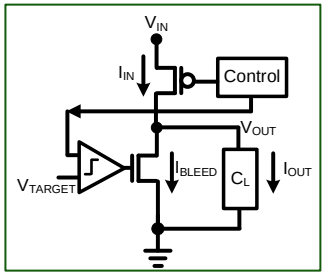
Prior Work: Power SCA resilient approaches

- Constant Current Signature
  - (a) Switch Capacitor Current Equalizer
  - (b) Shunt Regulator
- Randomized Current Signature
  - (c) Low Drop Out Regulator

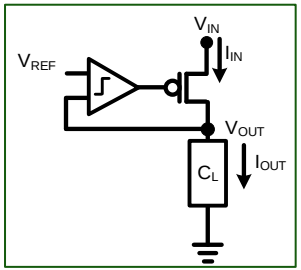
(a)



(b)

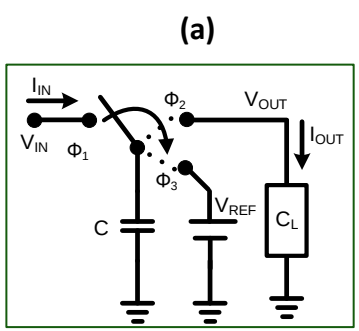


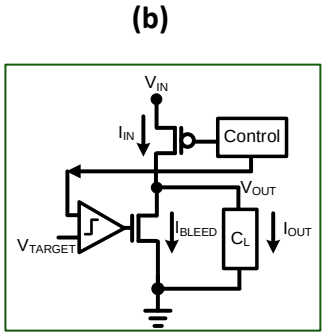
(c)

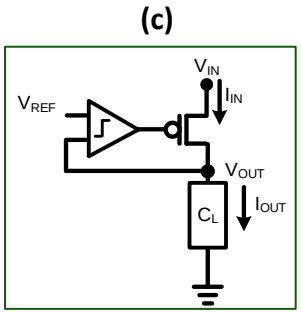


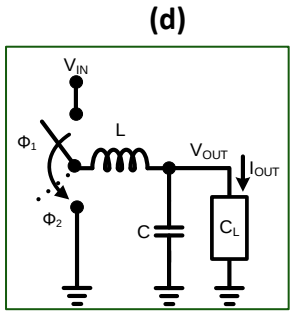
Prior Work: Power SCA resilient approaches

- Constant Current Signature
  - (a) Switch Capacitor Current Equalizer
  - (b) Shunt Regulator
- Randomized Current Signature
  - (c) Low Drop Out Regulator
  - (d) Buck Converter



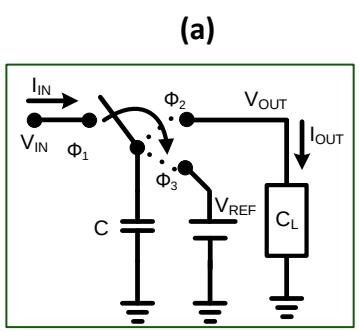


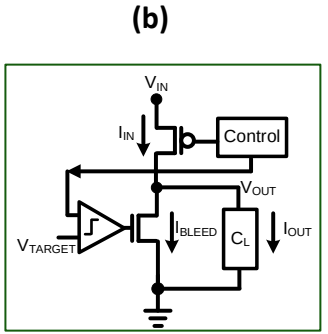


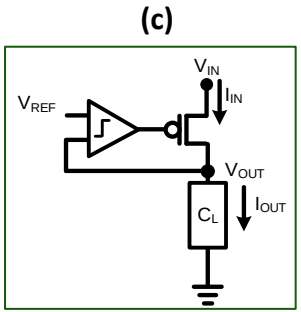


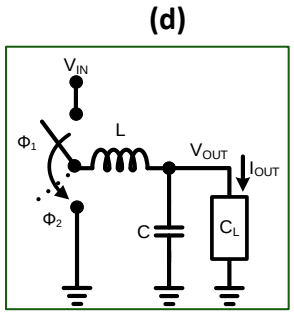
Prior Work: Power SCA resilient approaches

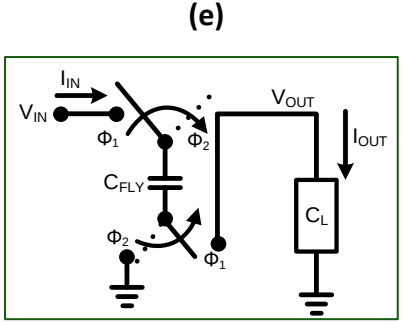
- Constant Current Signature
  - (a) Switch Capacitor Current Equalizer
  - (b) Shunt Regulator
- Randomized Current Signature
  - (c) Low Drop Out Regulator
  - (d) Buck Converter
  - (e) Switched-Capacitor Voltage Regulator







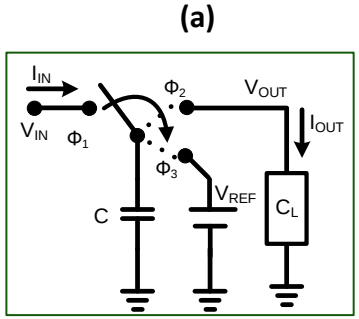


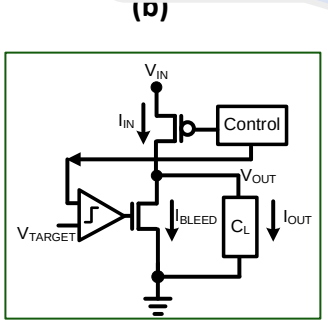


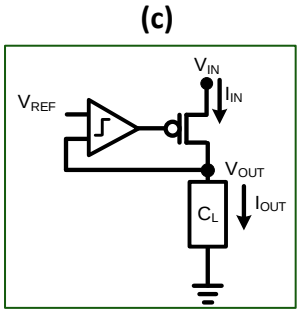
Prior Work: Power SCA resilient approaches

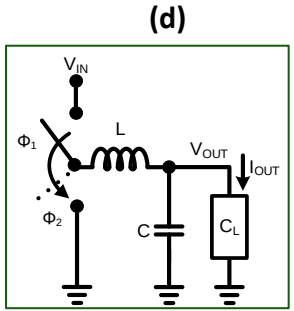
No VSS pins are isolated in these approaches

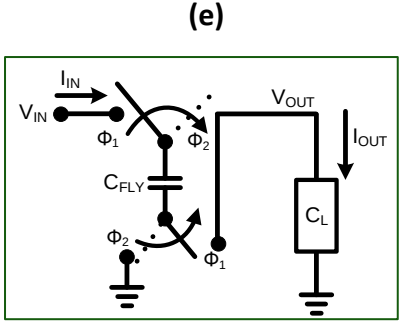
- Constant Current Signature
  - (a) Switch Capacitor Current Equalizer
  - (b) Shunt Regulator
- Randomized Current Signature
  - (c) Low Drop Out Regulator
  - (d) Buck Converter
  - (e) Switched-Capacitor Voltage Regulator







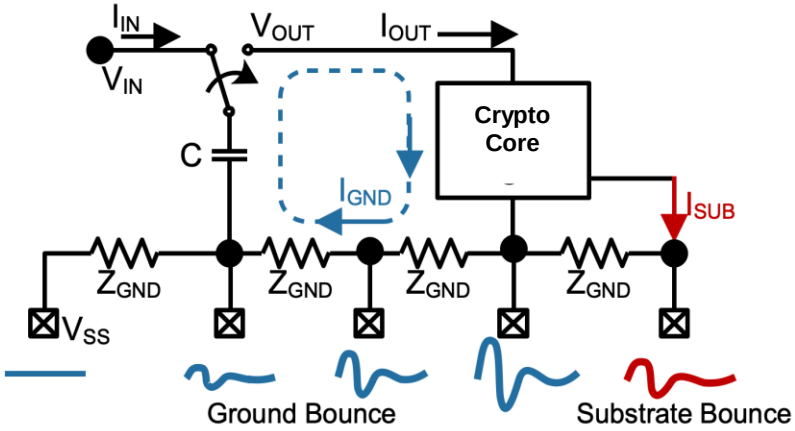


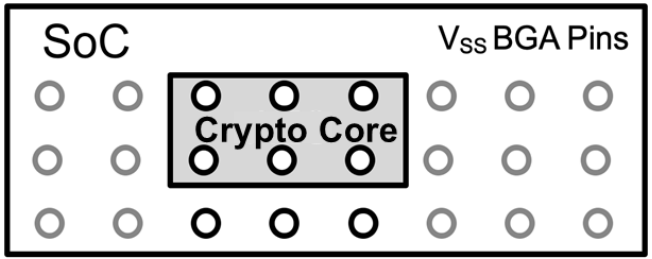


Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

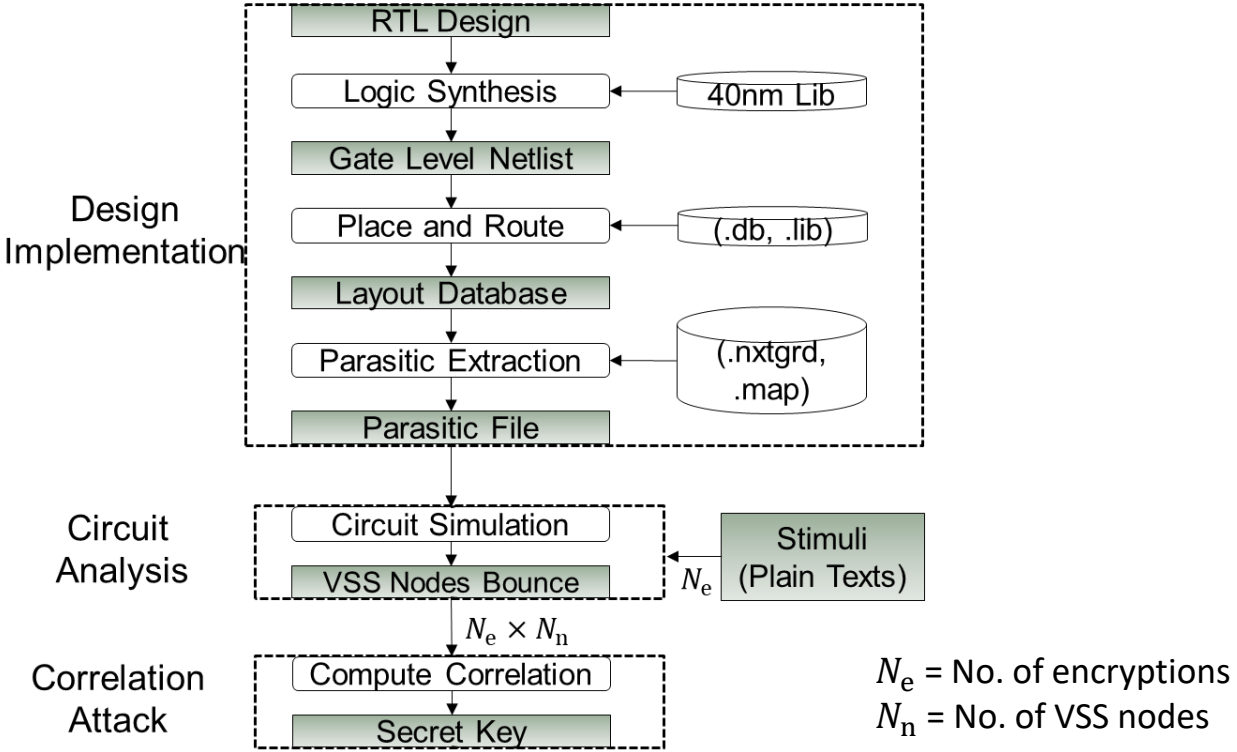
Motivation: Susceptibility to the ground bounce





