2021 IEEE International Symposium on Circuits and Systems (ISCAS) | 978-1-7281-9201-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ISCAS51556.2021.9401580

PG-CAS: Patterned-Ground Co-planar Capacitive Asymmetry Sensing for mm-range EM Side-channel Attack Probe Detection

Dong-Hyun Seo*, Mayukh Nath*, Debayan Das*, *Student Member, IEEE,*
Baibhab Chatterjee*, *Student Member, IEEE,* Santosh Ghosh† and Shreyas Sen*, *Senior Member, IEEE*
*School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA
†Intel Labs, Intel Corporation, Hillsboro, OR. USA

***Abstract*—Electromagnetic (EM) side-channel analysis (SCA) attack, which breaks cryptographic implementations, has become a major concern in the design of circuits and systems. This paper presents the design and analysis of the EM side-channel attack detection system utilizing patterned-ground co-planar capacitive asymmetry sensing (PG-CAS) for approaching probe, targeting to improve sensitivity, detection range, and power consumption compared to LC oscillator utilizing inductive sensing. The PG-CAS consists of a grid of four metal plates of the same size at the top metal layer and a patterned ground plane at a lower metal. As an EM probe approaches, electric field lines between the plates and plate-ground get distorted, thereby breaking the symmetry of the inter-plate and the plate-ground capacitance system and this change in capacitance is sensed. The PG-CAS circuit consists of two LC oscillators, mixer, low pass filter (LPF), resistive feedback amplifier (RFA) and a digital logic. By down-converting sensing signal to low-frequency using mixer, LPF, RFA and digital logic, the detection range is significantly improved. At a distance of 1 mm between the sensing metal plates and the approaching EM probe, system-level simulation results using TSMC 65nm technology and Ansys Maxwell show a $>10\%$ change in the output frequency from the baseline frequency, leading to a $>10\times$ improvement in the detection range and a $\sim 3\times$ improvement in power consumption over existing inductive sensing methods.**

***Index Terms*—Side-channel attack, electromagnetic leakage, co-planar capacitor, patterned-ground, capacitive asymmetry, inductive sensing, micro EM probe.**

I. Introduction

As the use of the internet, artificial intelligence, IoT, and wearable devices have increased, the need to ensure security and confidentiality of information, especially at these resource-constrained edge devices, have led to the development of computationally-secure cryptographic algorithms. However, side-channel analysis (SCA) based attacks can still be implemented on a mathematically-secure physical platform which leak critical information through power dissipation [1], electromagnetic (EM) radiation [2], [3], timing of the encryption operations [4], cache hits/misses, and so forth, allowing an attacker to extract the secret key from the device as described in Fig. 1(a). In order to protect against EM SCA attacks, various countermeasures have been proposed such as logical [5], architectural [6], and physical (circuit-level) [7], [8], [9], [10], [11], [12], [13], [14] as shown in Fig. 1(b). However, these countermeasures require significant overheads in terms of power and area.

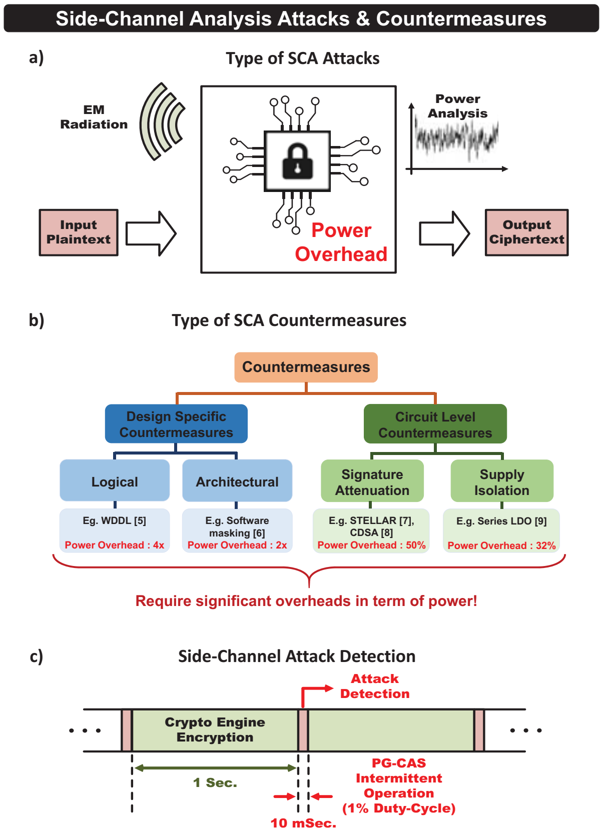


Fig. 1. Side-channel analysis attacks (SCA) and countermeasures (a) Types of SCA attacks, (b) types of SCA attacks countermeasures and (c) operation of intermittent side-channel attack detection with 1% duty cycle.

