25.3 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

Arvind Singh[1], Monodeep Kar[2], Sanu Mathew[2], Anand Rajan[2], Vivek De[2], Saibal Mukhopadhyay[1]

[1]Georgia Institute of Technology, Atlanta, GA
[2]Intel, Hillsboro, OR

Side channel attacks (SCA) exploit data-dependent information leakage through power consumption and electromagnetic (EM) emissions from cryptographic engines to uncover secret keys. Integrated inductive voltage regulators (IVR) with a randomized control loop [1] or switching frequency [2], and random voltage dithering [3] have demonstrated improved power side-channel analysis (PSCA) resistance. Simulation studies have shown PSCA resistance via shunt linear regulators [4]. This paper demonstrates improved power and EM SCA resistance of standard (unprotected) 128b AES engines with parallel (P-AES, 128b) and serial (S-AES, 8b) datapaths via an on-die security-aware all-digital series low-dropout (DLDO) regulator, commonly used for fine-grain SoC power management. The security-aware DLDO improves SCA resistance using control-loop induced perturbations in a baseline DLDO, enhanced by a random switching noise injector (SNI) via power stage control and a randomized reference voltage (R-VREF) generator coupled with all-digital clock modulation (ADCM).

The fabricated 130nm CMOS test-chip (Fig. 25.3.7) contains P-AES and S-AES cores powered by a DLDO with 0.5-to-1.22V input and 1.9nF on-die metal-insulator-metal (MIM) load capacitor (Fig. 25.3.1). The DLDO is implemented with a 32-element PMOS array power stage. The feedback loop, sampled at 250MHz, includes a 4b analog-to-digital converter (ADC) and a digital type-III (two zeros and two poles) proportional-integral-derivative (PID) compensator. Measured supply current at the input supply ($V_{IN,DLDO}$) of the chip is a transformed version of the internal on-die supply current of the AES engine measured at local supply node (V_{AES}). The DLDO power stage acts as a low-pass filter with bandwidth dictated by the equivalent resistance of the power stage and output capacitor, thereby attenuating the high-frequency current signatures. The DLDO control loop induces frequency-dependent small signal perturbations dictated by the loop delay and zero/pole locations. PID coefficients (K_P, K_I, K_D) can be modified at runtime to reduce information leakage, while modulating the transient response of the DLDO to load/reference changes.

The SNI generates programmable pulses in each DLDO clock cycle to disable all devices in the PMOS array for a fraction of the clock cycle, thus disconnecting an information leakage path from V_{AES} to $V_{IN,DLDO}$ (Fig. 25.3.2). The SNI consists of nine pulse generators – each generating a pulse using four of the nine phases of a 9-stage current-starved differential-delay-cell-based voltage-controlled-oscillator (VCO). A maximum length 4b linear-feedback shift register (LFSR) generates a signal to select one of the nine pulses randomly. As the SNI is activated, the output decoupling capacitor supplies the current required for AES operation when PMOS's are all off. When the PMOS's are enabled again, the DLDO feedback loop responds to the voltage droop at V_{AES}, thus adding amplitude noise at V_{AES} (and $V_{IN,DLDO}$) even when the power stage PMOS's are ON. In addition, since the AES and DLDO clocks are not synchronized, current signatures at $V_{IN,DLDO}$ and V_{AES} are de-synchronized. The R-VREF circuit randomly (with 4b LFSR – LFSR3) selects a digital word for the reference voltage (V_{REF}) from pre-loaded registers and induces an output voltage transition in programmable regular intervals, thus randomizing the AES supply voltage (V_{AES}) (Fig. 25.3.2). Reference registers are pre-loaded with V_{REF} words such that the mean is equal to the target operating voltage, while the injected randomness is governed by the standard deviation. Unlike voltage dithering [3], where V_{AES} only changes between encryptions, the R-VREF runs at high frequency (DLDO clock/16) randomizing V_{AES} even during an encryption. An on-die ADCM circuit uses critical-path replicas to modulate edges of the AES clock and ensure correct operation under transient supply droops and variations induced by both SNI and R-VREF. ADCM utilizes the random noise in V_{AES} to inject additional timing and amplitude randomizations in the current signatures [3].

