EM SCA & FI Self-Awareness and Resilience with Single On-chip Loop & ML Classifiers

Archisman Ghosh*, Debayan Das*, Santosh Ghosh† and Shreyas Sen*
*School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA
†Intel Labs, Intel Corporation, Hillsboro, OR. USA

***Abstract*—Securing ICs are becoming increasingly challenging with rapid improvements in electromagnetic (EM) side-channel analysis (SCA) and fault injection (FI) attacks. In this work, we develop a pro-active approach to detect and counter these attacks by embedding a single on-chip integrated loop around a crypto core (AES-256), designed and fabricated using TSMC 65nm process. The measured results demonstrate that the proposed system 1) provides EM-Self-awareness by acting as an on-chip H-field sensor, detecting voltage/clock glitching fault-attacks; 2) senses an approaching EM probe to detect any incoming threat; and 3) can be used to induce EM noise to increase resilience against EM attacks. This work combines EM analysis, ML based secured system and shows the efficacy by measurements from custom-built 65nm CMOS IC.**

***Index Terms*—On-chip Sensor, Fault injection detection, Approaching EM Probe detection, Inductive sensing, EM side-channel, Clock and Voltage glitch detection, machine learning classification, attack resilience.**

I. Introduction

Mathematically secure cryptographic algorithms are being used in almost all the modern embedded systems like smartphones, smartcards, ATMs, personal computers and other IoT devices to ensure data security and trust. It has been demonstrated that EM side channel information can be exploited for extracting correct key in last decade [1]. Data from these devices can be easily stolen from a distance using cheap EM probes ([2], [3]) or using fault-injection attack via clock glitching and voltage glitching [4]. Several recent works have revealed these vulnerabilities and have proposed solutions for different aspects such as glitch detection [5], [6], EM probe detection [7], and generic countermeasures against EM side channel attack [8], [9]. This paper uses EM signature of the on-chip loop followed by a low overhead ML classifier to detect FIA and EM SCA and demonstrates an additional way to mitigate EM SCA in addition to existing countermeasure. FIA typically relies on precisely timed clock/power glitch or corruption of the circuit operation due to higher temperature/UV-rays etc. during circuit operation. A differential observation of output between correct and faulty key can reveal the secret information easily [4], leading to differential fault attack (DFA). Recent countermeasures of EM SCA mostly suffer from high area, power, or performance overheads. One way to reduce its power overhead is to detect the attack and accordingly turn on the countermeasure. Noise injection is one of the countermeasures to mitigate SCA at the cost of high power overheads. However, once an EM SCA attack is detected, noise injection can be used in conjunction with another countermeasure to enhance EM SCA immunity.

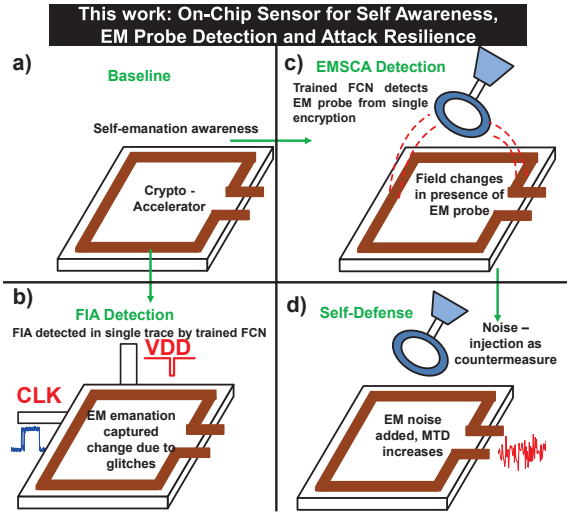


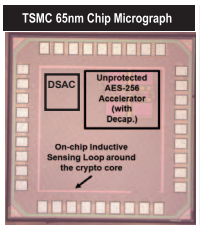
Fig. 1. On-chip multi-purpose Inductive sensor: a) induces magnetic field due to the switching activity of the circuit. b) Self-aware: Any fault injection (voltage/clock glitch) is reflected in the EM radiation picked up by the on-chip sensor, cen be detected by FCN classifier. c) EM SCA Attack Detection: An approaching EM probe would change the EM field pattern induced across the sensor and can be detected using a classifier like FCN. d) Self-defense: The multi-purpose sensor can be alternatively used as a noise injector using the top metal plate forming the loop to enhance EM SCA resilience in conjunction with any other countermeasure, once an attack is detected.

