Enhanced Detection Range for EM Side-channel Attack Probes utilizing Co-planar Capacitive Asymmetry Sensing

Dong-Hyun Seo*, Mayukh Nath*, Debayan Das*, *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 focuses on EM SCA and proposes the detection of an approaching EM probe even before an attack is performed. The proposed method of *co-planar capacitive asymmetry* sensing consists of a grid of four metal plates of the same size and dimension. As an EM probe approaches the sensing metal plates, the symmetry of the sensing metal plate system breaks, and the capacitance between each pair diverge from their baseline capacitances. Using Ansys Maxwell Finite Element Method (FEM) simulations, we demonstrate that the co-planar capacitive asymmetry sensing has an enhanced detection range compared to other sensing methods. At a distance of 1 mm between the sensing metal plates and the approaching EM probe, it shows >17% change in capacitance, leading to a $> 10\times$ improvement in detection range over the existing inductive sensing methods. At a distance of 0.1 mm, a $>$ 45% change in capacitance is observed, leading to a $> 3\times$ and $> 11\times$ sensitivity improvement over capacitive parallel sensing and inductive sensing respectively. Finally, we show that the co-planar capacitive asymmetry sensing is sensitive to both E-field and H-field probes, unlike inductive sensing which cannot detect an E-field probe.**

***Index Terms*—Side-channel attack, co-planar capacitive asymmetry sensing, inductive sensing.**

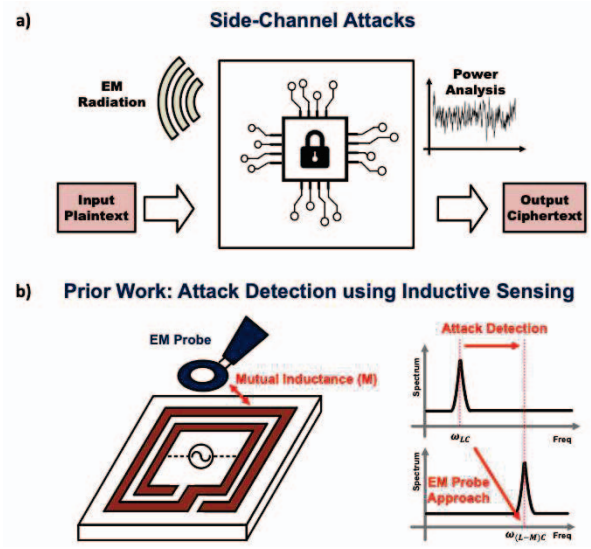

Fig. 1. Side-channel attacks and detection (a) Types of side-channel attacks and (b) previous work of attack detection using inductive sensing [5], [6]

I. Introduction

THE increasing growth of internet-connected devices has led to the development of computationally-secure cryptographic algorithms. Although these algorithms provide mathematical security, they are implemented on a 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 shown in Fig. 1(a).

A. Motivation & Related Works

In this work, we focus on the EM SCA and the propose detection of an approaching EM probe even before an attack is performed. Many countermeasures involving logical [7], architectural [8], and physical (circuit-level) [9], [10], [11], [12], [13], [14], [15], [16] have been proposed to provide immunity against these EM SCA attacks. However, these countermeasures incur significant area, power overheads as well as performance degradation, and may not be generic in nature. 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 mounted, thereby alleviating the overheads incurred by a countermeasure against such attacks.

Prior works in EM SCA attack detection have been reported in [5], [6]. Fig. 1(b) describes the previous work on the attack detection technique, which employs a inductive sensor coil-based LC oscillator. It detects variations in the EM field caused by an approaching EM probe. When an EM probe approaches the inductive sensor, the mutual inductance (M) between the EM probe and the integrated sensor coil increases. As current flows through the inductive sensor coil, the oscillation frequency of LC oscillator shifts due to the changing mutual inductance, as given by Eq. 1,

$$f_{LC\_shift} = \frac{1}{2\pi\sqrt{(L-M)C}} \quad (1)$$

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.