A test-control switch enables AES cores to operate in standalone (externally powered) or DLDO-powered modes (Fig. 25.3.1). Test vector leakage assessment (TVLA) and correlation power analysis (CPA) are performed for power and EM signatures in the time and frequency domains. Power signatures are measured as differential voltages across a 1Ω series resistor at V_{AES} (standalone AES) and $V_{IN,DLDO}$ (DLDO-AES) pins (Fig. 25.3.3). An external trigger is used to start AES encryptions. Measured patterns at $V_{IN,DLDO}$ show that the power signature, although distinguishable, is attenuated by ~5.6× compared to V_{AES}. When SNI and R-VREF are enabled, P-AES rounds are no longer distinguishable at $V_{IN,DLDO}$. EM signatures, though much weaker, show distinct peaks during the P-AES rounds. The power/EM signatures are filtered with narrow bandpass filters (10MHz) ranging from 5MHz to 305MHz to remove out-of-band noise. Filtered signatures are aligned with cross-correlation to remove the initial delay caused by use of an external trigger.

TVLA on P-AES shows high information leakage for the standalone AES (baseline) which reduces significantly for DLDO-AES (Fig. 25.3.4). When K_P=K_D=0 for the PID controller (integral compensator with K_I=1/32), TVLA leakage is maximum, while it is reduced for higher K_P and K_I values, which leads to underdamped response. Similarly, a faster R-VREF clock and larger SNI pulse width leads to more amplitude and timing (with ADCM) randomization, producing lower TVLA leakages. Although SNI increases noise at $V_{AES,}$ correct operation is ensured by ADCM with only 9.3% performance loss. The R-VREF generates V_{AES} levels with a mean close to the nominal value to ensure minimal (-1.1%) loss in the average throughput of the AES core.

CPA analysis on byte 9 (highest leaking byte) of the P-AES 128b key with 5 million measurement shows high correlation ratio (CR), defined as the ratio of absolute correlation for correct key guess and 2nd highest correlation for successful attack, across all bands for standalone AES. The CR value reduces for DLDO-AES with most of the bands still leaking (Fig. 25.3.5). With the R-VREF and SNI, CR reduces to 1.3 with only a few bands leaking. CPA in the frequency domain shows that byte 9 of the key in standalone P-AES can be uncovered with only 400 (minimum-traces-to-disclose, MTD) measurements, while 3.6 million measurements are required for DLDO-AES with the R-VREF and SNI. Note, when AES is powered externally through V_{OUT} (DLDO, R-VREF, SNI off) to emulate a design with an "on" power gate (test-control switch) with 1.9nF decap on the ungated input rail and 0.4nF on the virtual rail, the MTD increases to only 2200. All key bytes were extracted with up to 10 million measurements for frequency-domain CPA (Fig. 25.3.6). MTD for an 80% success rate (SR) (i.e. to reveal 13/16 key bytes) for baseline P-AES is 1900 (CPA) and 50K (CEMA), which improves to 8M (CPA) and 6.8M (CEMA) for DLDO-AES with the SNI and R-VREF. MTD considering both CPA and CEMA increases by 3579× for P-AES and by 2182× for S-AES. Including overheads due to the power stage, controller, and R-VREF/SNI, the DLDO-AES shows 36.9% higher area and 10.4% lower performance than the standalone AES, and 68% power-efficiency, while driving 40mA @ 0.84V.

A power injection attack (PIA) with a voltage glitch [2] is performed at V_{CTRL} (control supply that powers the DLDO loop, R-VREF, SNI, and LFSRs), and $V_{IN,DLDO}$. The PIA at V_{CTRL} introduced instability/noise at V_{AES} forcing random clock-skipping from ADCM, which de-synchronizes power/EM signatures [with 100mV glitch TVLA reduced to 5.8 (power) and 7.7 (EM)] but degrades encryption throughput. A PIA on $V_{IN,DLDO}$ can cause all power PMOS's to be always ON, rendering DLDO and R-VREF ineffective, but SNI remains effective; MTD of 8.4M (power) and 6.0M (EM) are observed for an 80mV glitch. The security of DLDO-AES can be further improved by using a TRNG to reduce predictability/repeatability of the LFSR and adding input sensing circuits at $V_{IN,DLDO}$ and V_{CTRL} to inhibit a PIA [2].

