Electromagnetic Analysis of Integrated On-Chip Sensing Loop for Side-Channel and Fault-Injection Attack Detection

Archisman Ghosh, *Graduate Student Member, IEEE*, Mayukh Nath, *Student Member, IEEE*, Debayan Das, *Member, IEEE*, Santosh Ghosh, *Member, IEEE*, and Shreyas Sen, *Member, IEEE*

***Abstract*— Securing crypto-cores is becoming increasingly difficult with the advent of electro-magnetic (EM) side-channel analysis (EMSCA) and fault injection attacks (FIAs). This letter presents an Ansys high-frequency structure simulator (HFSS)-based simulation framework for EM analysis of an integrated on-chip sensor for detecting EMSCA and FIA and validates the efficacy of an on-chip higher metal layer loop-based zero area-overhead sensor using a custom-built 65-nm CMOS IC. A simple technique for incoming H-probe detection is also presented by measuring the absolute average of the induced voltage for every encryption.**

***Index Terms*— Electro-magnetic (EM) analysis-based framework, EM probe detection, fault injection detection, glitch attack detection, on-chip sensor.**

I. Introduction

COMPUTATIONALLY secure cryptographic algorithms leak meaningful information in terms of electro-magnetic (EM) emanations, which can compromise the security of modern Internet of Things (IoT) devices such as smart cards, smartwatches, personal computers, and mobiles. It has been recently demonstrated that data can be easily snooped from a distance by simply using a cheap EM probe [1]. Moreover, techniques such as differential fault attacks (DFAs) [2] can potentially deduce sensitive data through glitch injection. Both fault injection attacks (FIAs) and EM side-channel attack (EMSCA) have been extremely popular due to their simplicity and low cost. Several circuit-level countermeasures for EMSCA [3]–[6], attack detection circuit for approaching probe [7], and FIA detection architectures [8], [9] have been recently explored. Recently, capacitive asymmetry sensing-based EM probe detection has become very popular [10], [11]. However, these letters did not explore inductive sensor-based approach. In this letter, we present an on-chip sensing loop through analysis using EM simulations & verification by measurement of: 1) coupling of transistor switching activity with higher-level metal layers & effect of FIA in the same and 2) change of the coupling in the presence of an approaching probe.

The contributions are threefold to tackle the abovementioned points: 1) Formulating an EM analysis flow by importing an example digital circuit layout using TSMC 65-nm library to Ansys high-frequency structure simulator (HFSS); 2) EM Analysis & simulation results to prove the efficacy of on-chip loop as sensor against power glitch-based FIA, as well as EMSCA by detecting approaching H-probe; and 3) measurement results from a custom IC fabricated in TSMC 65-nm process with an AES-256 encryption engine and an on-chip loop to demonstrate real-life examples of using the on-chip loop sensor for FIA and EMSCA detection, supporting the analysis and simulation results. An inductive loop along with machine learning-based system is explored and presented earlier [12] to detect approaching H-probe. This work does the EM analysis to prove the efficacy of higher metal layer loop as attack sensor against both EM side-channel analysis (EMSCA) and fault injection analysis (FIA). Moreover, a much simpler approach (by detecting higher absolute mean of induced voltage) has led to detect the approaching probe accurately.

II. Concepts and EM Analysis Flow

Modern crypto co-processors are implemented using CMOS technology. The movement of charges due to transistor switching activity creates time-varying electric field ($\mathbf{E}$). This, in conjunction with the oscillating currents ($\mathbf{J}$) in the metal layers, results in a time-varying magnetic field ($\mathbf{H}$) consistent with the well-known Maxwell's relation $\nabla \times \mathbf{H} = \mathbf{J} + \epsilon \partial_t \mathbf{E}$, where ϵ is the electric permittivity of the surrounding media. Now, if a metal loop is placed in the higher metal layers, the time-variant magnetic flux generated due to CMOS switching induces an electric field ($\mathbf{E}_l$) across the length of the loop as given by Faraday's law $\nabla \times \mathbf{E}_l = -\mu \partial_t \mathbf{H}$, where μ denotes magnetic permeability. We propose that due to its proximity to the crypto co-processor, such a higher metal-layer on-chip loop should be highly sensitive to the dynamics of CMOS circuit operations and be able to detect sudden changes in temporal behavior.

