A Multipole Approach Toward On-Chip Metal Routing for Reduced EM Side-Channel Leakage

Mayukh Nath, Debayan Das, *Member, IEEE*, and Shreyas Sen, *Senior Member, IEEE*

***Abstract*—With the proliferation of smart interconnected devices, the importance of securing computational data has increased manifold. While computational security layers like cryptographic algorithms protect against software-domain vulnerabilities, they cannot prevent leakage of electromagnetic (EM) fields from its parent device, hence compromising physical layer security. Most proposed methods of reducing EM side-channel leakage involve incorporating complex blocks into the design of an integrated circuit (IC). In this letter, we take an entirely novel stance, by borrowing fundamental concepts from multipole EM field decay and adapting the same for ICs by proposing a multipole routing approach. By building proof-of-concept scaled-up routing in PCBs, we demonstrate that unlike conventional dipole-style routing, metal layers incorporating higher-order multipoles result in a much faster-decaying side-channel leakage. Through detailed measurements, we infer guidelines toward optimizing the order of multipole needed to minimize side-channel leakage, thus enabling convenient implementation of physical layer security.**

***Index Terms*—Electromagnetic (EM) leakage, multipole routing, physical layer security, side-channel leakage.**

I. Introduction

COMPUTATIONAL security techniques such as cryptographic algorithms, while providing software-level protection against external attacks, do little to prevent leakage of critical "side-channel" information in the form of electromagnetic (EM) emissions [1], [2], power consumption [3], timing of encryption operations, and so on-from the physical integrated circuit (IC) device running the algorithm itself. Among these, EM side-channel analysis (SCA) has been one of the most prominent attacks on electronic devices [4]. EM SCA is performed by placing an EM probe noninvasively on top of an encryption device, picking up "side-channel" signals during its operation [5], and extracting the corresponding encryption key. The easy availability of low-cost EM probes raises security concerns for embedded devices [4], [5], and hence it is critical to develop low-overhead solutions to prevent EM SCA attacks.

Various approaches to prevent power and EM SCA attacks have been proposed including logic based [6], [7], algorithmic [8], and circuit based [9]–[11] solutions – most being clever work-arounds to prevent SCA despite the presence of EM leakage. A recent study revealed that EM leakage from ICs occurs predominantly through the higher metal layers [12], which due to their longer metal routings compared to lower metals, can "leak" EM fields more efficiently [13].

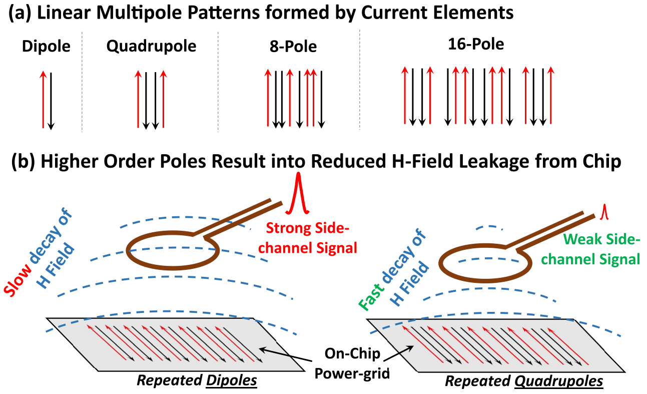
(a) Linear Multipole Patterns formed by Current Elements
Dipole
Quadrupole
8-Pole
16-Pole
(b) Higher Order Poles Result into Reduced H-Field Leakage from Chip
Slow decay of H Field
Strong Side-channel Signal
Fast decay of H Field
Weak Side-channel Signal
On-Chip Power-grid
Repeated Dipoles
Repeated Quadrupoles

Fig. 1. (a) Definition of linear current multipoles. (b) On-chip routing involving higher-order multipoles reduces side-channel H-field leakage.

