Improved EM Side-Channel Analysis Attack Probe Detection Range utilizing *Co-planar Capacitive Asymmetry Sensing*

Dong-Hyun Seo, Mayukh Nath, Debayan Das, *Student Member, IEEE*,
Santosh Ghosh and Shreyas Sen, *Senior Member, IEEE*

***Abstract*—While cryptographic implementations provide computational security in circuits and systems, hardware attack techniques e.g. Electromagnetic (EM) side-channel analysis (SCA) attack can still break through. The commonplace countermeasures for EM SCA attack require significant overheads in terms of power consumption. This paper explores an on-chip capacitive sensing technique for the purpose of detection of an approaching EM probe even before an attack is performed, thereby alleviating the overheads incurred by any countermeasure against such attacks. Different type of capacitive structures are considered in regards to sensitivity and area. The proposed method of *Co-planar capacitivE Asymmetry SEnsing (CEASE)* consists of a grid of four metal plates of the same size and dimensions determined through design space exploration. A comparison between capacitive and inductive sensing technique is also performed in terms of detection range through theoretical arguments and electromagnetic simulation. A >17% change in capacitance is shown at a distance of 1 mm, implying a $> 10\times$ improvement in detection range over inductive sensing methods. Further, at 0.1 mm distance, a > 45% change in capacitance is observed, leading to a $> 3\times$ and $> 11\times$ sensitivity improvement over capacitive parallel plate sensing and inductive sensing respectively.**

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

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. Motivation

In order to protect against EM SCA attacks, many countermeasures involving logical [5], architectural [6], and physical (circuit-level) [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17] have been proposed to provide immunity against these EM SCA attacks. However, these countermeasures incur significant area, power overheads (range from 32 % to 400 %) as well as performance degradation [18], and may not be generic [11], [19] in nature. This work, on the other hand, adopts a pro-active strategy to detect the presence of an EM side-channel attack even before an attack is mounted, thereby alleviating the overheads incurred by a countermeasure against such attacks. Also, this strategy of EM SCA detection can be augmented with an existing countermeasure such that the protection circuitry is only enabled when an attack is detected, which would significantly minimize the power overhead compared to the always-on countermeasure.

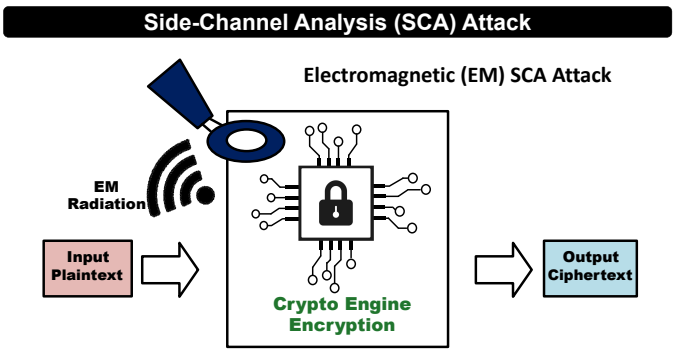

Fig. 1. Electromagnetic (EM) side-channel analysis (SCA) attack.

B. Background

The first EM SCA approaching probe detection was presented in [20], [21] and is summarized in Fig. 2, 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. An LC oscillator with this sensor coil as L, the oscillation frequency of LC oscillator shifts due to the changing mutual inductance. 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 was shown to be limited to a maximum of 0.1 mm. Often an EM SCA attacks can be successfully carried from 0.1 - 1 mm probe distance. Hence increasing the probe detection range is an open research problem.

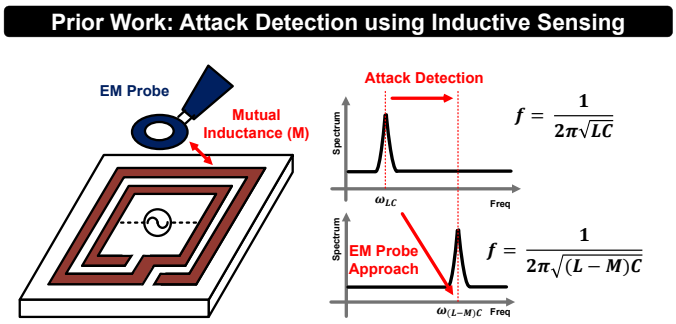

Fig. 2. Previous work of attack detection using inductive sensing [20], [21].

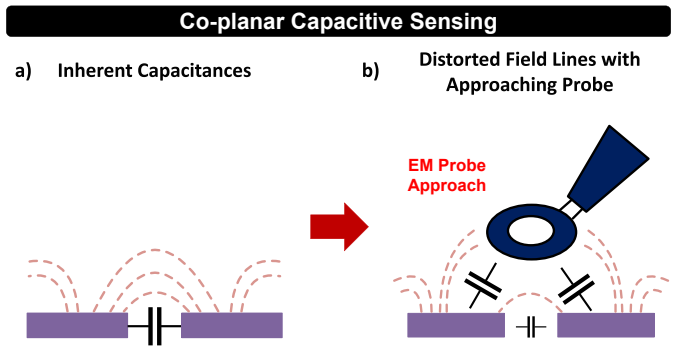

Fig. 3. Operating principle of co-planar capacitive sensing (a) Inherent capacitance of 2 co-planar plates and (b) distorted field lines with approaching probe.

C. Contribution

To provide a better alternative, a preliminary method was presented in [22] by introducing a new capacitive detection structure against an approaching probe in EM SCA attack. By adopting *co-planar capacitive asymmetry sensing (CEASE),* the proposed structure was shown to achieve a better sensitivity and a longer maximum detection distance compared to the pre-existing inductive sensing. Through electromagnetic simulations with approaching EM probes, the proposed technique was demonstrated to achieve $> 11\times$ improved sensitivity, and thus longer detection range compared to inductive sensing.

This paper expands upon the work presented in [22] by a comprehensive theoretical exploration into different capacitive sensing mechanisms and comparison with inductive sensing, as well as a simulation based design space exploration. The proposed structure uses co-planar capacitive asymmetry and detects a variety of microprobe-based EM attacks with a $\leq$ 1mm detection range. The focus of this work is to dive deep into EM theoretic aspects leading to the proposal of a new modality of EM probe sensor. The ASIC design with such a sensor is part of future work.

Specific contributions of this paper are:

- A theoretical analysis of the proposed CEASE technique utilizing four on-die top-layer metal plates is presented showing improvement in **detection range** compared to inductive sensing (previous work) and **detection both electric (E) and magnetic (H) field probes** with high sensitivity.
- A further deep dive on **capacitive sensing mechanism** for change in capacitance due to approaching probe and capacitor plate designs to maximize sensitivity is presented.
- A design-space exploration of the proposed CEASE to find an optimum plate size and inter-plate distance of the plates is performed showing the trade-off between sensitivity and area of the detection plates.
- A simulation framework is created with Ansys Maxwell which shows $>$ **3**$\times$ **and** $>$ **11**$\times$ **improvement in sensitivity** over alternative parallel-plate capacitive sensing technique and the inductive sensing (prior work) respectively, and can detect an approaching EM probe at a distance of 1 mm.

This paper is organized as follows. Section II describes the operating principle compared to other sensing methods and a new proposed structure. Section III addresses simulation results along with a comparison with the previous works. Finally, concluding remarks are presented in Section IV.

II. Capacitive Asymmetry Sensing of EM Side-Channel Attack

A. Basic Operating principle

The basic idea behind a co-planar capacitive detection is to include metal plates at the top metal layer of an IC or a PCB, and track the capacitance between pairs of these metal plates in some way; for example, by incorporating the capacitance pairs into LC oscillator circuits. 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. 3(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 and hence the peak resonant frequency of the corresponding LC oscillator system as described in Fig 3(b). This resonance-peak frequency of the LC oscillator systems can then be tracked to detect the presence of an approaching probe. If the deviation of a capacitance from its absolute value is solely used for detection, it is a **symmetric detection**; while the difference in the relative deviation between multiple capacitor pairs leads to **asymmetry** sensing (CEASE).

B. Parallel Plate vs Co-planar Capacitors

One 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 as shown in Fig. 4(a). In this paper however, we have taken a 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 capacitance (C), but relative capacitance - where the amount of deviation in capacitance (ΔC) relative

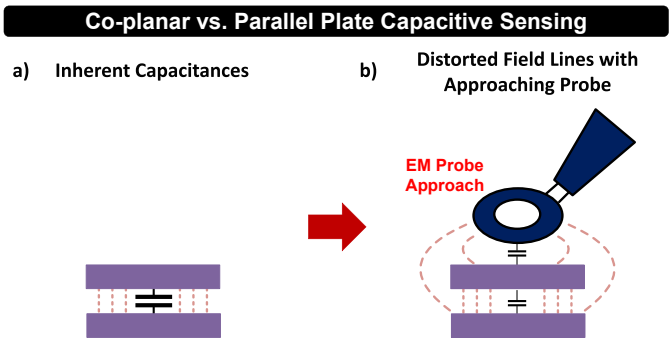

Fig. 4. Operating principle of parallel plate capacitive sensing (a) Inherent capacitance of 2 parallel plates and (b) distorted field lines with approaching probe.

