27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation

Debayan Das[1], Josef Danial[1], Anupam Golder[2], Nirmoy Modak[1], Shovan Maity[1], Baibhab Chatterjee[1], Donghyun Seo[1], Muya Chang[2], Avinash Varna[3], Harish Krishnamurthy[4], Sanu Mathew[4], Santosh Ghosh[4], Arijit Raychowdhury[2], Shreyas Sen[1]

[1]Purdue University, West Lafayette, IN
[2]Georgia Institute of Technology, Atlanta, GA, [3]Intel, Chandler, AZ
[4]Intel Labs, Portland, OR

Computationally-secure cryptographic algorithms when implemented on physical platforms leak critical physical signals correlated with the secret key in the form of power consumption and electromagnetic (EM) emanations. This can be exploited by an adversary, leading to side-channel attacks (SCA) that can recover the secret key. Circuit-level on-chip countermeasures include a switched-capacitor current equalizer [1], charge-recovery logic [2], an integrated voltage regulator (IVR) [3], and an all-digital low-dropout (LDO) regulator [4], which suffer from performance degradation, high power/area overheads because of large embedded passives, as well as EM leakage from large metal-insulator-metal (MIM) capacitor top plates. Alternatively, simulations of shunt LDO-based regulators have been shown to be effective for power SCA resistance [5]. Noting that the correlated current is the source of both power (at supply pin) and EM leakage (radiation throughout current path), this work embraces current-domain 'signature attenuation' (CDSA) as a low-overhead generic countermeasure against both EM and power side-channel attacks to achieve the highest minimum traces to disclosure (MTD>1B) reported to date.

The 65nm CMOS test chip contains both protected and unprotected AES256 implementations, running at a clock frequency of 50MHz. By embedding the crypto engine within the CDSA, the supply current becomes almost constant, i.e. independent of the AES current (Fig. 27.3.1), increasing the MTD for power SCA by a factor of the square of attenuation factor. This also improves EM SCA MTD, as the current flowing through higher-level radiating structures (e.g. pins, board traces) is near constant. Through 3D finite element method (FEM) simulation of metal traces, it is validated that the EM leakage is a strong function of the metal dimensions carrying the correlated current. To avoid on-chip structures radiating correlated signatures, before the current passes through CDSA, lower-metal routing (only up to M6, Fig. 27.3.1) is adopted between the crypto core and the physically close CDSA circuit, while limiting additional IR drop to <0.4mV (Fig. 27.3.3). AES256 is implemented with parallel datapaths to provide high performance and requires 14 cycles per encryption. Designs include unprotected (Mode 1), power protected but EM unprotected (Mode 2, to analyze effect of different metal layers on EM leakage) and both power + EM protected (Mode 3, default protection mode).

The CDSA circuit (Fig. 27.3.2) utilizes a digitally tunable cascode current source (CS) with high output impedance to power the AES. The goal of the CDSA circuit is to provide the average load (AES) current plus a delta current that leaks through the bypass PMOS bleed path to ground, providing local negative feedback, which leads to the ability to support any I_{AESavg} in between two quantized current levels of the CS (i.e. aids in analog regulation without a high-power shunt-loop). The CS consists of 32 PMOS slices, 16 of which are turned on nominally. A slow digital switched-mode control (SMC) LDO tracks and regulates the voltage across the AES (V_{DIG} between $V_{TARGET}+\Delta_+$ and $V_{TARGET}-\Delta_-$) by turning on or off the required number of PMOS CS slices. The unit current (~94μA) is chosen such that it is higher than the key-dependent variation in I_{AESavg} (~72μA), so that the key-dependent information in average DC current is not transferred to supply current and is leaked by the bleed PMOS, making the design highly secure. The SMC loop can handle any PVT variation from chip-to-chip (Fig. 27.3.3). At start-up, CDSA requires <500μs to settle, which can be dummy operations. It should be noted that the SMC LDO is a low-BW loop (clocked at <10KHz, V_{DIG} output pole at ~106kHz) and has a dead band of 50mV, such that it remains disengaged during steady-state operation of the CDSA-AES circuit. Two dynamic comparators compare V_{DIG} with $V_{TARGET}+\Delta_+$ and $V_{TARGET}-\Delta_-$ respectively, and a 32b up-down counter with averaging (to control the loop frequency) controls the appropriate number of CS slices to be turned on. Unlike traditional series LDOs, the supply current in CDSA does not track the AES current. Instead, we choose to tolerate the ~30-to-50mV voltage droop across the AES engine (V_{DIG} is guard-banded to ensure no performance degradation at the cost of some power overhead), and the high impedance (r_{ds} >10KΩ) (Fig. 27.3.2) CS on top ensures that the current fluctuation at the supply is attenuated by $\omega_{AES}C_L r_{ds}$, i.e. >350×. The use of a cascode CS biased in subthreshold saturation increases r_{ds} by ~10× compared to a one-stack CS, allowing 10× reduction in C_L (only 150pF, iso-attenuation) across the crypto engine. C_L uses only MOS cap (lower metal layers) rather than MIM (top metal layers) so that the EM radiation is minimized. The shunt-path PMOS bias (near-threshold operation), as well as the number of PMOS legs ON are scan controllable to analyze the effect of the extra bleed current on signature attenuation (Fig. 27.3.3).

