IEEE Open Journal of
Circuits and Systems

Received 23 February 2023; revised 5 May 2023; accepted 26 June 2023. Date of publication 24 July 2023; date of current version 13 October 2023.

Digital Object Identifier 10.1109/OJCAS.2023.3292712

PG-CAS: Pro-Active EM-SCA Probe Detection Using Switched-Capacitor-Based Patterned-Ground Co-Planar Capacitive Asymmetry Sensing

DONG-HYUN SEO [1], ARCHISMAN GHOSH [1] (Graduate Student Member, IEEE), DEBAYAN DAS [1] (Student Member, IEEE), MAYUKH NATH [1], SANTOSH GHOSH [2], AND SHREYAS SEN [1] (Senior Member, IEEE)

[1]Purdue University, West Lafayette, IN 47906, USA

[2]Intel Labs, Hillsboro, OR, USA

This article was recommended by Associate Editor A. Shrivastava.

CORRESPONDING AUTHOR: D. SEO (e-mail: seo60@purdue.edu)

ABSTRACT This paper presents the design and analysis of a pro-active strategy to detect the presence of an electromagnetic (EM) side-channel analysis (SCA) attack, using Patterned-Ground co-planar Capacitive Asymmetry Sensing (PG-CAS) system. The PG-CAS system senses the asymmetry created in the plate-ground capacitance and turns on a SCA countermeasure in presence of an EM probe. The proposed PG-CAS system for approaching probe consists of the EM SCA detection sensor plate and circuits. The EM SCA detection sensor is implemented as a grid of four metal plates of the same dimensions using the top metal layer along with a patterned-ground plane at the immediate lower metal layer. The EM SCA detection system consists of a proximity to capacitance conversion circuit, digital synchronization logic circuit to detect and alarm the IC, and an EM SCA countermeasure. When an attack is detected, the countermeasure is turned on based on the deviation of the symmetry of the plate-ground capacitance pairs. The PG-CAS system-level post-layout simulation results using TSMC 65nm technology and Ansys Maxwell show a $> 5\times$ improvement in the detection range and a $\sim 29\times$ improvement in power consumption over existing inductive sensing methods for attack detection.

INDEX TERMS Side-channel attack, electromagnetic leakage, patterned-ground, capacitive asymmetry, switched capacitor, AES protection.

I. INTRODUCTION

With the advent of the Internet, artificial intelligence, IoT, and wearable devices, 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. Even though most of the Internet-connected devices use cryptographic algorithms to provide the confidentiality of data, side-channel analysis (SCA) attacks have been demonstrated to exploit critical information through electromagnetic (EM) radiation [1], power dissipation [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. Mathematically-secure crypto algorithms like AES-256 can be broken by extracting the secret key even from a distance of 1 meter using an EM probe. EM SCA provides a crucial advantage to attacker compared to power SCA as it does not require probing the power supply pin physically to monitor the power consumption. Another main distinction of EM SCA is that it can perform the precise observation of information leakage from a specific part of the target IC (Integrated Circuit) as described in Fig. 1(a), compared to power SCA where the global power consumption is measured. Hence, EM SCA can lead to high signal-to-noise ratio (SNR) measurements for side channel attack.

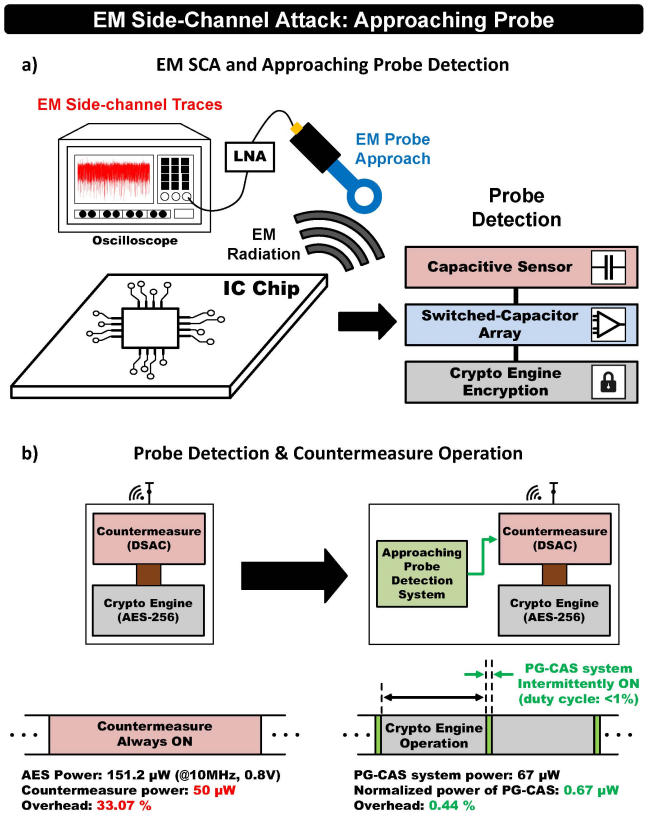

FIGURE 1. Electromagnetic (EM) side-channel analysis (SCA) attack countermeasure (a) approaching probe detection and (b) countermeasure operation.

A. MOTIVATION & RELATED WORK

As these EM SCA attacks gradually evolve, various countermeasures have been proposed to protect against EM SCA. Countermeasures against EM SCA can be classified as logical [8], architectural [9], both of which belong to design specific countermeasures, and generic physical (Circuit-level) countermeasures [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25]. However, these countermeasures suffer from significantly high power overheads which ranges from 32% to 400%, as well as performance degradation, and may not be generic to any crypto algorithms. Moreover, some of the circuit-level techniques suffer from large embedded passives (MIM capacitors and inductors) [17].

The related works on EM SCA detection have been reported in [5], [6], [7] as shown in Fig. 2. The previous work on an EM probe detection is based on inductive sensing, which is implemented using an inductive sensor coil-based LC oscillator as described in Fig. 3. When an EM probe approaches the inductive sensor, the mutual inductance (M), generated by the variations in the EM field, between the EM probe and the integrated sensor coil increases. The oscillation frequency of LC oscillator that is connected with inductive sensor shifts due to the changing mutual inductance, allowing detection of the presence of an EM probe. However, the effective detection range between the EM probe and the inductive sensor coil is limited to a maximum of 0.1 mm, which poses a major challenge. Hence, in this work, we focus on designing an on-chip sensor to increase the maximum detection range of an incoming EM probe. Few other recently presented inductive sensing based detection system directly detects the approaching probe from time-domain [26], [27] with help of a machine learning (ML) algorithm. However, they suffer from similar shortcomings as stated above. Recently, capacitive sensing-based EM probe detection have been explored in [28], [29]. However, its efficacy in a real IC design environment with ground planes around and the circuit design for the sensing system have not been explored yet. In modern CMOS technology, capacitive sensing is challenging as the thickness of the top metal layers is below μm range (65nm in our experiments) and hence the resolution becomes very limited because the capacitance between two co-planar capacitive plate is $<$ fF range.

To overcome the challenges discussed above, this paper introduces a new detection sensor, circuit, and system for an approaching EM probe with an improved detection range and lower power overhead.

B. CONTRIBUTION

Specific contributions of this paper are:

- Explore of the concept of capacitive sensing in an IC layout and co-optimizing both the ground plane capacitance and the sensing capacitance to maximize sensitivity.
- Design of the post-processing circuits and systems with ultra-low power for sensing attacks and to prove the efficacy through the post-layout simulation results.
- Integration with digital SCA protection and AES-256 crypto core and checking the efficacy of the proposed method using the integrated detection and countermeasure system in post-layout simulations.

The goal of this 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 detecting attacks and operating the proximity to capacitance conversion circuit and digital synchronization logic circuit leading to reduction in power consumption. The proposed technique achieves $> 5\times$ better maximum detection distance compared to the existing inductive sensing [5], [6]. Power overhead is also $> 29\times$ less when it is operated intermittently at 1% duty-cycle as shown in Fig. 1(b) with respect to always-on state-of-the-art countermeasure. An AES-256 operating at 10 MHz, 0.8 V when simulated in SPICE consumes 151.2 μW power. Countermeasure needs a 50 μW power to operate the AES at 10 MHz, 0.8 V, contributing to power overhead of 33.07%. Now PG-CAS system consumes 67 μW power when activated. But, it is required to be activated at just 1% of the time reducing normalized power consumption to 0.67 μW which is only 0.44% with respect to unprotected AES.