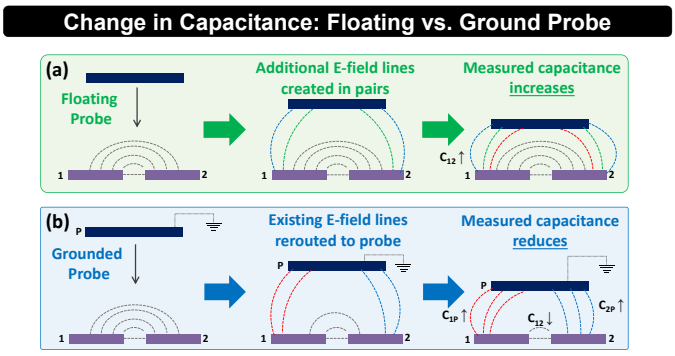

Fig. 5. Mechanisms of change in capacitance for capacitive sensing: (a) Floating probe causes an increase in measured capacitance, and (b) ground-referenced probe causes a reduction in measured capacitance.

to its absolute value or with another capacitance pair is much more meaningful. To that end, using a co-planar capacitance ensures that the electric field lines between the plates traverse through the surrounding environment (a parallel plate configuration would avoid that as described in Fig. 4(b)) and can easily get intercepted by an approaching probe. In addition, the co-planar capacitor can be applied to the flipped chip. This is because even if the plate consisting of top metal is located at the bottom of the chip, there exists a coupling between the EM probe and the plate. However, there will be coupling the detection range will be more limited. Now, the CEASE structure does not have to be only limited to on-IC. The concept can be extended to have a similar structure on the backside of the IC, on the package, granted at the expense of additional routing. This is part of future research.

C. Mechanisms for Change in Capacitance

As mentioned above, the simplest way to look at the change in capacitance due to an approaching probe is the distortion of the electric fields between the capacitor plates caused by the probe. In this subsection, we will shortly look at the three different mechanisms that can cause such disruption in the fields:

1) ***Non-metallic object****:* A non-metallic object or a dielectric, when present close to a co-planar capacitor, will cause an increase in the capacitance if the dielectric constant of that object is higher than air, by increasing the effective ε of the path of the E-field lines. An example of this will be the insulation or the PCB backing used on an EM probe, that can cause a change in capacitance of the co-planar capacitor.

2) ***Floating metallic object****:* A floating metallic object, for example a metallic probe, when brought close to the plates of a co-planar capacitance, will get **polarized** due to induction of charges from the electric fields of the capacitor. This will cause the approaching probe to form an additional parallel capacitance to the pre-existing co-planar capacitance, and hence increase the net capacitance. An easy way to visualize this is by drawing field lines between the capacitor plates, as shown in Fig.5(a). When the probe approaches, additional pairs of field lines are formed between each of the plate and the probe. The important point to note here is that as the probe is floating, the new lines are complementary, i.e. for each new line formed between a positively charged plate and the probe, a complementary line is formed between the negatively charged plate and the probe. As a result, these pairs of field lines can be interpreted as new continuous field lines between the two capacitor plates. So effectively, the number of field lines between the two plates increase, resulting into an increase in capacitance.

Another way to look at this, is that if a fixed potential difference is maintained between the plates of the co-planar capacitance, an approaching probe will cause a temporary reduction of that potential due to induction of opposite charges on the areas of the probe close to a specific plate, hence reducing the overall energy of system due proximity of opposite charges. To regain the original potential difference, the capacitor plate will need to be supplied additional charges. So a higher amount of charge (Q) is required to maintain the same potential (V), giving rise to a higher capacitance (C), as $Q = CV$ and for a constant V, increase in Q implies increase in C.

3) ***Grounded metallic object****:* If the floating metallic object is grounded or partially grounded however, i.e. it has some path to earth's ground - either directly or through some parasitic capacitances, then a different case may arise, especially when the co-planar capacitor detector setup is also referenced to earth's ground. Let us look at the extreme case where the approaching probe is completely shorted to earth's ground, and the detector setup is also referenced to earth's ground. In this case, irrespective of the position of the approaching probe, a fixed potential difference is enforced between the probe and each of the plates, by the earth's ground. Here, if the potential on one of the plate changes, the difference is compensated by additional charges on the grounded probe that are supplied by earth's ground, without affecting the distribution of charges on the other capacitor plates. The closer the grounded probe is to the capacitor plates, the higher is this balancing effect of earth's ground. This implies that the charges in the plates are controlled by the grounded probe and not the capacitor plates itself, and as a result, the effective capacitance of the co-planar plates see a reduction when the grounded probe approaches.

The field line picture is also quite different compared to the earlier floating ground case, as shown in Fig.5(b). When the probe approaches the capacitor plates, it 'steals' some of

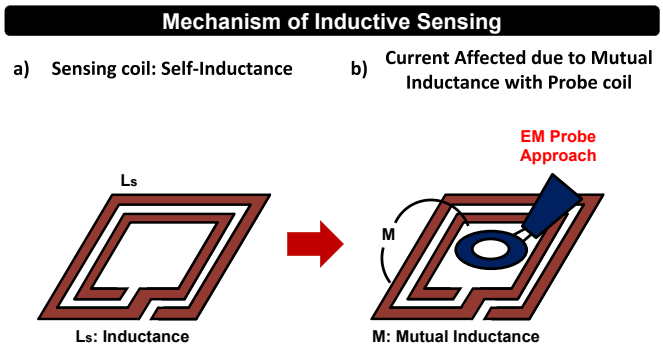

Fig. 6. Operating principle of coil based Inductive Sensing (a) Sensing coil without the presence of a probe (b) Magnetic field due to induced current at the approaching probe modifies the default current flow at the sensing coil, due to mutual inductance of between the sensing and probe coils

the field lines that were already present between the plates. Some of the field lines that originated from, say the positively charged plate, now terminate on the probe, instead of the other negatively charged plate. The closer the probe is, the higher is this conversion of direct field lines to plate to probe field lines. Further, these plate-to-probe field lines are not complementary, as a fixed potential difference already exists between each of the plate and the probe due to referencing to earth's ground. So effectively, the closer the probe is, the number of field lines reduces between the plates - reducing the capacitance, unlike the earlier floating probe case - where an effective increase in field lines would have been observed.

D. Inductive vs Capacitive Sensing

At this point, it is useful to go through the fundamental differences between capacitive sensing (this work) and inductive sensing [20] modalities, and motivate the reason we propose to explore the capacitive sensing method.

- **Firstly**, capacitive sensing is agnostic of attack probe types, such as E or H field probes - it is dependent only on the surface area of the sensing pads and the probe, and the distance between them. For the inductive sensing case however, the technique relies on the probe to have a coil, i.e. be an H field probe. The probe first picks up alternating magnetic field created by sensitive components of the IC, in order to perform side-channel attack. This induces an Electro-motive Force (EMF) at the probe, and creates a current in the probe coil. This current, in turn, creates a magnetic field that interacts with the sensing coil to modify its current response: e.g. move the peak resonant frequency, when the sensing coil is being used as part of an LC oscillator. So, in addition to having a coil-probe, the method relies on the probe to have some current flow in the first place. If the sensing coil has an inductance L_S, it is used in series with a capacitance C_S, the mutual inductance between the sensing coil and the probe coil is M and the probe has a series impedance of Z_S for taking measurements,

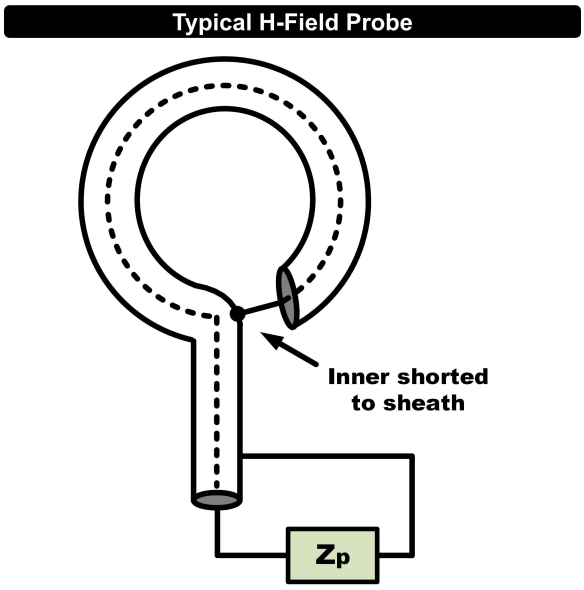

Fig. 7. Typical H-field probe

then the current I_S in the sensing coil can be written implicitly as:

$$I_S = \frac{V_S}{j\omega\left(L_S - M\frac{I_P}{I_S} - \frac{1}{\omega^2 C_S}\right)} \tag{1}$$

giving the peak resonant frequency as approximately:

$$f_{peak} \sim \frac{1}{2\pi\sqrt{\left(L_S - M\frac{I_P}{I_S}\right)C_S}} \tag{2}$$