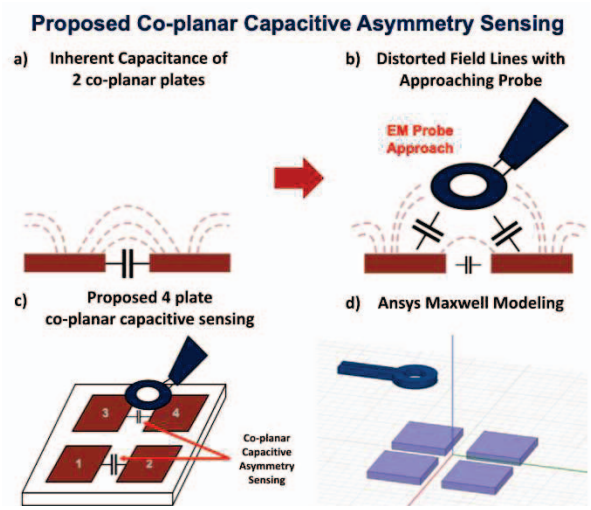

Fig. 2. (a) Inherent capacitance of 2 co-planar plates, (b) distorted field lines with approaching probe, (c) proposed 4-plate co-planar capacitive asymmetry sensing and (d) Ansys Maxwell simulation modeling

When an EM probe approaches, mutual inductance changes, and consequently the oscillation frequency of the LC oscillator shifts. Thus, it is possible to detect the presence of an EM probe by detecting the frequency shifts using an LC oscillator. However, the effective detection range between the EM probe and the chip is limited to a maximum of 0.1 mm.

This work aims to enhance the detection range of an approaching EM probe by adopting a co-planar capacitive asymmetry sensing technique. Using Ansys Maxwell simulations with approaching EM probes, the proposed technique achieves $> 11\times$ improved sensitivity, and thus longer detection range compared to the existing inductive sensing.

B. Contribution

Specific contributions of this paper are:

- The proposed co-planar capacitive sensing technique utilizing four metal plates senses the inter-plate capacitance. As an EM probe approaches, the symmetry of the four-plate system breaks and the change in capacitance can be sensed to detect an EM SCA attack.
- Using Ansys Maxwell simulations, we see that the proposed technique detects both electric (E) and magnetic (H) field probes with high sensitivity, unlike the inductive sensing.
- A design-space exploration of the proposed co-planar capacitive asymmetry sensing reveals that smaller metal plate size provides higher sensitivity, while a higher inter-plate distance up to a certain limit increases the sensitivity of detection of an approaching EM probe.
- Finally, the designed four-plate co-planar capacitive sensing system shows $> 45\%$ change in the inter-plate capacitance breaking the symmetry of the structure. A thorough comparison with an alternative parallel-plate capacitive sensing technique and the inductive sensing (prior work) reveals that our proposed co-planar capacitive sensing achieves $> 3\times$ and $> 11\times$ improvement in sensitivity respectively, and can detect an approaching EM probe at a distance of 1 mm.

II. Co-planar Capacitive Asymmetry Sensing of EM Side-channel Attack

A. Operating Principle

The capacitance between any two plates will depend on the presence of objects between the plates and the surrounding environment, as the Electric Field lines between the two plates would get coupled to any nearby objects. As shown in Fig. 2(a), 2 co-planar plates that are not affected by the surrounding environment form their own capacitance. If a detection probe is to approach a pair of plates, some of the electric field lines between the plates will get coupled to the probes and thereby affect the capacitance as described in Fig 2(b). As shown in Fig. 2(c), the proposed structure consists of four aligned metal plates of the same size and dimension. The capacitance values generated by the electric field are the same due to the symmetrical structure. However, as an EM probe approaches the four aligned metal plates, the symmetry of the system breaks because of coupling capacitance from EM probe. This results in the change of the capacitance between the pairs, as it diverges from the baseline capacitance, which can be detected.