Fig. 1 provides an overview of the multi-purpose single on-chip inductive sensing loop. It senses the EM emanations due to the switching activity in the 65nm CMOS IC as shown in Fig. 1(a). Fig. 1(b) shows the on-chip loop as a fault injection attack detector. Induced voltage pattern changes in presence of glitches from the normal pattern which can be easily detected by post-processing as discussed in Sec. IV. Fig. 1(c) shows the working principle of the on-chip inductive sensor as an approaching EM probe detector by self-emanation. Fig. 1(d) shows EM noise injection utilizing the higher metal layer inductor (sensor) once an attack is detected to enhance EM side-channel immunity in conjunction to any existing countermeasures [10]. Thus, the implemented on-chip inductive sensing loop senses FIA, detects an approaching probe, and injects noise once attack is detected to thwart EM SCA.

II. Background and Related Works

Countermeasures have been proposed over the years against FIA, which mainly detect the faults and attempts to correct them [11]. Timing-failure-resilient techniques such as glitch detector [5], tunable replicas [12] have been used as counter-

978-3-9819263-6-1/DATE22/©2022 EDAA



Test Chip	Process	65nm CMOS LP
	Package	Wire-bond (Glob-Top Encapsulation)
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
On-chip sensor	Area	0.025 mm^2
	Metal layer	M9
	Effective area-overhead	0%*
*M9 not used in design		

Fig. 2. 65nm CMOS IC with an AES-256 accelerator and the integrated on-chip sensor. Table on the right summarizes the chip details.

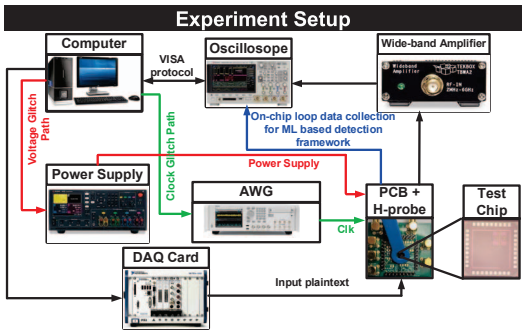


Fig. 3. Experiment setup.

measures. Recently fast digital clock modulation circuit has been implemented and demonstrated as a countermeasure [13].

EM SCA attack is another growing threat on ICs due to its non-invasiveness and increasing availability of cheap equipment [1]. Many countermeasures [14], [8], [9] have been proposed and proven to be secure against EM SCA. Standard EM SCA attack sensors use an on-chip coil-based LC oscillator [7] or capacitive sensing-based framework [15], [16].

Injecting noise [17] is one of the most popular technique for countermeasure of power side channel attack. Note that, not many studies have been performed on EM-based noise injection. This work presents EM noise injection as a countermeasure which can be easily embedded with existing countermeasures for further SCA immunity.

This work, thus, proposes the design of a single on-chip loop for inductive sensing of the EM radiation to provide FIA detection and detection of an incoming EM probe characterizing time-domain induced voltage traces using a lightweight fully connected neural network (FCN) classifier, and enhancing the EM SCA resilience through noise injection using the metal plates of the EM sensor once an approaching probe is detected. This is the first integrated sensor design to provide protection against both FIA & EM SCA.

