Galvanically Isolated, Power and Electromagnetic Side-Channel Attack Resilient Secure AES Core 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

Abstract: A galvanic isolation (GI) technique for cryptographic cores is proposed to mitigate power and electromagnetic (EM) side-channel analysis (SCA) attacks. The design uses deep N-well technology and an integrated charge pump-based power delivery and management to completely isolate V_{CC}, V_{SS}, and substrate nodes from the external supply and ground pins, improving the SCA resilience due to supply as well as ground bounce. Measured results from a 128-bit Advanced Encryption Standard (AES) core implemented in a 40nm CMOS show >600x and >220x improvement against a correlation power analysis (CPA) and coarse-grained EM SCA attack, respectively, while operating at 20% lower frequency, consuming 2.3x more power, and occupying 0.0136 mm^2 larger area.

Galvanic isolation for SCA mitigation: Cryptographic integrated circuits such as AES cores, are vulnerable to SCA attacks due to ease of physical access and unintentional data-dependent information leakage. Various countermeasures based on voltage regulator and power management techniques, such as switched capacitor current equalizers, analog and digital low dropout regulators, and buck converters have been explored [1-4]. They isolate the external supply pin (V_{CC}) or randomize the supply current signatures to improve the resilience of the AES core against SCA attacks. However, the shared external ground pins (V_{SS}) between the AES core and the power converter remain susceptible to SCA attacks. This is particularly critical in modern SoCs wherein multiple V_{SS} pins are arranged in a ball grid array (BGA). Side channel information can be obtained by monitoring the voltage bounce and substrate noise coupling [5] on these V_{SS} BGA pins, especially those in close proximity with the AES core (Fig. 1a). Post-layout simulation of a 128-bit AES core shows about 6000 V_{SS} bounce traces on the top-level metal layers revealing the secret key to a correlation power analysis (CPA) attack confirming the vulnerability of the Vss pins to the SCA attacks (Fig. 1b). To mitigate the SCA vulnerability due to supply as well as ground bounces, we propose a galvanically isolated (GI) power delivery mechanism that completely separates the AES current loop from the external V_{CC}/V_{SS} pin loops (Fig. 1c). The proposed approach is inspired by the galvanic isolation principle employed in high-voltage power converters [6]. Using the transformer principle, the circuits connected on the secondary side of the high-voltage power converter are galvanically isolated and protected from the potentially high transient voltages and currents present on the primary side. The galvanic isolation for the AES core is achieved using a reconfigurable capacitor bank built with backend MoM (Metal-over-Metal) capacitors which act as an energy reservoir (Fig. 1d). The capacitor bank, along with an integrated power management unit (PMU), supplies the required charge for the AES computation, thus completely isolating its compute current loop from the external V_{CC}/V_{SS} supply loops. The deep N-well secures the AES core by reducing the substrate noise-induced side-channel leakage.

Charge pump boost circuits: The GI-AES computation is performed in 3 phases (Fig. 2). In the first phase (precharge phase), the PMOS P_1 header and NMOS N_1 footer are activated, with all capacitors connected in parallel and precharged to V_{CC}. In the second phase (compute phase), both P_1 and N_1 transistors are deactivated, isolating the capacitor bank from external V_{CC} and V_{SS} pins. The AES core is connected between V_{TOP} and V_{BOT} rails which are shared across the capacitor bank. V_{TOP} and V_{BOT} rails are internal and not routed as external pins, thus concealing the crypto-compute signature. Initially, only C_0 capacitor supplies charge to the AES core with other capacitors are isolated from V_{TOP} and V_{BOT} rails. As C_0 charge depletes, the voltage swing across V_{TOP} and V_{BOT} reduces. This voltage swing is monitored with the help of two sense amplifiers and predetermined reference voltages (Vref-1,2). Once the voltage swing below a critical voltage (V_{crit}) is detected, the PMU triggers voltage doubling on the first capacitor stage (C_{1A} and C_{1B}) by asserting the $Boost_1$ signal, connecting both C_{1A} and C_{1B} in series. As C_{1A} and C_{1B} capacitors are precharged to V_{CC} in the first phase, the voltage across this series-connected capacitor stage is boosted to $2{*}V_{cc}$ (Fig. 2b). This boosted voltage capacitor branch (C_{1A} and C_{1B} in series) when connected in parallel with the C_0 capacitor, the resulting charge-pumping operation increases the voltage swing (V_{TOP} - V_{BOT}) across the AES core larger than the V_{crit}. The AES compute activity continues and when the voltage across V_{TOP} and V_{BOT} rails goes below V_{crit}, the PMU triggers another voltage doubler capacitor stage (C_{2A} and C_{2B}) by asserting $Boost_2$ signal. The capacitor bank voltage would vary depending upon the encryption activity and utilization of boosting stages. In the third charge-share (CS) phase, once all voltage doubler capacitor stages are utilized, V_{TOP} and V_{BOT} rails are shorted using a transistor to achieve a pre-set voltage, hiding the AES compute signature during the subsequent precharge phase. If AES computation is completed before the estimated time interval, the PMU remains idle for the remaining duration of this phase. Thus, constant timing duration, along with the fixed precharge current (or charge) signature, ensures no data-dependent side-channel leakage to the external supply/ground pins. Multiple voltage boosting stages gradually transferring charge from precharged capacitor stages to the active capacitor bank, can prolong AES computations by maintaining V_{TOP}-V_{BOT} swing above V_{crit}. The AES operating frequency is set based on V_{crit} to mitigate any timing errors due to variable V_{TOP}-V_{BOT} voltage swing. Incremental charge transfers also reduce EM emanations and mitigate EM SCA vulnerabilities. The PMU can also enable additional off-chip capacitors based boosting stages. Differential sense amplifiers act as level shifters to convert V_{TOP}/V_{BOT} swing AES outputs to full V_{CC}/V_{SS} swing output scan bits.