Fig. 1 shows an overview of the on-chip loop. As shown in Fig. 1(a), time-varying EM fields due to switching activity of the digital circuit ($V_{\text{switching}}$) induces an electromotive force in the on-chip loop in metal, creating an oscillating voltage pattern (V_{loop}). A transfer function (TF) can be defined by $\text{TF} = V_{\text{loop}}/V_{\text{switching}}$, giving $V_{\text{loop}} = \text{TF} \times V_{\text{switching}}$. Voltage

Manuscript received February 28, 2022; accepted March 15, 2022. This work was supported in part by NSF under Grant CNS 17-19235 and in part by Intel Corporation. *(Corresponding author: Archisman Ghosh.)*

Archisman Ghosh, Mayukh Nath, and Shreyas Sen are with the Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: ghosh69@purdue.edu; nathm@purdue.edu; shreyas@purdue.edu).

Debayan Das and Santosh Ghosh are with Intel Corporation, Hillsboro, OR 97124 USA (e-mail: das60@purdue.edu; santosh.ghosh@intel.com).

This article was presented at the IEEE MTT-S International Microwave Symposium (IMS 2022), Denver, CO, USA, June 19–24, 2022.

Color versions of one or more figures in this letter are available at https://doi.org/10.1109/LMWC.2022.3161001.

Digital Object Identifier 10.1109/LMWC.2022.3161001

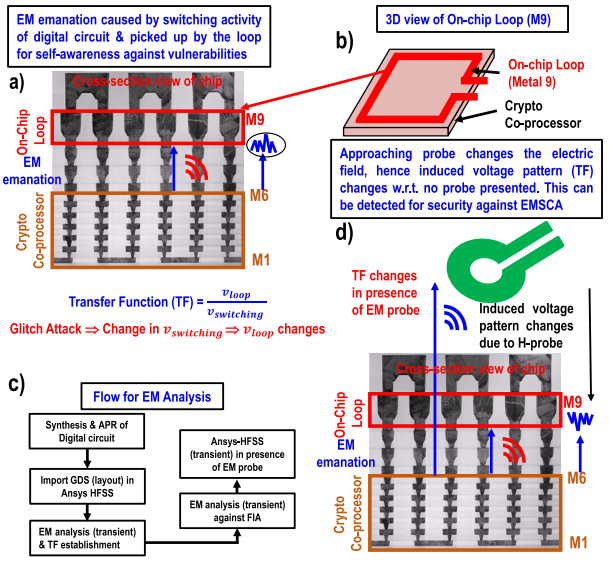

Fig. 1. (a) EM emanation caused by switching activity of crypto co-processor and received by a metal 9 on-chip loop can be used for awareness of presence of suspicious body to sneak the data. Voltage glitch can be detected by seeing induced voltage pattern in the loop. (b) Three-dimensional view of on-chip loop on top of crypto co-processor. (c) Flow for EM analysis. (d) Presence of extra probe changes the induced voltage pattern.

glitch creates sudden drop in V_{DD} reducing switching activity of the circuit. Here, change in $V_{\text{switching}}$ causes a change in induced V_{loop}. This is the reason behind malfunctioning of the circuit for a very small time and this idea is the core of DFA [2]. Fig 1(b) shows a conceptual 3-D view of the crypto co-processor with on-chip loop. A brief flow of EM analysis is presented in Fig. 1(c).

Furthermore, when an external EM probe (intending to perform EMSCA) is brought in close proximity to the system, the probe disturbs the EM fields generated from the CMOS switching. This fact can be exploited to detect EMSCA attacks using the same on-chip loop. Fig. 1(d) presents a conceptual view of the IC in the presence of an H-field probe. The probe disturbs the local fields, hence modifying the TF itself, again causing a change in V_{loop} which can be sensed to detect EMSCA. It should be noted that this attack sensing technique is completely passive, no active component or excitation is required, which makes it energy-efficient.