Note that this depends on the probe current I_P, which is given by V_P/Z_P, where V_P is the induced EMF at the probe. If the probe uses a high impedance detection mechanism, i.e. Z_p is large, then $I_p \sim 0$, reducing eqn (2) to:

$$f_{peak} \sim \frac{1}{2\pi\sqrt{L_S C_S}} \tag{3}$$

- which is just the natural peak frequency of the LC oscillator circuit, thus rendering this kind of sensing circuit useless in this scenario. Note that an intelligent attacker could in fact choose to use $Z_p \to \infty$, as that simultaneously helps to 1) maximize V_p (i.e. ability to attack) that can be picked up with a high Z voltage mode sensor, such as a CMOS common source amplifier; and 2) minimize I_P, hence reducing the chance of attack detection. A capacitive sensing method on the other hand, is independent of the type of the probes and its impedance, and hence is free from this kind of exploit. Fig. 7 shows how an H-field probe would typically look. We note that practically, even if the ends of the coil are left as an open circuit, there will be a parasitic capacitance present between the two ends, creating a finite impedance. An intelligent attacker would design an attack probe to maximize this impedance as much as possible, to minimize current flow and hence risks of

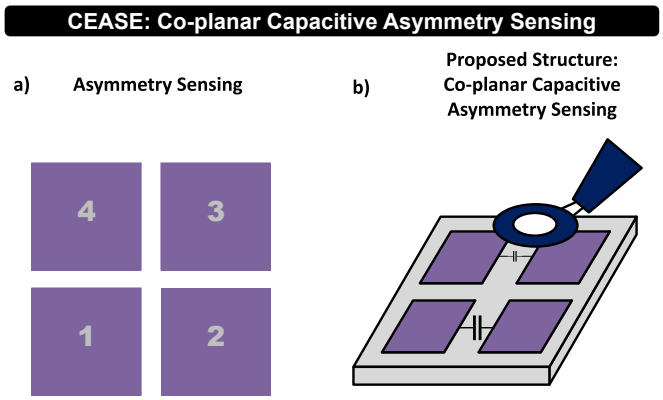

Fig. 8. The co-planar capacitive asymmetry sensing (CEASE) (a) principle of asymmetry sensing and (b) the proposed structure: CEASE

inductive detection of the attack - and maximize induced EMF across the coil terminals, to be picked up using a high input impedance voltage detector.

- **Secondly**, for *capacitive sensing*, it can be shown that the sensitivity (or the mutual capacitance between the probe and the sensing pads) **drops with distance as** $\sim \mathbf{1/d}$, where d is the distance between the pad and the probe. This can be intuitively seen as well, as the electric potential from a local charge drops as $\sim 1/distance$. Now for a circular loop, the axial magnetic field can be shown to drop with distance as $\sim 1/d^{3/2}$. However, this effect is doubled here: first the probe picks up magnetic field from the chip, and then the sensing coil picks up magnetic field due to the induced current at the probe. As a result, for *Inductive sensing*, sensitivity in fact **drops as** $\sim \mathbf{1/d^3}$, potentially making it a much worse candidate for longer distance detection.

E. Significance of Asymmetry Sensing

Asymmetric sensing, as we have briefly introduced, incorporates more than one pair of capacitance plates. This would require the use of at least three plates, resulting in 3 distinct pairs; the example in Fig 8(a) shows the use of 4 plates, where more than two or more pairs can be selected from the six possible combinations. As we mention above, the capacitance between a pair of plates is affected by any objects in the surrounding environment - be that the wall of a building, metal wall of the chassis, a person - it is not restricted to an approaching probe. So it is important to distinguish between different cases, and that is where the asymmetry detection comes in. While any relatively far away big objects such as a wall or a person could create significant deviation in capacitance, the change in capacitance would be similar among multiple pairs. Only 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.

F. Proposed Co-planar Capacitive Asymmetry Sensing (CEASE)

As shown in Fig. 8(b), the new proposed structure consists of four aligned metal pads of the same size and dimension. Since the cross section of each metal pad faces the cross section of another metal pad, electric field occurs between the cross section. The capacitance values generated by the electric field are the same due to the symmetrical structure. However, as an EM probe approached the four aligned metal pads, the symmetry of the system breaks because of coupling capacitance from EM probe. This results in the change of the capacitance between the pairs diverges from the baseline capacitance, which can be detected.

G. Optimum capacitor plate design considerations

At this point, let us consider the different potential design choices for the co-planar capacitance. As we mentioned briefly in the subsection above, to maximize sensitivity, one should try to maximize $\Delta C/C$. However, depending on the area available on a chip, the configuration with the maximum sensitivity, i.e. maximum $\Delta C/C$, may have a very small absolute C, which may make detection of that base capacitance difficult. In that case, a designer may choose a configuration with slightly worse sensitivity, to attain a higher base capacitance. Also, if one is incorporating asymmetry detection as part of their design, that may also suggest the use of a particular design that may not have the highest overall sensitivity. With that out of the way, let us look at a few possible designs of the co-planar capacitor:

1) Single plate: The single plate design (Fig. 9(a)) would be the most basic design choice, where all of the available area for the capacitor is used as a single metal plate, used as one plate of the capacitor. The other plate of the capacitor is left floating. The plate operates analogous to an electrical monopole, and the base capacitance in this case is just the self capacitance of the plate. Since it operates as a monopole, this configuration would have the slowest possible decay of electric fields ($\sim 1/r^2$) away from the plate. So in theory, this design should offer the highest sensitivity among all the listed cases here. However, as the base capacitance is just the self capacitance of the plate, this configuration will also exhibit the lowest base capacitance, making it harder to incorporate into a detection circuit in the chip dimensions. Also, due to the monopole nature of this configuration, electric fields are less confined compared to other cases, thus reducing the resolution of asymmetry sensing.

2) Dual plate: A dual plate design (Fig. 9(b)) is effectively the most common two-plate capacitance design, where the two plates are placed on a same plane. This co-planar dual plate system has been used for the simulation based analysis in the rest of this paper. The dual plate behaves like an electrical dipole, and so it would see a **faster decay of electric fields** ($\sim 1/r^3$) compared to the single plate case, making the sensitivity of this configuration drop faster with distance. However, the base capacitance will be higher compared to the single plate case, making the detection circuitry relatively easier to implement. Also, the fields will be more locally

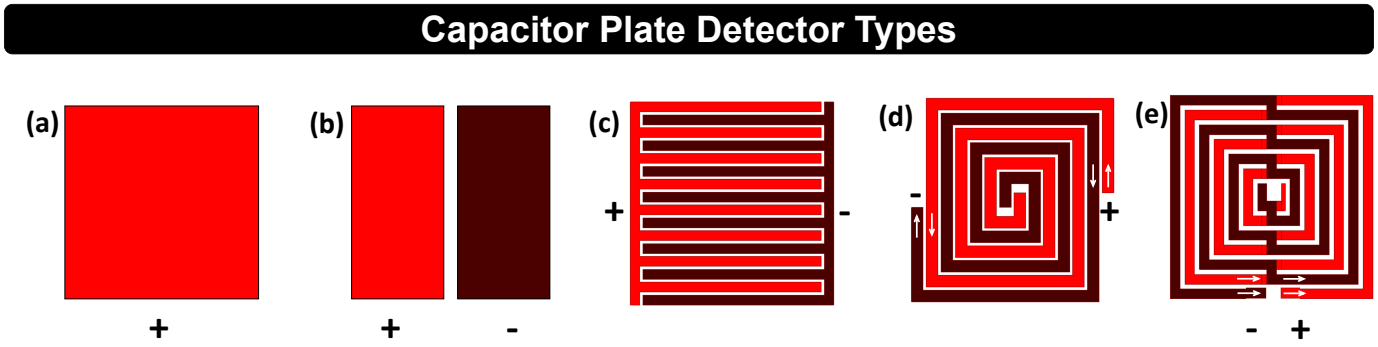

Fig. 9. Capacitor plate detector types: (a) Single plate, (b) Dual plate, (c) Comb structure, (d) Flux cancelling spiral, and (e) Flux maintaining spiral.

confined in this case, making it better suitable for asymmetric detection of an approaching probe.

3) Comb structure: This is a modification of the dual plate design, where the edge overlap between the two structures is maximized by an interleaved comb structure (Fig. 9(c)). Due to the increased edge overlap, this case will show a significantly higher base capacitance compared to the basic dual plate case. Note however, that the comb basically operates as a closely spaced repeating dipoles, as opposed to one single dipole in the dual plate case. As a result, this case will show an even higher local confinement of electric fields (hence the higher base capacitance), making the sensitivity even lower compared to the dual plate case, while improving the spatial resolution for asymmetry sensing.