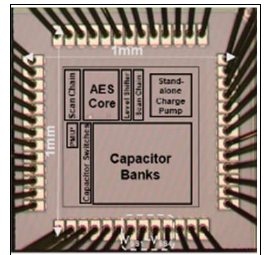


Fig.7 GI-AES die photo

Measurement results: Fig. 7 shows the die-photograph of a 40nm AES test-chip implementing proposed galvanic isolation technique. Oscilloscope waveform traces from a stand-alone charge pump voltage boost circuit (no AES load) demonstrate successful triggering of multiple boosting stages and increasing the voltage swing across V_{TOP} and V_{BOT} rails (Fig. 3a). Observed V_{TOP}/V_{BOT} waveforms during 3 phase operations, PMU control signal waveforms and trigger points matched to the system flow chart confirm the functionality of the proposed GI-AES design (Fig. 3b & 3c). The ground bounce on four randomly located V_{SS} grid nodes is monitored for both designs (Fig. 3d & 3e). Test vector leakage assessment (TVLA) is performed using two sets, each containing 20,000 fixed plaintexts and 20,000 random plaintexts [7]. The proposed GI-AES design succeeds in reducing the maximum absolute t-value by ~6.5x in time-domain and ~25x in frequency-domain under 4.5 threshold, protecting the design against power SCA (Fig. 4a). Correlation-based SCA attacks are performed on power (Fig. 4b) and coarse-grained EM signatures (Fig. 4c) [8]. With the baseline AES, the CPA attack reveals the first correct key byte after ~5000 traces, the correct key correlation is 47% higher than the next possible key guess. Fig. 5a and 5b show the power and EM SCA attack setup. The coarse-grain EM SCA attack uses a 10-mm H-field probe 1-mm above the package and reveals the first key byte after ~9000 traces. With the proposed GI-AES, no correct key byte is detected by CPA even after 3 million traces and by coarse-grain EM SCA after 2 million traces, increasing the measurements to disclose (MTD) key bytes by >600x and >220x respectively. The GI-AES technique’s ability to mitigate fine-grain EM SCA attacks [9] is currently under investigation. Fig.6 compares the GI-AES measured results with prior schemes. Test-chip summary is shown in Fig. 5c.

Acknowledgments: 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.

References:

[1] C. Tokunaga, *et al.*, *ISSCC*, 2009, [2] M. Kar, *et al.*, *ISSCC*, 2017, [3] M. Doulcier-Verdier, *et al.*, *ISSCC*, 2011 [4] A. Singh, *et al.*, *ISSCC*, 2019 [5] D. Fujimoto, *et al.*, *HOST*, 2014 [6] N. Mohan, *et al.*, 3rd edition [7] G. Goodwill, *et al.*, *NIST Technical Report*, 2008 [8] G. Ding, *et al.*, *WMWA*, 2009 [9] V. V. Iyer, *et al., WMCS*, 2019