This paper is organized as follows. Section II explains the purpose of PG-CAS system and the proposed architecture of

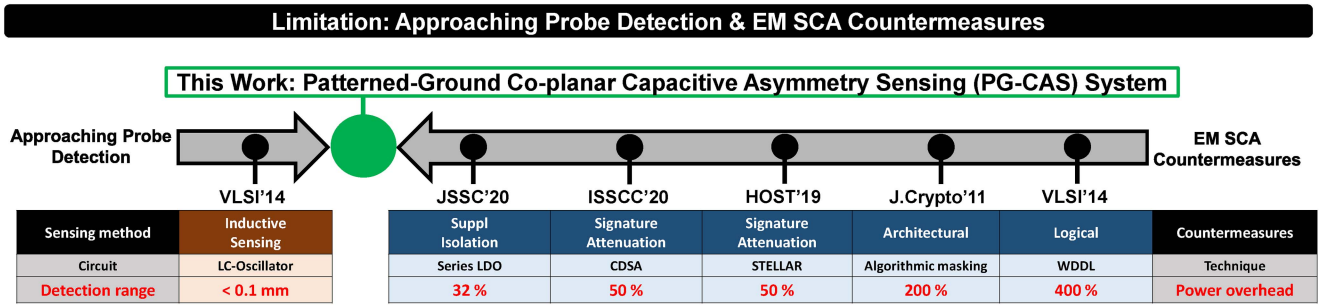

FIGURE 2. Limitation of related works: types of EM SCA countermeasures and EM SCA detection.

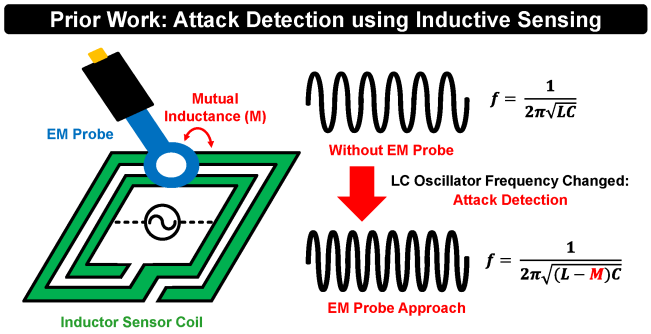

FIGURE 3. Previous Work of EM SCA detection utilizing a inductive sensor coil-based LC oscillator [5], [6], [7].

PG-CAS system. Section III describes the operating principle of EM SCA detection sensor: PG-CAS. Section IV presents the details of circuit design. Section V shows simulation results of the PG-CAS system. Finally, concluding remarks are presented in Section VI.

II. PATTERNED-GROUND CO-PLANAR CAPACITIVE ASYMMETRY SENSING SYSTEM OF EM SCA

The PG-CAS system can detect the presence of an EM side-channel attacker even before an attack is performed. When an EM probe approaches to a targeted subject, the PG-CAS system senses the attack and turns on the countermeasure to protect against EM SCA, which could significantly minimize the power overheads in comparison to the always-on countermeasure. The PG-CAS system of an EM SCA consists of the EM SCA detection sensor and circuits. Fig. 4 illustrates the conceptual block diagram of the PG-CAS system. The simplified system architecture of the PG-CAS system of EM SCA, comprises of a EM SCA detection sensor plate, proximity to capacitance conversion circuits, digital synchronization logic circuits, and integration of AES protection with sense, is described. The EM SCA detection sensor plate, which is named PG-CAS, senses the plate-ground capacitance. As the EM probe approaches, the change in capacitance can be sensed to detect an EM SCA. The capacitive sensing circuits sense the amount of change in the capacitance and converts sensor capacitance value to the oscillation frequency. Digital synchronization logic circuits determine the operation of EM SCA circuit-level countermeasure, through the detected attack, and operate the capacitive sensing circuit intermittently at $< 1\%$ duty-cycle leading to reduce power consumption. Depending on the detected attack, the AES countermeasure circuit is turned on. Digital Signature Attenuation-based Countermeasure (DSAC) [23], [30] is used as countermeasure against EM SCA attack here. It should be noted that, DSAC with help of lower metal layer routing reduces EM leakage significantly, however causes $> 25\%$ power overhead being always on. In this work, we overcome this problem by turning on DSAC only when an EM SCA is detected.

III. EM SCA DETECTION SENSOR: PG-CAS

The proposed PG-CAS technique utilizing four metal plates of the same size at the top metal layer and patterned-ground at the immediate lower metal senses plate-ground capacitance as shown in Fig. 5. The key idea of the PG-CAS is to track the capacitance between pairs of metal plates and patterned-ground plane caused by an EM probe that forms an electrical coupling with the measured object, generating mutual capacitance between them when they are close to each other, thereby breaking the symmetry of the plate-ground capacitance and the change in this capacitance can be sensed to detect EM SCA. In the case of co-planar plates and patterned-ground plane when there is no any object around, they form their own capacitances since they are not affected by the surrounding environment, as described in Fig. 6(a). If an EM probe approaches a pair of metal plates, some of the previously formed electrical field lines between the plates and patterned-ground plane will be distorted and are taken away by the EM probe. Subsequently, the capacitance between the plates and patterned-ground plane is reduced, as presented in Fig. 6(b).

A. PATTERNED-GROUND

Any metal plate and the ground-grid creates a capacitance in CMOS integrated circuit (IC) technology since the ground-grid always exists. Strong electric field lines are formed as described in Fig. 6(c), when the entire metal plate region is covered by the ground metal. Sensitivity decreases as an approaching probe has less impact on these field lines than

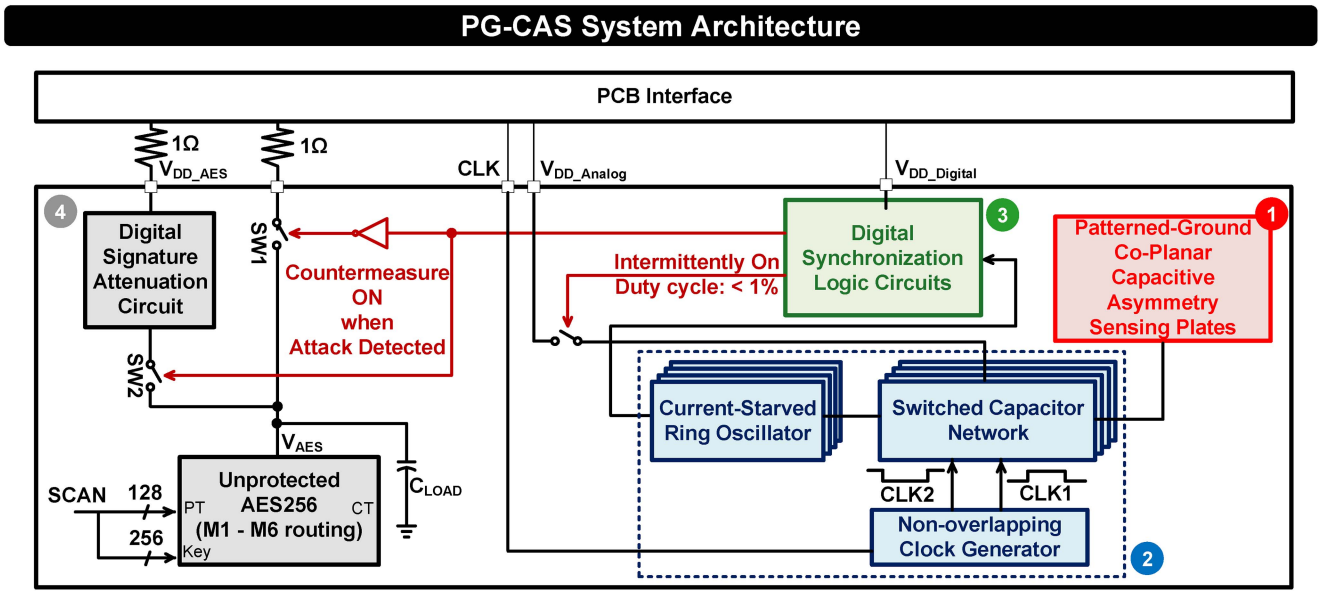

FIGURE 4. PG-CAS System architecture: The simplified system architecture of the PG-CAS system of EM SCA, composed of an EM SCA detection sensor plate (PG-CAS), proximity to capacitance conversion circuits, digital synchronization logic circuits, and integration of AES protection with sense.