4) Notched spirals - Combined capacitive and inductive sensing: Finally, another way of increasing the edge overlap to increase base capacitance at the expense of sensitivity, is to use overlapping spiral structures with discontinuities introduced to maintain two separate electrodes of the capacitor. This kind of spiral structures will have the added benefit of a high self inductance, making it self resonant at a frequency that can be manipulated through design. A designer may choose to utilize this self resonant frequency to detect an approaching probe, and this will eliminate the need of designing a separate inductor for an LC oscillator for detection purposes. Do note however, an approaching probe can cause a change in the inductance of the structure due to mutual inductance, in addition to altering the capacitance. If these effects are opposing, then this would cause even further reduction in sensitivity. Now as we saw earlier, an approaching probe will typically cause reduction in effective inductance, whereas the capacitance may either increase or decrease depending on ground loading. If ground loading is significant and the net capacitance also reduces along with the inductance, the spiral cases should see an increase in sensitivity over the comb case. If ground loading is minimal however, and the net capacitance increases, this case will see a reduction in sensitivity. Now, depending on which case a designer want to prioritize, the effect of change in inductance can be reduced or increased, by the design of the spirals as described below:

- *Flux maintaining spiral:* As the name suggests, a flux maintaining case includes two overlapping spirals with current flow in the same direction (Fig. 9(e)), so that the total magnetic flux from the two spirals add up. This case will have a higher self inductance and will be more sensitive to change in inductance due to an approaching probe.
- *Flux cancelling spiral:* This is the other possible scenario, where the overlapping spirals exhibit opposing current flow (Fig. 9(d)), and hence the magnetic flux from those partially cancel each other out. This case will have a lower self inductance, and will see a lower sensitivity to change in inductance.

H. Configuration of detector and probe for this work

As we have discussed above, the direction of change in capacitance at the detector is dependent on whether the probe is floating or grounded/ground-referenced. While the former causes an increase in capacitance, the later causes an reduction in the same. This is also observed in our initial simulation results in Fig.10(b), where the capacitance C_{34} is observed to increase in the case of a floating probe, and reduce for a grounded probe. In reality, most of today's electrical measurement systems will either be referenced to earth's ground, or at least partially referenced to ground through parasitic capacitances between it's ground plates and the surrounding environment or a human operator. Also, considering the initial simulation results in Fig.10(b) and (c), the grounded probe case appears to be worse of the two - as the capacitance increase for a floating probe can be theoretically infinite, where as capacitance reduction due to a grounded probe can only be finite - as it can reduce to zero from its baseline value. In other words, it is easier to detect an approaching probe when the probe is floating, and harder when it is grounded. Now, as we are trying to devise an attack prevention technique, we as designers have no control on whether the probe is grounded or floating - so we must assume the worst-case scenario of the two. An intelligent attacker would always choose a grounded probe, to lower the chance of detection. This is why, we choose to demonstrate our detection technique in this work with a grounded probe henceforth, knowing that it would also work for a floating probe as inferred from the initial simulation results.

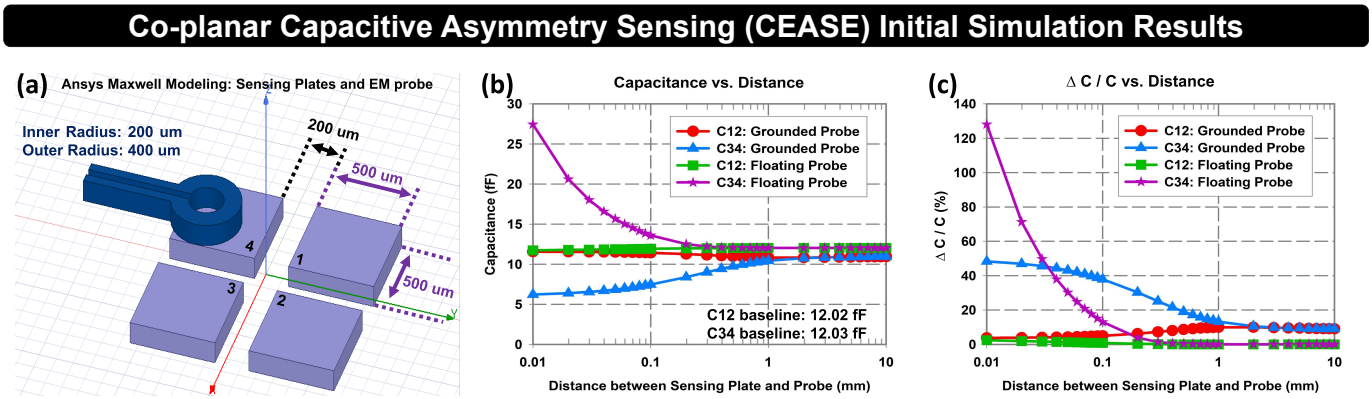

Fig. 10. Baseline simulation results of CEASE with respect to distance between sensing plates and EM probe (a) CEASE simulation modeling in Ansys Maxwell, (b) capacitance change of CEASE, (c) capacitance change rate of CEASE.

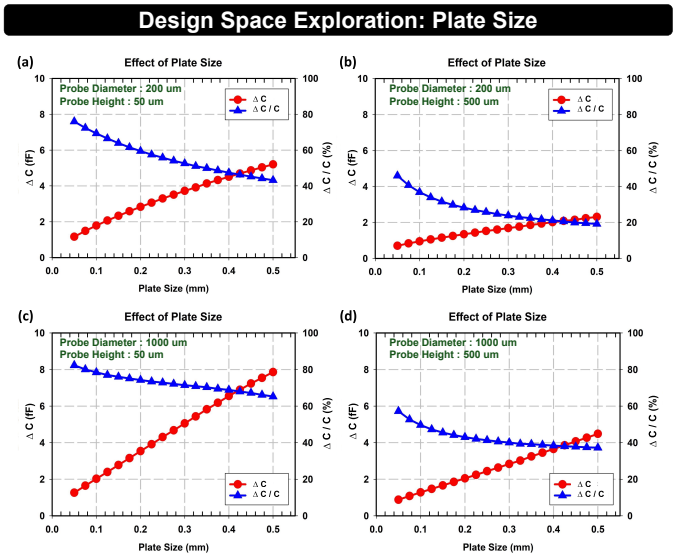

Fig. 11. Design space exploration to analyze the plate size of CEASE (a) probe diameter: 200μm and height: 50μm, (b) probe diameter: 200μm and height: 500μm, (c) probe diameter: 1000μm and height: 50μm and (d) probe diameter: 1000μm and height: 500μm.

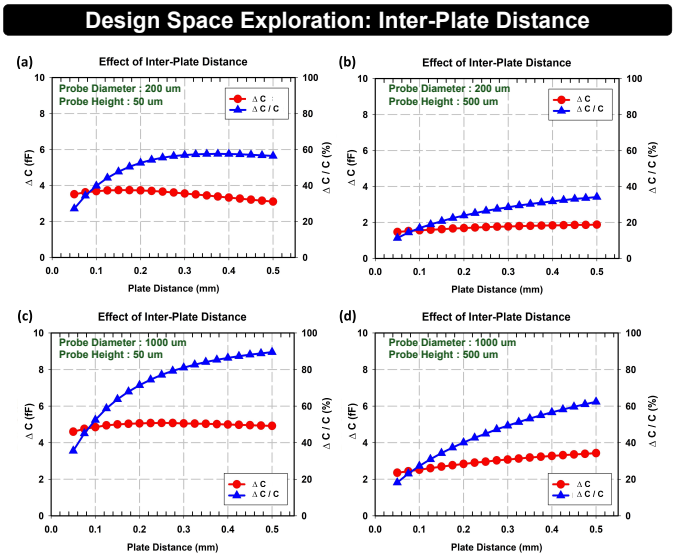

Fig. 12. Design space exploration to analyze the inter-plate distance of CEASE (a) probe diameter: 200μm and height: 50μm, (b) probe diameter: 200μm and height: 500μm, (c) probe diameter: 1000μm and height: 50μm and (d) probe diameter: 1000μm and height: 500μm.

Further, as per our discussion of the detector configuration, the different configuration amplifies different factors such as absolute capacitance or sensitivity, and so an optimization needs to be made depending on which factor is most important for a specific use case. We discussed that a single plate detection maximizes percentage change in capacitance, while minimizing absolute baseline capacitance and sensitivity towards asymmetry. A very complex structure such as a comb or a notched spiral on the other hand, maximizes absolute capacitance and sensitivity towards asymmetry, while minimizing percentage change in capacitance. In this work, we have used a dual plate configuration as a compromise - which while not being the highest demonstrator of any of the three factors, still exhibits a balance between all three and hence a potential good choice of optimum detector configuration.

III. 3D-FEM Modeling & Simulation Results

This section presents simulation results of the proposed CEASE system using Ansys Maxwell. The simulation results demonstrate the operating principle as described in the previous section and are presented as follows: 1) baseline analysis of the CEASE structure; 2) design space analysis of the CEASE structure for finding optimal conditions; 3) detailed comparative analysis of CEASE, parallel plate capacitive sensing, and inductive sensing; and 4) comparative analysis with E-field and H-field probes. Simulations were computed and verified via Ansys Maxwell simulation.