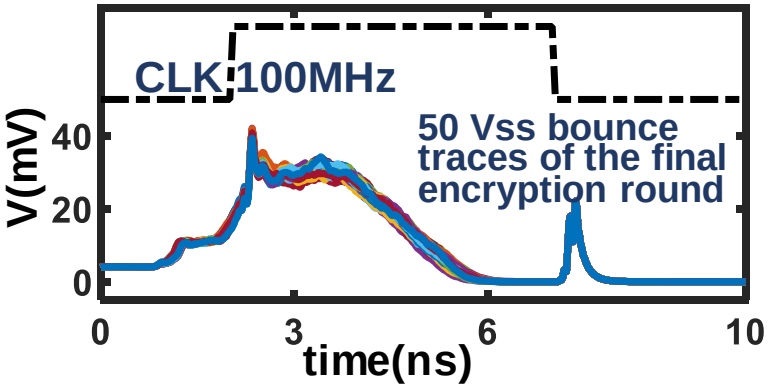
- Ball grid array (BGA) pins near to crypto core may reveal circuit VSS bounce that can be used for side-channel analysis

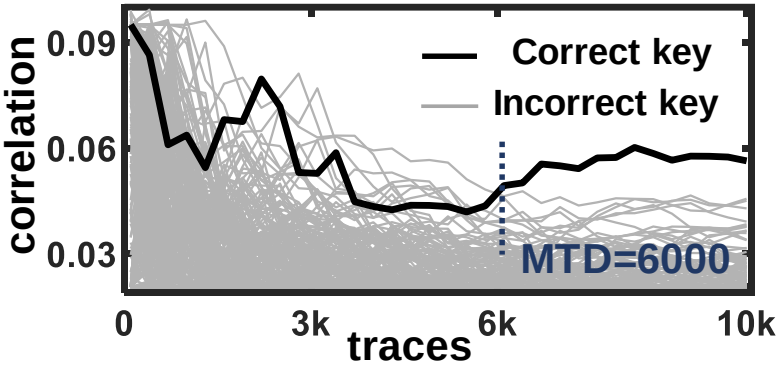
Simulation flow



N_e = No. of encryptions
N_n = No. of VSS nodes

Simulation results on a 128-bit AES computing core





- Implement a 128b Advanced Encryption standard (AES) core
- Simulated VSS bounce waveforms for correlation attack

- Correlation attack shows key byte 1 is revealed using 6000 traces

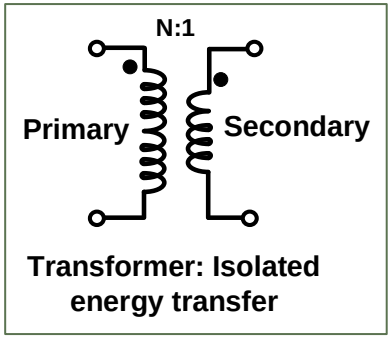
Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

Principle of Galvanic Isolation (GI)

- Isolates two electrical systems, preventing direct current flow and breaking ground loops between two circuits.

- Transformer:
  - Primary (input) side potentially lethal transient voltages and currents
  - Secondary side is completely isolated for safety

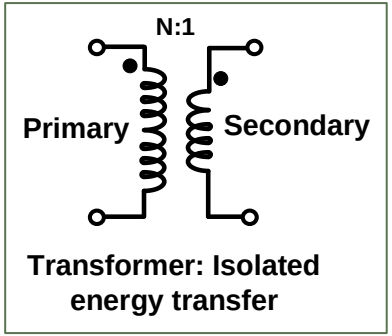


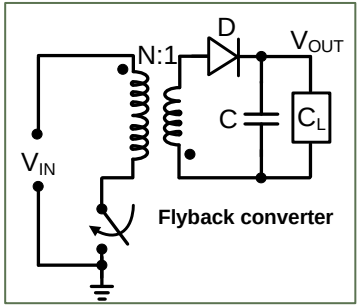
Transformer: Isolated energy transfer

Principle of Galvanic Isolation (GI)

- Isolates two electrical systems, preventing direct current flow and breaking ground loops between two circuits.

- Transformer:
  - Primary (input) side potentially lethal transient voltages and currents
  - Secondary side is completely isolated for safety
  - Flyback converter:
    - Inductor based Galvanic Isolation topology
    - Protecting low voltage devices from high voltages transients



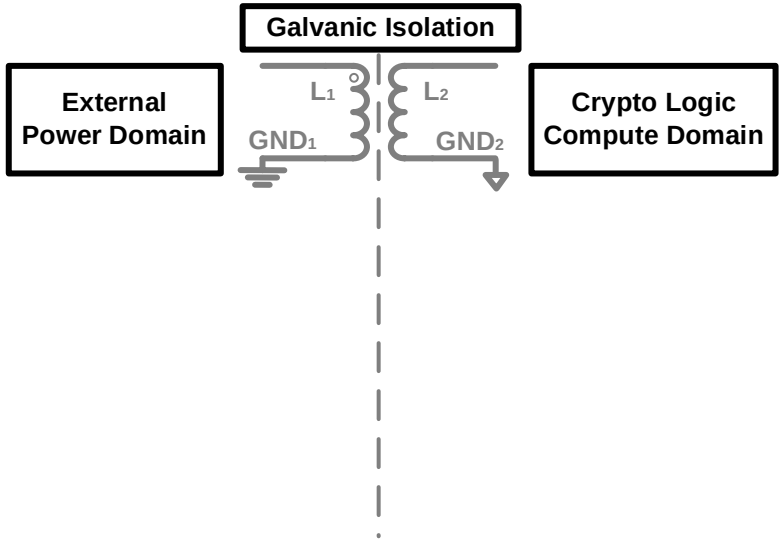


Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

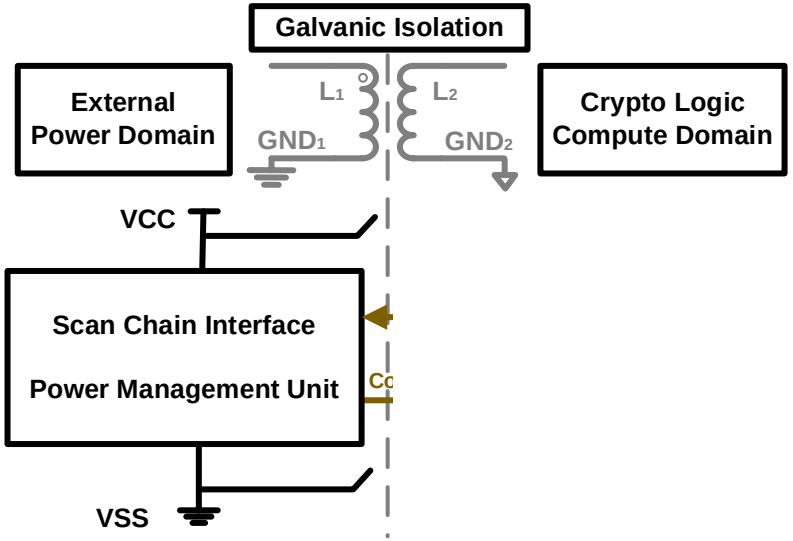
Proposed GI AES

- Apply capacitor based Galvanic Isolation topology to minimize ground bounce susceptibility
- Primary side: external power domain
- Secondary side: crypto core power domain



Proposed GI AES

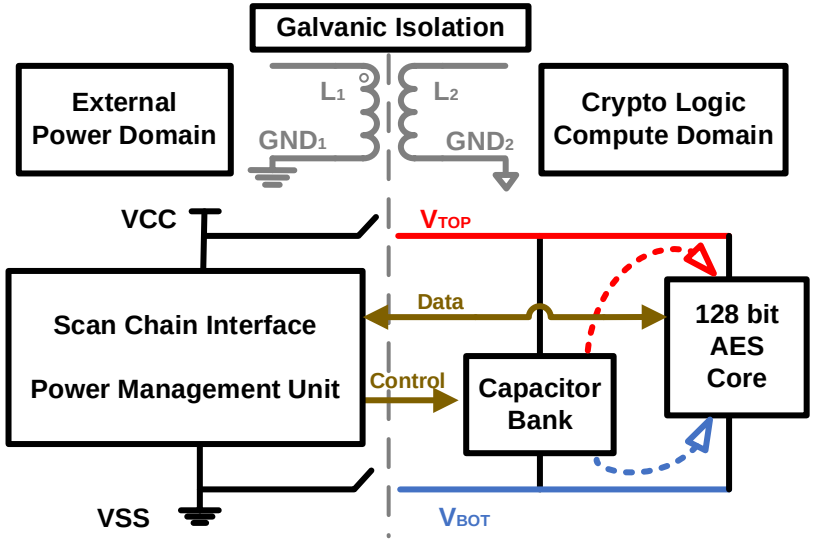
- Apply capacitor based Galvanic Isolation topology to minimize ground bounce susceptibility
- Primary side: external power domain
  - Scan chain Interface
  - Power management unit
- Secondary side: crypto core power domain



Proposed GI AES

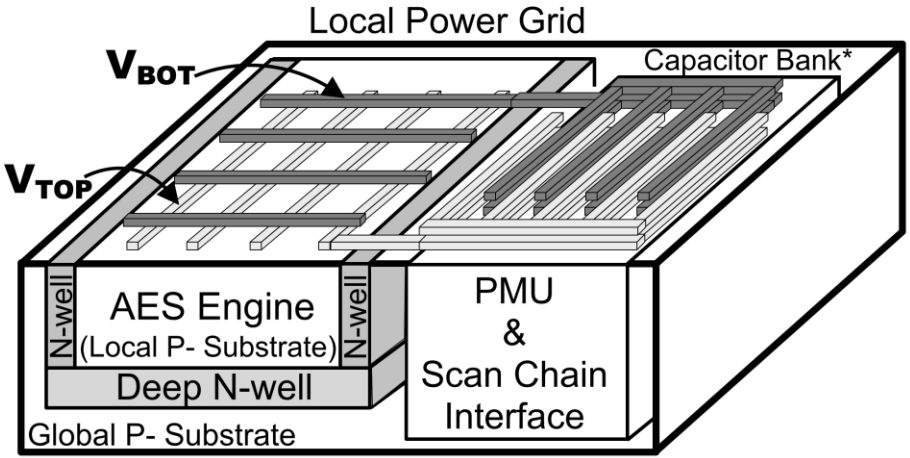
Galvanic isolation decouples AES engine compute domain and external power domain completely

- Apply capacitor based Galvanic Isolation topology to minimize ground bounce susceptibility
- Primary side: external power domain
  - Scan chain Interface
  - Power management unit
- Secondary side: crypto core power domain
  - Capacitor bank
  - A 128-bit AES core