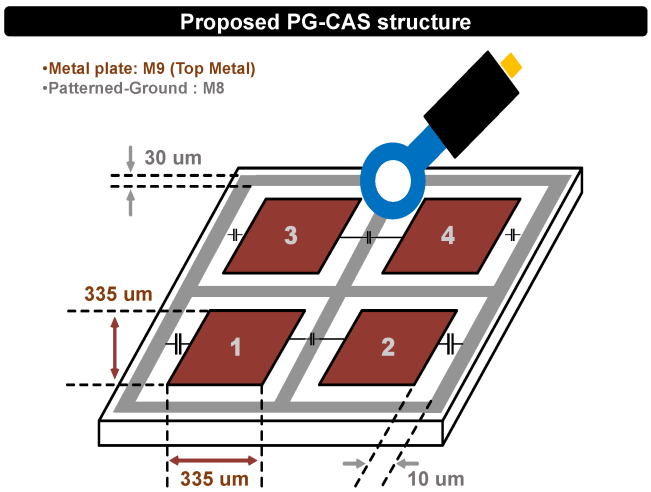

FIGURE 5. The proposed PG-CAS detection sensor structure with detail dimensions of the sensing plates and patterned-ground plane.

it would have on the surrounding environment. A patterned-ground strategy is proposed to get rid of this issue and enhance the sensitivity of the PG-CAS circuit as shown in Fig. 6(d). The co-planar capacitive plates that is made of the metal layer below the top metal are employed to create the ground patterning. By reducing the absolute capacitance between the plate and ground and increasing the relative shift in plate-ground capacitance as a probe approaches for a potential attack, ground patterning increases sensitivity.

B. ASYMMETRY SENSING

It is possible to detect an attack effectively using asymmetry sensing along with the principle that the capacitance changes when an object approaches. Asymmetry sensing incorporates more than two pairs of capacitance between plates and patterned-ground plane. Fig. 6(d) shows the use of 2 asymmetry sensing, where more than two or more pairs can be selected from the four possible combinations.

When an EM probe approaches, the electric field intercepted is different for different pairs of plates, the change in the plate-ground capacitance would diverge between the pairs. Note that the absolute plate to ground capacitance for each plate also changes, and the change in this absolute capacitance is higher than the relative change between two plates. However, the absolute capacitance change, due to it's possible susceptibilty to far away objects, can not distinguish easily between a small probe adjacent to the sensor, and a large object farther away from the sensor - as long as both provide similar change in absolute capacitance. As a result, the absolute capacitance - if used for sensing - can result in false positive detections. On the other hand, the relative change between the two plate-to-ground capacitances is affected by objects that are closer to the sensor and intercept the field lines between the two plates, as shown in Fig. 6(b). So a positive detection is triggered only when there is divergence or "asymmetry" between the two absolute plate-to-ground capacitances. This, in addition to the patterned ground mentioned in the previous subsection, allows asymmetry sensing sensitive to closely approaching objects to the sensor.

Distinguishing different cases in asymmetry detection helps in detecting approaching probe. 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. As already mentioned, that even change in one capacitance could help in approaching probe detection. However, due to its nature of raising false positives, that will need significant effort in post-silicon tuning to make sure that

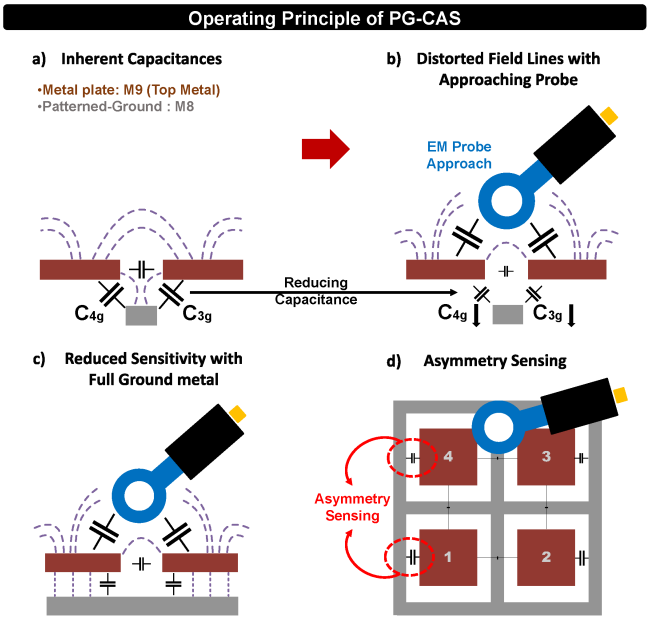

FIGURE 6. Operating principle of PG-CAS (EM SCA detection sensor) (a) Inherent capacitance of inter plates and plate-ground, (b) distorted field lines with approaching probe thereby reducing capacitance, (c) reduced sensitivity with full ground metal and (d) the concept of capacitive asymmetry sensing.

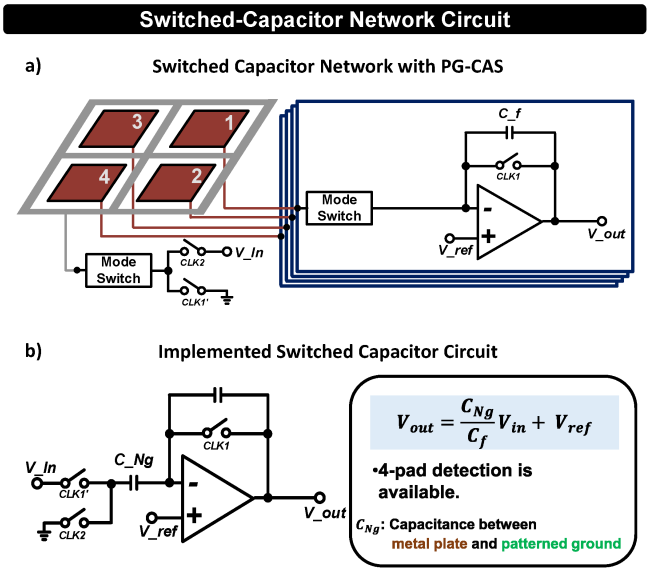

FIGURE 7. Proximity to capacitance conversion circuit: switched-capacitor network circuit (a) the combination of PG-CAS sensor plates and unit circuit package involving an operational transconductance amplifier, feedback capacitor, and switches and (b) implemented switched-capacitor network circuit from the connection.

capacitance-to-frequency converter is in the correct range. However, asymmetry sensing inherently takes that into consideration and by relative value, approaching probe can be detected even without much effort in post-silicon tuning.

IV. EM SCA DETECTION CIRCUIT DESIGN

The EM SCA detection circuit is divided into 3 parts: proximity to capacitance sensing circuits, digital synchronization logic circuits and integration of state-of-the-art AES protection [30] with sensing.

A. PROXIMITY TO CAPACITANCE CONVERSION CIRCUIT

A signal sensing circuit to measure the capacitance value is required to convert the relative capacitance change into voltage, frequency, pulse-width, or current so that relative change in capacitance can be detected using synthesizable circuit. A capacitive sensing interface circuit typically employs a simple oscillator circuit that is easily affected by parasitics, drift, and temperature sensitivity. But, the switched-capacitor circuits can overcome these drawbacks, allowing sensing of accurate capacitance value with high sensitivity [31], [32].