III. Numerical Analysis and Results

For numerical analysis, layout of an AND gate is imported into Ansys HFSS [as shown in Fig. 2(a)] and a sinusoidal excitation is provided at the imported layout of gate to replicate the powering and switching in post-silicon verification. Parameterized resistors between source and drain are introduced to enable or disable individual transistors—low (short) and high (open) resistances resemble ON and OFF of transistor in the case of dynamic switching. The loop is implemented in metal 9 as shown in Fig. 2(b), and the induced voltage (V_{loop}) across it is measured to verify its functionality as a sensor.

A. EM Signature From FIA: Varying Input, Constant Transfer Function

Voltage glitch in FIA modifies CMOS switching activity ($V_{\text{switching}}$), causing a momentary reduction in induced voltage

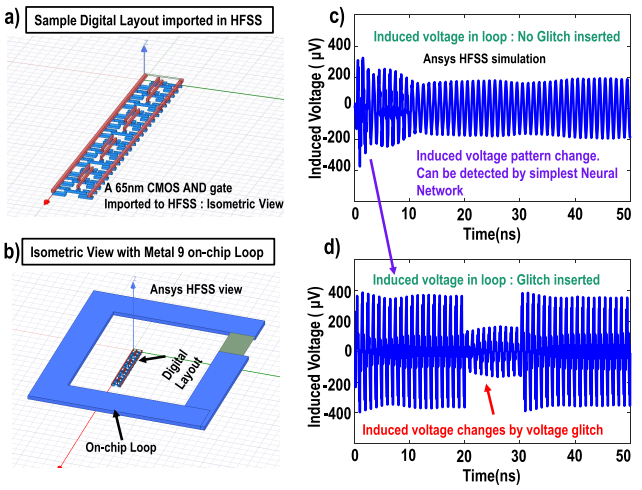

Fig. 2. (a) Imported AND gate layout in HFSS. (b) Isometric view of the AND layout with M9 loop. (c) Induced voltage in the loop in absence of voltage glitch. (d) Induced voltage in the loop in presence of voltage glitch.

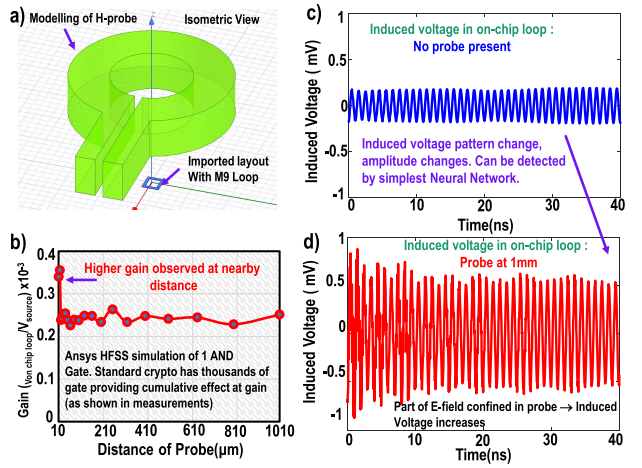

Fig. 3. (a) Modeling of EM probe in HFSS. (b) Gain changes with respect to distance. (c) Transient simulation of the on-chip with excitation in the digital AND gate. (d) Transient simulation as (c) in the presence of probe at 1-mm distance. (c) and (d) ensures induced voltage change in presence of on-chip loop which can be exploited to detect the approaching probe.

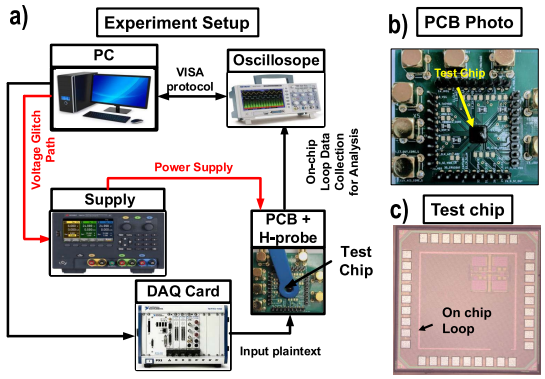

Fig. 4. (a) Experiment setup. (b) PCB photo. (c) Die micrograph.