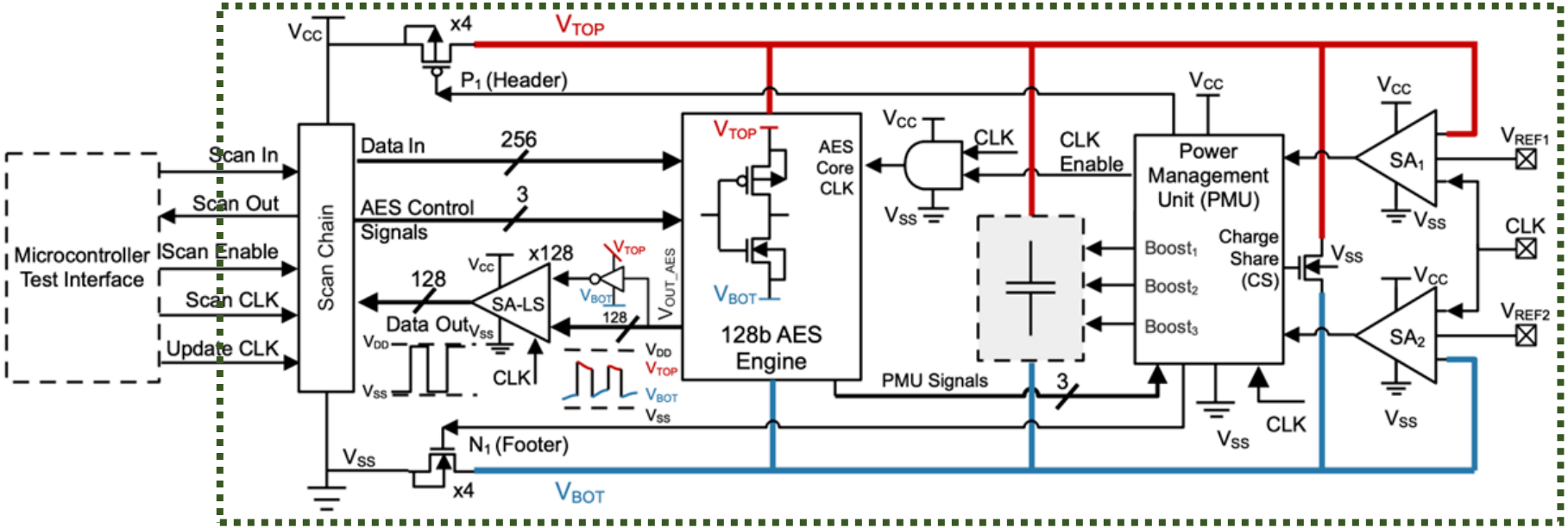


Proposed GI AES

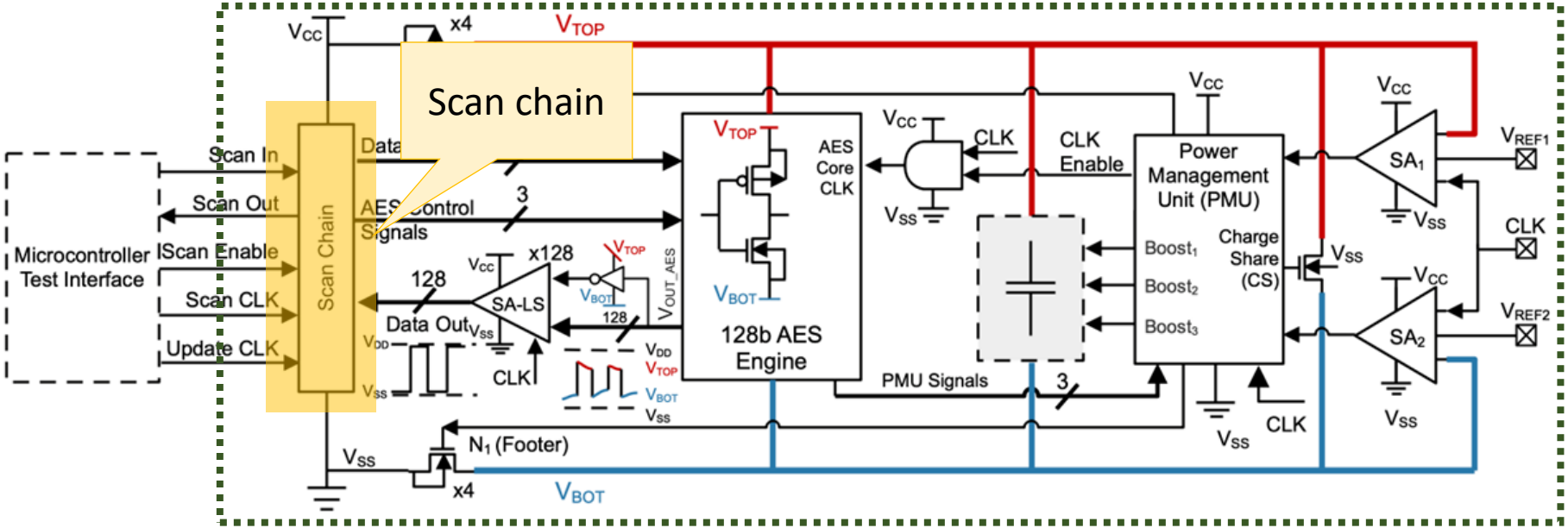
- 3D illustration:
  - AES in deep N-well, isolated P-substrate, powered by V_{TOP} V_{BOT}
  - Capacitor bank (*2 layers drawn for illustration purpose)
  - PMU and scan chain interface



GI-AES Architecture: System overview

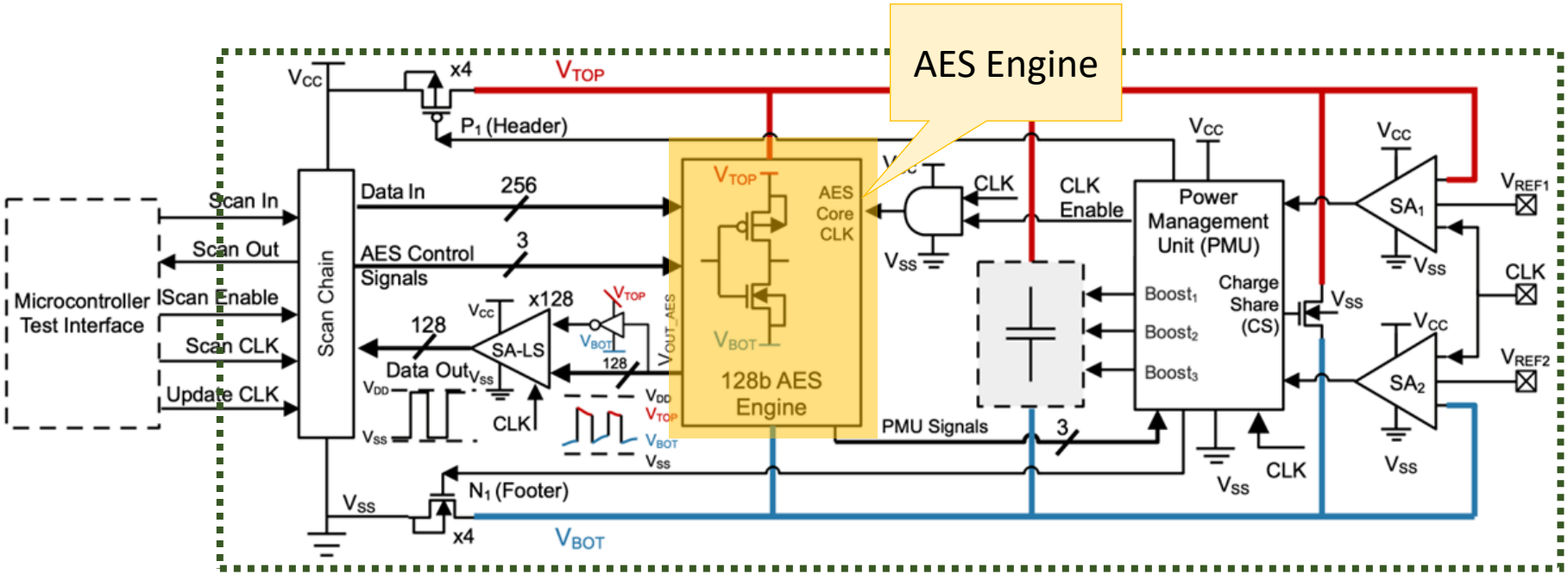


GI-AES Architecture: Main blocks



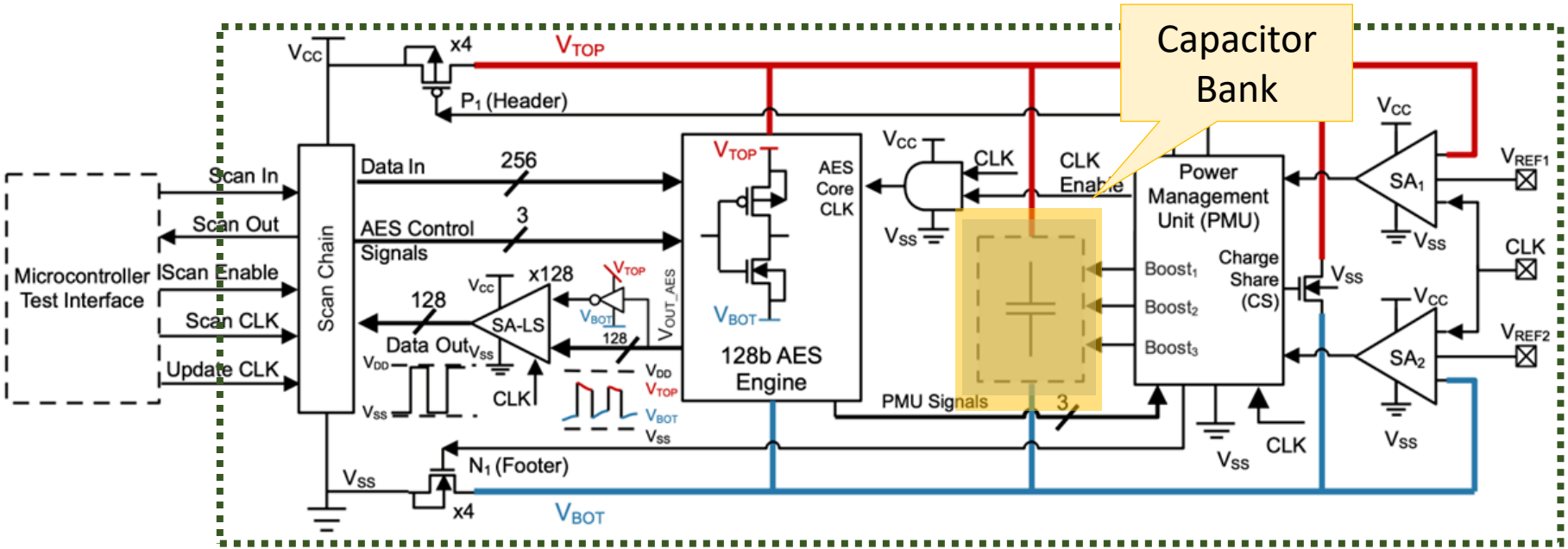
- Scan chain interface for data exchanging