This work, on the other hand, adopts a pro-active strategy to detect the presence of an EM side-channel attacker even before an attack is carried out, thereby alleviating the overheads incurred by a countermeasure against such attacks. Also, this strategy of EM side-channel attack detection can be augmented with an existing countermeasure such that the protection circuitry is only enabled when an attack is detected, which would also significantly minimize the power overheads compared to the always-on countermeasure. The goal of this

This work was supported in part by the National Science Foundation (NSF) under Grants CNS 17-19235, CNS 19-35573, and in part by Intel Corporation.

978-1-7281-9201-7/21/$31.00 ©2021 IEEE

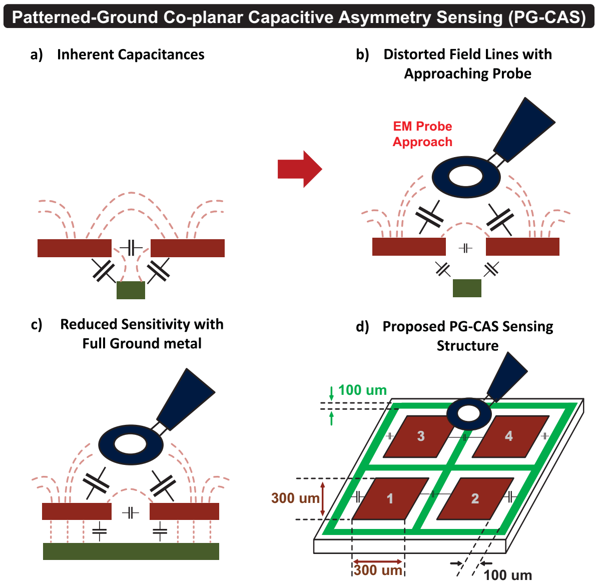

Patterned-Ground Co-planar Capacitive Asymmetry Sensing (PG-CAS)
a) Inherent Capacitances
b) Distorted Field Lines with Approaching Probe
EM Probe Approach
c) Reduced Sensitivity with Full Ground metal
d) Proposed PG-CAS Sensing Structure
100 um
300 um
3
4
1
2
300 um
100 um

Fig. 2. Proposed patterned-ground co-planar capacitive asymmetry sensing (PG-CAS) (a) Inherent capacitance of inter plates and plate-ground, (b) distorted field lines with approaching probe, (c) reduced sensitivity with full ground metal and (d) proposed PG-CAS structure.

work is to enhance the detection range of an approaching EM probe by adopting patterned-ground co-planar capacitive asymmetry sensing (PG-CAS), followed by down-conversion of the sensed signal for low-power processing. The proposed technique achieves $> 10\times$ better maximum detection distance compared to the existing inductive sensing [15], [16] with $> 2\times$ reduced power consumption by operating the PG-CAS circuit intermittently at $< 1\%$ duty-cycle as shown in Fig. 1(c).

Specific contributions of this paper are:

- The proposed co-planar capacitive sensing technique senses the inter-plate capacitance. As the EM probe approaches, electric field lines between the plates are distorted and the change in capacitance can be sensed to detect an EM SCA attack.
- The proposed patterned-ground improves the sensitivity by minimizing the capacitance between the plate and ground, leading to a higher relative change in effective capacitance (inter-plate + plate-ground).
- As the EM probe approaches, the symmetry of the inter-plate and plate-ground capacitance system breaks and the change in capacitance can be sensed to detect an EM SCA attack. The proposed PG-CAS structure shows $> 40\%$ change in capacitance breaking the symmetry of the structure and thereby achieving $> 8\times$ improvement in sensitivity at a distance of 0.1mm compared to the existing inductive sensing (prior work).
- The designed PG-CAS system amplifies the percentage change in frequency between the two LC oscillators by down-converting the sensing signal to a lower-frequency. This allows $> 10\times$ improvement in maximum detection range, allowing detection of an approaching EM probe at a distance of 1 mm with $> 2\times$ improved power compared to the inductive sensing (prior work).