Now, if current flowing through individual metal lines is viewed as individual current elements, the spatial arrangement of those elements in an IC metal layer would determine the characteristics of the EM field emitted from that layer. In this work, we extend this concept of the spatial arrangement of current elements by exploring specific arrangements of metal routings in the form of multipoles. More specifically, we investigate magnetic field leakage from different multipole-based routing patterns for IC power grid (supply, ground (V_{DD}, V_{SS}) routing), which is conventionally a high leakage layer [13]. By building proof-of-concept PCBs, we demonstrate for the first time the positive effect of multipole-based routing on reducing EM side-channel leakage as well as provide design guidelines toward choosing the right combination of multipoles in a real-life IC design. The proposed routing strategy is architecture agnostic, has zero additional area and power overheads, and can be implemented both independently and in tandem with any existing countermeasure technique to improve overall resistance to EM SCA.

II. Multipole Patterned On-Chip Routing

A. Definitions

Before we dive into the concept of multipole metal routing, a few key terminologies need to be explained.

Manuscript received February 20, 2021; accepted February 24, 2021. Date of publication March 1, 2021; date of current version June 7, 2021. This work was supported by the National Science Foundation (NSF) under Grant CNS 17-19235. *(Corresponding author: Shreyas Sen.)*

The authors are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: nathm@purdue.edu; shreyas@purdue.edu).

This article was presented at the IEEE MTT-S International Microwave Symposium (IMS 2021), Atlanta, GA, USA, June 6–11, 2021.

Color versions of one or more figures in this letter are available at https://doi.org/10.1109/LMWC.2021.3062809.

Digital Object Identifier 10.1109/LMWC.2021.3062809

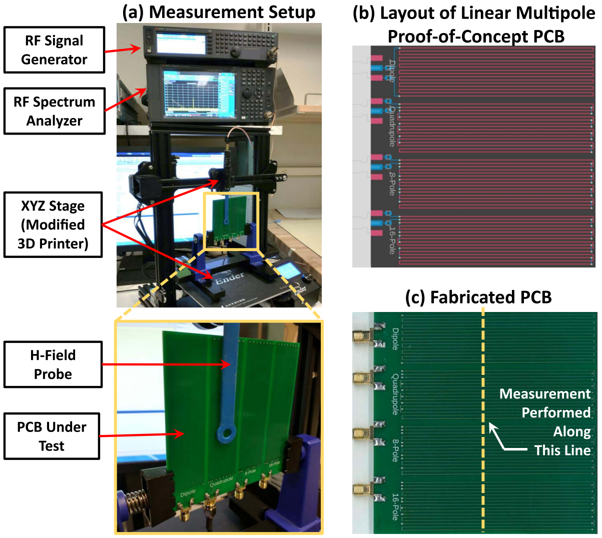

Fig. 2. (a) Measurement setup. The PCB is mounted on a modified 3-D printer, functioning as XYZ stage for H-field probe scanning. (b) Layout and (c) fabricated version of linear multipole routing PCB.

1) In the context of this letter, "multipole" elements are defined as *linear arrays* of current elements (as opposed to the usual planar array definition). This is done to best replicate on-chip routing on a single metal layer – more specifically power grid structures-where V_{DD} and V_{SS} metals are usually alternately placed parallel to each other. As shown in Fig. 1(a), two opposing current elements are defined as a dipole.
2) Two opposing dipoles form a quadrupole, two opposing quadrupoles form an 8-pole and so on [Fig. 1(a)].

B. Concept

Noting that the typical operation frequency of a commercial IC lies in the order of 1 GHz, the corresponding wavelength being 30 cm, we can assume that the magnetic field leakage from the IC would be magneto-quasi-static in nature, i.e., the dynamic parts of EM field equations could be ignored for analysis. With that in mind, H-field emanated from an infinitely long $n-$pole array would decay as

$$H \sim 1/d^{n}, \quad \text{for } d \gg a \tag{1}$$

where d is the vertical distance from an $n-$pole array, and a is the width of a single $n-$pole element in the array. As a result, leaked magnetic field would decay faster for a higher-order pole-based routing. As illustrated in Fig. 1(b): a quadrupole power-grid routing should result into a faster decaying H-field when compared to the conventional dipole routing. Faster decay would imply a lower EM side-channel signal picked-up by an H-field probe isodistant from the two chips, hence resulting in a more secure chip.