Fig. 7(a) describes the combination of the PG-CAS sensor plate and switched-capacitor circuit. Each capacitor sensor plate is connected to a unit circuit package involving an operational transconductance amplifier, feedback capacitor (C_f), and switch operated by CLK1. The patterned-ground is connected to two switches operated by CLK1' and CLK2, respectively. This combination enables the capacitance of capacitor sensor plate and patterned-ground to be implemented as shown in Fig. 7(b). This allows the four capacitor sensor plates to have independent capacitances, leading to detect the direction of the EM SCA attackers while they approach. The C_{Ng} is formed capacitance between capacitor sensor plate and patterned-ground and the C_f is an on-chip. The circuit converts the capacitance (C_{Ng}) into a proportional sampled voltage (V_{out}). During CLK1, C_f is isolated and entire charge of $Q_{Ng} = -C_{Ng}V_{ref}$ is sampled in C_{Ng}. During CLK2, the sampled charges are transferred to C_f. As a result, the output voltage is defined by Eq. (1).

$$V_{out} = V_{in}\frac{C_{Ng}}{C_f} + V_{ref} \tag{1}$$

An operational transconductance amplifier with a high open loop gain is used so that the output voltage will be insensitive to the input parasitics and temperature drift, which can be significant sources of the inaccuracy in these capacitive sensors.

The non-overlapping clock generator used to run the switched-capacitor circuits to ensure accurate charge transfer and the timing diagram are presented in Fig. 8(a). The switched-capacitor circuits are controlled by CLK1 and CLK2. CLK1' whose falling edge is advanced in time, compared to the falling edge of CLK, is required. All clock outputs are driven by inverting clock drivers that have the high driving capability and the equal rise and fall times.

Fig. 8(b) shows the current-starved ring oscillator. The current-starved ring-oscillator plays a role of ADC for low frequency high resolution sensing. Note that this PG-CAS system output should be digital for easy and convenient post-processing to increase self awareness in the IC against EM SCA. The simplest way would be to have a traditional ADC. The ADC will give the digital output and based on that EM SCA can be detected with high accuracy. However, because this is a very low frequency signals,

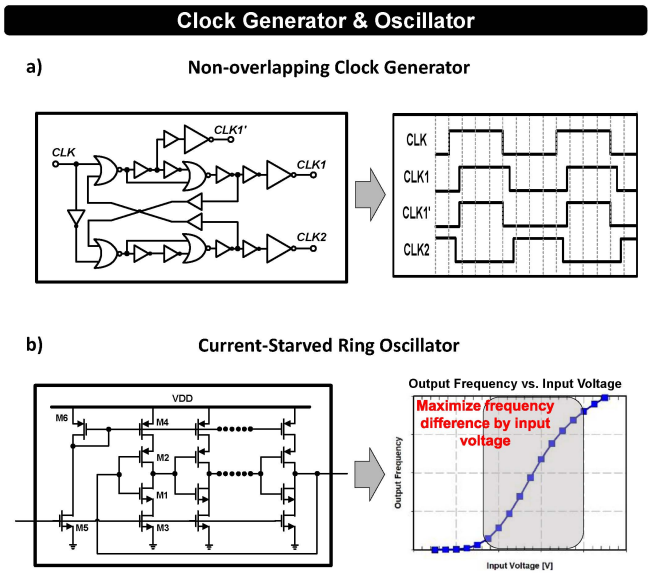

FIGURE 8. Other required to proximity to capacitance conversion circuit (a) detailed circuit schematic of non-overlapping clock generator and timing diagram showing the clock phases and (b) detailed circuit schematic of current-starved ring-oscillator and non-linearity characteristic.

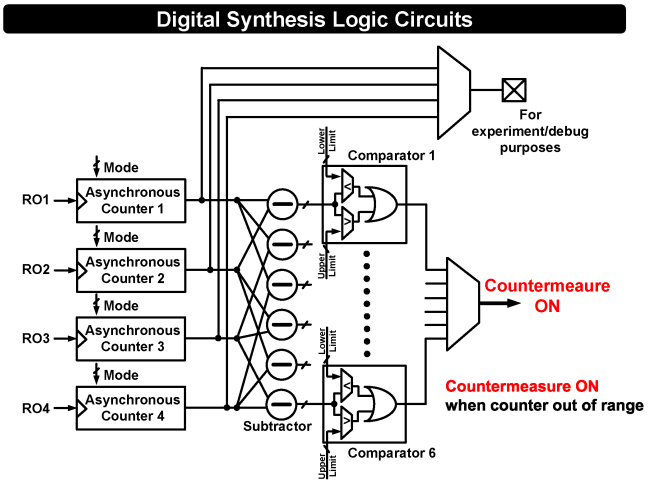

FIGURE 9. Digital synthesis logic circuits for synchronization with asynchronous counters, subtractors and comparators. This circuit processes ring oscillator frequency change and turns on the countermeasure when approaching probe is detected.

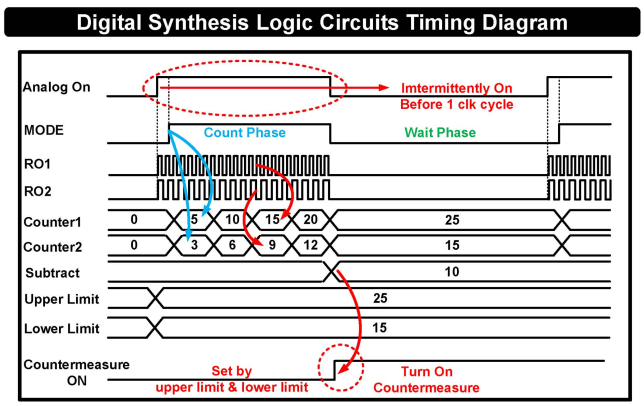

FIGURE 10. Timing diagram of digital synthesis logic circuits with count and wait modes showing detection of EM SCA and starting of the countermeasure operation, and turning on the sensing circuits intermittently.

for low frequency signal's high resolution measurement better done with integration using the ring oscillator [33], [34], [35]. It is observed that M3 and M4 (Fig. 8(b)) operate as a current source and M1 and M2 (Fig. 8(b)) operate as an inverter. The current sources limit the current available to the inverter. The M5 and M6 (Fig. 8(b)) drain currents are the same and are set by input control voltage V_{out} in this case. Finally, we can say the current-starved ring-oscillator converts the sensor capacitance value to the oscillation frequency of the current-starved ring-oscillator as a clock output. The output frequency of the current-starved ring-oscillator is non-linear with respect to the input control voltage. This non-linear characteristic helps the PG-CAS system to be self-aware of an incoming EM SCA attack. The change in the oscillation frequency of the current-starved ring-oscillator can be maximized in operating input control voltage. This means that the output frequency can be widely changed through the current-starved ring-oscillator, even if the change in the capacitance is small in the switched-capacitor network of the previous stage. Therefore, in this proximity to capacitance conversion circuits, non-linearity that allows output frequency of current-starved ring-oscillator to maximize frequency difference by intelligently calibrating the input control voltage. The phase noise and output noise of current-starved ring-oscillator is -104.45dBc/Hz @ 1MHz offset and 2.69μV/sqrt(Hz).

B. DIGITAL LOGIC CIRCUIT FOR SYNCHRONIZATION

The digital synchronization logic circuit is implemented as described in Fig. 9 to determine the possibility of approaching probe nearby. The digital synchronization logic circuit has 2 modes: a) the count phase and b) the wait phase. In Fig. 10, the timing diagram of the digital synchronization logic circuit is presented, showing the detection of EM SCA and the start of the countermeasure operation, and turning on the sensing circuits intermittently. The converted sensor capacitance value in terms of the oscillation frequency of current-starved ring-oscillator is supplied to the asynchronous counter in count mode. The digital count from the output oscillation frequency of the current-starved ring-oscillator are fed to a digital subtractor, which calculates the difference between the digital count occurring on each counter (Fig. 9). Each calculated number is compared with the threshold range that is set by lower and upper limit numbers (Fig. 10). If the digital count is out of the threshold range (greater than the upper limit or less than the lower limit), the digital synchronization logic circuit outputs an alarm ('Countermeasure ON' as shown in Fig. 9) to start the operation of the countermeasure which would significantly minimize the power overheads compared to the always-on countermeasure. In addition, the synchronization logic circuit outputs an alarm to start the operation of the proximity

to capacitance conversion circuits only before 1 clock cycle than the start of the count phase. Proximity to capacitance conversion circuits are turned off in wait phase. This allows the proximity to capacitance conversion circuit to operate intermittently at $< 1\%$ duty-cycle leading to reduce power consumption.