V_{loop} [see Fig. 2(d)] from standard induced voltage pattern [see Fig. 2(c)]. Simulation results clearly show the difference in induced voltage pattern in absence and presence of voltage glitch [see Fig. 2(c) and (d)], which is used in detecting voltage glitch attack.

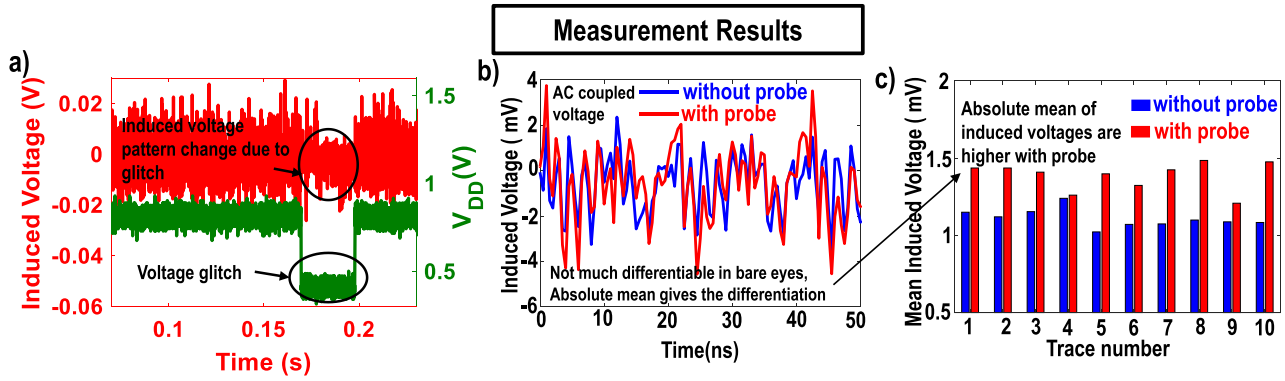

Fig. 5. Measurement results. (a) Voltage glitch-based FIA. (b) Time-domain measured waveform of induced voltage in loop in the presence and absence of EM probe. (c) Average of absolute trace in both in the presence and absence of an approaching probe showing the efficacy of detection.

B. EM Signature From Approaching Probe: Varying Transfer Function, Constant Input

To analyze the change in induced voltage pattern from an approaching probe, a commercially available H-field probe (Langer ICR HH100-27, diameter 100 μm) is modeled as shown in Fig. 3(a). It is observed that the voltage pattern changes with the distance of the probe from the IC. Higher gain is observed at a lower distance of probe from IC as shown in Fig. 3(b). Transient simulation from HFSS [see Fig. 3(c) and (d)] reaffirms the fact that a higher gain in V_{loop} is observed even if the probe is kept at 1-mm distance. This is due to the fact that part of the emanated fields are scattered and confined by the cylindrical structure of the probe, resulting into an increase in the induced voltage in the loop.

It should be noted that the induced voltage in the simulation results is in mV range—as only one gate is simulated for simplicity. However, the implemented encryption engine in the IC (parallel AES) has nearly ∼14 300 gates and superposition of all the gates generally contribute to higher induced voltage, as we will see in Section IV.

IV. Measurement Results

A. Measurement Setup

A 65-nm CMOS test-chip with parallel AES-256 encryption engine [13] is fabricated. Metal 9 of the IC is used to create the on-chip loop. Metal 9 is not used for routing of the circuit. Hence this detection sensor has zero area overhead. The test chip is integrated on a printed circuit board (PCB) with chip-on-board packaging. The IC consumes 0.78-mW power running at 50-MHz clock (provided by an external Arbitrary Wave Generator) at 0.8-V supply voltage.

Experimental setup is shown in Fig. 4(a). A computer controls a NI-DAQ card to send the input plaintexts through the scan-chain interface of the circuit. Moreover, a precisely configured power supply is used to inject glitch in V_{DD} of the chip. Voltage glitch of 0.4 V is used for voltage glitch attack. A 10-mm H-probe located at a distance of 1 mm is used for this experiment. Traces collected from the on-chip loop using a 400 Msps oscilloscope is sent to a PC for further processing. PCB photo and chip micrograph are shown in Fig. 4(b) and (c).