978-1-7281-7581-2/21/$31.00 ©2021 IEEE

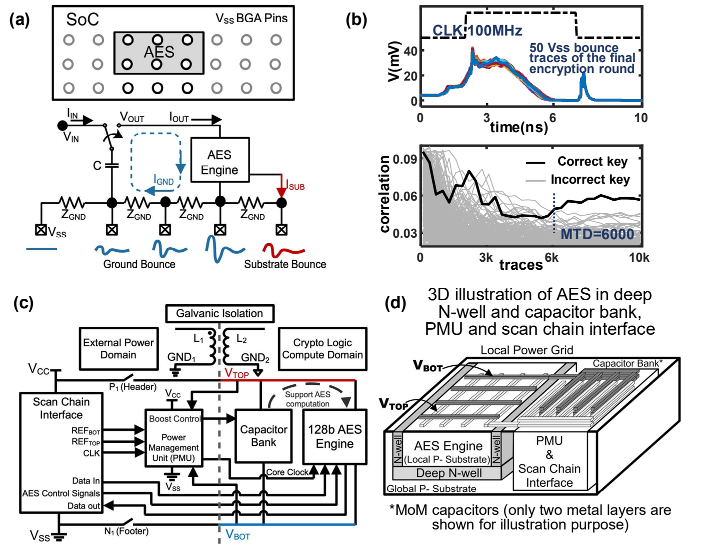
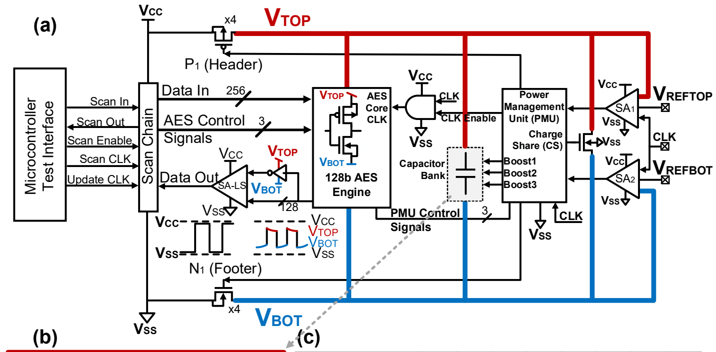
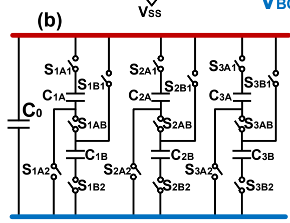


Fig. 1. (a) Ground and substrate bounces in BGA arranged V_{SS} pins (b) Baseline AES post-layout simulation and CPA results (c) & (d) Proposed Galvanically Isolated (GI) AES operates in the crypto logic domain, completely isolated from the external domain





(c)

Mode		S_{1A1}	S_{1A2}	S_{1AB}	S_{1B1}	S_{1B2}	CS	P_1	N_1
Baseline		OFF	OFF	OFF	OFF	OFF	OFF	ON	ON
GI AES	Precharge	ON	ON	OFF	ON	ON	OFF	ON	ON
	Compute	ON	OFF	ON	OFF	ON	OFF	OFF	OFF
	Charge Share	ON	ON	OFF	ON	ON	ON	OFF	OFF

Fig. 2. (a) Block diagram of the proposed GI AES system with PMU and dual side level shifter circuit (b) Capacitor bank diagram with three boosts settings (c) Capacitor bank switching patterns for baseline AES and GI AES (three phases)

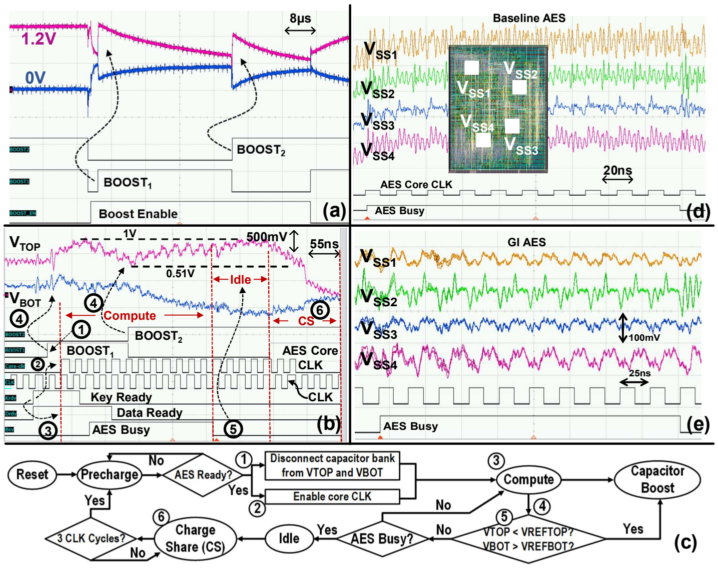


Fig. 3. Experimental demonstration (a) Stand-alone charge pump voltage boost circuit (b)&(c) GI AES core operation: control signal with V_{TOP}/V_{BOT} and flow chart (d)&(e) Four randomly located V_{SS} nodes for ground bounce monitoring on Baseline and GI AES