Acknowledgements:
This material is based on work supported in part by Intel Corporation and Semiconductor Research Corporation through TxACE (#2810.002 and #2712.002).

References:
[1] M. Kar, et al., "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator," *IEEE JSSC*, vol. 53, no. 8, pp. 2399-2414, 2018.
[2] W. Yang, et al., "An Enhanced-Security Buck DC-DC Converter with True-Random-Number-Based Pseudo Hysteresis Controller for Internet-of-Everything (IoE) Devices," *ISSCC*, pp. 126-128, 2018.
[3] A. Singh, et al., "Improved Power Side Channel Attack Resistance of a 128-bit AES Engine with Random Fast Voltage Dithering," *ESSCIRC*, pp. 51-54, 2017.
[4] 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.
[5] 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.
[6] C. Tokunaga, et al., "Secure AES Engine with a local Switched-Capacitor Current Equalizer," *ISSCC*, pp. 64-65, 2009.

 978-1-5386-8531-0/19/$31.00

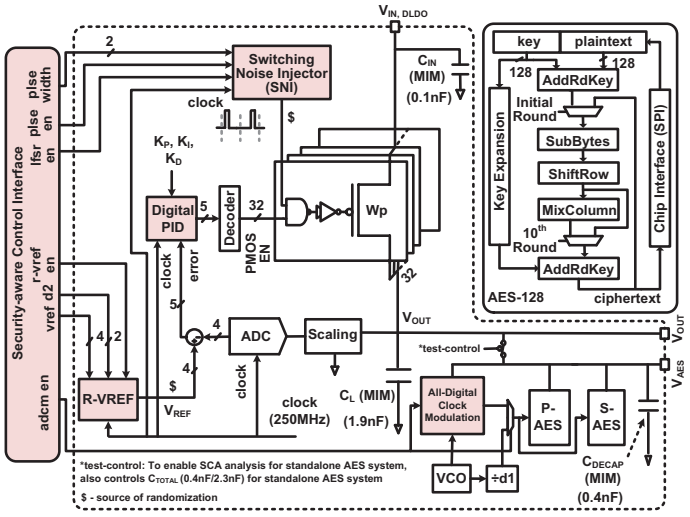


Figure 25.3.1: Architecture of security-aware digital LDO. Circuit blocks to enhance resistance to side channel attacks are shaded.