C. Proof-of-Concept Testing Methodology

To test the abovementioned concept of multipole routing, two different PCBs [Figs. 2(b) and 4(a)] are designed, representing different scaled-up version of on-chip routings. The relevant dimensions of the scaled-up PCBs are in the order of 10 mm, and the frequency of measurement is in turn scaled down to 100 MHz - to maintain quasi-static operation,

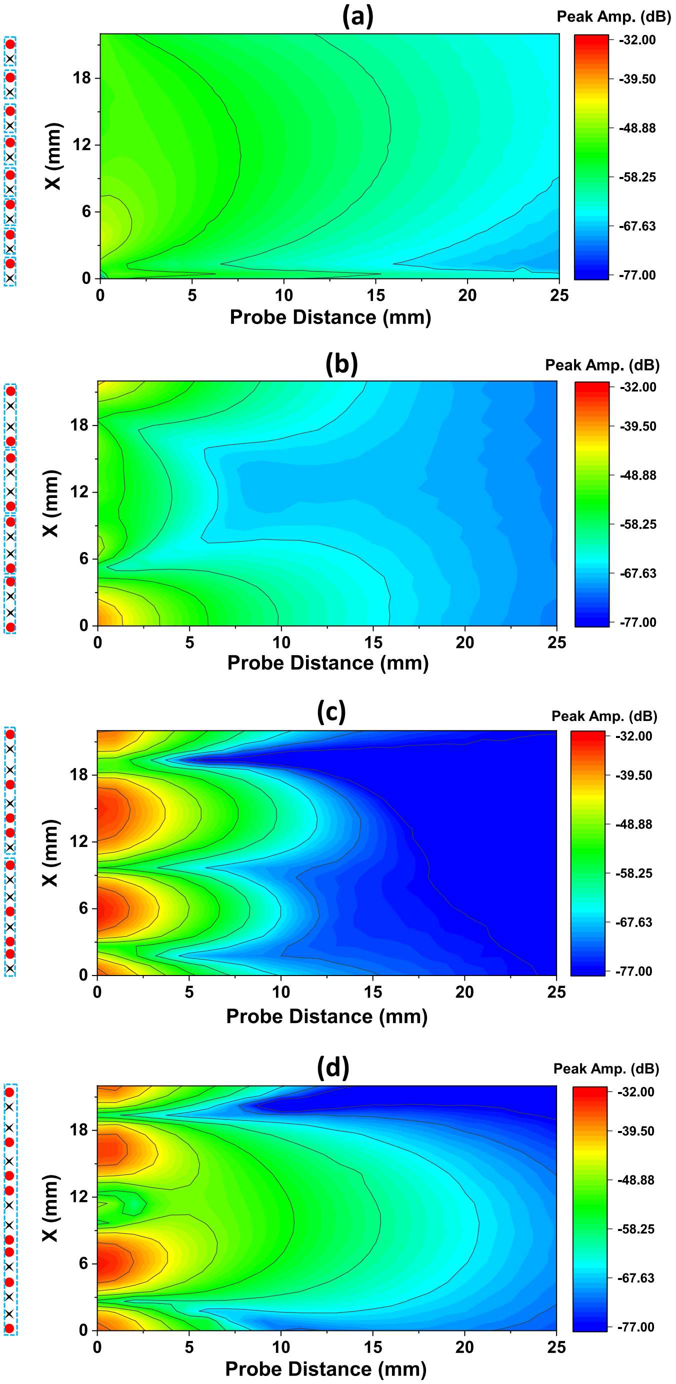

Fig. 3. Measured H-field decay with distance for different linear multipole configurations. (a) Dipole. (b) Quadrupole. (c) 8-Pole. (d) 16-Pole. Higher-order multipole exhibits faster decay far from the board, but stronger local fields up close to the board.

as would be the case for a ~1 mm × 1 mm chip operating at 1 GHz. The routings on the PCBs are terminated by 50-Ω resistors to maintain impedance matching with the RF test equipment. Excitation is provided as a sinusoidal wave at 100 MHz, 0 dBm - generated by a Keysight RF generator. To measure the leaked magnetic field, an H-field probe from Tekbox is used, in conjunction with a Keysight RF-spectrum analyzer. As shown in Fig. 2(a), a modified 3-D printer is used as a XYZ stage to scan the H-field probe over a test-PCB.

