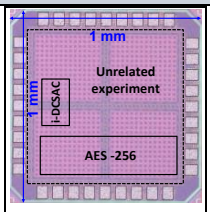
A Digital *Cascoded* Signature Attenuation Countermeasure with Intelligent Malicious Voltage Drop Attack Detector for EM/Power SCA Resilient Parallel AES-256

Archisman Ghosh[1], Dong-Hyun Seo[1], Debayan Das[1,2], Santosh Ghosh[2], Shreyas Sen[1]

[1]Purdue University, IN, USA, [2]Intel Corp. Portland, OR, USA,

Computationally secure cryptographic algorithm leaks meaningful side-channel information which can be exploited to extract confidential data. Circuit level countermeasures against power/ EM side channel attack (SCA) like current equalizer [1], series LDO with randomization [2], integrated buck regulator (IBR) [3] had been demonstrated recently providing moderate security (~10M) against Correlational Power/EM attack (CPA/CEMA). Current domain signature attenuation (CDSA) [4] achieved >1B minimum-traces-to-disclosure (MTD) with a single analog technique. Randomized non-linear LDO cascaded with arithmetic countermeasure achieves similar security [5], albeit with combination of two techniques. A process-scalable version of [4] achieved ~250M MTD [6] with bleed-RO randomization, and ~20M MTD without it [7]. Cascading this solution with TVTF [6] provided highest security till date. On the other hand, digital friendly NL-DLDO suffers from higher overhead. Arithmetic countermeasure is fully synthesizable, but algorithm specific, cannot be easily ported to another encryption algorithm. In [6], the digital friendly current source (CS) brings the benefit of signature attenuation in digital domain, however, lacks the high attenuation and MTD from Analog Cascode CS in [4]. Most importantly, a dedicated attack on the state-of-the-art (SoA) countermeasures is still left unexplored. This work for the first time explores the possibility of an attack on signature attenuation hardwares using malicious reduction of voltage and utilizes an intelligent attack detector circuit to detect such attacks and adapt to it to guarantee the efficacy of such signature attenuation-based countermeasures. Moreover, an improved digital-friendly *cascoded* CS is implemented achieving the highest signature attenuation with digital-friendly technique till date, i.e. a ~10x improvement without RO-bleed randomization. A detailed progress of countermeasure along with motivation is presented in Fig. 1. The 65nm CMOS test chip (side figure) consists of a parallel AES-256 encryption engine along with an Intelligent Digital *Cascoded* Signature Attenuation Circuit (i-DCSAC) as countermeasure and malicious attack detector.

The i-DCSAC (Fig. 2) consists of a digital *cascoded* current source (DCCS), multiple scan-controlled parallel ring oscillators (RO) as the bleed path to bypass the delta changes in the supply current, thereby stabilizing the V_{AES} node voltage by providing local negative feedback and hiding small key-dependent current changes. Simultaneously, the RO-bleed is the input of the global feedback (switch mode controller) which is a slow loop to compensate for PVT variation or sudden changes in the crypto current due to frequency variation of the encryption engine. The DCCS consists of 32 CS slices. Each slice uses 2 PMOS which are biased in saturation region to provide a high attenuation like the analog CS in [4]. Multi-stage parallel self-biased NAND gates are utilized to generate a tunable bias voltage to bias top PMOS at an internal voltage within $0.5V_{DD}$ to V_{DD}. Bias voltage can be tuned by turning on or off the other input of the NAND gate. On the other hand, bottom PMOS is biased by a self-biased NOT gate providing $0.5V_{DD}$. The post-layout simulation of this digital-friendly i-DCSAC circuit shows a signature attenuation of ~343x and hence expected MTD increase of 343^2 or >100,000x compared to unprotected AES. Fig. 2 shows the attack modality on the signature attenuation-based countermeasures. High suppression is achieved by the CS in saturation. For an intelligent attacker, supplying the same amount of current while maintaining the CS in linear region will reduce the signature attenuation and increase the correlated power/EM leakage. As shown in Fig. 2, if an attacker reduces V_{DD} from the desired value such that the CS goes to the linear region while the lower threshold and upper threshold of the global SMC loop remain constant, more CS slices will be turned on due to the SMC operation, drawing the same amount of current (unlike CS being in saturation) from the supply pin, to operate AES-256. At that optimal region for attack, the CS will remain in linear region with the AES operating correctly, thus enabling an intelligent attacker to reduce the efficacy of signature attenuation and break the secret key with a low number of traces. However, lowering V_{DD} by a significant amount will cause the SMC loop failing to supply the AES current making V_{AES} drop continuously, and hence the crypto itself will not work, failing the attack.



