36.2 An EM/Power SCA Resilient AES-256 with Synthesizable Signature Attenuation using Digital-Friendly Current Source and RO-Bleed based Integrated Local Feedback and Global Switched-Mode Control

Archisman Ghosh[1], Debayan Das[1], Josef Danial[1], Vivek De[2], Santosh Ghosh[2], Shreyas Sen[1]

[1]Purdue University, West Lafayette, IN
[2]Intel Labs, Portland, OR

Mathematically secure cryptographic algorithms leak side-channel information in the form of correlated power and electromagnetic (EM) signals, leading to physical side channel analysis (SCA) attacks. Circuit-level countermeasures against power/EM SCA include current equalizer [1], series LDO [2], IVR [3], enhancing protection up to 10M traces. Recently, current domain signature attenuation [4] and randomized NL-LDO cascaded with arithmetic countermeasures [5] achieved >1B minimum traces to disclosure (MTD) with a single and two countermeasures, respectively. Among these, the highest protection with a single strategy is achieved using signature attenuation [4], [6], which utilized a current source making the supply current mostly constant. While being highly resilient to SCA, [4] required analog-biased cascode current sources and an analog bleed path, making it not easily scalable across different technology generations. Conversely, [2], [5] are synthesizable but a single countermeasure only achieved moderate protection (up to 10M MTD). This work embraces the concept of signature attenuation in the current domain, but makes it fully-synthesizable with digital current sources, control loop and the bleed to increase the MTD from 10M [5] to 250M (25× improvement, Fig. 36.2.1) using a single synthesizable countermeasure. Finally, combining the digital signature attenuation circuit (DSAC) with a second synthesizable generic technique in the form of time-varying transfer function (TVTF), this work achieves an MTD>1.25B for both EM and power SCA.

The 65nm CMOS IC consists of both unprotected (Mode 1) and protected (Mode 2 and 3) parallel AES-256 implementations. Mode 2 utilizes a Digital-friendly Signature Attenuation Circuit (DSAC) which leverages the benefits of a high attenuation current source, while making the countermeasure synthesizable. Mode 3 is the combined strategy with DSAC along with the TVTF, which provides time-domain obfuscations before signature attenuation through a synthesizable switched-capacitor circuit (unlike the non-synthesizable analog switched cap array with reset used in [1]).

The DSAC (Fig. 36.2.2) consists of: 1) a synthesizable Current Source (CS), multiple parallel multi-stage ring oscillators (ROs) as the bleed path which assist in 2) Local Negative Feedback (LNFB), 3) Global Negative Feedback (GNFB) fully digital Switched Mode Control (SMC) Loop and 4) RO-bleed strength randomization. 1) The synthesizable CS consists of 32 digitally tunable stacked PMOS slices and are biased in saturation using a self-biased inverter, generating the required bias voltage and pass-gates to control the biasing, removing any analog blocks and making the CS synthesizable. 2) LNFB: The RO-based digitized bleed bypasses a small excess current (=Quantized CS current value – average AES current) to mask the key-dependent small variations in average crypto current, by enabling LNFB through the supply of the RO. The gain ($\Delta I_{bleed}/\Delta V_{AES}$) can be controlled by tuning the number of parallel RO-bleed that are turned on. 3) GNFB SMC Loop: The same RO changes its frequency as a function of V_{AES}, which is counted by the digital SMC control logic and a deadband is employed in count domain (in-between the upper/lower limit) where the GNFB loop disengages in steady state and PMOS works as a CS, allowing high signature attenuation (dynamics shown in Fig. 36.2.3). Due to process, voltage, and temperature (PVT) variations or at startup, if ΔV_{AES} goes outside the desirable range, the GNFB loop turns ON or OFF the required number of current source slices and brings it back to the desirable range and disengages. Unlike [4], that had a separate analog bleed path and control loop with analog comparators, we adopt a fully digital RO-bleed-based integrated LNFB and GNFB, making the countermeasure synthesizable. The low-bandwidth of the GNFB loop (clocked at <10KHz) ensures ultra-low power. 4) The number of parallel RO stages that are ON can also be switched randomly to inject small current noise to further enhance protection of the DSAC. A 41-stage RO is chosen to minimize the area overhead and the power consumption (Fig. 36.2.3). The digital-friendly CS stage in the DSAC biased in saturation provides high output impedance and ensures that any voltage droop (~20-30mV) across the AES is suppressed before it reaches the supply pin (Fig. 36.2.2). Similar to [4] the DSAC hardware employs local lower-level metal routing and MOS cap to reduce EM leakage.