GI-AES Architecture: Main blocks



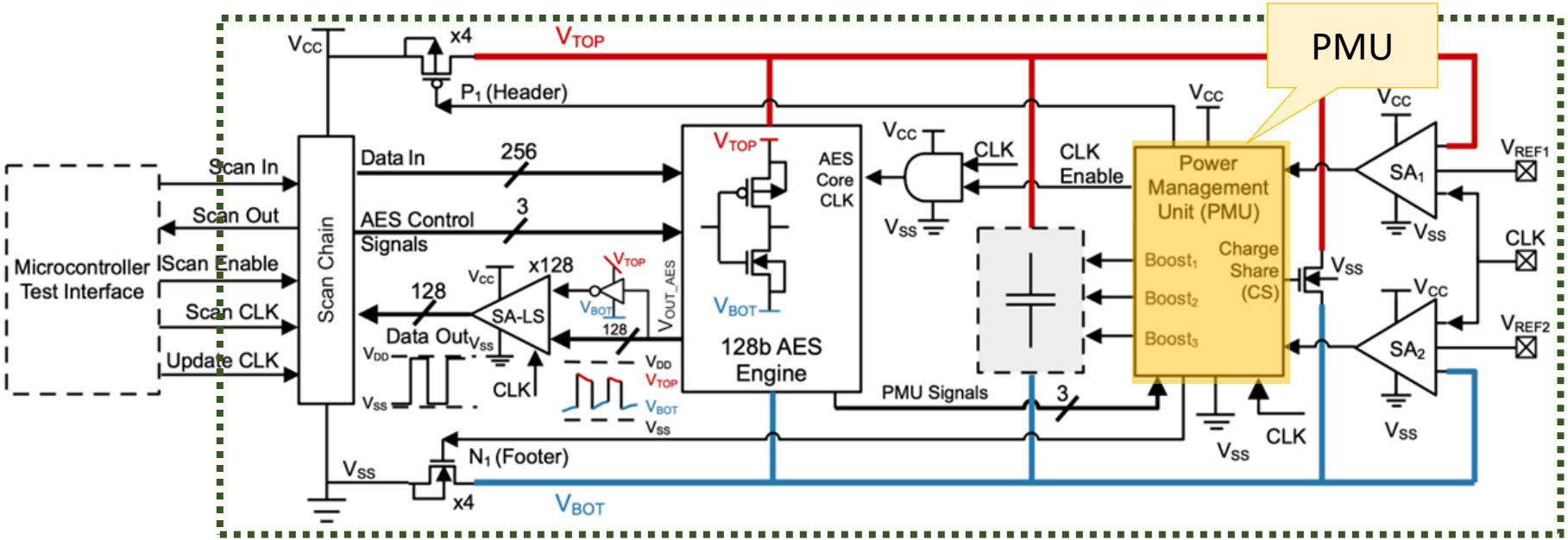
- A 128b AES Engine for data encryption
- Operating in V_{TOP}/V_{BOT} power domain

GI-AES Architecture: Main blocks



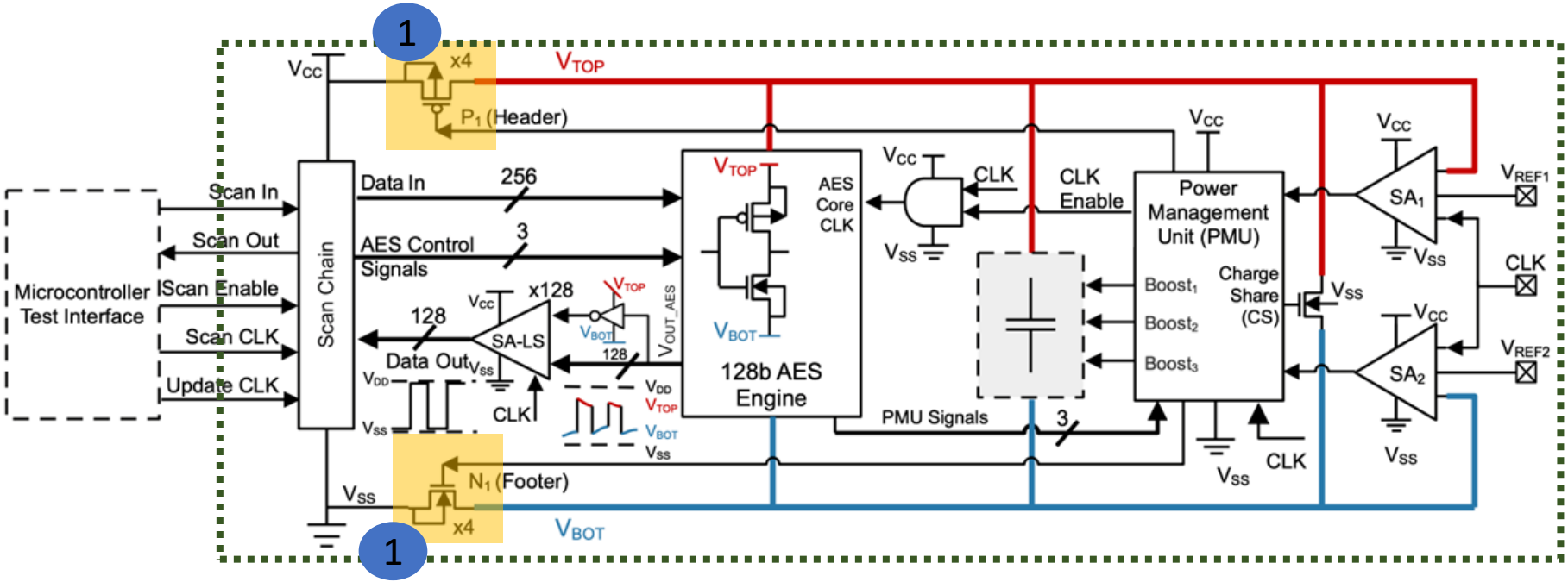
- Capacitance based galvanic isolation
- Power AES in V_{TOP}/V_{BOT} domain during encryption

GI-AES Architecture: Main blocks



- Control capacitor bank to maintain functional V_{TOP}/V_{BOT} voltage range

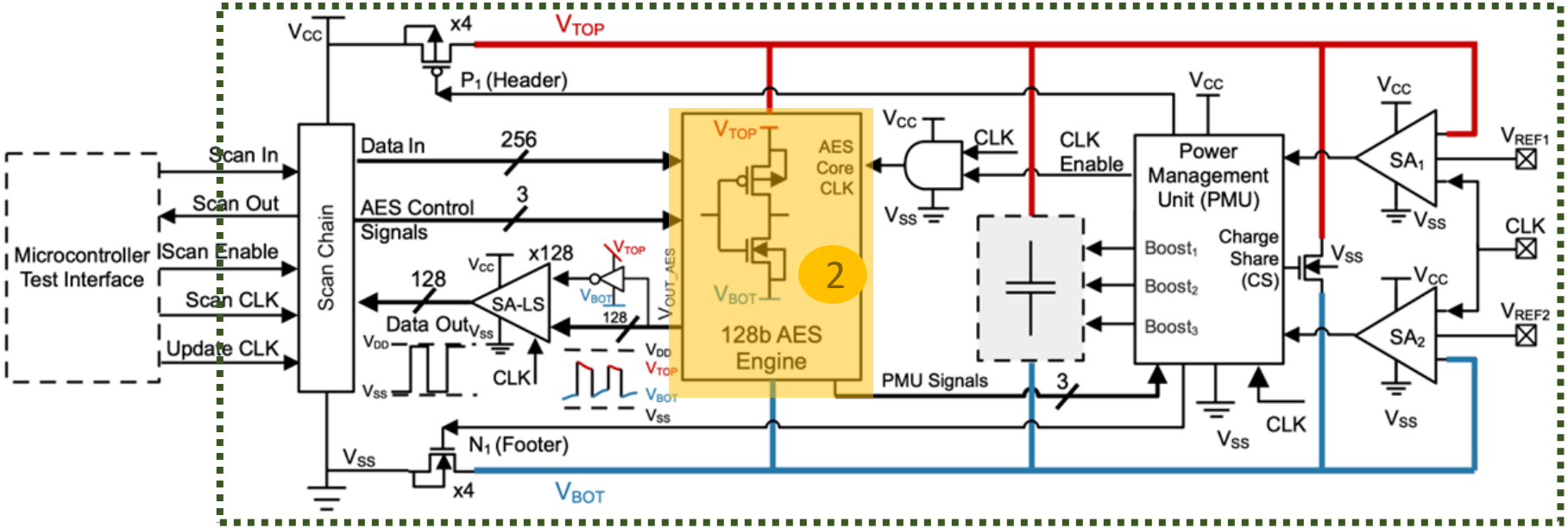
GI-AES Architecture: Design techniques



1 Header and footer transistors: decouple V_{TOP}/V_{BOT} rail from VCC/VSS rail

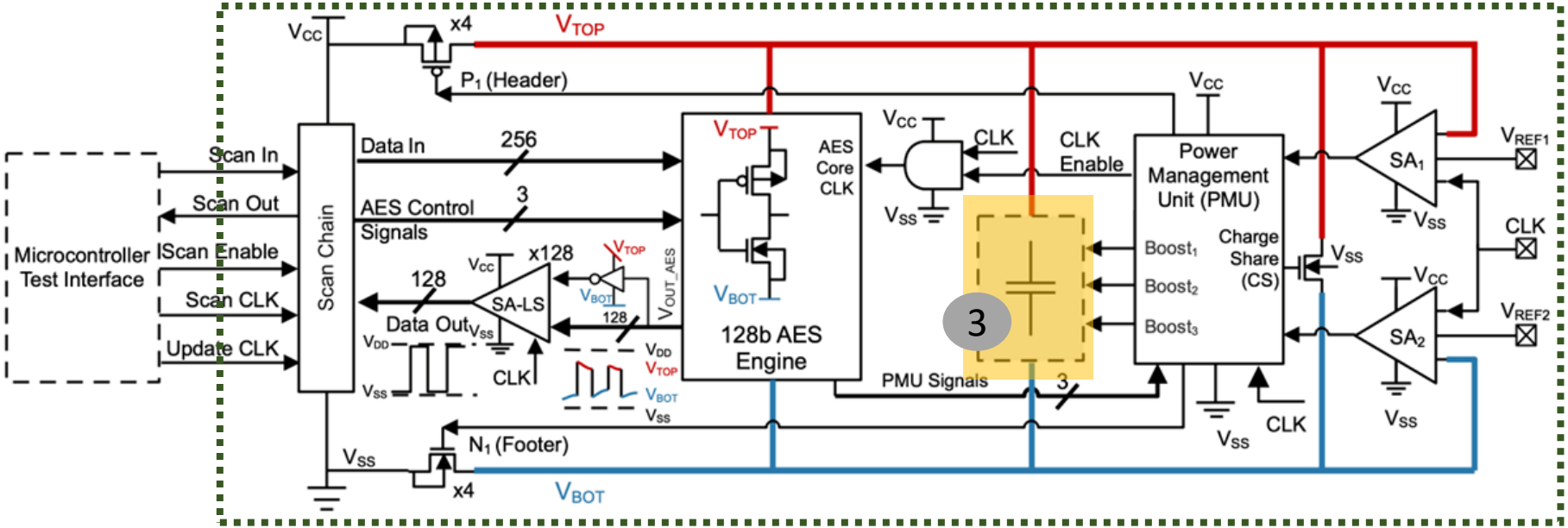
- Isolate the external and the internal power domain (AES).