Die micrograph.

Fig. 3 shows load characterization of the circuit (Point of experiment: 20MHz). System behavior for the voltage drop attack is shown in Fig. 3(top right). To further enhance the security (Fig. 3) while keeping the combined countermeasure generic, an intelligent attack detector circuit is implemented. If CS goes out of saturation region, the circuit outputs an alarm to stop the operation of the encryption engine which can also be used to activate other higher-power countermeasures intermittently, when the attacker is present. The Bleed RO, which serves the dual purpose of integrated local negative feedback and input to the global feedback is also leveraged in the intelligent malicious voltage drop attack detector block. The attack detector uses the bleed RO and a second replica RO driven from a voltage divider from V_{DD} to match the divided voltage close to V_{AES}. The count from both the ROs are fed to a digital comparator, which decides if the CS is out of saturation (detecting a malicious voltage drop) depending on the output of the counter and subsequently alarms the encryption engine to turn off. Area of intelligent malicious voltage drop detector is $0.008mm^2$ (<6% with respect to AES-256). A sample waveform is presented in Fig. 3 (middle right), showing detection of voltage drop. The PCB equipped for SCA on the i-DCSAC AES 256 IC is shown in Fig. 3. MTD of unprotected AES is 2.3K & 4.4K using CPA & CEMA (Fig. 3). Fig. 4 shows the efficacy of the i-DCSAC countermeasure. The measured timing waveforms showing attenuation is presented. CPA/CEMA is unable to recover the key until 200M traces both in time and frequency domain. Test Vector Leakage Assessment (TVLA) on the power traces reveals that meaningful leakage (t-value > 4.5) requires 500,000x more traces compared to the unprotected counterpart to reach the t-value of 4.5. Fig. 5 shows the voltage drop -based attack on signature attenuation countermeasure. CPA reveals the correct key byte with 105K traces which is much lower than protected i-DCSAC-AES (>200M). A measured timing waveform is presented in this Fig. 5 confirming the efficacy of the intelligent malicious drop detector showing <1ms latency of attack detection, in which CPA/CEMA attack is impossible. Fig. 6 presents the comparison table with existing state-of-the-art. Our countermeasure for the first time includes an intelligent attack detector for sustainability of the countermeasure against power delivery system manipulation based intelligent attack. With only a single digital-friendly *cascoding* technique without RO-bleed randomization, i-DCSAC achieves the highest MTD by any digital signature attenuation (20M → 200M, 10x over SoA), and highest power TVLA improvement with respect to unprotected counterpart. It can be cascaded to any other generic countermeasure for higher security.

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

References:

[1] C. Tokunaga, et al., ISSCC, 2009. [2] A. Singh et al., ISSCC, 2019. [3] M. Kar et al., ISSCC, 2017. [4] D. Das, et al., ISSCC, 2020. [5] R. Kumar, et al., VLSI 2020. [6] A. Ghosh et al., ISSCC 2021. [7] A. Ghosh et al., JSCC 2021.

2022 IEEE Custom Integrated Circuits Conference (CICC) | 978-1-6654-0756-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/CICC53496.2022.9772853

978-1-6654-0756-4/22/$31.00 ©2022 IEEE

Authorized licensed use limited to: Purdue University. Downloaded on May 24,2022 at 22:11:58 UTC from IEEE Xplore. Restrictions apply.

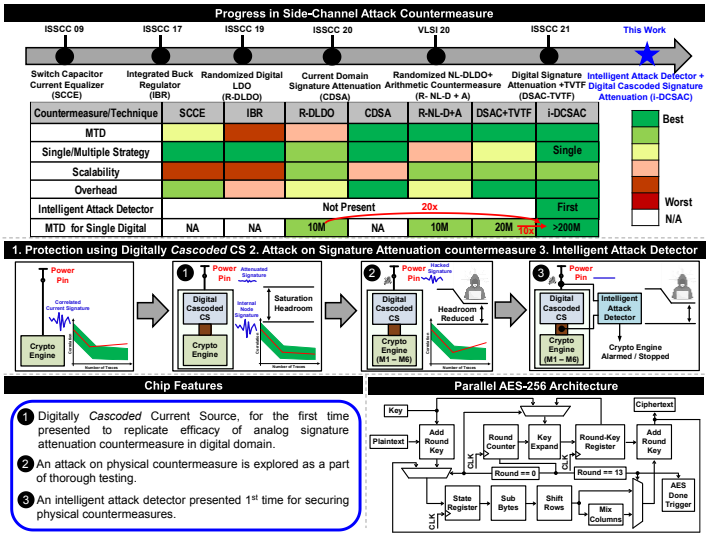


Fig. 1. Progress of circuit level countermeasures. Motivation for attack on signature attenuation countermeasures & Chip features.