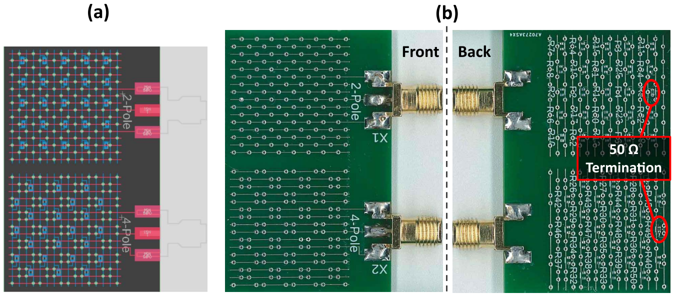

Fig. 4. (a) Layout and (b) fabricated versions of two-layer cross-grid stacked routing PCBs, featuring dipole and quadrupole configurations.

III. Experimental Results

Two different routing structures are tested to investigate the characteristics of multipole routing structures.

A. Ideal Linear Multipole Structures

First, to investigate the validity of (1) for finite linear n-poles, routing structures are designed representing ideal n-poles, for $n = 2, 4, 8, 16$ [Fig. 2(b) and (c)]. The routing for each n-pole comprises of a single meandering signal line, designed to represent linear n-poles as defined in Fig. 1(a). H-field probe signals are recorded at various distances from the routing, along the cross section line indicated in Fig. 2(c). The resulting heat-map is presented in Fig. 3. Two observations can be made immediately. *Firstly*, the field at probe distance of 25 mm clearly keeps falling as we move to higher-order poles from dipole till 8-pole. *Secondly*, fields close to the routing increase with the order of poles instead. This, in fact, would intuitively follow from (1), as the required condition for (1) to hold is $d \gg a$. Since the spacing between adjacent routing lines is kept fixed, the width of an n-pole element (a) keeps doubling for each doubling of n, while halving the number of individual elements in the n-pole array. For $n = 16$, the array has only one element, with $a \sim 22$ mm. So at $d = 25$ mm, $d \sim a$. Therefore, given a fixed d, as n is increased, the beneficial effect of multipole routing would disappear beyond a certain n due to an increase in the local fields.

B. Cross-Grid Structure

With the linear multipole cancellations validated, a more realistic two-layer cross-grid routing is designed akin to power-grid routings in ICs. With a cross-grid routing, the current flow between two points would get distributed or spread out and as a result, we would expect a somewhat diminished multipole canceling compared to the previous ideal uniform current cases. The designed cross-grid PCB is shown in Fig. 4(a) and (b). Two different variations are designed in this case, one with traditional alternate V_{DD} and V_{SS} grid structure (two-pole), whereas the second one using a quadrupole grid (four-pole) for the two layers. Provisions are kept for terminating the PCB at multiple places. For the present work, a single 50-Ω termination is made at the indicated locations in Fig. 4(b). Measurements are made at surfaces parallel to the grid routings, at two different probe distances. The resulting heat-map from measuring the cross-grid routings are presented in Fig. 5. From the results, we note that our two prior observations from the ideal linear multipole cases are replicated in the cross-grid case as well. For the dipole grid stack [Fig. 5(a)], a much slower field decay with probe distance is observed, compared to the quadrupole grid [Fig. 5(b)]. Further, a stronger local field magnitude is observed in the quadrupole case when the probe is closer.