II. Patterned-Ground Co-planar Capacitive Asymmetry Sensing (PG-CAS) of EM SCA Attack

The detection of the approaching probe is based on the fundamental principle that an EM probe forms an electrical coupling with the measured object (co-planar metal plates and patterned ground structure in this case) when they are close to each other. Plate-to-plate and plate-to-ground capacitances will depend on the presence of objects between the plates and the surrounding environment, as the electric field lines between the plates would get coupled to any nearby objects. As shown in Fig. 2(a), co-planar plates and patterned-ground that are not affected by the surrounding environment form their own capacitances. If an EM probe approaches a pair of metal plates, some of the electric field lines between the plates and ground will get coupled to the probes and thereby affecting the inter-plate capacitance and hence the peak resonant frequency of the corresponding LC oscillator system, as described in Fig. 2(b).

A. *Co-planar Capacitor*

The co-planar capacitor design uses only the top metal layer to create multiple large-area plates. While a co-planar capacitor has a lower absolute capacitance compared to an equally-sized parallel-plate capacitor, the idea is not to measure absolute capacitance - rather the relative change in capacitance - where the amount of deviation in capacitance relative to its absolute value or another capacitance pair is much more meaningful. Using a co-planar capacitance ensures that a larger portion of the electric field lines between the plates traverse through the surrounding environment (a parallel plate configuration would avoid that) and can be easily intercepted by an approaching EM probe.

B. *Patterned-ground*

In CMOS integrated circuit (IC) technology, the ground-grid always exists and any metal plate and the ground-grid would form a capacitance. If the ground metal covers the whole metal plate area, strong electric field lines are formed as described in Fig. 2(c). Since these field lines are not affected as much by an approaching probe in the surrounding environment, it would lead to a degradation in sensitivity. To circumvent this issue and to improve the sensitivity of the PG-CAS circuit, a patterned-ground approach is proposed as shown in Fig. 2(d). The ground patterning is formed by using the metal layer immediately below the top metal which are used as the co-planar capacitive plates. This ground patterning improves the sensitivity by lowering the absolute capacitance between the plate and ground, while raising the relative change in plate-ground capacitance when a probe approaches - leading to a higher relative change in the net effective capacitance (inter-plate + plate-ground capacitance, referred to as C_{tank} in the next sub-section).

C. *Asymmetry Sensing*

In addition to the techniques mentioned above, detection specificity can be further improved by asymmetric sensing -