GI-AES Architecture: Design techniques



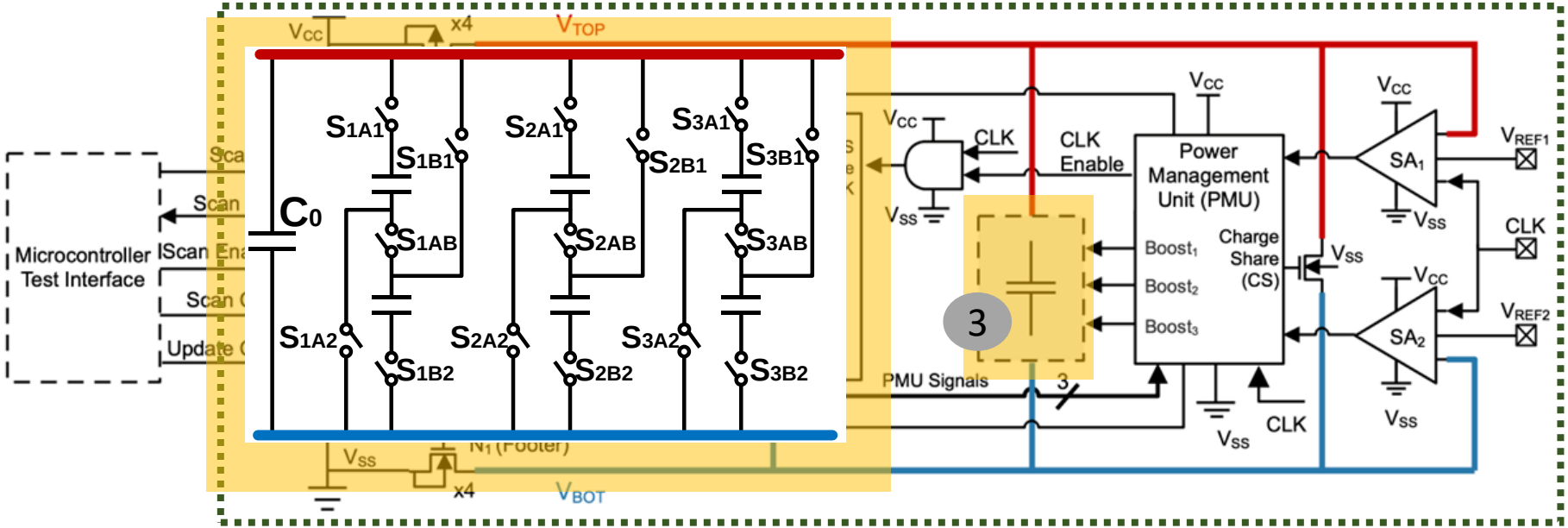
2 Deep N well: covering the AES engine, isolating the local substrate
AES ground is completely isolated

GI-AES Architecture: Design techniques



3 Capacitor banks: charge pump based voltage doubler circuit

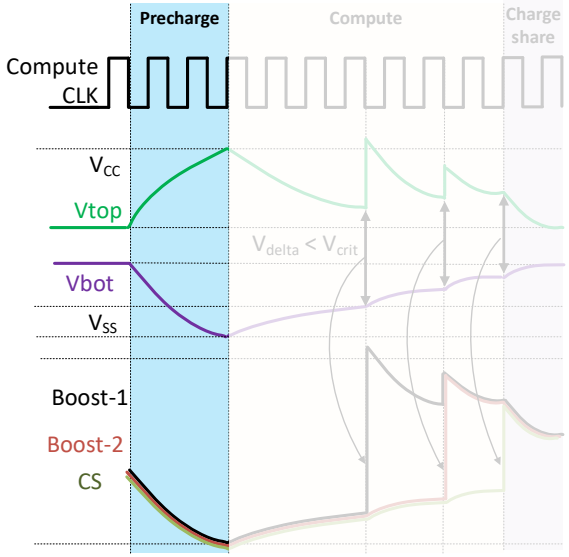
GI-AES Architecture: Design techniques



3 C_0 as the main capacitor and multiple smaller capacitor pairs

- Multi-stage voltage doubler circuit

GI-AES Architecture: Design techniques

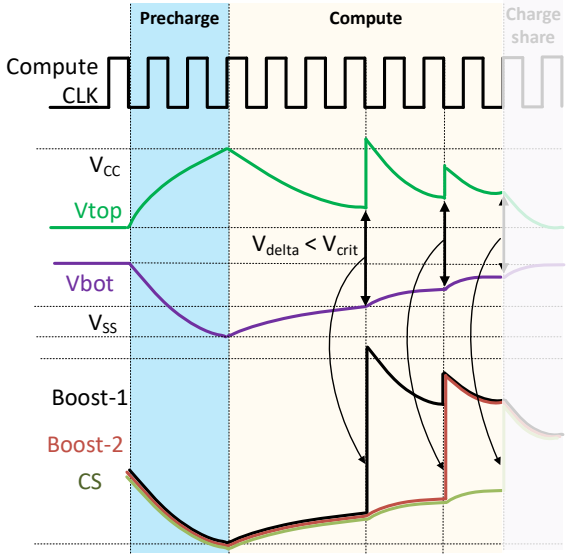


Precharge phase:

- **Header and footer are connected**
- **All capacitors are fully charged to VCC/VSS**

3 Three operation phases: Precharge, Compute, Charge sharing

GI-AES Architecture: Design techniques

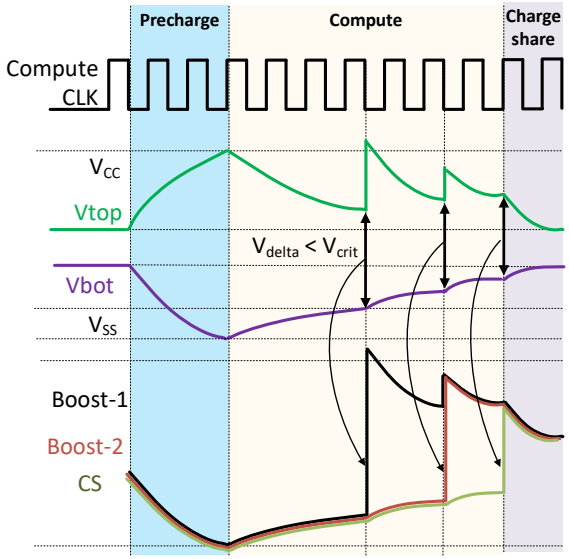


Precharge phase:
- **Header and footer are connected**
- **All capacitors are fully charged to VCC/VSS**

Compute phase:
- **Header and footer are disconnected**
- **Capacitor bank powers AES Core**
- **Voltage boostings are triggered sequentially**

3 Three operation phases: Precharge, Compute, Charge sharing

GI-AES Architecture: Design techniques



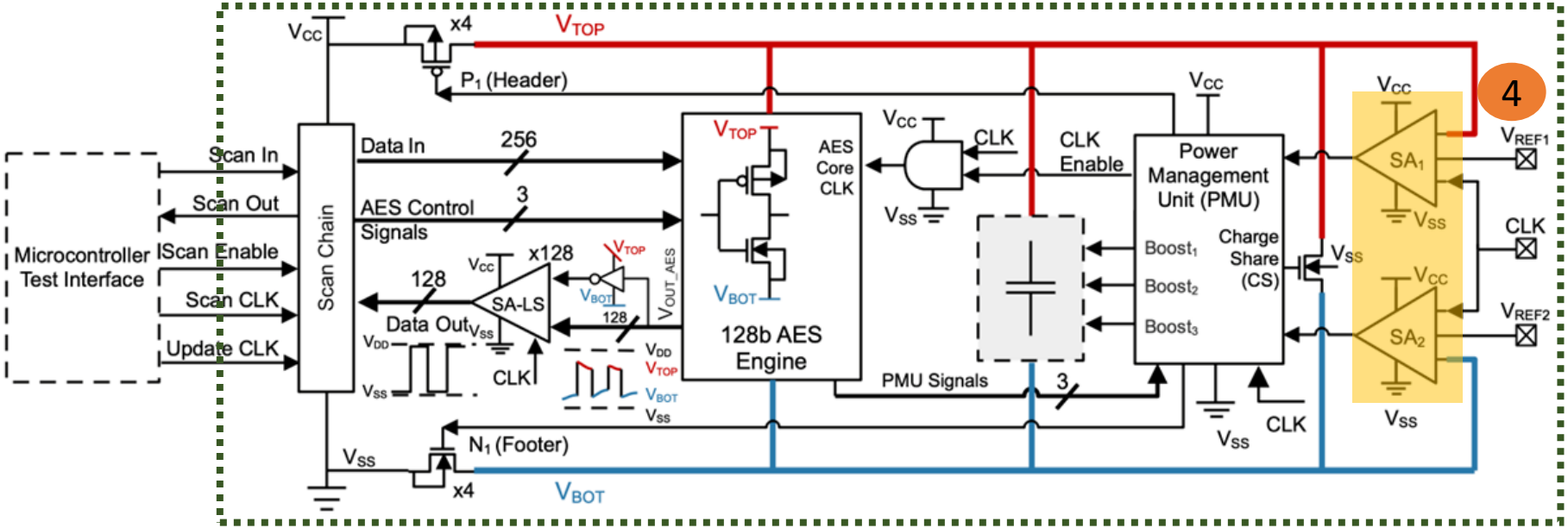
Precharge phase:
- **Header and footer are connected**
- **All capacitors are fully charged to VCC/VSS**

Compute phase:
- **Header and footer are disconnected**
- **Capacitor bank powers AES Core**
- **Voltage boostings are triggered sequentially**