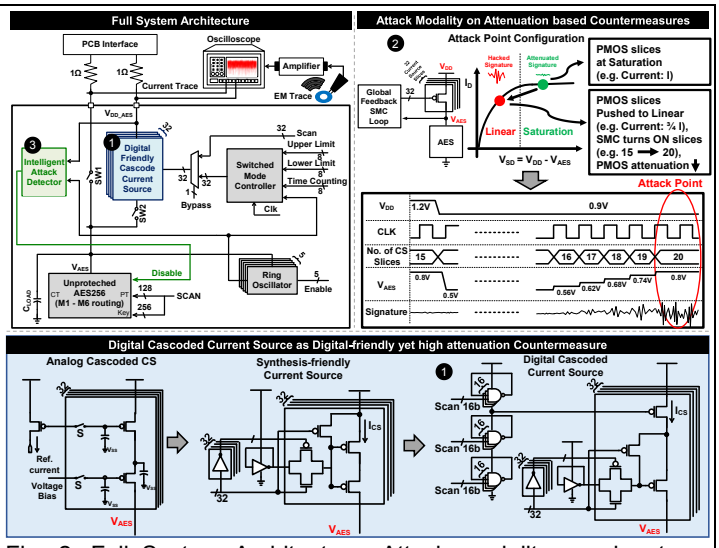


Fig. 2. Full System Architecture. Attack modality on signature attenuation & based countermeasures & architecture for digital cascoded CS.

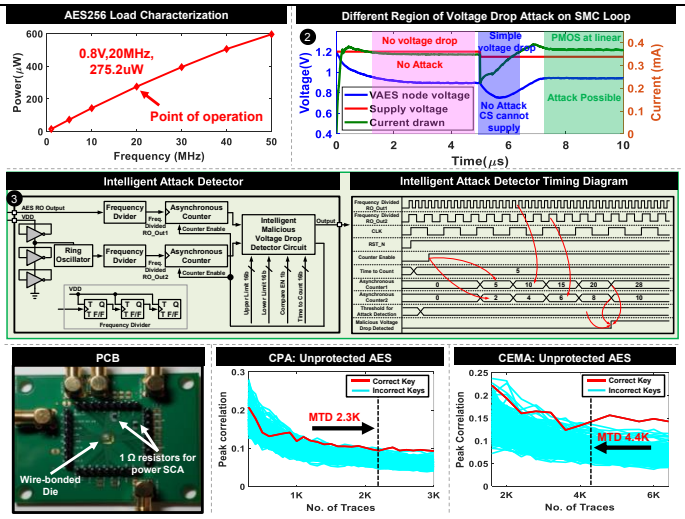


Fig. 3. Load characteristics of parallel AES-256. System-level simulation results showing transient at different nodes after voltage drop attack. Architecture & timing diagram of Intelligent Attack detector. CPA & CEMA on unprotected implementation.

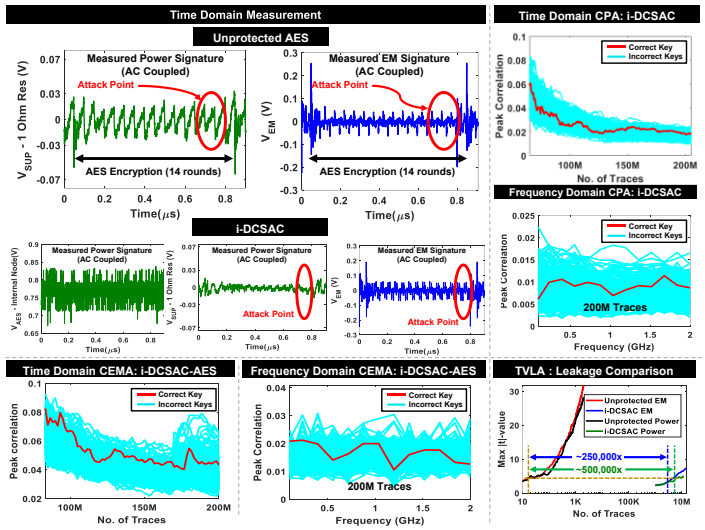


Fig. 4. Time domain measurement is shown. Time/frequency domain CPA/CEMA are perform on i-DCSAC. TVLA analysis-based comparison (bottom right)