III. Experiment Setup with 65nm Custom-built IC

Custom-built IC with On-Chip Loop: A 65nm CMOS test-chip is fabricated with a parallel AES-256 implementation, a state-of-the-art countermeasure named as Digital Signature Attenuation Circuit (DSAC) [10] and an on-chip loop. The die micrograph and specification details are shown in Fig. 2. AES encryption engine is operated at 10MHz frequency and 0.8V. It consumes 189uW power in the specified conditions

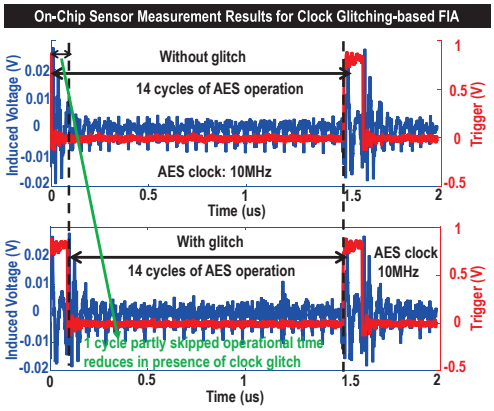


Fig. 4. Time-domain measurements of the on-chip sensor shows that time duration of traces have been reduced in presence of a clock glitch which can be detected by proposed FCN classifier.

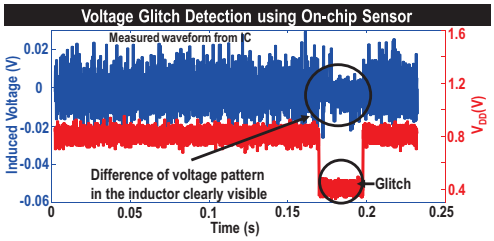


Fig. 5. Time-domain measurements of voltage glitch picked by on-chip sensor.

and occupies $0.15mm^2$ area. It should be noted that all the results presented here are directly measured from the chip and fed to the ML classifier for attack detection.

FIA Setup: Experiment setup is presented in Fig. 3. The 65nm CMOS test chip integrated in the PCB is powered up using a controlled power supply (red) and the clock is provided through an AWG (green). Both the power supply and AWG are controlled by the PC to mount FIA. A clock glitch of 10ns is introduced which is 10× shorter than the time-period of AES, and a voltage glitch of 0.4V is injected for voltage glitch based attack.

ML-based Attack Detection: Collected traces from the on-chip loop located in the IC are captured by an 400 MSps, 10-bit oscilloscope and fed to a lightweight ML classifier running on a PC (discussed in following sections). After training, classifier uses the trained model to detect the attacks directly using time-domain signatures. This ML classifier alleviates the requirement of spectrum analyzer for frequency domain post-processing circuits [7] for FIA/EM SCA detection.

EM SCA setup: A 10-mm H-probe is used for collecting traces for Correlational EM Attack (CEMA). Collected traces are amplified by a wide-band amplifier before feeding into a 10-bit, 400MSps oscilloscope as presented in Fig. 3. A DAQ card is used for the interfacing of the chip. DAQ card sends the input plaintexts using scan-chain interface of the IC. Power supply is used for noise injection through the on-chip loop.

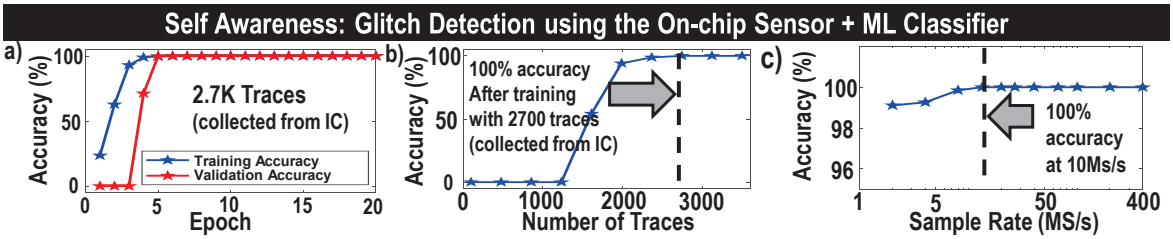


Fig. 6. Self-Awareness: a) Accuracy with Epoch: Both training and validation accuracy reaches $\sim 100\%$ after being trained with 2.7K traces. b) Test accuracy with no. of Training Traces: Single-trace glitch detection is possible after training with as low as 2.7K traces using proposed light-weight FCN. c) Test accuracy with sample rate: $\sim 100\%$ test accuracy in FIA detection is observed even with 10 MSps sampling rate.