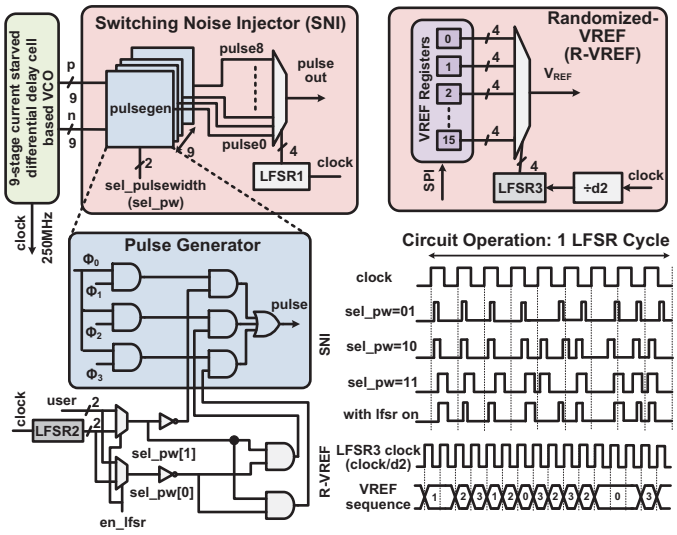
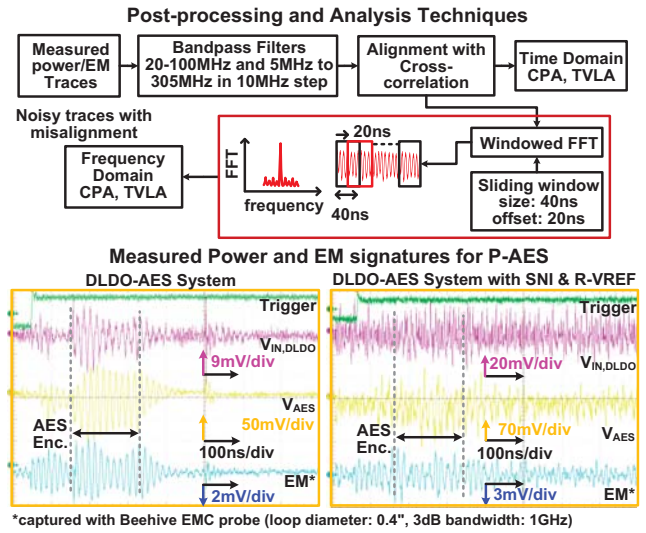
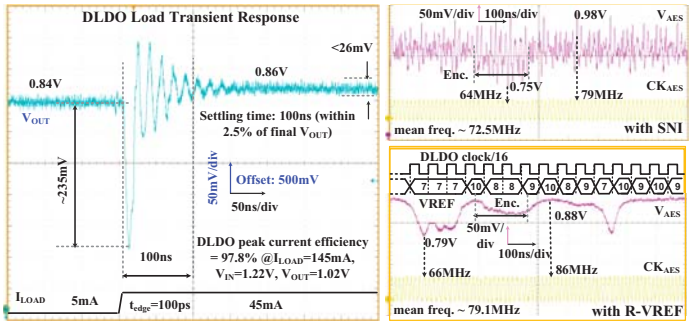


Figure 25.3.2: Circuit techniques and circuit operation for SNI and R-VREF circuits.



*captured with Beehive EMC probe (loop diameter: 0.4", 3dB bandwidth: 1GHz)

Figure 25.3.3: Filtering and alignment techniques for the measured signatures for SCA in time and frequency domains.



TVLA Analysis for Baseline and DLDO-AES system with SNI & R-VREF for P-AES

Circuit Technique	Baseline AES	DLDO-AES							
		PID Controller (K_P, K_I, K_D)			LFSR clock for R-VREF		Pulse width for SNI		
Configurations	-	22/32, 24/32, 9/32*	10/32, 7/32, 2/32	0, 1/32, 0	DIV16*	DIV64	$\frac{T_{clock}}{9}$	$\frac{2T_{clock}}{9}$	$\frac{3T_{clock}*}{9}$
TVLA Peak	258	23.4	25.2	32.9	13.1	17.4	14	13.7	11.9

* configuration used for final SCA-resistant design

Figure 25.3.4: Load transient response of DLDO and measured SNI and R-VREF waveforms with ADCM and TVLA analysis with different configurations.

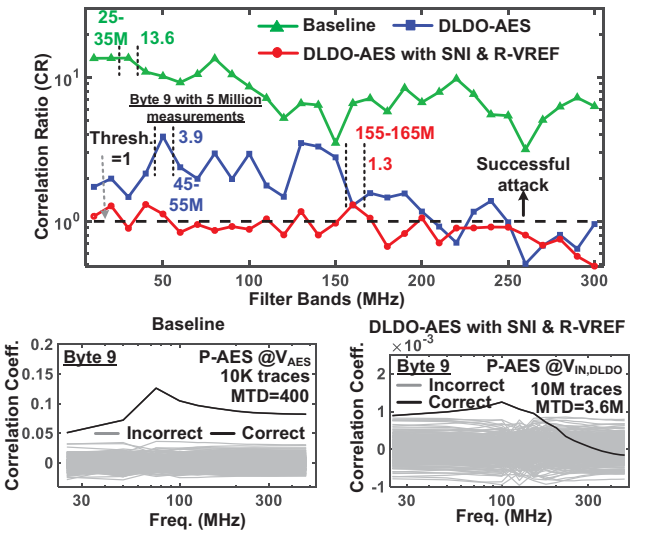
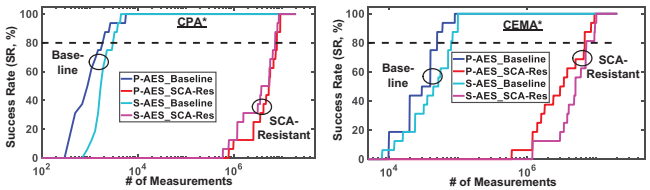


Figure 25.3.5: Correlation ratio plotted against filter bands and correlation plots in frequency domain showing successful key recovery.