To provide high EM SCA resilience, both the protected AES along with the CDSA circuit embedding the AES engine locally is routed in lower metal layers up to M6 (Fig. 27.3.3), which suppresses the correlated local EM leakage significantly, before passing the attenuated signature (i.e. almost constant current) through to the top-level metal layers. The design has scan-controlled highly isolating switches (SW1, Fig. 27.3.1) to connect the V_{DIG} node to an external pin for observability (SW1 ON) or disconnect without leaking EM during normal operations. Lower-metal routing (up to M6) provides a local attenuation of ~6× (compared to passing the signature directly to M9 which has larger dimensions and radiates more) (Fig. 27.3.3). Time-domain measurements of the unprotected AES vs. CDSA-AES show a signature attenuation of >350× for both the power and EM traces. Design space exploration of the CDSA-AES reveals the optimal operating point at dropout voltage of 0.3V across the CS stage and a bleed bias of 0.35V. The unprotected AES is powered with 0.8V input and consumes ~1mA average current at 50MHz.

Figure 27.3.4 shows the hamming distance (HD) attack model used between the last 2 rounds of AES (13th round output and the ciphertext) and a correlational power attack (CPA) on the unprotected AES implementation shows an MTD of 8K, while the CDSA-AES is protected even after 1B traces. While all key bytes show similar trends, we demonstrate the efficacy of the countermeasure with attacks on the 1st key byte. Fixed vs. random Test Vector Leakage Assessment (TVLA) on the unprotected AES shows a t-value of 1056 after 200M traces compared to ~12 for CDSA-AES. Frequency-domain CPA with windowed FFT has been performed with a window size of 10MHz and the center frequency is swept from 10MHz to 1GHz. However, the correct key byte was not revealed even after 1B traces, showing an MTD improvement of ~125,000×.

CEMA on the unprotected AES shows an MTD of ~12K, while the CDSA-AES is not broken after 1B measurements (Fig. 27.3.5). TVLA on the unprotected AES shows a t-value of 961 compared to a t-value of 5.1 for the CDSA-AES (with lower-metal routing – Mode 3: Fig. 27.3.1). The effect of higher-metal-layer routing on EM leakage is analyzed by turning on highly isolating switches (SW2-SW4) that connects V_{DIG} to higher metal radiating structures (Fig. 27.3.2). In this Mode (2) with all M7-M9 connected, the EM leakage crosses the threshold of 4.5 within 20M traces, compared to ~170M traces for Mode 3, demonstrating the effect of local attenuation (>7×) and the significance of the local lower-metal routing for EM SCA protection. In comparison with previous countermeasures, CDSA-AES achieves 100× higher MTD (10M ⟶ >1B) and >125,000× (power) and 83,333× (EM) MTD improvement compared to the unprotected implementation, without any performance overhead and comparable power/active area overheads (Fig. 27.3.6). The die photograph and chip characteristics are shown in Fig. 27.3.7.

Acknowledgements:
This work was supported in part by the National Science Foundation under Grant CNS 17-19235, CNS 16-24731 (CAEML), Semiconductor Research Corporation (Grant 2720.001), and Intel Corporation.

References:
[1] C. Tokunaga et al., "Secure AES Engine with a local Switched-Capacitor Current Equalizer," *ISSCC*, pp. 64-65, Feb. 2009.
[2] S. Lu et al., "1.32GHz High-Throughput Charge-Recovery AES Core with Resistance to DPA Attacks," *IEEE Symp. on VLSI Circuits*, pp. C246-C247, 2015.
[3] M. Kar et al., "Improved Power-Side-Channel-Attack Resistance of an AES-128 Core via a Security-Aware Integrated Buck Voltage Regulator", *ISSCC*, pp. 142-143, Feb. 2017.
[4] A. Singh et al. "A 128b AES Engine with Higher Resistance to Power and Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low-Dropout Regulator", *ISSCC*, pp. 403-404, Feb. 2019.
[5] D. Das et al., "ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity," *IEEE TCAS-I*, vol. 65, no. 10, pp. 3300-3311, 2018.