Charge sharing
- **Discharge capacitors to mask real charge consumption**

3 Three operation phases: Precharge, Compute, Charge sharing

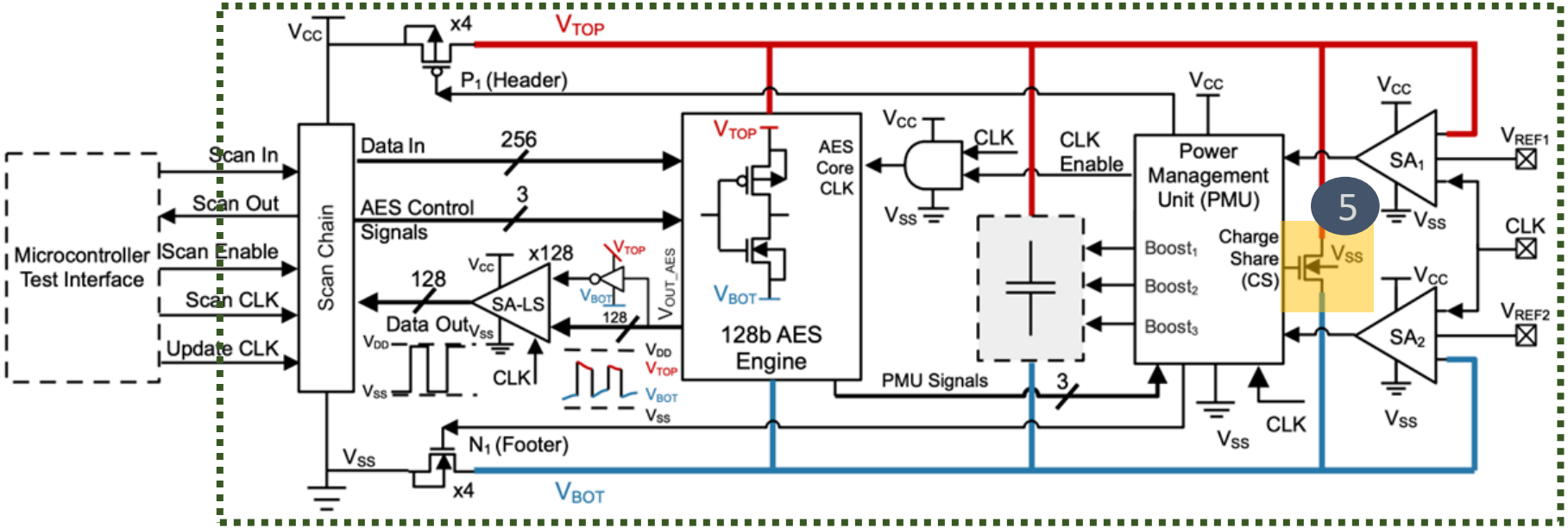
GI-AES Architecture: Design techniques



4 Dual rail sense amp: trigger the next boosting stage if V_{TOP} and V_{BOT} are below V_{ref}

- Current signature remain the same in each cycle, not prone to SCA

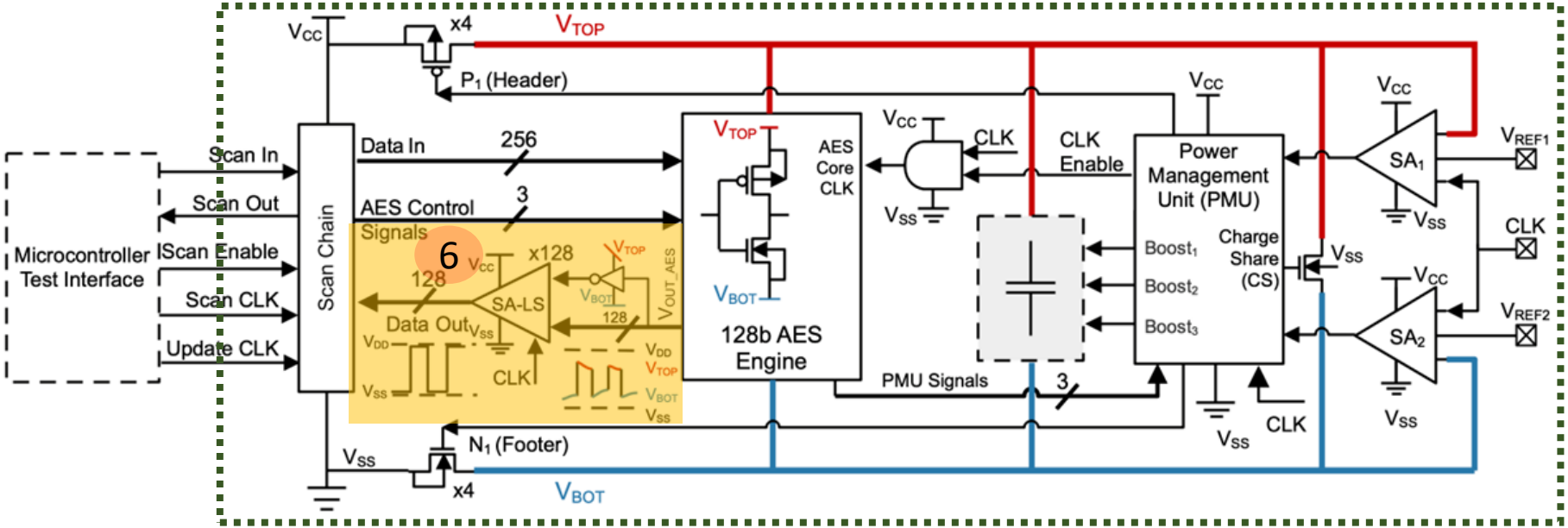
GI-AES Architecture: Design techniques



5 Charge share transistor: discharges all the capacitors to certain predefined voltage.

- Uniform on V_{TOP} and V_{BOT} before each precharge cycle

GI-AES Architecture: Design techniques



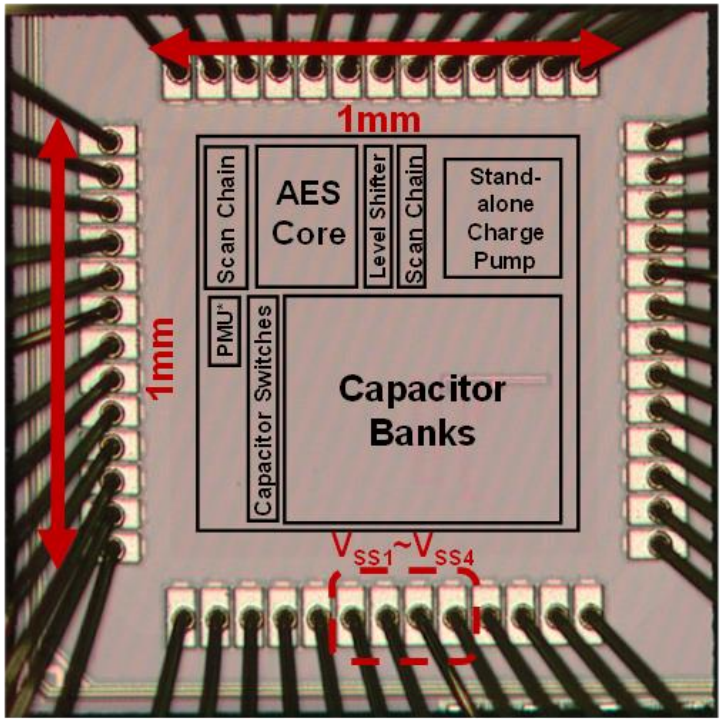
6 Dual rail sense amp (uniform current signature) as a level shifter to transfer signal from voltage level V_{TOP}/V_{BOT} to voltage level VCC/VSS .

Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

Die photo, Measurement Summary

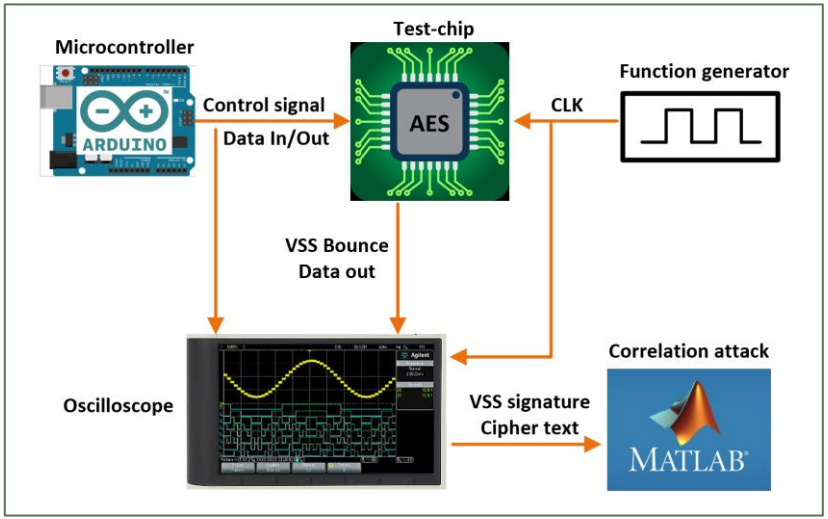
- Technology: 40 nm CMOS
- Power@1.2V: 23 mW
- Area(mm^2):
  - AES Core 0.032
  - Level Shifter 0.00795
  - PMU 0.00136
  - Capacitor Switches 0.00429
  - Capacitor Bank 0.178
  - Total Area 0.2236

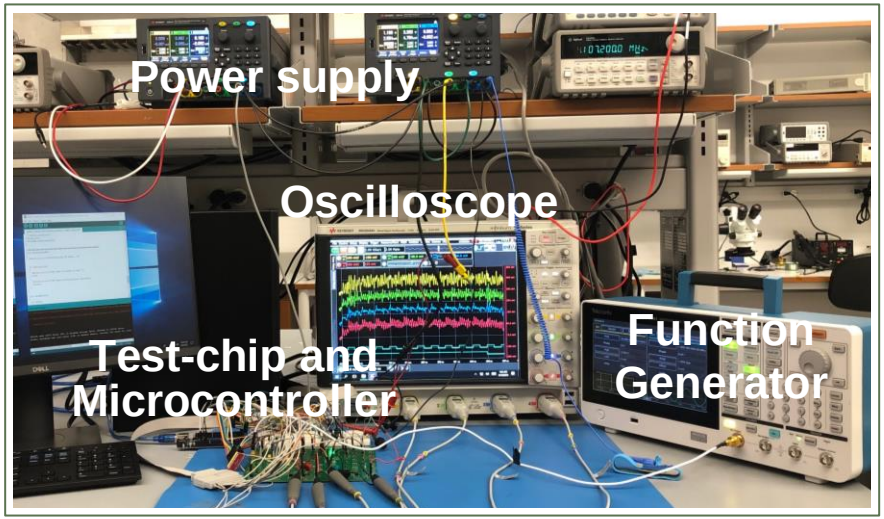


Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - VSS bounce SCA
  - EM SCA
- Comparison & Conclusion

VSS Bounce SCA Measurement: Setup

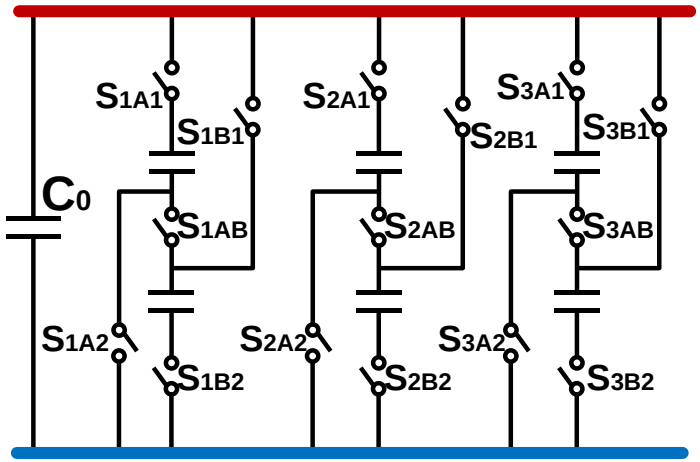


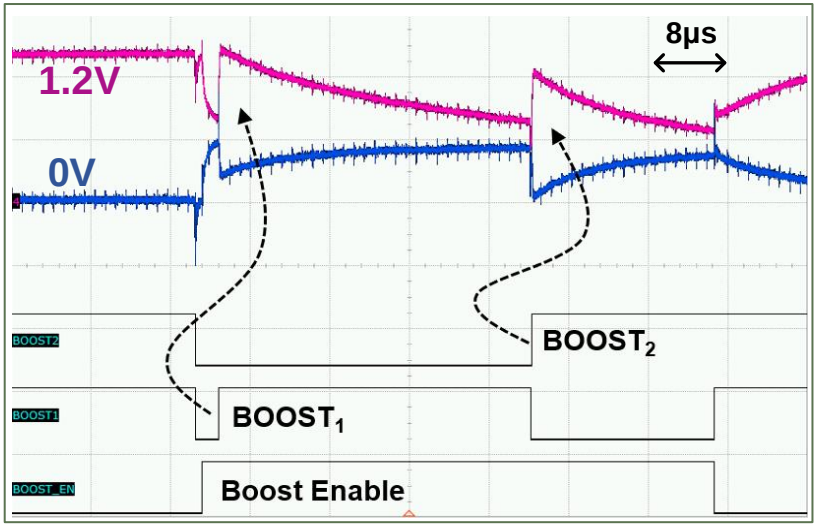


- VSS bounce waveforms and cipher text collected by the oscilloscope are used for SCA