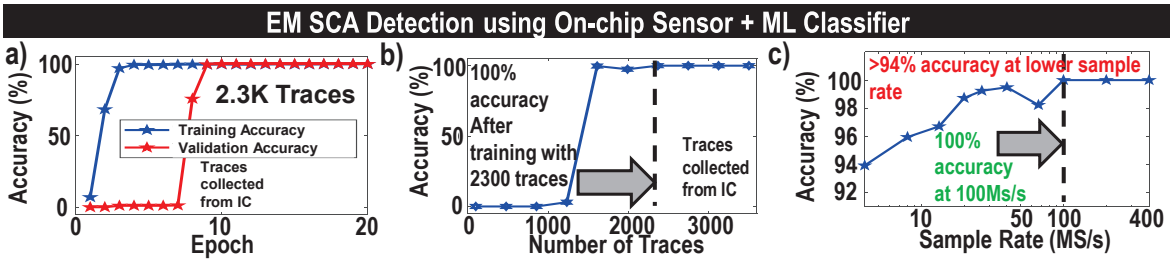


Fig. 7. a) Training accuracy and validation accuracy after training with 2.3K traces. b) Test accuracy reaches $\sim 100\%$ after training with 2.3K traces. c) Higher accuracy is achieved even with lower sample rate. Test accuracy reaches $\sim 100\%$ at a sampling rate of 100 MSps.

IV. Self-awareness: FIA Detection

All the modern processors today are implemented using CMOS technology. Due to the state changes, interrupt routine generation or through other circuit activities, charges accumulate, leading to the dynamic current. Moving charges create electric field and changes in the electric field produces magnetic field, leading to the EM radiation, which is then sensed by the higher metal layer on-chip loop. This induced magnetic field in terms of current can be captured and utilized for post-processing.

Fig. 4 shows the changes in the induced voltage measured across the on-chip sensor coil with the clock glitching-based FIA. It is clearly seen that almost one cycle of the crypto operation is reduced due to the glitch which changes the duration of entire parallel hardware-AES-256 operation and hence produces erroneous outputs. The trigger signal shows the end of an encryption. Hence, the time between two consecutive triggers clearly reveals the presence of a clock glitch from the traces collected from the on-chip sensor. Similarly, the efficacy of the sensor is verified against a voltage glitch FIA. Induced voltage in the on-chip loop deviates from normal voltage pattern whenever glitch is introduced as shown in Fig. 5. FCN with 3 hidden layers each with 32 neurons and a learning rate of 0.00001 can easily detect the pattern after training with 2.7K traces and achieves $\sim$100% training and validation accuracy (Fig. 6(a)) in collected trace. The trained neural network is then able to detect clock glitch based FIA with a single encryption trace with $\sim$100% accuracy as shown in Fig. 6(b). Fig. 6(c) shows that our technique performs well even at lower sampling rates and can detect FIA with $\sim 100\%$ accuracy at sampling rates as low as 10 MSps.

V. EM SCA Attack Detection

EM SCA is only possible by distorting the EM field itself as an EM probe approaches on top of the chip [18]. This distortion can be detected using our on-chip EM sensor and can be used for attack detection and defense.