A. Model & Baseline Simulation

Fig. 10 shows the initial simulation results of CEASE. The purpose of this simulation was to observe how the EM probe affects capacitance and to verify how mechanism of EM probe affects when it approaches a CEASE plate as

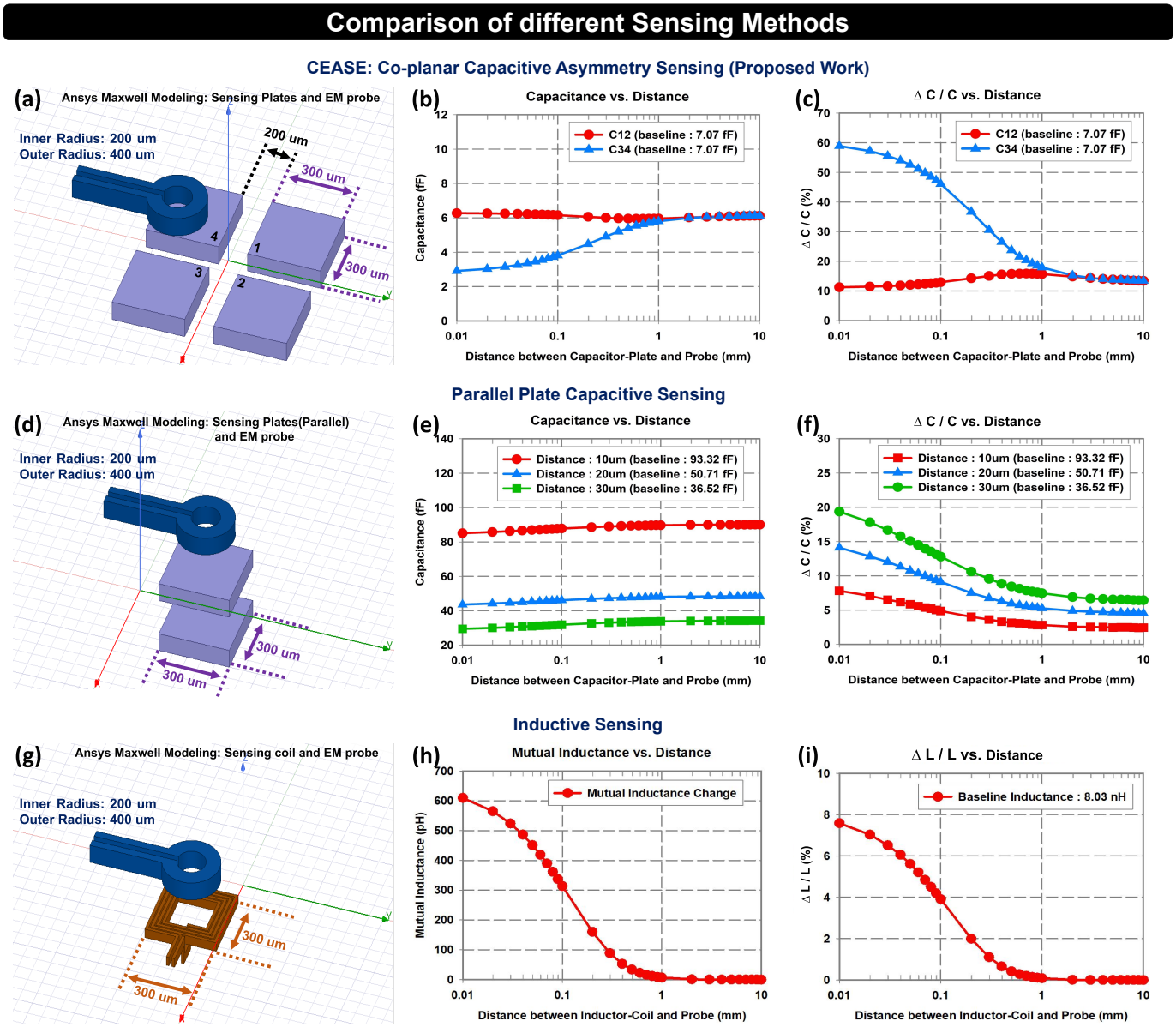

Fig. 13. Comparison of capacitive sensing and inductive sensing with respect to distance between sensing plates and EM probe (a) CEASE simulation modeling in Ansys Maxwell, (b) capacitance change of CEASE, (c) capacitance change rate of CEASE, (d) capacitive parallel sensing simulation modeling in Ansys Maxwell (e) capacitance change of capacitive parallel sensing, (f) capacitance change rate of capacitive parallel sensing, (g) inductive sensing simulation modeling in Ansys Maxwell (h) mutual inductance change of inductive sensing and (i) inductance rate of inductive sensing.

we explained in Section II, subsection C. As shown in Fig. 10(a), the EM probe approached the mid-point of plates 3 and 4 vertically. The sensing plate size and the distance of each plate were 500μm and 200μm, respectively. Fig. 10(b) shows the simulated capacitance values of CEASE structure as the EM probe approaches the sensing plates for grounded and floating probe mechanisms. 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 were 12.02 fF. When the grounded mechanism of EM probe approached, C34 reduces due to the coupling effect of EM probe. However, when the floating mechanism of EM probe approached, C34 increases due to the induction of charges from the electric fields of the plate. The magnitude of capacitance change in floating mechanism was more than grounded mechanism. As the distance between the sensing plates and grounded/floating mechanism of EM probe becomes $<$0.1 mm, a capacitance change of $>$35% and $>$15% is observed, respectively, while at a distance of 1 mm or shorter, the capacitance diverges by $>$10% compared to the baseline in grounded EM probe cases as shown in Fig. 10(c). Subsequently, the results imply that using capacitive asymmetry, the EM probe approaching can be detected as C12 and C34 diverges from their baseline capacitance due to asymmetry in probe positioning with respect to the pads. To obtain better sensitivity and detection range using capacitive asymmetry, it is significantly vital to optimize the parameters of the sensing plate.

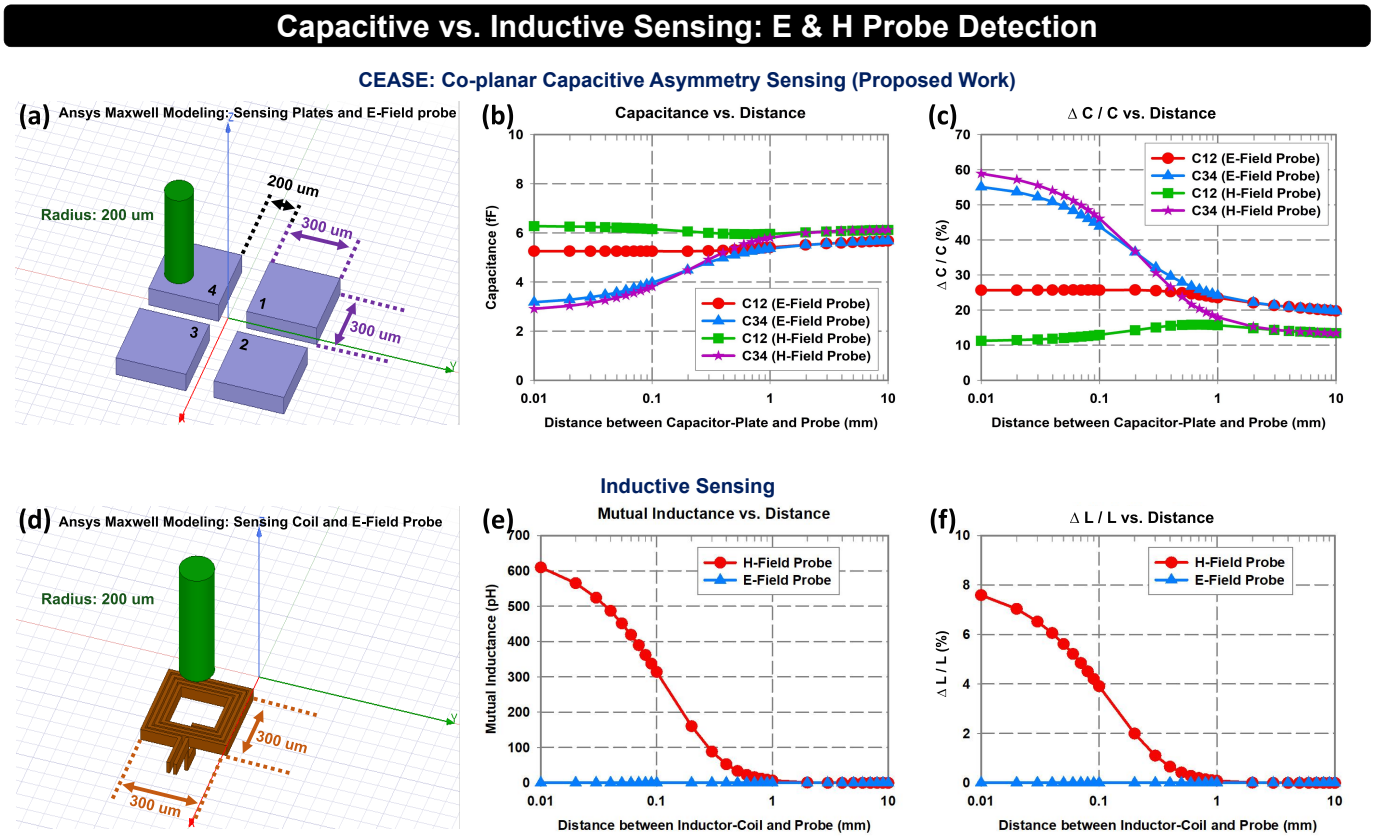

Fig. 14. Comparison of E-field and H-field probe detection with respect to distance between sensing plates and probe (a) CEASE simulation modeling in Ansys Maxwell, (b) capacitance change of CEASE, (c) capacitance change rate of CEASE, (d) inductive sensing simulation modeling in Ansys Maxwell, (e) mutual inductance change of inductive sensing and (f) inductance rate of inductive sensing.