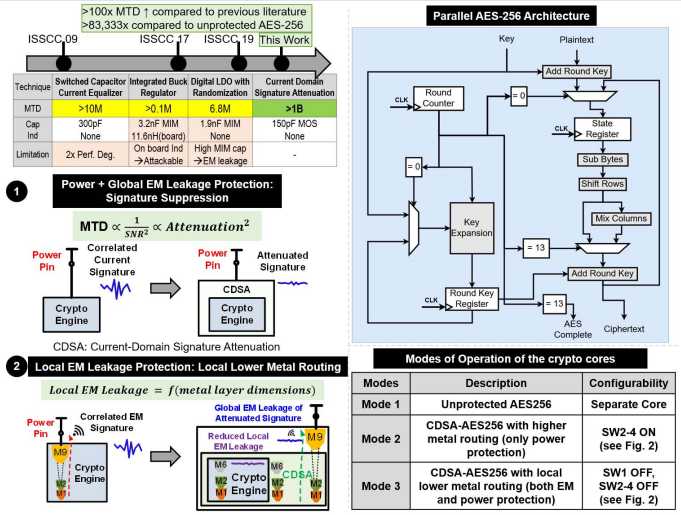


Figure 27.3.1: Motivation and overview of the design principles for Current Domain Signature Attenuation (CDSA) hardware to achieve both power and EM SCA resilience.

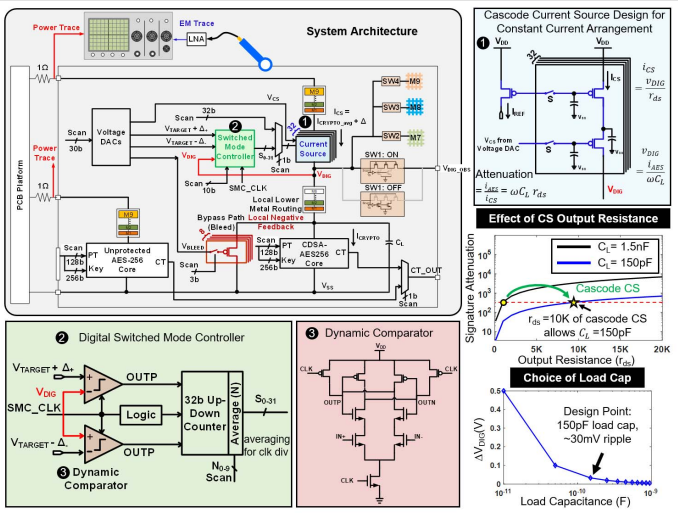


Figure 27.3.2: System architecture showing the circuit details of the cascode CS and the digital SMC loop, and the design choices for the different components.

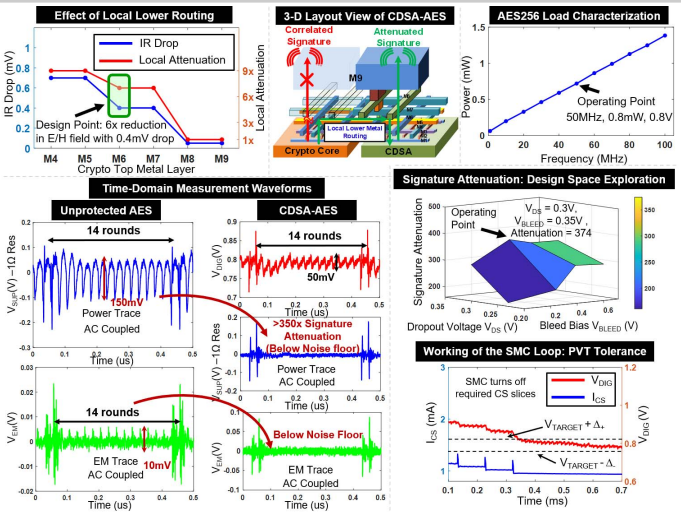


Figure 27.3.3: Techniques for EM SCA resilience and time-domain. Measurement Results showing >350× attenuation for both power and EM traces.