C. INTEGRATED AES PROTECTION WITH SENSING

Full system architecture presented in Fig. 4 consists of state-of-the-art Digital Signature Attenuation-based Countermeasure (DSAC) which is presented in [23], [24], [30]. It should be noted that DSAC is already silicon-proven. DSAC provides >200M minimum traces to disclosure being a single digital synthesizable countermeasure in silicon [30]. This work directly uses the post-layout extracted netlist of the same architecture. Traditionally, an attacker uses emanated EM radiation to correlate with attack model to get correct keybyte. Standard DSAC circuit consists of digital current sources (CS) [30]. The current source attenuates the meaningful leakage due to high output impedance of the current sources. ROs are used as local negative feedback (LNFB) to stabilize the voltage at V_{AES} node and a switch mode controller (SMC) loop is used as global negative feedback (GNFB) to make sure CS is operating in saturation region [30]. Note that, DSAC architecture optimally works only when current sources are in saturation region. When activated, this technique makes sure to reduce meaningful EM emanation to protect the crypto engine from adversary. However, in previous work [23], [30] the countermeasure was always active causing significant power overhead. Here, once 'countermeasure ON' signal is high, SW1 is turned off and SW3 is turned on as shown in Fig. 4 lowering overall power/energy overhead of the countermeasure. AES is routed in lower metal layer (upto M6) to reduce EM leakage at source. This design choice gives us the flexibility to use upper metal layer (M7-M10) as sensor of PG-CAS system. As the countermeasure is intermittently turned on in case of EM attack which reduces lower overall-power/energy overhead w.r.t the state-of-the-art. Switching between the power nodes have been incorporated by standard power-gates. Capacitors are implemented using DCAP cells from digital library and placed and routed entirely through industry-standard commercial tool (Synopsys Design Compiler for synthesis and Cadence Innovus for Place & Route). Hence, entire design is synthesizable barring the amplifier.

V. SIMULATION RESULTS

This section presents the post-layout based simulation results of the proposed PG-CAS system. Fig. 11 shows the implemented layout of the PG-CAS system. The simulation results demonstrate the operating principle as described in the previous section and are presented as follows: 1) sensitivity analysis of the PG-CAS structure; 2) design analysis of the proximity to capacitance conversion circuits; and 3) probe detection and countermeasures. The PG-CAS structure simulation was computed and verified via Ansys Maxwell, and the proximity to capacitance conversion circuits and detection simulations were computed and verified via *Spectre*^{TM}

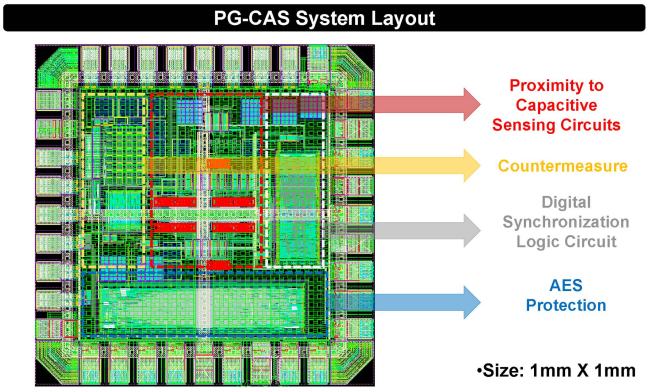

FIGURE 11. Implemented layout of PG-CAS system.

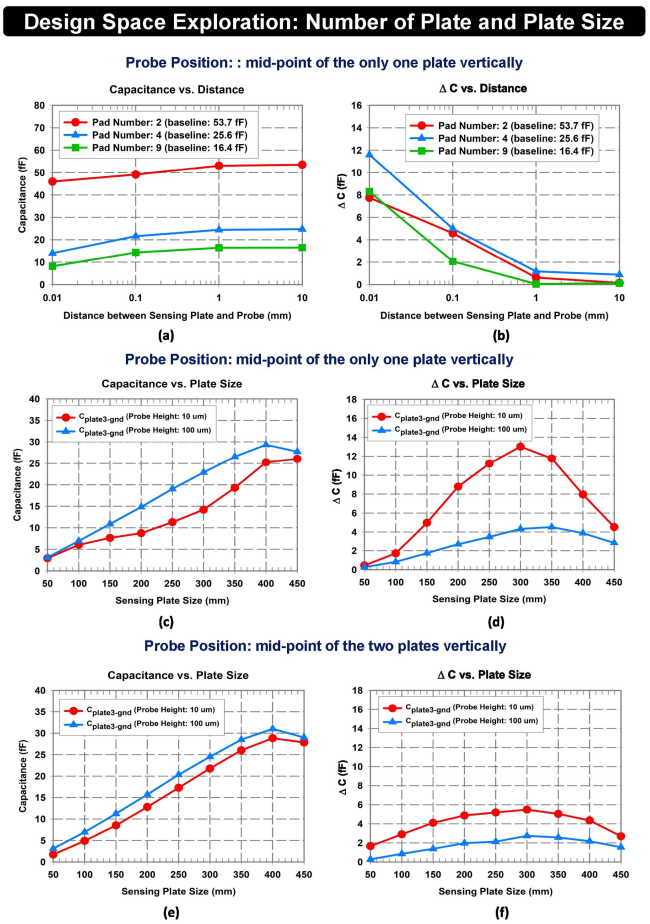

FIGURE 12. Design space exploration to analyze the number of plate and plate size of PG-CAS (a) capacitance change of PG-CAS with respect to the number of plate, (b) deviation in capacitance (ΔC) with respect to the number of plate, (c) capacitance change rate of PG-CAS with respect to plate size (probe Position: mid-point of the only one plate vertically), (d) deviation in capacitance (ΔC) with respect to plate size (probe Position: mid-point of the only one plate vertically), (e) capacitance change of PG-CAS with respect to plate size (probe Position: mid-point of the two plates vertically) and (f) capacitance change rate of PG-CAS (probe Position: mid-point of the two plates vertically).