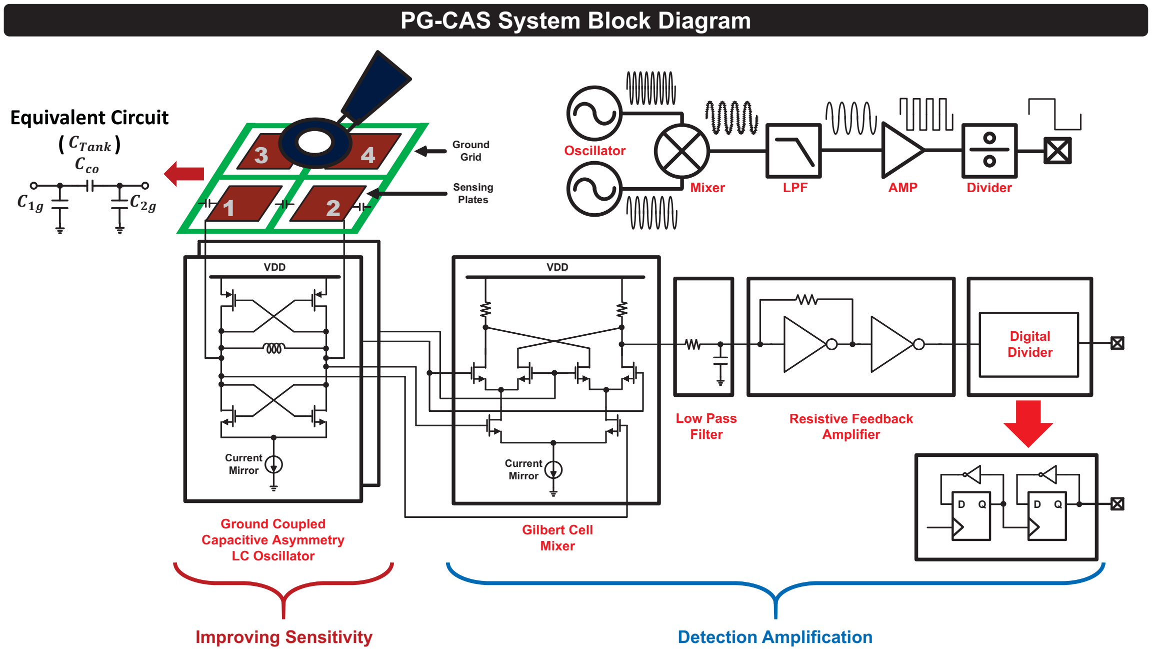


Fig. 3. PG-CAS System block diagram: Detailed circuit schematic consisting of the LC oscillator with ground coupled co-planar capacitive asymmetry sensor, mixer, LPF, resistive feedback amplifier and the digital divider.

that incorporates more than one pair of plates. As mentioned above, the capacitance between a pair of plates is affected by any objects in the surrounding environment - that object being a close-by probe, or a relatively far large object. So it is important to distinguish between different cases. When any object, such as an EM probe, is close enough to the plates so that the amount of electric field intercepted is different for different pairs of plates, the change in the effective capacitance (inter-plate + plate-ground) would diverge between the pairs. As long there are more than two plates, application-specific algorithms can be developed to work in tandem with our proposed PG-CAS system, to design intelligent attack sensing mechanisms.

D. Amplification by Down-converting

Fig. 3 describes a system diagram of PG-CAS and detailed circuit schematic for the EM SCA attack detection. It consists of two LC oscillators, mixer, low pass filter (LPF), resistive feedback amplifier (RFA) and the digital divider. Two LC oscillators are connected to the two pairs of PG-CAS plates. The resonance-peak frequency of the LC oscillator depends on the value of the effective inter-plate capacitance (C_{tank}). The C_{tank} consists of three different combinations of capacitance. The first is the capacitance formed between the plates (C_{co}) and the second and third is the capacitance formed between the plates and patterned-ground (C_{1g} and C_{2g}), respectively. The capacitance value of C_{1g} and C_{2g} are the same because the size and dimension of metal plates are equal and the patterned-ground is symmetrical, hence the C_{tank} can be expressed as given by Eq. 1,