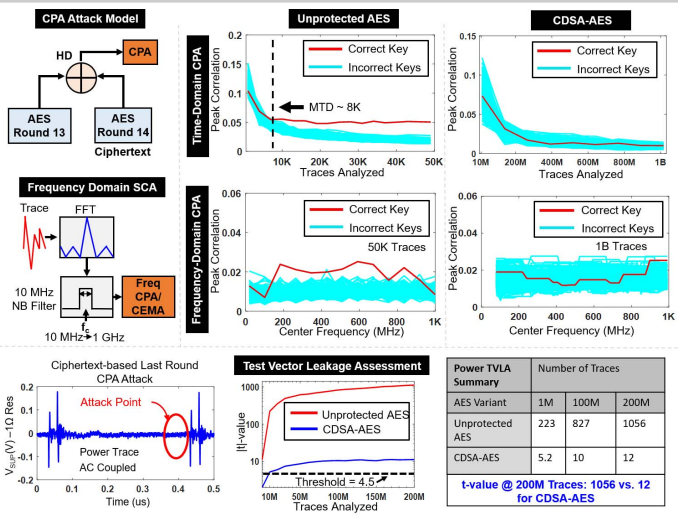


Figure 27.3.4: Measurement results: power SCA (both time and frequency domain) and leakage analysis demonstrating the resiliency of CDSA-AES256 (MTD > 1B, i.e. >125,000× improvement).

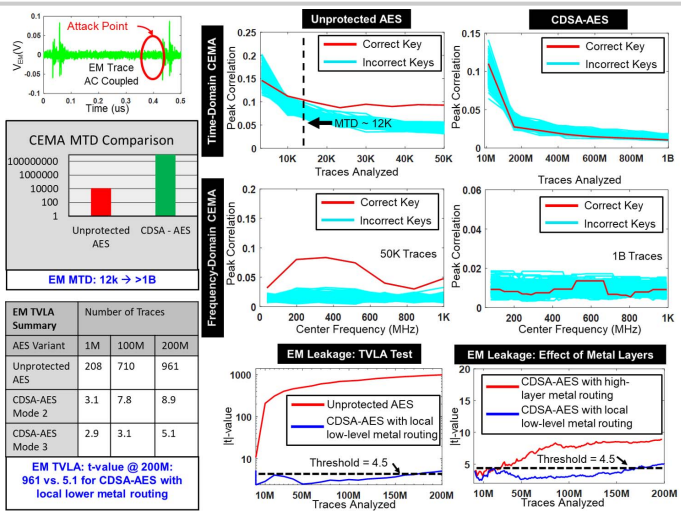


Figure 27.3.5: Measurement results: time and frequency domain CEMA attack and TVLA on the unprotected vs. CDSA-AES256. Effect of metal routing on TVLA is demonstrated for the first time.

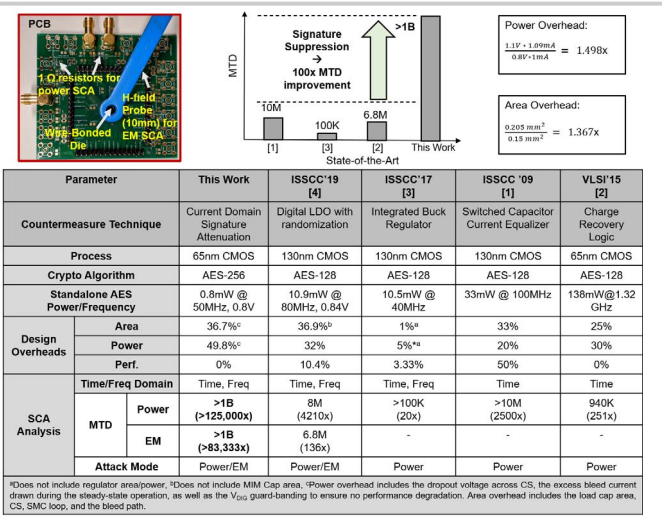
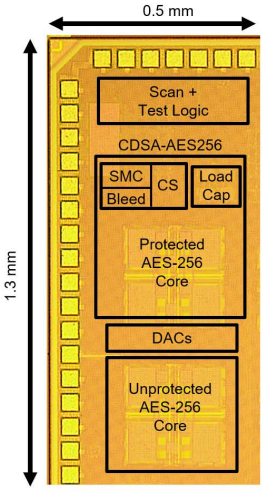


Figure 27.3.6: PCB for the test chip, overhead analysis and comparison with state-of-the-art countermeasures (>100× improved MTD compared to the state-of-the-art).