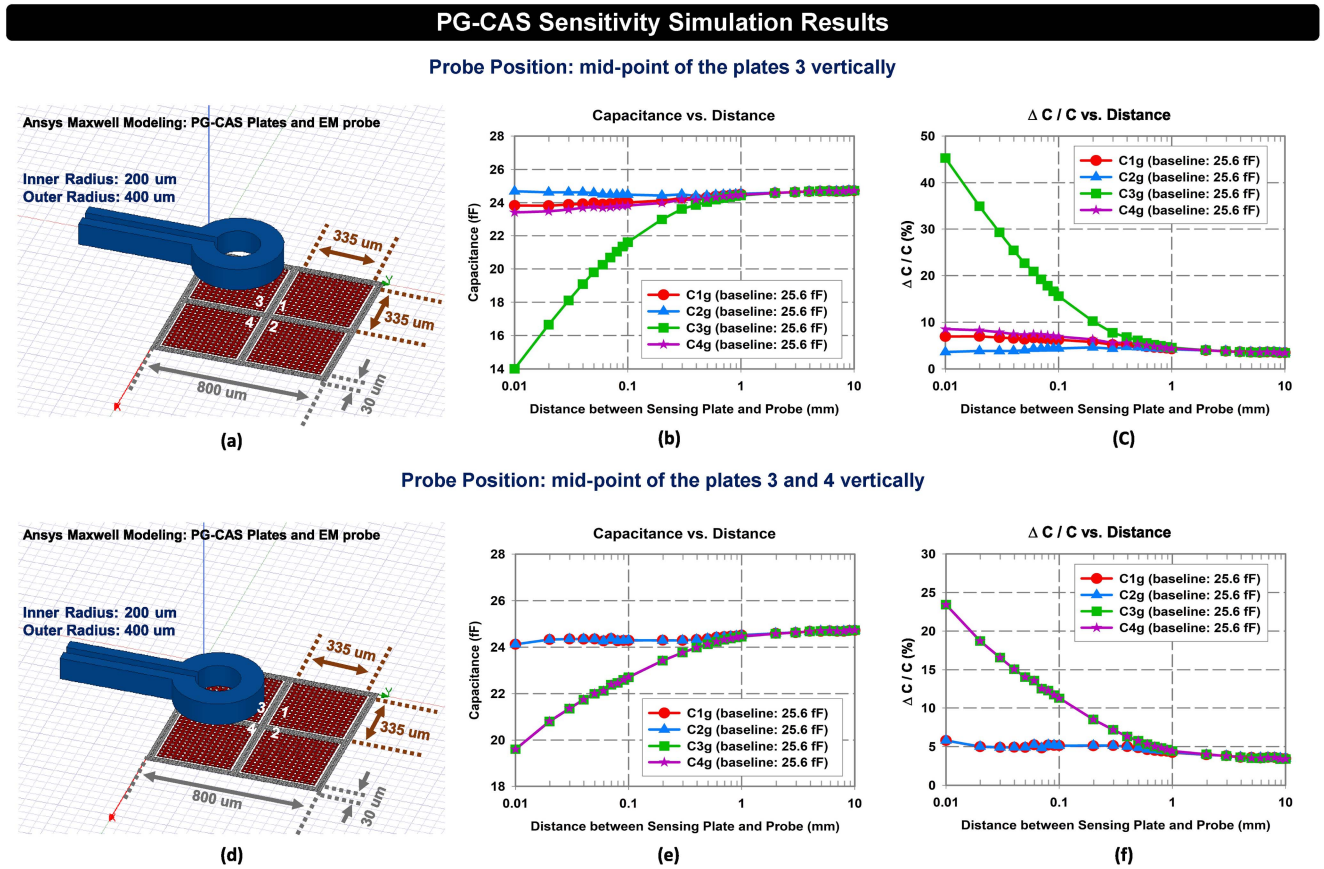

FIGURE 13. Simulation results of attack detection sensor (PG-CAS) with respect to distance between sensing plates and EM probe (a) PG-CAS simulation modeling in Ansys Maxwell: probe position on the mid-point of plates 3 vertically, (b) capacitance change of PG-CAS, (c) capacitance change rate of PG-CAS, (d) PG-CAS simulation modeling in Ansys Maxwell: probe position on the mid-point of plates 3 and 4 vertically, (e) capacitance change of PG-CAS and (f) capacitance change rate of PG-CAS.

using TSMC 65nm technology. All the simulations are post-layout parasitic extracted simulation which closely replicates actual IC implementation.

A. SENSITIVITY OF PG-CAS

Fig. 12 shows the design space exploration to analyze the number of plate and plate size of PG-CAS. To find the optimal pairs of sensing plate, various situations were applied to the simulation by changing the number of sensing plate (Fig. 12(a) and (b)). This simulation was carried out to examine the values and variations of capacitance as the number of sensing plates varied, respectively 2, 4, and 9 plates, with an EM probe vertically approaching the mid-point of one of the plates selected from the multiple plates. Fig. 12(a) show the simulated capacitance values of the PG-CAS structure as the EM probe approached the sensing plates. When the number of sensing plates is increased within a limited size (1mm $\times$ 1mm, in this case), the dimension of the sensing plates is reduced due to the decrease in the formation of electric field lines with the patterned-ground plane. The deviation in capacitance (ΔC) reached its maximum when the number of pairs to be 4 as shown in Fig. 12(b). Based on this result, the maximum sensitivity of PG-CAS can be determined, and the number of plates are 4.

To find the optimal sensing plate size, various situations were applied to the simulation by changing the sensing plates and patterned-ground. The EM probe approached the mid-point of the only one plate vertically (Fig. 12(c) and (d)), and the mid-point of the two plates vertically (Fig. 12(e) and (f)). From this simulation results, we can confirm the following: 1) As the sensing plate size increased, the simulated capacitance values of PG-CAS increase up to a certain point, and then decrease thereafter (Fig. 12(c) and (e)). 2) The deviation in capacitance (ΔC) reached its maximum at a specific plate size (Fig. 12(d) and (f)). Based on this result, the maximum sensitivity of PG-CAS can be determined, and a plate size of 335μm and the patterned-ground size of length and width is 800μm and 30μm has been identified, respectively. It is effective for the PG-CAS system to cover the entire area of the chip. If only a portion of the chip is covered, there is a possibility that it may not detect or detect late for the probe approaching from the uncovered area.

Fig. 13 shows the simulation results of the PG-CAS structure. The purpose of this simulation is to observe how the EM probe affects the change in the capacitances as we explained in Section III. As shown in Fig. 13(a), the EM probe approached the mid-point of plate 3 vertically. Fig. 13(b) shows the simulated capacitance values of the

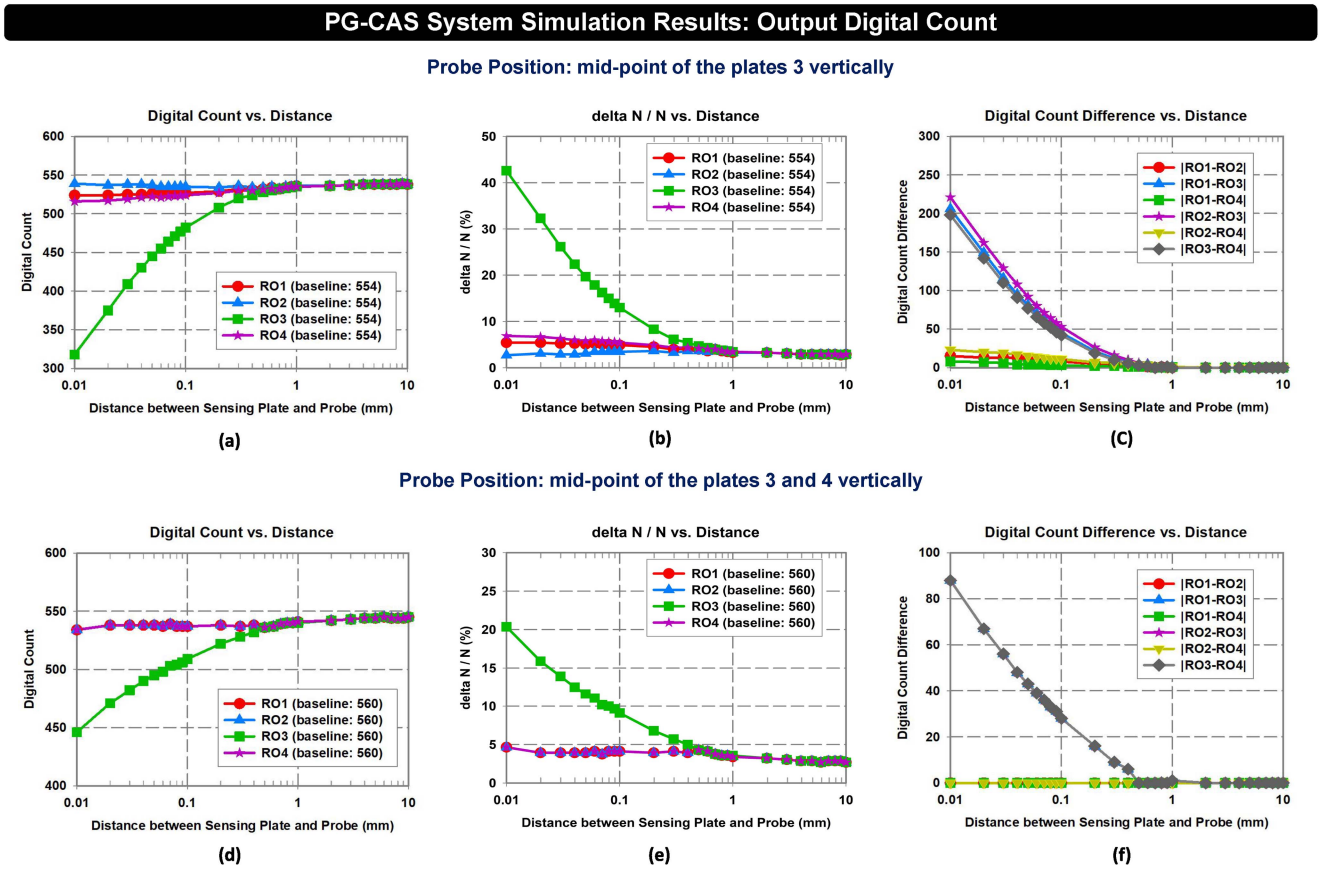

FIGURE 14. Simulation results of attack detection circuit with respect to distance between sensing plates and EM probe (a) digital count change of PG-CAS system: probe position on the mid-point of plates 3 vertically, (b) digital count change rate of PG-CAS system, (c) digital count difference between each counter, (d) digital count change of PG-CAS system: probe position on the mid-point of plates 3 and 4 vertically, (e) digital count change rate of PG-CAS system, (f) digital count difference between each counter.