To further enhance the security (Fig. 36.2.3) while keeping the combined countermeasure generic, unlike [5], a synthesizable 16-phase switched-capacitor circuit is utilized which randomly shuffles the voltage across the AES in time realizing a physical Time-Varying Transfer Function (TVTF) to provide significant time-domain obfuscation. Unlike [1], that had a 1:1 relation between V_{AES} and V_{DD} in time and hence needed an analog residual equalizing circuit (switch S3), this work puts each time point residual to multiple random time-points creating a time-obfuscated random TF between V_{AES} and V_{DD}, removing the need for any analog equalizer, making the design synthesizable and lower power. A lightweight digital controller involving a 16b Fibonacci LFSR is used to randomly choose a capacitor to charge and another to discharge at any given time, using 2 separate 8×4 memories. Hence, the AES signature gets shuffled across different points in the time domain as the capacitor charging the AES at a given time connects to the supply at a different point in time. Time-domain measurements of the DSAC-TVTF embedding the AES-256 show that the traces are highly obfuscated and suppressed both for power, as well as EM side-channels (Fig. 36.2.3). The unprotected AES is powered with 0.8V input and consumes ~189μA average current at 10MHz.

A Hamming distance (HD) attack model on the last 2 rounds of the AES is used and a correlational power analysis (CPA) attack performed on the unprotected AES implementation shows an MTD of 7K (Fig. 36.2.4). Frequency-domain CPA is also performed with windowed FFT with a window size of 10MHz and the center frequency is varied from 10MHz to 2GHz. The protected AES in mode 2 (only DSAC turned ON) shows an MTD of 820M and 380M in the time and frequency domain, respectively, showing >54,285× improvement over the unprotected AES, and >38× improvement compared to the best single-technique synthesizable countermeasure [5]. In mode 3, with DSAC-TVTF, the correct key byte could not be revealed even after 1.25B encryptions, both in time, as well as in the frequency domain, showing a >178,000× improvement over the unprotected AES. Power TVLA results show ~95,000× and ~290,000×improvement in TVLA MTD (max |t|-score of 4.5) for DSAC and DSAC-TVTF compared to the unprotected AES-256.

A correlational EM analysis (CEMA) attack mounted on the unprotected AES-256 shows an MTD of 9K (Fig. 36.2.5), while the correct key for the DSAC-AES (mode 2) was revealed in 250M traces, showing >27,777× improvement over the unprotected AES, and >25× improvement over the state-of-the-art single technique synthesizable countermeasure. In mode 3, with both TVTF and the DSAC enabled, the key could not be recovered with 1.25B measurements using CEMA, both in time as well as in the frequency domain. Compared to the previous countermeasures, DSAC-TVTF AES-256 achieves 25% higher MTD (1B□>1.25B) and >178,000× (power) and >138,888× (EM) MTD improvement compared to the unprotected AES, without any performance overhead and comparable power/active area overheads (Fig. 36.2.6). The die photograph and chip characteristics are shown in Fig 36.2.7.

Acknowledgement:
This work was partly supported by NSF (Grant CNS 17-19235), and Intel Corporation.

References:

[1] C. Tokunaga, et al., "Secure AES Engine with a local Switched-Capacitor Current Equalizer," ISSCC, pp. 64-65, 2009.

[2] 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, 2019.

[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, 2017.

[4] D. Das, et al., "EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation," ISSCC, pp. 424-426, 2020.