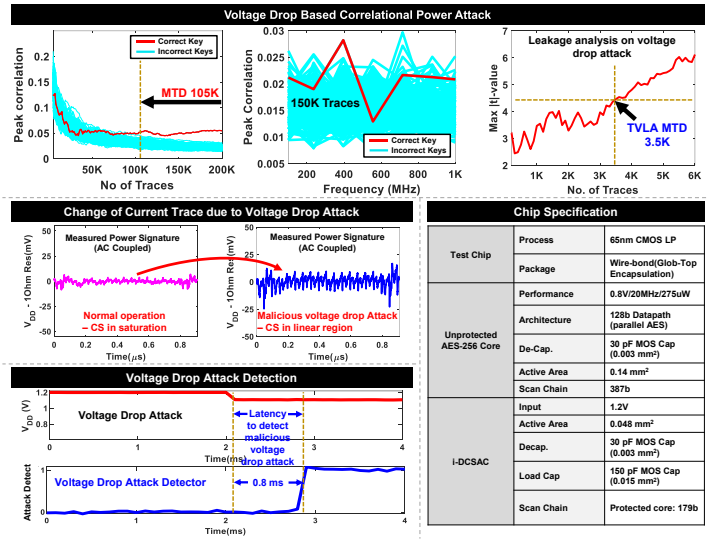


Fig. 5. Voltage drop based correlational power attack. Attenuation changes in measured waveform & voltage drop attack detection.

Parameter		This Work	ISSCC'21 [6]	VLSI'20 [5]	ISSCC'20 [4]	ISSCC'19 [2]	ISSCC'17 [3]	ISSC '09 [1]
Countermeasure Technique		Intelligent Digital Cascode Signature Attn.Circuit (i-DCSAC)	Digital Signature Attn (DSAC) +TVTF	NL-DLDO + Arithmetic Counter-measures	Current Domain Signature Attenuation	Digital LDO with randomization	Integrated Buck Regulator	Switched Capacitor Current Equalizer
Process		65nm CMOS	65nm CMOS	14nm CMOS	65nm CMOS	130nm CMOS	130nm CMOS	130nm CMOS
Crypto Algorithm		AES-256	AES-256	AES-128	AES-256	AES-128	AES-128	AES-128
Standalone AES Power/Frequency		275.2uW @ 20MHz, 0.8V	189uW @ 10MHz, 0.8V	-	0.8mW @ 50MHz, 0.8V	10.9mW @ 80MHz,0.84V	10.5mW @ 40MHz	33mW @ 100MHz
Single Strategy		Yes	No	No	Yes	No	Yes	Yes
Design Overheads	Area	35%	28% & 52%	8%[c]	36.7%	36.9%[b]	1%[a]	33%
	Power	50%	33% & 50%	10%[c]	49.8%	32%	5%[a]	20%
	Perf.	0%	0%	0.7%	0%	10.4%	3.33%	50%
SCA Analysis	Time/Freq Domain	Time, Freq	Time, Freq	Time	Time, Freq	Time, Freq	Time, Freq	Time
	MTD CPA	>200M	390M(~20M)* & >1.25B	1B (>1,00,000x)	>1B (1,25,000x)	8M (4210x)	>100K (20x)	>10M (2500x)
	MTD CEMA	>200M	248M(~20M)* & >1.25B	1B (>1,00,000x)	>1B (>83,333x)	6.8M (136x)	-	-
	MTD Power TVLA	>500,000x	195,000x & 290,000x	>250,000x	-	-	-	-
	MTD EM TVLA	>250,000x	>50,000x &>70,000x	>250,000x	-	-	-	-
	Attack Mode	Power/EM	Power/EM	Power/EM	Power/EM	Power/EM	Power	Power
	Attack on Countermeasure Detection	Yes	-	-	-	-	-	-

*Regulator area/power not included, [b]Cap area not included, [c]DLDO area/power not included. Area overhead >150% with DLDO (estimated), [a]20M MTD without bleed randomization (with only digital CS).

Fig. 6. Comparison with State-of-the-Art countermeasures.

Authorized licensed use limited to: Purdue University. Downloaded on May 24,2022 at 22:11:58 UTC from IEEE Xplore. Restrictions apply.