PG-CAS structure as the EM probe approaches the sensing plates. In the absence of the EM probe, C1g, C2g, C3g, and C4g (baseline capacitance between each plates and patterned-ground, respectively) are measured to be were 25.6 fF. When the EM probe approached, C3g reduces due to the coupling effect of the EM probe. As the distance between the sensing plates and EM probe becomes <0.1 mm, a capacitance change of >45% is observed, while at a distance of 0.6 mm or shorter, the capacitance diverges by >6% compared to the baseline EM probe cases as shown in Fig. 13(c). Fig. 13(d) shows the EM probe approached the mid-point of plates 3 and 4 vertically. The sensing plate size of each plate and the patterned-ground size of length and width are the same conditions. Fig. 13(e) shows the simulated capacitance values of the PG-CAS structure as the EM probe approaches the sensing plates. The capacitance value of C2g and C4g is the same as C1g and C3g due to the probe position. When the EM probe approached, C3g reduces due to the coupling effect of the EM probe. As the distance between the sensing plates and EM probe becomes <0.1 mm, a capacitance change of >11% is observed, while at a distance of 0.5 mm or shorter, the capacitance diverges by >5% compared to the baseline EM probe cases as shown in Fig. 13(f). Subsequently, the results imply that using capacitive asymmetry, the EM probe approaching can be detected as C1g, C2g, C4g, and C3g diverges from their baseline capacitance due to asymmetry in probe positioning with respect to the pads.

B. PG-CAS SYSTEM

Fig. 14 shows the post-layout simulation results of the PG-CAS system attack detection circuits. The purpose of this simulation was to verify the capacitance value is converted to a digital number for post-processing and to determine how the circuit can detect the attack when an EM probe approaches PG-CAS plates. By using switched-capacitor network, changed capacitance as EM probe approaching converts output frequency of current-starved ring-oscillator and is fed to digital logic circuit. The transient full-system post-layout SPICE simulation were performed with proximity to capacitance conversion circuit and digital logic synchronization circuit to check if countermeasure is turned on appropriately. In the case of the PG-CAS system, the probe approaches the mid-point of plate 3, similar to Fig. 13(a). Fig. 14(a) shows the simulated digital count of PG-CAS system as the EM probe approaches the sensing plates. In the absence of the EM probe, the digital count of each output is counted to be constant (e.g., 554 in 10 us, at nominal corner). When the EM probe approached, the digital count of

RO3 (connected with plate 3) reduces since the capacitance between the plate 3 and patterned-ground plane (C3g) is reduced. As the distance between the sensing plates and EM probe becomes <0.1 mm, a maximum change of >42% in counted number is observed. Maximum change is observed while being at a distance of 0.5 mm or shorter, the digital count diverges by >4% compared to the baseline EM probe cases as shown in Fig. 14(b). 14(c) shows the digital count difference between each counter. When the EM probe is close to plate 3, the digital count difference between RO3 and RO1, RO2, and RO4 is increased.

In the case of the PG-CAS system, the probe approaches the mid-point of plate 3, similar to Fig. 13(d). Fig. 14(d) shows the simulated digital count of the PG-CAS system as the EM probe approaches the sensing plates. In the absence of the EM probe, the digital count of each output is counted to be were 560. When the EM probe approached, the digital count of RO3 (connected with plate 3) reduces since the capacitance between the plate 3 and patterned-ground plane (C3g) is reduced. The digital count of RO2 and RO4 is the same as RO1 and RO3 due to the probe position. As the distance between the sensing plates and EM probe becomes <0.1 mm, a digital count change of >20% is observed, compared to the baseline EM probe cases as shown in Fig. 14(e). Fig. 14(f) shows counter output difference between each counter. When the EM probe is close to plates 3 and 4, the counter output difference between RO3 and RO1 is increased. The results clearly imply that using the PG-CAS system, the approaching the EM Probe can be detected.

C. PROBE DETECTION & COUNTERMEASURES

Fig. 15 shows an EM SCA detection. Since the proposed PG-CAS system operate the proximity to capacitance conversion circuit intermittently at < 1% duty-cycle, the time-frame is significantly important to detect an attack and turn on countermeasures. The time gap between an EM probe approaching and turning on countermeasure is only 2.99 μs, making the PG-CAS system possible to operate the proximity to capacitance conversion circuit intermittently at < 1% duty-cycle even though the attack is performed random time frame. One important point to note that any practical attack is not possible in this short period of time making the solution practical even in commercial low-power edge applications.

D. SENSITIVITY OF PG-CAS SYSTEM WITH NON-IDEAL EFFECTS

Various non-ideal effects can affect the sensing plate and proximity to capacitance conversion circuit of the PG-CAS system. 1) The sensor capacitance and subsequent range of oscillation are both sensitive to process variation. 2) The voltage gain of the switched-capacitor circuit highly depends on the matching between C_f and C_{Ng} (Fig. 7) as well as the parasitics at the input. 3) the noise of each circuit can certainly affect sensitivity. However, the PG-CAS system focuses on relative value of capacitance rather than absolute value. The

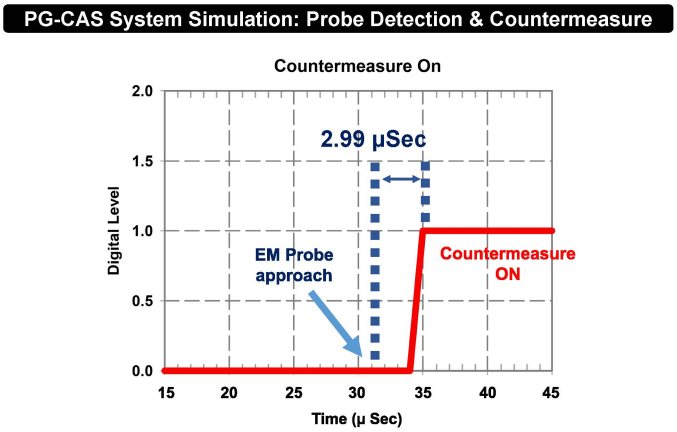

FIGURE 15. EM SCA detection and countermeasure turn-on time.

capacitance changes caused by an approaching probe are converted into frequency change by the proximity to capacitance conversion circuit. The digital count from the output oscillation frequency of the current-starved ring-oscillator are fed to a digital subtractor, which calculates the difference between the digital count occurring on each counter. Furthermore, the digital count is calibrated by the baseline capacitance, even when the capacitance changes. Thus, even though the absolute value of capacitance may change due to process variation, the change is already compensated through the calibration process. This represents another advantage of the PG-CAS system.

VI. CONCLUSION

This paper presents the design and analysis of an EM SCA detection system utilizing PG-CAS sensing structure and circuit to detect variations in the EM field caused by an approaching EM probe. The PG-CAS system for approaching probe consists of the EM SCA detection sensor plate and circuits. The EM SCA detection sensor that can sense an EM probe approaching due to the breaking of the symmetry of the plate-ground capacitance pair system was implemented in a grid of four metal plates of the same size at the top metal layer and a patterned-ground plane at a lower metal. The EM SCA detection circuit comprises of proximity to capacitance conversion circuits that can detect the change in capacitance between the plates and patterned-ground Plane, digital synchronization logic circuits that determine the operation of EM SCA circuit-level countermeasure through the detected attack, and operate the proximity to capacitance conversion circuit intermittently at < 1% duty-cycle leading to reduced power consumption, and integration of AES protection with sense. When an attack is detected, AES protection is turned on based on the detection signal. The PG-CAS system 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 > 42% deviation from the without attack. PG-CAS provides a 3.9× improvement for a detection range of 0.1 mm, compared to

TABLE 1. Simulated performance summary of the comparison table.