B. Effect of Plate Size

Fig. 11 shows the design space exploration to analyze the size of the plates of the CEASE structure. To find the optimal sensing plate size, various situations were applied to the simulation by changing the EM probe diameter and sensing plate to EM probe vertical distance. From this simulation results, we can confirm the following: 1) As the sensing plate size increased, the deviation in capacitance (ΔC) increases and the ΔC/C value reduces as shown in Fig. 11(a). 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. 2) As the sensing plate to EM probe vertical distance increased, the effect of the smaller sensing plate size became more apparent. This can be confirmed by comparing the sensing plate to EM probe vertical distance in two cases. When the sensing plate to EM probe vertical distance was 500μm (Fig. 11(b) and (d)), the ΔC/C slope went higher as the size of the sensing plate becomes smaller than the case of the sensing plate to EM probe vertical distance is 50μm (Fig. 11(a) and (c)). 3) As the EM probe diameter increased, the effect of the sensing plate size decreased. This can be confirmed by comparing the EM probe diameter in two cases. When the EM probe diameter was 1000μm (Fig. 11(c) and (d)), the change range of ΔC/C was narrower than the case of the EM probe diameter, which was 200μm (Fig. 11(a) and (b)).

C. Effect of Inter-Plate Distance

Fig. 12 shows the design space exploration to analyze the inter-plate distance of the CEASE structure. To find the optimal sensing plate distance, various situations were applied to the simulation by changing the EM probe diameter and sensing plate to EM probe vertical distance. From these simulation results, we can confirm the following: 1) For all cases except Fig. 12(a), ΔC/C keeps increasing as the inter-plate distance is increased. This is owing to the fact that the baseline inter-plate capacitance C reduces as the plates are moved further from each other, whereas the change ΔC remains similar, owing to the electric field lines being affected similarly by the probe in all cases. 2) For Fig. 12(a), we see a saturation in the ΔC/C curve with increase in plate distance. Here, due to the smaller probe diameter (200 μm) and the smaller probe height (50 μm), not enough of the field lines between the plates are being affected by the probe, when the plates are moved further. As a result, ΔC also reduces with increasing plate distance.

To find an optimal inter-plate distance, we should look at the cases where the probe is further from the plates (Fig. 12(b) and (d)). The results suggest that as long as there is enough chip area, and baseline capacitance C does not fall below sensitivity of the detection circuitry, the inter-plate distance should be kept as large as possible, after optimizing plate size as explained in the previous sub-section.

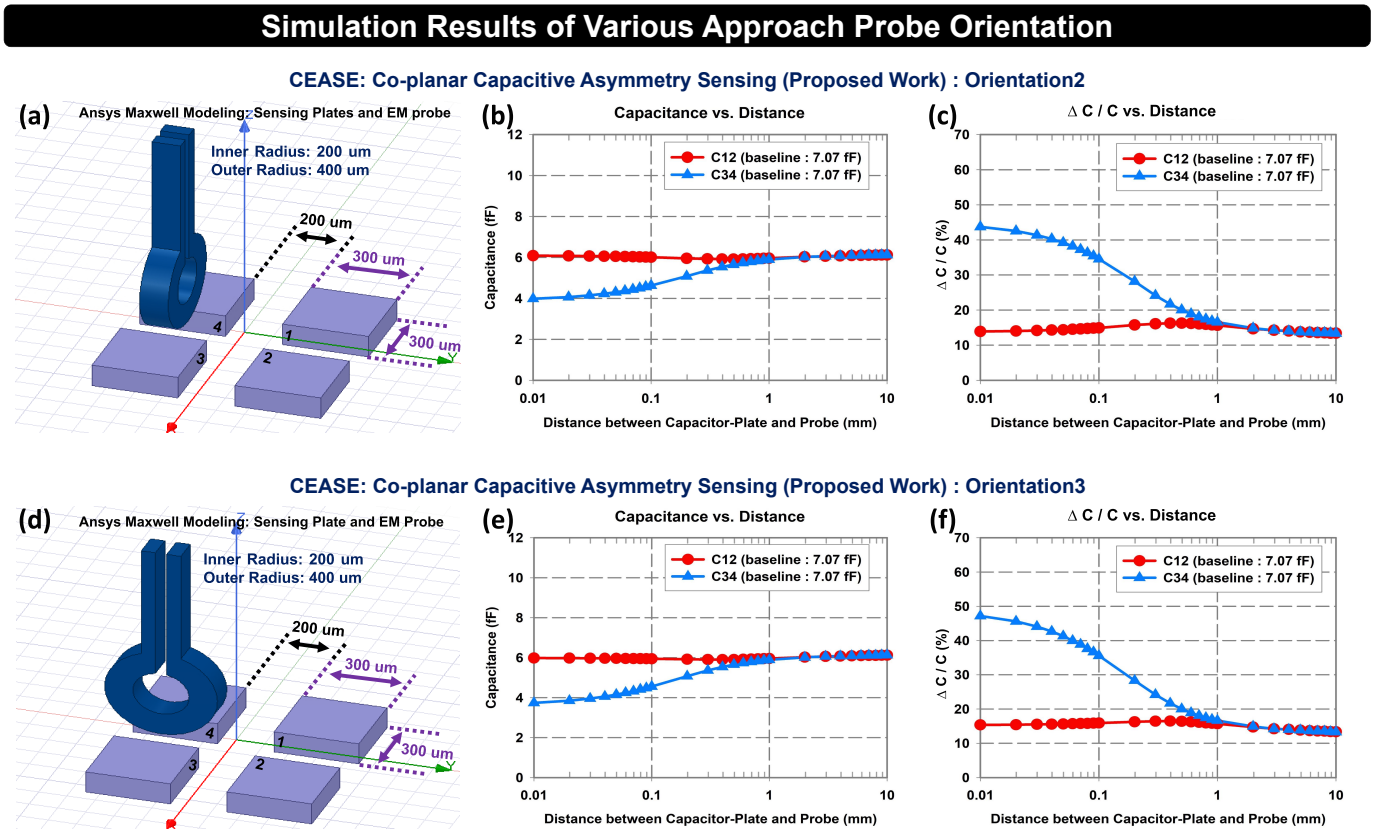

Fig. 15. Simulation results of various approaching probe orientation with respect to distance between sensing plates and probe (a) CEASE simulation (orientation 2) modeling in Ansys Maxwell, (b) capacitance change of CEASE, (c) capacitance change rate of CEASE, (d) CEASE simulation (orientation 3) modelling in Ansys Maxwell (e) capacitance change of CEASE and (f) capacitance change rate of CEASE.

D. Comparison with other Sensing Methods

Fig. 13 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 CEASE. As shown in Fig. 13(a), the EM probe approached the mid-point of the plates 3 and 4 vertically. The sensing plate size and the distance between each pair of plates are 300μm and 200μm, respectively. Fig. 13(b) shows the simulated capacitance values of CEASE 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 $>$17% compared to the baseline as shown in Fig. 13(c).

Next, we demonstrate the simulation results for the case of capacitive parallel plate-based sensing. As shown in Fig. 13(d), the EM probe approaches the mid-point of the 2 plates vertically. The sensing plate size was the same as CEASE plates. Fig. 13(e) shows the simulated capacitance values for capacitive parallel sensing when the EM probe approaches. As the EM probe approaches, the capacitance is reduced due to the coupling effect of the EM probe (some of the field lines get coupled to the probe, and hence the reduction). 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. 13(f).

We now present the simulation results for inductive sensing. As shown in Fig. 13(g), The EM probe approaches the mid-point of the coil vertically. The coil has an inductance of 8.03 nH, while the EM probe has an inductance 457 pH according to the EM field simulation in Maxwell. Fig. 13(h) 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. 13(i) shows the inductance change rate when the probe approaches. As the EM probe approaches, the inductance changes due to the coupling effect with the EM probe, which leads to changing mutual inductance. When the distance between the coil and the EM probe becomes $<$0.1 mm, the inductance only changes by $\sim$3%, while for $<$1 mm, the inductance does not show any deviation from the baseline.