Test Chip	Process	65nm CMOS Low Power
	Package	Wire-bond (Glob-Top Encapsulation)
Unprotected AES-256 Core	Performance	0.8V/50MHz/0.8mW
	Architecture	128b Datapath (parallel AES)
	Supply Decap	80 pF MOS Cap (0.008 mm^2)
	Active Area	0.15 mm^2
	Scan Chain	387b
CDSA-AES256	Input	1.1V
	Active Area	0.205 mm^2
	Supply Decap	80 pF MOS Cap (0.008 mm^2)
	Current Efficiency	91.74%@1mA load (90uA through bleed)
	Load Cap	150 pF MOS Cap (0.015 mm^2)
	Scan Chain	AES Core: 387b
		CDSA: 114b

Figure 27.3.7: Die micrograph of the system in 65nm CMOS process and design summary.

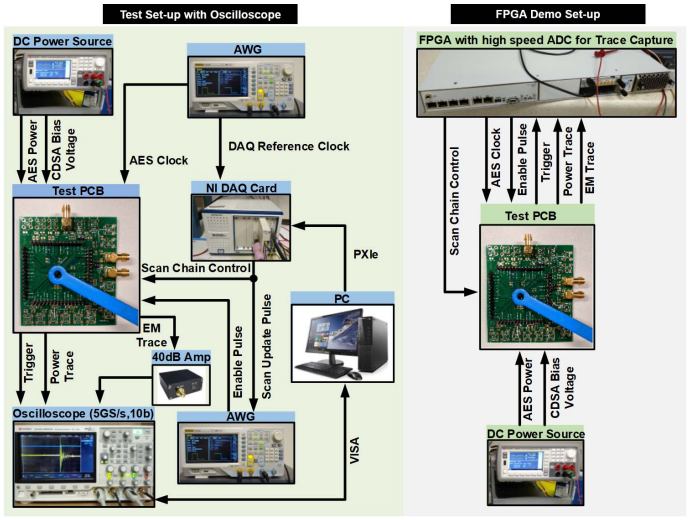


Figure 27.3.S1: SCA attack setup using oscilloscope and PC (used for all the reported results). FPGA-based setup for fast SCA evaluation in real-time.

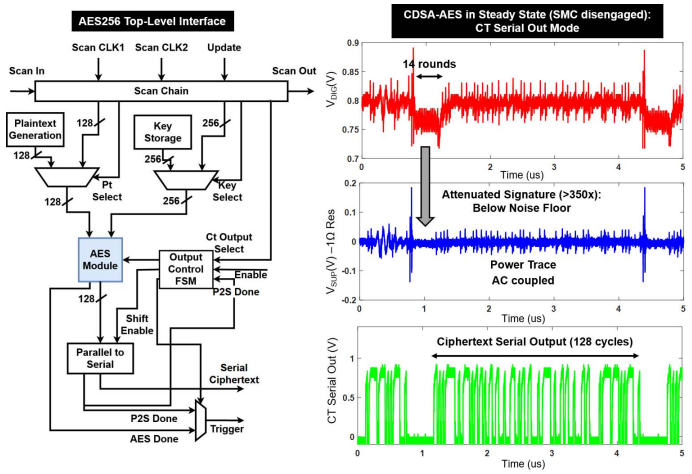


Figure 27.3.S2: AES-256 top-level interface block diagram. Measured time-domain waveforms of the CDSA-AES operating in steady state in ciphertext (CT) out mode.

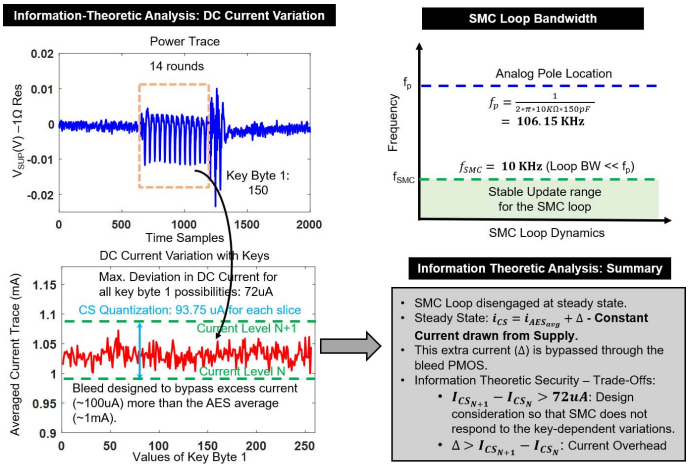


Figure 27.3.S3: Design considerations for the CDSA circuit to guarantee information theoretic security.

978-1-7281-3205-1/20/$31.00 ©2020 IEEE