B. Parallel Plate vs Co-planar Capacitors

The traditional way to incorporate capacitors near the top-level metal layers of a chip is to stack large area metal plates vertically, incorporating multiple metal layers - making it a standard parallel plate capacitor. In this paper however, we have taken a very different approach, where we use only the top metal layer to create multiple large area plates, making them co-planar capacitors. Now while a co-planar capacitor has a lower absolute capacitance with respect to a similarly sized parallel plate capacitor, the idea is not to measure absolute, but relative capacitance - where the amount of deviation in capacitance relative to the absolute value or another capacitance pair is much more meaningful.

C. Significance of Asymmetry

Asymmetric sensing, as we have briefly introduced, incorporates more than one pair of capacitance plates. The capacitance between a pair of plates is affected by any objects in the surrounding environment. When a small object - such as a probe - gets close enough to the plates so that the amount of electric field intercepted by that object is different for different pairs of plates, the capacitance changes would diverge. It is this divergence in capacitance, that is key to successfully detecting an approaching probe in asymmetric co-planar capacitive sensing.

III. Simulation Results

This section presents simulation results of the proposed co-planar capacitive asymmetry system using Ansys Maxwell. The modeling of the proposed structure along with an EM probe in Ansys Maxwell is shown in Fig. 2(d). The simulation

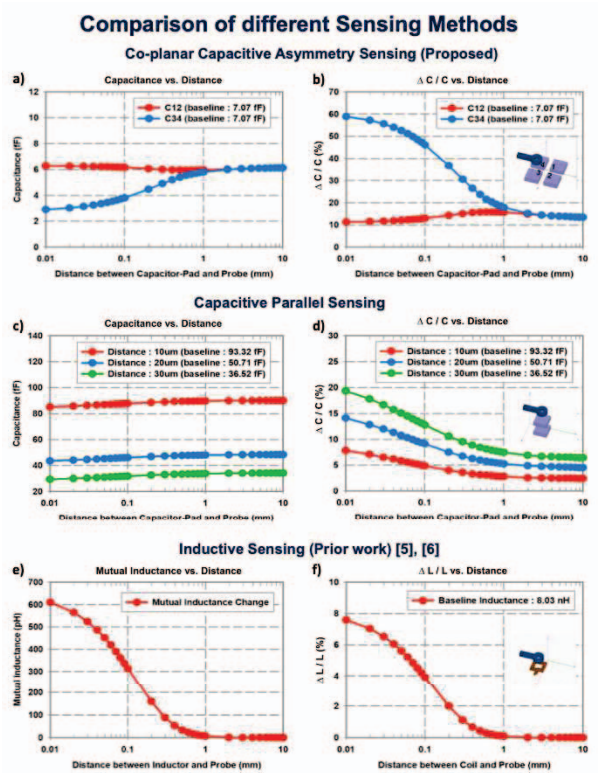

Fig. 3. Comparison of capacitive sensing and inductive sensing with respect to distance between sensing plates and EM probe. (a) Capacitance change of co-planar capacitive asymmetry sensing, (b) capacitance change rate of co-planar capacitive asymmetry sensing, (c) capacitance change of capacitive parallel sensing, (d) capacitance change rate of capacitive parallel sensing, (e) mutual inductance change of inductive sensing and (f) inductance change rate of inductive sensing.

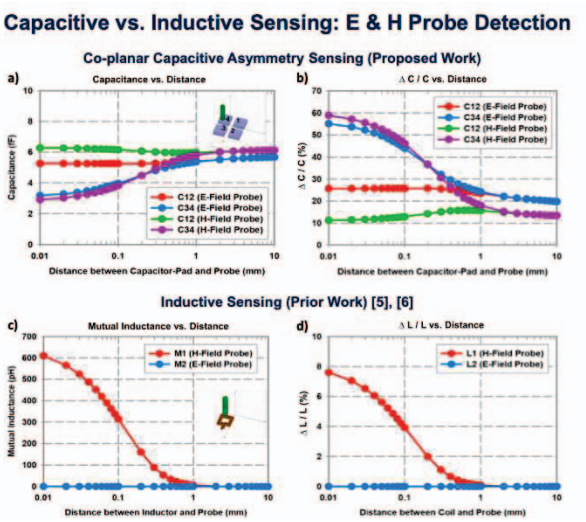

Fig. 4. Comparison of E-field and H-field probe detection with respect to distance between sensing plates and probe. (a) Capacitance change of co-planar capacitive asymmetry sensing, (b) capacitance change rate of co-planar capacitive asymmetry sensing, (c) mutual inductance change of inductive sensing and (d) inductance change rate of inductive sensing.