[5] R. Kumar, et al., "A SCA-Resistant AES Engine in 14nm CMOS with Time/Frequency-Domain Leakage Suppression using Non-linear Digital LDO Cascaded with Arithmetic Countermeasures", VLSI 2020.

[6] D. Das et al., "Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS," IEEE CICC, 2020.

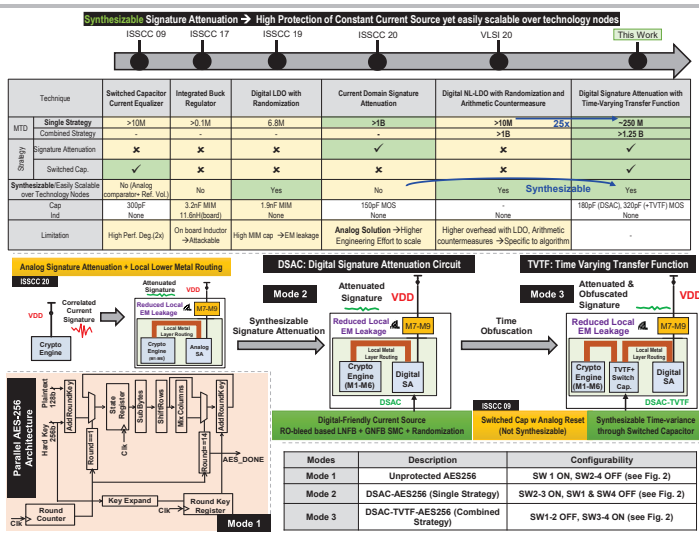


Figure 36.2.1: Motivation and overview of the design principles for the Digital Signature Attenuation Circuit (DSAC) combined with time-varying transfer function (TVTF) for both power and EM SCA protection.

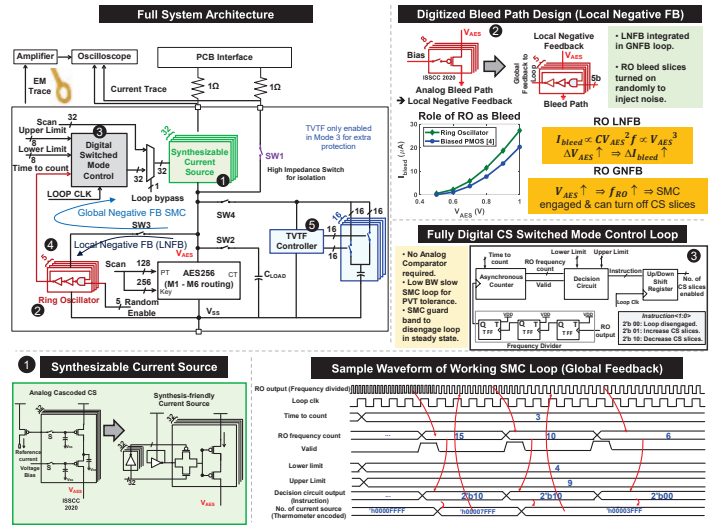


Figure 36.2.2: System Architecture showing the circuit details of the digital current source along with the role of the digital bleed to provide local negative feedback (LNFB) integrated with the switched mode control (SMC) loop providing the global negative feedback (GNFB).