$$C_{tank} = C_{co} + \frac{C_{1g}C_{2g}}{C_{1g} + C_{2g}} \quad (1)$$

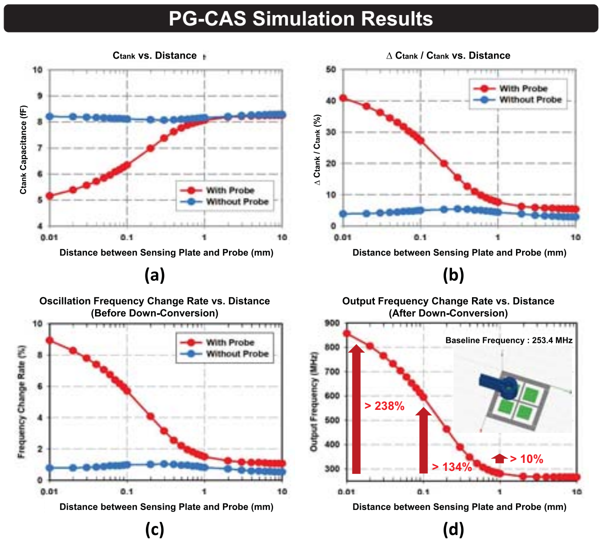
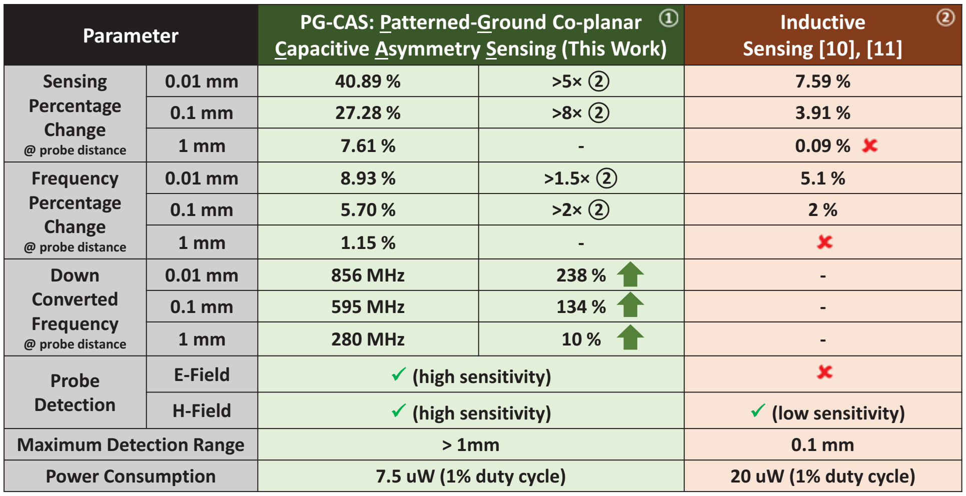


Fig. 4. Comparison of probe detection with respect to distance between sensing plates and probe (a) total capacitance change of C_{tank}, (b) total capacitance change rate of C_{tank}, (c) oscillation frequency shift change rate before down-conversion and (d) output frequency shift change rate caused by an approaching probe after down-conversion

In order to maximize the sensitivity for detection of the change in C_{tank}, the MOS width should be minimized, which allows the LC oscillators to operate at a high base-line frequency, as the absolute capacitance value formed by sensing plates and patterned-ground remains small. As an EM probe approaches one of the PG-CAS plates, the two LC oscillators produce a difference in frequency depending on the asymmetry in capacitance. To amplify the relative output frequency differences between two LC oscillators, the

TABLE I

Simulated performance summary of the comparison table



Parameter		PG-CAS: Patterned-Ground Co-planar Capacitive Asymmetry Sensing (This Work) ①		Inductive Sensing [10], [11] ②
Sensing Percentage Change @ probe distance	0.01 mm	40.89 %	>5× ②	7.59 %
	0.1 mm	27.28 %	>8× ②	3.91 %
	1 mm	7.61 %	-	0.09 % ✘
Frequency Percentage Change @ probe distance	0.01 mm	8.93 %	>1.5× ②	5.1 %
	0.1 mm	5.70 %	>2× ②	2 %
	1 mm	1.15 %	-	✘
Down Converted Frequency @ probe distance	0.01 mm	856 MHz	238 % ⬆	-
	0.1 mm	595 MHz	134 % ⬆	-
	1 mm	280 MHz	10 % ⬆	-
Probe Detection	E-Field	✓ (high sensitivity)		✘
	H-Field	✓ (high sensitivity)		✓ (low sensitivity)
Maximum Detection Range		> 1mm		0.1 mm
Power Consumption		7.5 uW (1% duty cycle)		20 uW (1% duty cycle)

mixer performs frequency translation by multiplying the two oscillation frequencies, LPF to only pass the difference of the two frequencies, RFA to convert the sine waveform to square and finally a digital divider. By down-converting this sensing frequency, the relative change in frequency shift is magnified, leading to improved sensing and increased detection range for an approaching EM probe.