The induced voltage traces were collected from the chip in 3 different ways - without any EM probe, with an approaching 10mm H-probe, and with the probe on top, using the same set-up as discussed in Sec. III. It should be noted that the position of the probe is critical as Danial et al. [19] showed improved EM SCA with automatic scanning the chip (movement of probe on top) to obtain an optimum point for the attack.

FCN with 3 hidden layers with 32 neurons each and learning rate of 0.00001 can correctly predict the output with just a single trace with an accuracy of $\sim 100\%$ (Fig. 7(a, b)) after being trained with 2300 traces. Further, the efficacy of the attack detection scheme is investigated with lower sampling rate of the ADC. Proposed system can detect an EM probe very accurately ($\sim 96\%$ test accuracy) even with lower sampling rate of 10MSps as shown in Fig. 7(c), while it achieves $\sim 100\%$ accuracy with 100MSps sampling rate.

VI. Self-Defense: Attack resilience through on-chip coil

Noise injection is one of solutions to protect against power and EM side channel attacks [20]. Minimum-traces to disclosure (MTD) depends on signal to noise ratio (SNR) of the leakage signal as, $MTD \propto \frac{1}{SNR^2}$ [20]. EM noise is injected using an off-chip loop removing the requirement of off-chip noise injection circuit [21]. Time domain waveform for unprotected AES256, protected AES with countermeasure (DSAC), protected AES with DSAC and noise injection are presented in the Fig. 8. 14 cycles of the unprotected AES operation

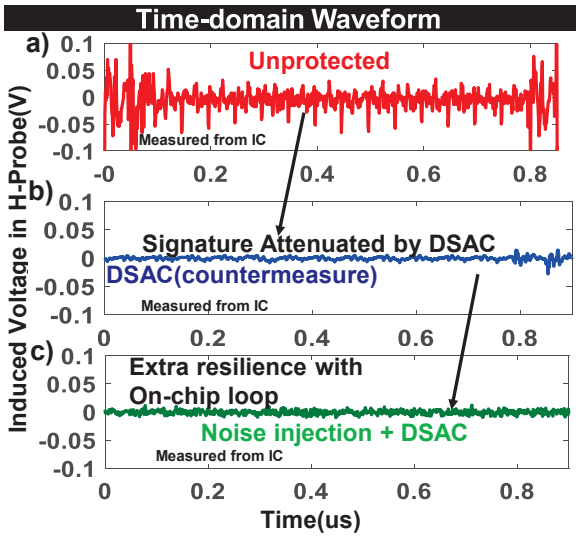


Fig. 8. Time-domain waveform for: a) unprotected AES b) attenuated signature using DSAC [10] c) Noise injection after attenuation.

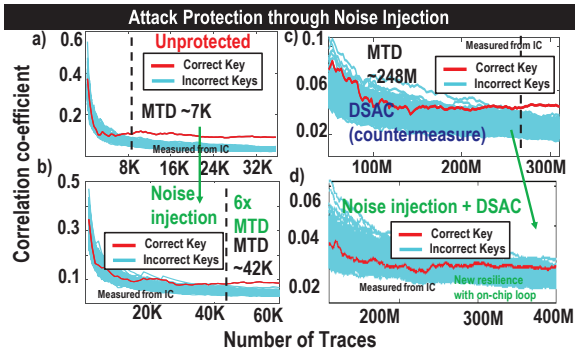


Fig. 9. Self-defense: CEMA for a) Unprotected AES-256, b) Unprotected AES-256 with noise injection, c) In presence of DSAC countermeasure [10], d) Noise injection + DSAC.

are visible as shown in Fig. 8(a). However, attenuation is clearly observed in case of DSAC (Fig. 8(b)). Distortion in the waveform in presence of noise injection is shown in Fig. 8(c). Correct key for the unprotected AES is revealed within 7K traces (Fig. 9(a)). A similar design of [10] (DSAC) is used as countermeasure which helps in achieving 248M MTD against CEMA (Fig. 9(c)). As shown in Fig. 9(d), noise injection after attenuation using DSAC shows high resilience as the correct key is not revealed even after 400M traces. To ascertain the efficacy of noise injection, the countermeasure is disabled and the correct key comes out after 42K traces (increased by $\sim 6\times$) as seen from Fig. 9(b).