B. Measurement Results

Inserted glitch and induced voltage pattern are shown in Fig. 5(a). Amplitude of the induced voltage reduces at the time of the glitch injection.

Similarly, the induced voltage is measured by the above-mentioned setup both in presence and absence of H-probe. The voltage pattern is shown in Fig. 5(b). Although all the gates are contributing together in the leakage providing higher gain, there is another phenomenon that is counteracting this. Measurement noise creates difficulty in differentiating the probe's presence. However, an intelligent post-processing proves the fact as shown by simulation results. Ten traces are collected for both in the presence and in the absence of the probe. To avoid any ambiguity and to reduce the effect of noise, we have collected trace with the same input plaintext and same key. Also, each trace is collected by averaging 1000 same encryption (same plaintext and same key) for both the cases. Finally, the mean of absolute value of ac coupled voltage is calculated. Results are shown for each trace in bar graph of Fig. 5(c). This clearly shows higher induced voltage in presence of an EM probe.

V. Conclusion

This work presents an EM analysis of an integrated on-chip higher metal loop as sensor to detect: 1) FIA by utilizing the induced voltage pattern between switching gates and the loop sensor and 2) approaching probe for EMSCA, utilizing induced voltage change in the presence of an approaching probe. For the first time, the results from an integrated EM analysis framework of 3-D FEM HFSS analysis on an imported Cadence layout of CMOS transistors, are validated through measurements of a custom-IC, pave the path to identifying low-cost circuits that could be used for on-chip detection as a part of future work.

References

[1] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2002, doi: 10.1007/3-540-36400-5_4.

[2] M. Tunstall *et al.*, "Differential fault analysis of the advanced encryption %standard using a single fault," in *Proc. Int. Workshop Inf. Secur. Theory Practices*, 2011, pp. 224–233.

[3] D. Das *et al.*, "EM and power SCA-resilient AES-256 in 65nm CMOS through >350× current-domain signature attenuation," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2020, pp. 424–426.

[4] 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 Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2019, pp. 11–20.

[5] 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 *IEEE ISSCC Dig. Tech. Papers*, Feb. 2021, pp. 499–501.

[6] A. Ghosh, D. Das, J. Danial, V. De, 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. CICC*, Oct. 2022, pp. 1–2.

[7] N. Miura, D. Fujimoto, M. Nagata, N. Homma, Y. Hayashi, and T. Aoki, "EM attack sensor: Concept, circuit, and design-automation methodology," in *Proc. 52nd Annu. Design Autom. Conf.*, Jun. 2015, pp. 1–6.

[8] L. Zussa *et al.*, "Efficiency of a glitch detector against electromagnetic fault injection," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2014, pp. 1–6.

[9] M. Doulcier-Verdier, J.-M. Dutertre, J. Fournier, J.-B. Rigaud, B. Robisson, and A. Tria, "A side-channel and fault-attack resistant AES circuit working on duplicated complemented values," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2011, pp. 274–276.

[10] D.-H. Seo, M. Nath, D. Das, B. Chatterjee, S. Ghosh, and S. Sen, "PG-CAS: Patterned-ground co-planar capacitive asymmetry sensing for mm-range EM side-channel attack probe detection," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Daegu, South Korea, May 2021, pp. 1–5, doi: 10.1109/ISCAS51556.2021.9401580.

[11] D.-H. Seo, M. Nath, D. Das, S. Ghosh, and S. Sen, "Enhanced detection range for EM side-channel attack probes utilizing co-planar capacitive asymmetry sensing," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Grenoble, France, Feb. 2021, pp. 1016–1019, doi: 10.23919/DATE51398.2021.9474155.

[12] A. Ghosh *et al.*, "EM SCA & FI self-awareness and resilience with single on-chip loop & ML classifiers," in *Proc. IEEE/ACM*, Sep. 2022, pp. 1–4.

[13] 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.