III. Simulation Results

This section presents the simulation results of the PG-CAS system. The modeling of the proposed structure along with an EM probe and circuits are shown in Fig. 3. As an example, we consider the EM probe approaching the mid-point of the plates 3 and 4 vertically. The sensing plate size and the distance of each plate are 300 um and 100 um, respectively. The distance between the sensing plates and the patterned-ground is 100 um. Fig. 4 shows the comparison for sensitivity and maximum detection range of PG-CAS. Fig. 4(a) shows the simulated capacitance values of PG-CAS as the EM probe approaches the sensing plates. In the absence of the EM probe, the effective inter-plate capacitance (C_{tank}) is measured to be 8.54 fF. When the EM probe approaches, C_{tank} reduces due to the coupling effect of the EM probe. As the distance between the sensing plates and the EM probe becomes <0.01 mm, a C_{tank} change of >40% is observed, while at a distance of 1 mm or lesser, the capacitance diverges by >7% compared to the baseline as shown in Fig. 4(b). Fig. 4(c) shows the simulated oscillation frequency change rate before down-conversion. As the distance between the sensing plates and the EM probe becomes <0.01 mm, an oscillation frequency change of >8% is observed. Fig. 4(d) shows the simulated output frequency of the system (after down-conversion). In absence of the EM probe, the output frequency is 253.4 MHz. As the distance between the sensing plates and the EM probe becomes <0.01 mm, the output frequency change of >238% is observed, while at a distance of 1 mm or lesser, the output frequency changes by >10% compared to the baseline frequency.

These results demonstrate a $> 8\times$ improvement in sensitivity at a distance of 0.1mm with the proposed PG-CAS sensing technique. The designed PG-CAS system shows $> 10\times$ improved maximum detection distance and $> 2\times$ improved power consumption compared to the existing inductive sensing by down-converting.

IV. Conclusion

This paper presents the design and analysis of EM SCA attack detection system utilizing PG-CAS sensing structure and circuit to detect variations in the EM field caused by an approaching EM probe. PG-CAS system consists of a grid of four metal plates (2 pairs) of the same size and dimension at the top metal layer and patterned-ground at the lower metal layer. As the relative value of the effective inter-plate capacitance of the 2 pairs changes, the asymmetry of the two pairs create a difference in frequency with the LC oscillators, which is then down-converted to a low-frequency using mixer, LPF, RFA and a digital divider, improving the sensitivity and the detection range of an approaching EM probe significantly.

System-level simulation results demonstrate that the PG-CAS technique can be successfully utilized to sense approaching EM probes for a probe-chip distance of <0.01 mm, with $> 40\%$ deviation from the baseline C_{tank} capacitance. By down-converting the sensing frequency, the output frequency shows $> 238\%$ deviation from baseline. PG-CAS provides a $10\times$ improvement for a detection range of 0.1 mm, compared to the prior work on inductive sensing as shown in Table I. This intermittent PG-CAS circuit operation consumes 7.5uW of power, which is much lower ($\sim 3\times$) compared to the prior work (Table I). In addition, PG-CAS is sensitive to both E-field and H-field probes, unlike inductive sensing which cannot detect an E-field probe (as it does not have a loop and fields do not interact). Hence, using the proposed PG-CAS system intermittently, an EM side-channel attack can be pro-actively detected and consequently any countermeasure can be turned on, reducing the power overheads significantly.

REFERENCES

[1] P. Kocher et al. Differential Power Analysis. In *CRYPTO*, 1999.

[2] D. Agrawal et al. The EM Side-Channel(s). In *CHES*, August 2002.

[3] J. Quisquater et al. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. In *Smart Card Programming and Security*, pages 200–210. 2001.

[4] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *CRYPTO*, August 1996.

[5] 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*, 41(4):781–792, April 2006.

[6] A. Poschmann et al. Side-Channel Resistant Crypto for Less than 2,300 GE. *Journal of Cryptology*, 24(2):322–345, April 2011.

[7] D. Das et al. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In *IEEE HOST*, 2019.

[8] D. Das et al. 27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through $>$350x Current-Domain Signature Attenuation. In *IEEE ISSCC*, 2020.

[9] A. Singh et al. Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO. *IEEE JSSC*, 55(2):478–493, February 2020.

[10] D. Das et al. ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity. *IEEE TCAS-I*, 2018.

[11] D. Das et al. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In *IEEE HOST*, 2017.

[12] D. Das et al. EM and Power SCA-resilient AES-256 through $>$350x Current Domain Signature Attenuation & Local Lower Metal Routing. *IEEE JSSC*, 2020.

[13] D. Das et al. Killing EM Side-Channel Leakage at its Source. In *IEEE MWSCAS*, 2020.

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

[15] N. Miura et al. A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor. In *VLSI*, 2014.

[16] N. Homma et al. EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor. In *CHES*, 2014.