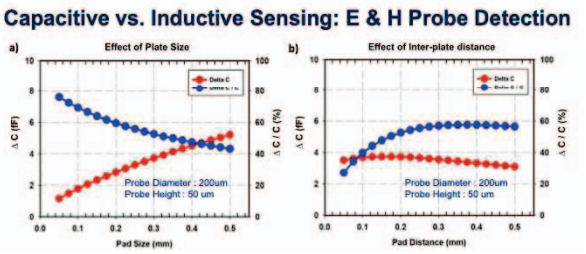

Fig. 5. Design space exploration of co-planar capacitive asymmetry sensing (a) effect of plate size and (b) effect of inter plate distance

results demonstrate the operating principle as described in the previous section and are presented as follows: 1) detailed comparative analysis of co-planar capacitive asymmetry sensing, capacitive parallel sensing, and inductive sensing; 2) comparative analysis with E-field and H-field probes; and 3) design space analysis of the co-planar capacitive asymmetry sensing structure.

A. Comparison with Other Sensing Methods

Fig. 3 shows the comparison for sensitivity and maximum detection range of co-planar capacitive asymmetry, capacitive parallel, and inductive sensing. The purpose of this simulation is to observe how the EM probe affects capacitance when it approaches the sensing plates in different configurations. First, we discuss the simulation results of co-planar capacitive asymmetry sensing. The sensing plate size and the distance between each pair of plates are 300μm and 200μm, respectively. Fig. 3(a) shows the simulated capacitance values of co-planar capacitive asymmetry sensing structure as the EM probe approaches the sensing plates. In the absence of the EM probe, C12 and C34 (baseline capacitance between the plates 1, 2 and 3, 4 respectively) is measured to be 7.07 fF. When the EM probe approaches, C34 reduces due to the coupling effect of the EM probe. As the distance between the sensing plates and the EM probe becomes $<$0.1 mm, a capacitance change of $>$45% is observed, while at a distance of 1 mm or shorter, the capacitance diverges by $>$15% compared to the baseline as shown in Fig. 3(b). Next, we demonstrate the simulation results for the case of capacitive parallel plate-based sensing. Fig. 3(c) shows the simulated capacitance values for capacitive parallel sensing when the EM probe approaches. When the distance between the sensing plate and the EM probe is $<$0.1 mm, the capacitance diverges by $\sim$12%, while for $<$1 mm, the capacitance changes by $\sim$7% as shown in Fig. 3(d). We now present the simulation results for inductive sensing. The coil has an inductance of 8.03 nH according to the EM field simulation in Maxwell. Fig. 3(e) shows the change in mutual inductance between EM probe and the coil in presence of the EM probe. When the EM probe approaches, the mutual inductance between the EM probe and the coil increases. Fig. 3(f) shows the inductance change rate when the probe approaches. When the distance between the coil and the EM probe becomes $<$0.1 mm, the inductance only changes by

TABLE I
SIMULATED PERFORMANCE SUMMARY OF THE 3 SENSING METHODS AND COMPARISON TABLE

Parameter		Capacitive Co-planar Asymmetry Sensing (This Work) ①			Capacitive Parallel Sensing ②	Inductive Sensing [5], [6] ③
Percentage Change @ probe distance	0.01 mm	58.90 %	>3× ②	>7× ③	19.37 %	7.59 %
	0.1 mm	46.11 %	>3× ②	>11× ③	12.79 %	3.91 %
	1 mm	17.95 %	>3× ②		7.46 %	0.09 % ✗
Maximum Detection Range		> 1 mm			> 1 mm	0.1 mm
Probe Detection	E-Field	✓ Highest Sensitivity			✓ Moderate Sensitivity	✗
	H-Field	✓ Highest Sensitivity			✓ Moderate Sensitivity	✓ Lowest Sensitivity

$\sim$3%, while for $<$1 mm, the inductance does not show any deviation from the baseline.