VSS Bounce SCA: Stand alone charge pump circuit

Charge pump design architecture

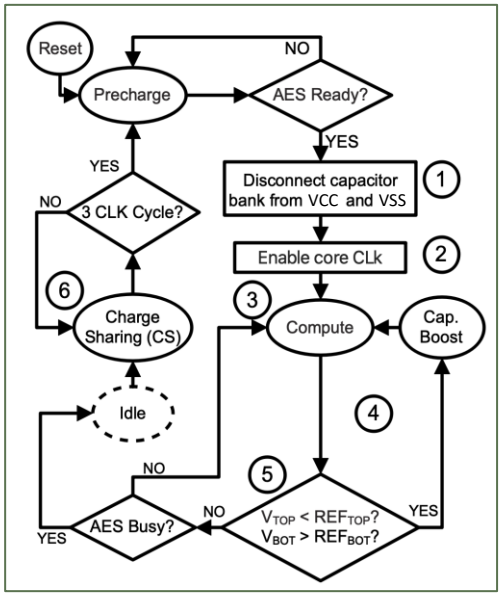




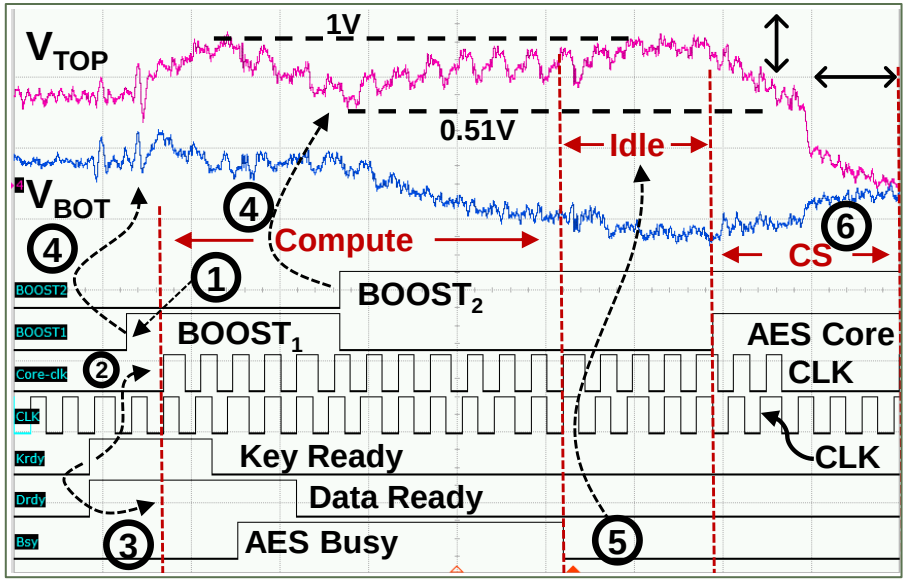
- Oscilloscope measurement show successful multiple voltage boosting

VSS Bounce SCA: Flow chart & Timing diagram

GI AES flow chart

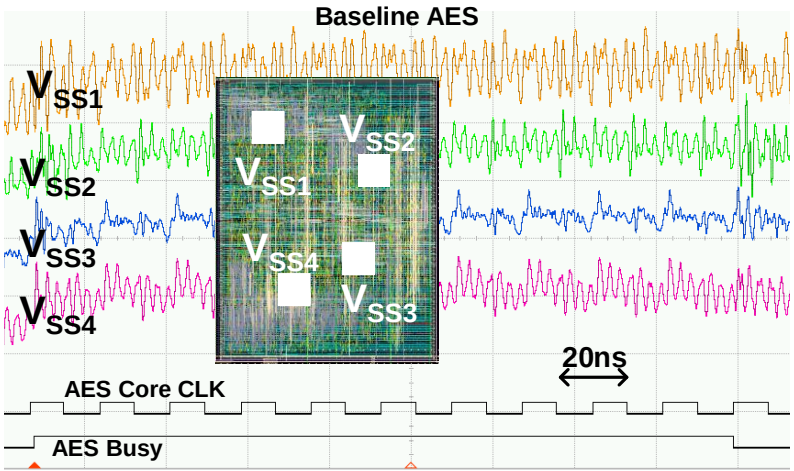


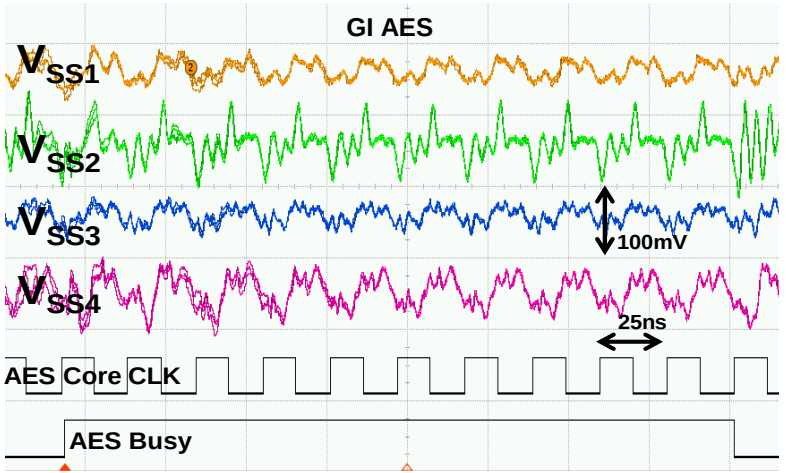
GI AES timing diagram & Vtop Vbot waveforms



- 6 major steps in one GI AES operation and successful V_{TOP}/V_{BOT} boostings are demonstrated in the oscilloscope measurements

VSS Bounce SCA Measurement



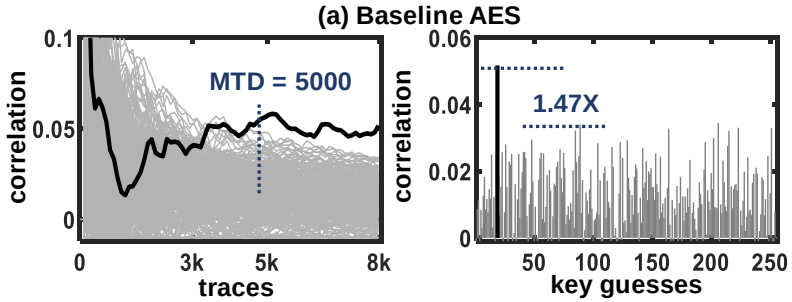


- Four randomly located VSS nodes for ground bounce monitoring

VSS Bounce SCA: Correlation attack

- Target on the last encryption round
- Baseline AES Key Byte 1 is revealed with 5000 traces.
- The correct key has a distinct high correlation value.

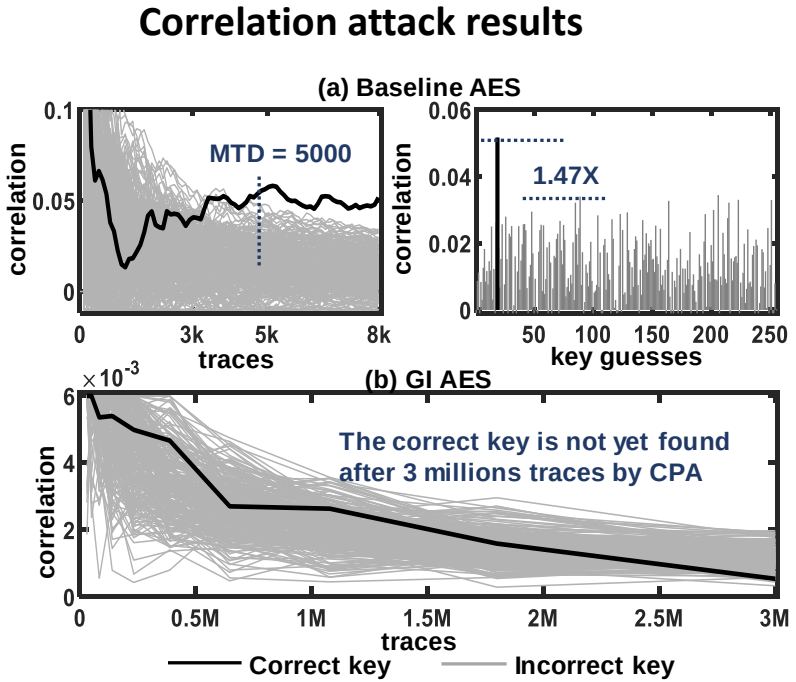
Correlation attack results



VSS Bounce SCA: Correlation attack

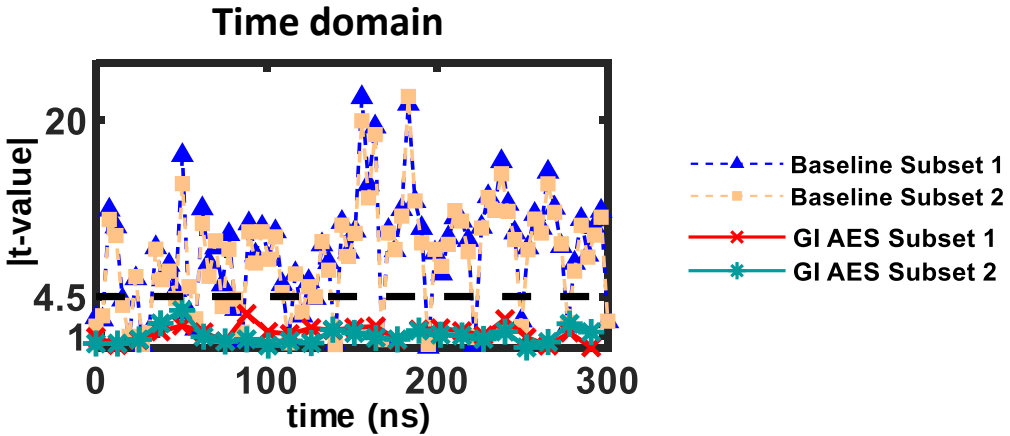
- Target on the last encryption round
- Baseline AES Key Byte 1 is revealed with 5000 traces.
- The correct key has a distinct high correlation value.

- GI AES :
- The secret key is not revealed within 3 million traces
- Improving power SCA resilience by >600X



VSS Bounce SCA: Test vector leakage assessment (TVLA)

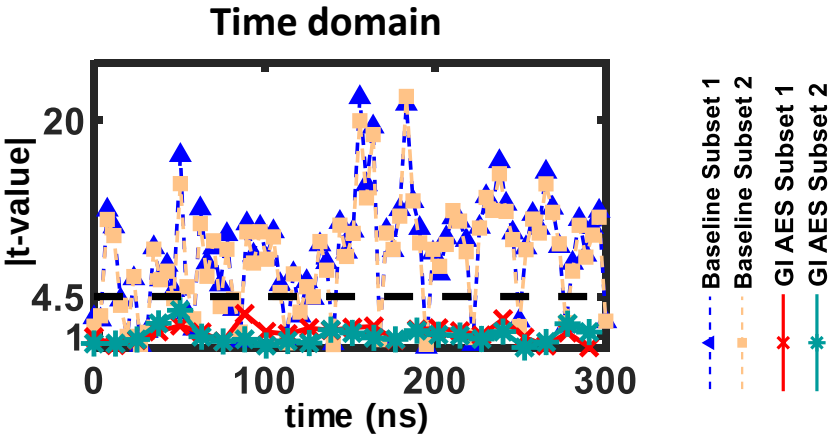
- Run encryption on two data sets, each containing 20,000 fixed plaintexts and 20,000 random plaintexts.