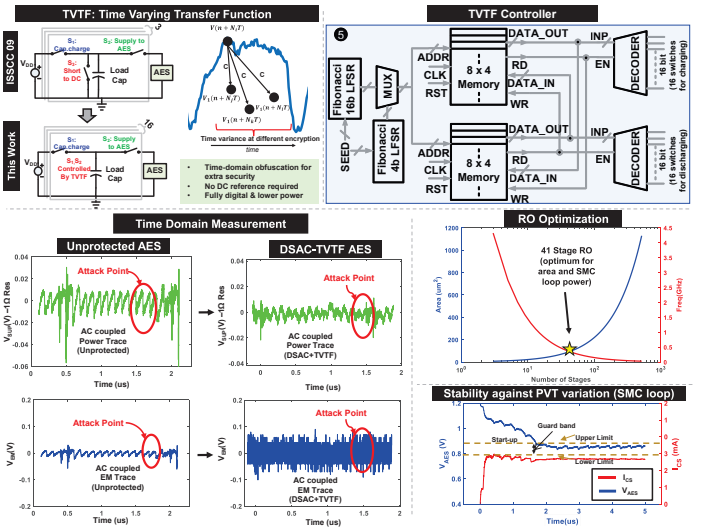


Figure 36.2.3: Time-varying transfer function (TVTF) involving multi-phase switched capacitors, and time-domain measurement results for the DSAC-TVTF AES256 for both power/EM traces.

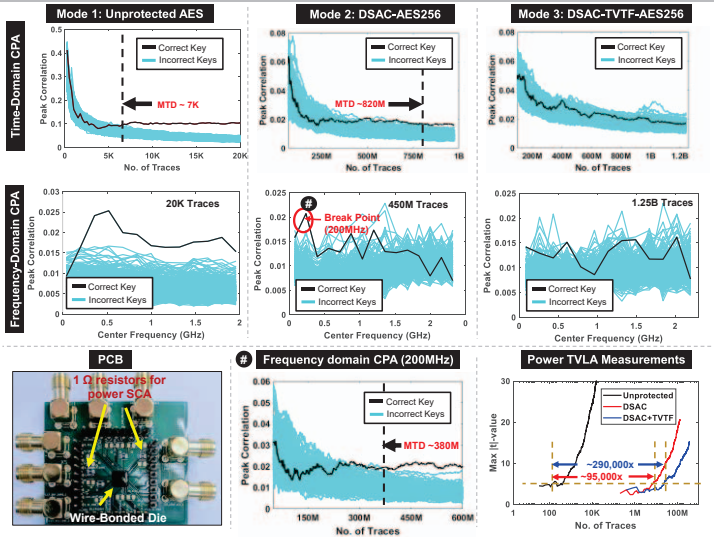
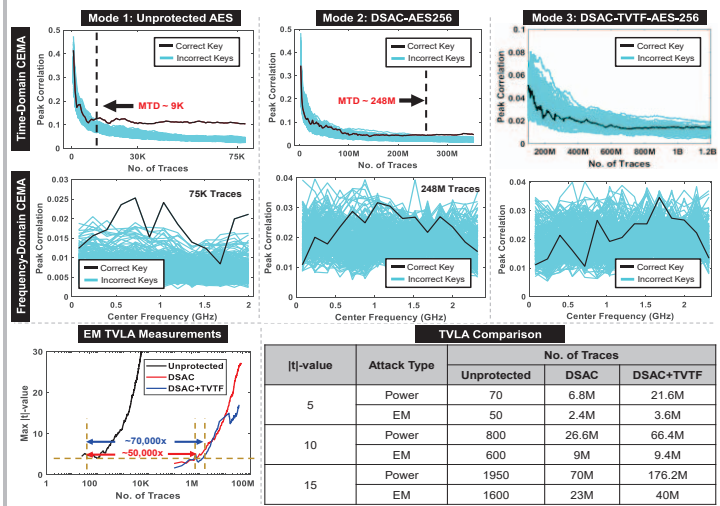


Figure 36.2.4: Measurement Results: Power SCA (both time and frequency domain) and Leakage Analysis demonstrating the resiliency of DSAC and DSAC-TVTF.



TVLA Comparison

|t|-value	Attack Type	No. of Traces		
		Unprotected	DSAC	DSAC+TVTF
5	Power	70	6.8M	21.6M
	EM	50	2.4M	3.6M
10	Power	800	26.6M	66.4M
	EM	600	9M	9.4M
15	Power	1950	70M	176.2M
	EM	1600	23M	40M

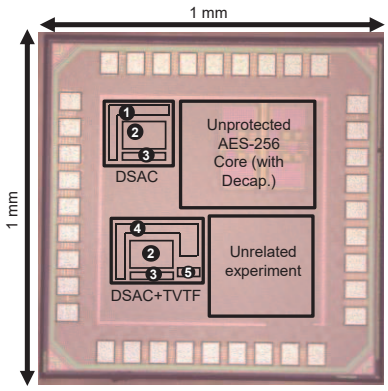
Figure 36.2.5: Measurement Results: Time and Frequency Domain CEMA attack and TVLA on the unprotected vs. DSAC/DSAC-TVTF AES256.