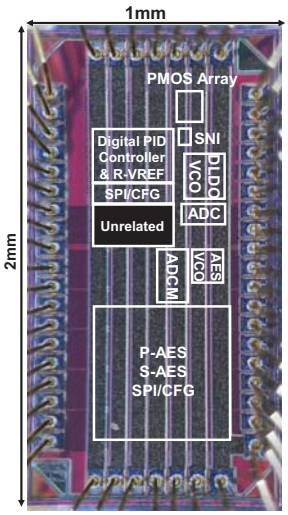
*powerModel: P-AES- hamming distance between 10th round input and ciphertext, S-AES- hamming weight for 1st SBOX output

Comparison with Existing Works

Metric		This Work	JSSC'18 [1]	ESSCIRC'17 [3]	VLSI'15 [5]	ISSCC'09 [6]	ISSCC'18 [2]
Countermeasure Technique		On-chip Digital Low Dropout Regulator with SNI & R-VREF	Integrated Buck Regulator	Random Fast Voltage Dithering	Charge Recovery Logic	Switch Capacitor Current Equalizer	Buck Regulator
Technology		130nm	130nm	130nm	65nm	130nm	55nm
AES power[a]		10.9mW @ 80MHz, 0.84V	10.5mW @40MHz	13.1mW @49.7MHz	138mW @1.32GHz	33mW @100MHz	No AES/other Encrypt-ion Engine present
Design Overheads[a]	Area	36.9%[b]	1%[c]	5.5%[c]	25%	33%	
	Power	32%[b]	5%[c]	5.9%[c]	30%	20%	
	Perf.	10.4%	3.33%	1.8%	0%	50%	
# of Measurements		10M	500K	500K	1M	10M	N/A[e] (No SCA)
SCA Analysis[d]	Time/Freq. Domain	Time, Freq.	Time, Freq.	Time	Time	Time	
	MTD for 80% SR	6.8M (3579×)[f]	>500K (100×)[g]	>500K (33×)[g]	940K (251×)[h]	>10M (2500×)[i]	
	Attack Mode	Power, EM	Power, EM	Power	Power	Power	

[a]With respect to parallel AES (P-AES). [b]Includes DLDO regulator area/power. [c]Doesn't include regulator area/power. [d]For P-AES. [e]Relative correlation based analysis. [f]Minimum of CPA MTD and CEMA MTD. [g]SCA performed for only 1 byte. [h]MTD to disclose all bytes. [i]None of the bytes could be disclosed.

Figure 25.3.6: Success rate for CPA/CEMA and comparison with existing works.



Test-chip	Process		130nm CMOS
	Package		LCC52
Digital LDO with SNI and R-VREF	Active Area		0.078mm^2
	V_{IN} [V]		0.5 – 1.22
	V_{OUT} [V]		0.35 – 1.17
	Current [mA]		5 – 145
	Load Cap [nF]		1.9 (0.44mm^2)
	Compensator		Type III
	ADC		4-bit delay line based
	Peak Current Eff. (DLDO)		97.8% @145mA, V_{IN}/V_{OUT}=1.22V/1.02V
ADCM	Clock [MHz]		600
	Op. range [V]		0.73 – 1.25
	Area		0.024mm^2
AES-128	Perf.	P-AES	80MHz/0.84V/10.9mW
		S-AES	80MHz/0.84V/2mW
	Arch.	P-AES	128b (datapath)
		S-AES	8b (datapath)
	Decap [nF]		0.4 (0.088mm^2)

Figure 25.3.7: Chip micrograph and design details.

978-1-5386-8531-0/19/$31.00 ©2019 IEEE