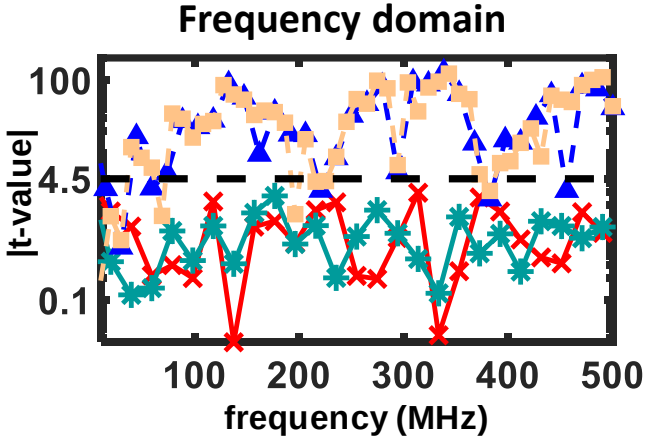


- GI AES reduces max |t-value| under 4.5 threshold value
- Improving TVLA results by 6.5X in time domain

VSS Bounce SCA: Test vector leakage assessment (TVLA)

- Run encryption on two data sets, each containing 20,000 fixed plaintexts and 20,000 random plaintexts.





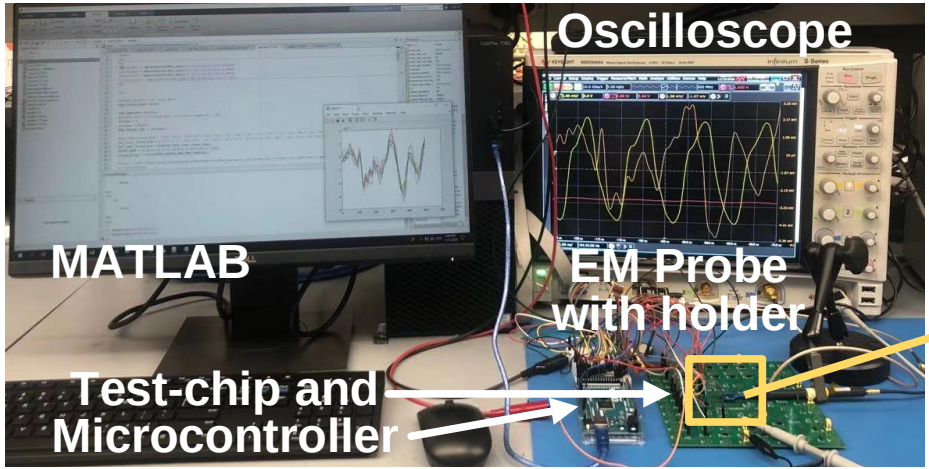
- GI AES reduces max |t-value| under 4.5 threshold value
- Improving TVLA results by 6.5X in time domain

- GI AES reduces max |t-value| under 4.5 threshold value
- Improving TVLA results by 25X in requency domain

Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

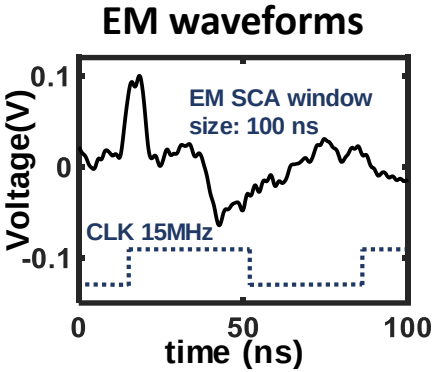
EM SCA Measurement Setup



- The EM SCA attack uses a 10-mm H-field probe 1-mm above the package.

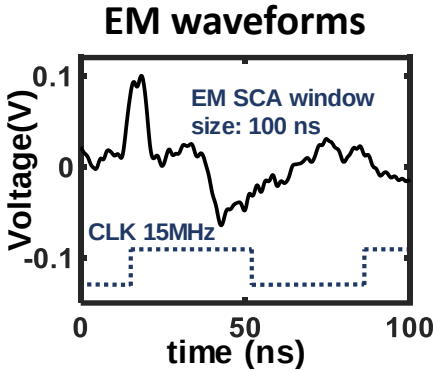
EM SCA Measurement & Correlation EM Attack (CEMA)

- EM waveforms at the last encryption cycle
  - CLK: 15 MHz
  - Correlation EM Attack window size 100 ns

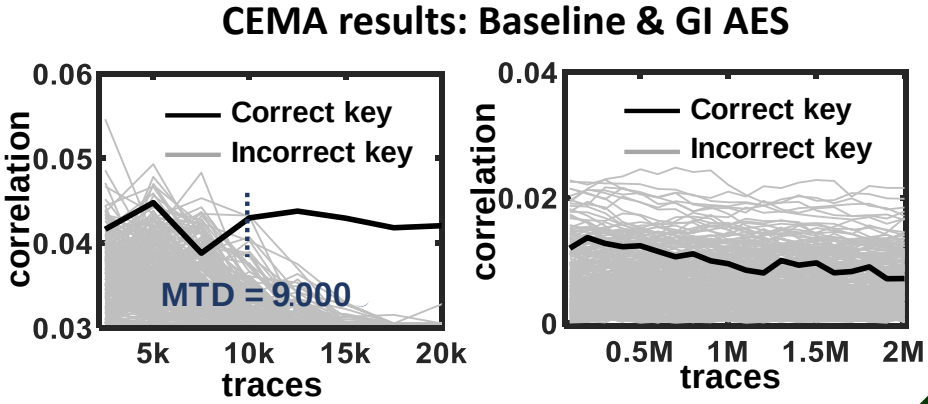


EM SCA Measurement & Correlation EM Attack (CEMA)

- EM waveforms at the last encryption cycle
  - CLK: 15 MHz
  - Correlation EM Attack window size 100 ns



- Baseline AES: Key Byte 1 is revealed with ~9000 traces.
- GI-AES secret key not revealed even within 2 million traces, improving resilience by >220X.



Outline

- Side Channel Analysis (SCA)
- Prior Work: Power SCA resilient approaches
- Motivation: Susceptibility to the ground bounce
- Proposed Work
  - Principle of Galvanic Isolation (GI)
  - Proposed GI-AES architecture
- Test-chip measurement
  - Die photo, Measurement summary
  - Power SCA
  - EM SCA
- Comparison & Conclusion

Comparison

Parameters	ISSCC'17 [3]	ISSCC'19 [4]	ISSCC'20 [5]	VLSI'20 [6]	This Work		
					Baseline	Proposed	Improvement
Technology	130nm	130nm	65nm	14nm	40nm		-
AES Power (mW)	10.5	10.9	1.2	8%+	10	23	-2.3X
AES Frequency	40MHz	80MHz	50MHz	100MHz	50MHz	40MHz	-20%
Area (mm^2)	[1]0.002135	1.75	0.205	10%+	0.032	[2]0.0456	-1.425X
Countermeasure Type	Integrated Voltage Regulator	Digital LDO Regulator	Current Attenuation	Digital LDO, Arithmetic	-	Galvanic Isolation	Improved Vcc, Vss, and substrate isolation
CPA MTD (1 Byte)	>100,000	8.4M	1B	1B	5,000	> 3M	> 600X+
Time Domain Max |t-value|	2.5	11.9	5.2 (1M traces)	4.5 (250M)	24	3.7	6.5X
Frequency Domain Max |t-value|	4	-	-	4.5 (250M)	97	3.9	25X
EM SCA MTD (1 Byte)	-	6M	1B	1B	9,000	> 2M	> 220X+

[1]Area overheads only [2]Area includes level shifters, PMU and capacitor switches

Conclusion

- VSS ground bounce can reveal the secret keys if tapped by the attacker.
- Proposed galvanic isolation technique for VCC, VSS and substrate isolation improves both power and EM resilience.
- Measured results from a 128-bit AES core show
  - >600X improvement against correlation power attack (CPA)
  - >220X improvement against coarse-grained EM SCA attack
  - 20% lower frequency,
  - 2.3X more power
  - 0.0136 mm^2 larger area.

Acknowledgements

This research is supported in parts by Intel, Silicon Labs, and NSF. Authors would like to thank TSMC for chip fabrication, Dr. Sanu Mathew, Dr. Raghavan Kumar, and Dr. Vivek De for helpful technical discussions.


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
شكراً
TEŞEKKÜR EDERIM
NA GODE
muchas gracias
obrigado
спасибо

What will happen if you use the AES within a SoC, will be possible to isolate the full SoC?

It’s not applicable to isolate the full SoC. Because capacitor based Glavanic Isolation design will require a huge capacitor bank to supply the full SoC, which is not area nor power efficient.

Isolating the AES core alone is sufficient to increase its resilience and because of the dual rial sense amp as level shifters, the AES core can exchange data with the SoC with no concerns.

Comparison

Parameters	ISSCC'09 [1]	ISSCC'11 [2]	ISSCC'17 [3]	ISSCC'19 [4]	ISSCC'20 [5]	VLSI'20 [6]	This Work		
							Baseline	Proposed	Improvement
Technology	130nm	130nm	130nm	130nm	65nm	14nm	40nm		-
AES Power (mW)	33.32	-	10.5	10.9	1.2	8%+	10	23	-2.3X
AES Frequency	100MHz	50MHz	40MHz	80MHz	50MHz	100MHz	50MHz	40MHz	-20%
Area (mm^2)	1.37	1.886	[1]0.002135	1.75	0.205	10%+	0.032	[2]0.0456	-1.425X
Countermeasure Type	SC Current Equalizer	Duplicated Data Paths	Integrated Voltage Regulator	Digital LDO Regulator	Current Attenuation	Digital LDO, Arithmetic	-	Galvanic Isolation	Improved Vcc, Vss, and substrate isolation
CPA MTD (1 Byte)	10M	1M	>100,000	8.4M	1B	1B	5,000	> 3M	> 600X+
Time Domain Max |t-value|	-	-	2.5	11.9	5.2 (1M traces)	4.5 (250M)	24	3.7	6.5X
Frequency Domain Max |t-value|	-	-	4	-	-	4.5 (250M)	97	3.9	25X
EM SCA MTD (1 Byte)	-	800,000	-	6M	1B	1B	9,000	> 2M	> 220X+

[1]Area overheads only [2]Area includes level shifters, PMU and capacitor switches

Comparison table reference

[1] C. Tokunaga, *et al.*, *ISSCC*, 2009

[2] M. Doulcier-Verdier, *et al.*, *ISSCC*, 2011

[3] M. Kar, *et al.*, *ISSCC*, 2017

[4] A. Singh, *et al.*, *ISSCC*, 2019

[5] D. Das, *et al., ISSCC,* 2020

[6] R. Kumar, *et al., VLSI,* 2020

Prior Work: Power SCA resilient approaches reference

C. Tokunaga, and D. Blaauw “Securing Encryption Systems with a Switched Capacitor Current Equalizer” IEEE Journal of Solid State Circuits (JSSC), pp. 23-31, Vol. 45, No. 1, January 2010

A. Singh, M. Kar, J. Ko, and S. Mukhopadhyay, “Exploring power attack protection of resource constrained encryption engines using integrated low-drop-out regulators,” in International Symposium on Low Power Electronics

Design, 2015, pp. 134–139.

M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, S. Mukhopadhyay, “Improved Power-Side-Channel-Attack Resistance of an AES-128 Core via a Security-Aware Integrated Buck Voltage Regulator” Proceedings of International Solid State Circuits Conference (ISSCC), 2017, pp. 142-143

D4. D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, “High Efficiency Power Side-Channel Attack Immunity using Noise Injection in Attenuated Signature Domain”, CoRR, abs/1703.10328, 2017