Parameter		This work (Post-layout Simulation)				[5], [6] (Measurement)
		Probe Position: Plate 3		Probe Position: Plates 3 & 4		
Sensing Method		PG-CAS (Patterned-Ground Co-planar Capacitive Asymmetry Sensing)				Inductive Sensing
Circuit Technique		Switched-Capacitor + Digital Logic				LC-Oscillator + Digital Logic
Sensing Percentage Change @ probe distance	0.01 mm	45.29 %	>5.9× ②	23.44 %	>3.0× ②	7.59 %
	0.1 mm	15.59 %	>3.9× ②	11.32 %	>2.8× ②	3.91 %
	0.5 mm	6.12 %	-	5.78 %	-	0.09 %
Digital Count Change @ probe distance	0.01 mm	42.59 %	-	20.36 %	-	-
	0.1 mm	12.99 %	-	9.10 %	-	-
	0.5 mm	4.69 %	-	4.29 %	-	-
Maximum Detection Range		0.5 mm				0.1 mm
Power Consumption		0.67 uW (1% duty cycle)				20 uW (1% duty cycle)

the prior work on inductive sensing as shown in Table 1. This intermittent PG-CAS circuit operation consumes 0.67 μW of power, which is much lower ($\sim 29\times$) compared to the prior work (Table 1). 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 counter-measure can be turned on, reducing the power overheads significantly.

Future works will involve fabricating a semiconductor chip for evaluating the proposed PG-CAS system. Several factors need to be considered during the design process. 1) It is imperative to verify the impact of capacitance resulting from metal filling, which is one of the pivotal steps in the semiconductor fabrication process. 2) In order to perform measurements, if the IC chip is to be mounted onto a PCB substrate, the design should take into account the capacitance resulting from wire-bonding.

REFERENCES

[1] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—Channel(s)," in *Proc. CHES*, Aug. 2002, pp. 29–45.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. CRYPTO*, 1999, pp. 388–397.

[3] J.-J. Quisquater and D. Samyde, "ElectroMagnetic analysis (EMA): Measures and counter-measures for smart cards," in *Proc. Smart Card Program. Security*, 2001, pp. 200–210.

[4] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. CRYPTO*, Aug. 1996, pp. 104–113.

[5] N. Miura et al., "A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor," in *Proc. VLSI Dig. Papers*, 2014, pp. 1–2.

[6] N. Homma et al., "EM attack is non-invasive? Design methodology and validity verification of EM attack sensor," in *Proc. CHES*, 2014, pp. 1–16.

[7] D. Ishihata et al., "Enhancing reactive countermeasure against EM attacks with low overhead," in *Proc. IEEE Int. Symp. Electromagn. Compat. Signal/Power Integrity (EMCSI)*, 2017, pp. 399–404.

[8] D. D. Hwang et al., "AES-based security coprocessor IC in 0.18μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[9] A. Poschmann, A. Moradi, K. Khoo, C.-W. Lim, H. Wang, and S. Ling, "Side-channel resistant crypto for less than 2,300 GE," *J. Cryptol.*, vol. 24, no. 2, pp. 322–345, Apr. 2011.

[10] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers*, 2009, pp. 64–65.

[11] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 10, pp. 3300–3311, Oct. 2018.

[12] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *Proc. IEEE HOST*, 2017, pp. 62–67.

[13] R. Kumar et al., "A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4k crypto-processor in 14-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 56, no. 4, pp. 1141–1151, Apr. 2021.

[14] M. Wang et al., "Physical design strategies for mitigating fine-grained electromagnetic side-channel attacks," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2021, pp. 1–2.

[15] D. Das et al., "27.3 EM and power SCA-resilient AES-256 in 65nm CMOS through >350x current-domain signature attenuation," in *Proc. IEEE ISSCC*, 2020, pp. 1–3.

[16] D. Das et al., "EM and Power SCA-resilient AES-256 through >350x current domain signature attenuation & local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2021.

[17] A. Singh et al., "Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO," *IEEE J. Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, Feb. 2020.

[18] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis," in *Proc. IEEE HOST*, 2019, pp. 11–20.

[19] R. Kumar et al., "A 7Gbps SCA-resistant multiplicative-masked AES engine in Intel 4 CMOS," in *Proc. IEEE Symp. VLSI Technol. Circuits*, 2022, pp. 138–139.

[20] D. Das, M. Nath, S. Ghosh, and S. Sen, "Killing EM side-channel leakage at its source," in *Proc. IEEE MWSCAS*, 2020, pp. 1108–1111.

[21] D. Das, J. Danial, A. Golder, S. Ghosh, A. R. Wdhury, and S. Sen, "Deep learning side-channel attack resilient AES-256 using current domain signature attenuation in 65nm CMOS," in *Proc. IEEE CICC*, 2020, pp. 1–4.

[22] D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "EM/Power side-channel attack: White-box modeling and signature attenuation countermeasures," *IEEE Design Test*, vol. 38, no. 3, pp. 67–75, Jun. 2021.

[23] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-STELLAR: An EM/power SCA-resilient AES-256 with synthesis-friendly signature attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2022.

[24] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "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 *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, vol. 64, 2021, pp. 499–501.

[25] R. Kumar et al., "A 435MHz, 2.5Mbps/W side-channel-attack resistant crypto-processor for secure RSA-4k public-key encryption in 14nm CMOS," in *Proc. IEEE Symp. VLSI Circuits*, 2020, pp. 1–2.

[26] A. Ghosh, M. Nath, D. Das, S. Ghosh, and S. Sen, "Electromagnetic analysis of integrated on-chip sensing loop for side-channel and fault-injection attack detection," *IEEE Microw. Wireless Compon. Lett.*, vol. 32, no. 6, pp. 784–787, Jun. 2022.

[27] A. Ghosh, D. Das, S. Ghosh, and S. Sen, "EM SCA & FI self-awareness and resilience with single on-chip loop & ml classifiers," in *Proc. Design, Autom. Test Europe Conf. Exhibition (DATE)*, 2022, pp. 592–595.

[28] D. H. Seo et al., "Enhanced detection range for EM side-channel attack probes utilizing co-planar capacitive asymmetry sensing," in *Proc. Design, Autom. Test Europe Conf. Exhibition (DATE)*, 2021, pp. 1016–1019.

[29] D.-H. Seo, M. Nath, D. Das, S. Ghosh, and S. Sen, "Improved EM side-channel analysis attack probe detection range utilizing co-planar capacitive asymmetry sensing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, early access, Jan. 6, 2023, doi: 10.1109/TCAD.2022.3227077.

[30] A. Ghosh, D.-H. Seo, D. Das, S. Ghosh, and S. Sen, "A digital cascoded signature attenuation countermeasure with intelligent malicious voltage drop attack detector for EM/power SCA resilient parallel AES-256," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2022, pp. 1–2.

[31] J. T. Kung, H.-S. Lee, and R. T. Howe, "A digital readout technique for capacitive sensor applications," *IEEE J. Solid-State Circuits*, vol. 23, no. 4, pp. 972–977, Aug. 1988.

[32] J. Zhang, J. Zhou, and A. Mason, "Highly adaptive transducer interface circuit for multiparameter microsystems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 1, pp. 167–178, Jan. 2007.

[33] B. Chatterjee et al., "A wearable real-time CMOS dosimeter with integrated zero-bias floating-gate sensor and an 861nw 18-bit energy-resolution scalable time-based radiation to digital converter," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2019, pp. 1–4.

[34] B. Chatterjee et al., "A wearable real-time CMOS dosimeter with integrated zero-bias floating gate sensor and an 861-nw 18-bit energy-resolution scalable time-based radiation to digital converter," *IEEE J. Solid-State Circuits*, vol. 55, no. 3, pp. 650–665, Mar. 2020.

[35] D. H. Seo, B. Chatterjee, S. M. Scott, D. J. Valentino, D. Peroulis, and S. Sen, "Design and analysis of a resistive sensor interface with phase noise-energy-resolution scalability for time-based resistance to digital converter," *Front. Electron.*, vol. 3, Apr. 2022, Art. no. 92326.