VII. Conclusion

This work, for the first time, utilizes an on-chip inductive loop for multi-modal security enhancement. On-chip loop proactively detects both FIA (clock/voltage glitch) as well as EM SCA on an AES-256 crypto engine fabricated in TSMC 65nm process based on deviation from normal EM emanations. Once an EM SCA attack is detected, the on-chip sensor is then utilized to inject noise in the system through the top metal coil to decorrelate the EM fields thereby enhancing the EM SCA security in conjunction with DSAC. The proposed sensor thus combines both FIA and EM SCA attack detection as it senses any change in the induced magnetic field across the on-chip coil, which is then passed through a trained classifier (FCN, in this work) to detect these attacks with a very high accuracy of $\sim 94-100\%$ (based on sampling rate), showing the feasibility of a single-trace attack detection.

References

[1] D. Agrawal et al. The EM Side-Channel(s). In *CHES 2002*.
[2] Fox-IT. TEMPEST attacks against AES. Technical report.
[3] J Danial et. al. EM-X-DL: Efficient cross-device deep learning side-channel attack with noisy em signatures. *J. Emerg. Technol. Comput. Syst.*, 18(1), sep 2021.
[4] Michael Tunstall et al. Differential fault analysis of the advanced encryption using a single fault. In *International workshop on information security theory and practices*, 2011.
[5] L. Zussa et al. Efficiency of a glitch detector against electromagnetic fault injection. In *IEEE DATE*, 2014.
[6] K. Mustafa et. al. Dfarpa: Differential fault attack resistant physical design automation. In *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 1171–1174, 2018.
[7] N. Miura et al. A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor. In *VLSI*, 2014.
[8] D. Das et al. EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350x Current-Domain Signature Attenuation. In *IEEE ISSCC*, 2020.
[9] A. Ghosh et. al. Syn-stellar: An em/power sca-resilient aes-256 with synthesis-friendly signature attenuation. *IEEE Journal of Solid-State Circuits*, pages 1–1, 2021.
[10] A. Ghosh et. al. 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. In *2021 ISSCC*, volume 64, pages 499–501, 2021.
[11] C. Yen et al. Simple error detection methods for hardware implementation of advanced encryption standard. *IEEE T. Computers*, 2006.
[12] K. Gomina et al. Power supply glitch attacks: Design and evaluation of detection circuits. In *IEEE HOST*, 2014.
[13] A. Singh et al. Mitigating power supply glitch based fault attacks with fast all-digital clock modulation circuit. In *IEEE DATE 2019*, pages 19–24.
[14] D. D. Hwang et al. AES-Based Security Coprocessor IC in 0.18um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks. *IEEE JSSC*, pages 781–792, April 2006.
[15] D.H. Seo et. al. Enhanced detection range for em side-channel attack probes utilizing co-planar capacitive asymmetry sensing. In *2021 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 1016–1019, 2021.
[16] D.H. Seo et. al. PG-CAS: Patterned-ground co-planar capacitive asymmetry sensing for mm-range em side-channel attack probe detection. In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5, 2021.
[17] D. Das et al. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In *HOST*, 2019.
[18] N. Miura et al. Em attack sensor: concept, circuit, and design-automation methodology. In *DAC*. IEEE, 2015.
[19] J. Danial et al. SCNIFFER: Low-cost, automated, efficient electromagnetic side-channel sniffing. *IEEE Access*, 2020.
[20] D. Das et. al. ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity. *IEEE TCAS-I*, 2018.
[21] M. Kar et. al. Blindsight: Blinding em side-channel leakage using built-in fully integrated inductive voltage regulator. *arXiv:1802.09096*, 2018.