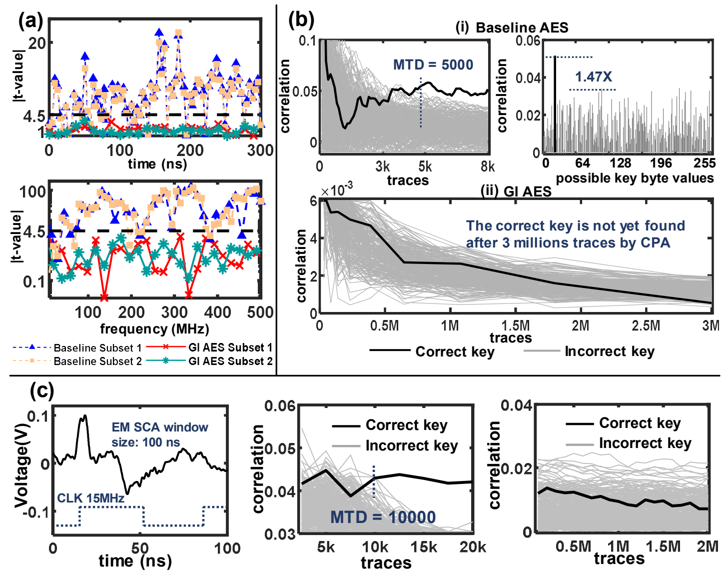
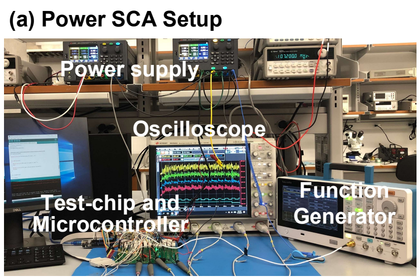
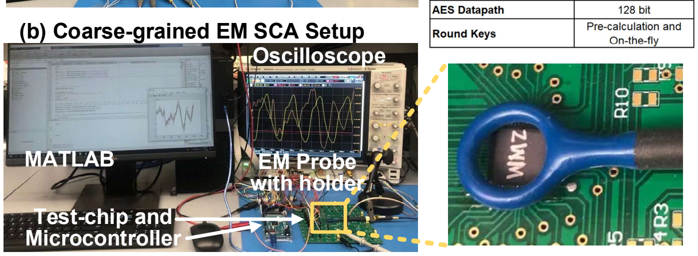


Fig. 4. Measured results (a) Power SCA TVLA in time and frequency domains (b) CPA results of (i) Baseline AES and (ii) GI AES (c) Measured coarse-grained EM signal and SCA results of Baseline and GI AES





(c)

Technology	40nm CMOS
Operating Voltage	0.9V ~1.3 V
Package	QFN 56
Power @1.2V (mW)	23
Input Clock Frequency	40~50 MHz
Area (mm^2)	
AES Core	0.032
Level Shifter	0.00795
Power Management Unit	0.00136
Capacitor Switches	0.00429
Capacitor Bank	0.178
Total Area (mm^2)	0.2236
MoM Capacitor	M4~M6
AES Datapath	128 bit
Round Keys	Pre-calculation and On-the-fly

Fig. 5. Measurement setup for (a) power and (b) coarse-grained EM SCA (c) Test-chip measurement summary

Parameters	ISSCC'09 [1]	ISSCC'17 [2]	ISSCC'11 [3]	ISSCC'19 [4]	This Work: Baseline	This Work: Proposed	This Work: Improvement
Technology	130nm	130nm	130nm	130nm	40nm	40nm	-
AES Power (mW)	33.32	10.5	-	10.9	10	23	-2.3X
AES Frequency	100MHz	40MHz	50MHz	80MHz	50MHz	40MHz	-20%
Area (mm^2)	1.37	[1]0.002135	1.886	1.75	0.032	[2]0.0456	-1.425X
Countermeasure Type	Switched-Capacitor Current Equalizer	Integrated Voltage Regulator	Duplicated Data Paths	On-chip Digital Low Dropout Regulator	-	Galvanic Isolation (Improved Vcc, Vss and substrate isolation)	Improved Vcc, Vss, and substrate isolation
CPA MTD (1 Byte)	10M	>100,000	1M	8.4M	5,000	> 3M	> 600X+
TVLA Time Domain Max |t-value|	-	2.5	-	11.9	24	3.7	6.5X
TVLA Frequency Domain Max |tvalue|	-	4	-	-	97	3.9	25X
Coarse-grained EM SCA MTD (1 Byte)	-	-	800,000	6M	9,000	> 2M	> 220X+

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

Fig. 6. Galvanically isolated AES performance summary and prior work comparison