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

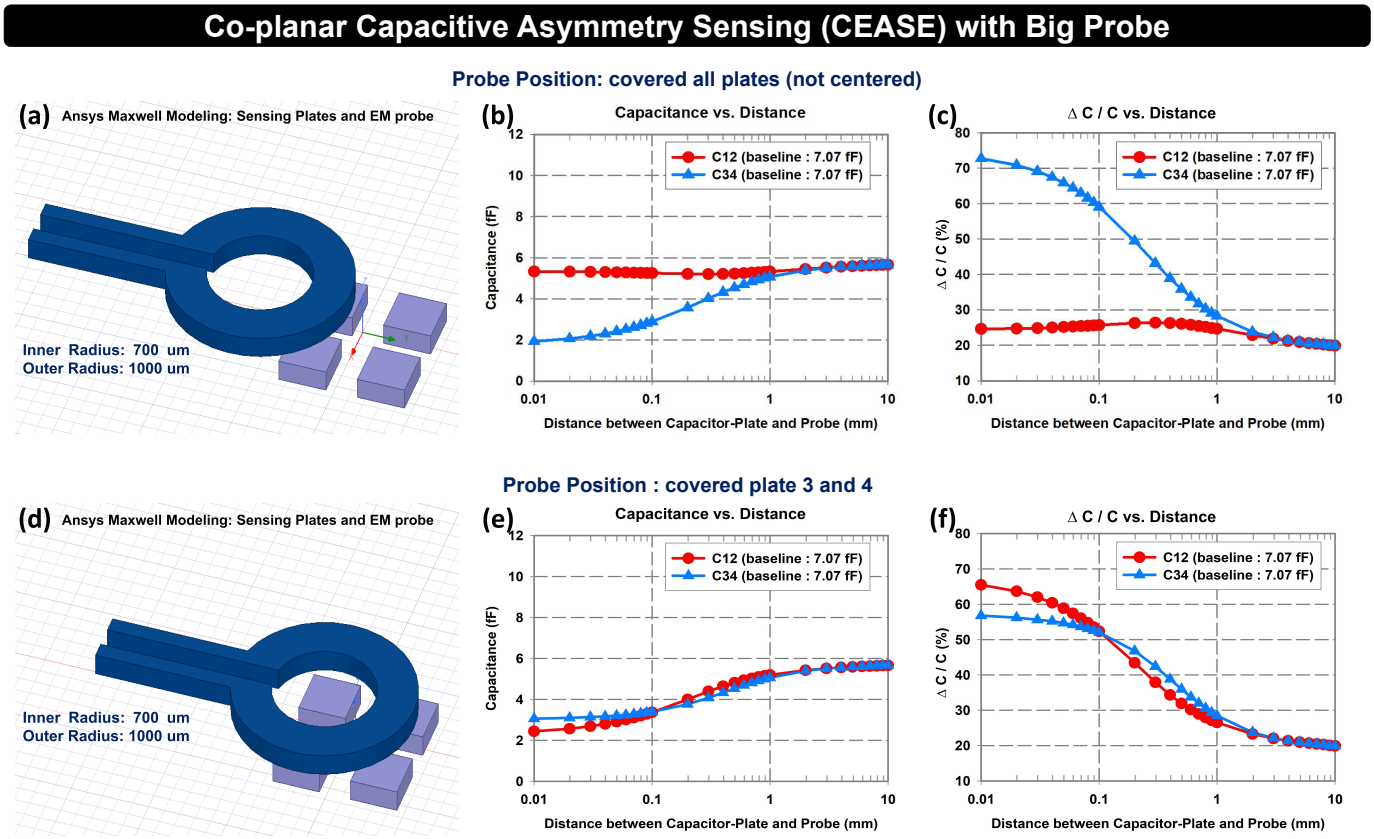

Fig. 16. Simulation results of a large loop area probe with respect to distance between sensing plates and probe (a) CEASE simulation (probe covers only plate 3 and 4) modeling in Ansys Maxwell, (b) capacitance change of CEASE, (c) capacitance change rate of CEASE, (d) CEASE simulation (probe covers all plates, but not exactly centered) modeling in Ansys Maxwell, (e) capacitance change of CEASE and (f) capacitance change rate of CEASE.

E. Detection Sensitivity and Range for Different Probe Types

Fig. 14 shows the comparison of the sensitivity and maximum detection range for the the proposed CEASE and the inductive sensing techniques for both H-& E-field probes.

In the case of CEASE, the probe approaches the mid-point of plates 3 and 4 as shown in Fig. 14(a) (shown for the E-probe), similar to Fig. 13(a). Fig. 14(b) shows the change in the capacitance values of CEASE 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. 14(c) shows the change in $\Delta C/C$ as the EM probe approaches. The magnitude of change in C34 was more than C12 in both cases.

In the case of inductive sensing, the probe approaching the center of the coil is modeled. as shown in Fig. 14(d). Fig. 14(e) 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 a E-field probe which does not have a loop. This implies that the inductive sensing is only effective for a H-field probe as described in Fig. 14(f).

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

F. Detection Sensitivity for Different Probe Orientations

Fig. 15 shows the comparison of the sensitivity and maximum detection range for the the proposed CEASE for different probe orientations.

As shown in Fig. 15(a) and (d), the EM probe approached with a different orientation from the Fig. 13(a). Fig. 15(b) and (e) shows the simulated capacitance values of CEASE 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 $>30\%$ is observed, while at a distance of 1 mm or shorter, the capacitance diverges by $>15\%$ compared to the baseline as shown in Fig. 15(c) and (f).

These results demonstrate that the CEASE structure can detect the EM probe even though it approaches various different probe orientations.

G. Detection Sensitivity for a Large Area Probe

Fig. 16 shows the simulation results of sensitivity and maximum detection range for the proposed CEASE for a large loop area EM probe. In the case of CEASE with large loop area EM probe, the probe approaches in two way: 1) the probe covers only plates 3 and 4 as shown in Fig. 16(a); the probe

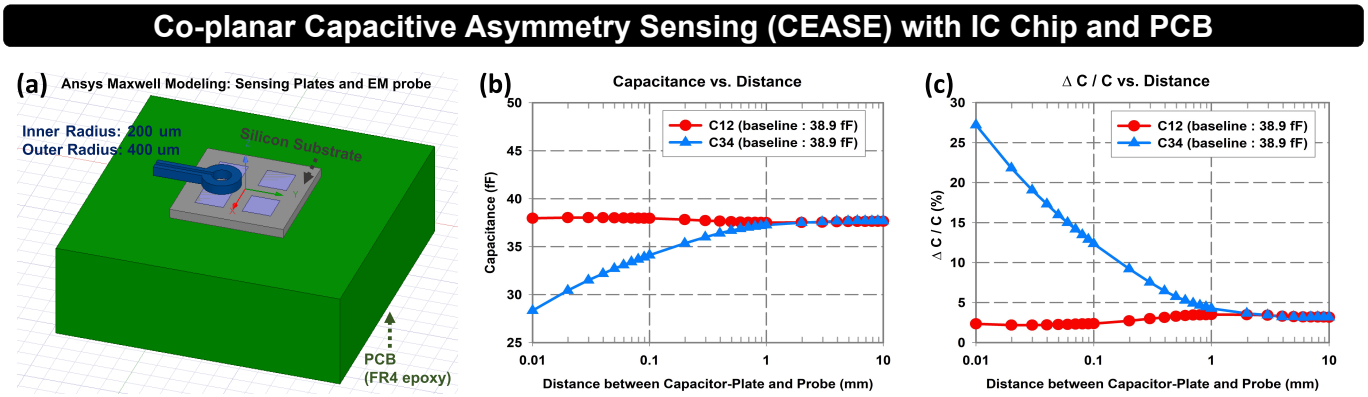

Fig. 17. Simulation results of CEASE in a practical situation of an IC chip and PCB (a) CEASE simulation (silicon substrate and FR4 epoxy material) modeling in Ansys Maxwell, (b) capacitance change of CEASE and (c) capacitance change rate of CEASE.

covers all plates, but is not exactly centered as shown in Fig. 16(d). In the absence of the EM probe, C12 and C34 (baseline capacitance between the plates 1, 2 and 3, 4 respectively) were measured to be 7.07 fF. Fig. 16(b) shows the simulated capacitance values of CEASE structure as a large loop area EM probe approaches the sensing plates and the probe covers only plates 3 and 4. 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 $>$58% is observed, while at a distance of 1 mm or shorter, the capacitance diverges by $>$28% compared to the baseline as shown in Fig. 16(c). Fig. 16(e) shows the simulated capacitance value of CEASE structure as a large loop area EM probe approaches the sensing plates and the probe covers all plates, but is not centered. When the EM probe approaches, C12 and C34 reduce due to the coupling effect of the EM probe respectively. However, since there is a difference in the area of the coupling effect between the EM probe and each sensing plate, the decreasing capacitance value is different. As a sequence, the diverged capacitance values compared to the baseline are different as shown in Fig. 16(f).

These results demonstrate that the CEASE structure can detect the EM probe if the EM probe does not approach the center exactly. If a probe has a large loop area and approaches the center exactly, it may induce a similar deviation in the capacitance for different pairs of plates, defeating the asymmetry sensing. Nevertheless, the proposed structure can still detect attacks if the baseline capacitance can be recorded and compared to changed capacitance. Furthermore, a probe with larger loop covers bigger area which makes the chip vulnerable to global-EM attacks, while nullifying the effects of local-EM attacks.

H. Detection Sensitivity in a practical situation of an IC chip and PCB

Fig. 17 shows the simulation results of CEASE in a practical situation of an IC chip and PCB. Co-planar plates are implemented top metal layer of an IC on the silicon substrate and PCB that represents the fundamental material of FR4 epoxy as shown in Fig. 17(a). In the case of CEASE in a practical way, the probe approaches the mid-point of plates 3 and 4 similar to previous simulations. Fig. 17(b) shows the change in the capacitance value of CEASE on silicon and PCB as the EM probe approaches. In the absence of the EM probe, C12 and C34 (baseline capacitance between the plate 1, 2 and 3, 4 respectively) were measured to be 38.9 fF. Baseline capacitance between the plate increased compared to the previous case. This is because the permittivity of dielectric between the plate increased due to the influence of PCB and silicon substrate. When the EM probe is close to the sensing plates, 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 $>$12% compared to the baseline is observed as shown in Fig. 17(c).