These results demonstrate that the co-planar capacitive asymmetry sensing structure achieves $>$ 3$\times$ and $>$ 11$\times$ improved sensitivity compared to the the capacitive parallel sensing and the inductive sensing techniques, respectively.

B. Detection Sensitivity and Range for Different Probe Types

Fig. 4 shows the comparison of the sensitivity and maximum detection range for the the proposed co-planar capacitive asymmetry sensing and the inductive sensing techniques for both H-& E-field probes. Fig. 4(a) shows the change in the capacitance values of co-planar capacitive asymmetry sensing as the EM probe approaches. When the E/H-field probe is close to the sensing structure, C34 is reduced in both cases, due to coupling with the EM probe. Fig. 4(b) shows the change in ΔC/C as the EM probe approaches. The magnitude of change in C34 was more than C12 in both cases. Fig. 4(c) presents the simulated mutual inductance between probe and the inductive coil in both cases. The mutual inductance changes as the H-field probe approaches, while no change in the mutual inductance is observed with the approaching E-field probe. Since the H-field probe is formed with a loop, it interacts with the magnetic field formed by the coil, unlike an E-field probe which does not have a loop. This implies that the inductive sensing is only effective for a H-probe (Fig. 4(d)).

Hence, the proposed 4-plate co-planar capacitive asymmetry structure can be used to detect both E-field and H-field probes with higher sensitivity.

C. Effect of Plate Size and Distance

Fig. 5 shows the design space exploration to analyze the size of the plates and the inter-plate distance of the co-planar capacitive asymmetry structure. Fig. 5(a) shows that the deviation in capacitance (ΔC) changes with the size of the sensing plates. As the sensing plate size is increased, the ΔC increases and the ΔC/C value reduces. This reveals that the smaller the sensing plate is, the better the performance of the capacitive asymmetry system, limited by the sensitivity of the detection circuit for ΔC. Fig. 5(b) shows that the deviation in change of capacitance (ΔC) with respect to the inter-plate distance. As the inter-plate distance increases, ΔC/C reaches a saturation point, revealing that the inter-plate distance up to the probe diameter increases the sensitivity of detection of an approaching EM probe.

IV. CONCLUSION

This paper presents the design and analysis of co-planar capacitive asymmetry sensing for efficient detection of approaching probe in EM side-channel attacks by detecting the variations in symmetry of co-planar capacitor plates. The results demonstrate that the proposed technique can be successfully utilized to sense approaching EM probes from a distance of $>$1mm, with $>$ 17% deviation from the baseline inter-plate capacitance. This provides a 10$\times$ improvement in detection range compared to inductive sensing (prior work). When the EM probe is within $\sim$0.1 mm, a deviation of $>$ 45% in the baseline capacitance is observed, leading to a $>$ 3$\times$ & $>$ 11$\times$ sensitivity improvement over capacitive parallel sensing and the inductive sensing respectively (Table I). Finally, the co-planar capacitive asymmetry sensing is sensitive to both E- & H-field probes, unlike inductive sensing.

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] N. Miura et al. A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor. In *VLSI*, 2014.
[6] N. Homma et al. EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor. In *CHES*, 2014.
[7] 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.
[8] A. Poschmann et al. Side-Channel Resistant Crypto for Less than 2,300 GE. *Journal of Cryptology*, 24(2):322–345, April 2011.
[9] D. Das et al. ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity. *IEEE TCAS-I*, 2018.
[10] D. Das et al. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In *IEEE HOST*, 2017.
[11] 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.
[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] 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.
[14] D. Das et al. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In *IEEE HOST*, 2019.
[15] D. Das et al. Killing EM Side-Channel Leakage at its Source. In *IEEE MWSCAS*, 2020.
[16] D. Das et al. Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS. In *IEEE CICC 2020*.