Power Overhead: $\frac{0.98V \times 206\mu A}{0.8V \times 189\mu A}$ = 1.33x | DSAC Area Overhead: $\frac{0.042\,mm^2}{0.15\,mm^2}$ = 28% | DSAC+TVTF Area Overhead: $\frac{0.078\,mm^2}{0.15\,mm^2}$ = 52%

Parameter			This Work	VLSI'20 [5]	ISSCC'20 [4]	ISSCC'19 [2]	ISSCC'17 [3]	ISSCC '09 [1]
Countermeasure Technique			Digital Signature Attn (DSAC) +TVTF	NL-DLDO + Arithmetic Countermeasures	Current Domain Signature Attenuation	Digital LDO with randomization	Integrated Buck Regulator	Switched Capacitor Current Equalizer
Process			65nm CMOS	14nm CMOS	65nm CMOS	130nm CMOS	130nm CMOS	130nm CMOS
Crypto Algorithm			AES-256	AES-128	AES-256	AES-128	AES-128	AES-128
Standalone AES Power/Frequency			189uW@ 10MHz,0.8V	-	0.8mW @ 50MHz, 0.8V	10.9mW @ 80MHz, 0.84V	10.5mW @ 40MHz	33mW @ 100MHz
Design Overheads	Area		28% & 52%[d]	8%[c]	36.7%	36.9%[b]	1%[a]	33%
	Power		33% & 50%[d]	10%[c]	49.8%	32%	5%[a]	20%
	Perf.		0%	0.7%	0%	10.4%	3.33%	50%
SCA Analysis	Time/Freq Domain		Time, Freq	Time	Time, Freq	Time, Freq	Time, Freq	Time
	MTD	Power	390M & >1.25B	1B (>1,00,000x)	>1B (1,25,000x)	8M (4210x)	>100K (20x)	>10M (2500x)
		EM	248M & >1.25B	1B (>1,00,000x)	>1B (>83,333x)	6.8M (136x)	-	-
	Attack Mode		Power/EM	Power/EM	Power/EM	Power/EM	Power	Power

[a]Does not include regulator area/power, [b]Does not include Cap area, [c]Does not include DLDO area/power. Area overhead >150% with DLDO (estimated), [d]Power overhead includes the dropout voltage across current source, the extra bleed current drawn, SMC loop and TVTF power. Area overhead includes all the extra components without unprotected and calculated with respect to unprotected AES-256.

Figure 36.2.6: Comparison with State-of-the-Art countermeasures and Overhead Analysis.



Test Chip	Process	65nm CMOS LP
	Package	Wire-bond (Glob-Top Encapsulation)
Unprotected AES-256 Core	Performance	0.8V/10MHz/189uW
	Architecture	128b Datapath (parallel AES)
	Supply Decap	60 pF MOS Cap (0.006 mm^2)
	Active Area	0.15 mm^2
	Scan Chain	387b
Protected-AES256	Input	0.98V
	Active Area	0.192 mm^2/0.222mm^2
	Supply Decap	60 pF MOS Cap (0.006 mm^2)
	Load Cap	180 pF MOS Cap (0.018 mm^2)
	Switched Cap	320pF Switched Cap (0.03 mm^2)
	Scan Chain	AES Core: 387b
		Protected core: 143b

❶ Load Cap.
❷ Current Source
❸ Current Source Controller
❹ Switched Cap. bank
❺ TVTF Controller

Figure 36.2.7: Die Micrograph of the system in 65nm CMOS process and design summary.