These results demonstrate that the CEASE structure can detect the EM probe in the case of an IC and PCB.

IV. Conclusion

This paper presents the design and analysis of co-planar capacitive asymmetry sensing (CEASE) technology for efficient detection of approaching probe in EM side-channel attacks by detecting the variations in symmetry of co-planar capacitor plates. Different types of capacitive detection structures are compared in terms of sensitivity and area overhead. The final proposed detector structure of consists of four co-planar metal plates of the same size and dimensions, arranged in a 2×2 grid. As an EM probe approaches the metal plates, the symmetry of the metal plate system breaks, and the capacitance between the pairs diverges from the baseline capacitance, triggering a detection of the approaching probe.

Further, the proposed capacitive structure is also compared with existing inductive sensing technique, as well as an alternative capacitive detection technique. Through theoretical arguments and Maxwell simulations, capacitive sensing is shown to have en enhanced detection range over inductive sensing. Simulation results indicate that CEASE 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). For the EM probe distance of $\sim$0.1 mm, a deviation of $>$ 45% in the

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

Parameter		CEASE: Co-planar Capacitive Asymmetry Sensing (This Work) ①			Capacitive Parallel Sensing ②	Inductive Sensing [20], [21] 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

baseline capacitance is observed, implying a $> 3\times$ & $> 11\times$ sensitivity improvement over capacitive parallel sensing and the inductive sensing respectively (Table I). Further, capacitive sensing is also shown to be effective for both E field and H field probes, unlike inductive sensing. This makes CEASE an overall improved technique for EM side channel attack prevention through pro-active detection of approaching probes and consequently turning on a possible countermeasure. As a result, power overhead is significantly reduced, compared to constantly running the same countermeasure on the chip. Subsequently, such low overheads make it possible to implement the proposed CEASE technique together with conventional countermeasures developed for other types of attacks.

Future works will involve ASIC design for evaluating the proposed CEASE structure using circuitry. Representative circuitry that can precisely and finely evaluate the delta C is switched-capacitor network that converts capacitance into voltage This will be coupled with a countermeasure enabling low-overhead EM SCA protection agnostic to any crypto algorithm.

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. ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity. *IEEE TCAS-I*, 2018.
[8] D. Das et al. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In *IEEE HOST*, 2017.
[9] 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.
[10] Das et al., D. EM and Power SCA-resilient AES-256 through >350x Current Domain Signature Attenuation & Local Lower Metal Routing. *IEEE JSSC*, 2020.
[11] 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.
[12] D. Das et al. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In *IEEE HOST*, 2019.
[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] D. Das et al. Em/power side-channel attack: White-box modeling and signature attenuation countermeasures. *IEEE Design & Test*, 38(3):67–75, 2021.
[16] A. Ghosh et al. Syn-stellar: An em/power sca-resilient aes-256 with synthesis-friendly signature attenuation. *IEEE Journal of Solid-State Circuits*, 57(1):167–181, 2021.
[17] 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 IEEE International Solid- State Circuits Conference (ISSCC)*, volume 64, pages 499–501, 2021.
[18] C. Tokunaga et al. Secure aes engine with a local switched-capacitor current equalizer. In *2009 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pages 64–65,65a, 2009.
[19] K. Raghavan et al. A 4900-μm^2 839-mb/s side-channel attack- resistant aes-128 in 14-nm cmos with heterogeneous sboxes, linear masked mixcolumns, and dual-rail key addition. *IEEE Journal of Solid-State Circuits*, 55(4):945–955, 2020.
[20] N. Miura et al. A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor. In *VLSI*, 2014.
[21] N. Homma et al. EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor. In *CHES*, 2014.
[22] 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.

Dong-Hyun Seo received the B.S. degree in electronics and radio engineering from Kyung Hee University, Seoul, South Korea, in 2013, and the M.S. degree in electronics computer engineering at Hanyang University, Seoul, South Korea, in 2015, and is currently working toward Ph.D. degree in the School of Electrical Engineering, Purdue University, West Lafayette, IN, USA. His research interests include CMOS low-power analog ,mixed signal and RF integrated circuit design for sensor node interfacing.

Mayukh Nath received BS in Physics from Indian Institute of Science, Bangalore (2016), and MS in Electrical Engineering from Purdue University, West Lafayette in 2021. He is currently pursuing PhD in Electrical Engineering at Purdue University as well. His research interests include electromagnetic theory and modelling of inter-device communications, such as Body Area Network based medical implants and wearables; as well as electromagnetic analysis of side channel attack and prevention techniques.

Debayan Das received his PhD and MS in Electrical and Computer Engineering from Purdue University, USA in 2021 and the Bachelor of Electronics and Telecommunication Engineering degree from Jadavpur University, India, in 2015. He is currently a Research Scientist at Intel Corporation, USA. Prior to his Ph.D., he worked as an Analog Design Engineer at a startup based in India. His research interests include mixed-signal IC design and hardware security.

Dr. Das was a recipient of the IEEE HOST Best Student Paper Award in 2017 and 2019, the Third Best Poster Award in the IEEE HOST 2018, and the 2nd Best Demo Award in HOST 2020. In 2019, one of his papers was recognized as a Top Pick in Hardware and Embedded Security published over the span of the last six years. He was recognized as the winner (third place) of the ACM ICCAD 2020 Student Research Competition (SRC). During his Ph.D., he has been awarded the ECE Fellowship during 2016-2018, the Bilsland Dissertation Fellowship in 2020-2021, the SSCS Predoctoral Achievement Award in 2021, and the Outstanding Graduate Student Research Award by the College of Engineering, Purdue University, in 2021 for his outstanding overall achievements. He has authored/co-authored more than 50 peer-reviewed conferences and journals including 2 book chapters and 2 US patents. He has been serving as a primary reviewer for multiple reputed journals and conferences including JSSC, TCAS-I, SSCL, TVLSI, TCAD, Design & Test, TODAES, JETCAS, TBME, IoTJ, DAC, VLSI Design, HOST.

Santosh Ghosh is a Research Scientist in Intel Labs. He has coauthored about 75 research publications in refereed international conferences and journals with a citation H-index of 21, and 41 issued with other 54 more patents filed (pending). The primary focus of his research includes: 1) Lightweight and post-quantum crypto algorithms; 2) low overhead innovative processor micro-architecture using lightweight crypto to solve long-lasting SW bugs & vulnerabilities and to protect side-channel attacks; 3) cryptographic hardware microarchitecture and RTL with the aggressive area, latency, and throughput constraints to meet requirements for high-volume Intel products; and 4) investigate and develop timing, power, EM and Photon side-channel countermeasures. Santosh received the Ph.D. degree from IIT Kharagpur, India in 2011, and completed his postdoctoral studies from COSIC, KU Leuven, Leuven, Belgium, in the area of cryptographic hardware and side-channel attacks.

Shreyas Sen is an Elmore Associate Professor of ECE & BME, Purdue University and received his Ph.D. degree from ECE, Georgia Tech. Dr. Sen has over 5 years of industry research experience in Intel Labs, Qualcomm and Rambus. His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Things (IoT), Biomedical, and Security. He has authored/co-authored 3 book chapters, over 175 journal and conference papers and has over 20 patents granted/pending. Dr. Sen serves as the Director of the Center for Internet of Bodies (C-IoB) at Purdue. Dr. Sen is the inventor of the Electro-Quasistatic Human Body Communication (EQS-HBC), or Body as a Wire technology, for which, he is the recipient of the MIT Technology Review top-10 Indian Inventor Worldwide under 35 (MIT TR35 India) Award in 2018 and Georgia Tech 40 Under 40 Award in 2022. To commercialize this invention Dr. Sen founded Ixana and serves as the Chairman and CTO. His work has been covered by 250+ news releases worldwide, invited appearance on TEDx Indianapolis, Indian National Television CNBC TV18 Young Turks Program, NPR subsidiary Lakeshore Public Radio and the CyberWire podcast. Dr. Sen is a recipient of the NSF CAREER Award 2020, AFOSR Young Investigator Award 2016, NSF CISE CRII Award 2017, Intel Outstanding Researcher Award 2020, Google Faculty Research Award 2017, Purdue CoE Early Career Research Award 2021, Intel Labs Quality Award 2012 for industrywide impact on USB-C type, Intel Ph.D. Fellowship 2010, IEEE Microwave Fellowship 2008, GSRC Margarida Jacome Best Research Award 2007, and nine best paper awards including IEEE CICC 2019, 2021 and in IEEE HOST 2017-2020, for four consecutive years. Dr. Sen's work was chosen as one of the top-10 papers in the Hardware Security field (TopPicks 2019). He serves/has served as an Associate Editor for IEEE Solid-State Circuits Letters (SSC-L), Nature Scientific Reports, Frontiers in Electronics, IEEE Design & Test, Executive Committee member of IEEE Central Indiana Section and Technical Program Committee member of DAC, CCS, CICC, IMS, DATE, ISLPED, ICCAD, ITC, VLSI Design, among others. Dr. Sen is a Senior Member of IEEE.