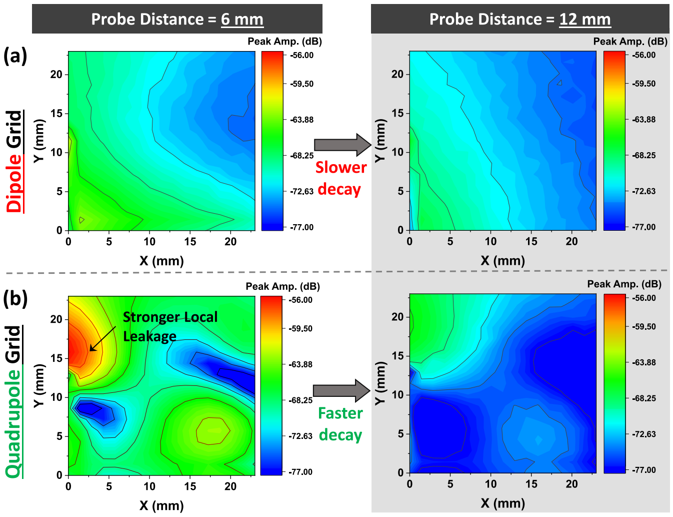

Fig. 5. H-field probe measurements on planes parallel to the cross-grid routings, and at 6- and 12-mm probe distances. (a) Dipole configuration displays a slower field decay versus distance with respect to quadrupole. (b) Quadrupole configuration shows faster field decay, but stronger local leakage close to the routing.

C. Proposed Design Considerations

The following section summarizes the key design concepts for multipole based routings inferred from the experimental observations.

1) The higher the multipole order n, the higher the cancellation in H-field as long as the threshold distance $d \gg a$, resulting in lower side-channel leakage.
2) The higher the multipole order n, the higher the strength of local fields at $d < a$. Also, a higher n would imply a higher a, thus increasing the threshold distance beyond which multipole cancellation is actually beneficial.
3) Finally, higher the multipole order n, higher the complexity of design.

An optimized n can therefore be determined depending on specific application scenarios, e.g., maintaining $n = 8$ or 16 for smaller, lower-level metal-based local power grids for sensitive IC blocks (such as a crypto block) can make sense – as smaller dimensions could allow higher-order n-poles before a becomes comparable to d. On the other hand, restricting n to 4 for larger, higher-level metal global power grids can be a good compromise both in terms of side-channel leakage and design complexity.

IV. Conclusion

In conclusion, we propose a novel routing approach for ICs, based on linear multipoles formed by current elements on metal layers. Scaled-up versions of proposed routing structures are designed for validation. Measurement results on the designed PCBs provide proof-of-concept for the proposed technique as well as intuitions for optimized implementation of multipole routings in an actual IC design.

References

[1] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, “The EM side—Channel (s),” in *Cryptographic Hardware and Embedded Systems*, B. S. Kaliski, Ç. K. Koç, and C. Paar, Eds. Berlin, Germany: Springer, 2003, pp. 29–45.

[2] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Concrete results,” in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2001, pp. 251–261.

[3] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2004, pp. 16–29.

[4] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, “Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation,” in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2015, pp. 207–228.

[5] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, “ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs,” in *Topics in Cryptology*. New York, NY, USA: Springer, 2016, pp. 219–235.

[6] S. Patranabis *et al.*, “Lightweight design-for-security strategies for combined countermeasures against side channel and fault analysis in IoT applications,” *J. Hardw. Syst. Secur.*, vol. 3, no. 2, pp. 103–131, Jun. 2019, doi: 10.1007/s41635-018-0049-y.

[7] M. A. Kf, V. Ganesan, R. Bodduna, and C. Rebeiro, “PARAM: A microprocessor hardened for power side-channel attack resistance,” in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 23–34.

[8] O. Reparaz, B. Bilgin, S. Nikova, B. Gierlichs, and I. Verbauwhede, “Consolidating masking schemes,” in *Advances in Cryptology* (Lecture Notes in Computer Science), R. Gennaro and M. Robshaw, Eds. Berlin, Germany: Springer, 2015, pp. 764–783.

[9] 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.

[10] W. Yu and S. Kose, “Exploiting voltage regulators to enhance various power attack countermeasures,” *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 2, pp. 244–257, Apr. 2018.

[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, 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.

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